FULLY EXECUTED
Contract Number: 4400014635
Original Contract Effective Date: 11/10/2015
Valid From: 04/27/2015 To: 06/06/2024

All using Agencies of the Commonwealth, Participating Political Subdivision, Authorities, Private Colleges and Universities

Your SAP Vendor Number with us: 163299

Supplier Name/Address:
UNISYS CORPORATION
UNISYS CORPORATION
4750 LINDLE RD
HARRISBURG PA 17111-2428 US

Supplier Phone Number: 770-407-1765
Supplier Fax Number: 717-526-1175

Contract Name:
Data Center (PACS)

Purchasing Agent
Name: Hosler Raeden
Phone: 717-787-4103
Fax:

Please Deliver To:

To be determined at
the time of the Purchase Order
unless specified below.

Payment Terms
NET 45 DAYS

Solicitation No.: Issuance Date:

Supplier Bid or Proposal No. (if applicable): Solicitation Submission Date:

This contract is comprised of: The above referenced Solicitation, the Supplier's Bid or Proposal, and any documents attached to this Contract or incorporated by reference.

Item	Material/Service Desc	Qty	UOM	Price	Per Unit	Total
1	PA Computing Services	0.000	Month	0.00	1	0.00

General Requirements for all Items:

Information:

Supplier's Signature _____ Title _____

Printed Name _____ Date _____

FULLY EXECUTED

Contract Number: 4400014635

Original Contract Effective Date: 11/10/2015

Valid From: 04/27/2015 To: 06/06/2024

Supplier Name:

UNISYS CORPORATION

Header Text

Contract 4400014635 is a statewide contract that will replace the existing agency contract #4400012832 for Pennsylvania Compute Services (PACS). The original contract was established as an Office of Administration agency contract which restricted the creation of purchase orders to OA only.

The replacement contract is strictly an administrative change required by SRM to provide all agencies with the ability to create purchase orders referencing the contract. No changes have been made to the contract documents.

Upon final approval of contract #4400014635, the existing agency contract #4400012832 will be deactivated.

7.20.2021 – Contract manager contact info has been updated to DGS commodity specialist Raeden Hosler. rsh

No further information for this Contract

Information:

FULLY EXECUTED
Contract Number: 4400014635
Contract Effective Date: 11/10/2015
Valid From: 04/27/2015 To: 06/06/2022

All using Agencies of the Commonwealth, Participating Political Subdivision, Authorities, Private Colleges and Universities

Your SAP Vendor Number with us: 163299

Supplier Name/Address:
UNISYS CORPORATION
UNISYS CORPORATION
PHILADELPHIA PA 19178-0001 US

Supplier Phone Number: 717-526-1187
Supplier Fax Number: 717-526-1175

Contract Name:
Data Center (PACS)

Purchasing Agent
Name: OA OIT
Phone: 717-787-5440
Fax: 717-787-4523

Please Deliver To:

To be determined at
the time of the Purchase Order
unless specified below.

Payment Terms
NET 45 DAYS

Solicitation No.: Issuance Date:

Supplier Bid or Proposal No. (if applicable): Solicitation Submission Date:

This contract is comprised of: The above referenced Solicitation, the Supplier's Bid or Proposal, and any documents attached to this Contract or incorporated by reference.

Item	Material/Service Desc	Qty	UOM	Price	Per Unit	Total
1	PA Computing Services	0.000	Each	0.00	1	0.00

General Requirements for all Items:

Header Text
Contract 4400014635 is a statewide contract that will replace the existing agency contract #4400012832 for Pennsylvania Compute Services (PACS). The original contract was established as an Office of Administration agency contract which restricted the creation of purchase orders to OA only.

The replacement contract is strictly an administrative change required by SRM to provide all agencies with the ability to create purchase orders referencing the contract. No changes have been made to the contract documents.

Upon final approval of contract #4400014635, the existing agency contract #4400012832 will be deactivated.
No further information for this Contract

Information:

Supplier's Signature _____ Title _____

Printed Name _____ Date _____

Amendment No. 1

to Contract No. 4400012832

Between

COMMONWEALTH OF PENNSYLVANIA
GOVERNOR'S OFFICE OF ADMINISTRATION

and

UNISYS CORPORATION

for

Data Center Computing Services

THIS AMENDMENT ("Amendment No. 1") is entered into by and between the Commonwealth of Pennsylvania ("Commonwealth"), acting through its Governor's Office of Administration ("OA"), and Unisys Corporation, a Delaware corporation headquartered in Blue Bell, Pennsylvania ("Contractor"), collectively referred to as the "Parties".

WITNESSETH:

WHEREAS, OA issued a Request for Proposals, RFP No. 6100022698, for data center computing services ("Services); and,

WHEREAS, on December 9, 2013, the contract resulting from the RFP (known as the Pennsylvania Compute Services Contract, hereinafter the "PACS Contract") was awarded to Contractor; and

WHEREAS, prior to the full execution of the PACS Contract, a bid protest was filed by a competing offeror; and

WHEREAS, on June 4, 2014, OA and Contractor entered into the PACS Contract, Contract No. 4400012832, with an Effective Date of June 6, 2014; and

WHEREAS, resolution of the bid protest delayed execution of the PACS Contract, thus delaying and adversely affecting the Parties' anticipated transition schedule; and

WHEREAS, the Parties now wish to amend the PACS Contract to extend the due dates for certain Transition Milestones and to extend the term by one (1) year; and

WHEREAS, Contractor will continue to provide services to the Commonwealth under its Contract #ME-98136, known as the Data Power House Contract ("DPH Contract"), during calendar year 2015 while Contractor transitions the Services to the PACS contract; and

WHEREAS, Contractor has agreed not to charge the Commonwealth under the PACS Contract for Services transitioned from the DPH Contract during calendar year 2015.

NOW THEREFORE, the Parties, intending to be legally bound, hereby agree to amend the PACS Contract as follows:

1. The above Recitals are incorporated herein by reference as a material part of the PACS Contract and this Amendment No. 1.

2. Through this Amendment No. 1, OA has exercised its option set forth in Section 1(b) of the PACS Contract to renew the PACS Contract for one (1) year. The term of the PACS Contract shall now expire on June 6, 2022 ("the Expiration Date"). Per Section 1(b) of the PACS Contract, two (2) optional renewal years remain.

3. Schedule D (Transition Milestones) of the PACS Contract is hereby deleted and replaced in its entirety with Schedule D (Transition Milestones v 2.0), attached hereto and made a part hereof as though fully set forth herein. Transition Milestone M-4.1 (Detailed Transition Plan Update) has been added and the due dates for the following Transition Milestone have been modified in the attached Schedule D (Transition Milestones v. 2.0):

   - Milestone Number M-5 (Commonwealth Compute Services Manual)
   - Milestone Number M-8 (ITSM System Integration)
   - Milestone Number M-14 (EDC Operational Transition Completed)

4. Section 20 (Fees), Subsection g., of the PACS Contract is hereby deleted and replaced in its entirety by the following:

   g. Contractor presently provides the Commonwealth services under Contract Number ME-981363 (the "DPH Contract") which, through its Amendment No. 4, has been amended to extend the termination date to December 31, 2015 at a price of $91,816,512.00. The price may be adjusted via change order. Any Time and Material Services will be billed separately. The services provided under the DPH Contract are similar to the Services to be provided under this [PACS] Contract. Commencing on the Effective Date of Amendment No. 4 of the DPH Contract and ending on December 31, 2015, Contractor shall not charge the Commonwealth under this [PACS] Contract for any Services transitioned from the DPH Contract to this [PACS] Contract.

   Contractor may charge the Commonwealth for new Services ordered by the Commonwealth under the terms of the [PACS] Contract which are unique from those provided by Contractor under the DPH Contract, commencing on the date such new Services are delivered to and accepted by the Commonwealth.

5. This Amendment No.1 to the PACS Contract is contingent on the full execution of Amendment No. 4 of the DPH Contract. This Amendment shall not become effective until Amendment No. 4 of the DPH Contract has been fully executed by the Parties.

6. All other terms and conditions of the PACS Contract not modified by this Amendment No. 1 shall remain in full force and effect.

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

IN WITNESS WHEREOF, the Parties hereto execute this Amendment No. 1 through their respective duly authorized officials on the dates indicated below.

Witness:

[redacted] 11/18/14
Signature Date

Ann M. Orner
Printed Name

Director, Client Management
Title

UNISYS CORPORATION

[redacted] 11-18-14
Signature Date

Reed Laughlin
Printed Name

Vice President
Title

SAP Vendor Number – 0006163299

COMMONWEALTH OF PENNSYLVANIA
GOVERNOR'S OFFICE OF ADMINISTRATION

[See Section 1 of PACS Contract]
Secretary

APPROVED:

[See Section 1 of PACS Contract]
Comptroller

APPROVED AS TO FORM AND LEGALITY:

[See Section 1 of PACS Contract]
Office of Chief Counsel

[See Section 1 of PACS Contract]
Office of General Counsel

[See Section 1 of PACS Contract]
Office of Attorney General

Schedule D

Transition Milestones (v 2.0)

Milestones include the completion of all tasks, deliverables and interim milestones associated with such Milestone as set forth in the Transition Plan. The Earn Back period is thirty (30) calendar days from the Transition Milestone Due Date and applies to those Milestones indicated with "Y" in the Earn Back column. The Acceptance Criteria for each Milestone includes criteria described in Schedule F and Schedule K of the contract.

Note: If a Milestone is dependent on another Milestone and the first Milestone is missed, the subsequent Milestones remain in effect. An example is: if M-3 is missed, M-5 is still enforced.

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
M-1	Key Staffing	30 calendar days from Contract Effective Date	• Key Personnel team completed per Schedule G • staffing plan approved • detailed project organizational chart approved • resumes for each key personnel listed on the team submitted • staff contingency plan approved	$50,000 One-time	N	• Commonwealth review and approval
M-2	Contract Management Plan	60 calendar days from Contract Effective Date	• Delivery and acceptance of the following Deliverables from Schedule K: o D-11.01 o D-11.02	$50,000 One-time	Y	• Commonwealth review and approval
M-3	Datacenter Architecture Plan and Roadmap	90 calendar days from Contract Effective Date	• Delivery and acceptance of the following Deliverables from Schedule K: o D-01.01 o D-01.02 (Initial Deliverable Approval) o D-01.03 (Initial Deliverable Approval) o D-01.04 (Initial Deliverable Approval) o D-01.05 (Initial Deliverable	$150,000 One-time	Y	• Commonwealth review and approval

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			Approval) o D-01.07 o D-03.01 o D-03.04 o D-03.08 o D-04.01 o D-04.05			
M-4	Detailed Transition Plan	180 calendar days from Contract Effective Date	• Completion of Data Gathering o All data gathering checklists completed, validated, reviewed and approved • Completion, submittal and acceptance of data gathering report on B2B interface to Commonwealth's ITSM system that includes interfaces for the following: o Incident Management o Change Management o Problem Management o Known Errors o Request Management o Invoicing Process • Completion and acceptance of the Detailed Transition Plan using Schedule M – Detailed Transition Plan • Delivery and acceptance of the following Deliverables from Schedule K: o D-05.01 o D-05.04 o D-05.10	$250,000 One-time	N	• Commonwealth review and approval

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			○ D-10.01 • The Detailed Transition plan must contain: ○ An **overall (master) plan** which includes but is not limited to: ▪ transition governance plan ▪ transition risk and mitigation plan ▪ due diligence timeline ▪ configuration / testing verification ▪ operational readiness ○ A **plan by Datacenter** which includes but is not limited to: ▪ transition governance plan ▪ transition risk and mitigation plan ▪ due diligence timeline ▪ configuration / testing verification ▪ operational readiness ○ A **plan by Agency** which includes but is not limited to: ▪ transition governance plan ▪ transition risk and mitigation plan ▪ due diligence timeline ▪ configuration / testing verification ▪ operational readiness ○ A **plan by Application** which includes but is not limited to:			

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			▪ transition governance plan ▪ transition risk and mitigation plan ▪ due diligence timeline ▪ configuration / testing verification ▪ operational readiness			
M-4.1	Detailed Transition Plan Update	May 1, 2015	• Completion of updates to the Detailed Transition Plan that account for the transition of services in the EDC to fully-managed. o All acceptance criteria of Transition Milestone M-4 apply. • Updates to the Detailed Transition Plan are required by Amendment No. 1 to the Contract which extended the Transition Milestone Due Date for M-14 (EDC Operational Transition Completed).	$10,000 One-time	N	• Commonwealth review and approval
M-5	Commonwealth Compute Process Manual (CCPM)	270 calendar days from Contract Effective Date	• Delivery and acceptance of the following Deliverables from Schedule K: o D-02.01 o D-02.04 o D-02.09 o D-02.15 o D-02.17 o D-02.18 o D-02.23 o D-02.26 o D-02.29	$75,000 One-time	Y	• Commonwealth review and approval

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			○ D-02.32 ○ D-02.37 ○ D-02.42 ○ D-02.47 ○ D-02.52 ○ D-02.57 ○ D-02.62 ○ D-02.67 ○ D-02.70 ○ D-02.75 ○ D-02.81 • Completion and Acceptance of final CCPM as listed within Schedule L of this contract. This includes but is not limited to: ○ Incident (including Security) ○ Problem ○ Change ○ Order/Request ○ Billing ○ Service Level			
M-6	Network Connectivity	120 calendar days from Contract Effective Date	• Completion and Acceptance of the Network Connectivity to the Commonwealth	$250,000 One-time	N	• Commonwealth review, testing and approval
M-7	Security	180 calendar days from Contract Effective	• Completion and acceptance of security architecture, solution, policies and procedures which included but is not limited to:	$250,000 One-time	N	• Commonwealth review and approval

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
		Date	○ Delivery and acceptance of the following Deliverables from Schedule K: ▪ D-07.01 ▪ D-07.06 ▪ D-01.03 (Initial Deliverable Approval) ▪ D-09.01 ▪ D-09.02 ○ Implement security management plan ○ Implement security and firewall plan ○ Policies and procedures are in place for physical security ○ Policies and procedures are in place for data and network security ○ Policies and procedures are in place for personnel security, such as annual background checks ○ Security assessment is conducted to ensure data safety and confidentiality			
M-8	ITSM System Integration	270 calendar days from Contract Effective Date	• Completion and Acceptance of Integration between Commonwealth's ITSM system and Offeror's ITSM System including but is not limited to: ○ Incident connectivity has been tested and incidents created and updated on either side flow back and forth between systems ○ Problem connectivity has been tested and problems created and	$100,000 One-time	Y	• Commonwealth review and approval

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			updated on either side flow back and forth between systems o Change requests connectivity has been tested and requests created and updated on either side flow back and forth between systems o Configuration items in both system CMDBs are reconciled o Test Invoices have been processed through the ITSM system to the Commonwealth's AP system o Reporting from Offeror's ITSM system is available to Commonwealth			
M-9	Financial Management	180 calendar days from Contract Effective Date	• Completion and acceptance of billing process and form of invoice approved • Schedule K Deliverable D-02.01 completed • Process implemented, tested and accepted providing an enterprise bill providing the details required by the Commonwealth	$75,000 One-time	Y	• Commonwealth review and approval
M-10	Operational Readiness	240 calendar days from Contract Effective Date	• Completion and acceptance of an Operational Readiness Report indicating Offeror is "Ready" to transition the Commonwealth's Applications and Services to other Datacenters. This report must include but is not limited to the following: o Delivery and acceptance of the following Deliverables from	$150,000 One-time	N	• Commonwealth review and approval

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			Schedule K: ▪ D-01.01 ▪ D-01.02 ▪ D-01.03 ▪ D-01.04 ▪ D-01.05 ▪ D-01.06 ▪ D-01.07 o Transition Project Office established and fully staffed o Program plan and architecture developed and approved by the Commonwealth o Processes and Tools implemented to support the transition change control, schedule, quality, communications, risk and issue management o Datacenter environment configured , tested and acceptance			
M-11	SSAE 16 Audits of EDC	On the July 31st following the Commonwealth's acceptance of Milestone M-14	• Completion and Issuance of a SSAE-16 Audit Reports as detailed with the Appendix A (Terms and Conditions) on the Commonwealth's EDC Datacenter • Schedule K Deliverable D-08.02	$100,000 One-time	Y	• Commonwealth review and approval
M-12	DPH Transition Completed (1)	18 months from	• Completion and acceptance of ALL applications transitioned from the DPH	$2,500,000 per month or	N	• Commonwealth review and approval of work product

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
		Contract Effective Date	to new Datacenters which includes but is not limited to the following for each application: o High availability, backup and DR are operational for identified systems. o CCPM specific details for application are available in KMP. o Operations dashboards to report immediately on status and alerts for transitioned applications. o Service Level agreements are identified and supporting metrics in place. o System operational for scheduling and tracking of ticket-based tasks and incidents. o System is available to begin data collection to produce configuration, monitoring and management status reports. o Systems with DR plans have an updated DR plan and test scheduled. o Operational support assumed and workloads migrated. • High-Speed direct link to current DPH location is disconnected. • Signoff that all Services provided by DPH have been successfully transitioned	partial month for six (6) months		plus assisting in data gathering, planning, ordering, implementing, testing and accepting the transition of the applications
M-13	DPH Transition Completed (2)	24 months from Contract Effective Date	• Completion and acceptance of ALL applications transitioned from the DPH to new Datacenters which includes but is not limited to: o High availability, backup and DR are operational for identified systems.	$5,000,000 per month or partial month	N	• Commonwealth review and approval of work product plus assisting in data gathering, planning, ordering, implementing,

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			○ CCPM contains specific details for apps transitioned are available in KMP. ○ Operations dashboards are in place to report immediately on status and alerts for transitioned apps. ○ Service Level agreements have been identified and supporting metrics in place. ○ System is operational for scheduling and tracking of ticket-based tasks and incidents. ○ System available to begin data collection in order to produce configuration, monitoring and management status reports. ○ Systems with DR plans have a replacement plan and test scheduled. ○ Operational support has been assumed and workloads migrated. ○ High-Speed direct link to current DPH location is disconnected. ○ Signoff that all Services provided by DPH have been successfully transitioned			testing and accepting the transition of the applications
M-14	EDC Operational Transition Completed	07/1/2016	• Completion and acceptance of operational control and support of the EDC which includes but is not limited to the following: ○ Schedule K deliverable D-01 ○ Schedule K deliverable D-08.01 ○ Schedule K deliverable D-08.06 ○ Verification CMDB of record with Offeror's configuration info includes EDC assets and CI's	$100,000 per month or partial month	N	• Commonwealth review and approval of work product plus assisting in data gathering, planning, ordering, implementing, testing and accepting the transition of the applications

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			○ Service catalogs, processes, and procedures are transitioned ○ Multi environments/instances are available for identified systems ○ High availability, backup and DR are operational for identified system ○ CCPM specific details for applications are available in KMP. ○ Operations dashboards are in place to report immediately on status and alerts for apps ○ Service Level agreements have been identified and supporting metrics in place ○ System is operational for scheduling and tracking of ticket-based tasks and incidents ○ System is available to begin data collection in order to produce configuration, monitoring and management status reports ○ Transition orders completed and accepted by the Commonwealth			
M-15	Department of Labor and Industry Datacenter Transition Completed	30 months from Contract Effective Date	• Completion and acceptance of ALL applications transitioned from the DLI Datacenter to new Datacenters which includes but is not limited to the following: ○ Service catalogs, processes and procedures fully established, documented and approved ○ Multi environments and instances are fully functional for transitioned systems ○ High availability, backup and DR are	$1,000 000 One-time	N	• Commonwealth review and approval of work product plus assisting in data gathering, planning, ordering, implementing, testing and accepting the transition of the applications

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			operational for transitioned systems o CCPM contains specific details for apps transitioned are available in KMP o Operations dashboards are in place to report immediately on status and alerts for transitioned apps o Service Level agreements have been identified and supporting metrics in place o System is operational for scheduling and tracking of ticket-based tasks and incidents o System available to begin data collection in order to produce configuration, monitoring and management status reports o Transition orders completed and accepted by the Commonwealth			
M-16	Department of Revenue Datacenter Transition Completed	30 months from Contract Effective Date	• Completion and acceptance of ALL applications transitioned from the DOR Datacenter to new Datacenters which includes but is not limited to the following: o Service catalogs, processes and procedures fully established, documented and approved o Multi environments and instances are fully functional for transitioned systems o High availability, backup and DR are operational for transitioned systems o CCPM contains specific details for applications transitioned are available in KMP o Operations dashboards are in place to	$1,000,000 One-time	N	• Commonwealth review and approval of work product plus assisting in data gathering, planning, ordering, implementing, testing and accepting the transition of the applications

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			report immediately on status and alerts for transitioned apps o Service Level agreements have been identified and supporting metrics in place o System is operational for scheduling and tracking of ticket-based tasks and incidents o System available to begin data collection in order to produce configuration, monitoring and management status reports o Transition orders completed and accepted by the Commonwealth			
M-17	Pennsylvania State Police Datacenter Transition Completed	30 months from Contract Effective Date	• Completion and acceptance of ALL applications transitioned from the PSP Datacenter to new Datacenters which includes but is not limited to the following: o Service catalogs, processes and procedures fully established, documented and approved o Multi environments and instances are fully functional for transitioned systems o High availability, backup and DR are operational for transitioned systems o CCPM contains specific details for applications transitioned are available in KMP o Operations dashboards are in place to report immediately on status and alerts for transitioned apps o Service Level agreements have been identified and supporting metrics in	$1,000,000 One-time	N	• Commonwealth review and approval of work product plus assisting in data gathering, planning, ordering, implementing, testing and accepting the transition of the applications

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			place o System is operational for scheduling and tracking of ticket-based tasks and incidents o System available to begin data collection in order to produce configuration, monitoring and management status reports o Transition orders completed and accepted by the Commonwealth			
M-18	Department of Public Welfare Datacenter Transition Completed	30 months from Contract Effective Date	• Completion and acceptance of ALL applications transitioned from the DPW Datacenter to new Datacenters which includes but is not limited to the following: o Service catalogs, processes and procedures fully established, documented and approved o Multi environments and instances are fully functional for transitioned systems o High availability, backup and DR are operational for transitioned systems o CCPM contains specific details for apps transitioned are available in KMP o Operations dashboards are in place to report immediately on status and alerts for transitioned apps o Service Level agreements have been identified and supporting metrics in place o System is operational for scheduling and tracking of ticket-based tasks and incidents o System available to begin data	$1,000,000 One-time	N	• Commonwealth review and approval of work product plus assisting in data gathering, planning, ordering, implementing, testing and accepting the transition of the applications

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			collection in order to produce configuration, monitoring and management status reports o Transition orders completed and accepted by the Commonwealth			
M-19	Department of Health Datacenter Transition Completed	30 months from Contract Effective Date	• Completion and acceptance of ALL applications transitioned from the DOH Datacenter to new Datacenters which includes but is not limited to the following: o Service catalogs, processes and procedures fully established, documented and approved o Multi environments and instances are fully functional for transitioned systems o High availability, backup and DR are operational for transitioned systems o CCPM contains specific details for apps transitioned are available in KMP o Operations dashboards are in place to report immediately on status and alerts for transitioned apps o Service Level agreements have been identified and supporting metrics in place o System is operational for scheduling and tracking of ticket-based tasks and incidents o System available to begin data collection in order to produce configuration, monitoring and management status reports o Transition orders completed and accepted by the Commonwealth	$1,000,000 One-time	N	• Commonwealth review and approval of work product plus assisting in data gathering, planning, ordering, implementing, testing and accepting the transition of the applications

Amendment No. 2

to Contract No. 4400012832

Between

COMMONWEALTH OF PENNSYLVANIA
GOVERNOR'S OFFICE OF ADMINISTRATION

and

UNISYS CORPORATION

for

DATA CENTER COMPUTING SERVICES

THIS AMENDMENT ("Amendment No. 2") to Contract No. **4400012832** is entered into by and between the Commonwealth of Pennsylvania ("Commonwealth"), acting through its Governor's Office of Administration ("OA"), and Unisys Corporation, a Delaware corporation headquartered in Blue Bell, Pennsylvania ("Contractor"), collectively referred to as the "Parties."

WITNESSETH:

WHEREAS, OA issued a Request for Proposals, RFP No. 6100022698, for data center computing services ("Services); and,

WHEREAS, on December 9, 2013, the contract resulting from the RFP (known as the Pennsylvania Compute Services Contract, hereinafter the "PACS Contract") was awarded to Contractor; and

WHEREAS, on June 4, 2014, OA and Contractor entered into the PACS Contract, Contract No. 4400012832, with an Effective Date of June 6, 2014; and

WHEREAS, on December 12, 2014, the Parties amended the PACS Contract through Amendment No. 1 to extend the term, revise certain Transition Milestones, and state that the Commonwealth will not pay for services transitioned from the Data Power House Contract (Number ME-981363) for calendar year 2015; and

WHEREAS, the Parties now wish to further amend the PACS Contract to require Contractor to submit invoices directly to each Commonwealth agency for Services rendered rather than submitting a single invoice to OA and to revise a Transition Milestone due date; and

WHEREAS, OA must recreate the PACS Contract in its electronic contract processing system in order for individual Commonwealth agencies to issue purchase orders and make payments to Contractor; and

WHEREAS, as a result of this strictly administrative change to the PACS Contract, a new contract number has been assigned to the PACS Contract;

WHEREAS, the new PACS Contract Number is **4400014635**; and

WHEREAS, other than as set forth in this Amendment No. 2, no terms or conditions of the PACS Contract were modified when the new PACS Contract number was created.

NOW THEREFORE, the Parties, intending to be legally bound, hereby agree to amend the PACS Contract as follows:

1. The above Recitals are incorporated herein by reference as a material part of the PACS Contract and this Amendment No. 2.

2. Section 2 (PURCHASE ORDERS) of the PACS Contract is hereby deleted and replaced in its entirety by the following:

    a. The Commonwealth Agencies will issue Purchase Orders against the Contract. These orders constitute the Contractor's authority to make delivery. All Purchase Orders received by the Contractor up to and including the Expiration Date of the Contract are acceptable and must be performed in accordance with the Contract. Contractors are not permitted to accept Purchase Orders which require performance in excess of those performance time periods specified in the Contract. Each Purchase Order will be deemed to incorporate the terms and conditions set forth in the Contract.

    b. Purchase Orders will not include an ink signature by the Commonwealth Agencies. The electronically-printed name of the purchaser represents the signature of the individual who has the authority, on behalf of the Commonwealth Agency, to authorize the Contractor to proceed.

    c. Purchase Orders may be issued electronically. The electronic transmission of a Purchase Order shall require acknowledgement of receipt of the transmission by the Contractor.

    d. Contractor's acknowledgment of receipt of the electronic transmission of the Purchase Order shall constitute receipt of an order.

    e. Purchase Orders received by the Contractor after 4:00 p.m. will be considered received the following business day.

f. The Commonwealth and the Contractor specifically agree as follows:

(1) No handwritten signature shall be required in order for the Contract or Purchase Order to be legally enforceable.

(2) Upon receipt of a Purchase Order, the Contractor shall promptly and properly transmit an acknowledgement in return. Any order which is issued electronically shall not give rise to any obligation to deliver on the part of the Contractor, or any obligation to receive and pay for delivered products on the part of the Commonwealth Agency, unless and until the Commonwealth Agency transmitting the order has properly received an acknowledgement.

(3) The parties agree that no writing shall be required in order to make the Purchase Order legally binding. The parties hereby agree not to contest the validity or enforceability of the Contract or a genuine Purchase Order or acknowledgement that has been issued electronically under the provisions of a statute of frauds or any other applicable law relating to whether certain agreements shall be in writing and signed by the party bound thereby. The Contract and any genuine Purchase Order or acknowledgement issued electronically, if introduced as evidence on paper in any judicial, arbitration, mediation, or administrative proceedings, will be admissible as between the parties to the same extent and under the same conditions as other business records originated and maintained in documentary form. Neither party shall contest the admissibility of copies of the Contract or any genuine Purchase Order or acknowledgements under either the business records exception to the hearsay rule or the best evidence rule on the basis that the Contract or Purchase Order or acknowledgement were not in writing or signed by the parties. A Purchase Order or acknowledgment shall be deemed to be genuine for all purposes if it is transmitted to the location designated for such documents.

(4) Each party will immediately take steps to verify any document that appears to be obviously garbled in transmission or improperly formatted to include re-transmission of any such document if necessary.

3. Section 21 (PAYMENT SCHEDULE AND INVOICES) of the PACS Contract is hereby deleted and replaced in its entirety by the following:

a. **Service Fees**. On or before the 15th day of each calendar month of the Term, Contractor shall provide each Commonwealth Agency with an invoice, or multiple invoices as required, for applicable Service Fees based on the associated approved Purchase Order(s). Each such invoice shall include the Fees for the

prior month. Service Level Credits then payable by Contractor to the Commonwealth Agency or refundable by the Commonwealth Agency to the Contractor will be issued on a separate invoice via a .pdf document.

b. **Detailed Invoices.** Contractor shall provide on the monthly invoices varying degrees of detail (e.g., per Agency, end-user, department, project, site) as specified in *Schedule H* (Commonwealth Computing Procedures Manual). The detailed invoices must be delivered in an electronic format compatible with the Commonwealth's Invoice Processing System. An Invoice Summary that includes all charges detailed on the monthly invoices sent to Commonwealth Agencies, and any additional detail as specified in *Schedule H* (Commonwealth Computing Procedures Manual) must be delivered to OA each month for management, budgeting, and SLA calculation purposes.

c. **Time of Payment**. Any sum due Contractor pursuant to any such invoice shall be due and payable on the last business day of the calendar month following the calendar month during which such invoice was delivered to Commonwealth Agency. (e.g., an invoice delivered to Commonwealth on July 15, 2015 will be due and payable on August 31, 2015, the last business day of August, 2015.). In the event any invoices remain unpaid after such due date, the Commonwealth may pay interest as determined by the Secretary of Budget in accordance with Act No. 266 of 1982 and regulations promulgated pursuant thereto. Contractor shall, subject to Section 32(f) of this Contract, continue to provide the Services even in the event payment is delayed or is not made in timely fashion.

d. **Fee Dispute**. During the pendency of a dispute between a Commonwealth Agency and Contractor pursuant to which a Commonwealth Agency, in good faith, believes it is entitled to withhold, and does withhold, payment, Contractor shall continue to fully provide the Services and otherwise fully perform its obligations under this Contract. Notwithstanding the foregoing, the Commonwealth will not withhold more than twenty-five percent (25%) of the total of any monthly Invoice Summary.

4. The following definitions in *Schedule A (Definitions)* are hereby deleted and replaced in their entirety:

At-Risk Amount - The amount that the Contractor will have at risk for all Service Level Credits in each month. The "At-Risk Amount" is 15% of the sum of all monthly invoices submitted to Commonwealth Agencies, as detailed in the Invoice Summary.

Contract Year – Contract Year 1 is June 6, 2014 – June 30, 2015. Each subsequent year aligns with Commonwealth fiscal year except for last year of contract which will end June 5 of the applicable year.

5. The following definition has been added to *Schedule A (Definitions)*:

Invoice Summary - A monthly report submitted by Contractor to the Commonwealth Office of Administration that includes all charges detailed on the monthly invoices sent to Commonwealth Agencies, and any additional detail as specified in *Schedule H* (Commonwealth Computing Procedures Manual).

6. Schedule D (Transition Milestones 2.0) of the PACS Contract is hereby deleted and replaced in its entirety with Schedule D (Transition Milestones v 3.0), attached hereto and made a part hereof as though fully set forth herein. The Due Date for Transition Milestone M-12 (DPH Transition Completed (1)) has been changed in the attached Schedule D (Transition Milestones v. 3.0) to December 31, 2015.

7. This Amendment No.2 to the PACS Contract is contingent on the full execution of a Contract Change Request for the SAP Implementation of the Project. This Amendment shall not become effective until the Contract Change Request for the SAP Implementation of the Project has been fully executed by the Parties.

8. All other terms and conditions of the PACS Contract not modified by this Amendment No. 2 shall remain in full force and effect.

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

IN WITNESS WHEREOF, the Parties hereto execute this Amendment No. 2 through their respective duly authorized officials on the dates indicated below.

Witness:

[redacted] 10/19/15
Signature Date

Rita S. Spicher
Printed Name

Contract Compliance Manager
Title

UNISYS CORPORATION

[redacted] 10/19/2015
Signature Date

Reed Laughlin
Printed Name

Vice President
Title

SAP Vendor Number – 000163299

COMMONWEALTH OF PENNSYLVANIA
GOVERNOR'S OFFICE OF ADMINISTRATION

[See Section 1 of PACS Contract]
Secretary

APPROVED:

[See Section 1 of PACS Contract]
Comptroller

APPROVED AS TO FORM AND LEGALITY:

[See Section 1 of PACS Contract]
Office of Chief Counsel

[See Section 1 of PACS Contract]
Office of General Counsel

[See Section 1 of PACS Contract]
Office of Attorney General

Schedule D

Transition Milestones (v 3.0)

Milestones include the completion of all tasks, deliverables and interim milestones associated with such Milestone as set forth in the Transition Plan. The Earn Back period is thirty (30) calendar days from the Transition Milestone Due Date and applies to those Milestones indicated with "Y" in the Earn Back column. The Acceptance Criteria for each Milestone includes criteria described in Schedule F and Schedule K of the contract.

Note: If a Milestone is dependent on another Milestone and the first Milestone is missed, the subsequent Milestones remain in effect. An example is: if M-3 is missed, M-5 is still enforced.

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
M-1	Key Staffing	30 calendar days from Contract Effective Date	• Key Personnel team completed per Schedule G • staffing plan approved • detailed project organizational chart approved • resumes for each key personnel listed on the team submitted • staff contingency plan approved	$50,000 One-time	N	• Commonwealth review and approval
M-2	Contract Management Plan	60 calendar days from Contract Effective Date	• Delivery and acceptance of the following Deliverables from Schedule K: o D-11.01 o D-11.02	$50,000 One-time	Y	• Commonwealth review and approval
M-3	Datacenter Architecture Plan and Roadmap	90 calendar days from Contract Effective Date	• Delivery and acceptance of the following Deliverables from Schedule K: o D-01.01 o D-01.02 (Initial Deliverable Approval) o D-01.03 (Initial Deliverable Approval) o D-01.04 (Initial Deliverable Approval) o D-01.05 (Initial Deliverable	$150,000 One-time	Y	• Commonwealth review and approval

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			Approval) o D-01.07 o D-03.01 o D-03.04 o D-03.08 o D-04.01 o D-04.05			
M-4	Detailed Transition Plan	180 calendar days from Contract Effective Date	• Completion of Data Gathering o All data gathering checklists completed, validated, reviewed and approved • Completion, submittal and acceptance of data gathering report on B2B interface to Commonwealth's ITSM system that includes interfaces for the following: o Incident Management o Change Management o Problem Management o Known Errors o Request Management o Invoicing Process • Completion and acceptance of the Detailed Transition Plan using Schedule M – Detailed Transition Plan • Delivery and acceptance of the following Deliverables from Schedule K: o D-05.01 o D-05.04 o D-05.10	$250,000 One-time	N	• Commonwealth review and approval

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			○ D-10.01 • The Detailed Transition plan must contain: ○ An **overall (master) plan** which includes but is not limited to: ▪ transition governance plan ▪ transition risk and mitigation plan ▪ due diligence timeline ▪ configuration / testing verification ▪ operational readiness ○ A **plan by Datacenter** which includes but is not limited to: ▪ transition governance plan ▪ transition risk and mitigation plan ▪ due diligence timeline ▪ configuration / testing verification ▪ operational readiness ○ A **plan by Agency** which includes but is not limited to: ▪ transition governance plan ▪ transition risk and mitigation plan ▪ due diligence timeline ▪ configuration / testing verification ▪ operational readiness ○ A **plan by Application** which includes but is not limited to:			

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			▪ transition governance plan ▪ transition risk and mitigation plan ▪ due diligence timeline ▪ configuration / testing verification ▪ operational readiness			
M-4.1	Detailed Transition Plan Update	May 1, 2015	• Completion of updates to the Detailed Transition Plan that account for the transition of services in the EDC to fully-managed. o All acceptance criteria of Transition Milestone M-4 apply. • Updates to the Detailed Transition Plan are required by Amendment No. 1 to the Contract which extended the Transition Milestone Due Date for M-14 (EDC Operational Transition Completed).	$10,000 One-time	N	• Commonwealth review and approval
M-5	Commonwealth Compute Process Manual (CCPM)	270 calendar days from Contract Effective Date	• Delivery and acceptance of the following Deliverables from Schedule K: o D-02.01 o D-02.04 o D-02.09 o D-02.15 o D-02.17 o D-02.18 o D-02.23 o D-02.26 o D-02.29	$75,000 One-time	Y	• Commonwealth review and approval

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			○ D-02.32 ○ D-02.37 ○ D-02.42 ○ D-02.47 ○ D-02.52 ○ D-02.57 ○ D-02.62 ○ D-02.67 ○ D-02.70 ○ D-02.75 ○ D-02.81 • Completion and Acceptance of final CCPM as listed within Schedule L of this contract. This includes but is not limited to: ○ Incident (including Security) ○ Problem ○ Change ○ Order/Request ○ Billing ○ Service Level			
M-6	Network Connectivity	120 calendar days from Contract Effective Date	• Completion and Acceptance of the Network Connectivity to the Commonwealth	$250,000 One-time	N	• Commonwealth review, testing and approval
M-7	Security	180 calendar days from Contract Effective	• Completion and acceptance of security architecture, solution, policies and procedures which included but is not limited to:	$250,000 One-time	N	• Commonwealth review and approval

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
		Date	○ Delivery and acceptance of the following Deliverables from Schedule K: ▪ D-07.01 ▪ D-07.06 ▪ D-01.03 (Initial Deliverable Approval) ▪ D-09.01 ▪ D-09.02 ○ Implement security management plan ○ Implement security and firewall plan ○ Policies and procedures are in place for physical security ○ Policies and procedures are in place for data and network security ○ Policies and procedures are in place for personnel security, such as annual background checks ○ Security assessment is conducted to ensure data safety and confidentiality			
M-8	ITSM System Integration	270 calendar days from Contract Effective Date	• Completion and Acceptance of Integration between Commonwealth's ITSM system and Offeror's ITSM System including but is not limited to: ○ Incident connectivity has been tested and incidents created and updated on either side flow back and forth between systems ○ Problem connectivity has been tested and problems created and	$100,000 One-time	Y	• Commonwealth review and approval

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			updated on either side flow back and forth between systems o Change requests connectivity has been tested and requests created and updated on either side flow back and forth between systems o Configuration items in both system CMDBs are reconciled o Test Invoices have been processed through the ITSM system to the Commonwealth's AP system o Reporting from Offeror's ITSM system is available to Commonwealth			
M-9	Financial Management	180 calendar days from Contract Effective Date	• Completion and acceptance of billing process and form of invoice approved • Schedule K Deliverable D-02.01 completed • Process implemented, tested and accepted providing an enterprise bill providing the details required by the Commonwealth	$75,000 One-time	Y	• Commonwealth review and approval
M-10	Operational Readiness	240 calendar days from Contract Effective Date	• Completion and acceptance of an Operational Readiness Report indicating Offeror is "Ready" to transition the Commonwealth's Applications and Services to other Datacenters. This report must include but is not limited to the following: o Delivery and acceptance of the following Deliverables from	$150,000 One-time	N	• Commonwealth review and approval

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			Schedule K: ▪ D-01.01 ▪ D-01.02 ▪ D-01.03 ▪ D-01.04 ▪ D-01.05 ▪ D-01.06 ▪ D-01.07 o Transition Project Office established and fully staffed o Program plan and architecture developed and approved by the Commonwealth o Processes and Tools implemented to support the transition change control, schedule, quality, communications, risk and issue management o Datacenter environment configured , tested and acceptance			
M-11	SSAE 16 Audits of EDC	On the July 31st following the Commonwealth's acceptance of Milestone M-14	• Completion and Issuance of a SSAE-16 Audit Reports as detailed with the Appendix A (Terms and Conditions) on the Commonwealth's EDC Datacenter • Schedule K Deliverable D-08.02	$100,000 One-time	Y	• Commonwealth review and approval
M-12	DPH Transition Completed (1)	December 31, 2015	• Completion and acceptance of ALL applications transitioned from the DPH	$2,500,000 per month or	N	• Commonwealth review and approval of work product

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			to new Datacenters which includes but is not limited to the following for each application: o High availability, backup and DR are operational for identified systems. o CCPM specific details for application are available in KMP. o Operations dashboards to report immediately on status and alerts for transitioned applications. o Service Level agreements are identified and supporting metrics in place. o System operational for scheduling and tracking of ticket-based tasks and incidents. o System is available to begin data collection to produce configuration, monitoring and management status reports. o Systems with DR plans have an updated DR plan and test scheduled. o Operational support assumed and workloads migrated. • High-Speed direct link to current DPH location is disconnected. • Signoff that all Services provided by DPH have been successfully transitioned	partial month for six (6) months		plus assisting in data gathering, planning, ordering, implementing, testing and accepting the transition of the applications
M-13	DPH Transition Completed (2)	24 months from Contract Effective Date	• Completion and acceptance of ALL applications transitioned from the DPH to new Datacenters which includes but is not limited to: o High availability, backup and DR are operational for identified systems.	$5,000,000 per month or partial month	N	• Commonwealth review and approval of work product plus assisting in data gathering, planning, ordering, implementing,

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			○ CCPM contains specific details for apps transitioned are available in KMP. ○ Operations dashboards are in place to report immediately on status and alerts for transitioned apps. ○ Service Level agreements have been identified and supporting metrics in place. ○ System is operational for scheduling and tracking of ticket-based tasks and incidents. ○ System available to begin data collection in order to produce configuration, monitoring and management status reports. ○ Systems with DR plans have a replacement plan and test scheduled. ○ Operational support has been assumed and workloads migrated. ○ High-Speed direct link to current DPH location is disconnected. ○ Signoff that all Services provided by DPH have been successfully transitioned			testing and accepting the transition of the applications
M-14	EDC Operational Transition Completed	07/1/2016	• Completion and acceptance of operational control and support of the EDC which includes but is not limited to the following: ○ Schedule K deliverable D-01 ○ Schedule K deliverable D-08.01 ○ Schedule K deliverable D-08.06 ○ Verification CMDB of record with Offeror's configuration info includes EDC assets and CI's	$100,000 per month or partial month	N	• Commonwealth review and approval of work product plus assisting in data gathering, planning, ordering, implementing, testing and accepting the transition of the applications

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			○ Service catalogs, processes, and procedures are transitioned ○ Multi environments/instances are available for identified systems ○ High availability, backup and DR are operational for identified system ○ CCPM specific details for applications are available in KMP. ○ Operations dashboards are in place to report immediately on status and alerts for apps ○ Service Level agreements have been identified and supporting metrics in place ○ System is operational for scheduling and tracking of ticket-based tasks and incidents ○ System is available to begin data collection in order to produce configuration, monitoring and management status reports ○ Transition orders completed and accepted by the Commonwealth			
M-15	Department of Labor and Industry Datacenter Transition Completed	30 months from Contract Effective Date	• Completion and acceptance of ALL applications transitioned from the DLI Datacenter to new Datacenters which includes but is not limited to the following: ○ Service catalogs, processes and procedures fully established, documented and approved ○ Multi environments and instances are fully functional for transitioned systems ○ High availability, backup and DR are	$1,000 000 One-time	N	• Commonwealth review and approval of work product plus assisting in data gathering, planning, ordering, implementing, testing and accepting the transition of the applications

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			operational for transitioned systems o CCPM contains specific details for apps transitioned are available in KMP o Operations dashboards are in place to report immediately on status and alerts for transitioned apps o Service Level agreements have been identified and supporting metrics in place o System is operational for scheduling and tracking of ticket-based tasks and incidents o System available to begin data collection in order to produce configuration, monitoring and management status reports o Transition orders completed and accepted by the Commonwealth			
M-16	Department of Revenue Datacenter Transition Completed	30 months from Contract Effective Date	• Completion and acceptance of ALL applications transitioned from the DOR Datacenter to new Datacenters which includes but is not limited to the following: o Service catalogs, processes and procedures fully established, documented and approved o Multi environments and instances are fully functional for transitioned systems o High availability, backup and DR are operational for transitioned systems o CCPM contains specific details for applications transitioned are available in KMP o Operations dashboards are in place to	$1,000,000 One-time	N	• Commonwealth review and approval of work product plus assisting in data gathering, planning, ordering, implementing, testing and accepting the transition of the applications

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			report immediately on status and alerts for transitioned apps o Service Level agreements have been identified and supporting metrics in place o System is operational for scheduling and tracking of ticket-based tasks and incidents o System available to begin data collection in order to produce configuration, monitoring and management status reports o Transition orders completed and accepted by the Commonwealth			
M-17	Pennsylvania State Police Datacenter Transition Completed	30 months from Contract Effective Date	• Completion and acceptance of ALL applications transitioned from the PSP Datacenter to new Datacenters which includes but is not limited to the following: o Service catalogs, processes and procedures fully established, documented and approved o Multi environments and instances are fully functional for transitioned systems o High availability, backup and DR are operational for transitioned systems o CCPM contains specific details for applications transitioned are available in KMP o Operations dashboards are in place to report immediately on status and alerts for transitioned apps o Service Level agreements have been identified and supporting metrics in	$1,000,000 One-time	N	• Commonwealth review and approval of work product plus assisting in data gathering, planning, ordering, implementing, testing and accepting the transition of the applications

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			place o System is operational for scheduling and tracking of ticket-based tasks and incidents o System available to begin data collection in order to produce configuration, monitoring and management status reports o Transition orders completed and accepted by the Commonwealth			
M-18	Department of Public Welfare Datacenter Transition Completed	30 months from Contract Effective Date	• Completion and acceptance of ALL applications transitioned from the DPW Datacenter to new Datacenters which includes but is not limited to the following: o Service catalogs, processes and procedures fully established, documented and approved o Multi environments and instances are fully functional for transitioned systems o High availability, backup and DR are operational for transitioned systems o CCPM contains specific details for apps transitioned are available in KMP o Operations dashboards are in place to report immediately on status and alerts for transitioned apps o Service Level agreements have been identified and supporting metrics in place o System is operational for scheduling and tracking of ticket-based tasks and incidents o System available to begin data	$1,000,000 One-time	N	• Commonwealth review and approval of work product plus assisting in data gathering, planning, ordering, implementing, testing and accepting the transition of the applications

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			collection in order to produce configuration, monitoring and management status reports o Transition orders completed and accepted by the Commonwealth			
M-19	Department of Health Datacenter Transition Completed	30 months from Contract Effective Date	• Completion and acceptance of ALL applications transitioned from the DOH Datacenter to new Datacenters which includes but is not limited to the following: o Service catalogs, processes and procedures fully established, documented and approved o Multi environments and instances are fully functional for transitioned systems o High availability, backup and DR are operational for transitioned systems o CCPM contains specific details for apps transitioned are available in KMP o Operations dashboards are in place to report immediately on status and alerts for transitioned apps o Service Level agreements have been identified and supporting metrics in place o System is operational for scheduling and tracking of ticket-based tasks and incidents o System available to begin data collection in order to produce configuration, monitoring and management status reports o Transition orders completed and accepted by the Commonwealth	$1,000,000 One-time	N	• Commonwealth review and approval of work product plus assisting in data gathering, planning, ordering, implementing, testing and accepting the transition of the applications

CERTIFIED COPY OF RESOLUTIONS
of the
BOARD OF DIRECTORS
of
UNISYS CORPORATION

I, Susan B. Asch, Assistant Secretary of Unisys Corporation, a Delaware corporation, do hereby certify that the following is a true and correct copy of resolutions duly adopted at a regular meeting of the Board of Directors of said Corporation held on September 27, 1990, which on the date hereof remain in full force and effect:

Bids, Proposals, and Contracts:

RESOLVED, that the officers of the Corporation at the level of elected Vice President or above be, and each of them hereby is, authorized and empowered, in the name and on behalf of the Corporation, to make, execute, enter into and deliver bids, proposals and contracts for the selling, leasing, licensing, supplying, performing, and delivering of computer products (including, without limitation, hardware and system software incorporated therein, application software, parts and supplies), systems and other services, other products and goods of the Corporation (whether or not manufactured or developed by the Corporation or others) to any customer, governmental or otherwise; and further

RESOLVED, that the officers of the Corporation above the level of elected Vice President be, and each of them hereby is, authorized and empowered, in the name and on behalf of the Corporation, to delegate the authority granted by the foregoing resolution to additional officers and/or employees of the Corporation, or to revoke any such delegation previously granted, which delegation, or revocation thereof, shall become effective when it is filed in writing with the Secretary of the Corporation; and further

RESOLVED, that the Secretary or any Assistant Secretary of the Corporation be, and each of them hereby is, authorized and empowered to certify, to any entity or person, the authority granted to any officer or employee of the Corporation pursuant to the foregoing resolutions, with such certification constituting conclusive evidence, binding upon the Corporation, of the authority of such officer or employee to make, execute, enter into or deliver the bids, proposals or contracts referred to in the foregoing resolutions.

I further certify that, on the date hereof, J. Edward Coleman is the duly elected Chairman and Chief Executive Officer of Unisys Corporation.

IN WITNESS WHEREOF, I have hereunto set my hand and affixed the seal of said Corporation this 25th day of November 2013.

[redacted]

Assistant Secretary

Contract Between

COMMONWEALTH OF PENNSYLVANIA
GOVERNOR'S OFFICE OF ADMINISTRATION

and

UNISYS CORPORATION

for

Data Center Computing Services

CONTRACT NO. _____

TABLE OF CONTENTS

1. CONTRACT TERM 1
2. PURCHASE ORDERS 2
3. IDENTIFICATION NUMBER 4
4. ORDER OF PRECEDENCE, DEFINITIONS AND CONSTRUCTION 4
5. CONTRACT INTEGRATION 5
6. SERVICES 5
7. EQUIPMENT 8
8. THIRD PARTY SOFTWARE 9
9. DATA SECURITY 9
10. CONDUCT OF SERVICES 12
11. QUALITY ASSURANCE AND INTERNAL CONTROLS 12
12. SERVICE LOCATIONS 14
13. CONDITIONS OF CONTRACTOR'S OCCUPANCY OF COMMONWEALTH-PROVIDED REAL PROPERTY 16
14. TRANSITION 19
15. DISASTER RECOVERY AND BUSINESS CONTINUITY 23
16. PRIME CONTRACTOR RESPONSIBILITIES 24
17. KEY POSITIONS/CONTRACTOR PERSONNEL 25
18. THIRD PARTY SERVICES 27
19. COMPENSATION 28
20. FEES 28
21. PAYMENT SCHEDULE AND INVOICES 29
22. INSPECTION AND ACCEPTANCE OF DELIVERABLES AND MILESTONES 30
23. SERVICE LEVELS 31
24. LIQUIDATED DAMAGES 32
25. CONTINUOUS IMPROVEMENT AND BENCHMARKING 33
26. GOVERNANCE 36
27. CHANGE CONTROL 36
28. NOTICE OF DELAYS 38
29. NOTICE 38
30. DEFAULT 38
31. STEP-IN RIGHTS 41
32. TERMINATION 42
33. TERMINATION ASSISTANCE 45
34. CONTRACT CONTROVERSIES 52

35. COMMONWEALTH HELD HARMLESS 53
36. LIMITATION OF LIABILITY 54
37. CONFIDENTIALITY 55
38. SENSITIVE INFORMATION 58
39. PATENT, COPYRIGHT, TRADEMARK, AND TRADE SECRET PROTECTION 59
40. PROPRIETARY RIGHTS 61
41. PUBLICATION RIGHTS AND/OR COPYRIGHTS 65
42. REPORTS AND DATA 66
43. SECURITY AND PROTECTION OF INFORMATION 67
44. BACKGROUND CHECKS 68
45. INSURANCE 68
46. WARRANTIES AND AGREEMENTS 70
47. CONTRACTOR RESPONSIBILITY PROGRAM 72
48. OFFSET PROVISION FOR COMMONWEALTH CONTRACTS 73
49. TAXES-FEDERAL, STATE, AND LOCAL 73
50. POLICIES AND PROCEDURES 73
51. AUDIT OBLIGATIONS 74
52. VIRUS AND MALICIOUS CODE 76
53. THE AMERICANS WITH DISABILITIES ACT 77
54. NONDISCRIMINATION CLAUSE/SEXUAL HARASSMENT CLAUSE 78
55. CONTRACTOR INTEGRITY PROVISIONS 79
56. RIGHT-TO-KNOW LAW 85
57. ENVIRONMENTAL PROTECTION 86
58. ASSIGNABILITY 87
59. INDEPENDENT CAPACITY OF CONTRACTOR 87
60. THIRD PARTY BENEFICIARIES 88
61. CERTIFICATION REGARDING SUSPENSION 88
62. SUSPENSION OF SUBCONTRACTORS 88
63. ASSIGNMENT OF RIGHTS UNDER THE ANTITRUST LAWS 88
64. SIGNIFICANT EVENTS 89
65. FORCE MAJEURE 89
66. CONFLICT OF INTEREST 90
67. OFFICIALS NOT TO BENEFIT 90
68. CONSENTS, APPROVALS, NOTICES AND REQUESTS 90
69. REQUIRED CONSENTS 90
70. REQUIREMENTS FOR INFORMATION IN LEGAL PROCEEDINGS 91
71. EXAMINATION OF RECORDS 91

72. SURVIVAL 92
73. SEVERABILITY 92
74. WAIVER 92
75. PERIOD OF PERFORMANCE 92
76. SPECIAL REQUIREMENTS 92
77. GOVERNING LAW 92
78. COMPLIANCE WITH LAWS 93
79. SMALL DIVERSE BUSINESS COMMITMENT 93
80. ACKNOWLEDGEMENT 93
81. COVENANT OF FURTHER ASSURANCES 93
82. COVENANT OF GOOD FAITH 94
83. AMENDMENTS 94
84. ENTIRE CONTRACT 94
APPENDIX A - BUSINESS ASSOCIATE APPENDIX LANGUAGE 1
APPENDIX A - BUSINESS ASSOCIATE APPENDIX LANGUAGE 2
PERMITTED USES AND DISCLOSURES 7
OF PROTECTED HEALTH INFORMATION 7

TABLE OF SCHEDULES

SCHEDULE A - DEFINED TERMS
SCHEDULE B - GOVERNANCE
SCHEDULE C – SERVICES CATALOG
SCHEDULE D - TRANSITION MILESTONES
SCHEDULE E – DATA CENTER LOCATIONS
SCHEDULE F –DATA CENTER STATEMENT OF WORK
SCHEDULE G - STAFFING PLAN AND KEY POSITIONS
SCHEDULE H - COMMONWEALTH COMPUTING PROCEDURES MANUAL
SCHEDULE I - INTENTIONALLY OMMITTED
SCHEDULE J.1 – DATA CENTER SERVICE LEVEL MANAGEMENT
SCHEDULE J.2 – DATA CENTER SERVICE LEVEL MATRIX
SCHEDULE J.3 – DATA CENTER SLA DEFINITIONS
SCHEDULE K - KEY PROGRAM DELIVERABLES
SCHEDULE L – APPROVED SUBCONTRACTORS
SCHEDULE M – DETAILED TRANSITION PLAN
SCHEDULE N – ENTERPRISE DATA CENTER FLOOR PLAN
SCHEDULE O – COMMONWEALTH DATA CENTERS TO BE TRANSITIONED

THIS CONTRACT ("Contract") is entered into by and between the Commonwealth of Pennsylvania ("Commonwealth"), acting through its Governor's Office of Administration ("OA"), and Unisys Corporation, a Delaware corporation headquartered in Blue Bell, Pennsylvania ("Contractor").

WITNESSETH:

WHEREAS, the Office of Administration issued a Request for Proposals, RFP No. 6100022698 (the "RFP"), for data center computing services; and,

WHEREAS, the Contractor submitted a proposal in response to the RFP (the "Proposal"); and,

WHEREAS, after taking into consideration all of the evaluation factors set forth in the RFP, the Commonwealth determined that the Proposal was the most advantageous to the Commonwealth; and,

WHEREAS, the Contractor was selected for contract negotiations; and,

WHEREAS, the Commonwealth and the Contractor negotiated this Contract as their final and entire agreement with respect to the Services.

NOW THEREFORE, intending to be legally bound hereby, the Commonwealth and the Contractor agree as follows:

1. CONTRACT TERM

a. The term of the Contract shall commence on the Effective Date and shall end in seven (7) years ("the Expiration Date"), subject to the other provisions of the Contract. The Effective Date shall be: a) the date the Contract has been fully executed by the Contractor and by the Commonwealth and all approvals required by Commonwealth contracting procedures have been obtained or b) the date referenced in the Contract, whichever is later. The Contract shall not be a legally binding contract until after the fully-executed Contract has been sent to the Contractor.

b. The Commonwealth may, in its sole discretion, renew the Contract for three (3) one (1) year periods, or any combination thereof on the terms and conditions in force at the date of the renewal and utilizing pricing to be negotiated but consistent with and no less favorable than the pricing in force at the date of the renewal. Further, the Commonwealth reserves the right to extend this Contract or any part of this Contract up to three (3) months, or as necessary to prevent a lapse in Contract coverage.

c. The Commonwealth reserves the right to execute the Contract, Purchase Orders or any follow-up Contract documents in ink or electronically. The Contractor understands and agrees that the receipt of an electronically-printed Contract with the printed name of the Commonwealth purchasing agent constitutes a valid, binding contract with the Commonwealth. The printed name of the purchasing agent on the Contract represents the signature of that individual who is authorized to bind the Commonwealth to the obligations contained in the Contract. The printed name also indicates that all approvals required by Commonwealth contracting procedures have been obtained.

d. The Contractor shall not start performance, and the Commonwealth shall not be liable to pay the Contractor for any supply furnished or work performed or expenses incurred, until all of the following have occurred:

(1) The Effective Date has arrived;

(2) The Contractor has received a copy of the fully executed Contract (or written notice from the Commonwealth that the Contract has been fully executed); and

(3) The Contractor has received a Purchase Order or other written notice to proceed signed by the Commonwealth Contracting Officer.

No Commonwealth employee has the authority to verbally direct the commencement of any work or delivery of any supply under this Contract prior to the Effective Date.

2. PURCHASE ORDERS

a. The Commonwealth may issue Purchase Orders against the Contract. These orders constitute the Contractor's authority to make delivery. All Purchase Orders received by the Contractor up to and including the Expiration Date of the Contract are acceptable and must be performed in accordance with the Contract. Contractors are not permitted to accept Purchase Orders which require performance in excess of those performance time periods specified in the Contract. Each Purchase Order will be deemed to incorporate the terms and conditions set forth in the Contract.

b. Purchase Orders will not include an ink signature by the Commonwealth. The electronically-printed name of the purchaser represents the signature of the individual who has the authority, on behalf of the Commonwealth, to authorize the Contractor to proceed.

c. Purchase Orders may be issued electronically or through facsimile equipment. The electronic transmission of a Purchase Order shall require acknowledgement of receipt of the transmission by the Contractor.

d. Contractor's acknowledgment of receipt of the electronic or facsimile transmission of the Purchase Order shall constitute receipt of an order.

e. Purchase Orders received by the Contractor after 4:00 p.m. will be considered received the following business day.

f. The Commonwealth and the Contractor specifically agree as follows:

(1) No handwritten signature shall be required in order for the Contract or Purchase Order to be legally enforceable.

(2) Upon receipt of a Purchase Order, the Contractor shall promptly and properly transmit an acknowledgement in return. Any order which is issued electronically shall not give rise to any obligation to deliver on the part of the Contractor, or any obligation to receive and pay for delivered products on the part of the Commonwealth, unless and until the Commonwealth Agency transmitting the order has properly received an acknowledgement.

(3) The parties agree that no writing shall be required in order to make the Purchase Order legally binding. The parties hereby agree not to contest the validity or enforceability of the Contract or a genuine Purchase Order or acknowledgement that has been issued electronically under the provisions of a statute of frauds or any other applicable law relating to whether certain agreements shall be in writing and signed by the party bound thereby. The Contract and any genuine Purchase Order or acknowledgement issued electronically, if introduced as evidence on paper in any judicial, arbitration, mediation, or administrative proceedings, will be admissible as between the parties to the same extent and under the same conditions as other business records originated and maintained in documentary form. Neither party shall contest the admissibility of copies of the Contract or any genuine Purchase Order or acknowledgements under either the business records exception to the hearsay rule or the best evidence rule on the basis that the Contract or Purchase Order or acknowledgement were not in writing or signed by the parties. A Purchase Order or acknowledgment shall be deemed to be genuine for all purposes if it is transmitted to the location designated for such documents.

(4) Each party will immediately take steps to verify any document that appears to be obviously garbled in transmission or improperly

formatted to include re-transmission of any such document if necessary.

g. Purchase Orders under ten thousand dollars ($10,000) in total amount may also be made using a Commonwealth Procurement VISA Card in person or by telephone. When an order is placed by telephone, the Commonwealth Agency shall provide the Agency name, employee name, credit card number, and expiration date of the card. The Contractor agrees to accept payment through the use of the Commonwealth Procurement VISA card.

3. IDENTIFICATION NUMBER

The Contractor must have a SAP Vendor Number.

4. ORDER OF PRECEDENCE, DEFINITIONS AND CONSTRUCTION

a. If any conflicts or discrepancies should arise in the terms and conditions of this Contract, or the interpretation thereof, the order of precedence shall be:

(1) This Contract (first, the Contract, including the terms and conditions, second the Schedules, RFP Exhibits, which have been incorporated herein and Appendix A); then
(2) The Contractor's Proposal (including the clarifications and the Best and Final Offer), as accepted by the Commonwealth; and then
(3) The RFP.

b. Except as otherwise expressly provided in the Contract, all capitalized terms used in the Contract shall have the meanings set forth in *Schedule A* (Defined Terms).

c. Interpretation:

(1) The terms defined in the Contract include the plural as well as the singular and the derivatives of such terms. Unless otherwise expressly stated, the words "herein," "hereof," and "hereunder" and other words of similar import refer to the Contract as a whole and not to any particular Paragraph, Section, subsection or other subdivision. The words "include" and "including" shall not be construed as terms of limitation.

(2) Headings preceding the text of Paragraphs or Sections, and headings to Schedules and Appendices, the table of contents and the table of Schedules and Appendices included in or attached to the Contract are used for convenience only and are not to be considered in construing or interpreting the Contract.

(3) References to any law refer to such law in changed or supplemented form, or to a newly adopted law replacing a previous law.

(4) Except as may be expressly set forth herein, all references to time herein refer to Eastern Standard Time or Eastern Daylight Time, as applicable.

(5) The Contract includes each Schedule, Exhibit and Appendix referenced herein, all of which are incorporated into the Contract by this reference

5. CONTRACT INTEGRATION

a. This Contract, including the Contract signature pages, together with the Schedules and Appendices, Contractor's Proposal, the Contractor's clarifications and the Contractor's Best and Final Offer, and the RFP and addenda thereto that are incorporated herein by reference, constitutes the final, complete, and exclusive Contract between the parties containing all the terms and conditions agreed to by the parties.

b. All representations, understandings, promises, and agreements pertaining to the subject matter of this Contract made prior to or at the time this Contract is executed are superseded by this Contract.

c. There are no conditions precedent to the performance of this Contract except as expressly set forth herein.

d. No contract terms or conditions are applicable to this Contract except as they are expressly set forth herein.

6. SERVICES

a. The Contractor agrees to provide the Services to the Commonwealth as such services are defined in this Contract, the RFP and the Contractor's Proposal, and in accordance with the terms of this Contract.

b. The Contractor shall provide to Commonwealth the following Services pursuant to the terms of the Contract:

(1) Commencing as of the Effective Date, the Transition Services set forth in *Section 14* (Transition) and *Schedule D* (Transition Milestones);

(2) Commencing as of the Effective Date and continuing until the Expiration Date:

(i) The services, function and responsibilities described in the Contract, including the Services set forth in Schedule C (Services Catalog) and *Schedule F* (Data Center Statement of Work);

(ii) Any incidental services, functions or responsibilities not specifically described in the Contract, but which are inherent or required for the proper performance and delivery of the Services; and

(3) Commencing upon written notice by Commonwealth to Contractor in accordance with *Section 33* (Termination Assistance).

c. The services set forth in (1) through (3) above shall be collectively referenced as the "Services," as they may evolve during the Term of the Contract or be supplemented, enhanced, modified or replaced pursuant to the terms hereof. The Services provided under this Contract are not exclusive to Contractor. The Commonwealth may in-source or re-procure any or all of the Services,

d. The Commonwealth may request a change to the Services through a Request for Services to increase or decrease the amount of the Services provided under this Contract, according to Commonwealth's demand for the Services. The parties shall use the Change Control Procedures to implement the changes required by the Request for Services and revise the Fees as applicable.

e. Except as may be necessary on an emergency basis to maintain the continuity of the Services or in the event of a declared disaster, Contractor shall not, without Commonwealth's written consent, modify (1) the composition of the Services, (2) the manner in which the Services are to be provided or delivered if such modification would have an adverse effect on the operations of Commonwealth, or (3) the applicable Services Levels.

f. Except as otherwise expressly provided in this Contract, Contractor is responsible for providing, and is financially and operationally responsible for, the facilities, Personnel, Equipment, materials, technical knowledge, expertise and other resources necessary to provide the Services (including all upgrades, improvements, replacements and additions to such resources).

g. Contractor acknowledges that Commonwealth encourages Contractor to provide the Services in a shared data processing environment, if such environment will materially reduce Commonwealth's costs under this Contract and can be accomplished within the confidentiality and physical security constraints imposed upon Contractor elsewhere in this Contract. Accordingly, upon the migration of any of Commonwealth's data processing to a Contractor Services Location, Contractor may provide the related Services from such Contractor Services Location in a shared data processing environment if Contractor reasonably believes such environment will materially reduce Commonwealth's costs under

this Contract and if such shared environment and Contractor's use thereof to provide the Services otherwise comports with the terms of this Contract. Commonwealth reserves to itself the right of prior approval of any Third Party proposed by Contractor to share such data processing environment, such approval not to be unreasonably withheld. Contractor acknowledges that Commonwealth will be entitled to withhold its approval of any such Third Party if, among other things, there is no or insufficient economic benefit to Commonwealth from the proposed sharing arrangement or if any federal or state confidentiality issues are not resolved to the satisfaction of the applicable federal or state governmental entity.

h. **Technical Architecture and Product Standards**. As part of the Services, Contractor shall suggest to Commonwealth information management technical architecture and product standards to be in effect at the Contractor Services Locations during the Term and the parties shall work together in good faith to develop information management technical architecture and product standards that are mutually acceptable to the parties and consistent with the Services Levels then in effect.

i. **Remote Access Capabilities**. As part of the Services, Contractor shall provide remote access capabilities for use by authorized personnel of the Commonwealth. All such remote access capabilities shall meet or exceed all Commonwealth technology and security standards as set forth in *Section 12* (Service Locations).

j. **Contractor Licenses and Permits**. As part of the Services, Contractor is responsible for obtaining, and has financial responsibility for, all necessary licenses, consents, approvals, permits and authorizations that are legally required to be obtained in order for Contractor to perform the Services. Commonwealth shall reasonably cooperate with and assist Contractor in obtaining any such licenses, consents, approvals, permits and authorizations. Notwithstanding the foregoing, Commonwealth will retain responsibility for obtaining, and the financial responsibility for, all necessary licenses, consents, approvals, permits and authorizations necessary to enable Contractor and its Subcontractors to use the Commonwealth Software to the extent necessary for Contractor's performance of the Services and with Contractor's cooperation as further described in *Section 8* (Commonwealth Third Party Software), and Contractor will cooperate, and will cause the Contractor Subcontractors to cooperate, in good faith and at no additional cost to Commonwealth, in obtaining such licenses, consents, approvals, permits and authorizations.

k. **Changes in Law and Regulations**. Each party shall identify, and notify the other party of, any changes in applicable statutes, regulations, or policies that may directly or indirectly relate to Contractor's performance of the Services. Contractor and Commonwealth shall work together to identify any impact of such changes upon Commonwealth's use, or Contractor's delivery, of the Services. Contractor shall be responsible for any fines and penalties arising from its

noncompliance with any such identified statutes, regulations, or policies relating to the business of providing the Services and shall not be responsible for any fines and penalties assessed against Commonwealth by federal governmental entities from Commonwealth's noncompliance with any federal legislative enactments or federal regulatory requirements relating to Commonwealth's operations that does not result from Contractor's actions or inactions under this Contract. As part of the Services, Contractor shall, if possible, perform the Services regardless of changes in legislative enactments or regulatory requirements. If such changes prevent Contractor from performing any of its obligations under this Contract or increase Contractor's costs in connection therewith, Contractor shall provide written notice thereof to Commonwealth within five (5) days of learning of the change and, if possible, will develop and implement a suitable workaround until such time as Contractor can fully perform its obligations under this Contract without such workaround. Contractor shall bear any costs relating to any legislative enactments and regulatory requirements relating to its business, and Commonwealth shall bear all reasonable out of pocket expenses, excluding attorney's fees, incurred by Contractor relating to legislative enactments and regulatory requirements that require modification of the Services by Contractor. If the parties are unable to agree as to the allocation of such costs, the changes and costs that are the subject of this *Section 6(k)* shall be subject to the Change Control Procedures.

l. **Access**. Upon Contractor's receipt of appropriate, advance notice (which except in an emergency situation shall not be less than three (3) business days) and subject to Contractor's reasonable security requirements, authorized representatives of Commonwealth, Commonwealth agents and agents of the Federal government shall be permitted access to any Contractor Services Location.

7. Equipment

Contractor shall provide the Services using the Equipment. Commonwealth shall provide Contractor with the required access and authorization to use the Commonwealth Equipment.

a. **Replacement and Upgrades of the Equipment**.

Contractor shall maintain and upgrade the Commonwealth Equipment and shall replace each Commonwealth Equipment at its respective end of life or as otherwise required to provide the Services. All upgrades shall be addressed through the CCPM.

b. **Equipment Maintenance**.

As part of the Services, Contractor shall provide to Commonwealth maintenance and support Services in respect of the Equipment and shall, at its own cost and

expense, maintain and support the Contractor Equipment as necessary for Contractor to perform the Services in accordance with the Services Levels. All costs and expenses incurred in connection with the provision of maintenance and support Services in respect of the Equipment (including Third Party maintenance fees) shall be the responsibility of Contractor.

8. THIRD PARTY SOFTWARE

a. As part of the Services, Contractor shall have operational responsibility for the Commonwealth Third Party Software for which Commonwealth has a valid license and current maintenance agreement ("Commonwealth Third Party Software") and shall be responsible for applying upgrades, enhancements and fixes as provided and directed by the applicable Agency. The Commonwealth shall have financial responsibility for any Commonwealth Third Party Software license, upgrade, maintenance and support fees, except that Contractor shall be responsible for any Third Party consulting fees in connection with the installation or implementation of any Software upgrade, revision or replacement required by Contractor.

b. As part of the Services, Contractor shall have financial, administration, operational and maintenance responsibility for all Contractor Software provided by the Contractor and Third Party Software provided by the Contractor as part of the Services, including but not limited to the Third Party Software listed in *Exhibit B.4* to the RFP.

c. As part of the Services, except for the cost of the license, Contractor shall have financial, administration, operational and maintenance responsibility for the Third Party Software listed in *Exhibit B.10* to the RFP, for which the Commonwealth has a valid license ("Hybrid Third Party Software").

d. The Contractor shall not require the Commonwealth to sign a software license agreement for any Contractor Software or Third Party Software, including but not limited to any click through agreement or other terms purported to apply to the Software.

e. The Commonwealth will continue to support and maintain the Software owned or licensed by the Commonwealth ("Commonwealth Software") as necessary for Contractor's performance of the Services.

9. DATA SECURITY

a. Commonwealth will retain administration of logical and Data access security, and Contractor will host Commonwealth security applications Software utilized by the Commonwealth in managing logical and Data access security, and will not implement configurations that would prevent Commonwealth from managing logical and Data access security. As part of the Services, Contractor shall implement and maintain the Commonwealth's safeguards against the disclosure,

destruction, loss or alteration of the Commonwealth Data in the possession of Contractor in accordance with the terms of this Contract and with Commonwealth's other security policies and procedures provided, in writing, to Contractor. In any event, Contractor, as part of the Services, is required to meet or exceed the most stringent of any applicable federal or state law, statute, rule or regulation applicable to Contractor's and/or Contractor's Subcontractor's possession of, or access to, any Commonwealth Data (which includes *Section 12(d)*, herein). All changes or additions to any such Commonwealth security policies or procedure or any changes to any applicable federal or state law, statute, rule or regulation shall be implemented by Contractor. Any changes or additions which result in a material additional cost to Contractor shall be subject to the Change Control Procedures. To the degree such change applies to other Contractor customers, Contractor will mitigate the Commonwealth's economic exposure to additional cost by equitably spreading the additional cost of compliance to its multiple customers.

b. The Contractor shall not store the Commonwealth Data outside of the continental United States of America.

c. All of Contractor's activities relating to the safeguarding of Commonwealth Data shall be subject to periodic review and monitoring by Commonwealth and related federal agencies, and Contractor shall cooperate fully with all such reviews and monitoring. In addition to, and not in limitation of, any restrictions set forth elsewhere in this Contract, Contractor shall have operational access to the Commonwealth Data only on an as-needed basis.

d. At no cost to the Commonwealth, and as part of the Services, Contractor shall, upon request at any time during the term of this Contract, or upon termination, cancellation, cessation of Termination Assistance, expiration or other conclusion of the Contract, Contractor shall (1) promptly return to the Commonwealth, in a form that is freely accessible to the Commonwealth and not in a Contractor proprietary format, all or the requested portion of the Commonwealth Data then in Contractor's possession or under its control, or (2) erase or destroy such Commonwealth Data. If the Commonwealth requests Contractor to destroy the Data, the Commonwealth shall have the right to conduct an audit to ensure the Data has been destroyed. This provision shall also apply to all Commonwealth Data that is in the possession of Subcontractors of Contractor. Contractor shall complete such return or destruction within ten (10) days of the request or after the conclusion of this Contract. Within such ten (10) day period, Contractor shall certify in writing to Commonwealth that such return or destruction has been completed. Contractor shall make available to the Commonwealth for a complete and secure (i.e. encrypted and appropriately authenticated) download file of the Commonwealth Data in XML format, or such other format as specified by the Commonwealth, including all schema and transformation definitions and/or delimited text files with documented, detailed schema definitions along with

attachments in their native format. Contractor shall be available to answer questions about data schema, transformations, and other elements required to fully understand and utilize the Commonwealth's Data file. Unless the Commonwealth agrees or specifies otherwise, the Contractor shall also deliver to the Commonwealth any copies, duplicates, summaries, abstracts or other representations of any such Commonwealth Data or any part thereof, in whatever form, then in the Contractor's possession or control in accordance with the "NIST Guidelines for Media Sanitization" (SP 800-88).

e. Contractor shall comply with all state and federal data breach laws as they relate to the delivery of Services, including but not limited to the Commonwealth Breach of Personal Information Notification Act (73 P.S. § §2301 *et seq*.). In the event Contractor or any of Contractor's Subcontractors discover or are notified of a data breach or potential breach of security involving any of the Commonwealth Data, Contractor shall immediately notify the Commonwealth Project Manager and the Commonwealth's Chief Information Security Officer of the same and describe the nature of the breach, the Data compromised, the involved parties, mitigation efforts, and corrective actions to be taken by the Contractor. In addition, at Commonwealth's request and at Contractor's sole cost and expense, Contractor shall:

(1) Promptly provide Commonwealth data security reports to Commonwealth in a form to be agreed upon by Commonwealth and Contractor; and

(2) Cooperate with any efforts by Commonwealth to investigate or prosecute any breach of security of the Commonwealth Data; and

(3) Provide credit monitoring services to all individuals or organizations that may be impacted by the security breach.

f. Contractor shall be solely responsible for any costs, losses or damages actually incurred by the Commonwealth due to Personal Information being accessed, used, released, disclosed and/or acquired in an unauthorized manner to the extent caused by Contractor or its Personnel, and/or Subcontractors. In the event of any data breach by Contractor or any of the Contractor Subcontractors involving any of the Commonwealth Data, Contractor shall be assessed a credit against Fees due for Service provided during the period of breach of security.

g. Credit Card Information

(1) By providing the Services under this Contract, the Contractor may create, receive, or have access to credit card records or record systems containing cardholder data including credit card numbers (collectively the "Cardholder Data"). Contractor shall comply with the Payment Card Industry Data Security Standard ("PCI DSS") requirements for Cardholder Data that are prescribed by the

payment brands (including but not limited to Visa, MasterCard, American Express, and Discover), as they may be amended from time to time. Contractor acknowledges and agrees that Card Holder Data may only be used for assisting in completing a card transaction, for fraud control services, for loyalty programs, or as specifically agreed to by the payment brands, for purposes of this Contract or as required by applicable law. If the Contractor incurs additional costs as a result of amended PCI DSS, it may follow the process set out in *Section 27* (Change Control) of this Contract.

(2) Contractor shall conform to and comply with the PCI DSS standards as defined by The PCI Security Standards Council at: https://www.pcisecuritystandards.org/security_standards/index.php. Contractor shall monitor these PCI DSS standards and will promptly notify the Commonwealth if its practices should not conform to such standards. Contractor shall provide a letter of certification to attest to meeting this requirement within one week of Contractor's receipt of the annual PCI DSS compliance report.

10. CONDUCT OF SERVICES

a. Following execution of the Contract, Contractor shall proceed diligently with all Services and shall perform such Services with qualified personnel, in accordance with the completion criteria set forth in the Contract.

b. The Contractor's Services hereunder shall be monitored by the Commonwealth and the Commonwealth's designated representatives. If the Commonwealth reasonably determines that the Contractor has not performed to the requirements in the Contract or has otherwise exposed the Commonwealth to material risk, the Commonwealth and the Contractor will attempt to reach agreement with respect to such matter. Failure of the Commonwealth or the Contractor to arrive at such mutual determinations shall be a dispute concerning a question of fact within the meaning of *Section 34* (Contract Controversies) of this Contract.

c. As part of the Services, Contractor shall conduct enterprise-wide Commonwealth satisfaction surveys, which surveys shall be conducted annually until completion of the Transition. Upon completion of the Transition, Contractor shall conduct the Commonwealth satisfaction surveys semi-annually for two years and annually thereafter.

11. QUALITY ASSURANCE AND INTERNAL CONTROLS

a. Contractor will develop and implement quality assurance and internal controls, including implementing tools and methodologies, to ensure that the Services are performed in an accurate and timely manner, in accordance with the Contract. Without limiting the foregoing, Contractor will:

(1) Maintain a strong control environment in day-to-day operations;

(2) Develop and execute a process to ensure regular internal control self-assessments are performed with respect to all Services and report the outcome of such self-assessments to the Commonwealth;

(3) Maintain an internal audit function sufficient to monitor the processes and systems used to provide the Services (i.e., perform audits, track control measures, communicate status to management, drive corrective action, etc.); and

(4) Provide to Commonwealth a summary of audit activity performed, associated significant findings, status of follow-up activity, summary of control incidents (i.e., frauds, conflict of interest situations, etc.) and related corrective action, every six (6) months.

b. As part of the Services and included in the Fees, Contractor shall:

(1) Implement and maintain independently audited quality certification (ISO 27001, ISO 9001 and ISO/IEC 20000 accreditation) and provide copies of its certification under such program and also any relevant audit or report documentation whenever so requested by the Commonwealth.

(2) Maintain valid security certifications including CISSP (Certified Information Systems Security Professional) or Comp TIA-Security+ or CASP and provide copies of its certification under such program and also any relevant documentation whenever so requested by the Commonwealth.

(3) Maintain compliance with Federal and State mandated policies including CJIS (Criminal Justice Information Services) and CHRIA (Criminal History Record Information Act) and provide copies of any relevant documentation whenever so requested by the Commonwealth.

(4) Undertake at least annually, and shall cause to be undertaken by Contractor's material Subcontractors, a SSAE 16 Type II audit that covers the existing controls as defined in the then current SSAE16 Type II audit for any Contractor sites where Contractor performs work for the Commonwealth; provide the reports from such audits to the Commonwealth; and perform these SSAE 16 Type II audits at such time(s) that shall mean the audit report is recent enough for Commonwealth to rely upon it in meeting its reporting obligations.

12. SERVICE LOCATIONS

a. **Services Locations**. The Services shall be provided from and to the Service Locations as detailed in *Schedule E* (Data Center Locations). Contractor shall not (1) provide the Services from a location other than a Service Location or (2) use the Commonwealth Enterprise Data Center to provide services to a Third Party without Commonwealth's consent. Authorized representatives of Commonwealth, Commonwealth agents and agents of the Federal government shall be permitted access to any Services Location, subject to the terms of *Section 12(d)*.

b. **Location of Performance.** Except where Contractor obtains the Commonwealth's prior written approval, Contractor shall perform all of the Services only from or at locations within the geographic boundaries of the continental United States. Any Commonwealth approval for the performance of Services outside of the continental United States shall be limited to the specific instance and scope of such written approval, including the types of Services and locations involved.

c. Right to Audit and Inspect:

(1) The Contractor shall permit the Commonwealth (or a Third Party provider selected by the Commonwealth) to perform an onsite inspection of the Contractor's Service Locations, infrastructure and security practices as reasonably requested by the Commonwealth.

(2) The Commonwealth shall have the right to request Third Party audits and/or certifications related to each Serve Location's infrastructure and security, including penetration testing and vulnerability assessments. Any reports produced from these audits and certifications will be provided to the Commonwealth for review at no cost.

(3) The Contractor shall provide the Commonwealth infrastructure and security specifications in written format for each Service Location as requested and at no cost to the Commonwealth.

(4) The Contractor shall provide the Commonwealth access to the performance records of the Contractor, as well as access to daily and weekly service quality statistics as requested and at no cost to the Commonwealth.

d. Security Procedures

(1) As part of the Services, Contractor shall maintain and enforce environmental and physical security standards and procedures at each of the Contractor Services Locations and shall comply with

environmental and physical security procedures as described in *Schedule F* (Data Center Statement of Work) and pursuant to the physical security and environmental chapters of the Commonwealth Computing Procedures Manual, which compliance will be confirmed by Contractor's SSAE 16 Type II audit report which will be delivered to the Commonwealth. If the Commonwealth requests any changes to environmental and security standards after the Effective Date and such changes would subject Contractor to material additional costs, those changes will be addressed through the Change Control Procedures. In addition, each Contractor Services Location must meet a minimum of Class C2 controlled access protection as defined in the Federal Department of Defense Trusted Computer System Evaluation (DOD 5200.28-STD).

(2) Each Commonwealth Agency's specific security requirements must be satisfied prior to the migration of its Data or processing activities to any Contractor Services Location, including any facilities to be used to support Disaster Recovery. Contractor shall maintain a log recording all entry to any Contractor Services Location, which log shall at all times be subject to Commonwealth review and audit. All of Contractor's security procedures required under this Contract shall be subject to periodic review by Commonwealth, any Commonwealth Agency or any agency of the United States federal government directly or indirectly having any dealings with any Commonwealth Agency.

(3) Contractor, as part of the Services, shall address any concerns any such reviewing entity may have regarding those security procedures and, if Commonwealth is not the reviewing entity, shall promptly inform Commonwealth of the expressed concerns and its plans to address the same. Contractor acknowledges that, because Commonwealth is a governmental entity, Commonwealth is subject to various federal and state statutory and regulatory confidentiality and security requirements, all of which will be binding upon Contractor during the Term. This Contract and the business relationship between Commonwealth and Contractor will be subject to review and approval by impacted Commonwealth Agencies and impacted federal agencies and other entities. At a minimum, Contractor will be required to comply with the Privacy Act of 1974, as amended (42 U.S.C.A. § 2000aa *et seq.*), the Drivers Privacy Protection Act, as amended (18 U.S.C.A. § 2721 *et seq.*), the Tax Information Security Guidelines promulgated by the Internal Revenue Service; and various confidentiality regulations promulgated by the U.S. Department of Health and Human Services, all as though Contractor were a governmental entity. Contractor will also be required to comply with the Health Insurance Portability and

Accountability Act of 1996, Pub.L. 104-191 (HIPAA) and the regulations promulgated related thereto (45 C.F.R. 160.101, *et seq.*) as a Business Associate as that term is defined by HIPAA according to the Business Associate Contract included as Appendix A (which Contract shall apply to covered portions of the Commonwealth as a hybrid entity as agencies direct, and which Contract shall govern only insofar as no other more stringent law otherwise applies to that Data, and only insofar as the Contract does not conflict with more stringent provisions of the Business Associate Contract, where "more stringent" is defined as in 45 C.F.R. 160.202). If and only to the extent specifically required in writing by a federal agency, in order for Contractor to be granted operational access to Commonwealth Data in connection with its performance of the Services, Contractor may be appointed as an agent of Commonwealth for the limited purpose of having operational access to certain Commonwealth Data not as a contractor of Commonwealth, but as an agent of Commonwealth having an agent's fiduciary obligations to Commonwealth as its principal. Contractor shall deliver to Commonwealth written notice of any breach of such security standards and procedures of which Contractor then has knowledge, which notice shall be delivered as promptly as is reasonable under the circumstances. Any breach by Contractor of such security standards or procedures under this *Section 12(d)* shall be subject to the provisions of *Section 30* (Default). As more fully set forth in *Section 59* (Independent Capacity of Contractor), parties to this Contract agree that the Services performed by the Contractor under the terms of this Contract are performed as an independent contractor.

13. CONDITIONS OF CONTRACTOR'S OCCUPANCY OF COMMONWEALTH-PROVIDED REAL PROPERTY

a. General

(1) The Contractor shall use and occupy the property provided by the Commonwealth (the "Enterprise Data Center") continuously as a data processing center and for related administrative uses. No other use shall be permitted. A summary of the Enterprise Data Center is attached to the RFP as *Exhibit D.7* (EDC Summary and Requirements) and incorporated herein.

(2) The Contractor shall have the sole responsibility to comply with all federal, state, and municipal laws, ordinances and regulations in its use and occupancy of the property.

(3) The Contractor agrees to accept the property in an "as-is" condition. The Contractor agrees that the Commonwealth extends no warranty

of any kind, express or implied, in regard to the property provided to the Contractor for its use.

(4) The Commonwealth is immune from the payment of real estate taxes. If any relevant taxing authority deems the use of the property by the Contractor to cause the property to become taxable, the Contractor shall have sole responsibility for the timely payment of any tax levied. Payment of such taxes may be temporarily withheld if Contractor is, in good faith, contesting the assessment or tax in a court of competent jurisdiction.

(5) The Contractor agrees that this Contract does not grant or otherwise convey any legal interest in the real property to the Contractor.

b. Upkeep and Improvements

(1) The Contractor, at its sole cost and expense, is responsible for all maintenance, security and upkeep of the real property under its control. The Contractor agrees to keep the real property in substantially the same condition as it was upon the Effective Date of the Contract, ordinary wear and tear excepted.

(2) Except for minor, non-structural alterations costing less than $10,000, any and all Contractor alterations and additions to the property shall be performed in accordance with plans and specifications prepared by a Pennsylvania-licensed architect and/or engineer. The Contractor shall submit plans and specifications to OA and the Department of General Services concurrently for approval prior to initiation of construction. Any and all alterations to the property shall be performed in a good and workmanlike manner, in conformity with all laws, rules, ordinances and other requirements of all governmental entities having jurisdiction. The Department of General Services and the OA reserve the right to specify standards that must be maintained for any alterations and additions to the property.

(3) The Contractor is solely responsible for all costs and expenses associated with any Contractor alterations or additions.

(4) The Contractor shall fully comply with Pennsylvania law governing contracting for construction, alteration or repair of a public building, including but not limited to the Prevailing Wage Act, Steel Products Procurement Act, and the Uniform Construction Code.

(5) To the fullest extent permitted by law, all Contractor contracts for alterations and additions must include a "No-Lien" clause requiring that the property be kept free from mechanics' or materialmens' liens and that the parties must file the necessary documentation in the appropriate public offices to effectuate waivers of contractors', mechanics' and materialmens' liens.

(6) Any and all alterations and additions made to the property by either the Contractor or the Commonwealth shall become part of the real estate and become the property of the Commonwealth.

c. Utilities

Contractor shall have installed, at its sole cost, separate electric meters and distribution panels to support the raised floor compute space. The Contractor will be responsible to timely reimburse the Commonwealth for electricity consumed in the raised floor compute space.

d. Reserve Account

Contractor shall establish a capital improvement fund ("Reserve Account") into which Contractor shall deposit monthly ($84,000) dollars. The amount deposited into the Reserve Account may be changed via *Section 27* (Change Control). The Reserve Account shall be cumulative, intended for capital improvements or major repairs to the Enterprise Data Center and disbursements from which shall be made only upon mutual agreement of the Commonwealth and the Contractor. Any remaining sums in the Reserve Account at termination of this Agreement shall be paid or credited to the Commonwealth. In the event that at any time during the Term of this Contract sums in the Reserve Account are insufficient to cover the cost of an agreed-to capital improvement or major repair, Contractor shall be reimbursed by the Commonwealth in an amount equal to such insufficiency. Contractor shall provide the Commonwealth at least semi-annually a report of all activity in the Reserve Account.

e. Termination Assistance

Contractor shall vacate the Enterprise Data Center and return to the Commonwealth, if not previously returned, any resources that are implicated by the relevant Assistance Event, as described in *Section 33* (Termination Assistance), and that are owned, leased or licensed by the Commonwealth or any Commonwealth contractor, including the Commonwealth owned or leased Equipment, the Commonwealth owned materials and the Commonwealth licensed materials, in condition at least as good as the condition of such facilities and resources when they were made available to Contractor, ordinary wear and tear excepted. Such

facilities and resources shall be vacated and/or returned as of the later of the effective date of the relevant Assistance Event and the completion of the Termination Assistance requiring such facilities or resources.

14. TRANSITION

a. **Transition.** Contractor shall perform the Transition Services, including provision of the Deliverables described in the Detailed Transition Plan. Contractor shall accomplish the Transition in a transparent, seamless, orderly, and uninterrupted manner. Contractor's responsibilities with respect to the transition include:

(1) Transfer of the Services to Contractor and subsequent transition of the Services to realize any planned cost reductions and Service performance improvements in accordance with the Transition Plans agreed to by Commonwealth and including a number of Transition Milestones;

(2) Performing the transition without disruption to Commonwealth's operations;

(3) Assuming responsibility for all costs associated with the transition; and

(4) Otherwise performing such transition and migration tasks as are necessary to enable Contractor to provide the Services in accordance with the terms of the Contract, including the applicable Service Levels.

b. **Transition Plan.** The preliminary Transition Plan is attached to this Contract as part of Contractor's Proposal. Contractor shall complete, and submit to Commonwealth for review a final Detailed Transition Plan on or before the date set forth in *Schedule D* (Transition Milestones). If a Detailed Transition Plan submitted by Contractor is not acceptable to Commonwealth, Contractor will address and resolve any questions or concerns Commonwealth may have and will promptly incorporate any modifications, additions or deletions requested by Commonwealth. Contractor will revise and resubmit the Detailed Transition Plan until accepted by Commonwealth. Upon Commonwealth's acceptance, the Detailed Transition Plan shall automatically be incorporated into this Contract as *Schedule M* (Detailed Transition Plan) and shall supersede and replace all prior Transition Plans. The Detailed Transition Plan shall detail the specific activities to be performed by each party, and, unless otherwise requested by Contractor and agreed to by Commonwealth in its sole discretion, shall be consistent in all material respects with any preliminary Transition Plan, including with respect to the activities, Deliverables, Transition Milestones, and Transition Milestone Credits described therein. The Detailed Transition Plan may thereafter be amended as mutually agreed by the parties.

The parties recognize and agree that timeliness is important for a successful Transition and have designated certain actions and projects in the Detailed Transition Plan as Transition Milestones (“Transition Milestones”). Contractor shall achieve all such Transition Milestone by the date corresponding thereto in *Schedule D* (Transition Milestones). Without limiting the foregoing, the Detailed Transition Plan shall specify, among other things:

(1) the Deliverables to be completed by Contractor,

(2) the date(s) by which each such activity or Deliverable is to be completed (the "Transition Milestones"),

(3) a process and set of standards to which Contractor shall adhere in the performance of the Transition Services and that shall enable Commonwealth to determine whether Contractor has successfully completed the transition and the activities and Deliverables associated with each Transition Milestone,

(4) any transition responsibilities to be performed or transition resources to be provided by Commonwealth and/or Commonwealth Customers,

(5) any transition responsibilities to be performed or transition resources to be provided by another Commonwealth contractor, and

(6) a detailed description of the processes and procedures that Contractor will implement (and associated implementation schedules) to effect the seamless integration and coordination of the Services with related services to be provided by other Commonwealth contractors.

The Detailed Transition Plan shall identify any related documents contemplated by this Contract and/or required to effectuate the transition that shall be executed by either of the parties.

c. **Performance**. Contractor shall perform the Transition Services in accordance with the timetable and the Transition Milestones set forth in the Detailed Transition Plan. Contractor shall assist Commonwealth in connection with Commonwealth's evaluation or testing of the Deliverables set forth in the Detailed Transition Plan. Except as otherwise expressly stipulated in the Detailed Transition Plan, Contractor shall perform the Transition Services in a manner that shall not (i) disrupt or have an unnecessary adverse impact on the activities or operations of Commonwealth or the Commonwealth Customers, (ii) materially, as reasonably determined by the Commonwealth, degrade the Services then being received by Commonwealth or the Commonwealth

Customers or (iii) materially, as reasonably determined by the Commonwealth, disrupt or interfere with the ability of Commonwealth or the Commonwealth Customers to obtain the full benefit of the Services. In Contractor's performance and completion of Transition Services, no functionality of Commonwealth's then current business operations or environment will be discontinued until Contractor demonstrates to Commonwealth's reasonable satisfaction that the affected processes and operations have been successfully migrated to Contractor's target environment and are functioning properly in that environment.

Without limiting its obligations or responsibilities, prior to undertaking any transition activity, Contractor shall discuss with Commonwealth and the relevant Commonwealth Customers all known Commonwealth and Commonwealth Customer-specific material risks and shall not proceed with such activity until Commonwealth is reasonably satisfied with the plans with regard to such risks (provided that, neither Contractor's disclosure of any such risks to Commonwealth, nor Commonwealth's acquiescence in Contractor's plans, shall operate or be construed as limiting Contractor's responsibility under this Contract). Contractor will, at Commonwealth's request, participate in transition meetings with other Commonwealth contractors. Commonwealth reserves the right to monitor, test and otherwise observe and participate in transition. Contractor will notify Commonwealth without delay if any Commonwealth monitoring, testing or participation has caused (or Contractor expects it to cause) a problem or delay in transition and work with Commonwealth to prevent or circumvent the problem or delay.

d. **Reports**. Beginning on the Effective Date, Contractor shall meet at least weekly with the Commonwealth to report on Contractor's progress in performing its responsibilities and meeting the timetable and Transition Milestones set forth in the Detailed Transition Plan. Contractor also shall provide written reports to Commonwealth at least weekly regarding such matters, and shall provide oral reports more frequently if requested by Commonwealth. Promptly upon receiving any information indicating that Contractor may not perform its responsibilities or meet the timetable or Transition Milestones set forth in the Detailed Transition Plan, Contractor shall notify Commonwealth of such delays and shall identify for Commonwealth's consideration and approval specific measures to address such delays and mitigate the risks associated therewith.

e. **Notification of Problems**. Contractor shall provide to Commonwealth written notice of any acts or omissions (whether by Commonwealth, a Commonwealth contractor, Subcontractor or any Third Party), any failure to perform any of each such party's obligations under the Contract and any other events that may affect Contractor's performance of the Transition Services. Contractor shall provide such written notice within thirty (30) days after Contractor first knew or should have known of such acts, omissions, or failures or other events. Such

written notice shall describe in reasonable detail such acts, omissions, failures or other events and the manner in which the foregoing may affect Contractor's performance.

f. **Corrective Action Plan**. In the event that either (1) the Commonwealth determines that Contractor has failed or is reasonably likely to fail to deliver the Transition Services, or (2) Contractor has determined that it has failed or is reasonably likely to fail to deliver the Transition Services, then Commonwealth or Contractor, as applicable, will notify the other party of such failure (a "Transition CAP Notice"). Concurrently with such notice, Contractor will:

(1) immediately take steps to mitigate any harmful effects of such failure, and

(2) promptly (and in any event as soon as reasonably practical) perform a Root Cause Analysis and prepare a corrective action plan with respect to such failure, and

(3) take all actions necessary to prevent its recurrence, including, without limitation, providing all additional resources necessary to resolve such failure.

If Commonwealth determines that any such corrective action plan is not adequately addressing the failure, Contractor shall revise the corrective action plan until it is accepted by the Commonwealth. In the event that Contractor is unable to complete the Transition Services on or before the dates specified in the Detailed Transition Plan (a "Transition Failure Event"), then Contractor will meet with Commonwealth to develop a workaround plan to address the Transition Failure Event, which plan, unless such Transition Failure Event was caused by Commonwealth, may include, at Commonwealth's option, obtaining the services to work around the Transition Failure Event from another Commonwealth contractor.

g. **Failure to Meet Transition Milestones**. Neither the Transition Services nor the activities and Deliverables associated with individual Transition Milestones shall be deemed complete until Commonwealth's acceptance of such activities and Deliverables. If Contractor fails to meet a Transition Milestone, Contractor shall pay Commonwealth the applicable Milestone Credits specified in *Schedule D* (Transition Milestones) or in the Detailed Transition Plan that are associated with such Transition Services.

h. **Additional Remedies**. In the event that Contractor fails to identify and resolve any problems that may impede or delay the timely completion of each task in the Detailed Transition Plan, without prejudice to Commonwealth's other rights and remedies under the Contract or at law or equity, (i) Contractor will provide, at its sole cost and expense, all such additional resources as are

necessary to identify and resolve any problems that may impede or delay the timely completion of each task in the Detailed Transition Plan, and (ii) Commonwealth may equitably reduce the Fees set forth in *Schedule C* (Services Catalog) in an amount reasonably estimated by Commonwealth to account for the Services that Commonwealth is not receiving or did not receive.

i. **Suspension or Delay of Transition Services.** Commonwealth reserves the right, in its sole discretion, to suspend or delay the performance of the Transition Services and/or the transition of all or any part of the Services. If Commonwealth elects to exercise this right and Commonwealth's decision is based in material part on concerns about Contractor's ability to perform material aspects of the Transition Services or Contractor's failure to perform its obligations under this Contract, the Commonwealth shall not incur any additional Fees or reimbursable expenses in connection with such decision, provided that Commonwealth shall work in good faith with Contractor to minimize the period of any such suspension or delay.

15. DISASTER RECOVERY AND BUSINESS CONTINUITY

a. Disaster Recovery Plan.

(1) Jointly with the Commonwealth, Contractor shall at least annually review and update the Disaster Recovery Plan, it being understood and agreed that the parties will work together and cooperate in good faith on any such review or updated of the Disaster Recovery Plan.

(2) With the Commonwealth's support as specified in the Disaster Recovery Plan, Contractor shall every six (6) months test the operability of the Disaster Recovery Plan then in effect.

(3) Within fifteen (15) business days of completion of a Disaster Recovery test, Contractor will certify to Commonwealth that the Disaster Recovery Plan was fully, timely and successfully implemented, or, if the Disaster Recovery Plan was not fully, timely and successfully implemented, report all deficiencies (including root cause analysis) and corrective actions, and certify that such corrective actions addressed all deficiencies; and

(4) Annually and at additional times at the request of Commonwealth, Contractor will certify to Commonwealth that that any applicable Third Party business recovery center agreement remains in full force and effect without any default, including payment, thereunder by any party thereto, and that Commonwealth is entitled, pursuant to the terms of the business recovery center agreement, to assume that agreement upon the expiration or termination of this Contract.

b. Disaster Recovery Event.

(1) As part of the Services, Contractor shall have responsibility for executing the Disaster Recovery Plan relating to the Services as described in *Schedule F* (Data Center Statement of Work). Contractor shall immediately provide Commonwealth with notice of the occurrence of any disaster affecting the provision or receipt of all or any material portion of the Services and implement the Disaster Recovery Plan then in effect. Contractor agrees to utilize the disaster recovery planning methodology software then utilized by Commonwealth in connection with activities contemplated under this *Section 15* (Disaster Recovery and Business Continuity).

(2) Contractor shall reinstitute the Services as promptly as possible but in any event within subscribed restitution hours, as set forth in the Disaster Recovery Plan then in effect, after the occurrence of a disaster. If the Services are not fully reinstituted within the subscribed restitution hours the Commonwealth shall have the right to terminate this Contract for critical failure pursuant to the provisions of *Section 32(c)*, except to the extent that the critical failure was caused by the Commonwealth, and Contractor shall, prior to or at the expiration of the applicable restitution period, deliver to Commonwealth a written report detailing the cause of the disaster, Contractor's plans to reinstitute the Services and its anticipated schedule to do so. Thereafter, Contractor and Commonwealth shall develop a plan to reinstitute the Services as promptly as is possible under the circumstances. Contractor shall prepare and deliver to Commonwealth updated reports such that Commonwealth shall at all times be fully informed as to the status of Contractor's efforts and anticipated schedule to reinstitute the Services. In the event that any Contractor Equipment is required to be replaced as a result of the disaster, Contractor shall replace such Contractor Equipment with Equipment to the extent then available and compatible with the associated application(s) which is capable of performing such that Contractor can meet applicable Service Levels under this Contract. Any Contractor obligations to implement a Disaster Recovery Plan set forth in this paragraph can be triggered by a notice of disaster provided to Contractor by Commonwealth.

16. PRIME CONTRACTOR RESPONSIBILITIES

The Contractor will be responsible for all Services in this Contract whether or not Contractor provides them directly. Further, the Contractor is the sole point of contact with regard to all contractual matters, including payment of any and all charges resulting from the Contract.

17. KEY POSITIONS/CONTRACTOR PERSONNEL

a. Contractor Project Manager and Transition Project Manager.

(1) Upon the Effective Date, the Contractor shall appoint the Contractor Project Manager identified in its proposal, who on a full-time basis shall be in charge of implementing the Services. Contractor shall replace the Contractor Project Manager only when required or permitted pursuant to *Section 17(c)*. The Contractor Project Manager shall at all times be subject to Commonwealth's continuing approval.

(2) Upon the Effective Date the Contractor shall appoint the Transition Project Manager identified in its proposal, who will have the responsibilities set forth in *Schedule F* (Data Center Statement of Work). Contractor shall replace the Transition Project Manager only when required or permitted pursuant to *Section 17(c)*. The Contractor Transition Manager shall at all times be subject to Commonwealth's continuing approval.

b. Key Positions. The positions identified in *Schedule G* (Staffing Plan and Key Positions), are designated by Commonwealth and Contractor as Key Positions within the Contractor's Personnel. All of the Key Personnel shall be dedicated to the Commonwealth account on a full-time basis. The Commonwealth Project Manager and the Contractor Project Manager shall meet once every year beginning with the first anniversary of the Effective Date or upon the request of either the Commonwealth Project Manager or the Contractor Project Manager to update the list of the Key Personnel. Each Key Personnel shall at all times be subject to Commonwealth's continuing approval. Except for a replacement or reassignment of Key Personnel pursuant to *Section 17(c)*, Contractor shall not reassign or replace any Key Personnel. As more fully set forth in *Section 59* (Independent Capacity of Contractor), parties to this Contract agree that the Services performed by the Contractor under the terms of this Contract are performed as an independent contractor.

c. Reassignment Waivers. Contractor shall not reassign or replace the Contractor Project Manager or any Contractor Services Location Manager during the first eighteen (18) months of his or her assignment as the Contractor Project Manager or a Contractor Services Location Manager unless Commonwealth consents to such reassignment or replacement or unless the individual (1) voluntarily resigns from Contractor, (2) is dismissed by Contractor for cause or replaced as a result of unsatisfactory performance in respect of his or her duties and responsibilities to Contractor or Commonwealth pursuant to this Contract, or (3) is unable to work due to his or her death or disability. In addition, Contractor shall, in connection with its assignment of other Key Personnel, use commercially reasonable efforts to assure the greatest degree of continuity possible among such Key Personnel. If, in any instance, Commonwealth withholds or withdraws its approval of any

Personnel or representative of Contractor for the performance of the Services, including without limitation, the Contractor Project Manager, any Contractor Services Location Manager or any other Key Employee, Contractor promptly shall reassign and replace such Personnel or representative.

d. **Subcontractors**. The Contractor may subcontract any portion of the Services described in this Contract to Third Parties selected by Contractor and approved in writing by the Commonwealth, which approval will not be unreasonably withheld. Approved Subcontractors will be listed on *Schedule L* (Approved Subcontractors). Notwithstanding the above, if Contractor has disclosed the identity of Subcontractor(s) together with the scope of work to be subcontracted in the Contractor's Proposal, award of the Contract is deemed approval of all named Subcontractors for the specified scope of work and a separate approval is not required. The existence of any subcontract shall not change the obligations of Contractor to the Commonwealth under this Contract. Upon written request of the Commonwealth, the Contractor shall promptly provide the Commonwealth with a copy of any specified subcontract agreement between the Contractor and the Subcontractor. If Commonwealth reasonably determines that a Subcontractor should no longer be retained by Contractor due to material performance deficiencies arising from the Subcontractor's performance, the Commonwealth reserves the right, for good cause, to require that the Contractor remove a Subcontractor from the project. As more fully set forth in *Section 59* (Independent Capacity of Contractor), parties to this Contract agree that the Services performed by the Contractor under the terms of this Contract are performed as an independent contractor.

e. **Managerial Control**. Subject to the other provisions of this Contract, including without limitation, provisions regarding security procedures and government security clearance and the other provisions of this *Section 17* (Key Positions/Contractor Personnel) Contractor shall have complete managerial control over its Personnel, and Contractor may dismiss, promote, replace or reassign a member of the Contractor Personnel; provided, however, that unless otherwise agreed to by Commonwealth, Contractor shall deliver a notice to Commonwealth before or immediately after dismissing any member of the Contractor's Personnel. In addition, Contractor shall deliver to Commonwealth written notice of any criminal activities undertaken by, or alleged to have been undertaken by, any member of the Contractor Personnel and of which Contractor then has knowledge, which notice shall be delivered as promptly as is reasonable under the circumstances, and Contractor will cooperate with any investigation undertaken by or through Commonwealth in respect of such actual or alleged criminal activities.

f. **Conduct of Contractor Personnel**. While at the Commonwealth Services Locations and the Contractor Services locations, Contractor's Personnel and Subcontractors (1) shall comply with all lawful requests, rules and regulations of Commonwealth regarding personal and professional conduct (including the

wearing of a particular uniform, identification badge or personal protective equipment and adhering to security regulations and general safety practices or procedures) and (2) otherwise shall conduct themselves in a businesslike manner.

g. **Unsatisfactory Conduct**. If the Commonwealth determines in its sole discretion that a particular Contractor Personnel or Subcontractor is not conducting himself or herself in an appropriate manner, Commonwealth may provide Contractor with notice of such conduct. Upon receipt of such notice, Contractor shall promptly investigate the matter and take appropriate action, which may include (1) removing the offending individual from the project and replacing him or her with a similarly qualified individual or (2) taking other appropriate disciplinary action to prevent a reoccurrence. In the event there are repeat violations of this *Section 17(g)* by a particular Contractor Personnel, contractor or Subcontractor, Contractor shall promptly remove him or her from the project as set forth above.

h. **Confidentiality.** Contractor shall:

(1) Cause each Contractor Personnel to maintain and enforce the confidentiality provisions of the Contract both during and after their assignment to the Commonwealth account; and

(2) Enter into, or shall have entered into, an agreement with each Contractor Personnel member which assigns, transfers and conveys to Contractor all of such Personnel's right, title and interest in and to any materials created pursuant to the Contract, including all rights of patent, copyright, trade secret or other proprietary rights in and to such materials.

18. THIRD PARTY SERVICES

a. Commonwealth shall have the right, in its sole discretion, to contract with any number of Third Parties to perform Services which would otherwise fall within the terms of this Contract. In the event Commonwealth contracts with a Third Party to perform any service on behalf of or for Commonwealth, Contractor, as part of the Services, shall cooperate with Commonwealth and such Third Party to the extent reasonably required by Commonwealth, including provision of (i) existing written requirements, standards and policies for systems operations so that the enhancements or developments of such Third Party may be operated by, and will be compatible with the operations of, Contractor, (ii) assistance and support services to such Third Party, and (iii) such access to the Systems as may be reasonably required by such Third Party (subject to all security standards, licenses, confidentiality restrictions and other standards and procedures then in effect at each of the Services Locations) to develop, test and deploy the service contracted for by Commonwealth. In addition thereto, Contractor shall not commit or permit any act which will unduly interfere with the performance of work by Commonwealth employees or any such Third Party, and Commonwealth

will not commit or permit any act which will interfere with Contractor's performance of the Services. All additional out-of-scope support costs, excluding attorney fees, incurred by Contractor as a result of a Commonwealth contract with a Third Party will be handled in accordance with the Change Control Procedures.

b. Throughout the Term, but not more than once every six months, Commonwealth may request that Contractor work together with Commonwealth and/or Third Parties to identify ways to achieve reductions in the cost of Service delivery and corresponding reductions in the price(s) quoted in the Contract. If so requested by Commonwealth, Contractor will, at its own expense, promptly prepare a detailed proposal identifying all viable means of achieving the desired reductions without (to the extent practically possible) adversely impacting business objectives or requirements identified by Commonwealth. Commonwealth shall not be obligated to accept or implement any such proposal.

19. COMPENSATION

In consideration of Contractor providing the Services, subject to the terms of this Contract, Commonwealth shall pay to Contractor the Fees as set out at *Schedule C* (Services Catalog). All items shall be performed within the time period(s) specified in the Contract. The Contractor shall be compensated only for items supplied and performed consistent with the terms of this Contract.

20. FEES

a. **Service Fees**. In consideration of Contractor providing the Services, subject to the terms of this Contract, Commonwealth shall pay to Contractor the Fees pursuant to *Schedule C* (Services Catalog).

b. **Cost of Living Adjustment.** The Fees shall not be subject to any cost of living or inflationary adjustment or any other adjustment based on Contractor's costs to provide the Services.

c. **Expenses**. Except as expressly provided otherwise in this Contract, expenses of Contractor relating to the Services are included in the Fees, and no such expenses or other costs or fees shall be reimbursed by Commonwealth unless agreed to by Commonwealth in writing. The Contractor shall not be allowed or paid travel or per diem expenses unless agreed to by Commonwealth in writing.

d. **Pro-ration**. All periodic Fees or charges under this Contract are to be computed on a calendar month basis and shall be prorated on a per diem basis for any partial month.

e. **Unused Credits**. Any unused credits against future payments owed to either party by the other pursuant to this Contract shall be paid to the applicable party within forty-five (45) days after the expiration or termination for any reason of Contractor's obligation to provide the Services or of this Contract. This *Section 20(e)* shall survive the expiration or any termination of this Contract.

f. **Pricing Protection**. Notwithstanding anything to the contrary elsewhere in this Contract, the Fees relating to time and materials Services shall in no event and at no time during the Term exceed Contractor's then lowest charges for such services to Contractor's state governmental customers generally receiving comparable goods and services at comparable volumes and upon material terms and conditions comparable to those contained in this Contract and pursuant to an outsourcing agreement dated after the Effective Date. Upon Commonwealth's request from time to time, and in any event on each anniversary of the Effective Date, Contractor shall advise Commonwealth in writing that this *Section 20(f)*has not been contradicted by any transaction entered into by Contractor on or after the Effective Date. If Contractor is unable to provide such written notice because of a transaction entered into by Contractor contradicting this *Section 20(f),* Contractor shall offer to Commonwealth an adjustment to the Fees to correct such contradiction.

g. Contractor presently provides the Commonwealth services under Contract Number ME-981363 (the "DPH Agreement") at the Fees set forth in Exhibit 21.01A (the "2014 DPH Fees") of the DPH Agreement. The services provided under the DPH Agreement are similar to the Services to be provided under this Contract. Commencing on the Effective Date of this Contract and ending on December 31, 2014, Unisys will deduct any amounts paid for Services transitioned to this Contract from the DPH Agreement from the 2014 DPH Fees invoiced to the Commonwealth under the DPH Agreement. The deduction will be by Agency transitioned and will exclude any Services not transitioned from the DPH Agreement. If the amount paid under this Contract in 2014 is greater than the sum of the 2014 DPH Fees, the amount invoiced under the DPH Agreement will be zero ($0).

On or before October 31, 2014, Unisys and the Commonwealth will negotiate what potential changes or reductions, if any, will be made related to Services which have not been transitioned from the DPH Agreement.

21. PAYMENT SCHEDULE AND INVOICES

a. **Service Fees**. On or before the 15th day of each calendar month of the Term, Contractor shall provide Commonwealth with a single invoice for the Service Fees. Each such invoice shall include the Fees, if applicable, for the then current month, as well as any Service Level Credits then payable by Contractor or refundable by Commonwealth, or other reimbursable charges to Commonwealth for Services actually rendered prior to the date of such invoice.

b. **Detailed Invoices.** Contractor shall provide on the monthly invoices varying degrees of detail (e.g., per Agency, end-user, department, project, site) as specified in *Schedule H* (Commonwealth Computing Procedures Manual). The detailed invoice will be delivered both in an electronic format compatible with the Commonwealth's Invoice Processing System and a summary Invoice will be delivered for management and budgeting purposes.

c. **Time of Payment**. Any sum due Contractor pursuant to any such invoice shall be due and payable on the last business day of the calendar month following the calendar month during which such invoice was delivered to Commonwealth. (e.g., an invoice delivered to Commonwealth on July 15, 2015 will be due and payable on August 31, 2015, the last business day of August, 2015.). In the event any invoices remain unpaid after such due date, the Commonwealth may pay interest as determined by the Secretary of Budget in accordance with Act No. 266 of 1982 and regulations promulgated pursuant thereto. Contractor shall, subject to Section 32(f) of this Contract, continue to provide the Services even in the event payment is delayed or is not made in timely fashion.

d. **Fee Dispute**. During the pendency of a dispute between Commonwealth and Contractor pursuant to which Commonwealth, in good faith, believes it is entitled to withhold, and does withhold, payment, Contractor shall continue to fully provide the Services and otherwise fully perform its obligations under this Contract. Notwithstanding the foregoing, Commonwealth will not withhold more than twenty-five percent (25%) of any monthly invoice.

22. INSPECTION AND ACCEPTANCE OF DELIVERABLES AND MILESTONES

a. Acceptance of Deliverables related to transition will occur in accordance with the Acceptance Criteria set out in *Schedule D* (Transition Milestones) and *Schedule K* (Key Program Deliverables) as it relates to Transition, and the Detailed Transition Plan.

b. Acceptance of Deliverables other than those related to transition will occur in accordance with the Commonwealth Computing Procedures Manual.

c. If the Deliverables are in compliance with the specifications, then the Commonwealth shall provide the Contractor with Commonwealth's written conditional acceptance of the Deliverables. If the Deliverables are not in compliance with the specifications, then the Commonwealth shall provide the Contractor with Commonwealth's written rejection of the Deliverable. Payment will only be made if the Commonwealth has accepted the Deliverable through written acceptance.

d. If the Deliverables do not meet an accessibility standard as set out in ITB-ACC001, the Contractor must provide written justification for its failure to meet the standard. The justification must provide specific details as to why the

standard has not been met. The Commonwealth may either waive the requirement as not applicable to the Commonwealth's business requirements or require that the Contractor provide an acceptable alternative. Any Commonwealth waiver of the requirement must be in writing.

e. Unless otherwise set forth in *Schedule H* (Commonwealth Computing Procedures Manual), upon the Contractor's receipt of the Commonwealth's written notice of rejection, which must identify the reasons for the failure of the Deliverables to comply with the Contract, the Contractor shall have fifteen (15) business days, or such other time as the Commonwealth and Contractor may agree is reasonable, within which to correct all such failures, and resubmit the corrected Deliverables, certifying to the Commonwealth, in writing, that the failures have been corrected, and that the Deliverables have been brought into compliance with the Contract. Upon receipt of such corrected and resubmitted Deliverable and certification, the Commonwealth shall have thirty (30) business days to test the corrected Deliverable to confirm that it is in compliance with the Contract. If the corrected Deliverable is in compliance with the Contract, then the Commonwealth shall provide the Contractor with Commonwealth's acceptance of the Deliverable.

f. If, in the opinion of the Commonwealth, the corrected Deliverable still contains material failures, the Commonwealth may either:

(1) Repeat the procedure set forth above; or

(2) Terminate the Contract in accordance with *Section 32* (Termination).

23. SERVICE LEVELS

a. The Contractor shall comply with the procedures and requirements of *Schedule J.1* (Data Center Service Level Management), *Schedule J.2* (Data Center Service Level Matrix), and *Schedule J.3* (Data Center SLA Definitions) during the term of the Contract.

b. All Services without expressly defined Service Levels must be performed at least to the same degree of accuracy, completeness, efficiency, quality and timeliness as is provided by well-managed suppliers providing services similar to the Services, so long as such performance is operationally reasonable. For where there are expressly defined Service Levels, Contractor will measure and report its performance against these standards on at least a monthly basis, except as may otherwise be agreed between the parties in respect of Services performed less frequently than monthly.

c. The Commonwealth's acceptance of any Service Level Credit shall not bar or impair Commonwealth's rights and remedies in respect of the failure or root cause as set

forth elsewhere in this Contract, including without limitation claims for liquidated damages, injunctive relief and termination rights, provided however, Service Level Credits paid would be credited against any such claim for damages.

24. LIQUIDATED DAMAGES

a. By accepting this Contract, the Contractor agrees to the delivery requirements of this Contract. If a Contract schedule is not met, including Transition Milestones set out in Transition Plan, the delay will interfere with the Commonwealth's program. In the event of any such delay, it would be impractical and extremely difficult to establish the actual damage for which the Contractor is the material cause. The Commonwealth and the Contractor therefore agree that, in the event of any such delay the amount of damage shall be the amount set forth in this *Section 24* and agree that the Contractor shall pay such amount as liquidated damages, not as a penalty.

b. The amount of liquidated damages for failure to meet Transition Milestones is set forth in *Schedule D* (Transition Milestones).

c. If, *Schedule D* (Transition Milestones) indicates that Contractor may earn back liquidated damages, then Contractor shall have the time specified in *Schedule D* (Transition Milestones), as indicated, to meet the Acceptance Criteria for the Transition Milestone and earn back the Milestone Credit. If Contractor fails to meet the Acceptance Criteria within 30 days following the Milestone Due Date or, if an Earn-Back period is specified, then 30 days following the end of the specified Earn-Back period, the Commonwealth, at no additional expense and at its option, may either:

(1) Immediately terminate the Contract and all Software, documentation, reports, Developed Materials and any other materials provided for or created for the Commonwealth as a result of this Contract shall be given to the Commonwealth, and the Commonwealth shall be entitled to its remedies under Subsection 24(c); or

(2) Order the Contractor to continue with no decrease in effort until the work is completed in a manner acceptable to the Commonwealth or until the Commonwealth terminates the Contract. If the Contract is continued, the liquidated damages will also continue until the work is completed.

d. Liquidated damages shall be paid by the Contractor and collected by the Commonwealth by deducting them from the invoices submitted under this Contract or any other contract Contractor has with the Commonwealth, by collecting them through the performance security, if any, or by billing the Contractor as a separate item.

e. To the extent that the delay or failure is caused by the Commonwealth, as described in *Schedule D* (Transition Milestones), no liquidated damages will be applied.

f. Contractor shall not be liable for liquidated damages if the delay to the Contract arises out of causes beyond the control of and without the fault or negligence of the Contractor and/or its Subcontractors. Such causes may include, but are not limited to, acts of God or of the public enemy, fires, floods, epidemics, quarantine restrictions, strikes, work stoppages, freight embargoes, acts of terrorism, and unusually severe weather; but in every case, the delay must be beyond the control of, and without the fault or negligence of, the Contractor and/or its Subcontractors. The Contractor shall notify the Commonwealth immediately in writing of its inability to perform because of a cause beyond the control of the Contractor.

g. If the delays are caused by the default of a Subcontractor, and if such default arises out of causes beyond the control of both the Contractor and Subcontractor, and without their fault or negligence, the Contractor shall not be liable for liquidated damages for delays, unless the supplies or services to be furnished by the Subcontractor were obtainable from other sources in sufficient time to permit the Contractor to meet the required performance schedule.

25. CONTINUOUS IMPROVEMENT AND BENCHMARKING

a. **Benchmark Overview**. Prior to the expiration of the second anniversary of the Effective Date, Commonwealth and Contractor shall establish the details of the Benchmarking process intended to ensure that Contractor provides Commonwealth with technology and Services Levels equal to or greater than other organizations receiving similar services. The parties acknowledge and agree that the benchmarking process is intended to assist Commonwealth in making decisions necessary to balance the desire for then current technology against the cost and uncertain performance of newly evolving technology.

b. **Benchmarker**. The Benchmark shall be conducted by a Benchmarker selected by the Commonwealth, subject to Contractor's approval thereof, in writing, such approval not to be unreasonably withheld, delayed or conditioned. The fees and expenses charged by the Benchmarker shall be paid by Commonwealth. Contractor shall at its expense cooperate with and assist the Benchmarker and any other third parties involved in the Benchmarking process, including meeting with Commonwealth and the Benchmarker before and throughout the benchmarking process and providing data relating to the provision of the Services, as requested by Commonwealth or the Benchmarker.

c. **Benchmark**. If Commonwealth undertakes the Benchmarking, Commonwealth and Contractor, in good faith, shall attempt to agree upon the period during which

the Benchmarking shall be conducted. If the parties are unable to so agree, Commonwealth shall specify the relevant period, subject to Contractor's approval thereof, in writing, such approval not to be unreasonably withheld, delayed or conditioned.

d. **Benchmark information**. Commonwealth and Contractor shall jointly determine the Benchmark information with appropriate input from the Benchmarker. Commonwealth and Contractor shall (1) review the Benchmark information, and (2) schedule a meeting to address any issues either party may have with the Benchmark information. Contractor shall provide the Benchmark information at no additional cost to Commonwealth; provided, however, that if Commonwealth wishes the Benchmarker to use information which Contractor does not otherwise have access to in the course of its business, Commonwealth shall provide such information at its own cost and Contractor may use such information but, unless Commonwealth expressly agrees otherwise in writing, only in connection with providing the Services.

e. **Benchmarking Results**. Within thirty (30) days after the completion of Benchmarking, the Benchmarker shall deliver the Benchmark Results to the Commonwealth Project Manager and the Contractor Project Manager for distribution to the members of the Management Committee.

f. **Benchmark Results Review Period and Adjustments**. The members of the Management Committee shall utilize the Benchmark Review Period to review such Benchmark Results, and the Management Committee shall meet during the Benchmark Review Period to collectively assess the Benchmark Results.

g. **Disputes of Benchmark Results**. Either Commonwealth or Contractor may in good faith dispute the Benchmark Results, in writing, prior to the expiration of the Benchmark Review Period. Any such notice of dispute issued by either party shall include a description of the nature of such dispute in sufficient detail so as to enable the Benchmarker and the other party to assess the motive and merit of the dispute. Within ten (10) days after receipt of such notice, the parties shall cause the Benchmarker to issue a written response addressing the dispute, and if such dispute requires a change to any of the Benchmark Results, the Benchmarker shall be directed to issue revised Benchmark Results. Upon issuing such revised Benchmark Results, Commonwealth and Contractor, as applicable, shall have another Benchmark Review Period to review the revised Benchmark Results in accordance with *Section 25(f)*. In the event either party disputes the revised Benchmark Results within the second Benchmark Review Period or if the parties are unable to agree as to the need for revised Benchmark Results, original Benchmark Results or the revised Benchmark Results, as the case may be, shall be subject to the contract controversy procedures set forth in *Section 34* (Contract Controversies).

h. **Benchmarking: Price Protection**. In addition to the Benchmarking provided for in this *Section 25* (Continuous Improvement and Benchmarking), no earlier than sixty (60) days after the end of Year 2 of this Contract, and no more frequently than annually thereafter, the Commonwealth may engage a Benchmarker, in accordance with the provisions of this *Section 25* (Continuous Improvement and Benchmarking) for the purpose of assessing the extent to which the prices paid for the Services hereunder are comparable to prices of a comparable reference group of clients for Services. This Benchmarking Price Protection process shall be an objective measurement and comparison process utilizing baseline methods and industry standards. The parties acknowledge and agree that this Benchmarking Price Protection process is intended to assure the Commonwealth that pricing and pricing models employed in this engagement are consistent with the reference group throughout the later years of the Contract, as it may be extended or renewed.

i. **Benchmark: Pricing Adjustments**. If the results of a Benchmarking Price Protection analysis, as reflected in written Benchmarking Results delivered to Contractor, reveal that amounts to be paid under the terms of the Contract for Services exceed by a factor of ten percent (10%) or more than the average of amounts paid by the reference group for comparable services (the "Market Rate"), the Commonwealth may elect to renegotiate those prices. When notified of the Commonwealth's intent to renegotiate the prices, the Contractor shall, as soon as practical following notification of the Commonwealth's intent, negotiate in good faith with Commonwealth for the adjustment and reduction of fees for the Services. If an agreement is reached for a pricing adjustment such agreement will be effective as of the date of delivery of the Benchmarking Price Protection Results. If the parties are unable to agree to a pricing adjustment within sixty (60) days after delivery of the Benchmarking Price Protection Results, the matter shall be submitted to the various dispute resolution procedures contained in *Section 34* (Contract Controversies) of the Contract. If the dispute resolution procedure results in a pricing adjustment, that adjustment will be effective as of the date of delivery of the Benchmarking Price Protection Results. In no event will Contractor increase the Fees as a result of any review pursuant to this *Section 25* (Continuous Improvement and Benchmarking).

j. **Annual Best Practices Reviews.** Within thirty (30) days of each anniversary of the Effective Date, Contractor shall, in accordance with procedures agreed upon by the Commonwealth Project Manager and the Contractor Project Manager, identify for Commonwealth any best practices that have emerged (within Contractor’s organization or, to the knowledge of Contractor, within the processing services outsourcing market generally), that, if implemented by the Contractor would materially benefit the Commonwealth in terms of price reductions or performance improvement. If requested by Commonwealth, within sixty (60) days Contractor shall provide Commonwealth with proposals for the implementation of such best practices in a manner consistent with the

Change Control Procedures of the Contract. If approved by Commonwealth, Contractor shall implement such best practices on behalf of Commonwealth as expeditiously as possible.

26. GOVERNANCE

Provisions for the governance of this Contract and the Services delivered pursuant hereto are set forth in *Schedule B* (Governance) to this Contract.

27. CHANGE CONTROL

a. Change Control Procedures. The following Change Control Procedures will apply if either party wishes to implement or have Contractor implement a Change. The requesting party will forward to the other party a Change Order which will include the following:

(1) Project identification
(2) Originator's name and title
(3) The date of the Change Order
(4) A description of the proposed Change
(5) The reason for the proposed Change

For Contractor, all Change Orders must be directed to or originate from Contractor's Project Manager. For Commonwealth, all Change Orders must be directed to or originate from the Commonwealth Project Manager.

(6) For any Contractor-initiated Change Order, Commonwealth shall have the option of accepting or rejecting that Change Order.

(7) Contractor will assign a number to and log each Change Order.

(8) All Change Orders will be categorized by Commonwealth as Priority 1 (urgent), Priority 2 (ordinary) or Priority 3 (low).

(9) Contractor will make reasonable efforts to investigate the impact of the Change Order on the Fees, timetable, specifications, Services, Service Levels, terms and conditions and, the relative obligations of the parties under this Contract and the (the "Impact Study") in accordance with a schedule that reflects the applicable priority category.

(10) Contractor will inform Commonwealth if there will be any charges for Contractor Services in conducting the Impact Study and Commonwealth will decide whether Contractor should conduct the Impact Study. Contractor shall be entitled hereunder to charge Commonwealth only for those expenses incurred by Contractor in connection with the conduct of the Impact Study that are (i)

Contractor's out-of-pocket expenses paid by Contractor to Third Parties (other than Contractor's or any Contractor's Subcontractor's employees) for expertise not otherwise possessed by or available to Contractor or (ii) for Personnel of Contractor or any Contractor Subcontractor not theretofore engaged in the provision of the Services. In order for any of the foregoing expenses to be reimbursable to Contractor, Contractor must first provide an estimate thereof to Commonwealth and obtain from Commonwealth its prior written approval thereof. If Contractor provides any such estimate and Commonwealth does not approve the estimated expenses, Contractor shall not be obligated to proceed with the Impact Study. In all cases, Contractor shall make a good faith effort to maximize its use of Contractor Personnel and the employees of Contractors Subcontractors then engaged in the provision of the Services to the extent Contractor can do so without adversely affecting its ability to provide the Services in accordance with the Services Levels. Any disputes between the parties regarding the validity, estimated amount or actual amount of any reimbursable expenses shall be subject to the dispute resolution provisions of *Section 34* (Contract Controversies).

(11) If both parties agree on the Impact Study and any necessary Changes to the Services, the relative obligations of the parties under this Contract, and the Fees, a Change Order will be issued to reflect the agreed to Changes.

(12) If the parties cannot agree upon the Impact Study or the resultant Changes to this Contract, any Commonwealth-initiated Change Order will nevertheless be implemented at Commonwealth's option and Contractor shall perform the Services, and either party may elect to have all outstanding related matters treated as a dispute between the parties under *Section 34* (Contract Controversies). During the pendency of any such dispute, Commonwealth shall pay to Contractor any undisputed amounts. Any changes to Service Levels which are required by the implementation of the Changes will be reflected in the Change Order that is issued.

b. All Changes shall be made pursuant to the Change Control Procedures. Contractor shall:

(1) schedule all Changes so as not to interrupt or unduly interfere with Commonwealth's operations,

(2) prepare and deliver to Commonwealth each month a ninety-day rolling schedule for ongoing proposed and approved and planned Changes,

(3) review and determine the cause of any failed Changes and deviations from scheduled Changes, and

(4) document and provide to the Management Committee and to the Commonwealth Project Manager, individually, same-day notification (which may be given orally provided that such oral notice is confirmed in writing to such persons within three (3) Commonwealth business days) of all changes performed on an emergency basis to maintain the continuity of the Services.

c. Without limiting any other provision of this Contract, the following Schedules may be modified through the Change Control Procedures set forth in this *Section 27* (Change Control):

(1) Schedule C – Services Catalog
(2) Schedule E – Data Center Locations
(3) Schedule G – Staffing Plan and Key Positions
(4) Schedule J.1 – Data Center Service Level Management
(5) Schedule J.2 – Data Center Service Level Matrix
(6) Schedule J.3 – Data Center SLA Definitions
(7) Schedule H – Commonwealth Computing Procedures Manual
(8) Schedule O – Commonwealth Data Centers to be Transitioned

28. NOTICE OF DELAYS

Whenever the Contractor encounters any difficulty that delays or threatens to delay the timely performance of this Contract (including actual or potential labor disputes), the Contractor shall immediately give notice thereof in writing to the Commonwealth stating all relevant information with respect thereto. Such notice shall not in any way constitute a basis for an extension of the delivery schedule or be construed as a waiver by the Commonwealth of any rights or remedies to which it is entitled by law or pursuant to provisions of this Contract. Failure to give such notice, however, may be grounds for denial of any request for an extension of the delivery schedule because of such delay. If an extension of the delivery schedule is granted, it will be done consistent with *Section 27*(Change Control).

29. NOTICE

Any written notice to any party under this Contract shall be deemed sufficient if delivered personally, or by facsimile, telecopy, electronic or digital transmission (provided such delivery is confirmed), or by a recognized overnight courier service (e.g., DHL, Federal Express, etc.), with confirmed receipt, or by certified or registered United States mail, postage prepaid, return receipt requested, sent to the address such party may designate by notice given pursuant to this section.

30. DEFAULT

a. The Commonwealth may, subject to the provisions of *Section 28* (Notice of Delays), and in addition to its other rights under the Contract, declare the Contractor in default by written notice thereof to the Contractor, and terminate for cause (as provided in *Section 32* (Termination)) the whole or any part of this Contract and shall further have the right to seek damages from Contractor for any of the following reasons:

(1) Failure to begin work within the time specified in the Contract or as otherwise specified;

(2) Failure to successfully complete a Major Milestone in accordance with the agreed Transition or Transition Plans or to complete specified work in accordance with the Contract terms;

(3) Multiple failures over time of a single Service Level or a pattern of failure over time across multiple Service Levels (a Service Level Termination Event) as set out in *Schedule J.1*(Data Center Service Level Management), *Schedule J.2* (Data Center Service Level Matrix), *and Schedule J.3* (Data Center SLA Definitions) to this Contract; this will include failures of Service Levels and key Service Levels;

(4) Failure to make agreed-upon adjustments to the fees or Service Levels in accordance with the outcome of Benchmarking Procedures;

(5) Failure or refusal to remove material, or remove and replace any work rejected as defective or unsatisfactory;

(6) Abandonment or willful refusal to provide the Services or any part of the Services;

(7) Failure to perform its responsibilities under any Business Continuity Plans or Disaster Recovery Plans, including such Business Continuity Plans or Disaster Recovery Plans that apply to Contractor's own locations used for the delivery of the Services;

(8) Any breach by Contractor of security standards or procedures under *Section 12(d)* of this Contract;

(9) Failure or refusal within 30 days after written notice by the Contracting Officer, of the Contractor to make payment or show cause why payment should not be made, of any amounts due for materials furnished, labor supplied or performed, for equipment rentals, or for utility services rendered;

(10) Failure to protect, to repair, or to make good any damage or injury to property as required under the terms of this Contract;

(11) Breaches of covenants, agreements, obligations, representations or warranties in the Contract occurring simultaneously or over time, whether or not each such breach is a material breach, and whether or not each such breach was cured, that taken together constitute a material breach of the Contract after Contractor has been made aware of such breaches, on an individual basis. Regardless of any other provision in this Contract to the contrary no cure period is available to Contractor should the Commonwealth terminate under this *Section 30(a)(11)*;

(12) An act or omission of Contractor in the performance of this Contract, which is not otherwise explicitly required or permitted under this Contract, and which results in any Regulatory Entity notifying Commonwealth that it is subjecting the Commonwealth to a hearing or tribunal or withdrawing any license granted to Commonwealth or Contractor and such hearing, tribunal or withdrawal would have a material and adverse effect on Commonwealth's operations or business or the Services. Regardless of any other provision in this Contract the contrary no cure period is available to Contractor should the Commonwealth terminate under this *Section 30(a)(12)*;

b. In the event that the Commonwealth terminates this Contract in whole or in part as provided in Subparagraph (a) above, the Commonwealth may procure, upon such terms and in such manner as it determines, services similar or identical to those so terminated, and the Contractor shall be liable to the Commonwealth for any reasonable excess costs for such similar or identical services included within the terminated part of the Contract.

c. If the Contract is terminated as provided in Subparagraph (a) above, the Commonwealth, in addition to any other rights provided in this *Section 30* (Default), may require the Contractor to transfer title and deliver immediately to the Commonwealth in the manner and to the extent directed by the Commonwealth, such partially completed work, including, where applicable, reports, working papers and other documentation, as the Contractor has specifically produced or specifically acquired for the performance of such part of the Contract as has been terminated. Except as provided below, payment for completed work accepted by the Commonwealth shall be at the Contract price. Except as provided below, payment for partially completed work including, where applicable, reports and working papers, delivered to and accepted by the Commonwealth shall be in an amount agreed upon by the Contractor and the Commonwealth. The Commonwealth may withhold from amounts otherwise due the Contractor for such completed or partially completed work, such sum

as the Commonwealth determines to be necessary to protect the Commonwealth against loss.

d. The rights and remedies of the Commonwealth provided in this *Section 30* (Default) shall not be exclusive and are in addition to any other rights and remedies provided by law or under this Contract.

e. The Commonwealth's failure to exercise any rights or remedies provided in this *Section 30* (Default) shall not be construed to be a waiver by the Commonwealth of its rights and remedies in regard to the event of default or any succeeding event of default.

f. Following exhaustion of the Contractor's administrative remedies as set forth in *Section 34* (Contract Controversies), the Contractor's exclusive remedy shall be to seek damages in the Board of Claims.

31. STEP-IN RIGHTS

a. In the event that Contractor is failing to deliver all or part of the Services, the Commonwealth shall give the Contractor notice of the failure. The Contractor shall have fifteen (15) days to provide the Commonwealth with a correction plan. If the correction plan is not received within fifteen (15) days or the failure is not corrected within thirty (30) days of the notice provided under this paragraph, Commonwealth may assign Commonwealth staff or Third Parties to step-in and perform failing elements of the Services, to the extent those Services are listed below, until such time as Contractor can demonstrate the ability to resume provision of such Services. The correction plan will describe the criteria which the Contractor must meet for the Commonwealth to transfer control of the Services back to Contractor. Provided, however, that if in the Commonwealth's sole discretion the failure creates an emergency, no notice is required for the Commonwealth to exercise its rights under this paragraph.

(1) Management of Commonwealth owned Equipment located within the Enterprise Data Center;
(2) Network Connectivity between the Commonwealth and the Contractor's datacenter(s).

b. All costs associated with the exercise of such step-in rights shall be borne by Contractor.

c. Commonwealth's exercise of its step-in rights shall not constitute a waiver by Commonwealth of any termination rights or rights to pursue a claim for damages arising out of the failure that led to the step-in rights being exercised.

d. Upon successful implementation of the correction plan, the Commonwealth will transfer control over the Services back to the Contractor.

32. TERMINATION

a. For Convenience

The Commonwealth may terminate this Contract without cause by giving Contractor thirty (30) calendar days prior written notice (Notice of Termination) whenever the Commonwealth shall determine that such termination is in the best interest of the Commonwealth (Termination for Convenience). Any such termination shall be effected by delivery to the Contractor of a Notice of Termination specifying the extent to which performance under this Contract is terminated either in whole or in part and the date on which such termination becomes effective.

In the event of Termination for Convenience, Contractor shall receive a Termination for Convenience fee ("Termination for Convenience Fee"):

The Termination for Convenience Fee shall equal the applicable amount set out in *Schedule C* (Services Catalog) minus the value of all Services performed by the Contractor consistent with the terms of the Contract prior to the effective date of termination.

In no event shall the Contractor be paid for any loss of anticipated profit (by the Contractor or any Subcontractor), loss of use of money, or administrative or overhead costs.

Failure to agree on any termination costs shall be a dispute handled in accordance with *Section 34* (Contract Controversies) of this Contract.

The Contractor shall cease Services as of the date set forth in the Notice of Termination, and shall be paid only for such Services as have already been satisfactorily rendered up to and including the termination date set forth in said notice, or as may be otherwise provided for in said Notice of Termination, and for such services performed during the thirty (30) calendar day notice period, if such services are requested by the Commonwealth, for the collection, assembling, and transmitting to the Commonwealth of at least all materials, manuals, magnetic media, studies, drawings, computations, maps, supplies, and survey notes including field books, which were obtained, prepared, or developed as part of the Services required under this Contract.

The above shall not be deemed to limit the Commonwealth's right to terminate this Contract for any reason as permitted by the other provisions of this Contract, or under applicable law.

b. Non-Appropriation

Any payment obligation or portion thereof of the Commonwealth created by this Contract is conditioned upon the availability and appropriation of funds. When funds (state or federal) are not appropriated or otherwise made available to support continuation of performance in a subsequent fiscal year period, the Commonwealth shall have the right to terminate the Contract. The Contractor shall be reimbursed in the same manner as that described in this section related to Termination for Convenience to the extent that appropriated funds are available.

c. Default

The Commonwealth may, in addition to its other rights under this Contract, terminate this Contract in whole or in part by providing written notice of default to the Contractor if the Contractor materially fails to perform its obligations under the Contract and does not cure such failure within forty-five (45) days or, if a cure within such period is not practical, commence a good faith effort to cure such failure to perform within the specified period or such longer period as the Commonwealth may specify in the written notice specifying such failure, and diligently and continuously proceed to complete the cure. The Contracting Officer shall provide any notice of default or written cure notice for Contract terminations.

(1) Subject to *Section 36* (Limitation of Liability) of this Contract, in the event the Commonwealth terminates this Contract in whole or in part as provided in this Subsection 32(c), the Commonwealth may procure services similar to those so terminated, and the Contractor, in addition to liability for any liquidated damages, shall be liable to the Commonwealth for the difference between the Contract price for the terminated portion of the Services and the actual and reasonable cost (but in no event greater than the fair market value) of producing substitute equivalent services for the terminated Services, provided that the Contractor shall continue the performance of this Contract to the extent not terminated under the provisions of this section.

(2) Except with respect to defaults of Subcontractors, the Contractor shall not be liable for any excess costs if the failure to perform the Contract arises out of causes beyond the control of the Contractor. Such causes may include, but are not limited to, acts of God or of the public enemy, fires, floods, epidemics, quarantine restrictions, strikes, work stoppages, freight embargoes, acts of terrorism, and unusually severe weather. The Contractor shall notify the Commonwealth Contracting Officer promptly in writing of its inability to perform because of a cause beyond the control of the Contractor.

(3) Nothing in this *Subsection 32(c)* shall abridge the Commonwealth's right to suspend, debar, or take other administrative action against the Contractor.

(4) If it is later determined that the Commonwealth erred in terminating the Contract for default, then the Contract shall be deemed to have been terminated for convenience under Subsection (a).

(5) If this Contract is terminated as provided by this Subsection 32(c), the Commonwealth may, in addition to any other rights provided in this Subsection, and subject to *Section 40* (Proprietary Rights) of this Contract, require the Contractor to deliver to the Commonwealth in the manner and to the extent directed by the Contracting Officer, such reports and other documentation as the Contractor has specifically produced or specifically acquired for the performance of such part of the Contract as has been terminated. Payment for such reports and documentation will be made consistent with the Contract.

d. In the event that Contractor becomes insolvent for any reason whatsoever, or makes an assignment for the benefit of creditors, or has a receiver appointed, or if it is declared as bankrupt under the laws of the United States, or if a petition of reorganization or rearrangement is filed against it under the bankruptcy laws, Commonwealth shall have the exclusive option of continuing with Contractor or its successors or assigns or trustee in bankruptcy under the terms and conditions of this Contract for the full remaining term of this Contract, or continuing with Contractor or its successors or assigns or trustee in bankruptcy under the terms and conditions of this Contract for such period of time as is necessary or desirable to terminate this Contract.

e. In the event of the sale by Contractor of all or substantially all of its assets (in a single transaction or a series of related transactions) or the sale of a controlling interest in Contractor's outstanding stock, Contractor shall be entitled to assign this Contract to its successor upon written notice thereof to Commonwealth. Commonwealth shall be entitled to receive from Contractor, upon Commonwealth's request, such information as is reasonably requested by Commonwealth to enable Commonwealth to assess the financial, technical and management capabilities of such successor to assume Contractor's obligations under this Contract. If Commonwealth determines, in the exercise of its reasonable discretion, that such successor does not or may not have such requisite financial, technical or management capabilities, and if Commonwealth informs Contractor thereof in writing and describing in reasonable detail its basis therefore, then, and only then, such assignment by Contractor shall be subject to Commonwealth's prior written consent, which consent may be withheld, delayed or conditioned in Commonwealth's sole discretion. If Commonwealth withholds such consent, then Commonwealth shall have the exclusive option of continuing

under the terms and conditions of this Contract with Contractor or its successors or assigns for the full remaining term of this Contract, or continuing under the terms and conditions of this Contract with Contractor or its successors or assigns for such period of time as is necessary or desirable to terminate this Contract. Any termination by Commonwealth will be consistent with the provisions of *Section 32* (Termination) of this Contract.

f. In the event Commonwealth fails to pay undisputed Fees for twelve (12) consecutive months, Contractor may terminate this Contract for its convenience. In such event, notwithstanding any other provision of this Contract to the contrary, Contractor shall be released from any obligation to provide further Services pursuant to this Contract.

g. The rights and remedies of the Commonwealth provided in this Section shall not be exclusive and are in addition to any other rights and remedies provided by law or under this Contract.

h. The Commonwealth's failure to exercise any rights or remedies provided in this Section shall not be construed to be a waiver by the Commonwealth of its rights and remedies in regard to the event of default or any succeeding event of default.

i. In no event shall the Contractor be paid for any loss of anticipated profit (by the Contractor or any Subcontractor), loss of use of money, or administrative or overhead costs. Any dispute regarding termination costs shall be a dispute handled in accordance with *Section 34* (Contract Controversies) of this Contract.

j. Following exhaustion of the Contractor's administrative remedies as set forth in *Section 34* (Contract Controversies), the Contractor's exclusive remedy shall be to seek damages in the Board of Claims.

33. TERMINATION ASSISTANCE

a. **General.** Upon the Commonwealth's request, Contractor shall provide Termination Assistance Services directly to the Commonwealth, or to any replacement provider designated by the Commonwealth, any successors or assigns of such entities or any of their designee(s). Contractor shall take all necessary and appropriate actions to accomplish a complete, timely, and seamless transition of any terminated Services from Contractor to the Commonwealth, or to any replacement provider designated by the Commonwealth, without material interruption of or material adverse impact on the terminated Services or any other services provided by Third Party or Services that Contractor shall continue to provide (each transition, an "Assistance Event"). Contractor shall cooperate with the Commonwealth and any new contractor and otherwise promptly take all steps required or reasonably requested to assist the Commonwealth in effecting a complete and

timely Termination Assistance Services of any terminated Services. Contractor shall provide all information regarding the terminated Services or as otherwise needed for Termination Assistance Services, including Data conversion, interface specifications, and related professional services. Contractor shall provide for the prompt and orderly conclusion of all terminated Services, as the Commonwealth may direct, including completion or partial completion of projects, documentation of work in process, and other measures to assure an orderly transition to the Commonwealth or the Commonwealth's designee. Contractor's obligation to provide the Termination Assistance Services shall not cease until an Assistance Event satisfactory to the Commonwealth, including the performance by Contractor of all asset-transfers and other obligations of Contractor provided in this *Section 33* (Termination Assistance), has been completed in accordance with mutually agreed to completion or acceptance criteria or if no agreed acceptance criteria exist, then to the Commonwealth's reasonable satisfaction.

(1) **Period of Provision**. Contractor shall provide Termination Assistance Services commencing on the date a determination is made by the Commonwealth that there shall be an Assistance Event**.**

(2) **Notice of an Assistance Event.** The Commonwealth will provide Contractor with written notice of an Assistance Event. Such notice will include a description of the Services that are to be terminated or discontinued, the affected Commonwealth Agencies, and the anticipated effective date of the Assistance Event. The Commonwealth may modify or update any of the information provided in the initial notice of an Assistance Event from time to time by a supplemental notice from the Commonwealth to Contractor.

(3) **Extension of Services**. The Commonwealth may elect, upon thirty (30) days prior notice to Contractor, to extend the period for performance of Termination Assistance Services (in whole or in part), in its sole discretion, provided that the total of all such extensions shall not result in Termination Assistance Services being performed beyond twenty-four (24) months following the effective date of the applicable Assistance Event without Contractor's consent. In each case, if the Commonwealth provides less than thirty (30) days prior notice of an extension, Contractor shall nonetheless use reasonable efforts to comply with the Commonwealth's request and provide the requested Services.

(4) **Firm Commitment**. Contractor shall provide Termination Assistance Services regardless of the reason for the Assistance Event.

(5) **Performance**. Contractor shall provide all Termination Assistance Services subject to and in accordance with the terms and conditions of this Contract. Contractor shall perform Termination Assistance Services with at least the same degree of accuracy, quality, completeness, timeliness, responsiveness and resource efficiency as it is or was required to provide the same or similar Services in accordance with this Contract. The quality and level of performance of Termination Assistance Services provided by Contractor shall continue to meet or exceed the Service Levels and shall not be degraded or deficient in any respect. Service Level Credits shall be assessed for any failure to meet Service Levels during any period in which Termination Assistance Services are provided. If any period for performing any Termination Assistance Services extends beyond the expiration or the effective date of any termination of this Contract, the provisions of this Contract shall remain in full effect for the duration of such period.

b. **Scope.** As part of the Termination Assistance Services, Contractor shall timely transfer the control and responsibility for Services previously performed by or for Contractor to the Commonwealth and/or its designee(s), and upon Commonwealth request, shall execute any documents reasonably necessary to effect such transfers. Contractor shall also provide any and all information and assistance requested by the Commonwealth required for:

(1) the systems and processes associated with the Services to operate and be maintained and enhanced efficiently;

(2) the Services to continue without interruption or adverse effect; and

(3) the orderly transfer of the Services (or replacement or supplemental services) to the Commonwealth and/or its designee(s).

c. **General Support**. Contractor shall:

(1) assist the Commonwealth and/or its designee(s) in developing a written plan for the migration of the Services to the Commonwealth and/or its designee(s), which plan shall include (as requested by the Commonwealth) capacity planning, process planning, facilities planning, human resources planning, technology planning, telecommunications planning and other planning necessary to effect the transition,

(2) perform programming and consulting services as requested to assist in implementing the transition plan,

(3) train personnel designated by the Commonwealth and/or its designee(s) in the use of any processes or associated Equipment, materials, systems or tools used in connection with the provision of the Services as needed for such personnel to assume responsibility for performance of the Services,

(4) provide a catalog of all processes, materials, the Commonwealth Data, Equipment, Software, Third Party Contracts and tools used to provide the Services,

(5) provide machine readable and printed listings and associated documentation for source code for Software owned by the Commonwealth and source code to which the Commonwealth is entitled under this Contract and assist in its re-configuration,

(6) provide technical documentation for Software used by Contractor to provide the Services as needed for continuing performance of the Services,

(7) analyze and report on the space required for the Commonwealth Data and the Software needed to provide the Services,

(8) assist in the execution of a parallel operation, data migration and testing process until the successful completion of the transition to the Commonwealth and/or its designee(s),

(9) create and provide copies of the Commonwealth Data in the format and on the media requested by the Commonwealth and/or its designee(s),

(10) If requested by the Commonwealth, provide a complete and up-to-date, electronic copy of the Commonwealth Computing Procedures Manual, and

(11) provide other technical and process assistance, documentation and information as requested by the Commonwealth and/or its designee(s).

d. Personnel.

(1) **List of Contractor Personnel**. Contractor shall promptly provide to the Commonwealth a list, organized by location, and of the Contractor Personnel dedicated (fifty percent (50%) or more to the performance of the Services that are implicated by each Assistance Event. Such list shall, specify each such Contractor Personnel's job title and job responsibilities. The Commonwealth agrees not to

disseminate any personally identifiable information contained in such list without Contractor's consent. Contractor shall not terminate, reassign or otherwise remove from the performance of the Services any such dedicated Contractor Personnel until after the end of the applicable Termination Assistance Services period unless such Contractor Personnel (1) voluntarily resigns from Contractor, (2) is dismissed by Contractor for cause or replaced as a result of unsatisfactory performance in respect of his or her duties and responsibilities to Contractor or Commonwealth pursuant to this Contract, 3) is unable to work due to his or her death or disability or 4) is not required by Contractor to provide the Termination Assistance Services.

(2) **Right to Hire**. The Commonwealth shall be permitted, without interference (including through counter-offers) from Contractor (subject to this *Section 33*), to meet with, solicit and hire, effective after the later of (i) the date of the Commonwealth's notice of an Assistance Event and (ii) the completion of the Termination Assistance Services requiring such Contractor Personnel, any Contractor Personnel dedicated to the performance of the Services during the twelve (12) month period prior to the date of the Commonwealth's notice of an Assistance Event who are implicated by that Assistance Event. Contractor hereby waives its rights, if any, under contracts with such Contractor Personnel restricting the ability of such Contractor Personnel to be recruited or hired by the Commonwealth (including waiving any right to restrict such personnel via non-compete agreements or other contractual means). Contractor shall provide the Commonwealth with reasonable assistance in their efforts to meet with, solicit and hire such Contractor Personnel, and shall give the Commonwealth and/or its designee(s) reasonable access to such Contractor Personnel for interviews, evaluations and recruitment. The Commonwealth shall endeavorto conduct the above-described activities in a manner that is not unnecessarily disruptive of Contractor's performance of its obligations under this Contract.

e. **Software and Developed Documentation**. The Contractor shall provide the Commonwealth with all Software and Developed Documentation as set forth in *Section 40* (Proprietary Rights).

f. **Equipment**.

(1) **List of Equipment**. Contractor shall promptly provide to the Commonwealth a list, organized by location, of the Equipment that is implicated by each Assistance Event. Such list shall specify information reasonably requested by the Commonwealth, including

all fields tracked by Contractor in any asset management system used by Contractor for tracking and managing Equipment, such Equipment's function, manufacturer, model number, age, and other pertinent information.

(2) **Right to Acquire**. The Commonwealth and/or its designee(s) shall have the right (but not the obligation) to purchase or assume the lease for any or all Equipment that is owned or leased by Contractor which is solely dedicated to the provision of the Services and that is implicated by the relevant Assistance Event. Such Equipment shall be transferred in good working condition, reasonable wear and tear excepted, as of the later of the effective date of the relevant Assistance Event and the completion of the Termination Assistance Services requiring such Equipment. Contractor shall maintain such Equipment through the date of transfer so as to be eligible for the applicable manufacturer's maintenance program. In the case of Contractor-owned Equipment (including Equipment owned by Contractor affiliates and Subcontractors and further including any such Equipment leased to Contractor), Contractor (or such Affiliate or Subcontractor) shall grant to the Commonwealth, and/or its designee(s) a warranty of title and a warranty that such Equipment is free and clear of all liens, security interests and other encumbrances. Such conveyance by Contractor (or Affiliate or Subcontractor) to the Commonwealth and/or its designee(s) shall be at fair market value (as shall be determined by an agreed-upon appraisal). At the Commonwealth's request, the parties shall negotiate in good faith and agree upon the form and structure of the purchase. In the case of leased Equipment, Contractor shall (1) represent and warrant that the lease is not in default, (2) represent and warrant that all payments thereunder have been made through the date of transfer and (3) notify the Commonwealth and/or its designee(s) of any lessor defaults of which it is aware at the time.

g. **Third Party Contracts.** Contractor shall promptly, but no less than thirty (30) days from the Commonwealth's issuance of notice of an Assistance Event provide to the Commonwealth a list of the Third Party contracts that are implicated by the relevant Assistance Event. Contractor shall, at the Commonwealth's request, cause the parties to such Third Party contracts to permit the Commonwealth and/or its designee(s) to assume prospectively any or all such Third Party contracts or to enter into new contracts with the Commonwealth and/or its designees on substantially the same terms and conditions, including price. Contractor shall transfer or assign those Third Party contracts that the Commonwealth elects to assume prospectively to the Commonwealth and/or its designee(s) as of the later of the effective date of the relevant Assistance Event and the completion of the Termination Assistance requiring such Third Party contracts. Such transfers or assignments shall be on

terms and conditions acceptable to all applicable parties, provided that (A) there shall be no fee, charge or other amount imposed on the Commonwealth and/or its designee(s) by Contractor or the counter-parties to such Third Party contracts for such transfer or assignment and (B) Contractor shall: (1) promptly cure and, in accordance with *Section 32(c)*, indemnify the Commonwealth against any default under such Third Party Contracts relating to the period prior to such transfer or assignment; (2) represent and warrant that all payments thereunder through the date of transfer or assignment are current; and (3) notify the Commonwealth and/or its designee(s) of any counter-party's default with respect to such Third Party contracts of which it is aware at the time of such transfer or assignment.

Contractor will request, with respect to any contracts applicable to Contractor Third Party Software being provided to Commonwealth and being used by Contractor to perform the Services, that the Third Party agree in writing that it will permit the assignment or transfer of the applicable agreement with Contractor to Commonwealth at the termination or expiration of this Contract. If any such Third Party refuses to provide such a written agreement, then Contractor will notify Commonwealth of this fact. Upon any such notification by Contractor, Commonwealth shall notify Contractor in writing whether Contractor may use such Third Party in connection with Contractor's performance of the Services. If Contractor is notified by Commonwealth that it must not use such Third Party services, then Contractor will make commercially reasonable efforts to locate an alternate Third Party provider, but Contractor is not responsible for any additional Third Party costs that may result from using an alternate provider. If no alternate provider can be located by Contractor, Contractor will so notify Commonwealth and the parties, both acting in good faith and through their respective project managers, will attempt to resolve the issue. The Contractor will not be responsible for any fees associated with the assignment or transfer of the license to the Commonwealth or for any breach by such Third Party of its agreement regarding the assignment or transfer.

h. **Rates and Charges**. Except as provided in this Subsection and *Section 33(j)*, Contractor shall provide all Termination Assistance Services at no additional charge. The parties anticipate that Termination Assistance Services requested by the Commonwealth shall be provided by Contractor using Contractor Personnel already assigned to the performance of the Services and without adversely affecting Contractor's ability to meet its performance obligations. If such Termination Assistance Services cannot be provided using the dedicated resources without adversely affecting Contractor’s ability to meet the Service Levels, charges for such Termination Assistance Services the Contractor may request a change via *Section 27* (Change Control).

i. **Proprietary Communications Network**. If Contractor uses a proprietary communications network to provide the Services, then for a period of up to two (2) years following the effective date of the relevant Assistance Event,

Contractor shall, if requested by the Commonwealth, continue to provide such proprietary communications network and other network Services to the Commonwealth, the Commonwealth and/or its designee at the rates, and subject to the terms and conditions, set forth in this Contract.

j. **Resources.** Contractor shall maintain capability on at least thirty (30) days' notice at all times during the Term to deploy all necessary resources to perform any Termination Assistance Services.

k. **Information.** At the Commonwealth's request, Contractor shall provide to and/or make available for the Commonwealth review, at Contractor's sole cost and expense, any and all reports, data and information that the Commonwealth deems necessary in order to evaluate all options related to an Assistance Event. Contractor shall provide all such reports, data and information regardless of whether the Commonwealth has provided notice of or otherwise declared an Assistance Event.

l. **Breach**. Contractor acknowledges and agrees that, upon any breach or threatened breach by Contractor of its obligations under this *Section 33* (Termination Assistance), Commonwealth shall be entitled to seek injunctive relief, including an order of specific performance. The provisions of this *Section 33* (Termination Assistance) will survive any expiration of the Term and any termination of this Contract.

34. CONTRACT CONTROVERSIES

a. All disputes between the parties arising under or relating to this Contract shall initially be referred in writing by either party to the Contractor Project Manager and the Commonwealth Project Manager. If the Contractor Project Manager and the Commonwealth Project Manager are unable to resolve the dispute within ten (10) Commonwealth business day(s) after referral of the matter to them or upon the earlier request by either the Contractor Project Manager or the Commonwealth Project Manager, the parties shall submit the dispute to the Management Committee for immediate review.

b. Within ten (10) Commonwealth business days after any dispute between the parties is submitted to the Management Committee pursuant to Subparagraph 34(a), the Management Committee shall meet for the purpose of attempting to resolve such dispute. At any meeting of the Management Committee at which more than one (1) dispute will be considered, Commonwealth may establish the order in which such disputes shall be addressed. If the Management Committee is unable to resolve a dispute within fifteen (15) Commonwealth business days after the date of the initial meeting of the Management Committee during which such dispute was considered, the Management Committee shall immediately notify Commonwealth and Contractor pursuant to Subparagraph 34(c).

c. In the event of a controversy or claim arising from the Contract that has not been resolved by the above process, the Contractor must, within six (6) months, file a written claim with the contracting officer for a determination. The claim shall state all grounds upon which the Contractor asserts a controversy exists

(1) The Commonwealth shall review timely-filed claims and issue a final determination, in writing, regarding the claim. The final determination shall be issued within 120 days of the receipt of the claim, unless extended by consent of the contracting officer and the Contractor. The Commonwealth shall send its written determination to the Contractor. If the Commonwealth fails to issue a final determination within the 120 days (unless extended by consent of the parties), the claim shall be deemed denied. The Commonwealth's determination shall be the final order of the purchasing Agency.

(2) Within fifteen (15) days of the mailing date of the determination denying a claim or within one hundred thirty five (135) days of filing a claim if no extension is agreed to by the parties, whichever occurs first, the Contractor may file a statement of claim with the Commonwealth Board of Claims.

d. Each of Commonwealth and Contractor acknowledge that the provision of the Services is critical to the operations of Commonwealth. Accordingly, in the event of a dispute between Commonwealth and Contractor arising under or relating to this Contract, Contractor shall continue to provide the Services in accordance with the terms of this Contract during the pendency of the resolution of such dispute, including the final judicial resolution thereof by Commonwealth's Board of Claims or any appeal thereof, and Commonwealth shall compensate the Contractor pursuant to the terms of the Contract.

35. COMMONWEALTH HELD HARMLESS

a. The Contractor shall hold the Commonwealth harmless from and indemnify the Commonwealth against any and all Third Party claims, demands and actions based upon or arising out of any activities performed by the Contractor and its Personnel and Subcontractors under this Contract, provided the Commonwealth gives Contractor prompt notice of any such claim of which it learns. Pursuant to the Commonwealth Attorneys Act (71 P.S. § 732-101, et seq.), the Office of Attorney General (OAG) has the sole authority to represent the Commonwealth in actions brought against the Commonwealth. The OAG may, however, in its sole discretion and under such terms as it deems appropriate, delegate its right of defense. If OAG delegates the defense to the Contractor, the Commonwealth will cooperate with all reasonable requests of Contractor made in the defense of such suits.

b. Notwithstanding the above, neither party shall enter into any settlement without the other party's written consent, which shall not be unreasonably withheld. The Commonwealth may, in its sole discretion, allow the Contractor to control the defense and any related settlement negotiations.

36. LIMITATION OF LIABILITY

a. The Contractor's liability to the Commonwealth under this Contract shall be limited to two hundred fifty million dollars ($250,000,000). This limitation will apply, except as otherwise stated in this *Section 36* (Limitation of Liability), regardless of the form of action, whether in contract or in tort, including negligence and whether related to direct, consequential, exemplary or punitive damages.

b. This limitation does not apply to damages for:

(1) Bodily injury

(2) Death;

(3) Intentional injury;

(4) Damage to real property or tangible personal property for which the Contractor is legally liable; or

(5) The Contractor's indemnity of the Commonwealth for patent, copyright, trade secret or trademark protection;

(6) Third Party claims related to confidential or proprietary data misuse of confidential information or data;

(7) Milestone Credits, provided, however that payment will accrue against the cap;

(8) Commonwealth's losses resulting from Contractor's gross negligence, willful misconduct; or

(9) Contractor's costs incurred for notification, mitigation, and credit monitoring services required due to a security breach; or

(10) The Commonwealth costs, losses or damages incurred due to Personal Information being accessed, used, released, disclosed and/or acquired in an unauthorized manner while in the control of the Contractor; or

(11) Contractor's abandonment of any Services, wrongful termination of the Contract or willful refusal to provide Termination Assistance Services.

c. Except as provided for in *Section 36(c)(1) through (4)*, neither party will be liable for indirect, incidental, special, consequential, exemplary or punitive damages arising out of or relating to the Contract:

(1) Additional costs to maintain the Services arising from a default by Contractor including the cost of work-arounds;

(2) Loss of or corruption to Commonwealth Data including, without limitation, the cost and expense of rectification of the Data arising out of a default (including for recovering, reconstructing, reformatting or reloading Data), but only to the extent such damages arise out of the failure of Contractor to comply with its obligations under *Section 52* (Virus and Malicious Code)

(3) Expenditure or charges incurred by Commonwealth and rendered necessary as a result of a default by Contractor; and

(4) Any regulatory losses, fines, expenses or other losses suffered by Commonwealth as a result of Contractor's failure to comply with any law or regulation.

37. CONFIDENTIALITY

a. For purposes of this Contract, Confidential Information of a party shall mean (1) with respect to Commonwealth, all Commonwealth Data and other information of Commonwealth or any Commonwealth Agency or any private individual, organization or public agency, in each case to the extent such information and documentation is not permitted to be disclosed to third parties under local, Commonwealth or Federal laws and regulations or pursuant to any policy adopted by Commonwealth or pursuant to the terms of any Third Party agreement to which Commonwealth is a party and (2) with respect to Contractor, all information identified in writing by Contractor as confidential or proprietary to Contractor, its Subcontractors or licensors.

b. All Confidential Information relating to a party shall be held in confidence by the other party to the same extent and in at least the same manner as such party protects its own confidential or proprietary information. Neither party shall disclose, publish, release, transfer or otherwise make available any Confidential Information of the other party in any form to, or for the use or benefit of, any person or entity without the other party's consent. Subject to the other provisions of this Contract, each party shall, however, be permitted to disclose relevant aspects of the other party's Confidential Information to its officers, agents,

Subcontractors and personnel and to the officers, agents, Subcontractors and personnel of its corporate affiliates or subsidiaries to the extent that such disclosure is reasonably necessary for the performance of its duties and obligations under this Contract; provided, however, that such party shall take all reasonable measures to ensure that Confidential Information of the other party is not disclosed or duplicated in contravention of the provisions of this Contract by such officers, agents, Subcontractors and personnel and that such party shall be responsible for any unauthorized disclosure of the Confidential Information of the other party by such officers, agents, Subcontractors or personnel; and further provided, that if the disclosure is by the Commonwealth to another contractor or sub-contractor, such disclosure is subject to a suitable non-disclosure agreement. The obligations in this Paragraph shall not restrict any disclosure by either party pursuant to any applicable law, or in accordance with the order of any court or government agency of competent jurisdiction (provided that the disclosing party shall give prompt notice to the non-disclosing party of such order) and, except to the extent provided otherwise by any applicable law, shall not apply with respect to information which:

(1) is developed by the other party without violating the disclosing party's proprietary rights,

(2) is or becomes publicly known (other than through unauthorized disclosure),

(3) is disclosed by the owner of such information to a Third Party free of any obligation of confidentiality,

(4) is already known by such party without an obligation of confidentiality other than pursuant to this Contract or any confidentiality contract entered into before the Effective Date between Commonwealth and Contractor, or

(5) is rightfully received by the disclosing party free of any obligation of confidentiality.

The confidentiality period for Confidential Information which is related to Equipment, Software, technical specifications, and methods and processes related to data processing and/or computing shall continue from the date of disclosure until two years following expiration or termination of this Contract. The immediately preceding sentence shall not release or relax, in whole or in part, Contractor's confidentiality obligations with respect to information pertaining to any private individual or, with respect to any Commonwealth Agency, information or documentation which is not permitted to be disclosed to third parties under local, Commonwealth or Federal laws and regulations or pursuant to the terms of any Third Party Contract to which Commonwealth is a party.

Nothing in this *Section 37(b)* shall supersede or limit, or be deemed to supersede or limit, any other provision of this Contract pertaining to confidentiality or disclosure of any Commonwealth Data or to any security procedures required to be followed by Contractor or its Personnel and other representatives. In addition to the confidentiality and non-disclosure and other restrictive provisions of this *Section 37(b)* and elsewhere in this Contract, Contractor shall be subject to, and shall be required to abide by, the provisions set forth in the *Exhibits* to the RFP, all of which are required to be incorporated into this Contract to satisfy the requirements of a particular Commonwealth Agency, a particular agency of the Federal government with whom Commonwealth interacts or other Third Party.

c. Each party shall:

(1) Notify the other party promptly of any known unauthorized possession, use or knowledge of the other party's Confidential Information by any person or entity.

(2) Promptly furnish to the other party full details known by such party relating to the unauthorized possession, use or knowledge thereof and shall use reasonable efforts to assist the other party in investigating or preventing the recurrence of any unauthorized possession, use or knowledge of the other party's Confidential Information.

(3) Use reasonable efforts to cooperate with the other party in any litigation and investigation against Third Parties deemed necessary by the other party to protect its proprietary rights.

(4) Promptly use all reasonable efforts to prevent a recurrence of any such unauthorized possession, use or knowledge of the other party's Confidential Information.

d. Each party shall bear the cost it incurs as a result of compliance with this Paragraph. The obligations in this Paragraph shall not restrict any disclosure by either party pursuant to any applicable law or pursuant to the order of any court or other legal process or government agency of competent jurisdiction (provided that the disclosing party shall give prompt notice to the non-disclosing party of such order).

e. There shall be no restriction with respect to the use or disclosure of any ideas, concepts, know-how or data processing techniques developed alone or jointly with Commonwealth in connection with Services provided to Commonwealth under this Contractor.

f. The Contractor shall use the following process when submitting information to the Commonwealth it believes to be confidential and/or proprietary information or trade secrets:

(1) Prepare an un-redacted version of the appropriate document, and

(2) Prepare a redacted version of the document that redacts the information that is asserted to be confidential or proprietary information or a trade secret, and

(3) Prepare a signed written statement that states:

(i) the attached document contains confidential or proprietary information or trade secrets;

(ii) the Contractor is submitting the document in both redacted and un-redacted format in accordance with 65 P.S. § 67.707(b); and

(iii) the Contractor is requesting that the document be considered exempt under 65 P.S. § 67.708(b)(11) from public records requests.

(iv) Submit the two documents with the signed written statement to the Commonwealth.

g. When the Contract expires or terminates, and at any other time at the written request of a party, the other party must promptly return to such party all of such party's Confidential Information and Data (and all copies of this information) that is in the other party's possession or control, in whatever form. With regard to Commonwealth's Confidential Information and/or Data, Contractor will comply with the requirements of Section 9(d).

38. SENSITIVE INFORMATION

a. The Contractor shall not publish or otherwise disclose, except to the Commonwealth or the Contractor's Subcontractors, any information or data obtained hereunder from private individuals, organizations, or public agencies, in a way that allows the information or data furnished by or about any particular person or establishment to be identified.

b. The parties shall not use or disclose any information about a recipient receiving services from, or otherwise enrolled in, a Commonwealth program affected by or benefiting from services under this Contract for any purpose not connected with the parties' Contract responsibilities.

c. Contractor, as directed, shall comply with all federal or state laws and regulations related to the use of information that constitutes protected health information (PHI) as defined by the regulations promulgated pursuant to the

Health Insurance Portability and Accountability Act (HIPAA). By signing this Contract, the Contractor agrees to the terms of the Business Associates Contract, which is incorporated into this Contract as Appendix A. If Agency, or relevant portion thereof, is a Covered Entity as defined in HIPAA, and the Contractor is performing the work of a Business Associate, the Agency will fill in the blanks in the attached Appendix and will present the complete Business Associate Contract to the Contractor through agreed-upon communication channels. It is understood that Appendix A is only applicable if the Agency follows the above-mentioned procedures. If not applicable to the entire Agency, Appendix A is only applicable with respect to the internal entities indicated by the Agency and agreed to by the Contractor.

d. Contractor will comply with all obligations applicable to it under all applicable data protection legislation in relation to all personal data that is processed by it in the course of performing its obligations under this Contract including by:

(1) Maintaining a valid and up to date registration or notification under the data protection legislation; and

(2) Complying with all data protection legislation applicable to cross border data flows of personal data and required security measures for personal data.

39. PATENT, COPYRIGHT, TRADEMARK, AND TRADE SECRET PROTECTION

a. The Contractor shall hold the Commonwealth harmless from any suit or proceeding which may be brought by a Third Party against the Commonwealth, its departments, officers or employees for the alleged infringement of any United States or foreign patents, copyrights, or trademarks, or for a misappropriation of trade secrets arising out of performance of this Contract, including all work, services, materials, reports, studies, and computer programs provided by the Contractor, and in any such suit or proceeding will satisfy any final award for such infringement, including costs. The Commonwealth agrees to give Contractor prompt notice of any such claim of which it learns. Pursuant to the Commonwealth Attorneys Act 71 P.S. § 732-101, *et seq*., the Office of Attorney General (OAG) has the sole authority to represent the Commonwealth in actions brought against the Commonwealth. The OAG may, however, in its sole discretion and under the terms it deems appropriate, delegate its right of defense. If OAG delegates the defense to the Contractor, the Commonwealth will cooperate with all reasonable requests of Contractor made in the defense of such suits. No settlement which prevents the Commonwealth from continuing to use the Developed Materials as provided herein shall be made without the Commonwealth's prior written consent. In all events, the Commonwealth shall have the right, to participate in the defense of any such suit or proceeding through counsel of its own choosing. It is expressly agreed by the Contractor that, in the event it requests

that the Commonwealth to provide support to the Contractor in defending any such claim, the Contractor shall reimburse the Commonwealth for all reasonable expenses (including attorneys' fees, if such are made necessary by the Contractor's request) incurred by the Commonwealth for such support. If OAG does not delegate the defense of the matter, the Contractor's obligation to indemnify ceases. The Contractor will, at its expense, provide whatever cooperation OAG requests in the defense of the suit.

b. If the defense of the suit is delegated to the Contractor, the Contractor shall pay all damages and costs finally awarded therein against the Commonwealth, when such damages and costs are required to be paid. If information and assistance are furnished by the Commonwealth at the Contractor's written request, it shall be at the Contractor's expense, but the responsibility for such expense shall be only that within the Contractor's written authorization.

c. If the products, materials, reports, studies, or computer programs furnished hereunder become subject to a claim of infringement of a United States patent, copyright, or trademark, or for a misappropriation of trade secret, or if any of the products, materials, reports, studies or computer programs provided by the Contractor are in such suit or proceeding held to constitute infringement and the use or publication thereof is enjoined, then without diminishing the Contractor's obligation to satisfy any final award, the Contractor may, at its option and expense, substitute functional equivalents for the alleged infringing products, materials, reports, studies, or computer programs or, at the Contractor's option and expense, obtain the rights for the Commonwealth to continue the use of such products, materials, reports, studies, or computer programs or modify them so that they are no longer infringing.

d. If the Contractor is unable to do any of the preceding, the Contractor agrees to pay the Commonwealth:

(1) Any amounts paid by the Commonwealth less a reasonable amount based on the acceptance and use of the Deliverable;

(2) Any license fee less an amount for the period of usage of any Software; and

(3) The prorated portion of any Fees representing the time remaining in any period of service for which payment was made.

e. The obligations of the Contractor under this *Section* 39 (Patent, Copyright, Trademark, and Trade Secret Protection) continue without time limit and survive the termination of this Contract.

f. Notwithstanding the above, the Contractor shall have no obligation for:

(1) Modification of any product, service, or deliverable provided by the Commonwealth or any Third Party, except for the Contractor or any of its Subcontractors;

(2) Any material provided by the Commonwealth to the Contractor and incorporated into, or used to prepare, a product, Service, or Deliverable;

(3) Use of the product, Service, or Deliverable in other than its specified operating environment;

(4) The combination, operation, or use of the product, Service, or Deliverable with other products, services, or deliverables not provided by the Contractor as a system or the combination, operation, or use of the product, Service, or Deliverable, with any products, data, or apparatus that the Contractor did not provide;

(5) Infringement of a non-Contractor product alone;

(6) The Commonwealth's distribution, marketing or use beyond the scope contemplated by the Contract;

(7) The Commonwealth's failure to use corrections or enhancements made available to the Commonwealth by the Contractor at no charge;

(8) Any infringement or claim thereof against the Commonwealth brought prior to the execution of this Contract, unless the infringement or claim relates to services provided by Contractor under another contract with the Commonwealth; or

(9) Infringement related to content provided by or on behalf of the Commonwealth, except as provided by the Contractor or any of its Subcontractors or suppliers.

g. The obligation to defend and indemnify the Commonwealth, under the terms of this *Section 39* (Patent, Copyright, Trademark, and Trade Secret Protection), shall be the Contractor's sole and exclusive obligation and the Commonwealth's sole and exclusive remedy against the Contractor for the infringement or misappropriation of intellectual property.

40. PROPRIETARY RIGHTS

a. **Commonwealth Software**. As between Commonwealth and Contractor, all Commonwealth Software shall be and shall remain the exclusive property of Commonwealth or its licensors, and Contractor shall have no rights or interests in

the Commonwealth Software by virtue of this Contract except as described in this *Section 40* (Proprietary Rights) or elsewhere in this Contract. Commonwealth hereby grants to Contractor, at no cost to Contractor, for the limited purpose of providing the Services, a nonexclusive, nontransferable, royalty-free right (subject to the terms of any Third Party agreement to which Commonwealth is a party and which theretofore is disclosed to Contractor) to (1) have access to the Commonwealth Software, (2) copy the Commonwealth Software for archival purposes or as may otherwise be required by this Contract, (3) modify the Commonwealth Software as required by this Contract, if permitted by the Software licensing terms and pursuant to the terms of Commonwealth Third Party Software license agreement, if applicable, and (4) sublicense Contractor's Subcontractors approved by Commonwealth to do any of the foregoing; provided, however, that neither Contractor nor any of its Subcontractors may decompile or reverse engineer, or attempt to decompile or reverse engineer, any of the Commonwealth Software.

As of the Effective Date and subject to the terms of any Third Party agreement to which Commonwealth is a party, (1) Commonwealth shall, at no cost to Contractor, provide Contractor with access to the Commonwealth Software in the form in use by Commonwealth as of the Effective Date and (2) Contractor, as part of the Services, shall compile and, as changes are made, update a list of all of the Commonwealth Software then in use by Contractor or any of its Subcontractors in connection with Contractor's performance of the Services. Upon the expiration or termination for any reason of Contractor's obligation to provide the Services or of this Contract, the rights granted to Contractor in this *Section 40(a)* shall immediately revert to Commonwealth or Commonwealth's designee, and Contractor forthwith shall, at no cost to Commonwealth, deliver to Commonwealth all of the Commonwealth Software (including any related source code and object code in Contractor's possession or under its control) in the form in use as of the effective date of such expiration or termination, together with a current copy of the list of Commonwealth Software in use as of the date of such expiration or termination. Concurrently therewith, Contractor shall destroy or erase all other copies of any of the Commonwealth Software then in Contractor's possession or under its control unless otherwise instructed by Commonwealth; provided, however, pursuant to and if permitted by the Commonwealth's license agreement for Commonwealth Third Party Software, if applicable, that Contractor may retain one archival copy of such Commonwealth Software, including the Developed Software, until the later of six (6) years after such expiration or termination of this Contract and the final resolution of any actively asserted pending disputes between the parties, such retention being for the sole purpose of establishing Contractor's performance under this Contract.

b. **Contractor Software and Contractor Tools**. As between Commonwealth and Contractor, all Contractor Software and Contractor Tools shall be and shall remain the exclusive property of Contractor, and Commonwealth shall have no rights or interests in the Contractor Software or the Contractor Tools by virtue of

this Contract except as described in this *Section 40(b)*. As part of the Services, Contractor shall during the Term (1) use the Contractor Software and the Contractor Tools to provide the Services, (2) make available the commercially available Contractor Software and the commercially available Contractor Tools to Commonwealth for use by Commonwealth solely in connection with the Services, and (3) maintain on Commonwealth's premises and make available to Commonwealth upon Commonwealth's request from time to time, for archival purposes only, a copy of the Contractor Software and the Contractor Tools owned by Contractor or its Subcontractors and then being used by Contractor to provide the Services.

Upon the expiration or termination for any reason of Contractor's obligation to provide the Services under this Contract and at the request of Commonwealth, Contractor shall, subject to mutually agreed terms and conditions, (1) grant, or cause its Subcontractors to grant, to Commonwealth a nonexclusive, nontransferable license to use and, if permitted by the terms of mutually agreed terms and conditions relating thereto, modify and make derivative works of, and unless Commonwealth terminates this Contract pursuant to the terms of *Section 32(a),(b), or (f)* to grant to third parties engaged by Commonwealth the right to use and, if permitted by mutually agreed terms and conditions relating thereto, modify and make derivative works of, all or any portion of the commercially available Contractor Software and the commercially available Contractor Tools owned by Contractor or its Subcontractors theretofore being used by Contractor in connection with the Services, the foregoing rights being granted to the extent reasonably necessary to facilitate Commonwealth's or such Third Party's performance of the activities or services substantially equivalent to the Services to be provided by Contractor under this Contract immediately prior to such expiration or termination and (2) deliver to Commonwealth the object code version of such commercially available Contractor Software and such commercially available Contractor Tools in the form being used by Contractor in connection with the Services immediately prior to such expiration or termination.

It is understood and agreed by Contractor that the rights granted to Commonwealth hereunder in respect of the commercially available Contractor Software and the commercially available Contractor Tools shall not restrict Commonwealth from using such Contractor Software and such Contractor Tools in the manner in which such items were used by Contractor and its Subcontractors to provide the Services immediately prior to the expiration or termination of this Contract. The foregoing obligations of Contractor shall be subject to mutually agreed terms and conditions. In consideration of the grant to Commonwealth of the foregoing license, Commonwealth shall be assessed license fees hereunder not in excess of any license fees therefor being offered, as of the date of termination, by Contractor or its Subcontractors, to their respective state governmental customers generally, unless Commonwealth terminates this Contract pursuant to the terms of *Section 32(a),(b) or (f)*, in which case the then-prevailing license fees of Contractor and its Subcontractors, as applicable, shall

apply. The foregoing shall not limit or otherwise affect Commonwealth's obligations to pay Third Party assignment or transfer fees as contemplated in *Section 33* (Termination Assistance); provided, however, that Commonwealth shall not be assessed any additional fees in respect thereof by Contractor.

c. **Developed Documentation.** Documentation developed by Contractor specifically for the Commonwealth in connection with its performance under this Contract is the sole and exclusive property of the Commonwealth and shall be considered "works made for hire" under the United States Copyright Act of 1976, as amended, 17 United States Code. In the event that the documentation does not fall within the specifically enumerated works that constitute works made for hire under the United States copyright laws, Contractor agrees to assign and, upon their authorship or creation, expressly and automatically assigns all copyright interests, proprietary rights, trade secrets, and other right, title, and interest in and to such documentation to Commonwealth. Commonwealth shall have all rights accorded an owner of copyright under the United States copyright laws including, but not limited to, the exclusive right to reproduce the documentation in multiple copies, the right to distribute, copies by sales or other transfers, the right to register all copyrights in its own name as author in the United States and in foreign countries, the right to prepare derivative works based upon the Creative Works and the right to display the documentation. Upon completion or termination of this Contract, all working papers, files and other documents related to the documentation shall immediately be delivered by Contractor to the Commonwealth. Contractor warrants that the documentation is original and does not infringe any copyright, patent, trademark, or other intellectual property right of any Third Party and are in conformance with the intellectual property laws of the United States. Provided however that Commonwealth's sole remedy for breach of this warranty is the indemnity contained in *Section 39* (Patent, Copyright, Trademark, and Trade Secret Protection).

d. All literary works, or other works of authorship (such as application programs, listings, programming tools, documentation, reports, drawings, procedure manuals and similar works) ("Developed Materials") developed hereunder shall be treated in accordance with the following general principles:

(1) If and to the extent Developed Materials modify, improve or enhance software programs generally licensed by Contractor to end-users, then such Developed Materials shall be the property of Contractor and Contractor hereby grants to Commonwealth a perpetual, non-exclusive, nontransferable, royalty-free license to use such Developed Materials in Commonwealth's receipt and use of the Services;

(2) If and to the extent Developed Materials modify, improve or enhance software or other materials owned by Commonwealth or licensed to Commonwealth by a Third Party (i.e., a licensor other than Contractor

or any Contractor Subcontractor), then such modification, improvement or enhancement and all related intellectual property rights therein shall, as between Commonwealth and Contractor, be the property of Commonwealth;

(3) If and to the extent Developed Materials constitute a newly created software program or module, and if Commonwealth funds the development cost thereof to any extent, then such software program or module and all related intellectual property rights therein shall be the property of Commonwealth; and

(4) If and to the extent Developed Materials constitute documentation, reports, drawings, procedure manuals and similar works, such Developed Materials shall be the property of Commonwealth. Contractor will not place trademarks or copyright notices on any such Developed Materials.

(5) Any Data related to the use of the Services by the Commonwealth shall be the property of the Commonwealth. For this purpose, Data includes ordering information, inventories, etc. At the end of the Contract, regardless of how it is ended, or at any time requested by the Commonwealth, the Contractor will provide the Commonwealth with such Data consistent with section 9(d).

e. **Residual Knowledge**. Either party, in the course of conducting business, may use any ideas, concepts, and know-how, relating to the Services which Contractor or Commonwealth (alone or jointly with the Commonwealth) develops or learns in connection with Contractor's provision of Services to Commonwealth under this Contract.

41. PUBLICATION RIGHTS AND/OR COPYRIGHTS

a. The Contractor shall not publish any of the results of the work, which identify the Commonwealth, without the written permission of the Commonwealth. The publication shall include the following statement: "The opinions, findings, and conclusions expressed in this publication are those of the author and not necessarily those of the Commonwealth of Pennsylvania." The Contractor shall not include in the documentation any copyrighted matter, unless the Contractor provides the Commonwealth with written permission of the copyright owner.

b. Except as otherwise provided in *Section 40* (Proprietary Rights) and the confidentiality provisions of *Section 37* (Confidentiality), the Commonwealth shall have unrestricted authority to reproduce, distribute, and use any submitted report or data designed or developed and delivered to the Commonwealth as part of the performance of the Contract.

c. Rights and obligations of the parties under this *Section 41* (Publication Rights and/or Copyrights) survive the termination of this Contract.

42. REPORTS AND DATA

a. Data. Commonwealth shall supply to Contractor the Commonwealth Data in the form maintained by the Commonwealth on such time schedules as may be agreed to by Commonwealth and Contractor from time to time. All Commonwealth Data is and shall remain the property of Commonwealth. Subject to *Section 40* (Proprietary Rights), the Commonwealth Data shall not be (1) used by Contractor or Contractor Subcontractors other than in connection with providing the Services, and then only in accordance with the terms of this Contract, (2) disclosed, sold, assigned, leased or otherwise provided to third parties by Contractor or Contractor Subcontractors without Commonwealth's consent and any applicable consent required by any federal governmental entity, or (3) commercially exploited by or on behalf of Contractor or Contractor Subcontractors.

b. Reports. As part of the Services, Contractor shall provide the reports, in electronic form, to Commonwealth. The reports shall be prepared by Contractor and provided to the Commonwealth in a manner readable by a normal Windows based personal computer. Acceptable formats include but are not limited to: Adobe Acrobat (PDF), Microsoft Word, Microsoft Excel, Microsoft PowerPoint, Text, Comma Separated Values (CSV).

c. Correction of Errors. In the event of any errors or inaccuracies in any of the Commonwealth Data or the reports, or any other data processing errors or unexpected interruptions (e.g., "abends" or “freeze”), Contractor and Commonwealth shall work together in good faith, using all reasonable efforts and commencing immediately upon the discovery of the situation, to correct such error, inaccuracy or interruption. The foregoing obligations of Contractor under this *Section 42(c)* shall be subject to any limitations placed upon Contractor's access to the Commonwealth Data by Commonwealth or pursuant to this Contract. Promptly upon the completion of the correction of such error, inaccuracy or interruption, the Commonwealth Project Manager and the Contractor Project Manager shall meet to determine and document the cause thereof. If the error, inaccuracy or interruption is determined to be caused by the error, negligence or omission of Contractor to perform an obligation under this Contract, there shall be no charge to Commonwealth for Contractor's participation in such correction. If the error, inaccuracy or interruption is determined to be caused by the error, negligence or omission of Commonwealth to perform an obligation under this Contract, Commonwealth shall reimburse Contractor for Contractor's out-of-pocket expenses paid by Contractor to third parties (other than Contractor's or any Contractor's Subcontractor's employees) for expertise not otherwise possessed by or

available to Contractor and Contractor's expenses for its Personnel or the Personnel of any Contractor Subcontractor not theretofore engaged in the provision of the Services.

d. Return of Data. At no cost to Commonwealth and as part of the Services, Contractor shall, upon Commonwealth's request at any time and at the cessation of the Termination Assistance return Commonwealth's Data consistent with *section 9(d).*

43. SECURITY AND PROTECTION OF INFORMATION

a. At all times during the Term, Contractor shall provide all Services, and use all resources related thereto, in accordance with the Commonwealth's security requirements, including the prevention and detection of fraud, abuse, or other inappropriate use or access of systems and networks by all appropriate means, including network management and maintenance applications and tools, and the use of appropriate encryption technologies. If the Contractor incurs additional costs as a result of changes to Commonwealth's security requirements, it may follow the process set out in *Section 27* (Change Control) of this Agreement. In addition, all Contractor Personnel (including personnel of any Subcontractors) shall be subject to and shall at all times conform to the Commonwealth's laws, rules, and requirements for the protection of premises, materials, equipment, and personnel, as they have been previously disclosed to Contractor in writing, including those set forth in the *Exhibits* to the RFP. Any violations or disregard of these rules shall be cause for denial of access by such personnel to the Commonwealth's property. Contractor shall exercise due care and diligence to prevent any injury to person or damage to property while on the Commonwealth's premises. The operation of Contractor vehicles or private vehicles of Contractor personnel on the Commonwealth's property shall conform to posted and other regulations and safe driving practices. Vehicular accidents on the Commonwealth's property and involving Contractor personnel shall be reported promptly to the appropriate Commonwealth's security personnel.

b. The Pennsylvania State Police's Criminal Justice Information Services Policy ("CJIS Policy"), is set forth in *Exhibits G.6 and G.7* to the RFP, and is hereby incorporated by this reference into this Contract. Contractor acknowledges and agrees that it is bound by all applicable provisions of the CJIS Policy. Contractor and the Commonwealth further agree that, in accordance with the CJIS Policy, the Commonwealth does not anticipate and will not authorize any requests to Contractor for the criminal history record information covered by the CJIS Policy, because Contractor is performing an IT support function. The Commonwealth's Office of Attorney General's CHRIA Handbook, attached as *Exhibit G.12* to the RFP, is also incorporated by reference into this Contract. Contractor acknowledges and agrees that it is bound by all applicable provisions of the CHRIA Handbook.

.

44. BACKGROUND CHECKS

a. The Contractor must, at its expense, arrange for a background check for each of its employees, as well as for the employees of its Subcontractors, who will have access to Commonwealth Services Locations, either through on site or remote access. Background checks will not be conducted by the Commonwealth but rather will be conducted by Contractor or its Subcontractors according to Contractor policy and practice and consistent with ITB-SEC009. The background check must be conducted prior to initial access by a Contractor employee and every two (2) years thereafter or at a longer interval if required by applicable law.

b. Before the Commonwealth will permit Contractor Personnel access to Commonwealth facilities, the Contractor must provide written confirmation to the office designated by the Agency that the background check has been conducted. If, at any time, it is discovered that a Contractor employee has a criminal record that includes a felony or misdemeanor involving terroristic threats, violence, use of a lethal weapon, or breach of trust/fiduciary responsibility; or which raises concerns about building, system, or personal security, or is otherwise job-related, the Contractor shall notify the Commonwealth Contracting Officer immediately, shall not assign that employee to any Commonwealth facilities, shall remove any access privileges already given to the employee, and shall not permit that employee remote access to Commonwealth facilities or systems, unless the Agency consents, in writing, prior to the access being provided. The Agency may withhold its consent at its sole discretion. Failure of the Contractor to comply with the terms of this Paragraph may result in default of the Contractor under its Contract with the Commonwealth.

c. The Commonwealth specifically reserves the right of the Commonwealth to conduct background checks over and above that described herein.

45. INSURANCE

a. Contractor Insurance Requirements. During the Contract Term, Contractor shall maintain at its own expense, insurance of the type and in the amounts specified below and issued by companies authorized to conduct such business under the laws of Pennsylvania:

(1) Statutory workers' compensation in accordance with all applicable Federal, state and local requirements, and employer liability in an amount not less than $2,000,000 per occurrence;

(2) Comprehensive general public liability (including contractual liability insurance) in an amount not less than $5,000,000 per occurrence;

(3) Comprehensive automobile liability covering all vehicles that Contractor owns, hires, or leases in an amount not less than $5,000,000 per occurrence (combined single limit for bodily injury and property damages).

(4) Personal property insurance, on a replacement basis, covering all of Contractor's and Contractor's Subcontractors' personal property located at any Contractor Services Location.

(5) Professional liability/error & omission in the aggregate amount of not less than $15,000,000.

(6) Comprehensive crime insurance in an amount of not less than $15,000,000 per claim.

(7) Network/Cyber Liability Insurance (including coverage for Technology Professional Liability if not covered under Contractor's Professional Liability/Errors and Omissions Insurance referenced above) in the amount of $20,000,000, per occurrence.

(8) Umbrella/excess in an aggregate amount of not less than $30,000,000.

b. Insurance Requirements for Subcontractors. During the Contract Term, Contractor shall require each of its Subcontractors listed in *Schedule L* (Approved Subcontractors) and any other Subcontractors performing any Services on-site at any of the Contractor Services Locations, to maintain at their own expense or Contractor's expense, insurance of the type and in the amounts specified below:

(1) Statutory workers' compensation in accordance with all applicable Federal, state and local requirements, and employer liability in an amount not less than $1,000,000 per occurrence;

(2) Comprehensive general public liability (including contractual liability insurance) in an amount not less than $2,000,000 per occurrence;

(3) If any of the Subcontractor personnel will be on-site at any of the Commonwealth's or Contractor's facilities, comprehensive automobile liability covering all vehicles owned, hired or leased by that Subcontractor and in an amount not less than $2,000,000 per occurrence (combined single limit for bodily injury and property damages);

(4) If the Subcontractor personnel will be on-site at any of Commonwealth's or Contractor's facilities, personal property

(5) insurance, on a replacement basis, covering all of that Subcontractor's personal property located at any such facilities; and

(6) Network/Cyber Liability Insurance (including coverage for Technology Professional Liability if not covered under Contractor's Professional Liability/Errors and Omissions Insurance referenced above) in the amount of $10,000,000, per occurrence; and

(7) Errors & Omissions liability in the amount of $2,000,000 each claim and aggregate (if applicable).

c. Prior to the expiration of any then effective insurance policy, Contractor shall furnish to Commonwealth certificates of insurance or other appropriate documentation (including evidence of renewal of insurance) evidencing all coverage referenced in this *Section 45* (Insurance), as applicable, and naming Commonwealth as an additional insured to the extent of Contractor's indemnities contained in this Contract. Contractor shall have included in all policies of insurance required hereunder a waiver by the insurer of all right of subrogation against Commonwealth in connection with any loss or damage thereby insured against. Such certificates or other documentation will include a provision whereby thirty (30) days' notice must be received by Commonwealth prior to coverage cancellation or alteration of the coverage by either Contractor or its Subcontractors or the applicable insurer. Such cancellation or alteration shall not relieve Contractor of its continuing obligation to maintain insurance coverage in accordance with this *Section 45* (Insurance).

d. For purposes hereof, Contractor and its Subcontractors may maintain "umbrella" insurance policies to fulfill the foregoing insurance requirements, as appropriate.

46. WARRANTIES AND AGREEMENTS

a. Contractor represents and warrants that as of the Contract's Effective Date:

(1) It is a corporation duly incorporated, validly existing, and in good standing under the laws of Delaware

(2) It has all requisite corporate power and authority to execute, deliver, and perform its obligations under this Contract.

(3) Contractor is duly licensed, authorized and qualified to do business and is in good standing in Pennsylvania and in every other jurisdiction where Services will be performed by Contractor pursuant to this Contract in which a license, authorization or qualification is required for the ownership or leasing of its assets or the transaction of business of the character transacted by it except where the failure to be so licensed, authorized or qualified would not have a material adverse

effect on Contractor's ability to fulfill its obligations under this Contract.

(4) The execution, delivery and performance of this Contract by Contractor has been duly authorized by Contractor.

b. Contractor agrees that:

(1) Contractor has not disclosed any Confidential Information of Commonwealth.

(2) The Contractor Software does not and will not, and the Developed Software and the Services will not, infringe upon the proprietary rights of any Third Party, provided that Contractor will have no obligation with respect to any losses to the extent the same arise out of or in connection with Commonwealth's modification or misuse of Equipment, systems, programs, or products or Commonwealth's combination, operation or use with devices, data, equipment, systems, programs or products not furnished by Contractor under this Contract.

(3) Contractor Personnel and Subcontractors that Contractor will use to provide and perform the Services have and during the Term will have, the suitable knowledge, skills, experience, qualifications and resources to provide and perform the Services:

(i) In accordance with the Contract.

(ii) In a diligent, workmanlike manner with due care and skill, consistent with the required level of quality and performance and in accordance with the Service Levels.

(4) Contractor shall cooperate fully with Commonwealth and with any Third Party appointed by Commonwealth to the extent that such cooperation may be necessary to permit Commonwealth or such Third Parties to complete any work related to or impacted by the Services provided to Commonwealth by Contractor under the Contract.

(5) Contractor shall collaborate fully with Commonwealth or with any Third Party appointed by Commonwealth to the extent that such cooperation may be necessary to permit Commonwealth or such Third Parties to in-source or transfer to a Third Party any aspect of the Services then provided by Contractor under the Contract.

c. Commonwealth represents, warrants and covenants that as of the Contract’s Effective Date:

(1) It is a sovereign entity and has all requisite power and authority to execute, deliver, and perform its obligations under this Contract.

(2) It has, or at any time of provision to Contractor, will have the right to use and to disclose to Contractor and Contractor Subcontractors and to allow Contractor and Contractor Subcontractors to use in accordance with the terms of this Contract any Commonwealth Software so disclosed to Contractor.

47. CONTRACTOR RESPONSIBILITY PROGRAM

a. The Contractor certifies, for itself and all its Subcontractors, that as of the date of its execution of this Contract, that neither the Contractor, nor any Subcontractors, nor any suppliers are under suspension or debarment by the Commonwealth or any governmental entity, instrumentality, or authority and, if the Contractor cannot so certify, then it agrees to submit, along with its bid, a written explanation of why such certification cannot be made.

b. The Contractor must also certify, in writing, that as of the date of its execution of this Contract, it has no tax liabilities or other Commonwealth obligations.

c. The Contractor's obligations pursuant to these provisions are ongoing from and after the effective date of the Contract through the termination date thereof. Accordingly, the Contractor shall have an obligation to inform the Commonwealth if, at any time during the term of the Contract, it becomes delinquent in the payment of taxes, or other Commonwealth obligations, or if it or any of its Subcontractors are suspended or debarred by the Commonwealth, the federal government, or any other state or governmental entity. Such notification shall be made within 15 days of the date of suspension or debarment.

d. The failure of the Contractor to notify the Commonwealth of its suspension or debarment by the Commonwealth, any other state, or the federal government shall constitute an event of default of the Contract with the Commonwealth.

e. The Contractor agrees to reimburse the Commonwealth for the reasonable costs of investigation incurred by the Office of State Inspector General for investigations of the Contractor's compliance with the terms of this or any other agreement between the Contractor and the Commonwealth, which results in the suspension or debarment of the Contractor. Such costs shall include, but shall not be limited to, salaries of investigators, including overtime; travel and lodging expenses; and expert witness and documentary fees. The Contractor shall not be responsible for investigative costs for investigations that do not result in the Contractor's suspension or debarment.

f. The Contractor may obtain a current list of suspended and debarred Commonwealth contractors by either searching the internet at *http://www.dgs.state.pa.us* or contacting the:

Department of General Services
Office of Chief Counsel
603 North Office Building
Harrisburg, PA 17125
Telephone No. (717) 783-6472
FAX No. (717) 787-9138

48. OFFSET PROVISION FOR COMMONWEALTH CONTRACTS

The Contractor agrees that the Commonwealth may set off the amount of any state tax liability or other obligation of the Contractor or its subsidiaries to the Commonwealth against any payments due the Contractor under any contract with the Commonwealth.

49. TAXES-FEDERAL, STATE, AND LOCAL

a. **Commonwealth Exemption**. No taxes from which the Commonwealth is exempt shall be included in the Fee. The Commonwealth is exempt from all excise taxes imposed by the Internal Revenue Service and has accordingly registered with the Internal Revenue Service to make tax-free purchases under registration No. 23-23740001-K. With the exception of purchases of the following items, no exemption certificates are required and none will be issued: undyed diesel fuel, tires, trucks, gas-guzzler emergency vehicles, and sports fishing equipment. The Commonwealth is also exempt from Pennsylvania sales tax, local sales tax, public transportation assistance taxes, and fees and vehicle rental tax. The Department of Revenue regulations provide that exemption certificates are not required for sales made to governmental entities and none will be issued.

b. **Contractor Taxes**. Fees are inclusive of any applicable sales, use, personal property and other taxes attributable to periods on or after the Effective Date and based upon or measured by Contractor's cost in acquiring or providing equipment, materials, supplies or services furnished or used by Contractor in performing or furnishing the Services, including without limitation, all personal property and use taxes, if any, due on Contractor Equipment.

c. **Segregation of Fees**. Commonwealth and Contractor shall cooperate to segregate the Fees into the following separate payment streams: (1) those for Services, and (2) those for which Contractor functions merely as a paying agent for Commonwealth in receiving goods, supplies, or services (including leasing and licensing arrangements).

50. POLICIES AND PROCEDURES

Contractor shall comply with
Commonwealth standards set out in IT Bulletins, standards and procedures related to the Services, including but not limited to those governing security, treatment of personal information, quality, change, and problem management, safety, data privacy and data security, and pervasive and transaction controls; provided, however that the Contractor may submit a request under *Section 27* (Change Control), if it believes that it has incurred costs or delay in complying with this Section due to changes in the IT Bulletins, standards and procedures related to the Services.

51. AUDIT OBLIGATIONS

a. SINGLE AUDIT ACT OF 1984

In compliance with the *Single Audit Act of 1984*, the Contractor agrees to the following:

(1) This Contract is subject to audit by federal and state agencies or their authorized representative in accordance with the auditing standards promulgated by the Comptroller General of the United States and specified in *Government Auditing Standards,* 1994 Revisions (Yellow Book).

(2) The audit requirement of this Contract will be satisfied if a single audit is performed under the provisions of the *Single Audit Act of 1984, 31 U.S.C.* § *7501, et seq*., and all rules and regulations promulgated pursuant to the Act.

(3) The Commonwealth reserves the right for federal and state agencies or their authorized representatives to perform additional audits of a financial/compliance, economy/efficiency, or program results nature, if deemed necessary.

(4) The Contractor further agrees to comply with requirements that may be issued by the state Agency upon receipt of additional guidance received from the federal government regarding the *Single Audit Act of 1984.*

b. Access by Commonwealth

(1) **Processing**. Upon reasonable written notice from Commonwealth, Contractor and Contractor Subcontractors shall provide such auditors and inspectors with access to the Services Locations and the Software and the Equipment for the purpose of performing audits or inspections of the Services and the operations of Commonwealth and Contractor,

subject always to Contractor's reasonable security requirements. Contractor shall provide, and shall cause Contractor Subcontractors to provide, to such auditors and inspectors any reasonable assistance that they may require. If any such audit results in Contractor being notified that it or any Contractor Subcontractor is not in compliance with any law, regulation, audit requirement or generally accepted accounting principle relating to the Services, Contractor shall, and shall cause such Contractor Subcontractor to, promptly take actions to comply with such law, regulation, audit requirement or generally accepted accounting principle. Commonwealth shall bear the expense of any such compliance that is (1) required by a law, regulation or other audit requirement relating to Commonwealth's operations to the extent the same was first enacted on or after the Effective Date or (2) necessary due to Commonwealth's noncompliance with any law, regulation or audit requirement imposed on Commonwealth. Contractor shall bear the expense of any such response that is (1) required by a law, regulation or other audit requirement relating to Contractor's business or enacted prior to the Effective Date, (2) to be performed by Contractor as part of the Services, or (3) necessary due to Contractor's noncompliance with any law, regulation or audit requirement imposed on Contractor. As part of the Services, Contractor shall provide to Commonwealth summary data of those portions of Contractor's and Contractor Subcontractors' internal audit reports relating solely to the Services.

(2) **Fees**. Upon reasonable written notice from Commonwealth, Contractor shall provide such auditors and inspectors with access to such financial records and supporting documentation as may reasonably be requested by Commonwealth, and such auditors and inspectors may audit the Fees charged to Commonwealth to determine that such Fees are accurate and in accordance with this Contract.

(3) **Overcharges**. If, as a result of such audit, Commonwealth determines that Contractor has overcharged Commonwealth, Commonwealth shall notify Contractor of the amount of such overcharge and Contractor shall promptly pay to Commonwealth the amount of the overcharge, plus interest at the rate of six percent (6%) per annum, calculated from the date of receipt by Contractor of the overcharged amount until the date of repayment to Commonwealth. In the event any such audit reveals an overcharge to Commonwealth during any calendar month during the Term exceeding fifteen percent (15%) of all Fees in the aggregate paid by Commonwealth in respect of such calendar month, Contractor shall reimburse Commonwealth for the cost of such audit. If as a result of such audit, Commonwealth or Contractor determines that Contractor has undercharged Commonwealth, Commonwealth shall promptly pay to Contractor the

amount of such undercharge, without interest. Any disagreement between the parties with regard to the results of any such audit shall be treated as a dispute between the parties subject to the provisions of *Section 34* (Contract Controversies).

(4) **Record Retention**. As part of the Services, Contractor shall (1) retain records and supporting documentation sufficient to document the Services and the Fees paid or payable by Commonwealth under this Contract for at least three (3) years after the expiration or termination of this Contract or until all questioned items relating to such records and documentation are resolved by the parties, whichever is later, and (2) upon notice from Commonwealth, provide such auditors and inspectors as are designated by Commonwealth with reasonable access to such records and documentation for inspection, audit and reproduction. Such records and documentation shall be in such detail as will properly reflect, in accordance with generally accepted accounting principles, all charges claimed under the provisions of this Contract. Any such records which relate to litigation or the settlement of claims arising out of the performance of this Contract, or any Fees as to which exception has been taken by the auditors, shall be retained by Contractor until such litigation, claims, or exceptions have been finally resolved. Such audit shall not require Contractor to disclose cost, profit and overhead data, including direct and indirect rates, markups, profit margins or confidential employee records or other trade secret information.

(5) **Inclusion in Subcontracts**. The provisions of this *Section 51* (Audit Obligations), except for *Section 51(b)3*, shall be applicable to and included in each subcontract under this Contract.

52. VIRUS AND MALICIOUS CODE

a. The Contractor shall be liable for any damage to any Data and/or Software owned or licensed by the Commonwealth if the Contractor or any of its employees, Subcontractors or consultants introduces a virus or malicious, mischievous or destructive programming into the Commonwealth's Software or computer networks and has failed to comply with the Commonwealth software security standards. The Commonwealth must demonstrate that the Contractor or any of its employees, Subcontractors or consultants introduced the virus or malicious, mischievous or destructive programming. The Contractor's liability shall cease if the Commonwealth has not fully complied with its own software security standards.

b. The Contractor shall be liable for any damages incurred by the Commonwealth including, but not limited to, the expenditure of Commonwealth funds to eliminate or remove a computer virus or malicious, mischievous or destructive

programming that result from the Contractor's failure to take proactive measures to keep virus or malicious, mischievous or destructive programming from originating from the Contractor or any of its employees, Subcontractors or consultants through appropriate firewalls and maintenance of anti-virus software and software security updates (such as operating systems security patches, etc.).

c. In the event of destruction or modification of Software, the Contractor shall eliminate the virus, malicious, mischievous or destructive programming, restore the Commonwealth's Software, and be liable to the Commonwealth for any resulting damages.

d. The Contractor shall be responsible for reviewing Commonwealth software security standards and complying with those standards.

e. The Commonwealth may, at any time, audit, by a means deemed appropriate by the Commonwealth, any computing devices being used by representatives of the Contractor to provide Services to the Commonwealth for the sole purpose of determining whether those devices have anti-virus software with current virus signature files and the current minimum operating system patches or workarounds have been installed. Devices found to be out of compliance will immediately be disconnected and will not be permitted to connect or reconnect to the Commonwealth network until the proper installations have been made.

f. The Contractor may use the anti-virus software used by the Commonwealth to protect Contractor's computing devices used in the course of providing services to the Commonwealth. It is understood that the Contractor may not install the software on any computing device not being used to provide services to the Commonwealth, and that all copies of the software will be removed from all devices upon termination of this Contract.

g. The Commonwealth will not be responsible for any damages to the Contractor's computers, data, software, etc. caused as a result of the installation of the Commonwealth's anti-virus software or monitoring software on the Contractor's computers.

53. THE AMERICANS WITH DISABILITIES ACT

During the term of this Contract, the Contractor agrees as follows:

(1) Pursuant to federal regulations promulgated under the authority of *The Americans With Disabilities Act*, 28 C.F.R.§ 35.101, *et seq.*, the Contractor understands and agrees that no individual with a disability shall, on the basis of the disability, be excluded from participation in this Contract or from activities provided for under this Contract. As a condition of accepting and executing this

Contract, the Contractor agrees to comply with the *General Prohibitions Against Discrimination*, 28 C.F.R. § 35.130, and all other regulations promulgated under Title II of *The Americans With Disabilities Act* which are applicable to the benefits, services, programs, and activities provided by the Commonwealth of Pennsylvania through contracts with outside contractors.

(2) The Contractor shall be responsible for and agrees to indemnify and hold harmless the Commonwealth of Pennsylvania from losses, damages, expenses claims, demands, suits, and actions brought by any party against the Commonwealth of Pennsylvania as a result of the Contractor's failure to comply with the provisions of subsection (a) above.

54. NONDISCRIMINATION CLAUSE/SEXUAL HARASSMENT CLAUSE

The Contractor agrees:

(1) In the hiring of any employee(s) for the manufacture of supplies, performance of work, or any other activity required under the Contract or any Subcontract, the Contractor, each Subcontractor, or any person acting on behalf of the Contractor or Subcontractor shall not, by reason of gender, race, creed, or color, discriminate against any citizen of this Commonwealth who is qualified and available to perform the work to which the employment relates.

(2) Neither the Contractor nor any Subcontractor nor any person on their behalf shall in any manner discriminate against or intimidate any employee involved in the manufacture of supplies, the performance of work, or any other activity required under the contract on account of gender, race, creed, or color.

(3) The Contractor and each Subcontractor shall establish and maintain a written sexual harassment policy and shall inform their employees of the policy. The policy must contain a notice that sexual harassment will not be tolerated and employees who practice it will be disciplined.

(4) The Contractor and each Subcontractor shall not discriminate by reason of gender, race, creed, or color against any Subcontractor or supplier who is qualified to perform the work to which the contracts relates.

(5) The Contractor and each Subcontractor shall, within the time periods requested by the Commonwealth, furnish all necessary employment documents and records and permit access to their

books, records, and accounts by the contracting Agency and the Bureau of Small Business Opportunities (BSBO), for purpose of ascertaining compliance with provisions of this Nondiscrimination/Sexual Harassment Clause. Within fifteen (15) days after award of any contract, the Contractor shall be required to complete, sign and submit Form STD-21, the "Initial Contract Compliance Data" form. If the contract is a construction contract, then the Contractor shall be required to complete, sign and submit Form STD-28, the "Monthly Contract Compliance Report for Construction Contractors", each month no later than the 15th of the month following the reporting period beginning with the initial job conference and continuing through the completion of the project. Those contractors who have fewer than five employees or whose employees are all from the same family or who have completed the Form STD-21 within the past 12 months may, within the 15 days, request an exemption from the Form STD-21 submission requirement from the contracting Agency.

(6) The Contractor shall include the provisions of this Nondiscrimination/Sexual Harassment Clause in every subcontract so that those provisions applicable to Subcontractors will be binding upon each Subcontractor.

(7) The Commonwealth may cancel or terminate the Contract and all money due or to become due under the Contract may be forfeited for a violation of the terms and conditions of this Nondiscrimination/Sexual Harassment Clause. In addition, the Agency may proceed with debarment or suspension and may place the Contractor in the Contractor Responsibility File.

55. CONTRACTOR INTEGRITY PROVISIONS

It is essential that those who seek to contract with the Commonwealth of Pennsylvania ("Commonwealth") observe high standards of honesty and integrity. They must conduct themselves in a manner that fosters public confidence in the integrity of the Commonwealth procurement process.

In furtherance of this policy, Contractor agrees to the following:

a. Contractor shall maintain the highest standards of honesty and integrity during the performance of this contract and shall take no action in violation of state or federal laws or regulations or any other applicable laws or regulations, or other requirements applicable to Contractor or that govern contracting with the Commonwealth.

b. Contractor shall establish and implement a written business integrity policy, which includes, at a minimum, the requirements of these provisions as they relate to Contractor employee activity with the Commonwealth and Commonwealth employees, and which is distributed and made known to all Contractor employees.

c. Contractor, its affiliates, agents and employees shall not influence, or attempt to influence, any Commonwealth employee to breach the standards of ethical conduct for Commonwealth employees set forth in *the Public Official and Employee Ethics Act, 65 Pa. C.S. §§1101 et seq.;* the *State Adverse Interest Act, 71 P. S. §776.1 et seq.;* and the *Governor's Code of Conduct, Executive Order 1980-18, 4 Pa. Code §7.151 et seq.*, or to breach any other state or federal law or regulation.

d. Contractor, its affiliates, agents and employees shall not offer, give, or agree or promise to give any gratuity to a Commonwealth official or employee or to any other person, at the direction or request of any Commonwealth official or employee.

e. Contractor, its affiliates, agents and employees shall not offer, give or agree or promise to give any gratuity to a Commonwealth official or employee or to any other person, the acceptance of which would violate the *Governor's Code of Conduct, Executive Order 1980-18, 4 Pa. Code §7.151 et seq.* or any statute, regulation, statement of policy, management directive or any other published standard of the Commonwealth.

f. Contractor, its affiliates, agents and employees shall not, directly or indirectly, offer, confer, or agree to confer any pecuniary benefit on anyone as consideration for the decision, opinion, recommendation, vote, other exercise of discretion, or violation of a known legal duty by any Commonwealth official or employee.

g. Contractor, its affiliates, agents, employees, or anyone in privity with him or her shall not accept or agree to accept from any person, any gratuity in connection with the performance of work under the contract, except as provided in the contract.

h. Contractor shall not have a financial interest in any other contractor, subcontractor, or supplier providing services, labor, or material on this project, unless the financial interest is disclosed to the Commonwealth in writing and the Commonwealth consents to Contractor's financial interest prior to the Commonwealth execution of the contract. Contractor shall disclose the financial interest to the Commonwealth at the time of bid or proposal submission, or if no bids or proposals are solicited, no later than Contractor's submission of the contract signed by Contractor.

i. Contractor, its affiliates, agents and employees shall not disclose to others any information, documents, reports, data or records provided to, or prepared by, Contractor under this contract without the prior written approval of the Commonwealth, except as required *by the Pennsylvania Right to Know Law, 65 P. S. §§ 67.101-3104,* or other applicable law or as otherwise provided in this contract. Any information, documents, reports, date, or records secured by Contractor from the Commonwealth or a third party in connection with the performance of this contract shall be kept confidential unless disclosure of such information is:

(1) Approved in writing by the Commonwealth prior to its disclosure; or

(2) Direction by a court or other tribunal of competent jurisdiction unless the contract required prior Commonwealth approval; or

(3) Required for compliance with federal or state securities laws or the requirements of national securities exchanges; or

(4) Necessary for purposes of Contractor's internal assessment and review; or

(5) Deemed necessary by Contractor in any action to enforce the provisions of this contract or to defend or prosecute claims by or against parties other than the Commonwealth; or

(6) Permitted by the valid authorization of a third party to whom the information, documents, reports, data, or records pertain; or

(7) Otherwise required by law.

j. Contractor certifies, to the best of its knowledge, that neither it nor any of its executive officers, directors, affiliates, or owners of 15% or more beneficial interest, has been officially notified of, charged with, or convicted of any of the following within the last two (2) years and agrees to immediately notify the Commonwealth agency contracting officer in writing if and when it is or it becomes aware that any officer or director has been officially notified of, charged with, convicted of, or officially notified of a government determination of any of the following (except as expressly provided above, as a publicly traded company, Contractor cannot verify if an owner would be subject to any of the following):

(1) Commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements or receiving stolen property;

(2) Commission of fraud or a criminal offense or other improper conduct associated with:

(i) obtaining;

(ii) attempting to obtain; or

(iii) performing a public contract or subcontract.

(3) Contractor's acceptance of the benefits known to have been derived from the conduct shall be deemed evidence of such knowledge, approval or acquiescence.

(4) Violation of federal or state antitrust statutes.

(5) Violation of any federal or state law regulating campaign contributions.

(6) Violation of any federal or state environmental law.

(7) Violation of any federal or state law regulating hours of labor, minimum wage standards or prevailing wage standards; discrimination in wages; or child labor violations.

(8) Violation of the *Act of June 2, 1915 (P. L. 736, No. 338)*, known as the *Workers' Compensation Act*, 77 P. S. 1 *et seq*.

(9) Debarment by any agency or department of the federal government or by any other state.

(10) Any other crime involving moral turpitude or business honesty or integrity.

(11) Contractor acknowledges that the Commonwealth may, in its sole discretion, terminate the contract for cause when the Commonwealth learns that Contractor has been officially notified of its debarment or convicted of a violation described above which derived from Contractor's activity to acquire or in furtherance of this Contract.

k. If this contract was awarded to Contractor on a non-bid basis, Contractor must, (as required by *Section 1641* of the *Pennsylvania Election Code*) file a report of political contributions with the Secretary of the Commonwealth on or before February 15 of the next calendar year. The report must include an itemized list of all political contributions known to Contractor by virtue of the knowledge

possessed by every officer, director, associate, partner, limited partner, or individual owner that has been made by:

(1) Any officer, director, associate, partner, limited partner, individual owner or members of the immediate family when the contributions exceed an aggregate of one thousand dollars ($1,000) by any individual during the preceding year; or

(2) Any employee or members of his immediate family whose political contribution exceeded one thousand dollars ($1,000) during the preceding year.

l. To obtain a copy of the reporting form, Contractor shall contact the Bureau of Commissions, Elections and Legislation, Division of Campaign Finance and Lobbying Disclosure, Room 210 North Office Building, Harrisburg, PA 17120.

m. Contractor shall comply with requirements of the *Lobbying Disclosure Act, 65 Pa. C. S. §13AO1 et seq.,* and the regulations promulgated pursuant to that law. Contractor employee activities prior to or outside of formal Commonwealth procurement communication protocol are considered lobbying and subjects the Contractor employees to the registration and reporting requirements of the law. Actions by outside lobbyists on Contractor's behalf, no matter the procurement stage, are not exempt and must be reported.

n. When Contractor has reason to believe that any breaks of ethical standards as set forth in the law, The Governor's Code of Conduct, or in these provisions has occurred or may occur, including but not limited to contact by a Commonwealth officer or employee which, if acted upon, would violate such ethical standards, Contractor shall immediately notify the Commonwealth contracting officer or Commonwealth Inspector General in writing.

o. Contractor, by submission of its bid or proposal and/or execution of this contract and by the submission of any bills, invoices or requests for payment pursuant to the contract, certifies and represents that it has not violated any of these contractor integrity provisions in connection with the submission of the bid or proposal, during any contract negotiations or during the term of the contract.

p. Contractor shall cooperate with the Office of Inspector General in its investigation of any alleged Commonwealth employee breach of ethical standards and alleged Contractor non-compliance with these provisions. Contractor agrees to make identified Contractor employees available for interviews at reasonable times and places. Contractor, upon inquiry or request of the Office of Inspector General, shall provide, or if appropriate, make promptly available for inspection or copying, any information of any type or form deemed relevant by the Inspector General to Contractor's integrity and

compliance with these provisions. Such information may include, but shall not be limited to, Contractor's business or financial records, documents or files of any type or form that refers to or concerns this contract.

q. For violation of any of these Contractor Integrity Provisions, the Commonwealth may terminate this and any other contract with Contractor, claim liquidated damages in an amount equal to the value of anything received in breach of these provisions, claim damages for all additional costs and expenses incurred in obtaining another contractor to complete performance under this contract, and debar and suspend Contractor from doing business with the Commonwealth. These rights and remedies are cumulative, and the use or non-use of any one shall not preclude the use of all or any other. These rights and remedies are in addition to those the Commonwealth may have under law, statue, regulations, or otherwise.

r. For purposes of these Contractor Integrity Provisions, the following terms shall have the means found in this Paragraph 17.

(1) "Confidential information" means information that a) is not already in the public domain; b) is not available to the public upon request; c) is not or does not become generally known to Contractor from a third party without an obligation to maintain its confidentiality; d) has not become generally known to the public through an act or omission of Contractor; or e) has not been independently developed by Contractor without the use of confidential information of the Commonwealth.

(2) "Consent" means written permission signed by a duly authorized officer or employee of the Commonwealth, provided that where the material facts have been disclosed, in writing, by pre-qualification, bid, proposal, or contractual terms, the Commonwealth shall be deemed to have consented by virtue of execution of this contract.

(3) "Contractor" means the Individual or entity that has entered into this contract with the Commonwealth, including those directors, officers, partners, managers, and owners having more than a five percent interest in Contractor.

(4) "Financial interest" means:

(i) Ownership of more than a five percent interest in any business; or

(ii) Holding a position as an officer, director, trustee, partner, employee, or holding any position of management**.**

(5) "Gratuity" means tendering, giving or providing anything of more than nominal monetary value including, but not limited to, cash travel, entertainment, gifts, meals, lodging, loans, subscriptions, advances, deposits of money, services, employment, or contracts of any kind. The exceptions set forth in the *Governor's Code of Conduct, Executive Order 1980-18*, the *4 Pa. Code §7.153(b)*, shall apply.

(6) "Immediate family" means a spouse and any unemancipated child.

(7) "Non-bid basis" means a contract awarded or executed by the Commonwealth with Contractor without seeking bids or proposals from any other potential bidder or offeror.

(8) "Political contributions" means any payment, gift, subscription, assessment, contract, payment of services, dues, loan, forbearance, advance or deposit of money or any valuable thing, to a candidate for public office or to a political committee, including but not limited to a political action committee, made for the purposes of influencing any election in the Commonwealth of Pennsylvania or for paying its debts incurred by or for a candidate or committee before or after any election.

56. RIGHT-TO-KNOW LAW

a. The Pennsylvania Right-to-Know Law, 65 P.S. §§ 67.101-3104, ("RTKL") applies to this Contract.

b. If the Commonwealth requires the Contractor's assistance in any matter arising out of the RTKL related to this Contract, it shall notify the Contractor using the legal contact information provided in this Contract. The Contractor, at any time, may designate a different contact for such purpose upon reasonable prior written notice to the Commonwealth.

c. Upon written notification from the Commonwealth that it requires the Contractor's assistance in responding to a request under the RTKL for information related to this Contract that may be in the Contractor's possession, constituting, or alleged to constitute, a public record in accordance with the RTKL ("Requested Information"), the Contractor shall:

(1) Provide the Commonwealth, within ten (10) calendar days after receipt of written notification, access to, and copies of, any document or information in the Contractor's possession arising out of this Contract that the Commonwealth reasonably believes is Requested Information and may be a public record under the RTKL; and

(2) Provide such other assistance as the Commonwealth may reasonably request, in order to comply with the RTKL with respect to this Contract.

d. If the Contractor considers the Requested Information to include a request for a Trade Secret or Confidential Proprietary Information, as those terms are defined by the RTKL, or other information that the Contractor considers exempt from production under the RTKL, the Contractor must notify the Commonwealth and provide, within seven (7) calendar days of receiving the written notification, a written statement signed by a representative of the Contractor explaining why the requested material is exempt from public disclosure under the RTKL.

e. The Commonwealth will rely upon the written statement from the Contractor in denying a RTKL request for the Requested Information unless the Commonwealth determines that the Requested Information is clearly not protected from disclosure under the RTKL. Should the Commonwealth determine that the Requested Information is clearly not exempt from disclosure, the Contractor shall provide the Requested Information within five (5) business days of receipt of written notification of the Commonwealth's determination.

f. If the Contractor fails to provide the Requested Information within the time period required by these provisions, the Contractor shall indemnify and hold the Commonwealth harmless for any damages, penalties, costs, detriment or harm that the Commonwealth may incur as a result of the Contractor's failure, including any statutory damages assessed against the Commonwealth.

g. The Commonwealth will reimburse the Contractor for any costs associated with complying with these provisions only to the extent allowed under the fee schedule established by the Office of Open Records or as otherwise provided by the RTKL if the fee schedule is inapplicable.

h. The Contractor's duties relating to the RTKL are continuing duties that survive the expiration of this Contract and shall continue as long as the Contractor has Requested Information in its possession.

57. ENVIRONMENTAL PROTECTION

In carrying out this Contract, the Contractor shall minimize pollution and shall strictly comply with all applicable environmental laws and regulations, including the *Clean Streams Law,* Act of June 22, 1937, as amended; the *Pennsylvania Solid Waste Management Act,* Act of July 7, 1980 (P.L. 380, No. 97), as amended; and the *Dam Safety and Encroachment Act,* Act of November 26, 1978 (P.L. 1375, No. 325), as amended.

58. ASSIGNABILITY

a. This Contract may not be assigned by Contractor, either in whole or in part without the prior written consent of the Commonwealth, which consent shall not be unreasonably withheld, conditioned, or delayed. Transfer of the majority of the stock or the majority of the assets of a corporation, or other change of ownership will be deemed an assignment. In the event that Contractor requests the right to assign this Contract, including an assignment to an affiliate or subsidiary, Contractor will provide the Commonwealth with copies of the following documents (to the extent they exist): most recent audited financial statements and such other documents as Commonwealth reasonably deems necessary. Within thirty (30) days of such notice, the Commonwealth shall provide its written decision regarding the requested assignment.

b. Subject to the terms and conditions of this *Section 58* (Assignability), the Contract is binding upon the parties and their respective successors and assigns.

c. Any assignment consented to by the Commonwealth shall be evidenced by a written assignment agreement executed by the Contractor and its assignee in which the assignee agrees to be legally bound by all of the terms and conditions of the Contract and to assume the duties, obligations, and responsibilities being assigned. In addition, the assignee must execute a contract with the Commonwealth in the same form as this Contract.

d. Notwithstanding the foregoing, the Contractor may, without the consent of the Commonwealth, assign its rights to payment to be received under the Contract, provided that the Contractor provides written notice of such assignment to the Commonwealth together with a written acknowledgement from the assignee that any such payments are subject to all of the terms and conditions of the Contract.

e. A change of name by the Contractor, following which the Contractor's federal identification number remains unchanged, is not considered to be an assignment. The Contractor shall give the Commonwealth written notice of any such change of name.

59. INDEPENDENT CAPACITY OF CONTRACTOR

a. The parties to this Contract agree that the Services performed by the Contractor under the terms of this Contract are performed as an independent contractor and nothing contained in this Contract shall be construed to make either Contractor or Commonwealth partners, joint venturers, principals, agents or employees of the other, except only to the extent that Contractor is expressly appointed under the Contract to act as the agent of Commonwealth and, in

those cases, only to the limited extent of such express appointment. No officer, director, employee, agent, affiliate or contractor retained by Contractor to perform work on Commonwealth's behalf hereunder shall be deemed to be an employee, agent or contractor of Commonwealth. Neither party shall have any right, power or authority, express or implied, to bind the other. As between Contractor and Commonwealth, Contractor is solely responsible for payment of all income, disability, withholding and other employment taxes, and all medical benefit premiums, vacation pay, sick pay and other fringe benefits resulting from Contractor's retention of any such officers, directors, employees, agents or contractors.

b. Except as otherwise provided by the terms of this Contract, the Commonwealth shall have no control over the manner in which the contractual Services are performed by the Contractor, or any Subcontractor. Any job specifications or standards of work attached to or incorporated into this Contract or any subcontracting restrictions contained in this Contract shall not be construed as the Commonwealth's direction or control over the manner of the performance of Services provided by the Contractor.

60. THIRD PARTY BENEFICIARIES

Each party intends that this Contract shall not benefit, or create any right or cause of action in or on behalf of, any person or entity other than Commonwealth and Contractor.

61. CERTIFICATION REGARDING SUSPENSION

Contractor certifies that it is not currently under suspension or debarment by Commonwealth, any other state, or the federal government.

62. SUSPENSION OF SUBCONTRACTORS

If Contractor enters into any subcontracts or employs under this Contract any Subcontractor's individuals who are currently suspended or debarred by Commonwealth or the federal government or who become suspended or debarred by Commonwealth or the federal government during the term of this Contract or any extensions or renewals thereof, Commonwealth shall have the right to require Contractor to terminate such subcontracts or employment.

63. ASSIGNMENT OF RIGHTS UNDER THE ANTITRUST LAWS

It is recognized that in actual economic practice, overcharges by Contractor's suppliers resulting from violations of state and federal antitrust laws are in fact borne by the Commonwealth. As part of the consideration for the award of this Contract, and intending to be legally bound, the Contractor assigns to the Commonwealth all rights, title, and interest in and to any claims Contractor now has or may hereafter acquire under state and federal antitrust laws relating to the goods and services which are provided by the Contractor under this Contract.

64. SIGNIFICANT EVENTS

Commonwealth requires the right to adjust the scope or volume of Services to be provided in response to an event, or series of events taken together, that have or will have a significant and sustained impact on Commonwealth's demand for the Services, and requires Contractor to equitably adjust the price for the Services to reflect any such changes to the scope or volume of the Services.

65. FORCE MAJEURE

No failure or delay by Contractor in the performance of its obligations pursuant to this Contract shall be deemed a default of this Contract or a ground for termination hereunder (except as provided in this Section 65 (Force Majeure) to the extent such failure or delay is due to a Force Majeure Event and such Force Majeure Event could not have been prevented by Contractor's reasonable precautions or efforts to mitigate damage. The occurrence of a Force Majeure Event does not limit or otherwise affect Contractor's obligation to provide normal recovery procedures and any Disaster Recovery Services described in Section 15 (Disaster Recovery and Business Continuity) to the extent such obligations are not directly precluded by the occurrence of that Force Majeure Event. The occurrence of a Force Majeure Event in respect of another customer of Contractor does not constitute a Force Majeure Event under this Contract, except to the extent such customer and Commonwealth experience the same Force Majeure Event at a site shared by Commonwealth and such other customer. The party delayed by a Force Majeure Event shall immediately orally notify the other party (to be confirmed in a written notice within three (3) business days after the inception of such delay) of the occurrence of a Force Majeure Event and describe in reasonable detail the nature of the Force Majeure Event. From and after becoming aware of a Force Majeure Event, the party delayed thereby shall undertake all commercially reasonable measures (including the use of alternative sources for products and services and workaround plans) to mitigate the impact and duration of the Force Majeure Event, and such party shall consistently and diligently prosecute such measures until the Force Majeure Event is relieved. If Contractor does not fulfill its obligations under the immediately preceding sentence and, as a result thereof, such Force Majeure Event precludes Contractor from delivering the Services for more than forty five (45) days, Commonwealth may terminate this Contract for cause under Section 32(c), but without regard to any additional cure periods provided for therein. In any other case in which a Force Majeure Event precludes Contractor from delivering the Services for more than forty-five (45) days (without consideration of any such Services performed from a business recovery center under Section 15 (Disaster Recovery and Business Continuity)), Commonwealth may terminate this Contract for convenience under Section 32(a), but without regard to any notice period or additional cure periods provided for therein. In the event of a Force Majeure Event, Contractor shall not increase the Fees under this Contract or charge Commonwealth usage fees in addition to the Fees except for applicable Disaster Recovery declaration and usage fees in accordance with the provisions of Section 15 (Disaster Recovery and Business Continuity).

66. CONFLICT OF INTEREST

Contractor, by signing this Contract, covenants that it has no undisclosed public or private interest, direct or indirect, and shall not acquire directly or indirectly any such interest, and that Contractor has no association, direct or indirect, which interest or association does or may conflict in any manner with the performance of the Services or any other obligations of Contractor under this Contract. Any such conflicts shall be disclosed to Commonwealth, and Commonwealth shall determine whether such conflict is cause for termination of this Contract. Contractor further covenants that, in the performance of this Contract, no person having such interest shall be employed by or associated with Contractor.

67. OFFICIALS NOT TO BENEFIT

No official or employee of the Commonwealth and no member of its General Assembly who exercises any functions or responsibilities under this Contract shall participate in any decision relating to this Contract which affects their personal interest or the interest of any corporation, partnership, or association in which they are, directly or indirectly, interested; nor shall any such official or employee of the Commonwealth or member of its General Assembly have any interest, direct or indirect, in this Contract or the proceeds thereof.

68. CONSENTS, APPROVALS, NOTICES AND REQUESTS

Unless otherwise specified in this Contract, all consents, approvals, notices and requests, acceptances or similar actions to be given by either party under this Contract shall not be unreasonably withheld, delayed or conditioned and each party shall make only reasonable requests under this Contract.

69. REQUIRED CONSENTS

The Commonwealth, with reasonable assistance at no additional cost by Contractor and its Subcontractors shall obtain all consents, approvals, authorizations, notices, requests and acknowledgements necessary to allow Contractor to use the Commonwealth Software, the Commonwealth Equipment and the services under Commonwealth's Third Party service contracts, all to the extent necessary to enable Contractor to provide the Services to Commonwealth. Commonwealth shall be responsible for all costs and expenses imposed by Third Parties in connection with obtaining any such consents. Contractor shall obtain all consents, approvals, authorizations, notices, requests and acknowledgements necessary to allow (1) Contractor to use the Contractor Software, the Developed Software and the Contractor Equipment to provide the Services to Commonwealth, and (2) Commonwealth to use the Contractor Software in accordance with the terms of this Contract upon the expiration or termination for any reason of Contractor's obligation to provide the Services or of this Contract. Contractor shall be responsible for all costs and expenses imposed by a Third Party in connection with any such consents described in the foregoing clause (1). Commonwealth's costs and expenses under the foregoing clause (2) shall be governed by the

terms of *Section 40(b).02*. Each party shall cooperate with and assist the other party in obtaining the consents contemplated in this *Section 69* (Required Consents).

70. REQUIREMENTS FOR INFORMATION IN LEGAL PROCEEDINGS

a. If the Commonwealth notifies Contractor, or Contractor is otherwise aware, that particular Commonwealth Confidential Information may be within attorney-client or work-product privileges of the Commonwealth, then regardless of any applicable exclusions, Contractor (i) shall not disclose such Confidential Information or take any other action that would result in waiver of such privileges and (ii) shall instruct all Contractor Personnel who may have access to such communications to maintain privileged material as strictly confidential and otherwise protect the Commonwealth privileges.

b. To the extent requested by the Commonwealth, Contractor shall comply with the Commonwealth's litigation response plan, including policies and procedures to prepare for and respond to discovery requests, subpoenas, investigatory demands, and other requirements for information related to legal and regulatory proceedings, as such plan may be revised from time to time, including preparing for and complying with requirements for preservation and production of data in connection with legal and regulatory proceedings and government investigations. Upon receipt of any request, demand, notice, subpoena, order or other legal information request relating to legal proceedings or investigations by third parties relating to any materials, the Confidential Information or related systems in Contractor possession, Contractor shall immediately notify the Commonwealth and provide the Commonwealth with a copy of all documentation of such legal information request, to the extent Contractor legally may do so and shall cooperate with the Commonwealth in responding to such request, demand, notice, subpoena, order or other legal information request.

c. Contractor 's cost of complying with this section shall be at no additional charge to the Commonwealth to the extent that compliance can be accomplished with Contractor's then existing resources. If additional resources are required for compliance, they will be agreed upon by the parties in accordance with the Change Control Procedures, provided, however, that Contractor will not be entitled for payment under this *Section 70* (Requirements for Information in Legal Proceedings) with regard to items for which the Contractor is required to indemnify the Commonwealth.

71. EXAMINATION OF RECORDS

The Commonwealth may, at reasonable times and places, audit the books and records of Contractor or its Subcontractors to the extent that the books and records relate to the performance of the Contract. Contractor shall maintain books and records related to the Contract for a period of three years from the date of final payment under the Contract.

Contractor shall include a requirement in agreements with Subcontractors that requires the Subcontractor to maintain its records for the same length of time.

72. SURVIVAL

Sections 4, 33, 35, 36, 37, 38, 38, 40, 41, 47, 48, 49, 52, 53, 72 shall survive the expiration or termination of the Contract.

73. SEVERABILITY

If any provision of this Contract is held by a court of competent jurisdiction to be contrary to law, then the remaining provisions of this Contract or the application of such provision to persons or circumstances other than those as to which it is invalid or unenforceable shall not be affected thereby, and each such provision of this Contract shall be valid and enforceable to the extent permitted by law.

74. WAIVER

No delay or omission by either party to exercise any right or power it has under this Contract shall impair or be construed as a waiver of such right or power. A waiver by any party of any breach or covenant shall not be construed to be a waiver of any succeeding breach or any other covenant. All waivers must be in writing and signed by the party waiving its rights.

75. PERIOD OF PERFORMANCE

The Contractor, for the life of this Contract, shall complete all Services as specified under the terms of this Contract. In no event shall the Commonwealth be responsible or liable to pay for any Services provided by the Contractor prior to the Effective Date, and the Contractor hereby waives any claim or cause of action for any such Services.

76. SPECIAL REQUIREMENTS

The Commonwealth reserves the right to purchase Services covered under this Contract through other procurement methods whenever the Commonwealth deems it to be in its best interest.

77. GOVERNING LAW

This Contract shall be interpreted in accordance with and governed by the laws of the Commonwealth of Pennsylvania, without giving effect to its conflicts of law provisions. Except as set forth in *Section 34* (Contract Controversies), Commonwealth and Contractor agree that the courts of the Commonwealth of Pennsylvania and the federal courts of the Middle District of Pennsylvania shall have exclusive jurisdiction over disputes under this Contract and the resolution thereof. Any legal action relating to this

Contract must be brought in Dauphin County, Pennsylvania, and the parties agree that jurisdiction and venue in such courts is appropriate.

78. COMPLIANCE WITH LAWS

a. The Contractor shall comply with all federal, state, and local laws in all material respects applicable to the operation of its business, including, but not limited to, all statutes, regulations and rules that are in effect as of the Effective Date of the Contract and shall procure at its expense all licenses and all permits necessary for the fulfillment of its obligations hereunder.

b. If any existing law, regulation or policy is changed or if any new law, regulation or policy is enacted that affects the Services provided under this Contract, the parties to the Contract shall modify this Contract, via *Section 27* (Change Control), to the extent reasonably necessary to:

(1) Ensure that such Services will be in full compliance with such laws, regulations and/or policies; and

(2) Modify the rates applicable to such Services; and

(3) Address any schedule impacts.

79. SMALL DIVERSE BUSINESS COMMITMENT

Contractor shall meet and maintain the commitments to small diverse businesses in the Small Diverse Business ("SDB") portion of its Proposal. Any proposed change to a SDB commitment must be submitted to the DGS Bureau of Small Business Opportunities ("BSBO"), which will make a recommendation as to a course of action to the Commonwealth Contracting Officer. Contractor shall complete the Prime Contractor's Quarterly Utilization Report and submit it to the Commonwealth Contracting Officer and BSBO within ten (10) workdays at the end of each calendar quarter that the Contract is in effect.

80. ACKNOWLEDGEMENT

Commonwealth and Contractor each acknowledge that the limitations and exclusions contained in this Contract have been the subject of active and complete negotiation between the parties and represent the parties' Contract based upon the level of risk to Commonwealth and Contractor associated with their respective obligations under this Contract and the payments to be made to Contractor and credits to be issued to, and Services to be provided to, Commonwealth pursuant to this Contract. The parties agree that the terms and conditions of this Contract shall not be construed in favor of or against any party by reason of the extent to which any party or its professional advisors participated in the preparation of this Contract.

81. COVENANT OF FURTHER ASSURANCES

Commonwealth and Contractor covenant and agree that, subsequent to the execution and delivery of this Contract and without any additional consideration, each of Commonwealth and Contractor will execute and deliver any further legal instruments and perform any commercially reasonable acts which are or may become necessary to effectuate the purposes of this Contract.

82. COVENANT OF GOOD FAITH

Each party agrees that, in its respective dealings with the other party under or in connection with this Contract, it shall act in good faith.

83. AMENDMENTS

No amendment to, or change, waiver, or discharge of, any provision of this Contract shall be valid unless in writing and signed by an authorized representative of the party against which such amendment, change, waiver or discharge is sought to be enforced.

84. ENTIRE CONTRACT

This Contract is the entire Contract between the parties with respect to its subject matter, and there are no other representations, understandings or Contracts between the parties relative to such subject matter

IN WITNESS WHEREOF, the parties hereto have signed this Contract on the dates indicated below.

Witness:

[redacted]

12-5-2013
Date

Janet Britschea Haugen
Printed Name

SVP & Chief Financial Officer
Title

UNISYS CORPORATION

[redacted]

12-5-2013
Date

J. Edward Coleman
Printed Name

Chairman & Chief Executive Officer
Title

Federal I.D. Number – [redacted]
SAP Vendor Number – 163299

COMMONWEALTH OF PENNSYLVANIA
GOVERNOR'S OFFICE OF ADMINISTRATION

[See Section 1]
Secretary

APPROVED:

[See Section 1]
Comptroller

APPROVED AS TO FORM AND LEGALITY:

[See Section 1]
Office of Chief Counsel

[See Section 1]
Office of General Counsel

[See Section 1]
Office of Attorney General

CERTIFIED COPY OF RESOLUTIONS
of the
BOARD OF DIRECTORS
of
UNISYS CORPORATION

I, Susan B. Asch, Assistant Secretary of Unisys Corporation, a Delaware corporation, do hereby certify that the following is a true and correct copy of resolutions duly adopted at a regular meeting of the Board of Directors of said Corporation held on September 27, 1990, which on the date hereof remain in full force and effect:

Bids, Proposals, and Contracts:

RESOLVED, that the officers of the Corporation at the level of elected Vice President or above be, and each of them hereby is, authorized and empowered, in the name and on behalf of the Corporation, to make, execute, enter into and deliver bids, proposals and contracts for the selling, leasing, licensing, supplying, performing, and delivering of computer products (including, without limitation, hardware and system software incorporated therein, application software, parts and supplies), systems and other services, other products and goods of the Corporation (whether or not manufactured or developed by the Corporation or others) to any customer, governmental or otherwise; and further

RESOLVED, that the officers of the Corporation above the level of elected Vice President be, and each of them hereby is, authorized and empowered, in the name and on behalf of the Corporation, to delegate the authority granted by the foregoing resolution to additional officers and/or employees of the Corporation, or to revoke any such delegation previously granted, which delegation, or revocation thereof, shall become effective when it is filed in writing with the Secretary of the Corporation; and further

RESOLVED, that the Secretary or any Assistant Secretary of the Corporation be, and each of them hereby is, authorized and empowered to certify, to any entity or person, the authority granted to any officer or employee of the Corporation pursuant to the foregoing resolutions, with such certification constituting conclusive evidence, binding upon the Corporation, of the authority of such officer or employee to make, execute, enter into or deliver the bids, proposals or contracts referred to in the foregoing resolutions.

I further certify that, on the date hereof, J. Edward Coleman is the duly elected Chairman and Chief Executive Officer of Unisys Corporation.

IN WITNESS WHEREOF, I have hereunto set my hand and affixed the seal of said Corporation this 25th day of November 2013.

[redacted]

Assistant Secretary

[certcopy.res\bidspro.con]

APPENDIX A - BUSINESS ASSOCIATE APPENDIX LANGUAGE

APPENDIX A - BUSINESS ASSOCIATE APPENDIX LANGUAGE

COMMONWEALTH OF PENNSYLVANIA
BUSINESS ASSOCIATE CONTRACT

WHEREAS, the ***[name of program and/or Department]*** (Covered Entity) and Contractor (Business Associate) intend to protect the privacy and security of certain Protected Health Information (PHI) to which Business Associate may have access in order to provide goods or services to or on behalf of Covered Entity, in accordance with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5 (Feb. 17, 2009), the HIPAA Privacy Rule (Privacy Rule), 45 C.F.R. Parts 160 and 164, and the HIPAA Security Rule (Security Rule), 45 C.F.R. Parts 160, 162 and 164, and all other applicable laws; and

WHEREAS, Business Associate may receive PHI from Covered Entity, or may create or obtain PHI from other parties for use on behalf of Covered Entity, which PHI can be used or disclosed only in accordance with this Agreement and the standards established by applicable laws; and

WHEREAS, Business Associate may receive PHI from Covered Entity, or may create or obtain PHI from other parties for use on behalf of Covered Entity that is in electronic form, which PHI must be handled in accordance with this Agreement and the standards established by HIPAA and the Security Rule and other applicable laws; and

NOW, THEREFORE, the parties to this Agreement set forth the following as the terms and conditions of their understanding.

1. Definitions.

a) "Breach" shall have the meaning assigned to such term at 42 USCS § 17921 and HIPAA regulations at 45 C.F.R. § 164.402.

b) "Business Associate" shall have the meaning given to such term under the Privacy and Security Rules, including but not limited to, 45 C.F.R. §160.103.

c) "Covered Entity" shall have the meaning given to such term under the Privacy and Security Rules, including, but not limited to, 45 C.F.R. §160.103.

d) "HIPAA" shall mean the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191.

e) "Privacy Rule" shall mean the standards for privacy of individually identifiable health information in 45 C.F.R. Parts 160 and 164.

f) "Protected Health Information" or "PHI" shall have the meaning given to such term under HIPAA and the HIPAA Regulations in 45 C.F.R. Parts 160, 162 and 164, including, but not limited to 45 C.F.R. §160.103.

g) "Security Rule" shall mean the security standards in 45 C.F.R. Parts 160, 162 and 164.

h) Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5 (Feb. 17, 2009), the HIPAA Privacy Rule (Privacy Rule),

45 C.F.R. Parts 160 and 164, and the HIPAA Security Rule (Security Rule), 45 C.F.R. Parts 160, 162 and 164.

2. Stated Purposes For Which Business Associate May Use Or Disclose PHI. The Parties hereby agree that Business Associate shall be permitted to use and/or disclose PHI provided by or obtained on behalf of Covered Entity for purposes stated in Attachment 1, except as otherwise stated in this Agreement or required by law.

NO OTHER USES OR DISCLOSURES OF PHI ARE PERMITTED.

3. BUSINESS ASSOCIATE OBLIGATIONS:

a) Security and Privacy Provisions Applicable to Business Associate. Business Associate shall abide by the security and privacy provisions applicable to Covered Entities which are made applicable to the Business Associate by 42 USCS § 17931 and 17934.

b) Limits On Use And Further Disclosure Established By Agreement And Law. Business Associate hereby agrees that the PHI provided by, or created or obtained on behalf of Covered Entity shall not be further used or disclosed other than as permitted or required by this Agreement or as Required by Law.

c) Appropriate Safeguards. Business Associate shall establish and maintain appropriate safeguards to prevent any use or disclosure of PHI other than as provided for by this Agreement. Appropriate safeguards shall include implementing administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI that is created, received, maintained, or transmitted on behalf of the Covered Entity.

d) Reports Of Improper Use Or Disclosure. Business Associate hereby agrees that it shall report to _____at _____**,** within five (5) business days of discovery of any use or disclosure of PHI not provided for or allowed by this Agreement.

e) Reports Of Security Incidents. In addition to following the breach notification requirements in section 13402 of the Health Information Technology for Economic and Clinical Health Act of 2009 ("HITECH Act") and related regulations, agency guidance and other applicable federal and state laws, Business Associate shall report to _____at _____**,** within five (5) business days of discovery of any security incident. If the Security Incident is caused by Business Associate or its agents, Business Associate shall cover costs associated with any such incident, including costs stemming from compliance with all federal and state breach notification requirements applicable to Business Associate and Covered Entity. Business Associate shall cover costs associated with any incident involving the acquisition, access, use or disclosure of Unsecured PHI in a manner not permitted under federal or state law and agency guidance if the incident is caused by Business Associate or its agents.

f) Subcontractors and Agents. Business Associate hereby agrees that any time PHI is provided or made available to any subcontractors or agents, Business Associate shall provide only the minimum necessary PHI for the purpose of the covered transaction and shall first enter into a subcontract or contract with the subcontractor or agent that contains the same terms, conditions and restrictions on the use and disclosure of PHI as contained in this Agreement.

g) Right Of Access To PHI. Business Associate hereby agrees to allow an individual who is the subject of PHI maintained in a designated record set, to have access to and copy that individual's PHI within fifteen (15) business days of receiving a written request from the Covered Entity or individual Business Associate shall provide PHI in the format requested, unless it cannot readily be produced in such format, in which case it shall be provided in standard hard copy or such other form and format as agreed to by Business Associate and the individual. Notwithstanding this

general rule, if the request is for information maintained electronically in one or more designated record sets and if the individual requests an electronic copy of such information, Business Associate must provide the individual with access to the PHI in the electronic form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by the Business Associate and the individual. If any individual requests from Business Associate or its agents or subcontractors access to PHI, Business Associate shall notify Covered Entity of same within five (5) business days. Business associate shall further conform with and meet all of the requirements of 45 C.F.R. §164.524, 42 USCS § 17936(e), and other applicable laws.

h) Amendment and Incorporation Of Amendments. Within fifteen (15) business days of receiving a request from Covered Entity for an amendment of PHI maintained in a designated record set, Business Associate shall make the PHI available and incorporate the amendment to enable Covered Entity to comply with 45 C.F.R. §164.526 and other applicable laws. If any individual requests an amendment from Business Associate or its agents or subcontractors, Business Associate shall notify Covered Entity within five (5) business days.

i) Provide Accounting Of Disclosures. Business Associate agrees to maintain a record of all disclosures of PHI by Business Associate in accordance with 45 C.F.R. §164.528, 42 USCS § 17935(c), and other applicable laws. Such records shall include, for each disclosure, the date of the disclosure, the name and address of the recipient of the PHI, a description of the PHI disclosed, the name of the individual who is the subject of the PHI disclosed, the purpose of the disclosure, and shall include disclosures made on or after the date that is six (6) years prior to the request or April 14, 2003, whichever is later. Business Associate shall make such record available to the individual or the Covered Entity within fifteen (15) business days of a request for an accounting of disclosures, or within such other time as may be dictated by applicable law.

j) Requests for Restriction. If Business Associate has the ability to perform such a request within the scope of the work performed under the underlying Contract, Business Associate shall comply with requests for restrictions on disclosures of PHI about an individual if the disclosure is to a health plan for purposes of carrying out payment or health care operations (and is not for treatment purposes), and the PHI pertains solely to a health care item or service for which the service involved was paid in full out-of-pocket. For other requests for restriction, Business associate shall otherwise comply with the Privacy Rule, as amended, and other applicable statutory and regulatory requirements

k) Access To Books And Records. Business Associate hereby agrees to make its internal practices, books, and records relating to the use or disclosure of PHI received from, or created or received by Business Associate on behalf of the Covered Entity, available to the Secretary of Health and Human Services or designee for purposes of determining compliance with the HIPAA Privacy Regulations.

l) Return Or Destruction Of PHI. At termination of this Agreement, Business Associate hereby agrees to return or destroy all PHI provided by or obtained on behalf of Covered Entity unless otherwise provided for in this Agreement or directed by Covered Entity. Business Associate agrees not to retain any copies of the PHI after termination of this Agreement. If return or destruction of the PHI is not feasible, Business Associate agrees to extend the protections of this Agreement to limit any further use or disclosure until such time as the PHI may be returned or destroyed. If Business Associate elects to destroy the PHI, it shall certify to Covered Entity that the PHI has been destroyed.

m) Maintenance of PHI. Notwithstanding any other provision of this Agreement, Business Associate shall retain only that PHI that is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities. Business Associate shall return to Covered Entity [or, if agreed to by Covered Entity, destroy] the remaining PHI that Business Associate still maintains in any form. Business Associate shall continue to use

appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic PHI to prevent use or disclosure of the PHI other than as provided for in this Section, for as long as Business Associate retains the PHI. Business Associate shall not use or disclose the PHI retained by Business Associate other than for the purposes for which such PHI was retained and subject to the same conditions set forth in this Agreement. Business Associate shall return to Covered Entity (or, if agreed to by Covered Entity, destroy) the PHI retained by Business Associate when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities.

Business Associate shall continue to maintain the information required under §5(h) of this Agreement for a period of six (6) years after termination of the Agreement, unless Covered Entity and Business Associate agree otherwise.

n) Mitigation Procedures. Business Associate agrees to establish and to provide to Covered Entity upon request, procedures for mitigating, any harmful effect from the use or disclosure of PHI by Business Associate in a manner contrary to this Agreement or applicable laws. In the event of a Security Incident, Business Associate further agrees to mitigate any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of this Agreement or applicable law.

o) Training. Business Associate will train all members of its workforce involved in the performance of the Services who may have access to PHI on its policies and procedures with respect to PHI as necessary and appropriate for the workforce members to carry out the functions required by this contract.

p) Sanction Procedures. Business Associate has a code of conduct policy requiring all employees and subcontractors to adhere to applicable laws and code of conduct and a human resources process for sanctioning employees that do not comply. Business Associate agrees that it shall abide by this process during the term of this Agreement

q) Grounds For Breach by Covered Entity. Upon Business Associate's knowledge of a material breach by Commonwealth of this Business Associate Agreement, Business Associate shall notify Commonwealth of such breach and Commonwealth shall have at least (30) days to cure such breach. In the event Commonwealth does not cure the breach, Business Associate shall have the right to report the violation to the Secretary. Notwithstanding any other language in this Agreement, the parties agree that termination by the Business Associate is infeasible.

r) Grounds For Breach. Any non-compliance by Business Associate with this Agreement or the Privacy or Security Rules will automatically be considered to be a breach of the Agreement, if Business Associate knew or reasonably should have known of such non-compliance and failed to immediately take reasonable steps to cure the non-compliance. Business Associate shall have forty-five (45) days to cure such breach from the date of notice to cure by the Commonwealth. In the event Business Associate does not cure the breach, the Commonwealth shall have the right to immediately terminate this Agreement and the underlying agreement. If termination is infeasible, the Commonwealth shall report the violation to the Secretary.

s) Failure to Perform Obligations. In the event Business Associate fails to perform its obligations under this Agreement, Covered Entity may immediately discontinue providing PHI to Business Associate. Covered Entity may also, at its option, require Business Associate to submit to a plan of compliance, including monitoring by Covered Entity and reporting by Business Associate, as Covered Entity in its sole discretion determines to be necessary to maintain compliance with this Agreement and applicable law.

t) Privacy Practices. The Covered Entity will provide and Business Associate shall immediately begin using in its performance of the Services involving PHI for that Covered Entity any applicable form, including but not limited to, any form used for Notice of Privacy Practices, Accounting for Disclosures, or Authorization, upon the effective date designated by the Covered Entity. The Covered Entity retains the right to change the applicable privacy practices, documents and forms for its PHI. The Business Associate shall implement changes as soon as practicable, but not later than 45 days from the date of notice of the change.

4. OBLIGATIONS OF COVERED ENTITY:

a) Provision of Notice of Privacy Practices. Covered Entity shall provide Business Associate with the notice of privacy practices that the Covered Entity produces in accordance with applicable laws, as well as changes to such notice.

b) Permissions. Covered Entity shall provide Business Associate with any changes in, or revocation of, permission by individual to use or disclose PHI of which Covered Entity is aware, if such changes affect Business Associate's permitted or required uses and disclosures.

c) Restrictions. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of PHI that the Covered Entity has agreed to in accordance with 45 C.F.R. §164.522 and other applicable laws, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

d) Use or Disclosure of PHI. Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Rule if done by the Covered Entity.

5. MISCELLANEOUS:

a) Regulatory References. A reference in this Appendix to a section in the Privacy or Security Rules means the section as in effect or as amended as reasonably determined by the Covered Entity.

b) Amendment. The Parties agree to take such action as is necessary to amend this Appendix from time to time as is necessary for the Covered Entity to comply with the requirements of the Privacy and Security Rules and the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.

c) Survival. The respective rights and obligations of the Covered Entity and Business Associate under this Appendix shall survive the termination of the underlying Contract.

d) Interpretation. Any ambiguity in this Appendix shall be resolved to permit Covered Entity to comply with the Privacy and Security Rules as reasonably determined by the Covered Entity.

e) Changes in Law. Business Associate shall comply with all applicable privacy and security rules and regulations, including but not limited to HIPAA regulations and the HITECH Act and HITECH regulations which are now in effect or which take effect during the term of this contract.

Appendix A to Commonwealth of Pennsylvania Business Associate Agreement

Permitted Uses and Disclosures of Protected Health Information

1. Purpose of Disclosure of PHI to Business Associate: To allow _____ to meet the requirements of Contract # _____.

2. Information to be Disclosed to Business Associate shall include but may not be limited to: _____.

3. Use to Effectuate Purpose of Agreement: _____ may use and disclose PHI to the extent contemplated by Contract #_____ , and as permitted by law with Commonwealth approval and guidance.

Schedule A

DEFINED TERMS

Table of Contents

ABBREVIATIONS AND ACRONYMS **3**
DEFINED TERMS **7**

Abbreviations and Acronyms

Abbreviation / Acronym	Description
ADA	The Americans With Disabilities Act, 28 C.F.R. § 35.101 et seq.
ADM	Application Development and Maintenance
BSBO	Bureau of Small Business Opportunities
BYOD	Bring Your Own Device
CAB	Change Advisory Board
CCPM	Commonwealth Computing Procedures Manual
CHRIA	Criminal History Record Information Act
CI	Configuration Item
CJIS	Criminal Justice Information Services
CMDB	Configuration Management Database
CMs	Critical Measurements
COPANET	Commonwealth Network
CRDD	Customer Requested Due Date
CRQ	Change Request
CSV	Comma Separated Values
CTC	Commonwealth Technology Center
DBA	Database Administration
DGS	Department of General Services
DGS	Department of General Services
DLI	Department of Labor and Industry
DOC	Department of Corrections
DOH	Department of Health

Abbreviation / Acronym	Description
DOR	Department of Revenue
DOT	Department of Transportation
DPH	Data Power House
DPW	Department of Public Welfare
DR	Disaster Recovery
EDC	Enterprise Data Center
FIPS	Federal Information Processing Standards
FIRPA	Family Educational Rights and Privacy Act
GLBA	Gramm-Leach-Bliley Act of 1999
HIPAA	Health Insurance Portability and Accountability Act
HLE	High Level Estimate
HVAC	Heating, Ventilation, and Air Conditioning
IES	Integrated Enterprise Services
IFL	Integrated Facility for Linux
ITB	Information Technologies Bulletin
ITIL	Information Technology Infrastructure Library
ITSM	Information Technologies Service Management
KMs	Key Measurements
KMP	Knowledge Management Portal
LPAR	Logical Partition
MTTR	Mean-Time-to-Resolve
OA	Office of Administration
OA/OIT	Office of Administration / Office for Information Technologies

Abbreviation / Acronym	Description
OAG	Office of Attorney General
OIG	Office of Inspector General
PCI	Payment Card Industry
PCI DSS	Payment Card Industry Data Security Standard
PHI	Protected Health Information
PIP	Private IP
PMO	Program Management Office
PSP	Pennsylvania State Police
PUE	Power Usage Effectiveness
RCA	Root Cause Analysis
RFP	Request For Proposal
RTK	Right-to-Know
RTKL	Right-to-Know Law
RTO	Return To Operations
SDB	Small Diverse Business
SDF	Service Delivery Failure
SDLC	Systems Development Life Cycle
SLAs	Service Level Agreements
SMP	Service Management Platform
SOW	Statement of Work
SOX	Sarbanes-Oxley Act of 2002
SSAE16	Statement on Standards for Attestation Engagements no. 16
TPMO	Transition Program Management Office

Abbreviation / Acronym	Description
UPS	Uninterruptable Power Supply
VRF	Virtual Routing and Forwarding

Defined Terms

Term	Definition
24 x 7 x 365	A continuous, non-stop period of time.
Abandoned Telephone Calls	A telephone call that is initiated by a caller but disconnected prior to answer.
Acceptance Criteria	The list of predetermined objectives that define the minimum capabilities or work results those are acceptable to the Commonwealth.
Acceptance Testing Plan	A mutually agreed plan that includes the testing of application infrastructure performance characteristics prior to migrating each of the current application workloads to the Contractor's infrastructure.
Accurate	Means all Inventory Attributes are correctly and completely populated in the CMDB Inventory of Record.
Agency Agencies	One or more administrative division(s) of the Commonwealth of Pennsylvania.
Application Development and Maintenance (ADM)	The work needed to create, update and maintain software applications.
Application Infrastructure Availability	The time all or a portion the application infrastructure is Available and not in a Degraded Condition.
Assistance Event	As described in section 33 of the Contract.
At-Risk Amount	The amount that the Contractor will have at risk for all Service Level Credits in each month. The "At-Risk Amount" is 15% of the total monthly enterprise invoice submitted to the Commonwealth by the contractor each month.
Availability	The time a Service or application is fully functional (available) to perform the functions it is designed to produce.
Available Time	The time a Service or application is fully functional (available) to perform the functions it is designed to produce.
Backups	A copy of a program or file that is stored separately from the original.

Term	Definition
Baseline Data	The actual data measured during a Measurement Period or applicable historical data of the Commonwealth.
Batch	A common IT industry term representing an execution of a series of programs ("jobs") on a computer without manual intervention.
Benchmark Results	The details of the Benchmarking process intended to determine whether Contractor provides Commonwealth with technology and Services at Service Levels equal to or greater than other organizations receiving similar services.
Benchmark Review Period	The period to review Benchmark Reports to assess the Benchmark Results.
Benchmarker	An independent third-party that undertakes Benchmarking.
Benchmarking	The objective measurement and comparison process (utilizing resource baselines and industry standards) utilized by a Benchmarker to benchmark the quality of the Services and the Fees by Statement of Work or Statement of Works.
Benchmarking Price Protection	The process of an objective measurement and comparison process utilizing baseline methods and industry standards to determine pricing as more fully set forth within Section 25 of the Contract.
Best and Final Offer	As used in the RFP
Bronze	A level of service that has a specific Availability value or Response time interval requirement.
Bureau of Small Business Opportunities (BSBO)	A Bureau within the Commonwealth's Department of General Services responsible for certifying a small diverse businesses as a DGS-certified minority-owned business, woman-owned business, service-disabled veteran-owned business or veteran-owned business, or United States Small Business Administration-certified 8(a) small disadvantaged business concern, that qualifies as a small business.
Business Associate	As defined in the Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191 (HIPAA).
Business Continuity Plan	The plan set out to continue business operations of the Commonwealth in the event of a declared disaster.

Term	Definition
Business Partner	A third party entity that does business with the Commonwealth.
Capacity On Demand	A type of Service for which the capacity can be modified in an automated process with a short implementation time.
Card Holder Data	Credit card records or record systems containing cardholder information including credit card numbers.
Change	An alteration in specifications, services, delivery point, rate of delivery, period of performance, price, or other provisions of the Contract.
Change Advisory Board	A group of individuals authorized to approve or reject individual service and infrastructure changes and to set and guide the Change process.
Change Control Procedures	The procedures used to modify sections of the Contract or modify the configuration of an infrastructure component of a Service.
Change Management	The process responsible for controlling the lifecycle of all Changes, enabling beneficial Changes to be made with minimum interruption to the Services.
Change Order	The documentation used to request, validate, negotiate and approve a change to the Services provided under the Contract.
Change Proposal	The document presented to the Commonwealth by the Contractor to start the Change Control Procedures.
Change Request (CRQ)	The type of request created and processed within the Commonwealth's ITSM system to request authorization to modify an infrastructure component of a Service.

Term	Definition
Chronic Problem	A problem which meets any of the following criteria: 1. The existence two or more Incidents with the same root cause for the same Software, Service, process, or Equipment for which Contractor, the Commonwealth, or the Commonwealth Customer, have designated as a problem requiring a Root Cause Analysis with a corrective action plan. 2. The existence of three or more Service Delivery Failures or outages for the same Software, Service, process, or Equipment within the same month for any two (2) months within any rolling six (6) months. **3.** The existence of three (3) or more Service Delivery Failures or outages for the same Software, Service, process, or Equipment within any rolling six (6) month period for which no root cause has been determined.
CMDB Inventory of Record	The inventory of CIs, including all Equipment and Software, to be created and maintained by Contractor in accordance with the CCPM**.**
Co-location	The ability to provide space, power, and cooling to an asset that is not owned by the Contractor.
Comma Separated Values (CSV)	A type of Text file where the values are delineated with a comma.
Commencement Date	The date a Service is accepted by the Commonwealth.
Commonwealth	The Commonwealth of Pennsylvania.
Commonwealth Computing Procedures Manual (CCPM)	A detailed description of all processes and procedures used to support the computing needs of the Commonwealth via the Contractor's Knowledge/Service Portal. The CCPM contains specific sections dedicated to the operational procedures for each Commonwealth datacenter customer.
Commonwealth Computing Services	The centralized computing capabilities of the Commonwealth that includes Mainframe, Midrange and x86 based servers and the supporting infrastructure.
Commonwealth Contracting Officer	The person authorized to administer this Contract for the Commonwealth and to make written determinations with respect to the Contract.

Term	Definition
Commonwealth Customers	The end users deriving benefits from the Services provided from this Contract.
Commonwealth Enterprise Data Center	See Commonwealth Technology Center
Commonwealth Project Manager	The individual within the Commonwealth who is responsible for managing the Contract**.**
Commonwealth Proprietary Software	The Software owned by the Commonwealth.
Commonwealth Software	The software owned or licensed by the Commonwealth .
Commonwealth Technology Center (CTC)	The Commonwealth's datacenter and adjacent offices located at 1 Technology Park Drive, Harrisburg, PA 17110. Also known as "1 Tech Park" or the EDC.
Commonwealth Third Party Software	Third Party Software for which the Commonwealth has a valid license and current maintenance agreement.
Confidential Information	With regard to the Commonwealth, the data and other information of the Commonwealth or any private individual, organization or public agency, in each case to the extent such information and documentation is not permitted to be disclosed to third parties under local, Commonwealth or Federal laws and regulations or pursuant to any policy adopted by the Commonwealth or pursuant to the terms of any third-party agreement to which Commonwealth is a party. With regard to the Contractor, all Contractor Software and all Contractor documentation and manuals not made available in the ordinary course of business (except those items developed by Contractor specifically to deliver Services to the Commonwealth pursuant to this Contract), and any other information identified in writing by Contractor as confidential or proprietary to Contractor, its Subcontractors or licensors.
Confidential Proprietary Information	All Contractor Software and all Contractor documentation and manuals not made available in the ordinary course of business (except those items developed by Contractor specifically to deliver Services to the Commonwealth pursuant to this Contract), and any other information identified in writing by Contractor as confidential or proprietary to Contractor, its Subcontractors or licensors.

Term	Definition
Configuration Items (CI)	The database record(s) indicating the interrelationships and configuration of a Service, Equipment component, application, and Software
Configuration Management Database (CMDB)	The repository of configuration information related to all the components of the Contractor's datacenter services solution. It contains the details of each of the configuration items (CI) in the IT infrastructure. The CMDB helps provide the relationships between these components (e.g. Application Infrastructure) and track their configuration. The CMDB is a fundamental component of the ITIL framework's Configuration Management process.
Contract	The agreement for provision of Services between Contractor and Commonwealth of which this document is a part.
Contract Year	Change to "year" in contract. May need to specify anniversary date or something like that.
Contractor	Unisys Corporation
Contractor Personnel	People employed by the Contractor who provide or are involved in the provision of the Services.
Contractor Project Manager	The individual within the Contractor that who is responsible for managing the Contract.
Contractor Services Location Manager	Individual who manages a Contractor Service Location
Contractor Software	The software owned or licensed by the Contractor.
Contractor Tools	Any tools, either in object code or source code form, which Contractor has previously developed, or which Contractor independently develops or licenses from a Third Party, excluding any tools that Contractor creates pursuant to this Contract. Contractor Tools includes but is not limited to, methodologies, information, concepts, toolbars for maneuvering between pages, search engines, JAVA applets, and ActiveX controls.
Contractor's Proposal	Proposal submitted by Contractor in Response to the RFP
COPANET	The Commonwealth's private Fiber network.
Covered Entity	As defined in the Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191 (HIPAA).

Term	Definition
Criminal History Record Information Act (CHRIA)	Chapter 91 of the Crimes Code of Pennsylvania and Pennsylvania Consolidated Statues Annotated, 18 Pa. C.S.A. 9101 et. seq.
Criminal Justice Information Services (CJIS)	The policy that provides Criminal Justice Agencies and Noncriminal Justice Agencies with a minimum set of security requirements for the access to Federal Bureau of Investigation Criminal Justice Information Services (CJIS) Division systems and information and to protect and safeguard Criminal Justice Information.
Critical Application	Those applications designated as "Critical Applications" in the Commonwealth Compute Process Manual (CCPM)
Critical Inventory Attributes	Those database fields in an Inventory Record that are essential for Contractor's successful delivery of Service and necessary for the Commonwealth's successful performance of retained responsibilities, including architecture, IT planning, and reconciliation of invoices. Critical Inventory Attributes that must be audited are set out in the CCPM and may be modified over time in accordance with the CCPM.
Critical Measurements (CMs)	Performance measurements defined for the most important service areas
Critical Monthly Reports	A report identified by the Commonwealth as critical and which is required to be delivered monthly.
Critical Services	Those Services designated as "Critical Services" in the Commonwealth Compute Process Manual (CCPM)
Customer Request Date	The customer requested due date (CRDD) in the Contractor's service management platform (SMP).
Customer Time	See Hold Time
Data	Information in a form that can be input to, be created by, be processed by, be stored in, and/or be output by a computer. Data may be in the form of characters such as letters, numbers, punctuation marks, mathematical operators, control characters, or photographic display elements, e.g. pixels.
Data Gathering	The work effort of collecting information to discover and document a process, a procedure, or the configuration of a Service.

Term	Definition
Data Power House (DPH)	The Commonwealth accepted term encompassing the current managed datacenter contract, Services, and location.
Database Administration (DBA)	The function of implementing, configuring, monitoring, and troubleshooting structured data in a common platform/application.
Datacenter Architecture	The resulting equipment and associated network infrastructure viewed as an entire collection of services.
Day	For purposes of the Service Level Matrix, a "day" means a 24 hour period from the trigger for the measurement. For example, if a ticket is logged at 9:15am on Tuesday the 14th, a "day" ends at 9:15am on Wednesday day the 15th.
Days	Calendar days, unless specifically indicated otherwise.
Degraded Condition	A Service that tests as fully operational but is degraded below user expectations across a significant segment of the user population as determined by the Commonwealth.
Deliverable	A Milestone or Service that is subject to acceptance testing in the Acceptance Testing Plan.
Detailed Transition Plan	The plan developed by both the Contractor and the Commonwealth that describes the tasks necessary to complete the transition of the Service into this Contract.
Developed Documentation	Documentation developed by Contractor specifically for the Commonwealth in connection with its performance under this Contract as more fully set forth in Section 40(c) of the Contract.
Developed Materials	All literary works, or other works of authorship (such as application programs, listings, programming tools, documentation, reports, drawings, procedure manuals and similar works) developed under the Contract, as more fully set forth in Section 40(d) of the Contract
Disaster Recovery Plan	The plan created to restore Services to the Commonwealth in the event of a declared disaster.
Disaster Recovery (DR)	A series of events to restore a Service or Equipment in the advent of a major system or network failure, or a natural or man-made event that denies service for an extended period of time.

Term	Definition
Documentation	All written materials, work papers, configurations and manuals (including the CCPM) prepared by or on behalf of the Contractor or any of the Contractor's Subcontractors pursuant to the Contract as more fully set forth in Section 40 of the Contract.
Downtime	The duration a Service or Equipment is not fully functional based on the requirements of the Service or Equipment.
Earn-Back	The Offeror's opportunity to earn back Service Level Credits on Required Service Level Defaults, in accordance with Schedule J.1 (Datacenter Service Level Management).
Effective Date	a) The date the Contract has been fully executed by the Contractor and by the Commonwealth and all approvals required by Commonwealth contracting procedures have been obtained or b) the date referenced in the Contract, whichever is later. The Contract shall not be a legally binding contract until after the fully-executed Contract has been sent to the Contractor.the Contract
Emergency Downtime	Means downtime agreed by the Parties to enable maintenance and break fix i. necessary to address Service issues stemming from Force Majeure causes or **ii.** Otherwise agreed by the Commonwealth pursuant to the Emergency provisions of the Change Control Procedures.
Enterprise Data Center (EDC)	The Commonwealth's datacenter and adjacent offices located at 1 Technology Park Drive, Harrisburg, PA 17110.

Term	Definition
Equipment	All computing, networking, telecommunications and other equipment (hardware and firmware) procured, provided, operated, supported, or used by Contractor in connection with the Services, including but not limited to: a) mainframe, midrange, server and distributed computing equipment and associated attachments, features, accessories, peripheral devices and cabling, b) personal computers, laptop computers, workstations and personal data devices and associated attachments, features, accessories, printers, multi-functional printers, peripheral or network devices and cabling, and c) voice, data, video and wireless telecommunications and network and monitoring equipment and associated attachments, features, accessories, cell phones, peripheral devices and cabling.
ERP systems	Systems that integrate internal and external management information across an entire organization, typically including finance, accounting, sales, service, and customer relationship management, etc.
Expiration Date	The end of the Contract Term, as more fully set forth in Section 1 of the Contract.
Federal Information Processing Standards (FIPS)	Standards and guidelines that are developed by the National Institute of Standards and Technology (NIST) for Federal computer systems. Under the Information Technology Management Reform Act (Public Law 104-106), the Secretary of Commerce approves standards and guidelines that are developed by the National Institute of Standards and Technology (NIST) for Federal computer systems. These standards and guidelines are issued by NIST as Federal Information Processing Standards (FIPS) for use government-wide. NIST develops FIPS when there are compelling Federal government requirements such as for security and interoperability and there are no acceptable industry standards or solutions.
Fees	Any amounts payable by Commonwealth to Contractor.
Force Majeure Event	An event or effect that cannot be reasonably anticipated or controlled, as more fully set forth in Section 65 of the Contract.

Term	Definition
Fulfillment Time	The period of time set out in Schedule C.2 Services Catalog - Descriptions, within which the Contractor must deliver the Services.
Gold	A level of service that has a specific Availability value or Response time interval requirement
High Level Estimate (HLE)	Used when the Commonwealth has a clear technical direction and needs rough estimates on the cost of implementing the Service. HLEs may be used to attach a cost estimate to a prior conceptualization or technical opinion produced by the Offeror.
Hold Time	A period of time when Contractor is prevented from progressing the investigation or repair of an Incident (outage or degradation) due to Commonwealth required decisions or actions. Examples of this include, but are not limited to: i. Not providing physical access to a facility pursuant to the Contract so that Equipment can be tested or replaced ii. Not releasing a application or server for testing iii. Not providing accurate or complete information when opening an Incident resulting in a Contractor inability to progress the resolution of the logged Incident iv. Not responding with necessary additional information upon request to enable the effective investigation or repair of a logged Service ID v. related Incident vi. Commonwealth requested delays in the installation of required patches and/or upgrades vii. Failure of user authentication services, unique end-user VPN client software issues, or other components managed by the Commonwealth. In every case in which Contractor intends to place an Incident or ticket on Hold Time, Contractor will make the appropriate prior notification to the Commonwealth. Valid Hold Time is excluded as outage time in calculations of Service Level Availability and Resolution Time.

Term	Definition
Hybrid Third Party Software	Third Party Software for which the Commonwealth has a valid license, and except for the cost of the license, the contractor shall have financial, administration, operational and maintenance responsibility.
Identity Management	The identification of individuals in a system together with the control of such individual's access to resources within the system by associating rights and restrictions to the established identity.
Impact Study	Study conducted by Contractor related to a proposed Change.
Improved Technology	Any new commercially available information processing technology developments, including new software and hardware developments, that could reasonably be expected to have a positive impact on the Services in terms of increased efficiency or reduced cost.
Improvement Plan	A written plan for improving the Contractor's performance to satisfy Key Measurements.
Incident There are many places that "Incident" is not capitalized. Need to check to see if all that fit this definition are capitalized.	An ITIL term use to describe a failure or loss of capabilities of a Service where a temporary work around is not available or not in place.
Incident Management	ITIL term used to describe the business process related to how an organization is to process and resolve Incidents.
Information Technology Infrastructure Library (ITIL)	A cohesive set of best practices, drawn from the public and private sectors internationally.
Information Technology Service Management (ITSM)	A best practice approach driven both by technology and organizational environments on managing IT services as a whole.

Term	Definition
Inventory Attributes	Those database fields in an Inventory Record that are essential for Contractor's successful delivery of Service and necessary for The Commonwealth's successful performance of retained responsibilities, including architecture, IT planning, and reconciliation of invoices. Inventory Attributes that shall be audited are set out in Commonwealth Computing Procedures Manual and may be modified over time in accordance with the Commonwealth Computing Procedures Manual.
Inventory Record	The record for a single item of Equipment or Software in the CMDB, including all of the Inventory Attributes for that item.
IT Bulletins	Information Technology (IT) bulletins which are issued by the Governor's Office of Administration to set IT policy.
Key Measurements (KMs)	Performance target measurements for non-critical service areas.
Key Personnel	The Contractor's named staff that the Commonwealth determined to be critical to the success of the Project and required the Contractor to provide as defined and governed in Schedule G – Staffing Plan and Key Positions.
Key Positions	The positions that the Commonwealth determined to be critical to the success of the Project and required the Contractor to provide as defined and governed in Schedule G – Staffing Plan and Key Positions
Knowledge/Service Management Portal (KMP)	A software recording tool the Offeror uses to record all incidents, problems, service requests, change requests, and configuration information. All updates to the records, contacts with clients or vendors, and resolutions will be recorded in a real-time and consistent manner.
Management Committee	A committee comprised of ten members, five of whom shall be appointed by Commonwealth and five of whom shall be appointed by Contractor from Contractor's executive management staff.
Market Rate	The average of amounts paid by the reference group for comparable services.
Mean-Time-to-Resolve (MTTR)	The average of the Resolution Time(s) for Incidents that are Resolved within the Measurement Window.

Term	Definition
Measurement Period	The nine (9) consecutive months of measurements during which Baseline Data will be measured, which may be used by the Commonwealth and Contractor to determine Service Level Target and/or Minimum Service Levels. The Contractor will measure, collect and report to the Commonwealth the relevant measurements during such period.
Measurement Window	Shall mean the periodic evaluation and reporting frequency for each individual Service Level as specified in Schedule J.2 (Datacenter Service Level Matrix) (*e.g.*, monthly, quarterly, semi-annually, annually).
Milestone	A Transition Milestone or Critical Milestone.
Milestone Credit	The invoice credits due the Commonwealth if the Contractor fails to attain a Milestone defined in Schedule D - Transition Milestones.
Milestone Due Date	The date by which the Contractor must have completed a Milestone.
Monitoring System	The Equipment and Software used to monitor the performance, capacity, and other events occurring around or within a service provided to the Commonwealth.
Non-Excluded Outage Minutes	Minutes that are not considered Customer Time, Hold Time, or Scheduled Downtime.
Notice of Termination	Written notice provided from the Commonwealth to the Contractor to notify the Contractor that the Commonwealth is terminating the Contract.
OA Service Desk	The entity responsible for Tier I troubleshooting support to the end users by taking requests from end-users, performing triage on the request and escalating as necessary
Offeror	See Contractor.
Office of Administration	An organization within the Commonwealth that provides information technology, human resource, records management, and continuity of government services
Office of Attorney General (OAG)	The office of Pennsylvania's top law enforcement official, which has a wide range of responsibility to protect and serve the citizens and agencies of the Commonwealth.

Term	Definition
Office of Inspector General	An organization within the Commonwealth that works to prevent or find fraud, waste, and abuse in the Commonwealth's programs, operations, and contracts.
Outage	Any service interruption that is or may be experienced by the end-users of the service, application, or equipment.
P Series Servers	A general reference to the IBM collection of servers that typically operate on the AIX operating system.
Payment Card Industry Data Security Standard (PCI DSS)	An actionable framework for developing a robust payment card data security process -- including prevention, detection and appropriate reaction to security incidents.
Pennsylvania	The Commonwealth of Pennsylvania.
Pennsylvania Election Code	The act of June 3, 1937 (P.L.1333, No.320), known as the Pennsylvania Election Code.
Pennsylvania Right-to-Know Law ("RTKL")	The Pennsylvania Right-to-Know Law, 65 P.S. §§ 67.101-3104.
Power Usage Effectiveness ratio (PUE)	A ratio that represents the amount of power consumption of compute versus the total power consumption of a facility as defined by the Green Grid consortium.
Prevailing Wage Act	The Pennsylvania Prevailing Wage Act (43 P.S. §§ 165-1 through 165-17).
Problem	An ITIL term use to describe a failure or loss of capabilities of a Service where a temporary work around is in place.
Problem Management	The business process of managing Problems.
Program Management Office (PMO)	The organization with governance, implementation, and management of the overall engagement.
Protected Health Information (PHI)	The meaning given to such term under HIPAA and the HIPAA Regulations in 45 C.F.R. Parts 160, 162 and 164, including, but not limited to 45 C.F.R. §160.103
Purchase Order	Orders made in accordance with the ordering process set forth in Section 2 of the Contract.

Term	Definition
Regulatory Entity	Any supervisory or governmental agency, body or authority having regulatory or supervisory authority over the Commonwealth, its agencies, the Contractor's and Subcontractors' assets, resources or business and over the Services, including any organization reporting to such bodies.
Remote Hands Support	Shall mean the time and material effort by the Contractor to provide technical support to the Commonwealth in the support of the equipment in co-location.
Request for Criminal Record Check	The form and procedure for looking up and compiling criminal records, commercial records and financial records of an individual, a more fully set forth at Section 44 of the Contract.
Request for Service	The process used by the Commonwealth to order an addition, modification, or removal of a Service component or configuration using the Service Catalog.
Requested Information	Information related to this Contract that is the subject of a request under the Pennsylvania Right-to-Know Law that may be in the Contractor's possession, constituting, or alleged to constitute, a public record in accordance with the RTKL.
Requests	Replace with "project or solution request."
Required Service Level	The expected level of performance for a CM or a KM, as applicable, as set forth in Schedule J.1 (Service Level Methodology).
Reserve Account	A capital improvement fund into which Contractor shall deposit quarterly as specified in Section 13 of the Contract.
Resolution	An action that will resolve an Incident i.e., allow the users to carry out their business functions. This may be a temporary work-around or the permanent repair or replacement of a faulty configuration item.
Resolve	See Resolution
Resolution Time	The time between when an Incident is created (either automatically or manually) and the time the Incident is Resolved.
Respond	See Response

Term	Definition
Response	Contractor taking and logging meaningful action to progress the testing and restoration of any Service ID, or, as the case may be, security Services, that has an active Incident ticket opened in the Incident Management system as defined by the Incident and Problem Management process which is part of the CCPM. Examples of meaningful response actions include the following, all pursuant to the CCPM: • Calling the Commonwealth to obtain additional information to help progress the testing and restoration of the logged incident • Requesting access to a facility • Requesting release of a Service ID for testing • Requesting contact information required to progress the incident management process • Escalating the Incident to technical support for additional testing and analysis
RFP	The Request for Proposal (RFP 6100022698) issued by the Commonwealth for Data Center Computing Services.
Root Cause Analysis (RCA)	A formalized approach and report used to determine the base (or Root) cause of an Incident or Problem.
Run Book	A book containing all of the information needed to perform day-to-day operations and to respond to emergency situations. This information must include the following: •Resource information about the data center and its hardware and software •Process information, including step-by-step procedures for operational and emergency processes
SAP Vendor Number	A vendor identification number for the Commonwealth's SAP ordering and payment processing systems.
Scheduled Availability	24/7/365, unless otherwise specified in a Service Level, minus Scheduled Downtime, Customer Time, Hold Time, and Emergency Downtime.
Scheduled Downtime	Downtime expected and agreed to by the parties, expressed monthly, for which the underlying systems were taken off- line for routine or scheduled maintenance during the Measurement Window.

Term	Definition
Scheduled Uptime	All time except Scheduled Downtime.
Security Incidents	An Incident or Problem that is identified as negatively affecting the security of a Service or a security breach or attack.
Security Patches	A Software update that improves the security of a Service.
Security Update	An Equipment or Software update that improves the security of a Service.
Service Catalog	A listing of Services with pricing and descriptions that are available to the Commonwealth for delivery by Contractor.
Service Delivery Failure	A major recurring problem which is not directly reflected in Service Level performance and for which there is no formal Chronic Problem issue project underway.
Service Desk	The organization that interfaces with end-users on service requests and trouble reporting.
Service Fees	The fees set out in Schedule C, Service Catalog.
Service ID	the unique identifier assigned to a Service by Contractor.
Service Improvement Plan	A written plan submitted by the Contractor setting out the Contractor's plan for improving its Services.
Service Level	The quality and response standards set for Contractor's performance of the Services delivered and are defined in Schedules Schedule J.1 - Datacenter Service Level Management, Schedule J.2 - Datacenter Service Level Matrix, and Schedule J.3 - Datacenter SLA Definitions.
Service Level Agreements (SLAs)	A collection of Service Level commitments provided by Contractor with associated cures.
Service Level Availability	The actual availability of access and all functionality of the Services described in a Service Level expressed as percentage of the Scheduled Availability for such Services.
Service Level Credit	The credits due the Commonwealth in the event the Contractor fails to meet the SLA objectives defined in Schedules Schedule J.1 - Datacenter Service Level Management, Schedule J.2 - Datacenter Service Level Matrix, and Schedule J.3 - Datacenter SLA Definitions.

Term	Definition
Service Level Default	A single failure of the Contractor to meet the applicable Minimum Service Level for a specific CM or KM in the applicable Measurement Window (*e.g.*, monthly).
Service Level Management	The business process for managing compliance with Service Levels.
Service Level Termination Event	Multiple failures over time of a single Service Level or a pattern of failure over time across multiple Service Levels as set out in Schedule J to the Contract.
Service Outage	Any event that unexpectedly denies a service's full functionality to the end-users.
Service Restoral Incident(s)	An Incident where the Service was not available or was in a Degraded Condition and actions were taken to restore the Service to full functionality.
Service(s)	The Services, function and responsibilities described in the Contract, including the Services set forth in Schedule C (Services Catalog) and Schedule F (Statement of Work).
Services Locations	The locations from which Services are provided as agreed upon by the parties as listed in Schedule E (Datacenter Locations).
Severity Level	A priority setting assigned to an Incident or Change that represents the impact the event has on Service. This level is set by the person reporting the Incident or requesting the Change and may be adjusted by authorized personnel at the Commonwealth.
Silver	A level of service that has a specific Availability value or Response time interval requirement.
Small Diverse Business (SDB)	A minority, woman, veteran or service-disabled veteran business enterprise as determined by BSBO.
Software	A collection of one or more programs, databases or microprograms fixed in any tangible medium of expression that comprises a sequence of instructions (source code) to carry out a process in, or convertible into, a form executable by an electronic computer (object code).

Term	Definition
SSAE 16	A service organization reporting standard for performing an examination of a service organization's controls and processes. (Statement on Standards for Attestation Engagements (SSAE) No. 16)
Standard Service Request	A service request that is routine in nature and that does not require extensive engineering or solutioning to develop the request.
Statement of Work (SOW)	The Services, function and responsibilities described in the Agreement, including the services set forth in Schedule F (Datacenter Statement of Work).
Subcontractors	A third party (including an affiliate of Contractor) to which Contractor subcontracts or otherwise delegates its obligations to perform the Services.
Systems Development Life Cycle (SDLC)	A methodology used to create or modify a software application or system.
Targeted Application Infrastructure	Used to describe a particular Contractor's application's infrastructure related components or configuration items (CIs) When measuring actual application infrastructure related availability it is important to look at all the components that make up the application infrastructure such as all Servers, Storage, Networking, Firewalls, etc. components as defined in the CMDB.
Term	The duration the Contact between the Commonwealth and the Contract.
Termination Assistance Services	All necessary and appropriate actions to accomplish a complete, timely, and seamless transition of any Terminated Services from Offeror to the Commonwealth, or to any replacement provider designated by the Commonwealth.
Termination for Convenience	A termination based on a determination by the Commonwealth that termination is in its best interest.
Termination for Convenience Fee	A fee due to the Contractor in the event the Commonwealth terminates the Contract for convenience, as more fully set forth in Section 32(a) of the Contract.
Text	A data format in which information can be stored that is usable by a standard personal computer

Term	Definition
Third Party	Someone indirectly involved in the Contract, but who is not a principal party to the Contract.
Third Party Contract	A contract with a Third Party.
Third Party Software	All Software products (and all modifications, replacements, upgrades, enhancements, documentation, materials and media related thereto) that are provided under license or lease by a Third Party to Contractor or Commonwealth.
Tier III Datacenter Rating	Uptime Institute Tier Standard: Topology, TIA-942 Telecommunications Infrastructure Standard for Data Centers, and BICSI 002-2011 Data Center Design and Implementation Best Practices.
Tiered Disaster Recovery	A Disaster Recovery plan that allows for multiple Return to Operation (RTO) timeframes to satisfy varying Commonwealth requirements.
Transition CAP Notice	Written notice that Contractor has or is reasonably likely to fail to deliver the Transition Services.
Transition Failure Event	Failure of the Contractor to complete the Transition Services within the timeframe set out in the Detailed Transition Plan.
Transition Milestone	Those tasks and associated completion dates set forth in Schedule D (Transition Milestones).
Transition Orders	The orders for existing Commonwealth services that will be placed to transition those services into the Contract.
Transition Plan	The plan set out and agreed to by the parties in Schedule M – Detailed Transition Plan detailing the activities, timescales and responsibilities for transitioning the services from Commonwealth to Contractor, including Transition Milestones.
Transition Program Management Office (TPMO)	The organization responsible for transitioning services to the Contractor's control. The TPMO will provide program management Services to deliver architecture, transition plan integration, and organizational change management, as well as quality assurance, verification of testing, financial oversight, and operational readiness for the Mainframe and Server transition/consolidation program.

Term	Definition
Transition Services	The transition activities, functions and deliverables described in the Detailed Transition Plan and such other tasks as are necessary to enable Contactor provide the Services.
Vulnerability Analyses	A security analysis to determine the possibility of an unauthorized intrusion, loss of data, denial of service or other security breach.
x86	A series of computer microprocessor instruction set architectures based on the Intel 8086 CPU.
XML	A data format standard allowing computing systems to exchange information over a data connection.

SCHEDULE B

GOVERNANCE

1. **Management Meetings**. There shall be weekly meetings of the Management Committee during the Transition Period and monthly meetings thereafter. The purpose of such meetings shall be to (1) track the progress of the Transition and Transformation Plan, (2) review Contractor's performance of the Services Levels, (3) resolve disputes, (4) track the progress of the Services and other projects, (5) coordinate and plan for any new hardware or software acquisitions and service deployments, and (6) address any other matters properly brought before the Management Committee.

2. **Management Committee**. "*Management Committee"* shall be a committee comprised of ten members, five of whom shall be appointed by Commonwealth and five of whom shall be appointed by Contractor from Contractor's executive management staff. Commonwealth and Contractor shall each have one (1) vote with respect to matters that are brought before the Management Committee for resolution. Commonwealth shall designate one of its members on the Management Committee to act as the chairperson of the Management Committee. Both Commonwealth and Contractor can change the individuals on the Management Committee on an as-needed basis. The Management Committee shall be authorized and responsible for (1) generally overseeing the performance of this Contract, (2) providing input and advise to the Governor's Office of Administration regarding Commonwealth's strategic and tactical decisions in respect of the Services, the Systems and any other aspect of the business relationship between Commonwealth and Contractor under this Contract, and (3) monitoring and attempting to resolve disputes regarding the provision of the Services and the Services Levels.

3. **Commonwealth Computing Procedures Manual**. For each Commonwealth Agency and as part of the Services, Contractor shall establish procedures pursuant to which Contractor proposes that policies of Commonwealth and Contractor will be adhered to during the Term for the Commonwealth, and shall deliver to Commonwealth, not later than thirty (30) days prior to the commencement of the activities contemplated under the Transition Plan for the Commonwealth's approval or comment, a draft Commonwealth Computing Procedures Manual generally summarizing (1) the Services, (2) the computer hardware and software environments in which, and the various Services Locations at which, the Services will be performed, (3) the documentation, if any, which provides further details regarding the Services, (4) the procedures Contractor intends to use, and the activities Contractor proposes to undertake, in order to manage the Services, and (5) the procedures of a management reporting system that Contractor will use to manage this Contract and communicate to and with Commonwealth. Commonwealth may, at its request, participate to whatever degree it desires in the preparation of the draft Commonwealth Computing Procedures Manual. Contractor may periodically propose and, at the request of Commonwealth, shall promptly propose updates of the Commonwealth Computing Procedures Manual to reflect any changes in the operations or procedures described therein, all of which proposed changes shall be subject to Commonwealth's approval or comment. Reference Schedule H - Commonwealth Computing Procedures Manual for additional details.

Schedule C.1

SERVICES CATALOG

SERVICES CATALOG

Field Name ==>	Product Name	Unit	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use ==>	*Unique Identifier*	*Unit*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Server - Fully Managed																		
x86 Server Configurations (Windows)																		
x86 Physical Server - Windows - Fully Managed	2-way Quad-Core 2.0 GHz	Per Server	CCSU13310001-A						$ 28.41	$ 28.34	$ 28.27	$ 26.00	$ 22.88	$ 19.45	$ 16.53	$ 16.53	$ 16.53	$ 16.53
x86 Physical Server - Windows - Fully Managed	2-way Six-Core 2.4 GHz	Per Server	CCSU13310002-A						$ 58.53	$ 58.38	$ 58.24	$ 53.58	$ 47.15	$ 40.08	$ 34.07	$ 34.07	$ 34.07	$ 34.07
x86 Physical Server - Windows - Fully Managed	4-way Six-Core 2.0 GHz	Per Server	CCSU13310003-A						$ 48.01	$ 47.89	$ 47.77	$ 43.94	$ 38.67	$ 32.87	$ 27.94	$ 27.94	$ 27.94	$ 27.94
x86 Physical Server - Windows - Fully Managed	GB RAM	Per GB	CCSU13310004-A						$ 0.02	$ 0.02	$ 0.02	$ 0.02	$ 0.02	$ 0.02	$ 0.01	$ 0.01	$ 0.01	$ 0.01
x86 Physical Server - Windows - Fully Managed	Mirrored 146 15K Hard Drives	Per Primary + Mirror drive	CCSU13310005-A						$ 14.63	$ 14.60	$ 14.56	$ 13.39	$ 11.79	$ 10.02	$ 8.52	$ 8.52	$ 8.52	$ 8.52
x86 Physical Server - Windows - Fully Managed	SAN Attached Storage	Per GB	CCSU13310006-A						$ 0.15	$ 0.15	$ 0.14	$ 0.13	$ 0.12	$ 0.10	$ 0.08	$ 0.08	$ 0.08	$ 0.08
x86 Physical Server - Windows - Fully Managed	Windows Server 2008 R2	Per License	CCSU13310007-A						$ 162.58	$ 162.18	$ 161.77	$ 148.83	$ 130.97	$ 111.33	$ 94.63	$ 94.63	$ 94.63	$ 94.63
x86 Physical Server - Windows - Fully Managed	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization Site s Local SAN Storage from hourly data synchronization	Per Service	CCSU13310008-A						$ 308.91	$ 308.14	$ 307.37	$ 282.78	$ 248.85	$ 211.52	$ 179.79	$ 179.79	$ 179.79	$ 179.79
x86 Physical Server - Windows - Fully Managed	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Service	CCSU13310009-A						$ 236.12	$ 235.54	$ 234.95	$ 216.15	$ 190.21	$ 161.68	$ 137.43	$ 137.43	$ 137.43	$ 137.43
x86 Physical Server - Windows - Fully Managed	Fully Managed (No DR) - Platinum Tier	Per Server	CCSU13310010-A						$ 378.79	$ 377.85	$ 376.90	$ 346.75	$ 305.14	$ 259.37	$ 220.47	$ 220.47	$ 220.47	$ 220.47
x86 Physical Server - Windows - Fully Managed	Fully Managed (No DR) - Gold Tier	Per Server	CCSU13310011-A						$ 374.84	$ 373.90	$ 372.97	$ 343.13	$ 301.96	$ 256.66	$ 218.16	$ 218.16	$ 218.16	$ 218.16
x86 Physical Server - Windows - Fully Managed	Fully Managed (No DR) - Silver Tier	Per Server	CCSU13310012-A						$ 372.88	$ 371.95	$ 371.02	$ 341.34	$ 300.38	$ 255.32	$ 217.02	$ 217.02	$ 217.02	$ 217.02
x86 Physical Server - Windows - Fully Managed	Fully Managed (No DR) - Bronze Tier	Per Server	CCSU13310013-A						$ 372.14	$ 371.22	$ 370.29	$ 340.67	$ 299.79	$ 254.82	$ 216.60	$ 216.60	$ 216.60	$ 216.60
x86 Physical Server - Windows - Fully Managed	Fully Managed (No DR) - Basic Tier	Per Server	CCSU13310014-A						$ 370.86	$ 369.93	$ 369.01	$ 339.49	$ 298.75	$ 253.94	$ 215.85	$ 215.85	$ 215.85	$ 215.85
x86 Physical Server - Windows - Fully Managed	Fully Managed (24 Hr DR) - Platinum Tier	Per Server	CCSU13310025-A						$ 424.15	$ 423.09	$ 422.04	$ 388.28	$ 341.68	$ 290.43	$ 246.87	$ 246.87	$ 246.87	$ 246.87
x86 Physical Server - Windows - Fully Managed	Fully Managed (24 Hr DR) - Gold Tier	Per Server	CCSU13310026-A						$ 418.10	$ 417.06	$ 416.02	$ 382.73	$ 336.81	$ 286.29	$ 243.34	$ 243.34	$ 243.34	$ 243.34
x86 Physical Server - Windows - Fully Managed	Fully Managed (24 Hr DR) - Silver Tier	Per Server	CCSU13310027-A						$ 414.22	$ 413.19	$ 412.16	$ 379.19	$ 333.68	$ 283.63	$ 241.09	$ 241.09	$ 241.09	$ 241.09
x86 Physical Server - Windows - Fully Managed	Fully Managed (24 Hr DR) - Bronze Tier	Per Server	CCSU13310028-A						$ 412.59	$ 411.57	$ 410.54	$ 377.70	$ 332.37	$ 282.52	$ 240.14	$ 240.14	$ 240.14	$ 240.14
x86 Physical Server - Windows - Fully Managed	Fully Managed (24 Hr DR) - Basic Tier	Per Server	CCSU13310029-A						$ 410.45	$ 409.43	$ 408.41	$ 375.73	$ 330.65	$ 281.05	$ 238.89	$ 238.89	$ 238.89	$ 238.89
x86 Physical Server - Windows - Fully Managed	Fully Managed (72 Hr DR) - Platinum Tier	Per Server	CCSU13310030-A						$ 424.15	$ 423.09	$ 422.04	$ 388.28	$ 341.68	$ 290.43	$ 246.87	$ 246.87	$ 246.87	$ 246.87
x86 Physical Server - Windows - Fully Managed	Fully Managed (72 Hr DR) - Gold Tier	Per Server	CCSU13310031-A						$ 418.10	$ 417.06	$ 416.02	$ 382.73	$ 336.81	$ 286.29	$ 243.34	$ 243.34	$ 243.34	$ 243.34
x86 Physical Server - Windows - Fully Managed	Fully Managed (72 Hr DR) - Silver Tier	Per Server	CCSU13310032-A						$ 414.22	$ 413.19	$ 412.16	$ 379.19	$ 333.68	$ 283.63	$ 241.09	$ 241.09	$ 241.09	$ 241.09
x86 Physical Server - Windows - Fully Managed	Fully Managed (72 Hr DR) - Bronze Tier	Per Server	CCSU13310033-A						$ 412.59	$ 411.57	$ 410.54	$ 377.70	$ 332.37	$ 282.52	$ 240.14	$ 240.14	$ 240.14	$ 240.14
x86 Physical Server - Windows - Fully Managed	Fully Managed (72 Hr DR) - Basic Tier	Per Server	CCSU13310034-A						$ 410.45	$ 409.43	$ 408.41	$ 375.73	$ 330.65	$ 281.05	$ 238.89	$ 238.89	$ 238.89	$ 238.89
x86 Server Configurations (Linux)																		
x86 Physical Server - Linux - Fully Managed	2-way Quad-Core 2.0 GHz	Per Server	CCSU13310035-A						$ 28.41	$ 28.34	$ 28.27	$ 26.00	$ 22.88	$ 19.45	$ 16.53	$ 16.53	$ 16.53	$ 16.53
x86 Physical Server - Linux - Fully Managed	2-way Six-Core 2.4 GHz	Per Server	CCSU13310036-A						$ 58.53	$ 58.38	$ 58.24	$ 53.58	$ 47.15	$ 40.08	$ 34.07	$ 34.07	$ 34.07	$ 34.07
x86 Physical Server - Linux - Fully Managed	4-way Six-Core 2.0 GHz	Per Server	CCSU13310037-A						$ 48.01	$ 47.89	$ 47.77	$ 43.94	$ 38.67	$ 32.87	$ 27.94	$ 27.94	$ 27.94	$ 27.94
x86 Physical Server - Linux - Fully Managed	GB RAM	Per GB	CCSU13310038-A						$ 0.02	$ 0.02	$ 0.02	$ 0.02	$ 0.02	$ 0.02	$ 0.01	$ 0.01	$ 0.01	$ 0.01
x86 Physical Server - Linux - Fully Managed	Mirrored 146 15K Hard Drives	Per Primary + Mirror drive	CCSU13310039-A						$ 14.63	$ 14.60	$ 14.56	$ 13.39	$ 11.79	$ 10.02	$ 8.52	$ 8.52	$ 8.52	$ 8.52
x86 Physical Server - Linux - Fully Managed	SAN Attached Storage	Per GB	CCSU13310040-A						$ 0.15	$ 0.15	$ 0.14	$ 0.13	$ 0.12	$ 0.10	$ 0.08	$ 0.08	$ 0.08	$ 0.08
x86 Physical Server - Linux - Fully Managed	RedHat or SUSE	Per License	CCSU13310041-A						$ 139.57	$ 139.22	$ 138.87	$ 127.76	$ 112.43	$ 95.57	$ 81.23	$ 81.23	$ 81.23	$ 81.23
x86 Physical Server - Linux - Fully Managed	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Service	CCSU13310042-A						$ 285.90	$ 285.18	$ 284.47	$ 261.71	$ 230.31	$ 195.76	$ 166.40	$ 166.40	$ 166.40	$ 166.40
x86 Physical Server - Linux - Fully Managed	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Service	CCSU13310043-A						$ 213.11	$ 212.58	$ 212.05	$ 195.08	$ 171.67	$ 145.92	$ 124.03	$ 124.03	$ 124.03	$ 124.03
x86 Physical Server - Linux - Fully Managed	Fully Managed (No DR) - Platinum Tier	Per Server	CCSU13310044-A						$ 435.89	$ 434.81	$ 433.72	$ 399.02	$ 351.14	$ 298.47	$ 253.70	$ 253.70	$ 253.70	$ 253.70
x86 Physical Server - Linux - Fully Managed	Fully Managed (No DR) - Gold Tier	Per Server	CCSU13310045-A						$ 422.92	$ 421.87	$ 420.82	$ 387.15	$ 340.69	$ 289.59	$ 246.15	$ 246.15	$ 246.15	$ 246.15
x86 Physical Server - Linux - Fully Managed	Fully Managed (No DR) - Silver Tier	Per Server	CCSU13310046-A						$ 415.26	$ 414.23	$ 413.19	$ 380.14	$ 334.52	$ 284.34	$ 241.69	$ 241.69	$ 241.69	$ 241.69
x86 Physical Server - Linux - Fully Managed	Fully Managed (No DR) - Bronze Tier	Per Server	CCSU13310047-A						$ 411.92	$ 410.89	$ 409.87	$ 377.08	$ 331.83	$ 282.05	$ 239.75	$ 239.75	$ 239.75	$ 239.75

SERVICES CATALOG

Field Name ==>	Product Name	Unit	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use ==>	*Unique Identifier*	*Unit*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
x86 Physical Server - Linux - Fully Managed	Fully Managed (No DR) - Basic Tier	Per Server	CCSU13310048-A						$ 408.63	$ 407.61	$ 406.60	$ 374.07	$ 329.18	$ 279.80	$ 237.83	$ 237.83	$ 237.83	$ 237.83
x86 Physical Server - Linux - Fully Managed	Fully Managed (24 Hr DR) - Platinum Tier	Per Server	CCSU13310059-A						$ 536.37	$ 535.03	$ 533.70	$ 491.00	$ 432.08	$ 367.27	$ 312.18	$ 312.18	$ 312.18	$ 312.18
x86 Physical Server - Linux - Fully Managed	Fully Managed (24 Hr DR) - Gold Tier	Per Server	CCSU13310060-A						$ 513.64	$ 512.36	$ 511.08	$ 470.20	$ 413.77	$ 351.71	$ 298.95	$ 298.95	$ 298.95	$ 298.95
x86 Physical Server - Linux - Fully Managed	Fully Managed (24 Hr DR) - Silver Tier	Per Server	CCSU13310061-A						$ 497.95	$ 496.71	$ 495.47	$ 455.84	$ 401.14	$ 340.97	$ 289.82	$ 289.82	$ 289.82	$ 289.82
x86 Physical Server - Linux - Fully Managed	Fully Managed (24 Hr DR) - Bronze Tier	Per Server	CCSU13310062-A						$ 491.11	$ 489.88	$ 488.66	$ 449.57	$ 395.62	$ 336.28	$ 285.83	$ 285.83	$ 285.83	$ 285.83
x86 Physical Server - Linux - Fully Managed	Fully Managed (24 Hr DR) - Basic Tier	Per Server	CCSU13310063-A						$ 484.60	$ 483.39	$ 482.19	$ 443.61	$ 390.38	$ 331.82	$ 282.05	$ 282.05	$ 282.05	$ 282.05
x86 Physical Server - Linux - Fully Managed	Fully Managed (72 Hr DR) - Platinum Tier	Per Server	CCSU13310064-A						$ 536.37	$ 535.03	$ 533.70	$ 491.00	$ 432.08	$ 367.27	$ 312.18	$ 312.18	$ 312.18	$ 312.18
x86 Physical Server - Linux - Fully Managed	Fully Managed (72 Hr DR) - Gold Tier	Per Server	CCSU13310065-A						$ 513.64	$ 512.36	$ 511.08	$ 470.20	$ 413.77	$ 351.71	$ 298.95	$ 298.95	$ 298.95	$ 298.95
x86 Physical Server - Linux - Fully Managed	Fully Managed (72 Hr DR) - Silver Tier	Per Server	CCSU13310066-A						$ 497.95	$ 496.71	$ 495.47	$ 455.84	$ 401.14	$ 340.97	$ 289.82	$ 289.82	$ 289.82	$ 289.82
x86 Physical Server - Linux - Fully Managed	Fully Managed (72 Hr DR) - Bronze Tier	Per Server	CCSU13310067-A						$ 491.11	$ 489.88	$ 488.66	$ 449.57	$ 395.62	$ 336.28	$ 285.83	$ 285.83	$ 285.83	$ 285.83
x86 Physical Server - Linux - Fully Managed	Fully Managed (72 Hr DR) - Basic Tier	Per Server	CCSU13310068-A						$ 484.60	$ 483.39	$ 482.19	$ 443.61	$ 390.38	$ 331.82	$ 282.05	$ 282.05	$ 282.05	$ 282.05
x86 (Windows) - Virtual Servers																		
x86 Virtual Server - Windows - Fully Managed	2vCPU	Per Instance	CCSU13310069-A						$ 1.42	$ 1.42	$ 1.41	$ 1.30	$ 1.14	$ 0.97	$ 0.83	$ 0.83	$ 0.83	$ 0.83
x86 Virtual Server - Windows - Fully Managed	4vCPU	Per Instance	CCSU13310070-A						$ 2.84	$ 2.83	$ 2.83	$ 2.60	$ 2.29	$ 1.95	$ 1.65	$ 1.65	$ 1.65	$ 1.65
x86 Virtual Server - Windows - Fully Managed	8vCPU	Per Instance	CCSU13310071-A						$ 5.68	$ 5.67	$ 5.65	$ 5.20	$ 4.58	$ 3.89	$ 3.31	$ 3.31	$ 3.31	$ 3.31
x86 Virtual Server - Windows - Fully Managed	GB Ram	Per GB	CCSU13310072-A						$ 0.37	$ 0.36	$ 0.36	$ 0.33	$ 0.29	$ 0.25	$ 0.21	$ 0.21	$ 0.21	$ 0.21
x86 Virtual Server - Windows - Fully Managed	Windows Server 2008 R2	Per License	CCSU13310073-A						$ 18.25	$ 18.21	$ 18.16	$ 16.71	$ 14.70	$ 12.50	$ 10.62	$ 10.62	$ 10.62	$ 10.62
x86 Virtual Server - Windows - Fully Managed	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Server	CCSU13310078-A						$ 99.73	$ 99.48	$ 99.23	$ 91.29	$ 80.34	$ 68.29	$ 58.04	$ 58.04	$ 58.04	$ 58.04
x86 Virtual Server - Windows - Fully Managed	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Server	CCSU13310079-A						$ 26.94	$ 26.87	$ 26.81	$ 24.66	$ 21.70	$ 18.45	$ 15.68	$ 15.68	$ 15.68	$ 15.68
x86 Virtual Server - Windows - Fully Managed	Fully Managed (No DR) - Platinum Tier	Per Server	CCSU13310080-A						$ 374.50	$ 373.57	$ 372.64	$ 342.83	$ 301.69	$ 256.43	$ 217.97	$ 217.97	$ 217.97	$ 217.97
x86 Virtual Server - Windows - Fully Managed	Fully Managed (No DR) - Gold Tier	Per Server	CCSU13310081-A						$ 372.40	$ 371.47	$ 370.55	$ 340.90	$ 300.00	$ 255.00	$ 216.75	$ 216.75	$ 216.75	$ 216.75
x86 Virtual Server - Windows - Fully Managed	Fully Managed (No DR) - Silver Tier	Per Server	CCSU13310082-A						$ 370.49	$ 369.57	$ 368.64	$ 339.15	$ 298.45	$ 253.69	$ 215.63	$ 215.63	$ 215.63	$ 215.63
x86 Virtual Server - Windows - Fully Managed	Fully Managed (No DR) - Bronze Tier	Per Server	CCSU13310083-A						$ 369.59	$ 368.67	$ 367.75	$ 338.33	$ 297.73	$ 253.07	$ 215.11	$ 215.11	$ 215.11	$ 215.11
x86 Virtual Server - Windows - Fully Managed	Fully Managed (No DR) - Basic Tier	Per Server	CCSU13310084-A						$ 368.74	$ 367.82	$ 366.90	$ 337.55	$ 297.04	$ 252.49	$ 214.61	$ 214.61	$ 214.61	$ 214.61
x86 Virtual Server - Windows - Fully Managed	Fully Managed (24 Hr DR) - Platinum Tier	Per Server	CCSU13310095-A						$ 424.05	$ 422.99	$ 421.93	$ 388.18	$ 341.60	$ 290.36	$ 246.80	$ 246.80	$ 246.80	$ 246.80
x86 Virtual Server - Windows - Fully Managed	Fully Managed (24 Hr DR) - Gold Tier	Per Server	CCSU13310096-A						$ 419.85	$ 418.80	$ 417.76	$ 384.33	$ 338.21	$ 287.48	$ 244.36	$ 244.36	$ 244.36	$ 244.36
x86 Virtual Server - Windows - Fully Managed	Fully Managed (24 Hr DR) - Silver Tier	Per Server	CCSU13310097-A						$ 416.02	$ 414.98	$ 413.95	$ 380.83	$ 335.13	$ 284.86	$ 242.13	$ 242.13	$ 242.13	$ 242.13
x86 Virtual Server - Windows - Fully Managed	Fully Managed (24 Hr DR) - Bronze Tier	Per Server	CCSU13310098-A						$ 414.23	$ 413.20	$ 412.16	$ 379.19	$ 333.69	$ 283.64	$ 241.09	$ 241.09	$ 241.09	$ 241.09
x86 Virtual Server - Windows - Fully Managed	Fully Managed (24 Hr DR) - Basic Tier	Per Server	CCSU13310099-A						$ 412.51	$ 411.49	$ 410.46	$ 377.62	$ 332.31	$ 282.46	$ 240.09	$ 240.09	$ 240.09	$ 240.09
x86 Virtual Server - Windows - Fully Managed	Fully Managed (72 Hr DR) - Platinum Tier	Per Server	CCSU13310100-A						$ 424.05	$ 422.99	$ 421.93	$ 388.18	$ 341.60	$ 290.36	$ 246.80	$ 246.80	$ 246.80	$ 246.80
x86 Virtual Server - Windows - Fully Managed	Fully Managed (72 Hr DR) - Gold Tier	Per Server	CCSU13310101-A						$ 419.85	$ 418.80	$ 417.76	$ 384.33	$ 338.21	$ 287.48	$ 244.36	$ 244.36	$ 244.36	$ 244.36
x86 Virtual Server - Windows - Fully Managed	Fully Managed (72 Hr DR) - Silver Tier	Per Server	CCSU13310102-A						$ 416.02	$ 414.98	$ 413.95	$ 380.83	$ 335.13	$ 284.86	$ 242.13	$ 242.13	$ 242.13	$ 242.13
x86 Virtual Server - Windows - Fully Managed	Fully Managed (72 Hr DR) - Bronze Tier	Per Server	CCSU13310103-A						$ 414.23	$ 413.20	$ 412.16	$ 379.19	$ 333.69	$ 283.64	$ 241.09	$ 241.09	$ 241.09	$ 241.09
x86 Virtual Server - Windows - Fully Managed	Fully Managed (72 Hr DR) - Basic Tier	Per Server	CCSU13310104-A						$ 412.51	$ 411.49	$ 410.46	$ 377.62	$ 332.31	$ 282.46	$ 240.09	$ 240.09	$ 240.09	$ 240.09
x86 (Linux) - Virtual Servers																		
x86 Virtual Server - Linux - Fully Managed	2vCPU	Per Instance	CCSU13310105-A						$ 1.42	$ 1.42	$ 1.41	$ 1.30	$ 1.14	$ 0.97	$ 0.83	$ 0.83	$ 0.83	$ 0.83
x86 Virtual Server - Linux - Fully Managed	4vCPU	Per Instance	CCSU13310106-A						$ 2.84	$ 2.83	$ 2.83	$ 2.60	$ 2.29	$ 1.95	$ 1.65	$ 1.65	$ 1.65	$ 1.65
x86 Virtual Server - Linux - Fully Managed	8vCPU	Per Instance	CCSU13310107-A						$ 5.68	$ 5.67	$ 5.65	$ 5.20	$ 4.58	$ 3.89	$ 3.31	$ 3.31	$ 3.31	$ 3.31
x86 Virtual Server - Linux - Fully Managed	GB Ram	Per GB	CCSU13310108-A						$ 0.37	$ 0.36	$ 0.36	$ 0.33	$ 0.29	$ 0.25	$ 0.21	$ 0.21	$ 0.21	$ 0.21
x86 Virtual Server - Linux - Fully Managed	RedHat or SUSE	Per License	CCSU13310109-A						$ 59.26	$ 59.11	$ 58.96	$ 54.24	$ 47.73	$ 40.57	$ 34.49	$ 34.49	$ 34.49	$ 34.49
x86 Virtual Server - Linux - Fully Managed	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Server	CCSU13310114-A						$ 140.73	$ 140.38	$ 140.03	$ 128.83	$ 113.37	$ 96.36	$ 81.91	$ 81.91	$ 81.91	$ 81.91

SERVICES CATALOG

Field Name ==>	Product Name	Unit	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use ==>	*Unique Identifier*	*Unit*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
x86 Virtual Server - Linux - Fully Managed	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Server	CCSU13310115-A						$ 67.95	$ 67.78	$ 67.61	$ 62.20	$ 54.73	$ 46.52	$ 39.55	$ 39.55	$ 39.55	$ 39.55
x86 Virtual Server - Linux - Fully Managed	Fully Managed (No DR) - Platinum Tier	Per Server	CCSU13310116-A						$ 388.08	$ 387.11	$ 386.15	$ 355.26	$ 312.63	$ 265.73	$ 225.87	$ 225.87	$ 225.87	$ 225.87
x86 Virtual Server - Linux - Fully Managed	Fully Managed (No DR) - Gold Tier	Per Server	CCSU13310117-A						$ 378.33	$ 377.38	$ 376.44	$ 346.33	$ 304.77	$ 259.05	$ 220.19	$ 220.19	$ 220.19	$ 220.19
x86 Virtual Server - Linux - Fully Managed	Fully Managed (No DR) - Silver Tier	Per Server	CCSU13310118-A						$ 370.30	$ 369.37	$ 368.45	$ 338.98	$ 298.30	$ 253.55	$ 215.52	$ 215.52	$ 215.52	$ 215.52
x86 Virtual Server - Linux - Fully Managed	Fully Managed (No DR) - Bronze Tier	Per Server	CCSU13310119-A						$ 366.79	$ 365.88	$ 364.97	$ 335.77	$ 295.48	$ 251.16	$ 213.48	$ 213.48	$ 213.48	$ 213.48
x86 Virtual Server - Linux - Fully Managed	Fully Managed (No DR) - Basic Tier	Per Server	CCSU13310120-A						$ 363.57	$ 362.67	$ 361.76	$ 332.82	$ 292.88	$ 248.95	$ 211.61	$ 211.61	$ 211.61	$ 211.61
x86 Virtual Server - Linux - Fully Managed	Fully Managed (24 Hr DR) - Platinum Tier	Per Server	CCSU13310131-A						$ 492.78	$ 491.55	$ 490.33	$ 451.10	$ 396.97	$ 337.42	$ 286.81	$ 286.81	$ 286.81	$ 286.81
x86 Virtual Server - Linux - Fully Managed	Fully Managed (24 Hr DR) - Gold Tier	Per Server	CCSU13310132-A						$ 473.27	$ 472.09	$ 470.92	$ 433.24	$ 381.25	$ 324.07	$ 275.46	$ 275.46	$ 275.46	$ 275.46
x86 Virtual Server - Linux - Fully Managed	Fully Managed (24 Hr DR) - Silver Tier	Per Server	CCSU13310133-A						$ 457.22	$ 456.08	$ 454.94	$ 418.54	$ 368.32	$ 313.07	$ 266.11	$ 266.11	$ 266.11	$ 266.11
x86 Virtual Server - Linux - Fully Managed	Fully Managed (24 Hr DR) - Bronze Tier	Per Server	CCSU13310134-A						$ 450.21	$ 449.09	$ 447.97	$ 412.13	$ 362.67	$ 308.27	$ 262.03	$ 262.03	$ 262.03	$ 262.03
x86 Virtual Server - Linux - Fully Managed	Fully Managed (24 Hr DR) - Basic Tier	Per Server	CCSU13310135-A						$ 443.77	$ 442.66	$ 441.56	$ 406.24	$ 357.49	$ 303.86	$ 258.28	$ 258.28	$ 258.28	$ 258.28
x86 Virtual Server - Linux - Fully Managed	Fully Managed (72 Hr DR) - Platinum Tier	Per Server	CCSU13310136-A						$ 492.78	$ 491.55	$ 490.33	$ 451.10	$ 396.97	$ 337.42	$ 286.81	$ 286.81	$ 286.81	$ 286.81
x86 Virtual Server - Linux - Fully Managed	Fully Managed (72 Hr DR) - Gold Tier	Per Server	CCSU13310137-A						$ 473.27	$ 472.09	$ 470.92	$ 433.24	$ 381.25	$ 324.07	$ 275.46	$ 275.46	$ 275.46	$ 275.46
x86 Virtual Server - Linux - Fully Managed	Fully Managed (72 Hr DR) - Silver Tier	Per Server	CCSU13310138-A						$ 457.22	$ 456.08	$ 454.94	$ 418.54	$ 368.32	$ 313.07	$ 266.11	$ 266.11	$ 266.11	$ 266.11
x86 Virtual Server - Linux - Fully Managed	Fully Managed (72 Hr DR) - Bronze Tier	Per Server	CCSU13310139-A						$ 450.21	$ 449.09	$ 447.97	$ 412.13	$ 362.67	$ 308.27	$ 262.03	$ 262.03	$ 262.03	$ 262.03
x86 Virtual Server - Linux - Fully Managed	Fully Managed (72 Hr DR) - Basic Tier	Per Server	CCSU13310140-A						$ 443.77	$ 442.66	$ 441.56	$ 406.24	$ 357.49	$ 303.86	$ 258.28	$ 258.28	$ 258.28	$ 258.28
P-Series Server Configurations																		
AIX - Fully Managed	3.0GHz POWER7	Per Server	CCSI13310141-A						$ 97.49	$ 96.52	$ 95.55	$ 94.59	$ 93.64	$ 92.71	$ 91.79	$ 91.79	$ 91.79	$ 91.79
AIX - Fully Managed	Cores	Per .5 Core	CCSI13310142-A						$ 30.26	$ 29.95	$ 29.65	$ 29.36	$ 29.07	$ 28.77	$ 28.48	$ 28.48	$ 28.48	$ 28.48
AIX - Fully Managed	GB RAM	Per GB	CCSI13310143-A						$ 1.26	$ 1.25	$ 1.24	$ 1.23	$ 1.23	$ 1.22	$ 1.20	$ 1.20	$ 1.20	$ 1.20
AIX - Fully Managed	AIX	Per License	CCSI13310144-A						$ 47.07	$ 49.59	$ 51.27	$ 54.64	$ 57.15	$ 59.67	$ 63.04	$ 63.04	$ 63.04	$ 63.04
AIX - Fully Managed	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Server	CCSI13310145-A						$ 360.37	$ 366.72	$ 372.41	$ 380.40	$ 388.18	$ 395.64	$ 404.70	$ 404.70	$ 404.70	$ 404.70
AIX - Fully Managed	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Server	CCSI13310146-A						$ 206.34	$ 207.26	$ 207.37	$ 209.17	$ 210.16	$ 211.15	$ 212.99	$ 212.99	$ 212.99	$ 212.99
AIX - Fully Managed	Fully Managed (.5 Core and 6 GB RAM - No DR) - Platinum Tier	Per LPAR	CCSI13310147-A						$ 746.35	$ 757.45	$ 768.72	$ 780.15	$ 794.19	$ 757.66	$ 746.62	$ 746.62	$ 746.62	$ 746.62
AIX - Fully Managed	Fully Managed (.5 Core and 6 GB RAM - No DR) - Gold Tier	Per LPAR	CCSI13310148-A						$ 633.10	$ 645.72	$ 658.60	$ 671.74	$ 687.44	$ 651.76	$ 641.56	$ 641.56	$ 641.56	$ 641.56
AIX - Fully Managed	Fully Managed (.5 Core and 6 GB RAM -No DR) - Silver Tier	Per LPAR	CCSI13310149-A						$ 536.73	$ 550.02	$ 563.64	$ 577.60	$ 594.15	$ 559.31	$ 549.95	$ 549.95	$ 549.95	$ 549.95
AIX - Fully Managed	Fully Managed (.5 Core and 6 GB RAM - No DR) - Bronze Tier	Per LPAR	CCSI13310150-A						$ 440.41	$ 454.32	$ 468.67	$ 483.47	$ 500.86	$ 466.85	$ 458.34	$ 458.34	$ 458.34	$ 458.34
AIX - Fully Managed	Fully Managed (.5 Core and 6 GB RAM - No DR) - Basic Tier	Per LPAR	CCSI13310151-A						$ 344.29	$ 358.69	$ 373.70	$ 389.34	$ 407.57	$ 374.41	$ 366.73	$ 366.73	$ 366.73	$ 366.73
AIX - Fully Managed	Fully Managed (1 Core and 12 GB RAM - No DR) - Platinum Tier	Per LPAR	CCSI13310152-A						$ 757.27	$ 768.57	$ 780.04	$ 791.68	$ 805.91	$ 768.74	$ 757.06	$ 757.06	$ 757.06	$ 757.06
AIX - Fully Managed	Fully Managed (1 Core and 12 GB RAM - No DR) - Gold Tier	Per LPAR	CCSI13310153-A						$ 643.97	$ 656.00	$ 668.26	$ 680.75	$ 695.81	$ 659.48	$ 649.48	$ 649.48	$ 649.48	$ 649.48
AIX - Fully Managed	Fully Managed (1 Core and 12 GB RAM - No DR) - Silver Tier	Per LPAR	CCSI13310154-A						$ 547.57	$ 560.28	$ 573.29	$ 586.60	$ 603.35	$ 568.70	$ 559.55	$ 559.55	$ 559.55	$ 559.55
AIX - Fully Managed	Fully Managed (1 Core and 12 GB RAM - No DR) - Bronze Tier	Per LPAR	CCSI13310155-A						$ 451.35	$ 465.45	$ 480.00	$ 495.00	$ 512.59	$ 478.78	$ 470.46	$ 470.46	$ 470.46	$ 470.46
AIX - Fully Managed	Fully Managed (1 Core and 12 GB RAM - No DR) - Basic Tier	Per LPAR	CCSI13310156-A						$ 355.19	$ 369.81	$ 385.03	$ 400.87	$ 419.30	$ 386.32	$ 378.84	$ 378.84	$ 378.84	$ 378.84
AIX - Fully Managed	Fully Managed (1.5 Core and 18 GB RAM- No DR) - Platinum Tier	Per LPAR	CCSI13310157-A						$ 784.95	$ 795.65	$ 806.50	$ 817.49	$ 831.92	$ 794.94	$ 783.46	$ 783.46	$ 783.46	$ 783.46
AIX - Fully Managed	Fully Managed (1.5 Core and 18 GB RAM - No DR) - Gold Tier	Per LPAR	CCSI13310158-A						$ 671.74	$ 683.96	$ 696.41	$ 709.08	$ 724.34	$ 688.21	$ 677.57	$ 677.57	$ 677.57	$ 677.57

SERVICES CATALOG

Field Name ==>	Product Name	Unit	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use ==>	*Unique Identifier*	*Unit*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
AIX - Fully Managed	Fully Managed (1.5 Core and 18 GB RAM - No DR) - Silver Tier	Per LPAR	CCSI13310159-A						$ 562.68	$ 575.60	$ 588.82	$ 602.33	$ 618.44	$ 583.14	$ 573.34	$ 573.34	$ 573.34	$ 573.34
AIX - Fully Managed	Fully Managed (1.5 Core and 18 GB RAM - No DR) - Bronze Tier	Per LPAR	CCSI13310160-A						$ 478.93	$ 492.50	$ 506.45	$ 520.81	$ 537.76	$ 503.31	$ 494.33	$ 494.33	$ 494.33	$ 494.33
AIX - Fully Managed	Fully Managed (1.5 Core and 18 GB RAM - No DR) - Basic Tier	Per LPAR	CCSI13310161-A						$ 382.70	$ 396.83	$ 411.48	$ 426.68	$ 444.47	$ 410.85	$ 402.73	$ 402.73	$ 402.73	$ 402.73
AIX - Fully Managed	Fully Managed (1 Core and 12 GB RAM - 24 Hr DR) - Platinum Tier	Per LPAR	CCSI13310162-A						$ 1,254.37	$ 1,257.27	$ 1,260.17	$ 1,263.09	$ 1,269.40	$ 1,224.31	$ 1,203.85	$ 1,203.85	$ 1,203.85	$ 1,203.85
AIX - Fully Managed	Fully Managed (1 Core and 12 GB RAM - 24 Hr DR) - Gold Tier	Per LPAR	CCSI13310163-A						$ 1,027.52	$ 1,032.06	$ 1,036.62	$ 1,041.20	$ 1,049.21	$ 1,005.80	$ 988.70	$ 988.70	$ 988.70	$ 988.70
AIX - Fully Managed	Fully Managed (1 Core and 12 GB RAM - 24 Hr DR) - Silver Tier	Per LPAR	CCSI13310164-A						$ 834.29	$ 840.46	$ 846.67	$ 852.92	$ 864.31	$ 824.25	$ 808.85	$ 808.85	$ 808.85	$ 808.85
AIX - Fully Managed	Fully Managed (1 Core and 12 GB RAM - 24 Hr DR) - Bronze Tier	Per LPAR	CCSI13310165-A						$ 641.24	$ 650.60	$ 660.08	$ 669.71	$ 682.76	$ 644.39	$ 630.67	$ 630.67	$ 630.67	$ 630.67
AIX - Fully Managed	Fully Managed (1 Core and 12 GB RAM - 24 Hr DR) - Basic Tier	Per LPAR	CCSI13310166-A						$ 448.32	$ 459.10	$ 470.14	$ 481.45	$ 496.18	$ 459.49	$ 447.43	$ 447.43	$ 447.43	$ 447.43
AIX - Fully Managed	Fully Managed (1 Core and 12 GB RAM - 72 Hr DR) - Platinum Tier	Per LPAR	CCSI13310167-A						$ 1,254.37	$ 1,257.27	$ 1,260.17	$ 1,263.09	$ 1,269.40	$ 1,224.31	$ 1,203.85	$ 1,203.85	$ 1,203.85	$ 1,203.85
AIX - Fully Managed	Fully Managed (1 Core and 12 GB RAM - 72 Hr DR) - Gold Tier	Per LPAR	CCSI13310168-A						$ 1,027.52	$ 1,032.06	$ 1,036.62	$ 1,041.20	$ 1,049.21	$ 1,005.80	$ 988.70	$ 988.70	$ 988.70	$ 988.70
AIX - Fully Managed	Fully Managed (1 Core and 12 GB RAM - 72 Hr DR) - Silver Tier	Per LPAR	CCSI13310169-A						$ 834.29	$ 840.46	$ 846.67	$ 852.92	$ 864.31	$ 824.25	$ 808.85	$ 808.85	$ 808.85	$ 808.85
AIX - Fully Managed	Fully Managed (1 Core and 12 GB RAM - 72 Hr DR) - Bronze Tier	Per LPAR	CCSI13310170-A						$ 641.24	$ 650.60	$ 660.08	$ 669.71	$ 682.76	$ 644.39	$ 630.67	$ 630.67	$ 630.67	$ 630.67
AIX - Fully Managed	Fully Managed (1 Core and 12 GB RAM - 72 Hr DR) - Basic Tier	Per LPAR	CCSI13310171-A						$ 448.32	$ 459.10	$ 470.14	$ 481.45	$ 496.18	$ 459.49	$ 447.43	$ 447.43	$ 447.43	$ 447.43
Server - Managed Only x86 (Windows, Linux)																		
x86 Servers - Managed Only	Platinum Tier	Server/Instance	CCSU13320001-A						$ 435.89	$ 434.81	$ 433.72	$ 399.02	$ 351.14	$ 298.47	$ 253.70	$ 253.70	$ 253.70	$ 253.70
x86 Servers - Managed Only	Gold Tier	Server/Instance	CCSU13320002-A						$ 422.92	$ 421.87	$ 420.82	$ 387.15	$ 340.69	$ 289.59	$ 246.15	$ 246.15	$ 246.15	$ 246.15
x86 Servers - Managed Only	Silver Tier	Server/Instance	CCSU13320003-A						$ 415.26	$ 414.23	$ 413.19	$ 380.14	$ 334.52	$ 284.34	$ 241.69	$ 241.69	$ 241.69	$ 241.69
x86 Servers - Managed Only	Bronze Tier	Server/Instance	CCSU13320004-A						$ 411.92	$ 410.89	$ 409.87	$ 377.08	$ 331.83	$ 282.05	$ 239.75	$ 239.75	$ 239.75	$ 239.75
x86 Servers - Managed Only	Basic Tier	Server/Instance	CCSU13320005-A						$ 408.63	$ 407.61	$ 406.60	$ 374.07	$ 329.18	$ 279.80	$ 237.83	$ 237.83	$ 237.83	$ 237.83
Server - Managed Only UNIX (IBM P-Series, AIX)																		
AIX Servers - Managed Only	Platinum	LPAR	CCSI13320006-A						$ 728.02	$ 743.06	$ 758.40	$ 774.06	$ 791.48	$ 757.50	$ 749.88	$ 749.88	$ 749.88	$ 749.88
AIX Servers - Managed Only	Gold Tier	LPAR	CCSI13320007-A						$ 678.20	$ 694.06	$ 710.29	$ 726.90	$ 745.25	$ 712.21	$ 705.53	$ 705.53	$ 705.53	$ 705.53
AIX Servers - Managed Only	Silver Tier	LPAR	CCSI13320008-A						$ 630.19	$ 645.99	$ 662.18	$ 678.78	$ 697.13	$ 664.10	$ 657.43	$ 657.43	$ 657.43	$ 657.43
AIX Servers - Managed Only	Bronze Tier	LPAR	CCSI13320009-A						$ 572.89	$ 589.46	$ 606.52	$ 624.07	$ 643.36	$ 611.28	$ 605.53	$ 605.53	$ 605.53	$ 605.53
AIX Servers - Managed Only	Basic Tier	LPAR	CCSI13320010-A						$ 462.09	$ 479.27	$ 497.09	$ 515.57	$ 535.81	$ 504.67	$ 499.88	$ 499.88	$ 499.88	$ 499.88
Storage and Backup - Fully Managed (1)																		
Enterprise Storage																		
Storage and Backup - Fully Managed	* Dedicated - Config 1 - SAN Raid 5	GB	CCSZ13310172-A						$ 0.05	$ 0.05	$ 0.05	$ 0.05	$ 0.04	$ 0.04	$ 0.04	$ 0.04	$ 0.04	$ 0.04
Storage and Backup - Fully Managed	* Dedicated - Config 2 - SAN Raid 10	GB	CCSZ13310173-A						$ 0.36	$ 0.34	$ 0.32	$ 0.31	$ 0.29	$ 0.28	$ 0.26	$ 0.26	$ 0.26	$ 0.26
Storage and Backup - Fully Managed	Dedicated - Config 3 - Net Attached	GB	CCSZ13310174-A						$ 0.05	$ 0.06	$ 0.06	$ 0.05	$ 0.05	$ 0.05	$ 0.05	$ 0.05	$ 0.05	$ 0.05
Tape and Backup																		
Storage and Backup - Fully Managed	** Server Tape Stored	GB Stored	CCSU13310175-A						$ 0.02	$ 0.02	$ 0.02	$ 0.02	$ 0.01	$ 0.01	$ 0.01	$ 0.01	$ 0.01	$ 0.01
Storage and Backup - Fully Managed	** Offsite Tape Storage	Tapes	CCSU13310176-A						$ 0.38	$ 0.36	$ 0.35	$ 0.34	$ 0.33	$ 0.31	$ 0.31	$ 0.31	$ 0.31	$ 0.31
Limited Co-Lo (Data Center Only Charge) (3)																		
Limited Co-Lo Configurations																		
Limited Co-Location	1/4 Rack Configuration includes 10U Cabinet Space	Per 1/4 Rack	CCSU13330001-A						$ 50.08	$ 48.14	$ 46.16	$ 46.35	$ 43.85	$ 41.67	$ 39.42	$ 39.42	$ 39.42	$ 39.42
Limited Co-Location	1/2 Rack Configuration includes 21U Cabinet Space	Per 1/2 Rack	CCSU13330002-A						$ 77.62	$ 73.94	$ 70.15	$ 66.25	$ 64.08	$ 59.93	$ 55.65	$ 55.65	$ 55.65	$ 55.65
Limited Co-Location	Full Rack Configuration includes 42U Cabinet Space	Per Rack	CCSU13330003-A						$ 176.43	$ 169.37	$ 162.10	$ 154.60	$ 114.18	$ 106.18	$ 97.91	$ 97.91	$ 97.91	$ 97.91
Limited Co-Location	Network Bandwidth	Per GB	CCSU13330004-A						$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Limited Co-Location	100Mb/s Uplink	Each	CCSU13330005-A						$ 6.25	$ 6.44	$ 6.63	$ 6.83	$ 7.03	$ 7.25	$ 7.46	$ 7.46	$ 7.46	$ 7.46
Limited Co-Location	IP Addresses	Each	CCSU13330006-A						$ 0.75	$ 0.75	$ 0.75	$ 0.75	$ 0.75	$ 0.75	$ 0.75	$ 0.75	$ 0.75	$ 0.75
Limited Co-Location	110V AC Circuits	Per Circuit	CCSU13330007-A						$ 14.00	$ 14.42	$ 14.85	$ 15.30	$ 15.76	$ 16.23	$ 16.72	$ 16.72	$ 16.72	$ 16.72
Mainframe Services (4)																		

SERVICES CATALOG

Field Name ==>	Product Name	Unit	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use ==>	*Unique Identifier*	*Unit*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
IBM Mainframe																		
IBM Mainframe - Fully Managed	*** IBM Mainframe Allocated DASD	GB	CCSI13310177-A						$ 1.25	$ 1.19	$ 1.13	$ 1.08	$ 1.02	$ 0.97	$ 0.91	$ 0.91	$ 0.91	$ 0.91
IBM Mainframe - Fully Managed	IBM Tapes in Storage - VTS	GB	CCSI13310178-A						$ 0.29	$ 0.29	$ 0.28	$ 0.28	$ 0.27	$ 0.27	$ 0.25	$ 0.25	$ 0.25	$ 0.25
IBM Mainframe - Fully Managed	IBM Offsite Tape Storage	Tape/Reel	CCSI13310179-A						$ 0.38	$ 0.36	$ 0.35	$ 0.34	$ 0.33	$ 0.31	$ 0.31	$ 0.31	$ 0.31	$ 0.31
IBM Mainframe Configurations																		
IBM Mainframe - Fully Managed	IBM System zEnterprise Processor z/OS	Per MIP	CCSI13310180-A						$ 102.61	$ 104.92	$ 107.23	$ 101.87	$ 96.78	$ 91.94	$ 87.34	$ 87.34	$ 87.34	$ 87.34
IBM Mainframe - Fully Managed	IBM System zEnterprise Processor Virtual Linux Prod IFL	Per MIP	CCSI13310181-A						$ 90.16	$ 92.19	$ 94.22	$ 89.51	$ 85.04	$ 80.79	$ 76.75	$ 76.75	$ 76.75	$ 76.75
IBM Mainframe - Fully Managed	IBM System zEnterprise Processor Virtual Linux Prod IFLw/ Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per MIP	CCSI13310182-A						$ 104.67	$ 107.56	$ 110.44	$ 105.58	$ 100.57	$ 96.12	$ 91.71	$ 91.71	$ 91.71	$ 91.71
IBM Mainframe - Fully Managed	IBM i Series / AS400	Per CPW	CCSI13310183-A						$ 11.20	$ 11.45	$ 11.69	$ 11.12	$ 10.56	$ 10.03	$ 9.53	$ 9.53	$ 9.53	$ 9.53
IBM Mainframe - Fully Managed	IBM i Series / AS400 w/ Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per CPW	CCSI13310184-A						$ 28.17	$ 29.38	$ 30.58	$ 29.73	$ 28.57	$ 27.71	$ 26.71	$ 26.71	$ 26.71	$ 26.71
IBM Mainframe - Fully Managed	Mainframe Services (4-z/OS - No DR) - Platinum Tier	Per MIP	CCSI13310185-A						$ 115.12	$ 202.54	$ 289.95	$ 286.02	$ 282.44	$ 269.93	$ 266.76	$ 266.76	$ 266.76	$ 266.76
IBM Mainframe - Fully Managed	Mainframe Services (4 z/OS - No DR) - Gold Tier	Per MIP	CCSI13310186-A						$ 100.47	$ 187.56	$ 274.65	$ 271.46	$ 268.60	$ 256.79	$ 254.27	$ 254.27	$ 254.27	$ 254.27
IBM Mainframe - Fully Managed	Mainframe Services (4 z/OS - No DR) - Basic Tier	Per MIP	CCSI13310187-A						$ 90.32	$ 177.17	$ 264.03	$ 261.38	$ 259.02	$ 247.70	$ 245.64	$ 245.64	$ 245.64	$ 245.64
IBM Mainframe - Fully Managed	Mainframe Services (4 z/Linux IFL - No DR) - Platinum Tier	Per MIP	CCSI13310188-A						$ 101.14	$ 188.23	$ 275.33	$ 272.12	$ 269.22	$ 257.38	$ 254.84	$ 254.84	$ 254.84	$ 254.84
IBM Mainframe - Fully Managed	Mainframe Services (4 z/Linux IFL - No DR) - Gold Tier	Per MIP	CCSI13310189-A						$ 88.29	$ 175.10	$ 261.91	$ 259.36	$ 257.10	$ 245.87	$ 243.89	$ 243.89	$ 243.89	$ 243.89
IBM Mainframe - Fully Managed	Mainframe Services (4 z/Linux IFL - No DR) - Basic Tier	Per MIP	CCSI13310190-A						$ 79.37	$ 165.97	$ 252.58	$ 250.50	$ 248.69	$ 237.87	$ 236.30	$ 236.30	$ 236.30	$ 236.30
IBM Mainframe - Fully Managed	Mainframe Services (4-z/Linux IFL - 24 HR DR) - Platinum Tier	Per MIP	CCSI13310191-A						$ 187.78	$ 323.40	$ 459.02	$ 445.97	$ 434.11	$ 413.46	$ 402.72	$ 402.72	$ 402.72	$ 402.72
IBM Mainframe - Fully Managed	Mainframe Services (4 z/Linux IFL - 24 HR DR) - Gold Tier	Per MIP	CCSI13310192-A						$ 162.06	$ 297.12	$ 432.18	$ 420.45	$ 409.86	$ 390.42	$ 380.82	$ 380.82	$ 380.82	$ 380.82
IBM Mainframe - Fully Managed	Mainframe Services (4-z/Linux IFL - 24 Hr DR) - Basic Tier	Per MIP	CCSI13310193-A						$ 144.23	$ 278.87	$ 413.51	$ 402.74	$ 393.04	$ 374.43	$ 365.64	$ 365.64	$ 365.64	$ 365.64
IBM Mainframe - Fully Managed	Mainframe Services (4-iSeries - No DR) - Platinum Tier	Per CPW	CCSI13310194-A						$ 12.56	$ 97.66	$ 182.77	$ 184.17	$ 185.68	$ 178.02	$ 179.44	$ 179.44	$ 179.44	$ 179.44
IBM Mainframe - Fully Managed	Mainframe Services (4-iSeries - No DR) - Gold Tier	Per CPW	CCSI13310195-A						$ 10.96	$ 96.03	$ 181.10	$ 182.59	$ 184.18	$ 176.60	$ 178.07	$ 178.07	$ 178.07	$ 178.07
IBM Mainframe - Fully Managed	Mainframe Services (4- Series - No DR) - Basic Tier	Per CPW	CCSI13310196-A						$ 9.85	$ 94.90	$ 179.94	$ 181.49	$ 183.13	$ 175.60	$ 177.15	$ 177.15	$ 177.15	$ 177.15
IBM Mainframe - Fully Managed	Mainframe Services (4-iSeries - 24 Hr DR) - Platinum Tier	Per CPW	CCSI13310197-A						$ 30.21	$ 121.58	$ 212.94	$ 212.86	$ 212.96	$ 203.93	$ 204.07	$ 204.07	$ 204.07	$ 204.07
IBM Mainframe - Fully Managed	Mainframe Services (4-iSeries - 24 Hr DR) - Gold Tier	Per CPW	CCSI13310198-A						$ 27.02	$ 118.31	$ 209.61	$ 209.70	$ 209.95	$ 201.07	$ 201.36	$ 201.36	$ 201.36	$ 201.36
IBM Mainframe - Fully Managed	Mainframe Services (4-iSeries - 24 Hr DR) - Basic Tier	Per CPW	CCSI13310199-A						$ 24.80	$ 116.05	$ 207.29	$ 207.50	$ 207.87	$ 199.09	$ 199.48	$ 199.48	$ 199.48	$ 199.48
Unisys Mainframe																		
Unisys Mainframe - Fully Managed	*** Unisys DASD	GB	CCSU13310200-A						$ 0.14	$ 0.14	$ 0.14	$ 0.14	$ 0.14	$ 0.12	$ 0.12	$ 0.12	$ 0.12	$ 0.12
Unisys Mainframe - Fully Managed	Unisys Tapes in Storage - VTS	GB	CCSU13310201-A						$ 0.07	$ 0.07	$ 0.07	$ 0.07	$ 0.07	$ 0.05	$ 0.05	$ 0.05	$ 0.05	$ 0.05
Unisys Mainframe - Fully Managed	Unisys Offsite Tape Storage	Tape/Reel	CCSU13310202-A						$ 0.38	$ 0.36	$ 0.35	$ 0.34	$ 0.33	$ 0.31	$ 0.31	$ 0.31	$ 0.31	$ 0.31
Unisys Mainframe Configurations																		
Unisys Mainframe - Fully Managed	Unisys (Clearpath / Dorado)	Per MIP	CCSU13310203-A						$ 190.93	$ 188.45	$ 177.92	$ 176.87	$ 175.47	$ 174.53	$ 173.13	$ 173.13	$ 173.13	$ 173.13
Unisys Mainframe - Fully Managed	Unisys (Clearpath / Libra)	Per MIP	CCSU13310204-A						$ 79.83	$ 79.77	$ 79.77	$ 79.76	$ 78.42	$ 74.51	$ 73.23	$ 73.23	$ 73.23	$ 73.23

SERVICES CATALOG

Field Name ==>	Product Name	Unit	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use ==>	*Unique Identifier*	*Unit*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Unisys Mainframe - Fully Managed	Unisys (Clearpath / Dorado) w/ Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per MIP	CCSU13310205-A						$ 215.77	$ 212.93	$ 202.35	$ 200.91	$ 199.26	$ 197.93	$ 196.16	$ 196.16	$ 196.16	$ 196.16
Unisys Mainframe - Fully Managed	Unisys (Clearpath / Libra) w/ Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per MIP	CCSU13310206-A						$ 152.12	$ 152.05	$ 152.04	$ 152.07	$ 149.96	$ 144.93	$ 141.63	$ 141.63	$ 141.63	$ 141.63
Unisys Mainframe - Fully Managed	Mainframe Services (4-Unisys Dorado - No DR) - Platinum Tier	Per MIP	CCSU13310207-A						$ 111.33	$ 113.02	$ 114.69	$ 116.53	$ 118.40	$ 113.31	$ 114.99	$ 114.99	$ 114.99	$ 114.99
Unisys Mainframe - Fully Managed	Mainframe Services (4-Unisys Dorado - No DR) - Gold Tier	Per MIP	CCSU13310208-A						$ 111.09	$ 112.78	$ 114.47	$ 116.30	$ 118.17	$ 113.09	$ 114.77	$ 114.77	$ 114.77	$ 114.77
Unisys Mainframe - Fully Managed	Mainframe Services (4-Unisys Dorado - No DR) - Basic Tier	Per MIP	CCSU13310209-A						$ 108.79	$ 110.51	$ 112.32	$ 114.17	$ 116.06	$ 110.98	$ 112.68	$ 112.68	$ 112.68	$ 112.68
Unisys Mainframe - Fully Managed	Mainframe Services (4-Unisys Libra - No DR) - Platinum Tier	Per MIP	CCSU13310210-A						$ 101.29	$ 103.32	$ 105.00	$ 106.79	$ 108.48	$ 103.08	$ 105.40	$ 105.40	$ 105.40	$ 105.40
Unisys Mainframe - Fully Managed	Mainframe Services (4-Unisys Libra - No DR) - Gold Tier	Per MIP	CCSU13310211-A						$ 101.29	$ 103.32	$ 105.00	$ 106.79	$ 108.48	$ 103.08	$ 105.40	$ 105.40	$ 105.40	$ 105.40
Unisys Mainframe - Fully Managed	Mainframe Services (4-Unisys Libra - No DR) - Basic Tier	Per MIP	CCSU13310212-A						$ 101.29	$ 103.33	$ 105.01	$ 106.73	$ 108.48	$ 103.08	$ 105.40	$ 105.40	$ 105.40	$ 105.40
Unisys Mainframe - Fully Managed	Mainframe Services (4 Unisys Dorado - 24 Hr DR) - Platinum Tier	Per MIP	CCSU13310213-A						$ 110.44	$ 112.17	$ 114.77	$ 116.38	$ 118.05	$ 112.55	$ 115.32	$ 115.32	$ 115.32	$ 115.32
Unisys Mainframe - Fully Managed	Mainframe Services (4-Unisys Dorado - 24 Hr DR) - Gold Tier	Per MIP	CCSU13310214-A						$ 110.41	$ 112.14	$ 114.74	$ 116.35	$ 118.02	$ 112.52	$ 115.29	$ 115.29	$ 115.29	$ 115.29
Unisys Mainframe - Fully Managed	Mainframe Services (4-Unisys Dorado - 24 Hr DR) - Basic Tier	Per MIP	CCSU13310215-A						$ 110.11	$ 111.84	$ 114.44	$ 116.06	$ 117.73	$ 112.24	$ 115.02	$ 115.02	$ 115.02	$ 115.02
Unisys Mainframe - Fully Managed	Mainframe Services (4-Unisys Libra - 24 Hr DR) - Platinum Tier	Per MIP	CCSU13310216-A						$ 106.22	$ 108.01	$ 109.65	$ 111.32	$ 114.03	$ 108.60	$ 110.81	$ 110.81	$ 110.81	$ 110.81
Unisys Mainframe - Fully Managed	Mainframe Services (4-Unisys Libra - 24 Hr DR) - Gold Tier	Per MIP	CCSU13310217-A						$ 106.22	$ 108.01	$ 109.65	$ 111.32	$ 114.03	$ 108.60	$ 110.81	$ 110.81	$ 110.81	$ 110.81
Unisys Mainframe - Fully Managed	Mainframe Services (4-Unisys Libra - 24 Hr DR) - Basic Tier	Per MIP	CCSU13310218-A						$ 106.20	$ 108.01	$ 109.65	$ 111.32	$ 114.03	$ 108.60	$ 110.81	$ 110.81	$ 110.81	$ 110.81
IaaS x86 Server Configurations (Windows)																		
x86 Virtual Server - Windows - Infrastructure as a Service	2vCPU	Per Server	CCSU13340001-A						$ 1.42	$ 1.42	$ 1.41	$ 1.30	$ 1.14	$ 0.97	$ 0.83	$ 0.83	$ 0.83	$ 0.83
x86 Virtual Server - Windows - Infrastructure as a Service	4vCPU	Per Server	CCSU13340002-A						$ 2.84	$ 2.83	$ 2.83	$ 2.60	$ 2.29	$ 1.95	$ 1.65	$ 1.65	$ 1.65	$ 1.65
x86 Virtual Server - Windows - Infrastructure as a Service	8vCPU	Per Server	CCSU13340003-A						$ 5.68	$ 5.67	$ 5.65	$ 5.20	$ 4.58	$ 3.89	$ 3.31	$ 3.31	$ 3.31	$ 3.31
x86 Virtual Server - Windows - Infrastructure as a Service	GB Ram	Per GB	CCSU13340004-A						$ 0.37	$ 0.36	$ 0.36	$ 0.33	$ 0.29	$ 0.25	$ 0.21	$ 0.21	$ 0.21	$ 0.21
x86 Virtual Server - Windows - Infrastructure as a Service	Windows Server 2008 R2	Per License	CCSU13340005-A						$ 22.91	$ 22.78	$ 22.79	$ 21.57	$ 19.52	$ 17.43	$ 15.63	$ 15.63	$ 15.63	$ 15.63
x86 Virtual Server - Windows - Infrastructure as a Service	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Config	CCSU13340010-A						$ 99.73	$ 99.48	$ 99.23	$ 91.29	$ 80.34	$ 68.29	$ 58.04	$ 58.04	$ 58.04	$ 58.04
x86 Virtual Server - Windows - Infrastructure as a Service	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Config	CCSU13340011-A						$ 26.94	$ 26.87	$ 26.81	$ 24.66	$ 21.70	$ 18.45	$ 15.68	$ 15.68	$ 15.68	$ 15.68
IaaS x86 Server Configurations (Linux)																		
x86 Virtual Server - Linux - Infrastructure as a Service	2vCPU	Per Server	CCSU13340012-A						$ 1.42	$ 1.42	$ 1.41	$ 1.30	$ 1.14	$ 0.97	$ 0.83	$ 0.83	$ 0.83	$ 0.83
x86 Virtual Server - Linux - Infrastructure as a Service	4vCPU	Per Server	CCSU13340013-A						$ 2.84	$ 2.83	$ 2.83	$ 2.60	$ 2.29	$ 1.95	$ 1.65	$ 1.65	$ 1.65	$ 1.65
x86 Virtual Server - Linux - Infrastructure as a Service	8vCPU	Per Server	CCSU13340014-A						$ 5.68	$ 5.67	$ 5.65	$ 5.20	$ 4.58	$ 3.89	$ 3.31	$ 3.31	$ 3.31	$ 3.31
x86 Virtual Server - Linux - Infrastructure as a Service	GB Ram	Per GB	CCSU13340015-A						$ 0.37	$ 0.36	$ 0.36	$ 0.33	$ 0.29	$ 0.25	$ 0.21	$ 0.21	$ 0.21	$ 0.21
x86 Virtual Server - Linux - Infrastructure as a Service	RedHat or SUSE	Per License	CCSU13340016-A						$ 63.92	$ 63.68	$ 63.59	$ 59.10	$ 52.55	$ 45.50	$ 39.50	$ 39.50	$ 39.50	$ 39.50

SERVICES CATALOG

Field Name ==>	Product Name	Unit	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use ==>	*Unique Identifier*	*Unit*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
x86 Virtual Server - Linux - Infrastructure as a Service	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Server	CCSU13340021-A						$ 140.73	$ 140.38	$ 140.03	$ 128.83	$ 113.37	$ 96.36	$ 81.91	$ 81.91	$ 81.91	$ 81.91
x86 Virtual Server - Linux - Infrastructure as a Service	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Server	CCSU13340022-A						$ 67.95	$ 67.78	$ 67.61	$ 62.20	$ 54.73	$ 46.52	$ 39.55	$ 39.55	$ 39.55	$ 39.55
IaaS Storage Configurations																		
Storage - Infrastructure as a Service	SAN attached storage	Per GB	CCSU13340023-A						$ 0.15	$ 0.15	$ 0.14	$ 0.13	$ 0.12	$ 0.10	$ 0.08	$ 0.08	$ 0.08	$ 0.08
Storage - Infrastructure as a Service	Network Attached Storage	Per GB	CCSU13340024-A						$ 0.05	$ 0.06	$ 0.06	$ 0.05	$ 0.05	$ 0.05	$ 0.05	$ 0.05	$ 0.05	$ 0.05
Storage - Infrastructure as a Service	Raid 5	Per GB	CCSU13340025-A						$ 0.05	$ 0.05	$ 0.05	$ 0.05	$ 0.04	$ 0.04	$ 0.04	$ 0.04	$ 0.04	$ 0.04
Storage - Infrastructure as a Service	Raid 10	Per GB	CCSU13340026-A						$ 0.36	$ 0.34	$ 0.32	$ 0.31	$ 0.29	$ 0.28	$ 0.26	$ 0.26	$ 0.26	$ 0.26
Storage - Infrastructure as a Service	10K - 15K RPM discs	Per GB	CCSU13340027-A						$ 0.10	$ 0.10	$ 0.10	$ 0.09	$ 0.08	$ 0.07	$ 0.06	$ 0.06	$ 0.06	$ 0.06
IaaS Backup Configurations																		
Backup - Infrastructure as a Service	Remote Offsite backup per GB	Per GB	CCSU13340028-A						$ 0.02	$ 0.02	$ 0.02	$ 0.02	$ 0.01	$ 0.01	$ 0.01	$ 0.01	$ 0.01	$ 0.01
Reserve Account																		
	Reserve Account - Enterprise Datacenter								$84 000.00	$84 000.00	$84 000.00	$84 000.00	$84 000.00	$84 000.00	$84 000.00	$84 000.00	$84 000.00	$84 000.00
Additional Services																		
Third Party Software																		
B & L	BL/LIB Tape Library Management System	License	CCSU13350001-A			A			$ 1,392.42	$ 1,456.42	$ 1,497.92	$ 1,540.67	$ 1,584.69	$ 1,556.62	$ 1,603.94	$ 1,652.05	$ 1,701.60	$ 1,752.64
B & L	BL/SCHED Scheduling & Monitoring System	License	CCSU13350002-A			A			$ 1,756.92	$ 1,837.68	$ 1,890.04	$ 1,943.98	$ 1,999.53	$ 1,964.11	$ 2,023.81	$ 2,084.52	$ 2,147.04	$ 2,211.44
BMC Software	BMC AppSight for Windows/.NET - Division Edition	License	CCSU13350003-A			A			$ 5,686.25	$ 5,832.36	$ 5,980.83	$ 6,133.75	$ 6,291.26	$ 5,741.12	$ 5,910.50	$ 6,082.62	$ 6,259.90	$ 6,442.49
BMC Software	BMC AppSight Named Users	License	CCSU13350004-A			A			$ 40.62	$ 41.21	$ 41.81	$ 42.42	$ 43.06	$ 24.67	$ 25.36	$ 26.05	$ 26.76	$ 27.50
BMC Software	BMC AppSight QA Users	License	CCSU13350005-A			A			$ 24.65	$ 25.00	$ 25.36	$ 25.73	$ 26.11	$ 15.08	$ 15.49	$ 15.91	$ 16.33	$ 16.77
BMC Software	CONTROL-M Enterprise Manager	License	CCSU13350006-A			A			$ 408.64	$ 417.44	$ 426.39	$ 435.61	$ 445.10	$ 439.02	$ 449.23	$ 459.60	$ 470.28	$ 481.29
BMC Software	CONTROL-M Full Admin User	License	CCSU13350007-A			A			$ 30.76	$ 6.06	$ 6.23	$ 6.40	$ 6.58	$ 6.34	$ 6.54	$ 6.73	$ 6.94	$ 7.14
BMC Software	CONTROL-M Tasks (100 Tasks per Unit)	License	CCSU13350008-A			A			$ 580.77	$ 597.40	$ 614.31	$ 631.73	$ 649.67	$ 638.19	$ 657.47	$ 677.08	$ 697.27	$ 718.07
BMC Software	Database Director (D2)	License	CCSI13350009-A			A			$ 29,304.50	$ 29,304.50	$ 29,304.50	$ 29,304.50	$ 29,304.50	$ 29,304.50	$ 29,304.50	$ 29,304.50	$ 29,304.50	$ 29,304.50
BMC Software	Eclipse iBuild	License	CCSI13350010-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iChange	License	CCSI13350011-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iCheck	License	CCSI13350012-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iCopy	License	CCSI13350013-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iExtract	License	CCSI13350014-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iLM	License	CCSI13350015-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iLoad	License	CCSI13350016-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iRecover	License	CCSI13350017-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iSurvey	License	CCSI13350018-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iUnload	License	CCSI13350019-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Mission Control	License	CCSI13350020-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Business Objects	Crystal Reports	License	CCSU13350021-A			A			$ 11.44	$ 11.73	$ 12.02	$ 12.33	$ 12.64	$ 12.44	$ 12.78	$ 13.12	$ 13.47	$ 13.84
Bytware Inc.	StandGuard Anti-Virus	License	CCSU13350022-A			A			$ 103.79	$ 106.78	$ 109.82	$ 112.96	$ 116.18	$ 114.12	$ 117.59	$ 121.11	$ 124.75	$ 128.49
Citrix	XenApp Advanced (User Counts)	License	CCSU13350023-A			A			$ 4.44	$ 4.54	$ 4.64	$ 4.74	$ 4.85	$ 4.78	$ 4.89	$ 5.01	$ 5.13	$ 5.25
Citrix	XenApp Enterprise (User Counts)	License	CCSU13350024-A			A			$ 5.65	$ 5.77	$ 5.90	$ 6.03	$ 6.17	$ 6.08	$ 6.23	$ 6.38	$ 6.53	$ 6.69
Computer Associates International, Inc.	CA-Explore for CICS	License	CCSI13350025-A			A			$ 759.15	$ 781.93	$ 805.39	$ 829.55	$ 854.43	$ 880.07	$ 906.47	$ 933.67	$ 961.68	$ 990.52
Computer Associates International, Inc.	SOA Security Manager	License	CCSU13350026-A			A			$ 0.47	$ 0.48	$ 0.48	$ 0.49	$ 0.50	$ 0.50	$ 0.51	$ 0.52	$ 0.52	$ 0.54
Computer Associates International, Inc.	SOA Security Manager Additional Secured Web Services	License	CCSU13350027-A			A			$ 99.78	$ 102.13	$ 104.51	$ 106.97	$ 109.50	$ 107.88	$ 110.60	$ 113.37	$ 116.22	$ 119.15
Computer Associates International, Inc.	SOA Security Manager Additional Users	License	CCSU13350028-A			A			$ 0.32	$ 0.33	$ 0.34	$ 0.35	$ 0.36	$ 0.35	$ 0.36	$ 0.37	$ 0.38	$ 0.39
Corticon Technologies	Corticon Business Rules Server – Unlimited CPUs	License	CCSU13350029-A			A			$ 25,207.63	$ 25,735.71	$ 26,272.61	$ 26,825.61	$ 27,395.20	$ 27,030.56	$ 27,642.75	$ 28,265.16	$ 28,906.24	$ 29,566.56
Corticon Technologies	Corticon Server – per Non-Production Server	License	CCSU13350030-A			A			$ 733.13	$ 750.03	$ 767.21	$ 784.90	$ 803.13	$ 791.46	$ 811.05	$ 830.97	$ 851.48	$ 872.61
Corticon Technologies	Corticon Business Rules Modeling Studio – per Named User	License	CCSU13350031-A			A			$ 40.57	$ 41.63	$ 42.70	$ 43.81	$ 44.94	$ 44.22	$ 45.44	$ 46.68	$ 47.97	$ 49.29
CSI International	EPIC	License	CCSI13350032-A			A			$ 2 019.73	$ 2 080.32	$ 2 142.73	$ 2 207.01	$ 2 273.22	$ 2 341.41	$ 2 411.66	$ 2 484.01	$ 2 558.53	$ 2 635.29
CSI International	FAQS/PCS	License	CCSI13350033-A			A			$ 1 228.10	$ 1 264.94	$ 1 302.89	$ 1 341.98	$ 1 382.24	$ 1 423.71	$ 1 466.42	$ 1 510.41	$ 1 555.72	$ 1 602.40
CSI International	FAQS/ASO	License	CCSI13350034-A			A			$ 1 505.59	$ 1 550.76	$ 1 597.29	$ 1 645.20	$ 1 694.56	$ 1 745.40	$ 1 797.76	$ 1 851.70	$ 1 907.24	$ 1 964.46

SERVICES CATALOG

Field Name ==>	Product Name	Unit	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use ==>	*Unique Identifier*	*Unit*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
EMC Corporation	PowerPath	License	CCSU13350035-A			A			$ 2.87	$ 2.95	$ 3.04	$ 3.12	$ 3.21	$ 3.16	$ 3.25	$ 3.35	$ 3.45	$ 3.55
EMC Corporation	PowerPath (per CPU)	License	CCSU13350036-A			A			$ 2.87	$ 2.95	$ 3.04	$ 3.12	$ 3.21	$ 3.16	$ 3.25	$ 3.35	$ 3.45	$ 3.55
EMC Corporation	Symmetrix® VMAX Fully Automated Storage Tiering for Virtual Pools (FAST VP)	License	CCSU13350037-A			A			$ 189.51	$ 194.97	$ 200.53	$ 206.25	$ 212.14	$ 208.37	$ 214.71	$ 221.15	$ 227.78	$ 234.61
EMC Corporation	Vsphere Enterprise Plus	License	CCSU13350038-A			A			$ 73.26	$ 75.37	$ 77.52	$ 79.73	$ 82.01	$ 80.55	$ 83.00	$ 85.49	$ 88.06	$ 90.70
Experian QAS	NameSearch - Production (Licensed per Server up to 8 CPU)	License	CCSU13350039-A			A			$ 6,249.50	$ 6,413.80	$ 6,580.83	$ 6,752.87	$ 6,930.08	$ 6,816.64	$ 7,007.10	$ 7,200.73	$ 7,400.18	$ 7,605.61
Experian QAS	NameSearch - Non-Production (Licensed per Server)	License	CCSU13350040-A			A			$ 938.12	$ 963.06	$ 988.41	$ 1,014.53	$ 1,041.43	$ 1,024.21	$ 1,053.12	$ 1,082.51	$ 1,112.78	$ 1,143.96
Formula Consultants, Inc.	Star 1100	License	CCSU13350041-A			A			$ 197.81	$ 203.51	$ 209.31	$ 215.28	$ 221.43	$ 217.49	$ 224.11	$ 230.83	$ 237.75	$ 244.88
GlobalScape	CuteFTP Pro 2.0	License	CCSU13350042-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
HELPSYS	Robot/Schedule	License	CCSI13350043-A			A			$ 1,457.55	$ 1,501.27	$ 1,546.31	$ 1,592.70	$ 1,640.48	$ 1,689.70	$ 1,740.39	$ 1,792.60	$ 1,846.38	$ 1,901.77
Idea Integration	XGEN	License	CCSU13350044-A			A			$ 3,296.93	$ 3,391.98	$ 3,488.63	$ 3,588.17	$ 3,690.71	$ 3,625.07	$ 3,735.27	$ 3,847.31	$ 3,962.71	$ 4,081.57
Informatica Corporation	SSA-Name 3	License	CCSU13350045-A			A			$ 5,341.99	$ 5,496.02	$ 5,652.61	$ 5,813.90	$ 5,980.03	$ 5,873.68	$ 6,052.24	$ 6,233.77	$ 6,420.75	$ 6,613.34
Infragistics	NetAdvantage for .NET	License	CCSU13350046-A			A			$ 77.88	$ 80.13	$ 82.41	$ 84.76	$ 87.19	$ 85.64	$ 88.24	$ 90.89	$ 93.61	$ 96.42
KMSYS Worldwide, Inc.	IQU Plus-1	License	CCSU13350047-A			A			$ 492.57	$ 506.68	$ 521.00	$ 535.75	$ 550.94	$ 712.23	$ 728.59	$ 745.19	$ 762.28	$ 779.89
Levi, Ray and Shoup	VPS/PCL	License	CCSI13350048-A			A			$ 4 635.90	$ 4 774.98	$ 4 918.23	$ 5 065.77	$ 5 217.75	$ 5 374.27	$ 5 535.51	$ 5 701.57	$ 5 872.62	$ 6 048.80
Levi, Ray and Shoup	VPS/TCP/IP	License	CCSI13350049-A			A			$ 3,262.18	$ 3,360.04	$ 3,460.84	$ 3,564.67	$ 3,671.61	$ 3,781.76	$ 3,895.21	$ 4,012.07	$ 4,132.43	$ 4,256.40
Levi, Ray and Shoup	VPS/DRS	License	CCSI13350050-A			A			$ 1,650.55	$ 1,700.06	$ 1,751.06	$ 1,803.59	$ 1,857.70	$ 1,913.43	$ 1,970.84	$ 2,029.96	$ 2,090.86	$ 2,153.58
Levi, Ray and Shoup	VPS	License	CCSI13350051-A			A			$ 5,107.50	$ 5,260.73	$ 5,418.55	$ 5,581.11	$ 5,748.54	$ 5,921.00	$ 6,098.63	$ 6,281.58	$ 6,470.03	$ 6,664.13
MacKinney Systems, Inc.	CICS Response Time Monitor	License	CCSI13350052-A			A			$ 36.92	$ 38.03	$ 39.16	$ 40.34	$ 41.55	$ 42.80	$ 44.08	$ 45.40	$ 46.77	$ 48.17
Microsoft	BizTalk Adaptor for MQSeries	License	CCSU13350054-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	BizTalk Server Enterprise (Single Processor)	License	CCSU13350055-A			A			$ 1,758.82	$ 1,809.37	$ 1,860.76	$ 1,913.69	$ 1,968.21	$ 1,933.31	$ 1,991.91	$ 2,051.49	$ 2,112.85	$ 2,176.06
Microsoft	BizTalk Server Standard (Single Processor)	License	CCSU13350056-A			A			$ 402.78	$ 414.37	$ 426.15	$ 438.29	$ 450.78	$ 442.78	$ 456.22	$ 469.87	$ 483.94	$ 498.43
Microsoft	SQL Server CAL	License	CCSU13350057-A			A			$ 142.12	$ 146.21	$ 150.38	$ 154.67	$ 159.09	$ 156.26	$ 161.01	$ 165.84	$ 170.81	$ 175.94
Microsoft	SQL Server Enterprise (Single Processor)	License	CCSU13350058-A			A			$ 548.08	$ 563.80	$ 579.77	$ 596.23	$ 613.18	$ 602.33	$ 620.54	$ 639.06	$ 658.14	$ 677.79
Microsoft	SQL Server Enterprise	License	CCSU13350059-A			A			$ 545.48	$ 561.19	$ 577.17	$ 593.62	$ 610.57	$ 599.72	$ 617.94	$ 636.46	$ 655.54	$ 675.19
Microsoft	SQL Server Standard (Single Processor)	License	CCSU13350060-A			A			$ 142.92	$ 147.02	$ 151.18	$ 155.47	$ 159.89	$ 157.06	$ 161.81	$ 166.64	$ 171.62	$ 176.74
Microsoft	SQL Server Standard	License	CCSU13350061-A			A			$ 142.52	$ 146.61	$ 150.78	$ 155.07	$ 159.49	$ 156.66	$ 161.41	$ 166.24	$ 171.22	$ 176.34
Microsoft	SQL Server Standard per 2-Core	License	CCSU13350062-A			A			$ 285.03	$ 293.23	$ 301.56	$ 310.14	$ 318.98	$ 313.32	$ 322.82	$ 332.48	$ 342.43	$ 352.68
Microsoft	Visual Studio Foundation Server	License	CCSU13350063-A			A			$ 15.90	$ 16.33	$ 16.76	$ 17.21	$ 17.68	$ 17.38	$ 17.88	$ 18.38	$ 18.90	$ 19.44
Microsoft	Visual Studio Foundation Server CAL	License	CCSU13350064-A			A			$ 18.29	$ 18.78	$ 19.29	$ 19.80	$ 20.34	$ 19.99	$ 20.57	$ 21.15	$ 21.75	$ 22.37
Microsoft	Visual Studio Professional with MSDN	License	CCSU13350065-A			A			$ 24.65	$ 25.36	$ 26.09	$ 26.83	$ 27.59	$ 27.10	$ 27.93	$ 28.76	$ 29.63	$ 30.51
Microsoft	Windows Server Datacenter Edition (Single Processor)	License	CCSU13350066-A			A			$ 76.99	$ 79.21	$ 81.46	$ 83.79	$ 86.18	$ 84.65	$ 87.22	$ 89.84	$ 92.53	$ 95.31
Microsoft	Windows Server Enterprise Edition	License	CCSU13350067-A			A			$ 55.04	$ 56.63	$ 58.24	$ 59.91	$ 61.62	$ 60.52	$ 62.36	$ 64.23	$ 66.16	$ 68.14
Microsoft	Windows Server Standard Edition	License	CCSU13350068-A			A			$ 14.52	$ 14.94	$ 15.36	$ 15.80	$ 16.25	$ 15.96	$ 16.45	$ 16.94	$ 17.45	$ 17.97
Microsoft	Windows Terminal Service Client Access Licenses	License	CCSU13350069-A			A			$ 4.09	$ 4.21	$ 4.33	$ 4.45	$ 4.58	$ 4.50	$ 4.63	$ 4.77	$ 4.92	$ 5.06
Network Associates	McAfee Anti-Virus	License	CCSU13350070-A			A			$ 0.56	$ 0.57	$ 0.59	$ 0.61	$ 0.62	$ 0.61	$ 0.63	$ 0.65	$ 0.67	$ 0.69
Novell	Platespin Migrator	License	CCSU13350071-A			A			$ 8.25	$ 8.48	$ 8.73	$ 8.97	$ 9.23	$ 9.07	$ 9.34	$ 9.62	$ 9.91	$ 10.21
Novell	SuSE Linux	License	CCSI13350072-A			A			$ 59.13	$ 60.83	$ 62.57	$ 64.35	$ 66.19	$ 65.01	$ 66.99	$ 69.00	$ 71.07	$ 73.20
OpenText	Metastorm Integration Manager for CICS (MIM for CICS)	License	CCSI13350073-A			A			$ 8,752.02	$ 9,014.58	$ 9,285.02	$ 9,563.56	$ 9,850.47	$ 10,145.98	$ 10,450.37	$ 10,763.87	$ 11,086.79	$ 11,419.40
Oracle	Oracle Change Management Pack	License	CCSU13350074-A			A			$ 157.94	$ 161.82	$ 165.75	$ 169.81	$ 173.99	$ 171.31	$ 175.80	$ 180.37	$ 185.07	$ 189.91
Oracle	Oracle Database 10g Enterprise	License	CCSU13350075-A			A			$ 980.51	$ 1,009.92	$ 1,040.22	$ 1,071.42	$ 1,103.57	$ 1,136.67	$ 1,170.77	$ 1,205.89	$ 1,242.07	$ 1,279.33
Oracle	Oracle Database Enterprise Edition	License	CCSU13350076-A			A			$ 613.50	$ 628.83	$ 644.41	$ 660.47	$ 677.00	$ 666.42	$ 684.19	$ 702.25	$ 720.86	$ 740.03
Oracle	Oracle Diagnostic Pack	License	CCSU13350077-A			A			$ 88.86	$ 90.98	$ 93.15	$ 95.38	$ 97.67	$ 97.13	$ 99.60	$ 102.10	$ 104.69	$ 107.35
Oracle	Oracle Enterprise Linux	License	CCSU13350078-A			A			$ 142.35	$ 146.46	$ 150.63	$ 154.93	$ 159.35	$ 156.52	$ 161.28	$ 166.12	$ 171.10	$ 176.23
Oracle	Oracle Exadata Storage Software	License	CCSU13350079-A			A			$ 12 922.64	$ 13 200.97	$ 13 483.95	$ 13 775.41	$ 14 075.62	$ 13 883.43	$ 14 206.09	$ 14 534.14	$ 14 872.03	$ 15 220.05
Oracle	Oracle Partitioning	License	CCSU13350080-A			A			$ 144.57	$ 148.28	$ 152.05	$ 155.94	$ 159.94	$ 157.38	$ 161.68	$ 166.06	$ 170.56	$ 175.20
Oracle	Oracle Tuning Pack	License	CCSU13350081-A			A			$ 98.39	$ 101.03	$ 103.73	$ 106.52	$ 109.38	$ 109.42	$ 112.49	$ 115.62	$ 118.85	$ 122.17
Oracle	Real Application Cluster - Processor Perpetual	License	CCSU13350082-A			A			$ 310.27	$ 317.70	$ 325.24	$ 333.02	$ 341.02	$ 335.90	$ 344.50	$ 353.25	$ 362.26	$ 371.54
Oracle	Spatial and Graph - Processor Perpetual	License	CCSU13350083-A			A			$ 195.87	$ 201.52	$ 207.26	$ 213.18	$ 219.27	$ 215.37	$ 221.92	$ 228.57	$ 235.43	$ 242.49
Pitney Bowes	Finalist (Doc Sense)	License	CCSI13350084-A			A			$ 7,574.99	$ 7,802.24	$ 8,036.30	$ 8,277.39	$ 8,525.71	$ 8,781.49	$ 9,044.93	$ 9,316.27	$ 9,595.77	$ 9,883.64
Pitney Bowes	CODE-1 Plus	License	CCSU13350085-A			A			$ 732.62	$ 753.74	$ 775.22	$ 797.34	$ 820.12	$ 805.53	$ 830.02	$ 854.92	$ 880.56	$ 906.97
Pitney Bowes	CODE-1 Plus (Test / Development)	License	CCSU13350086-A			A			$ 335.78	$ 345.46	$ 355.31	$ 365.45	$ 375.89	$ 369.20	$ 380.43	$ 391.84	$ 403.59	$ 415.70
Pitney Bowes	Online Window for Finalist	License	CCSI13350087-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Quest	Central Performance Suite for SQL Server, Tier A	License	CCSU13350088-A			A			$ 52.03	$ 53.30	$ 54.59	$ 55.93	$ 57.30	$ 56.42	$ 57.89	$ 59.39	$ 60.93	$ 62.52
Quest	Central Performance Suite for SQL Server, Tier B	License	CCSU13350089-A			A			$ 44.10	$ 45.37	$ 46.66	$ 47.99	$ 49.36	$ 48.48	$ 49.95	$ 51.45	$ 53.00	$ 54.58

SERVICES CATALOG

Field Name ==>	Product Name	Unit	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use ==>	*Unique Identifier*	*Unit*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Quest	Foglight Database Management Suite for SQL Server	License	CCSU13350090-A			A			$ 48.85	$ 50.12	$ 51.41	$ 52.74	$ 54.11	$ 53.23	$ 54.71	$ 56.21	$ 57.75	$ 59.34
Quest	Foglight for SQL Server per CPU Socket	License	CCSU13350091-A			A			$ 23.53	$ 24.16	$ 24.81	$ 25.48	$ 26.16	$ 25.72	$ 26.46	$ 27.21	$ 27.98	$ 28.77
Quest	Foglight OS Management per CPU Socket	License	CCSU13350092-A			A			$ 23.39	$ 24.02	$ 24.67	$ 25.33	$ 26.02	$ 25.58	$ 26.32	$ 27.07	$ 27.84	$ 28.63
Quest	Foglight Server for FSM	License	CCSU13350093-A			A			$ 26.02	$ 26.65	$ 27.30	$ 27.96	$ 28.65	$ 28.21	$ 28.95	$ 29.69	$ 30.47	$ 31.26
RealVNC	VNC Enterprise Edition for Windows	License	CCSU13350094-A			A			$ 1.18	$ 1.21	$ 1.24	$ 1.28	$ 1.32	$ 1.29	$ 1.33	$ 1.37	$ 1.41	$ 1.45
Red Hat	Red Hat Enterprise Linux	License	CCSU13350095-A			A			$ 319.56	$ 328.77	$ 338.14	$ 347.79	$ 357.72	$ 351.36	$ 362.04	$ 372.90	$ 384.09	$ 395.61
Segus Inc.	OPC/Graph	License	CCSI13350097-A			A			$ 735.01	$ 757.06	$ 779.78	$ 803.17	$ 827.27	$ 852.08	$ 877.65	$ 903.98	$ 931.09	$ 959.03
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG20	License	CCSU13350098-A			A			$ 58.70	$ 60.35	$ 62.00	$ 63.71	$ 65.47	$ 151.73	$ 153.64	$ 155.57	$ 157.55	$ 159.59
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG40	License	CCSU13350099-A			A			$ 72.13	$ 74.16	$ 76.22	$ 78.33	$ 80.51	$ 166.50	$ 168.86	$ 171.24	$ 173.69	$ 176.21
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG60	License	CCSU13350100-A			A			$ 85.97	$ 88.40	$ 90.86	$ 93.39	$ 96.00	$ 181.72	$ 184.54	$ 187.39	$ 190.32	$ 193.35
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG80	License	CCSU13350101-A			A			$ 99.40	$ 102.22	$ 105.07	$ 108.01	$ 111.04	$ 196.48	$ 199.75	$ 203.06	$ 206.47	$ 209.97
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG130	License	CCSU13350102-A			A			$ 137.25	$ 141.16	$ 145.12	$ 149.21	$ 153.41	$ 238.10	$ 242.64	$ 247.23	$ 251.96	$ 256.83
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG20	License	CCSU13350103-A			A			$ 58.70	$ 60.35	$ 62.00	$ 63.71	$ 65.47	$ 151.73	$ 153.64	$ 155.57	$ 157.55	$ 159.59
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG40	License	CCSU13350104-A			A			$ 72.13	$ 74.16	$ 76.22	$ 78.33	$ 80.51	$ 166.50	$ 168.86	$ 171.24	$ 173.69	$ 176.21
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG60	License	CCSU13350105-A			A			$ 85.97	$ 88.40	$ 90.86	$ 93.39	$ 96.00	$ 181.72	$ 184.54	$ 187.39	$ 190.32	$ 193.35
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG80	License	CCSU13350106-A			A			$ 99.40	$ 102.22	$ 105.07	$ 108.01	$ 111.04	$ 196.48	$ 199.75	$ 203.06	$ 206.47	$ 209.97
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG130	License	CCSU13350107-A			A			$ 137.25	$ 141.16	$ 145.12	$ 149.21	$ 153.41	$ 238.10	$ 242.64	$ 247.23	$ 251.96	$ 256.83
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG140	License	CCSU13350108-A			A			$ 157.60	$ 162.10	$ 166.66	$ 171.35	$ 176.19	$ 260.48	$ 265.69	$ 270.98	$ 276.42	$ 282.03
Sightline	OS 2200 Interface Agent - MAPPER, SWG20	License	CCSU13350109-A			A			$ 58.70	$ 60.35	$ 62.00	$ 63.71	$ 65.47	$ 151.73	$ 153.64	$ 155.57	$ 157.55	$ 159.59
Sightline	OS 2200 Interface Agent - MAPPER, SWG40	License	CCSU13350110-A			A			$ 72.13	$ 74.16	$ 76.22	$ 78.33	$ 80.51	$ 166.50	$ 168.86	$ 171.24	$ 173.69	$ 176.21
Sightline	OS 2200 Interface Agent - MAPPER, SWG60	License	CCSU13350111-A			A			$ 85.97	$ 88.40	$ 90.86	$ 93.39	$ 96.00	$ 181.72	$ 184.54	$ 187.39	$ 190.32	$ 193.35
Sightline	OS 2200 Interface Agent - MAPPER, SWG80	License	CCSU13350112-A			A			$ 99.40	$ 102.22	$ 105.07	$ 108.01	$ 111.04	$ 196.48	$ 199.75	$ 203.06	$ 206.47	$ 209.97
Sightline	OS 2200 Interface Agent - MAPPER, SWG130	License	CCSU13350113-A			A			$ 137.25	$ 141.16	$ 145.12	$ 149.21	$ 153.41	$ 238.10	$ 242.64	$ 247.23	$ 251.96	$ 256.83
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG20	License	CCSU13350114-A			A			$ 59.72	$ 61.39	$ 63.08	$ 64.82	$ 66.61	$ 152.85	$ 154.79	$ 156.75	$ 158.77	$ 160.85
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG40	License	CCSU13350115-A			A			$ 72.13	$ 74.16	$ 76.22	$ 78.33	$ 80.51	$ 166.50	$ 168.86	$ 171.24	$ 173.69	$ 176.21
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG60	License	CCSU13350116-A			A			$ 85.97	$ 88.40	$ 90.86	$ 93.39	$ 96.00	$ 181.72	$ 184.54	$ 187.39	$ 190.32	$ 193.35
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG80	License	CCSU13350117-A			A			$ 99.40	$ 102.22	$ 105.07	$ 108.01	$ 111.04	$ 196.48	$ 199.75	$ 203.06	$ 206.47	$ 209.97
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG130	License	CCSU13350118-A			A			$ 137.25	$ 141.16	$ 145.12	$ 149.21	$ 153.41	$ 238.10	$ 242.64	$ 247.23	$ 251.96	$ 256.83
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG140	License	CCSU13350119-A			A			$ 157.60	$ 162.10	$ 166.66	$ 171.35	$ 176.19	$ 260.48	$ 265.69	$ 270.98	$ 276.42	$ 282.03
Sightline	OS 2200 Interface Agent - System Log, SWG20	License	CCSU13350120-A			A			$ 58.70	$ 60.35	$ 62.00	$ 63.71	$ 65.47	$ 151.73	$ 153.64	$ 155.57	$ 157.55	$ 159.59
Sightline	OS 2200 Interface Agent - System Log, SWG40	License	CCSU13350121-A			A			$ 72.13	$ 74.16	$ 76.22	$ 78.33	$ 80.51	$ 166.50	$ 168.86	$ 171.24	$ 173.69	$ 176.21
Sightline	OS 2200 Interface Agent - System Log, SWG60	License	CCSU13350122-A			A			$ 85.97	$ 88.40	$ 90.86	$ 93.39	$ 96.00	$ 181.72	$ 184.54	$ 187.39	$ 190.32	$ 193.35
Sightline	OS 2200 Interface Agent - System Log, SWG80	License	CCSU13350123-A			A			$ 99.40	$ 102.22	$ 105.07	$ 108.01	$ 111.04	$ 196.48	$ 199.75	$ 203.06	$ 206.47	$ 209.97
Sightline	OS 2200 Interface Agent - System Log, SWG130	License	CCSU13350124-A			A			$ 137.25	$ 141.16	$ 145.12	$ 149.21	$ 153.41	$ 238.10	$ 242.64	$ 247.23	$ 251.96	$ 256.83
Sightline	OS 2200 Interface Agent - System Log, SWG140	License	CCSU13350125-A			A			$ 157.60	$ 162.10	$ 166.66	$ 171.35	$ 176.19	$ 260.48	$ 265.69	$ 270.98	$ 276.42	$ 282.03
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG20	License	CCSU13350126-A			A			$ 58.70	$ 60.35	$ 62.00	$ 63.71	$ 65.47	$ 151.73	$ 153.64	$ 155.57	$ 157.55	$ 159.59
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG40	License	CCSU13350127-A			A			$ 72.13	$ 74.16	$ 76.22	$ 78.33	$ 80.51	$ 166.50	$ 168.86	$ 171.24	$ 173.69	$ 176.21
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG60	License	CCSU13350128-A			A			$ 85.97	$ 88.40	$ 90.86	$ 93.39	$ 96.00	$ 181.72	$ 184.54	$ 187.39	$ 190.32	$ 193.35
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG80	License	CCSU13350129-A			A			$ 99.40	$ 102.22	$ 105.07	$ 108.01	$ 111.04	$ 196.48	$ 199.75	$ 203.06	$ 206.47	$ 209.97

SERVICES CATALOG

Field Name ==>	Product Name	Unit	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use ==>	*Unique Identifier*	*Unit*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG130	License	CCSU13350130-A			A			$ 137.25	$ 141.16	$ 145.12	$ 149.21	$ 153.41	$ 238.10	$ 242.64	$ 247.23	$ 251.96	$ 256.83
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG140	License	CCSU13350131-A			A			$ 157.60	$ 162.10	$ 166.66	$ 171.35	$ 176.19	$ 260.48	$ 265.69	$ 270.98	$ 276.42	$ 282.03
Sightline	OS 2200 Power Agent, SWG20	License	CCSU13350132-A			A			$ 115.27	$ 118.55	$ 121.87	$ 125.29	$ 128.80	$ 213.94	$ 217.74	$ 221.58	$ 225.54	$ 229.62
Sightline	OS 2200 Power Agent, SWG40	License	CCSU13350133-A			A			$ 142.14	$ 146.19	$ 150.29	$ 154.52	$ 158.88	$ 243.47	$ 248.17	$ 252.93	$ 257.83	$ 262.88
Sightline	OS 2200 Power Agent, SWG60	License	CCSU13350134-A			A			$ 169.81	$ 174.66	$ 179.58	$ 184.64	$ 189.86	$ 273.91	$ 279.53	$ 285.23	$ 291.10	$ 297.14
Sightline	OS 2200 Power Agent, SWG80	License	CCSU13350135-A			A			$ 196.67	$ 202.30	$ 208.00	$ 213.88	$ 219.93	$ 303.44	$ 309.96	$ 316.57	$ 323.38	$ 330.40
Sightline	OS 2200 Power Agent, SWG130	License	CCSU13350136-A			A			$ 272.38	$ 280.19	$ 288.11	$ 296.27	$ 304.67	$ 386.68	$ 395.73	$ 404.92	$ 414.38	$ 424.12
Sightline	OS 2200 Power Agent, SWG140	License	CCSU13350137-A			A			$ 313.08	$ 322.06	$ 331.18	$ 340.57	$ 350.24	$ 431.43	$ 441.84	$ 452.41	$ 463.30	$ 474.51
Sightline	OS 2200 Torch Capacity Manager Power Agent, SWG40	License	CCSU13350138-A			A			$ 576.01	$ 592.57	$ 609.39	$ 626.72	$ 644.57	$ 720.53	$ 739.73	$ 759.23	$ 779.32	$ 800.01
Sightline	OS 2200 Torch Capacity Manager Power Agent, SWG60	License	CCSU13350139-A			A			$ 660.26	$ 679.25	$ 698.54	$ 718.41	$ 738.88	$ 813.17	$ 835.18	$ 857.55	$ 880.58	$ 904.31
Sightline	OS 2200 Torch Capacity Manager Power Agent, SWG130	License	CCSU13350140-A			A			$ 1,044.47	$ 1,074.54	$ 1,105.10	$ 1,136.57	$ 1,168.99	$ 1,235.62	$ 1,270.48	$ 1,305.90	$ 1,342.39	$ 1,379.97
Sightline	OS 2200 Torch Capacity Manager Power Agent, SWG140	License	CCSU13350141-A			A			$ 1,198.32	$ 1,232.83	$ 1,267.89	$ 1,304.01	$ 1,341.21	$ 1,404.78	$ 1,444.79	$ 1,485.44	$ 1,527.31	$ 1,570.43
Sightline	OS 2200 Torch Interface Agent - I/O TRACE, SWG40	License	CCSU13350142-A			A			$ 241.45	$ 248.36	$ 255.38	$ 262.60	$ 270.05	$ 352.67	$ 360.69	$ 368.82	$ 377.20	$ 385.83
Sightline	OS 2200 Torch Interface Agent - I/O TRACE, SWG60	License	CCSU13350143-A			A			$ 292.73	$ 301.12	$ 309.64	$ 318.42	$ 327.46	$ 409.06	$ 418.79	$ 428.66	$ 438.84	$ 449.31
Sightline	OS 2200 Torch Interface Agent - I/O TRACE, SWG130	License	CCSU13350144-A			A			$ 484.84	$ 498.77	$ 512.92	$ 527.50	$ 542.51	$ 620.28	$ 636.44	$ 652.84	$ 669.74	$ 687.14
Sightline	OS 2200 Torch Interface Agent - LOG, SWG40	License	CCSU13350145-A			A			$ 241.45	$ 248.36	$ 255.38	$ 262.60	$ 270.05	$ 352.67	$ 360.69	$ 368.82	$ 377.20	$ 385.83
Sightline	OS 2200 Torch Interface Agent - LOG, SWG60	License	CCSU13350146-A			A			$ 292.73	$ 301.12	$ 309.64	$ 318.42	$ 327.46	$ 409.06	$ 418.79	$ 428.66	$ 438.84	$ 449.31
Sightline	OS 2200 Torch Interface Agent - LOG, SWG130	License	CCSU13350147-A			A			$ 484.84	$ 498.77	$ 512.92	$ 527.50	$ 542.51	$ 620.28	$ 636.44	$ 652.84	$ 669.74	$ 687.14
Sightline	OS 2200 Torch Interface Agent - LOG, SWG140	License	CCSU13350148-A			A			$ 561.76	$ 577.91	$ 594.32	$ 611.22	$ 628.62	$ 704.87	$ 723.59	$ 742.61	$ 762.20	$ 782.37
Sightline	OS 2200 Torch Interface Agent - MAPPER, SWG40	License	CCSU13350149-A			A			$ 241.45	$ 248.36	$ 255.38	$ 262.60	$ 270.05	$ 352.67	$ 360.69	$ 368.82	$ 377.20	$ 385.83
Sightline	OS 2200 Torch Interface Agent - MAPPER, SWG60	License	CCSU13350150-A			A			$ 292.73	$ 301.12	$ 309.64	$ 318.42	$ 327.46	$ 409.06	$ 418.79	$ 428.66	$ 438.84	$ 449.31
Sightline	OS 2200 Torch Interface Agent - MAPPER, SWG130	License	CCSU13350151-A			A			$ 484.84	$ 498.77	$ 512.92	$ 527.50	$ 542.51	$ 620.28	$ 636.44	$ 652.84	$ 669.74	$ 687.14
Sightline	Windows 2000 Interface Agent - Internet Information Server	License	CCSU13350152-A			A			$ 24.72	$ 25.43	$ 26.15	$ 26.88	$ 27.64	$ 39.64	$ 40.46	$ 41.29	$ 42.14	$ 43.02
Sightline	Windows 2000 Interface Agent - .NET	License	CCSU13350153-A			A			$ 49.14	$ 50.56	$ 51.99	$ 53.46	$ 54.98	$ 66.49	$ 68.13	$ 69.79	$ 71.50	$ 73.26
Sightline	Windows 2000 Interface Agent - SQL Server	License	CCSU13350154-A			A			$ 81.93	$ 84.28	$ 86.67	$ 89.13	$ 91.66	$ 111.89	$ 114.61	$ 117.38	$ 120.23	$ 123.16
Sightline	Windows 2000 Power Agent Upto 32 CPU's	License	CCSU13350155-A			A			$ 269.33	$ 277.08	$ 284.96	$ 293.07	$ 301.42	$ 325.20	$ 334.19	$ 343.32	$ 352.72	$ 362.41
SMA	OpCon/xps EXEC LSAM, Group 3	License	CCSU13350156-A			A			$ 354.87	$ 363.36	$ 371.98	$ 380.85	$ 389.99	$ 379.97	$ 389.81	$ 399.80	$ 410.09	$ 420.68
SMA	OpCon/xps EXEC LSAM, Group 12	License	CCSU13350157-A			A			$ 2,159.97	$ 2,211.78	$ 2,264.38	$ 2,318.56	$ 2,374.36	$ 2,029.78	$ 2,089.84	$ 2,150.82	$ 2,213.63	$ 2,278.32
SMA	OpCon/xps EXEC LSAM Development, Group 2	License	CCSU13350158-A			A			$ 197.99	$ 103.21	$ 106.10	$ 109.07	$ 112.14	$ 165.19	$ 168.50	$ 171.85	$ 175.30	$ 178.85
SMA	OpCon/xps EXEC LSAM Development, Group 12	License	CCSU13350159-A			A			$ 1,080.61	$ 1,106.51	$ 1,132.81	$ 1,159.90	$ 1,187.80	$ 1,043.27	$ 1,073.31	$ 1,103.79	$ 1,135.20	$ 1,167.54
SMA	OpCon/xps Production SAM	License	CCSU13350160-A			A			$ 378.50	$ 387.58	$ 396.80	$ 406.30	$ 416.09	$ 345.94	$ 356.46	$ 367.16	$ 378.17	$ 389.51
SMA	OpCon/xps Starter Kit	License	CCSU13350161-A			A			$ 648.47	$ 664.03	$ 679.83	$ 696.11	$ 712.87	$ 592.68	$ 610.72	$ 629.04	$ 647.91	$ 667.34
SMA	OpCon/xps User Interface	License	CCSU13350162-A			A			$ 9.90	$ 5.13	$ 5.28	$ 5.43	$ 5.58	$ 5.46	$ 5.62	$ 5.79	$ 5.97	$ 6.14
Sybase	EAServer Deploy Advanced - Active	License	CCSU13350163-A			A			$ 149.21	$ 153.51	$ 157.89	$ 162.39	$ 167.03	$ 164.06	$ 169.05	$ 174.12	$ 179.34	$ 184.72
Sybase	EAServer Deploy Advanced - Passive	License	CCSU13350164-A			A			$ 37.36	$ 38.43	$ 39.53	$ 40.66	$ 41.82	$ 41.07	$ 42.32	$ 43.59	$ 44.90	$ 46.25
Symantec	Backup Exec System Recovery Server	License	CCSU13350165-A			A			$ 0.97	$ 1.00	$ 1.03	$ 1.05	$ 1.08	$ 1.07	$ 1.10	$ 1.13	$ 1.16	$ 1.20
Symantec	EndPoint Protection	License	CCSU13350166-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	Ghost Solution Suite	License	CCSU13350167-A			A			$ 0.66	$ 0.68	$ 0.69	$ 0.71	$ 0.73	$ 0.72	$ 0.74	$ 0.77	$ 0.79	$ 0.81
Symantec	NetBackup Client Application and Database Pack, UNX, Tier 3	License	CCSU13350168-A			A			$ 0.60	$ 0.62	$ 0.63	$ 0.65	$ 0.67	$ 0.66	$ 0.68	$ 0.70	$ 0.72	$ 0.74
Symantec	NetBackup Client Application and Database Pack, UNX, Tier 4	License	CCSU13350169-A			A			$ 174.97	$ 180.02	$ 185.15	$ 190.43	$ 195.87	$ 192.39	$ 198.24	$ 204.18	$ 210.31	$ 216.62
Symantec	NetBackup Client Application and Database Pack, WIN, Tier 2	License	CCSU13350170-A			A			$ 26.97	$ 27.75	$ 28.54	$ 29.36	$ 30.20	$ 29.66	$ 30.56	$ 31.48	$ 32.42	$ 33.39
Symantec	NetBackup Client Application and Database Pack, WIN, Tier 3	License	CCSU13350171-A			A			$ 34.93	$ 35.94	$ 36.96	$ 38.02	$ 39.10	$ 38.41	$ 39.58	$ 40.76	$ 41.99	$ 43.24
Symantec	NetBackup Client Application and Database Pack, WIN, Tier 4	License	CCSU13350172-A			A			$ 52.44	$ 53.95	$ 55.49	$ 57.07	$ 58.70	$ 57.66	$ 59.41	$ 61.19	$ 63.03	$ 64.92
Symantec	NetBackup Enterprise Client, UNX, Tier 4	License	CCSU13350173-A			A			$ 216.35	$ 222.59	$ 228.93	$ 235.46	$ 242.19	$ 237.88	$ 245.12	$ 252.47	$ 260.04	$ 267.84
Symantec	NetBackup Enterprise Client, WIN, Tier 1	License	CCSU13350174-A			A			$ 41.30	$ 42.49	$ 43.70	$ 44.95	$ 46.23	$ 45.41	$ 46.79	$ 48.19	$ 49.64	$ 51.13

SERVICES CATALOG

Field Name ==>	Product Name	Unit	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use ==>	*Unique Identifier*	*Unit*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Symantec	NetBackup Enterprise Client, WIN, Tier 2	License	CCSU13350175-A			A			$ 49.25	$ 50.67	$ 52.12	$ 53.61	$ 55.14	$ 54.16	$ 55.80	$ 57.48	$ 59.20	$ 60.98
Symantec	NetBackup Enterprise Client, WIN, Tier 3	License	CCSU13350176-A			A			$ 65.17	$ 67.05	$ 68.96	$ 70.92	$ 72.95	$ 71.65	$ 73.83	$ 76.05	$ 78.33	$ 80.68
Symantec	NetBackup Enterprise Server, WIN, Tier 2	License	CCSU13350177-A			A			$ 87.53	$ 90.05	$ 92.62	$ 95.26	$ 97.98	$ 96.24	$ 99.16	$ 102.14	$ 105.20	$ 108.36
Symantec	NetBackup Enterprise Server, WIN, Tier 3	License	CCSU13350178-A			A			$ 127.31	$ 130.98	$ 134.72	$ 138.56	$ 142.52	$ 139.98	$ 144.24	$ 148.57	$ 153.02	$ 157.61
Symantec	NetBackup Library Based Tape Drive Option, XPLAT	License	CCSU13350179-A			A			$ 47.74	$ 49.12	$ 50.52	$ 51.96	$ 53.44	$ 52.49	$ 54.09	$ 55.71	$ 57.38	$ 59.10
Symantec	NetBackup Media Server Encryption Option (MSEO) WIN, Tier 2	License	CCSU13350180-A			A			$ 87.53	$ 90.05	$ 92.62	$ 95.26	$ 97.98	$ 96.24	$ 99.16	$ 102.14	$ 105.20	$ 108.36
Symantec	NetBackup Platform Base, XPLAT (per Terabyte)	License	CCSU13350181-A			A			$ 198.93	$ 204.66	$ 210.49	$ 216.50	$ 222.69	$ 218.72	$ 225.37	$ 232.13	$ 239.10	$ 246.27
Symantec	NetBackup Shared Storage Option, XPLAT	License	CCSU13350182-A			A			$ 31.83	$ 32.75	$ 33.68	$ 34.64	$ 35.63	$ 35.00	$ 36.06	$ 37.14	$ 38.26	$ 39.40
Symantec	NetBackup Standard Client, XPLAT	License	CCSU13350183-A			A			$ 9.47	$ 9.74	$ 10.02	$ 10.31	$ 10.60	$ 10.41	$ 10.73	$ 11.05	$ 11.38	$ 11.72
Symantec	NetBackup Vault Additional Drive Option, XPLAT	License	CCSU13350184-A			A			$ 31.83	$ 32.75	$ 33.68	$ 34.64	$ 35.63	$ 35.00	$ 36.06	$ 37.14	$ 38.26	$ 39.40
Symantec	NetBackup Vault Base Option, XPLAT (4 tape drives per license)	License	CCSU13350185-A			A			$ 159.14	$ 163.73	$ 168.39	$ 173.20	$ 178.15	$ 174.98	$ 180.30	$ 185.71	$ 191.28	$ 197.01
Symantec	Veritas NetBackup Enterprise Server License, Tier 3	License	CCSU13350186-A			A			$ 127.31	$ 130.98	$ 134.72	$ 138.56	$ 142.52	$ 139.98	$ 144.24	$ 148.57	$ 153.02	$ 157.61
Symantec	Veritas NetBackup Windows Client, Tier 4	License	CCSU13350187-A			A			$ 52.44	$ 53.95	$ 55.49	$ 57.07	$ 58.70	$ 57.66	$ 59.41	$ 61.19	$ 63.03	$ 64.92
Tone Software Corp.	Dynastep	License	CCSU13350188-A			A			$ 1,469.71	$ 1,512.08	$ 1,555.17	$ 1,599.54	$ 1,645.25	$ 1,615.99	$ 1,665.11	$ 1,715.06	$ 1,766.50	$ 1,819.49
Unicon Group Ltd.	LOUIS II LCOM Host Module	License	CCSU13350189-A			A			$ 55.56	$ 57.16	$ 58.79	$ 60.46	$ 62.19	$ 61.09	$ 62.94	$ 64.83	$ 66.78	$ 68.78
Unicon Group Ltd.	LOUIS II Extract & Reporting Module	License	CCSU13350190-A			A			$ 892.57	$ 918.31	$ 944.47	$ 971.42	$ 999.18	$ 981.41	$ 1,011.24	$ 1,041.57	$ 1,072.82	$ 1,105.00
Unicon Group Ltd.	LOUIS II DERIVE Option	License	CCSU13350191-A			A			$ 62.37	$ 64.17	$ 66.00	$ 67.88	$ 69.82	$ 68.58	$ 70.67	$ 72.79	$ 74.97	$ 77.22
Unicon Group Ltd.	LOUIS II DMS Interface	License	CCSU13350192-A			A			$ 111.11	$ 114.32	$ 117.57	$ 120.93	$ 124.38	$ 122.17	$ 125.89	$ 129.66	$ 133.55	$ 137.56
Unicon Group Ltd.	LOUIS II RDMS Interface	License	CCSU13350193-A			A			$ 111.11	$ 114.32	$ 117.57	$ 120.93	$ 124.38	$ 122.17	$ 125.89	$ 129.66	$ 133.55	$ 137.56
Unicon Group Ltd.	LOUIS II RELATE Option	License	CCSU13350194-A			A			$ 89.03	$ 91.60	$ 94.21	$ 96.90	$ 99.67	$ 97.89	$ 100.87	$ 103.90	$ 107.01	$ 110.22
VanDyke Technologies	VShell Workgroup Server	License	CCSU13350195-A			A			$ 9.75	$ 10.03	$ 10.31	$ 10.61	$ 10.91	$ 10.72	$ 11.04	$ 11.38	$ 11.72	$ 12.07
Veeam	nWorks ESX Monitoring for SCOM	License	CCSU13350196-A			A			$ 12.88	$ 13.25	$ 13.63	$ 14.02	$ 14.42	$ 14.16	$ 14.59	$ 15.03	$ 15.48	$ 15.95
Veeam	nWorks Management Pack for VMWare	License	CCSU13350197-A			A			$ 12.88	$ 13.25	$ 13.63	$ 14.02	$ 14.42	$ 14.16	$ 14.59	$ 15.03	$ 15.48	$ 15.95
VMware, Inc.	VMware vSphere 4 Enterprise Plus for 1 Processor	License	CCSU13350198-A			A			$ 73.26	$ 75.37	$ 77.52	$ 79.73	$ 82.01	$ 80.55	$ 83.00	$ 85.49	$ 88.06	$ 90.70
VMware, Inc.	VMware vSphere 5 Enterprise Plus for 1 Processor	License	CCSU13350199-A			A			$ 73.26	$ 75.37	$ 77.52	$ 79.73	$ 82.01	$ 80.55	$ 83.00	$ 85.49	$ 88.06	$ 90.70
Winternals	Winternals Administrator's Pak	License	CCSU13350201-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
WinZip Computing	Winzip	License	CCSU13350202-A			A			$ 0.26	$ 0.26	$ 0.27	$ 0.28	$ 0.29	$ 0.28	$ 0.29	$ 0.30	$ 0.31	$ 0.32
XtremeSoft	AppMetrics	License	CCSU13350203-A			A			$ 1,373.66	$ 1,413.26	$ 1,453.53	$ 1,495.00	$ 1,537.72	$ 1,510.37	$ 1,556.29	$ 1,602.97	$ 1,651.05	$ 1,700.57
USPS	Correct Address	License	CCSU13350204-A			A			$ 997.17	$ 1,025.92	$ 1,055.15	$ 1,085.26	$ 1,116.27	$ 1,096.42	$ 1,129.75	$ 1,163.64	$ 1,198.54	$ 1,234.49
IBM	FileNet	License	CCSU13350205-A			A			$ 77.94	$ 15.35	$ 15.78	$ 16.22	$ 16.68	$ 16.07	$ 16.57	$ 17.06	$ 17.57	$ 18.10
Microsoft	SharePoint (with SA)	License	CCSU13350206-A			A			$ 909.08	$ 935.29	$ 961.94	$ 989.39	$ 1,017.66	$ 999.56	$ 1,029.95	$ 1,060.84	$ 1,092.66	$ 1,125.43
IBM	WebSphere MQ (Procesor Value Unit)	License	CCSU13350207-A			A			$ 13.38	$ 2.63	$ 2.71	$ 2.78	$ 2.86	$ 2.76	$ 2.84	$ 2.93	$ 3.02	$ 3.11
Xerox	XeroxDocuShare	License	CCSU13350208-A			A			$ 65.12	$ 66.22	$ 67.34	$ 68.49	$ 69.68	$ 41.96	$ 43.24	$ 44.54	$ 45.87	$ 47.25
Hybrid Third Party Software																		
Vendor	**Product**																	
Computer Associates International, Inc.	CA 90's Services (freeware)	License	CCSI13350209-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	Vision Bu lder	License	CCSI13350210-A			A			$ 23,918.41	$ 24,635.97	$ 25,375.04	$ 26,136.30	$ 26,920.38	$ 27,728.00	$ 28,559.83	$ 29,416.63	$ 30,299.13	$ 31,208.10
Computer Associates International, Inc.	Easytrieve Plus	License	CCSI13350211-A			A			$ 11,718.82	$ 12,070.38	$ 12,432.49	$ 12,805.47	$ 13,189.64	$ 13,585.32	$ 13,992.88	$ 14,412.66	$ 14,845.04	$ 15,290.39
Computer Associates International, Inc.	Easytrieve Plus MVS	License	CCSI13350212-A			A			$ 6,061.27	$ 6,243.10	$ 6,430.39	$ 6,623.31	$ 6,822.00	$ 7,026.67	$ 7,237.47	$ 7,454.60	$ 7,678.23	$ 7,908.58
Computer Associates International, Inc.	Easytrieve Plus IMS	License	CCSI13350213-A			A			$ 3,667.89	$ 3,777.92	$ 3,891.26	$ 4,007.99	$ 4,128.23	$ 4,252.08	$ 4,379.64	$ 4,511.03	$ 4,646.37	$ 4,785.75
Computer Associates International, Inc.	Easytrieve Plus IMS Option MVS	License	CCSI13350214-A			A			$ 1,897.06	$ 1,953.98	$ 2,012.59	$ 2,072.98	$ 2,135.17	$ 2,199.22	$ 2,265.19	$ 2,333.15	$ 2,403.14	$ 2,475.24
Computer Associates International, Inc.	Easytrieve Plus DB2 OPT	License	CCSI13350215-A			A			$ 5,523.37	$ 5,689.07	$ 5,859.73	$ 6,035.53	$ 6,216.60	$ 6,403.10	$ 6,595.18	$ 6,793.04	$ 6,996.83	$ 7,206.74
Computer Associates International, Inc.	Easytrieve Plus DB2 Option MVS	License	CCSI13350216-A			A			$ 2 856.79	$ 2 942.49	$ 3 030.77	$ 3 121.70	$ 3 215.35	$ 3 311.80	$ 3 411.16	$ 3 513.49	$ 3 618.90	$ 3 727.46
Computer Associates International, Inc.	Endevor/MVS Automated Configuration Mgr MVS	License	CCSI13350217-A			A			$ 1,401.59	$ 1,443.63	$ 1,486.95	$ 1,531.55	$ 1,577.49	$ 1,624.82	$ 1,673.56	$ 1,723.77	$ 1,775.48	$ 1,828.74
Computer Associates International, Inc.	Endevor/MVS External Security Int. MVS	License	CCSI13350218-A			A			$ 451.53	$ 465.08	$ 479.03	$ 493.40	$ 508.20	$ 523.45	$ 539.15	$ 555.33	$ 571.99	$ 589.15
Computer Associates International, Inc.	Endevor/MVS MVS	License	CCSI13350219-A			A			$ 4 275.18	$ 4 403.43	$ 4 535.53	$ 4 671.61	$ 4 811.75	$ 4 956.10	$ 5 104.79	$ 5 257.93	$ 5 415.67	$ 5 578.13
Computer Associates International, Inc.	Endevor/MVS Extended Processor	License	CCSI13350220-A			A			$ 2 304.84	$ 2 373.99	$ 2 445.21	$ 2 518.56	$ 2 594.11	$ 2 671.93	$ 2 752.10	$ 2 834.67	$ 2 919.70	$ 3 007.30
Computer Associates International, Inc.	CA-Librarian	License	CCSI13350221-A			A			$ 18,144.81	$ 18,689.16	$ 19,249.84	$ 19,827.33	$ 20,422.15	$ 21,034.81	$ 21,665.85	$ 22,315.84	$ 22,985.31	$ 23,674.87
Computer Associates International, Inc.	CA-META COBOL	License	CCSI13350222-A			A			$ 10,617.01	$ 10,935.52	$ 11,263.58	$ 11,601.49	$ 11,949.54	$ 12,308.03	$ 12,677.27	$ 13,057.58	$ 13,449.31	$ 13,852.79
Computer Associates International, Inc.	Panvalet	License	CCSI13350223-A			A			$ 8,352.61	$ 8,603.19	$ 8,861.29	$ 9,127.13	$ 9,400.95	$ 9,682.96	$ 9,973.46	$ 10,272.67	$ 10,580.84	$ 10,898.27
Computer Associates International, Inc.	Panvalet ISPF	License	CCSI13350224-A			A			$ 5,011.96	$ 5,162.31	$ 5,317.18	$ 5,476.70	$ 5,641.00	$ 5,810.22	$ 5,984.53	$ 6,164.08	$ 6,348.99	$ 6,539.47
Computer Associates International, Inc.	SORT (INCL DART)	License	CCSI13350225-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	SRAM	License	CCSI13350226-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -

SERVICES CATALOG

Field Name ==>	Product Name	Unit	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use ==>	*Unique Identifier*	*Unit*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
dotJ Software Inc.	dotJ Custom Tag Library	License	CCSU13350227-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Formula Consultants, Inc.	Star 1100	License	CCSU13350228-A			A			$ 197.81	$ 203.51	$ 209.31	$ 215.28	$ 221.43	$ 217.49	$ 224.11	$ 230.83	$ 237.75	$ 244.88
Idea Integration	XGEN	License	CCSU13350229-A			A			$ 3,296.93	$ 3,391.98	$ 3,488.63	$ 3,588.17	$ 3,690.71	$ 3,625.07	$ 3,735.27	$ 3,847.31	$ 3,962.71	$ 4,081.57
Informatica Corporation	Change DataMove for DB2 Source	License	CCSI13350230-A			A			$ 435.93	$ 449.02	$ 462.48	$ 476.36	$ 490.65	$ 505.38	$ 520.54	$ 536.15	$ 552.23	$ 568.80
Informatica Corporation	DataMove for DB2 Source	License	CCSI13350231-A			A			$ 87.84	$ 90.47	$ 93.18	$ 95.98	$ 98.86	$ 101.82	$ 104.88	$ 108.03	$ 111.27	$ 114.61
Informatica Corporation	Change DataMove	License	CCSI13350232-A			A			$ 11,513.82	$ 11,859.24	$ 12,215.01	$ 12,581.46	$ 12,958.90	$ 13,347.68	$ 13,748.11	$ 14,160.54	$ 14,585.36	$ 15,022.92
Informatica Corporation	DataMove for IMS Source	License	CCSI13350233-A			A			$ 1,016.77	$ 1,047.28	$ 1,078.70	$ 1,111.06	$ 1,144.39	$ 1,178.72	$ 1,214.08	$ 1,250.51	$ 1,288.02	$ 1,326.67
Informatica Corporation	Change DataMove for IMS Source	License	CCSI13350234-A			A			$ 1,091.57	$ 1,124.32	$ 1,158.05	$ 1,192.79	$ 1,228.58	$ 1,265.43	$ 1,303.40	$ 1,342.49	$ 1,382.77	$ 1,424.25
Informatica Corporation	DataMove	License	CCSI13350235-A			A			$ 1,365.32	$ 1,406.27	$ 1,448.46	$ 1,491.92	$ 1,536.68	$ 1,582.77	$ 1,630.26	$ 1,679.16	$ 1,729.54	$ 1,781.43
Informatica Corporation	Change DataMove DB2 Target	License	CCSI13350236-A			A			$ 601.51	$ 619.55	$ 638.14	$ 657.29	$ 677.00	$ 697.31	$ 718.23	$ 739.78	$ 761.97	$ 784.83
Informatica Corporation	DataMove DB2 Target	License	CCSI13350237-A			A			$ 300.76	$ 309.79	$ 319.07	$ 328.65	$ 338.51	$ 348.66	$ 359.12	$ 369.90	$ 380.99	$ 392.42
Informatica Corporation	Change DataMove/DataMove Target for UDB	License	CCSI13350238-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	SSA - Name 3	License	CCSU13350239-A			A			$ 5 341.99	$ 5 496.02	$ 5 652.61	$ 5 813.90	$ 5 980.03	$ 5 873.68	$ 6 052.24	$ 6 233.77	$ 6 420.75	$ 6 613.34
KMSYS Worldwide, Inc.	IQU Plus-1	License	CCSU13350240-A			A			$ 488.41	$ 502.49	$ 516.81	$ 531.56	$ 546.75	$ 537.02	$ 553.35	$ 569.94	$ 587.04	$ 604.65
KMSYS Worldwide, Inc.	IQU Reorg Composer	License	CCSU13350241-A			A			$ 345.96	$ 355.93	$ 366.07	$ 376.52	$ 387.28	$ 380.39	$ 391.95	$ 403.71	$ 415.82	$ 428.29
KMSYS Worldwide, Inc.	QPLXSS	License	CCSU13350242-A			A			$ 0.99	$ 1.02	$ 1.05	$ 1.08	$ 1.11	$ 1.09	$ 1.12	$ 1.16	$ 1.19	$ 1.23
KMSYS Worldwide, Inc.	QPLXSV	License	CCSU13350243-A			A			$ 85.85	$ 88.33	$ 90.85	$ 93.44	$ 96.11	$ 94.40	$ 97.27	$ 100.19	$ 103.19	$ 106.29
KMSYS Worldwide, Inc.	QPLXV	License	CCSU13350244-A			A			$ 76.31	$ 78.51	$ 80.75	$ 83.06	$ 85.43	$ 83.91	$ 86.46	$ 89.05	$ 91.73	$ 94.48
Microsoft	SQL Server Enterprise	License	CCSU13350246-A			A			$ 105.68	$ 108.73	$ 111.82	$ 115.02	$ 118.30	$ 116.20	$ 119.73	$ 123.32	$ 127.02	$ 130.83
SAS Institute, Inc.	Base SAS	License	CCSI13350247-A			A			$ 12,839.27	$ 13,224.45	$ 13,621.18	$ 14,029.82	$ 14,450.71	$ 14,884.24	$ 15,330.76	$ 15,790.69	$ 16,264.40	$ 16,752.34
SAS Institute, Inc.	SAS/ACCESS Interface for IMS	License	CCSI13350248-A			A			$ 8,127.40	$ 8,371.23	$ 8,622.37	$ 8,881.04	$ 9,147.47	$ 9,421.89	$ 9,704.55	$ 9,995.69	$ 10,295.56	$ 10,604.42
SAS Institute, Inc.	SAS/ACCESS DB2	License	CCSI13350249-A			A			$ 8,127.40	$ 8,371.23	$ 8,622.37	$ 8,881.04	$ 9,147.47	$ 9,421.89	$ 9,704.55	$ 9,995.69	$ 10,295.56	$ 10,604.42
SAS Institute, Inc.	SAS/AF	License	CCSI13350250-A			A			$ 8 127.40	$ 8 371.23	$ 8 622.37	$ 8 881.04	$ 9 147.47	$ 9 421.89	$ 9 704.55	$ 9 995.69	$ 10 295.56	$ 10 604.42
SAS Institute, Inc.	SAS/FSP	License	CCSI13350251-A			A			$ 8 127.40	$ 8 371.23	$ 8 622.37	$ 8 881.04	$ 9 147.47	$ 9 421.89	$ 9 704.55	$ 9 995.69	$ 10 295.56	$ 10 604.42
SAS Institute, Inc.	SAS/GRAPH	License	CCSI13350252-A			A			$ 11 135.74	$ 11 469.80	$ 11 813.90	$ 12 168.32	$ 12 533.37	$ 12 909,37	$ 13 296.65	$ 13 695.54	$ 14 106.41	$ 14 529.61
SAS Institute, Inc.	SAS/SHARE	License	CCSI13350253-A			A			$ 8,127.40	$ 8,371.23	$ 8,622.37	$ 8,881.04	$ 9,147.47	$ 9,421.89	$ 9,704.55	$ 9,995.69	$ 10,295.56	$ 10,604.42
SAS Institute, Inc.	SAS/STAT	License	CCSI13350254-A			A			$ 8,763.17	$ 9,026.06	$ 9,296.84	$ 9,575.74	$ 9,863.02	$ 10,158.91	$ 10,463.67	$ 10,777.59	$ 11,100.91	$ 11,433.94
SMA	OpCon/xps EXEC LSAM, Group 3	License	CCSU13350256-A			A			$ 296.25	$ 304.79	$ 313.47	$ 322.42	$ 331.63	$ 325.73	$ 335.63	$ 345.70	$ 356.07	$ 366.75
SMA	OpCon/xps EXEC LSAM, Group 8	License	CCSU13350257-A			A			$ 1,076.55	$ 1,107.59	$ 1,139.14	$ 1,171.65	$ 1,205.13	$ 1,183.69	$ 1,219.68	$ 1,256.26	$ 1,293.94	$ 1,332.76
SMA	OpCon/xps EXEC LSAM, Group 14	License	CCSU13350258-A			A			$ 2,780.73	$ 2,860.91	$ 2,942.42	$ 3,026.38	$ 3,112.86	$ 3,057.50	$ 3,150.44	$ 3,244.94	$ 3,342.27	$ 3,442.52
SMA	OpCon/xps Microsoft LSAM	License	CCSU13350259-A			A			$ 90.10	$ 92.70	$ 95.34	$ 98.06	$ 100.86	$ 99.07	$ 102.08	$ 105.14	$ 108.29	$ 111.54
SMA	OpCon/xps User Interface	License	CCSU13350260-A			A			$ 4.96	$ 5.11	$ 5.25	$ 5.40	$ 5.56	$ 5.46	$ 5.62	$ 5.79	$ 5.97	$ 6.14
Sybase	EAServer Deploy Advanced - Active	License	CCSU13350261-A			A			$ 149.21	$ 153.51	$ 157.89	$ 162.39	$ 167.03	$ 164.06	$ 169.05	$ 174.12	$ 179.34	$ 184.72
Sybase	EAServer Deploy Advanced - Passive	License	CCSU13350262-A			A			$ 37.36	$ 38.43	$ 39.53	$ 40.66	$ 41.82	$ 41.07	$ 42.32	$ 43.59	$ 44.90	$ 46.25
TRILOGexport, Inc.	TriTune Automation Component (APC)	License	CCSI13350263-A			A			$ 34 342.18	$ 5 723.73	$ 5 723.73	$ 5 723.73	$ 5 723.73	$ 5 723.73	$ 5 723.73	$ 5 723.73	$ 5 723.73	$ 5 723.73
Unicon Group Ltd.	LOUIS II Database Gateway	License	CCSU13350264-A			A			$ 892.57	$ 918.31	$ 944.47	$ 971.42	$ 999.18	$ 981.41	$ 1 011.24	$ 1 041.57	$ 1 072.82	$ 1 105.00
Unicon Group Ltd.	LOUIS II DMS Interface	License	CCSU13350265-A			A			$ 111.11	$ 114.32	$ 117.57	$ 120.93	$ 124.38	$ 122.17	$ 125.89	$ 129.66	$ 133.55	$ 137.56
Unicon Group Ltd.	LOUIS II Extract & Reporting Module	License	CCSU13350266-A			A			$ 892.57	$ 918.31	$ 944.47	$ 971.42	$ 999.18	$ 981.41	$ 1 011.24	$ 1 041.57	$ 1 072.82	$ 1 105.00
Unicon Group Ltd.	LOUIS II LCOM Host Module	License	CCSU13350267-A			A			$ 55.56	$ 57.16	$ 58.79	$ 60.46	$ 62.19	$ 61.09	$ 62.94	$ 64.83	$ 66.78	$ 68.78
Unicon Group Ltd.	LOUIS II MAPPER Interface	License	CCSU13350268-A			A			$ 111.11	$ 114.32	$ 117.57	$ 120.93	$ 124.38	$ 122.17	$ 125.89	$ 129.66	$ 133.55	$ 137.56
Unicon Group Ltd.	LOUIS II RDMS Interface	License	CCSU13350269-A			A			$ 111.11	$ 114.32	$ 117.57	$ 120.93	$ 124.38	$ 122.17	$ 125.89	$ 129.66	$ 133.55	$ 137.56
Verisign	Secure Site Pro SSL	License	CCSU13350270-A			A			$ 92.17	$ 97.52	$ 100.30	$ 103.16	$ 106.11	$ 104,24	$ 107.40	$ 110.63	$ 113.94	$ 117.36
WinZip	Self-Extractor 10-user license	License	CCSU13350272-A			A			$ 0.66	$ 0.67	$ 0.69	$ 0.71	$ 0.73	$ 0.72	$ 0.74	$ 0.76	$ 0.79	$ 0.81
Additional Technical Resources (Technical Staff Rate Card)																		
Infrastructure (mainframe, mid-range and x86) Architects/Engineers		Per Hour	CCSZ13360001-A	N/A	N/A	A			$ 130.00	$ 132.00	$ 135.00	$ 137.00	$ 140.00	$ 142.00	$ 145.00	$ 148.00	$ 150.00	$ 153.00
Microsoft Product Specialists (e.g. Exchange, SharePoint)		Per Hour	CCSZ13360002-A	N/A	N/A	A			$ 130.00	$ 132.00	$ 135.00	$ 137.00	$ 140.00	$ 142.00	$ 145.00	$ 148.00	$ 150.00	$ 153.00
Basis and SAP Oracle support		Per Hour	CCSD13360003-A	N/A	N/A	A			$ 190.00	$ 194.00	$ 199.00	$ 203.00	$ 207.00	$ 212.00	$ 217.00	$ 221.00	$ 226.00	$ 231.00
Performance Specialists		Per Hour	CCSZ13360004-A	N/A	N/A	A			$ 130.00	$ 132.00	$ 135.00	$ 137.00	$ 140.00	$ 142.00	$ 145.00	$ 148.00	$ 150.00	$ 153.00
Mainframe Systems Programmers		Per Hour	CCSZ13360005-A	N/A	N/A	A			$ 104.00	$ 106.00	$ 108.00	$ 110.00	$ 112.00	$ 114.00	$ 116.00	$ 118.00	$ 120.00	$ 123.00
Batch Administrators		Per Hour	CCSZ13360006-A	N/A	N/A	A			$ 93.00	$ 95.00	$ 96.00	$ 98.00	$ 100.00	$ 102.00	$ 104.00	$ 106.00	$ 108.00	$ 110.00
3rd Party Software Product Specialists		Per Hour	CCSZ13360007-A	N/A	N/A	A			$ 130.00	$ 132.00	$ 135.00	$ 137.00	$ 140.00	$ 142.00	$ 145.00	$ 148.00	$ 150.00	$ 153.00
System Administrator (Windows, AIX, Linux)		Per Hour	CCSZ13360008-A	N/A	N/A	A			$ 130.00	$ 132.00	$ 135.00	$ 137.00	$ 140.00	$ 142.00	$ 145.00	$ 148.00	$ 150.00	$ 153.00
System Administrator (Middleware support)		Per Hour	CCSZ13360009-A	N/A	N/A	A			$ 104.00	$ 106.00	$ 108.00	$ 110.00	$ 112.00	$ 114.00	$ 116.00	$ 118.00	$ 120.00	$ 123.00
Storage Administrator		Per Hour	CCSZ13360010-A	N/A	N/A	A			$ 104.00	$ 106.00	$ 108.00	$ 110.00	$ 112.00	$ 114.00	$ 116.00	$ 118.00	$ 120.00	$ 123.00
Data Backup Administrator		Per Hour	CCSZ13360011-A	N/A	N/A	A			$ 93.00	$ 95.00	$ 96.00	$ 98.00	$ 100.00	$ 102.00	$ 104.00	$ 106.00	$ 108.00	$ 110.00
Database Administrator		Per Hour	CCSZ13360012-A	N/A	N/A	A			$ 210.00	$ 215.00	$ 220.00	$ 225.00	$ 230.00	$ 235.00	$ 240.00	$ 245.00	$ 250.00	$ 256.00
Database Architects		Per Hour	CCSZ13360013-A	N/A	N/A	A			$ 172.00	$ 175.00	$ 179.00	$ 182.00	$ 185.00	$ 189.00	$ 192.00	$ 196.00	$ 200.00	$ 204.00
Database Analysts		Per Hour	CCSZ13360014-A	N/A	N/A	A			$ 100.00	$ 102.00	$ 104.00	$ 106.00	$ 108.00	$ 110.00	$ 112.00	$ 114.00	$ 116.00	$ 118.00
Project Management Support		Per Hour	CCSZ13360015-A	N/A	N/A	A			$ 148.00	$ 151.00	$ 154.00	$ 157.00	$ 159.00	$ 162.00	$ 166.00	$ 169.00	$ 172.00	$ 175.00
Network Administrator		Per Hour	CCSZ13360016-A	N/A	N/A	A			$ 130.00	$ 132.00	$ 135.00	$ 137.00	$ 140.00	$ 142.00	$ 145.00	$ 148.00	$ 150.00	$ 153.00
Facilities Administrator		Per Hour	CCSZ13360017-A	N/A	N/A	A			$ 72.00	$ 74.00	$ 75.00	$ 77.00	$ 78.00	$ 79.00	$ 81.00	$ 82.00	$ 84.00	$ 86.00
Security Administrator		Per Hour	CCSZ13360018-A	N/A	N/A	A			$ 130.00	$ 132.00	$ 135.00	$ 137.00	$ 140.00	$ 142.00	$ 145.00	$ 148.00	$ 150.00	$ 153.00
Security Architects		Per Hour	CCSZ13360019-A	N/A	N/A	A			$ 172.00	$ 175.00	$ 179.00	$ 182.00	$ 185.00	$ 189.00	$ 192.00	$ 196.00	$ 200.00	$ 204.00

SERVICES CATALOG

Field Name ==>	Product Name	Unit	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use *==>*	*Unique Identifier*	*Unit*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Security Analysts		Per Hour	CCSZ13360020-A	N/A	N/A	A			$ 100.00	$ 102.00	$ 104.00	$ 106.00	$ 108.00	$ 110.00	$ 112.00	$ 114.00	$ 116.00	$ 118.00
Asset Management Administrator		Per Hour	CCSZ13360021-A	N/A	N/A	A			$ 67.00	$ 68.00	$ 69.00	$ 71.00	$ 72.00	$ 73.00	$ 75.00	$ 76.00	$ 78.00	$ 79.00
Quality Assurance Support		Per Hour	CCSZ13360022-A	N/A	N/A	A			$ 85.00	$ 87.00	$ 89.00	$ 90.00	$ 92.00	$ 94.00	$ 95.00	$ 97.00	$ 99.00	$ 101.00
Remedy Support Specialist		Per Hour	CCSZ13360023-A	N/A	N/A	A			$ 157.00	$ 160.00	$ 163.00	$ 166.00	$ 169.00	$ 173.00	$ 176.00	$ 179.00	$ 183.00	$ 186.00
IT Service Continuity Specialist		Per Hour	CCSZ13360024-A	N/A	N/A	A			$ 130.00	$ 132.00	$ 135.00	$ 137.00	$ 140.00	$ 142.00	$ 145.00	$ 148.00	$ 150.00	$ 153.00

SCHEDULE C.2

SERVICES CATALOG - DESCRIPTIONS

Table of Contents

Introduction 4
Catalog of Services (Schedule C.1) 4
Enterprise Services Catalog Template 5
Compute Services - Fully Managed Services 7
Fully Managed - X86 (Windows and Linux) 7
Fully Managed - P-Series Server (AIX) 7
Compute Services - Managed Only Services 7
Managed Only Services – X86 (Windows and Linux) 7
Managed Only Services – P-Series (AIX) 7
Fully Managed - Storage and Backup 7
Storage Services 7
Tape and Backup Services 7
Compute Services - Co-Location Services 7
Compute Services - Mainframe Services 7
IBM Mainframe Storage and Backup 7
IBM Mainframe Storage Services 7
IBM Mainframe Backup and Tape Services 7
IBM Mainframe Service 7
Unisys Mainframe Storage and Backup 7
Unisys Mainframe Storage Services 7
Unisys Mainframe Backup and Tape Services 7
Unisys Mainframe Service 7
Compute Services - Infrastructure as a Service 7
Infrastructure as a Service (IaaS) – Windows and Linux 7
Infrastructure as a Service (IaaS) – Storage 8

Infrastructure as a Service - Backup 8
Third Party Software Management Service 8
Third Party Software – Unisys Vendor Supplied License and Management 8
Third Party Software – Commonwealth Supplied License, Unisys Vendor Supplied Maintenance 8
Additional Technical Resources 8
Additional Technical Services 8

Introduction

The Enterprise Services Catalog provides descriptions for the specific entries shown including descriptions of related Enterprise Services Catalog items that will be needed to place a selection into its proper context.

The Enterprise Services Catalog is laid out with the following sections.

1) Catalog of Services
2) Enterprise Services Catalog Template
3) Compute Services - Fully Managed Services
4) Compute Services - Managed Only Services
5) Compute Services - Co-location Services
6) Compute Services - Mainframe Services
7) Compute Services – Infrastructure as a Service
8) Third-Party Software
9) Additional Technical Resources
10) Additional Technical Services

Enterprise Services Catalog Template

Service Attribute	*Service Attribute Description*
Service Name	*Title of Service*
Provider Part Number	*Provider Part Number*
Orderable Unit	*Orderable Unit (e.g. Per Server, Per Request)*
Description	*Short description of the service*
Service Customers / Users	*Any participating Commonwealth agency, office, board, commission, or bureau; unless otherwise noted*
Service Prerequisites	*The identified technical prerequisite or related additional services or activities required when this service is ordered. This does not include contractual terms or conditions.*
Fulfillment Timeframe	*This attribute describes the timeframe required to fulfill the request. This applies only to Services which are available to process as a Standard Service Request. Otherwise, this is marked as Not Applicable.*

This page intentionally left blank.

Compute Services - Fully Managed Services

Fully Managed - X86 (Windows and Linux)

Fully Managed - P-Series Server (AIX)

Compute Services - Managed Only Services

Managed Only Services – X86 (Windows and Linux)

Managed Only Services – P-Series (AIX)

Fully Managed - Storage and Backup

Storage Services

Tape and Backup Services

Compute Services - Co-Location Services

Compute Services - Mainframe Services

IBM Mainframe Storage and Backup

IBM Mainframe Storage Services

IBM Mainframe Backup and Tape Services

IBM Mainframe Service

Unisys Mainframe Storage and Backup

Unisys Mainframe Storage Services

Unisys Mainframe Backup and Tape Services

Unisys Mainframe Service

Compute Services - Infrastructure as a Service

Infrastructure as a Service (IaaS) – Windows and Linux

Infrastructure as a Service (IaaS) – Storage

Infrastructure as a Service - Backup

Third Party Software Management Service

Third Party Software – Unisys Vendor Supplied License and Management

Third Party Software – Commonwealth Supplied License, Unisys Vendor Supplied Maintenance

Additional Technical Resources

Additional Technical Services

Schedule C.3

Termination Fees

Termination for Convenience Fees

	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
(A) Termination Fee Base	$30,000,000 00	$75,000,000 00	$30,000,000 00							
(B) Value of Services Performed*	(Services Performed)	(Services Performed)	(Services Performed)							
(C) Actual Termination for Convenience Fees	C =A-B	C =A-B	C =A-B							

No Termination for Convenience Fees are available after Year 3.

Termination for Conveinence Fees are not cumulative.

(*) The value of all Services performed by the Contractor consistent with the terms of the Contract prior to the effective date of termination

Schedule D

Transition Milestones

Milestones include the completion of all tasks, deliverables and interim milestones associated with such Milestone as set forth in the Transition Plan. The Earn Back period is thirty (30) calendar days from the Transition Milestone Due Date and applies to those Milestones indicated with "Y" in the Earn Back column. The Acceptance Criteria for each Milestone includes criteria described in Schedule F and Schedule K of the contract.

Note: If a Milestone is dependent on another Milestone and the first Milestone is missed, the subsequent Milestones remain in effect. An example is: if M-3 is missed, M-5 is still enforced.

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
M-1	Key Staffing	30 calendar days from Contract Effective Date	• Key Personnel team completed per Schedule G • staffing plan approved • detailed project organizational chart approved • resumes for each key personnel listed on the team submitted • staff contingency plan approved	$50,000 One-time	N	• Commonwealth review and approval
M-2	Contract Management Plan	60 calendar days from Contract Effective Date	• Delivery and acceptance of the following Deliverables from Schedule K: o D-11.01 o D-11.02	$50,000 One-time	Y	• Commonwealth review and approval
M-3	Datacenter Architecture Plan and Roadmap	90 calendar days from Contract Effective Date	• Delivery and acceptance of the following Deliverables from Schedule K: o D-01.01 o D-01.02 (Initial Deliverable Approval) o D-01.03 (Initial Deliverable Approval) o D-01.04 (Initial Deliverable Approval) o D-01.05 (Initial Deliverable	$150,000 One-time	Y	• Commonwealth review and approval

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			Approval) o D-01.07 o D-03.01 o D-03.04 o D-03.08 o D-04.01 o D-04.05			
M-4	Detailed Transition Plan	180 calendar days from Contract Effective Date	• Completion of Data Gathering o All data gathering checklists completed, validated, reviewed and approved • Completion, submittal and acceptance of data gathering report on B2B interface to Commonwealth's ITSM system that includes interfaces for the following: o Incident Management o Change Management o Problem Management o Known Errors o Request Management o Invoicing Process • Completion and acceptance of the Detailed Transition Plan using Schedule M – Detailed Transition Plan • Delivery and acceptance of the following Deliverables from Schedule K: o D-05.01 o D-05.04 o D-05.10	$250,000 One-time	N	• Commonwealth review and approval

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			○ D-10.01 • The Detailed Transition plan must contain: ○ An **overall (master) plan** which includes but is not limited to: ▪ transition governance plan ▪ transition risk and mitigation plan ▪ due diligence timeline ▪ configuration / testing verification ▪ operational readiness ○ A **plan by Datacenter** which includes but is not limited to: ▪ transition governance plan ▪ transition risk and mitigation plan ▪ due diligence timeline ▪ configuration / testing verification ▪ operational readiness ○ A **plan by Agency** which includes but is not limited to: ▪ transition governance plan ▪ transition risk and mitigation plan ▪ due diligence timeline ▪ configuration / testing verification ▪ operational readiness ○ A **plan by Application** which includes but is not limited to:			

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			▪ transition governance plan ▪ transition risk and mitigation plan ▪ due diligence timeline ▪ configuration / testing verification ▪ operational readiness			
M-5	Commonwealth Compute Process Manual (CCPM)	180 calendar days from Contract Effective Date	• Delivery and acceptance of the following Deliverables from Schedule K: o D-02.01 o D-02.04 o D-02.09 o D-02.15 o D-02.17 o D-02.18 o D-02.23 o D-02.26 o D-02.29 o D-02.32 o D-02.37 o D-02.42 o D-02.47 o D-02.52 o D-02.57 o D-02.62 o D-02.67 o D-02.70 o D-02.75 o D-02.81 • Completion and Acceptance of final	$75,000 One-time	Y	• Commonwealth review and approval

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			CCPM as listed within Schedule L of this contract. This includes but is not limited to: o Incident (including Security) o Problem o Change o Order/Request o Billing o Service Level			
M-6	Network Connectivity	120 calendar days from Contract Effective Date	• Completion and Acceptance of the Network Connectivity to the Commonwealth	$250,000 One-time	N	• Commonwealth review, testing and approval
M-7	Security	180 calendar days from Contract Effective Date	• Completion and acceptance of security architecture, solution, policies and procedures which included but is not limited to: o Delivery and acceptance of the following Deliverables from Schedule K: ▪ D-07.01 ▪ D-07.06 ▪ D-01.03 (Initial Deliverable Approval) ▪ D-09.01 ▪ D-09.02 o Implement security management plan o Implement security and firewall plan o Policies and procedures are in place	$250,000 One-time	N	• Commonwealth review and approval

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			for physical security o Policies and procedures are in place for data and network security o Policies and procedures are in place for personnel security, such as annual background checks o Security assessment is conducted to ensure data safety and confidentiality			
M-8	ITSM System Integration	180 calendar days from Contract Effective Date	• Completion and Acceptance of Integration between Commonwealth's ITSM system and Offeror's ITSM System including but is not limited to: o Incident connectivity has been tested and incidents created and updated on either side flow back and forth between systems o Problem connectivity has been tested and problems created and updated on either side flow back and forth between systems o Change requests connectivity has been tested and requests created and updated on either side flow back and forth between systems o Configuration items in both system CMDBs are reconciled o Test Invoices have been processed through the ITSM system to the Commonwealth's AP system o Reporting from Offeror's ITSM system is available to	$100,000 One-time	Y	• Commonwealth review and approval

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			Commonwealth			
M-9	Financial Management	180 calendar days from Contract Effective Date	• Completion and acceptance of billing process and form of invoice approved • Schedule K Deliverable D-02.01 completed • Process implemented, tested and accepted providing an enterprise bill providing the details required by the Commonwealth	$75,000 One-time	Y	• Commonwealth review and approval
M-10	Operational Readiness	240 calendar days from Contract Effective Date	• Completion and acceptance of an Operational Readiness Report indicating Offeror is "Ready" to transition the Commonwealth's Applications and Services to other Datacenters. This report must include but is not limited to the following: o Delivery and acceptance of the following Deliverables from Schedule K: ▪ D-01.01 ▪ D-01.02 ▪ D-01.03 ▪ D-01.04 ▪ D-01.05 ▪ D-01.06 ▪ D-01.07 o Transition Project Office established and fully staffed o Program plan and architecture developed and approved by the Commonwealth	$150,000 One-time	N	• Commonwealth review and approval

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			○ Processes and Tools implemented to support the transition change control, schedule, quality, communications, risk and issue management ○ Datacenter environment configured , tested and acceptance			
M-11	SSAE 16 Audits of EDC	On the July 31st following the Commonwealth's acceptance of Milestone M-14	• Completion and Issuance of a SSAE-16 Audit Reports as detailed with the Appendix A (Terms and Conditions) on the Commonwealth's EDC Datacenter • Schedule K Deliverable D-08.02	$100,000 One-time	Y	• Commonwealth review and approval
M-12	DPH Transition Completed (1)	18 months from Contract Effective Date	• Completion and acceptance of ALL applications transitioned from the DPH to new Datacenters which includes but is not limited to the following for each application: ○ High availability, backup and DR are operational for identified systems. ○ CCPM specific details for application are available in KMP. ○ Operations dashboards to report immediately on status and alerts for transitioned applications. ○ Service Level agreements are identified and supporting metrics in place. ○ System operational for scheduling and	$2,500,000 per month or partial month for six (6) months	N	• Commonwealth review and approval of work product plus assisting in data gathering, planning, ordering, implementing, testing and accepting the transition of the applications

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			tracking of ticket-based tasks and incidents. o System is available to begin data collection to produce configuration, monitoring and management status reports. o Systems with DR plans have an updated DR plan and test scheduled. o Operational support assumed and workloads migrated. • High-Speed direct link to current DPH location is disconnected. • Signoff that all Services provided by DPH have been successfully transitioned			
M-13	DPH Transition Completed (2)	24 months from Contract Effective Date	• Completion and acceptance of ALL applications transitioned from the DPH to new Datacenters which includes but is not limited to: o High availability, backup and DR are operational for identified systems. o CCPM contains specific details for apps transitioned are available in KMP. o Operations dashboards are in place to report immediately on status and alerts for transitioned apps. o Service Level agreements have been identified and supporting metrics in place. o System is operational for scheduling and tracking of ticket-based tasks and incidents. o System available to begin data collection in order to produce	$5,000,000 per month or partial month	N	• Commonwealth review and approval of work product plus assisting in data gathering, planning, ordering, implementing, testing and accepting the transition of the applications

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			configuration, monitoring and management status reports. o Systems with DR plans have a replacement plan and test scheduled. o Operational support has been assumed and workloads migrated. o High-Speed direct link to current DPH location is disconnected. o Signoff that all Services provided by DPH have been successfully transitioned			
M-14	EDC Operational Transition Completed	12/31/2014	• Completion and acceptance of operational control and support of the EDC which includes but is not limited to the following: o Schedule K deliverable D-01 o Schedule K deliverable D-08.01 o Schedule K deliverable D-08.06 o Verification CMDB of record with Offeror's configuration info includes EDC assets and CI's o Service catalogs, processes, and procedures are transitioned o Multi environments/instances are available for identified systems o High availability, backup and DR are operational for identified system o CCPM specific details for applications are available in KMP. o Operations dashboards are in place to report immediately on status and alerts for apps o Service Level agreements have been identified and supporting metrics in	$100,000 per month or partial month	N	• Commonwealth review and approval of work product plus assisting in data gathering, planning, ordering, implementing, testing and accepting the transition of the applications

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			place o System is operational for scheduling and tracking of ticket-based tasks and incidents o System is available to begin data collection in order to produce configuration, monitoring and management status reports o Transition orders completed and accepted by the Commonwealth			
M-15	Department of Labor and Industry Datacenter Transition Completed	30 months from Contract Effective Date	• Completion and acceptance of ALL applications transitioned from the DLI Datacenter to new Datacenters which includes but is not limited to the following: o Service catalogs, processes and procedures fully established, documented and approved o Multi environments and instances are fully functional for transitioned systems o High availability, backup and DR are operational for transitioned systems o CCPM contains specific details for apps transitioned are available in KMP o Operations dashboards are in place to report immediately on status and alerts for transitioned apps o Service Level agreements have been identified and supporting metrics in place o System is operational for scheduling and tracking of ticket-based tasks and incidents o System available to begin data	$1,000 000 One-time	N	• Commonwealth review and approval of work product plus assisting in data gathering, planning, ordering, implementing, testing and accepting the transition of the applications

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			collection in order to produce configuration, monitoring and management status reports o Transition orders completed and accepted by the Commonwealth			
M-16	Department of Revenue Datacenter Transition Completed	30 months from Contract Effective Date	• Completion and acceptance of ALL applications transitioned from the DOR Datacenter to new Datacenters which includes but is not limited to the following: o Service catalogs, processes and procedures fully established, documented and approved o Multi environments and instances are fully functional for transitioned systems o High availability, backup and DR are operational for transitioned systems o CCPM contains specific details for applications transitioned are available in KMP o Operations dashboards are in place to report immediately on status and alerts for transitioned apps o Service Level agreements have been identified and supporting metrics in place o System is operational for scheduling and tracking of ticket-based tasks and incidents o System available to begin data collection in order to produce configuration, monitoring and management status reports o Transition orders completed and	$1,000,000 One-time	N	• Commonwealth review and approval of work product plus assisting in data gathering, planning, ordering, implementing, testing and accepting the transition of the applications

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			accepted by the Commonwealth			
M-17	Pennsylvania State Police Datacenter Transition Completed	30 months from Contract Effective Date	• Completion and acceptance of ALL applications transitioned from the PSP Datacenter to new Datacenters which includes but is not limited to the following: o Service catalogs, processes and procedures fully established, documented and approved o Multi environments and instances are fully functional for transitioned systems o High availability, backup and DR are operational for transitioned systems o CCPM contains specific details for applications transitioned are available in KMP o Operations dashboards are in place to report immediately on status and alerts for transitioned apps o Service Level agreements have been identified and supporting metrics in place o System is operational for scheduling and tracking of ticket-based tasks and incidents o System available to begin data collection in order to produce configuration, monitoring and management status reports o Transition orders completed and accepted by the Commonwealth	$1,000,000 One-time	N	• Commonwealth review and approval of work product plus assisting in data gathering, planning, ordering, implementing, testing and accepting the transition of the applications
M-18	Department of Public Welfare Datacenter	30 months from Contract	• Completion and acceptance of ALL applications transitioned from the DPW Datacenter to new Datacenters which	$1,000,000 One-time	N	• Commonwealth review and approval of work product plus assisting in data

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
	Transition Completed	Effective Date	includes but is not limited to the following: o Service catalogs, processes and procedures fully established, documented and approved o Multi environments and instances are fully functional for transitioned systems o High availability, backup and DR are operational for transitioned systems o CCPM contains specific details for apps transitioned are available in KMP o Operations dashboards are in place to report immediately on status and alerts for transitioned apps o Service Level agreements have been identified and supporting metrics in place o System is operational for scheduling and tracking of ticket-based tasks and incidents o System available to begin data collection in order to produce configuration, monitoring and management status reports o Transition orders completed and accepted by the Commonwealth			gathering, planning, ordering, implementing, testing and accepting the transition of the applications
M-19	Department of Health Datacenter Transition Completed	30 months from Contract Effective Date	• Completion and acceptance of ALL applications transitioned from the DOH Datacenter to new Datacenters which includes but is not limited to the following: o Service catalogs, processes and procedures fully established, documented and approved	$1,000,000 One-time	N	• Commonwealth review and approval of work product plus assisting in data gathering, planning, ordering, implementing, testing and accepting the transition of the applications

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			○ Multi environments and instances are fully functional for transitioned systems ○ High availability, backup and DR are operational for transitioned systems ○ CCPM contains specific details for apps transitioned are available in KMP ○ Operations dashboards are in place to report immediately on status and alerts for transitioned apps ○ Service Level agreements have been identified and supporting metrics in place ○ System is operational for scheduling and tracking of ticket-based tasks and incidents ○ System available to begin data collection in order to produce configuration, monitoring and management status reports ○ Transition orders completed and accepted by the Commonwealth			

Schedule E

Data Center Locations

[redacted]

[redacted]

[redacted]

Schedule F

Data Center Statement of Work

Contents

1 Contractor Guidelines 5

2 Program Objectives 6

2.1 Service Level Agreements 8

2.2 Solution Requirements Overview 8

2.2.1 Datacenter 2+ Architecture 8

2.2.2 IP conversion strategy 9

2.2.3 Common Services Portfolio 10

2.2.4 Data Protection 11

2.2.5 Transition Services 12

3 Tasks 13

3.1 Establish Datacenter Architecture 13

3.1.1 Multi Datacenter Environment (2+ Architecture) 14

3.1.2 Network and Security Architecture 16

3.1.3 Datacenter Architecture and Technology 17

3.2 Enable Common Service Portfolio 19

3.2.1 Program & Service Management 20

3.2.1.1 PMO & Contract Management 20

3.2.1.2 Availability/SLA Management 30

The Contractor is responsible for storing raw data used to generate SLA reports for the duration of the contract plus 3 years. The Contractor must make that raw data available to the Commonwealth via the Contractor hosted knowledge management portal for no-less than the most recent 13 months. Data older than the most recent 13 months must be provided on request in a format prescribed by the Commonwealth within 5 business days of the request.. 31

3.2.1.3 Change & Release Management 33

3.2.1.4 +Service Desk 36

3.2.1.5 Technical Architecture 39

3.2.1.6 Account Management 44

3.2.1.7 Configuration Management 46

3.2.1.8 3rd Party License Management 48

3.2.2 Technical Services 49
3.2.2.1 Transition Management (New Customer and/or Services) 49
3.2.2.2 Infrastructure Architecture 51
3.2.2.3 Capacity Management 54
3.2.2.4 DR Planning & Testing 56
3.2.2.5 Security Management 60
3.3 Related to the project management and contract management role, the Contractor must provide Continual Service Improvement to reduce service risks. 62
3.3.1.1 Performance Monitoring & Management 64
3.3.2 Facilities Management 67
3.3.2.1 Facilities Architecture / Maintenance 67
3.3.2.2 Site Operations 70
3.3.3 Managed Hosting Services 74
3.3.3.1 Windows Support 74
3.3.3.2 Storage Management 78
3.3.3.3 ERP Hosting – SAP / Oracle 81
3.3.3.4 UNIX Support – AIX / Linux 85
3.3.3.5 Mainframe Services 89
3.3.3.6 Security & Firewall 94
3.3.3.7 Database Management Services 98
3.3.3.8 Limited-Use Colocation Services 100
3.3.4 Capacity on Demand Services 102
3.3.4.1 Server Capacity on Demand 102
3.3.4.2 Storage Capacity on Demand 105
3.3.4.3 DR Infrastructure on Demand 107
3.3.4.4 Additional Technical Services 108
3.4 Transition Services 109
3.4.1 Transition Services – Guiding Principals 109
3.4.2 Transition Planning/Governance 111
3.4.2.1 Transition Program Management 114

3.4.2.2 Security Transition Activities 119

1 Contractor Guidelines

This Schedule contains the Statement of Work ("SOW") for the Services. Note: references to Exhibits in this Schedule F refer to exhibits as they appeared in the RFP.

2 Program Objectives

The Commonwealth is seeking to implement a new datacenter service model that provides various infrastructures/computing platforms to service the needs of the Commonwealth in a secure and flexible manner. This initiative must realize the following objectives:

- Provide a reliable, flexible, secure, and robust IT infrastructure to support the transformation of the Commonwealth into an information-focused organization.
- Provide a multiple datacenter architecture utilizing the Contractor's datacenter assets to support the current and future capacity and service level demands.
- Include primary support for the Commonwealth's Enterprise Datacenter (EDC) operations and its computing assets including but not limited to datacenter facilities operations and infrastructure support.
- Leverage Contractor's established processes and tools necessary to ensure consistent and predictable pricing to facilitate accurate and timely budget projections.
- Provide engineering support that anticipates changes in business and technical requirements and make recommendations for staying current with industry best practices.
- Ensure that the Contractor's datacenters adhere to the Commonwealth's contractual, regulatory, and policy compliance requirements for security, architecture, and systems development life cycle (SDLC) standards.
- Establish a tiered service/capability to support high-availability hosting, backup, and disaster recovery (DR) Services to maintain continuity of government operations.
- Provide multiple environments and instances to support the enterprise application portfolio. For example; Development, Integration, System / User Acceptance Test (SAT/UAT), Training, load Testing, Pre-Production and Production.
- Continue to consolidate Commonwealth datacenters to achieve cost savings, energy consumption reductions, optimal space utilization, and improvements in IT asset utilization in accordance with the government-wide datacenter consolidation initiative currently underway.

To satisfy the Commonwealth diverse datacenter requirements, the Contractor must provide the necessary infrastructure for the following critical purposes:

- Provide production, development and hosting of new and legacy business applications and databases that run on mainframes (IBM and Unisys), mid-ranges and distributed platforms
- Support options for high-availability, backup/recovery, and multiple levels of DR Services in support of the Commonwealth.

The Contractor's datacenter architecture must consist of multiple geographically dispersed datacenters, referred below as a 2+ (two-plus) architecture. The Contractor must utilize the EDC as one of its datacenters and provide a minimum of one additional datacenter to meet the 2+ architecture requirement. It is the Contractor's option to utilize the EDC as one of its primary datacenters. The Contractor's datacenters must have the ability to provide multiple levels of DR Services in the event of a disaster, which must also include an option to support high availability (HA) application infrastructures.

The Contractor is responsible for ensuring successful delivery of IT infrastructure Services, providing the Commonwealth with visibility into (performance, capacity, security, SLA's etc.), as well as, working in partnership with the Commonwealth as required to ensure seamless operations. In turn, the Commonwealth will provide oversight to ensure that the Contractor is delivering agreed-upon Services and that the business requirements are clearly communicated and satisfied, and provide timely feedback on contractor performance. Commonwealth agencies, OA/OIT and the Contractor must work together on IT planning, including service and capacity planning, strategic and tactical planning, and IT resource and budget planning.

The datacenter approach must provide a computing infrastructure that delivers reliable, effective and technologically current Services seamlessly to the Commonwealth in a cost-effective manner. The cost for those Services must remain less than the cost the Commonwealth would have incurred for providing the same infrastructure itself. Applications hosted in the Contractor's datacenters must meet Quality of Service (QoS) requirements as determined by the Commonwealth agency application owners. The Commonwealth will avoid capital expenditure by acquiring Services through Capacity on Demand. The Commonwealth agencies will consume resources as a service and pay only for those resources that it uses. The Commonwealth and The Contractor must engage in proactive oversight of datacenter operations. The Commonwealth requires visibility into the Contractor's management practices and effective monitoring channels that include the following:

- Program and project progress reports that track milestones, deliverables, risks, and financial data.
- Commonwealth Computing Procedures Manual (CCPM) that provides up-to-date detailed description of all processes and procedures used to support the computing needs of the Commonwealth via the Contractor's Knowledge/Service Management Portal (KMP). The CCPM must contain specific sections dedicated to the operational procedures for each Commonwealth datacenter customer.
- Scheduling and tracking of ticket-based tasks and incidents.
- Operations dashboards with status and alerts based on real-time and historic data collected by instruments, agents, scanners, and logs that monitor the hosted applications, batch operations, network, security, and service performance measures.
- Other configuration, monitoring and management status reports as needed.

- Recommendations and offerings by the Contractor for improved processes and procedures for delivery of Services that are based on a program of continuous quality and process improvement as implemented by the Contractor.

2.1 Service Level Agreements

Service Level Agreements ("SLAs") are made part of this Contract as Schedule J.1, J.2, and J.3. The Contractor is also required to have or implement a quality and process improvement program that focuses not on just meeting minimum requirements but on meeting or exceeding the target requirements.

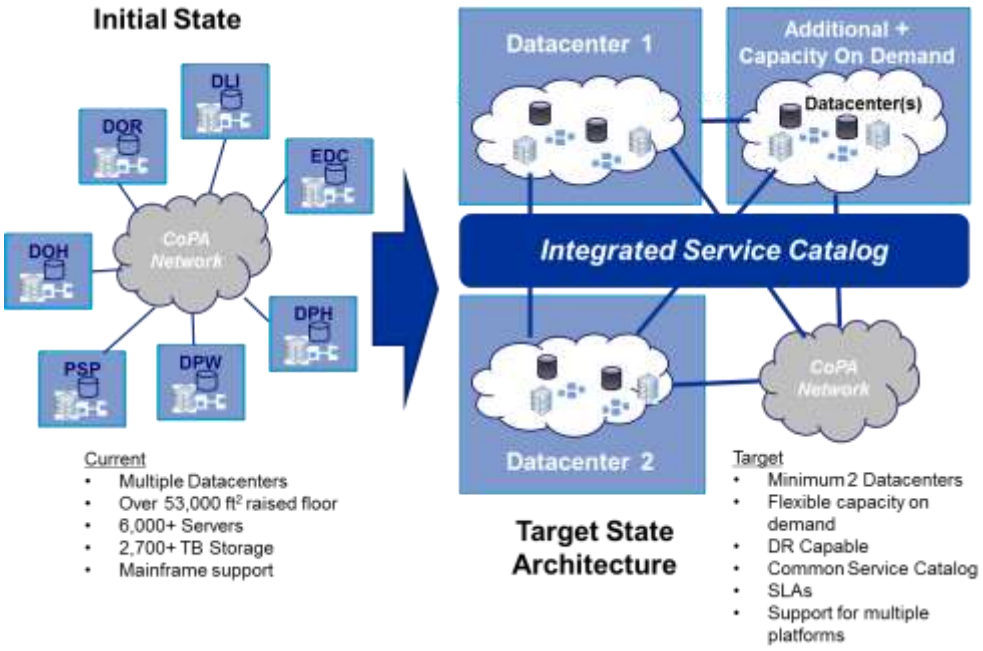
2.2 Solution Requirements Overview

A key outcome of the Commonwealth datacenter strategy is to transition from the current individually managed datacenters with different levels of service to enterprise level datacenter architecture with a common set of basic Services combined with available specialized Services dependent upon specific customer requirements. To facilitate this request for Services, the Commonwealth has structured the solution requirements into three areas, as follows:

- Transition Services;
- Datacenter 2+ Architecture (includes operations support for the Commonwealth's EDC); and
- Common Services Portfolio

2.2.1 Datacenter 2+ Architecture

The Contractor's architecture must leverage a minimum of two geographically separated datacenters located in the continental United States that would allow for enhanced disaster recovery capabilities as well as leverage excess capacity (virtual capacity on demand). The Commonwealth requires that the architecture include operations support for the EDC. The Contractor must be able to leverage additional capacity from other datacenter resources within its provider network to satisfy the needs of the Commonwealth. The architecture must support multiple computing platforms including but not limited to x86 (physical and virtual), midrange, mainframes, and storage systems. All of the Commonwealth computing workloads must be transitioned from the current state to the new target state architecture.



The 2+ datacenter architecture must include secure redundant network connections to the Commonwealth's network and the Internet. Contractor network connections must terminate at different end points within the Commonwealth's network. The Contractor must implement a multi DR solution to limit the impact of any disruptive event at any datacenter location. This requirement is targeted for all systems that are currently covered by a DR solution. The solution must also have the capability to support future disaster recovery requirements by providing tiered DR capability within its datacenters.

Each datacenter must have the ability to support multiple security and network zones to support specific agency requirements. For example: access, web, application, and data zones. The specific configuration and number of individual zones may be different per agency and application.

To support the potential of future demand and Services beyond the capacity of the two datacenters, the Contractor must be able to leverage additional capacity from other datacenter resources within its provider network.

2.2.2 IP conversion strategy

The Contractor must provide an IPv6 strategy which includes an enterprise migration plan to take the Commonwealth from the IPv4 address format to the IPv6 format.

The Contractor must provide infrastructure and equipment that supports IPv6 andIPv4, except were limited due to the requirement that the Initial transition approach of the Commonwealth's mainframe and SAP environments must be as close to the Commonwealth's current configuration as possible. As technology refreshes replace this equipment, the infrastructure and equipment must support IPv6 andIPv4

2.2.3 Common Services Portfolio

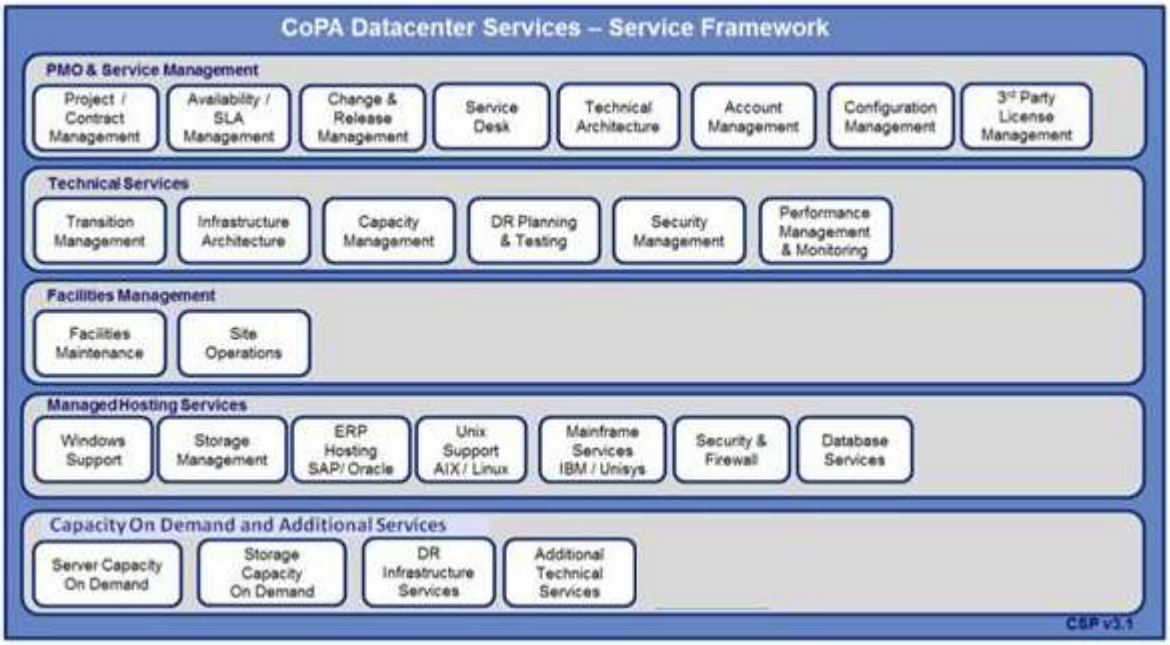
Based on the review of current and future requirements as well as industry offered Services; the following five (5) Key Services Areas must be used as a framework for the new datacenter common portfolio of Services.

Key Service Area Framework

	Key Service Area	Service Overview
1	Program Management Office (PMO) & Service Management	Provides for overall project management and operational service management (e.g. PMO, Account, Availability, Service Level Agreement (SLA))
2	Technical Services	Technical support services resources (e.g. Transition Management, Infrastructure Architecture, Capacity Planning)
3	Facilities Management	Facility operational support services (e.g. Facility Management, Operations Support)
4	Managed Hosting Services	Managed hosting/platform services for existing and future applications (e.g. Windows, Unix, SAP Hosting, Mainframe)
5	Capacity on Demand and Additional Services	Provides for additional capacity on demand offerings to support disaster recovery or increased demand for server and storage infrastructure (e.g. Cloud-centric offerings, Infrastructure as a Service (IaaS), Platform as a Service (PaaS)). Also access to additional skilled technology resources if required.

The Contractor is required to provide a complete set of Services within these service areas. The Services are presented below and the requirements are further detailed in the Task section that follows.

Expanded Services Framework



2.2.4 Data Protection

The Contractor must provide security of Commonwealth data. The Contractor must ensure that all data (at rest and in transit) is kept secure and confidential. If Contractor's solution involves data residing or routing outside the continental United States; the Contractor must meet the security requirements as described in this Contract to ensure the data is kept secure and confidential.

The Contractor must provide data protection Services including Data Loss Prevention (DLP) and Database Firewall (DBFW) Services to identify, monitor and protect sensitive and confidential Citizen Personal Identifiable Information (PII) in use, data in transit, and data at rest through deep content inspection and analysis of information exchange both at data storage locations and administrative/access endpoints.

Reference Documentation

N/A

Requirements

1.	The DLP service must: a) Discover confidential data wherever it is stored, inventory sensitive data, and automatically manage data cleanup. b) Monitor confidential data usage and provide enterprise visibility. c) Enforce security policies to proactively secure data and prevent confidential data from leaving Commonwealth systems. d) Manage policies across the enterprise, remediate and report on incidents, and detect content from centralized management platform. .
2.	The DBFW service must: a) Alert or block database attacks and abnormal access requests, in real time to protect against database attacks including SQL injection, Buffer overflow, Denial of Service. b) Detect and patch database software vulnerabilities c) Provide both agent based and network based database activity monitoring. d) Audit all access to sensitive data by privileged and application users, and enforce corporate policies on data usage e) Provide centralized management and advanced analytics f) Discover new databases and database objects in scope for security and compliance projects and automatically apply appropriate protection and audit policies
Deliverables	
Deliverables are defined in **Schedule K – Key Program Deliverables**	

2.2.5 Transition Services

Transition to the new baseline datacenter architecture and common Services portfolio must be carefully planned and executed. The Contractor is required to provide a proven methodology and plan to establish the target environment and then conduct an orderly transition of existing infrastructure and Services to the new environment.

The Contractor must transition Services from the incumbent contractor where there is an incumbent contractor, as well as, transitioning Services located at the Commonwealth managed datacenters. The Contractor must identify critical success factors and risk mitigation strategies, and describe how it must coordinate and manage other Commonwealth contractor related activities impacting the Contractor's plan. The Contractor must provide an estimate of any required Commonwealth resources, including the skills needed and the duration required for each of the resources required in order for the Contractor to implement its solution. The Commonwealth expects to provide limited resources.

The Contractor must thoroughly plan, evaluate and provide comprehensive and realistic activities and timeframes for accomplishment of transition activities given identified parameters within the Commonwealth's requirements as described in **Schedule K - Key Program Deliverables** and **Schedule D - Transition Milestones**.

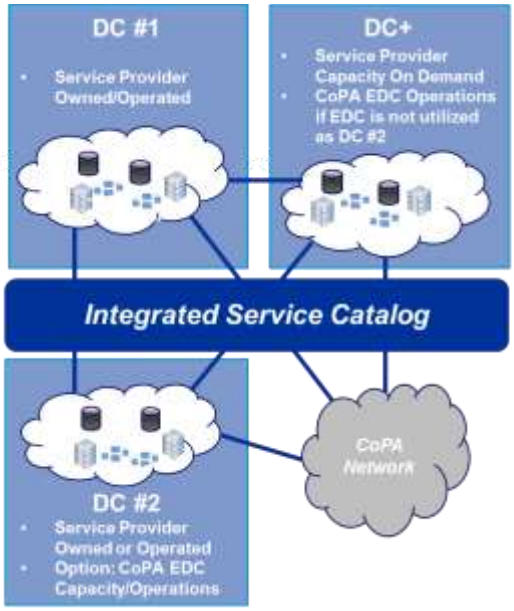
3 Tasks

3.1 Establish Datacenter Architecture

The Contractor must provide a multi-datacenter, multi-platform solution that must support the migration of all of the Commonwealth's current workloads. In order to support future Services, the Contractor must lead the Commonwealth into the future, and be able to address all current and future datacenter requirements. The Contractor must provide cost-effective, efficient, and forward-looking technologies for integrating Services. The Contractor must also address how it must allow for service updates and new technology offerings. The Contractor must describe how it must perform sizing exercises for different infrastructure to ensure the Commonwealth is getting a minimum of "like for like" or increased computing capabilities.

Baseline Architecture

In an effort to simplify the administration of IT assets, reduce IT costs, improve the provisioning of IT Services, and, in general improve the quality of IT Operations, the Commonwealth has established a preferred datacenter baseline target state architecture.



Baseline Datacenter Architecture

- Minimum 2 Datacenters
- Manage the CoPA EDC within architecture
- Flexible capacity on demand
- Redundant Secure Network Links between Datacenters and CoPA Network
- DR Capable
- Common Service Catalog
- SLAs
- Support for multiple platforms

The datacenter baseline target state architecture is based on a shared Services model in which a minimum of two geographically-separate datacenters (includes operations support for the EDC) provide a wide range of common IT Services to the Commonwealth. While not necessarily mirror images of each other, each datacenter must be capable of supporting critical

Commonwealth processing in the event the other datacenter goes offline (as, for example, in the event of a datacenter disaster). To address the need for additional capacity and new Services over time the Contractor may provide additional capacity beyond the two datacenters with secure connections to other Contractor capacity.

Initially, this target datacenter combination would host the Commonwealth's existing collection of shared information systems and currently outsourced Services. Over a prescribed period of time, the new datacenter architecture must support the transition of additional IT workloads presently being processed at a variety of datacenters owned and operated by Commonwealth agencies, thus permitting these datacenters to be decommissioned.

3.1.1 Multi Datacenter Environment (2+ Architecture)

The Contractor must provide a multi datacenter environment. All datacenters must be managed and maintained by the Contractor, including the Commonwealth's EDC and may be either a standalone facility, or integrated into existing qualified facilities. The multi datacenter environment is to facilitate high availability, capacity on demand, and the recovery of applications and Services that are deemed critical to the Commonwealth. The multi datacenter requirement is to provide a minimum of two datacenters. The Contractor may provide additional capacity and Services utilizing additional facilities beyond the two required datacenters.

Reference Documentation

Schedule E – Data Center Locations

Requirements

1.	The Contractor's datacenter architecture must consist of multiple geographically disbursed datacenters. Any datacenters being used in a back-up function must be at least 50 miles apart from the associated primary location for the service. Using **Schedule E – Data Center Locations**, the Contractor must list the address of all Datacenter locations from which the Contractor will provide the Services.
2.	
3.	The Commonwealth Equipment must be managed and maintained by the Contractor.

4.	Each datacenter must have the capability to provide DR for the other, for identified critical applications.
5.	The Contractor must utilize appropriate methods to achieve datacenter sustainability, such as realizing a low Power Usage Effectiveness (PUE) ratio.
6.	Each datacenter must have robust physical security, including biometric access control, video surveillance, and routine security officer patrols.
7.	In a datacenter environment that hosts both Commonwealth and non-Commonwealth clients, Contractor must provide segregation of Commonwealth data and computing resources from other clients' data and computing resources. The Contractor is required to provide system and data segregation between different agency application environments. The Contractor may not use the EDC to provide services to Non-Commonwealth clients. The Commonwealth may permit the Contractor to provide services to COSTARS members if written permission is granted by the Commonwealth.
8.	The Contractor must utilize elastic datacenter infrastructures to accommodate variable workloads.
9.	The Contractor must provide 24/7/365 staffing, (e.g. Operations staff, technical support staff, security staff, and management.) The Contractor must manage security/background checks, monitoring and reporting on employees and coordinate those requirements with Criminal Justice agencies.
10.	The Contractor must accommodate meeting and workspace for Commonwealth and Contractor IT staff and management.
Deliverables	
Deliverables are defined in **Schedule K – Key Program Deliverables**	

3.1.2 Network and Security Architecture

Secure and robust network connections are critical to the overall datacenter architecture. Connections between the datacenters and access to the Commonwealth's network must be planned, established, and tested prior to the transitioning of Services. All Contractor datacenters and locations must coordinate connections between the Contractor's network and the Commonwealth's fiber network (COPANET).

Reference Documentation

N/A

	Requirements
1.	All datacenter locations must connect to and provide access from COPANET.
2.	The Contractor must provide dual network termination points to connect to COPANET.
3.	The Contractor must provide network security via firewall and security devices.
4.	All Contractor datacenter facilities must have secure Internet access capabilities. Internet access must provide virus and intrusion protection systems with reporting capabilities.
5.	Multiple security zones must be configured within each datacenter to support specific agency requirements. For example: access, web, application, and data zones. The specific configuration and number of individual zones may be different per agency and application.
6.	Secure connections are required for traffic that may traverse between Datacenters and between Datacenters and Commonwealth. Encryption must be a minimum of 128-bit and must be FIPS 140-2 certified to meet Criminal Justice Information Services (CJIS) requirements. (Refer to Pennsylvania State Police (PSP) Summary of CJIS Requirements and CJIS Security Policy.)
7.	Remote access to datacenters supporting CJIS systems must meet minimum security requirements identified in CJIS Security Policy. These requirements include but are not limited to identifying remote user's identity, IP address and connection must be FIPS 140-2 certified with a minimum of 128-bit encryption.

Deliverables
Deliverables are defined in **Schedule K – Key Program Deliverables**

3.1.3 Datacenter Architecture and Technology

The Contractor must evaluate the Commonwealth computing infrastructure(s) and develop and implement an IT architecture that must support all current systems and applications, utilizing existing and/or underutilized technologies where appropriate, to provide a high level of quality computing Services to the Commonwealth, in a cost effective manner. An overall review of all Commonwealth computing Services is required, as the requirement is to consolidate all Commonwealth based computing Services into the Contractor's datacenter architecture. This architecture design is to include the current DR programs and structure and must be implemented along with the production and testing environments.

The Contractor must provide a multi-platform solution that must support the migration of all of the Commonwealth's current workloads. The Contractor must create a target environment that minimizes application latency concerns.

The Contractor must also develop an infrastructure environment, which must lead the Commonwealth into the future, and be able to address all current and future datacenter requirements.

Reference Documentation

Schedule J.1 – Data Center Service Level Management

Schedule J.2 – Data Center Service Level Matrix

Schedule J.3 – Data Center SLA Definitions

Requirements

1.	The Contractor must develop the architecture and define the technology to support the Commonwealth computing systems.

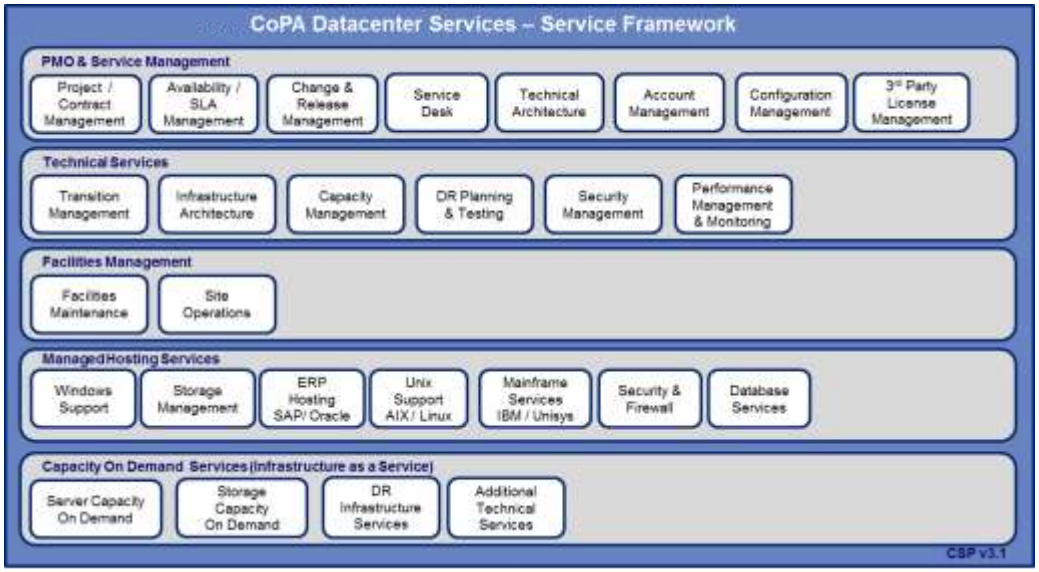
2.	The Contractor must Provide all technical system support and reporting including: • Multi-Platform Systems Support • Multi-Tiered Storage Management • Network Management • Security Management • Capacity planning • Performance analysis and tuning • Technology Refresh/Life Cycle Management • Annual Audits and Certifications
3.	The Contractor must provide a storage management approach which meets the Commonwealth's needs. The storage management approach must include, but not be limited to, the following: • **Basic** – based on Pay-As-You-Go allocation model with no upfront resource allocation and resources are reserved on demand per workload. (shared, multitenant) • **Committed** – based on Allocation Pool allocation model which gives a minimal initial commitment of resources plus the ability to burst above that minimum if additional capacity is needed – usually a percentage of resources reserved for agency with over-allocation. (shared, multitenant) • **Dedicated** – based on Reservation Pool allocation model – 100% of resources are reservation–guaranteed. (dedicated, single tenant)
4.	The Contractor must provide real-time monitoring and monthly reporting of system availability, performance, utilization, efficiency, and capacity reporting for the entire datacenter architecture.
5.	The Contractor must provide a tiered Disaster Recovery ("DR") solution to ensure that applications and associated hardware that currently have an active DR plan will continue to have offsite Services available in the event of a primary system outage. The tiered DR solution must include an option to support high availability (HA) architectures. The tiered DR solution must be in the overall datacenter architecture design.
6.	Configuration Item Reconciliation: The Contractor must perform an initial asset review of the targeted inventory for all datacenter configuration items (CI) that will be managed. The Contractor must reconcile and validate that appropriate relationships exist for all datacenter configuration information in the Configuration Management Database (CMDB) system. Contractor must ensure that CIs are properly mapped in order to support the established Service Level Agreements (SLAs). The Contractor must provide an automated interface between its CMDB and the

	Commonwealth's CMDB.
Deliverables	
Deliverables are defined in **Schedule K – Key Program Deliverables**	

3.2 Enable Common Service Portfolio

The Commonwealth requires that the Contractor's service management practices be based on the ITIL v3 framework and guidance. The Datacenter Architecture, which conforms to a service-oriented structure, is prescribed by the Commonwealth common service framework. The common service framework is comprised of 27 discrete IT Services divided into five (5) categories of service:

- **PMO & Service Management** – This category of service defines the overall datacenter management structure, including interactions with the Commonwealth and business partners.
- **Technical Services** – This category of service defines the datacenter architecture, and prescribes standards for datacenter continuity and security. This level also defines the workload transition process, for when Commonwealth Agencies migrate applications to the new datacenter computing Services model.
- **Facilities Management** – This category of service defines day-to-day datacenter operations and maintenance.
- **Managed Hosting Services** – This category of service defines a set of Commonwealth enterprise datacenter managed Services, each designed to accommodate the specific needs of the Commonwealth.
- **Capacity On Demand and Additional Services** – This category of service defines a set of infrastructure as a service (IaaS) offerings, each designed to provide just-in-time resources to the Commonwealth.



3.2.1 Program & Service Management

3.2.1.1 PMO & Contract Management

The PMO & Contract Management service is responsible for the overall program, projects, and contract elements, and must maintain an active working relationship with the Commonwealth project team. Contractor must assign an executive management team that must drive the processes to complete the due diligence required to make informed decisions and Services offerings that must meet the needs and requests of the Commonwealth. This executive team must also provide ongoing direction and leadership supporting the contract and designated Services, for the duration of the Contract.

The Contractor is required to provide and maintain operational, technical, and management staff contacts so that it is clear to the Commonwealth whom is the most direct contact for each operational area.

Reference Documentation

Schedule H - Commonwealth Computing Procedures Manual

Requirements

1.	The Contractor must establish and maintain a program and project management framework, throughout the term of the contract.

2.	The Contractor must establish and maintain a protocol for project estimation: ▪ Scope ▪ Hardware / Software ▪ Manpower to develop, test and implement ▪ All other resources required
3.	The Contractor must collaboration meetings, technical exchanges, and forums: Through established procedures and meetings address in good faith all issues, needs, technical exchanges and forums with the Commonwealth team. Provide the technical knowledge, and knowledgeable staff, to effectively support and guide the Commonwealth's technology needs.
4.	
5.	The Contractor must establish interim contract management procedures during the transition of datacenter Services to monitor and manage service delivery (conforming to Commonwealth policies and procedures) including but not limited to the following; Problem Management, Change Management, Service Level monitoring and reporting, physical and logical security, project management, etc. while the service is transitioned from the Commonwealth to the Contractor. All interim contract management procedures must be negotiated in good faith and approved by both parties.
6.	The Contractor must establish and maintain a process for change management for the Datacenter contract as requested or required. The final process developed must be coordinated with the Commonwealth contract compliance group and mutually agreed to by both parties.
7.	Subcontractor Relationship Management: The Contractor must establish and enforce standards for ensuring subcontractor performance. The Contractor is responsible for all Services provided by subcontractors.
Deliverables Deliverables are defined in **Schedule K – Key Program Deliverables**	

3.2.1.1.1 Financial Management

The Contractor must provide financial management for Services to provide accurate and cost effective stewardship of IT assets and resources. Financial management must be used to plan, control, and recover costs expended in providing the Services. Overall, the goal of financial management is to offer a truly transparent analysis of the Commonwealth spending on Services. This analysis of efficiency must be capable of being used to create intelligent, metric-based cost-reduction strategies.

Clear and transparent invoicing, both for the Commonwealth and for individual agencies, is required to insure integrity and accountability of all invoices. It is expected that invoicing may vary somewhat on a monthly basis whenever Services are either increased or decreased.

The Contractor must work with the Commonwealth to identify major investments as part of the budgetary planning process. The Commonwealth must review strategic and tactical objectives as indicated in the planning process to measure impact on its budget(s).

A significant percentage of the Commonwealth's funding comes from federal sources. Contractor must provide detailed service information necessary to ensure the uninterrupted flow of federal funds.

On a monthly basis, the Contractor must present the Commonwealth with a single enterprise invoice and multiple agency invoices for chargeback purposes. The agency's invoices must include sufficient detail to validate and accurately allocate charges to funding sources based on actual usage.

The Contractor is required to capture and provide information related to monthly volumes of work, counts, and utilization of specific infrastructure areas. The Contractor and the Commonwealth will develop a set of detailed, equitable and repeatable chargeback procedures for each provided Service based on either actual monthly utilization or allocation methods depending on which is most appropriate. The chargeback procedures must include the ability to map to discrete programs and funding sources identified by agencies with this requirement.

The Contractor must leverage any current chargeback procedures and implementation configuration to accelerate the implementation of the new process. The Contractor must expand the chargeback system to capture all related computing related charges associated with the Datacenter project.

Reference Documentation N/A	
Requirements	
1.	The Contractor must provide a uniform rate structure for the Services.
2.	The Contractor must provide monthly invoicing for Services to the Commonwealth. The Contractor must provide invoices that identify Services rendered, pricing, and agency specific service usage. The Contractor must connect to the Commonwealth's ITSM system. The Commonwealth does not require a full charge back system. The agency invoices must provide billing detail so the agency has full transparency into the services it consumed. Billing details must include all services procured by agency general ledger (GL) code. A Service may be allocated across multiple GL codes. Adjust agency level billing due to failing to meet SLAs.
3.	Invoices must reflect when Services are either increased or decreased.
4.	The Contractor must follow Interim Financial Management procedures for providing invoices, invoice verification and charge back to datacenter customers including but not limited to the following; service components, asset management, asset transfer, forecasting, etc ,as the Commonwealth transitions its current architecture to the Contractor's Services.
5.	The Contractor must provide cost effective approaches and suggestions to improve Services while maintaining or lowering the cost for Services.
6.	The Contractor must integrate Financial Management with other service management processes, especially with SLA, Capacity and Configuration Management.
Deliverables	
Deliverables are defined in **Schedule K – Key Program Deliverables**	

3.2.1.1.2 Governance & Policy Compliance

Major IT decisions related to this Contract must be reviewed and approved according to the Commonwealth's governance policy.

Reference Documentation

Schedule B - Governance

Requirements:

1.	Major IT decisions must be made under the guidance of the Commonwealth governance organization.
2.	Design and architecture decisions must be made with a high level of integrity and advance the interests of the Commonwealth. All designs must be approved by the Commonwealth.
3.	All policies and procedures must be executed in a consistent manner to ensure the Services are completed as planned and consistent with specifications. Audits must be conducted on a yearly basis to verify and report on compliance with policies and procedures.

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

3.2.1.1.3 Subcontractor Management

The Contractor may provide some of its Services and offerings via subcontractors. The Contractor must be the prime provider of Commonwealth Services, and is responsible to contract with subcontractors, manage its subcontractors, and for Contractor's performance and the performance of its subcontractors throughout the term of the Contract.

Reference Documentation

N/A

Requirements

1.	The Contractor must obtain, manage, and be responsible for all Services or offerings provided by subcontractors. Subcontractors may change over the course of this contract. Contractor is required to notify the Commonwealth of the new subcontractor(s) and assure the Commonwealth that there will not be a conflict of interest, and that the new subcontractor meets or exceeds the qualifications of the replaced subcontractor. The Commonwealth must approve all subcontractors.
2.	CJIS Security Policy requires fingerprint based background checks and executing a Management Control Agreement (MCA) and Security Addendum with the Pennsylvania State Police (additional information is provided in the PSP exhibit material).

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

3.2.1.1.4 Business Partners Management

The Commonwealth has business partners such as banks and insurance companies that require connections to its hosted systems and applications. The Contractor must coordinate with the Commonwealth to support any Commonwealth – Business Partner agreements that require a committed connection to its hosted systems.

Reference Documentation

N/A

	Requirements
1.	The Contractor must provide coordination and support of Commonwealth – Business Partner agreements that require connections and Services to the Contractor's datacenter Services to ensure that any committed connections and service levels are maintained.

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

3.2.1.1.5 Additional Planning Services

The Commonwealth may use different/additional methods for requesting technical information and support. Depending on the type of request those methods could include but not be limited to:

- Statement of Objectives (SOO)
- Work Order
- Service Request
- Request for Technical Analysis
  - Cost-Benefit Analysis
  - Conceptualization
  - High Level Estimate (HLE)
  - Technical Opinion(s)

Reference Documentation

N/A

Requirements	
1.	Statement of Objectives - The Contractor must perform requested additional Services across various functional areas, where the work requires funding either because of materials needed or because the activity requested is not part of the base contract.
2.	Work Orders - The Contractor must perform work across various functional areas, where the work is considered part of the base contract and where no additional funding is required.
3.	A Service Request will be used to request work within one functional area, where the work is considered part of the base contract and where no additional funding is required.
4.	Requests for Technical Analysis will be used to seek information regarding potential technical solutions. The documents generated by the Contractor must provide the Commonwealth with direction regarding a specific technology and possibly the estimated cost to implement the solution. Four types of requests for technical analysis may be made by the Commonwealth. These requests are described below: • Cost-Benefit Analysis - A cost-benefit analysis is requested when the Commonwealth wants to know not only the implementation cost of a solution, but also the cost-benefit ratio for Commonwealth implementation of the solution. It may be used to analyze a single solution against the status quo, or compare the relative costs of multiple solutions.

	• Conceptualization - A conceptualization is requested when the Commonwealth has an objective, but is unsure about the possible technical means of fulfilling it. The Contractor must examine multiple paths for achieving the objective, and provide the technical benefits and consequences of the possible solutions presented. Costs are not considered in a conceptualization. • High Level Estimate (HLE or sometimes referred to as a rough order of magnitude ROM) - A HLE is requested when the Commonwealth has a clear technical direction and needs rough estimates on the cost of implementing it. HLEs may be used to attach a cost estimate to a prior conceptualization or technical opinion produced by the Contractor. • Technical Opinion(s) - A technical opinion is requested when the Commonwealth has a specific technology or set of technologies it wants the Contractor to analyze for both technical merits and suitability for deployment in the Commonwealth environment. While product and operational costs provided in Contractor's literature may be considered in a technical opinion, the Contractor's deployment and operational costs must not be calculated or presented.
Deliverables	
Deliverables are defined in **Schedule K – Key Program Deliverables**	

3.2.1.1.6 Continual Service Improvement

The purpose of the Continual Service Improvement is to reduce risk, improve service quality, improve client satisfaction, and ensure service transparency through a continuous cycle of evaluation and improvement.

Reference Documentation

N/A

Requirements:

1.	Related to the project management and contract management role, the Contractor must provide Continual Service Improvement to reduce service risks.
2.	The Contractor must provide Continual Service Improvement to improve service quality.
3.	The Contractor must provide Continual Service Improvement to improve client satisfaction.
4.	The Contractor must provide Continual Service Improvement to ensure service transparency.
5.	Customer Satisfaction Surveys – Survey of Service Desk satisfaction is a key component of providing best in class customer service. The Contractor must perform surveys of Service Desk satisfaction for a subset of the problems, questions, or requests that are resolved by, or coordinated by, the Service Desk. The Contractor must create and advertise a web site for day-to-day feedback from datacenter customers which is accessible through the Contractor's KMP. The Contractor must perform customer satisfaction survey on a quarterly basis. The Contractor must receive completed surveys of Service Desk satisfaction from the Commonwealth and tabulate results from such surveys.
6.	The Contractor must provide Continual Service Improvement to improve/reduce costs.

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

3.2.1.2 Availability/SLA Management

The purpose of the System Availability and SLA function is to ensure that each service is delivered within, or exceeds, the agreed availability service level, and prescribed credits are received by the Commonwealth when the service level has not been achieved. Availability Management provides a point of focus and management for all availability related issues, ensuring that availability targets are established, measured, and achieved. The basic requirement is to balance the value and quality of Services with the costs of the Services. Availability and SLA management will be responsible for establishing and reviewing the SLA's to meet the Commonwealth's requirements. Contractor should review referenced exhibits for a list of SLAs and associated descriptions, tools and methodologies.

Availability/SLA Management ensures that datacenter service availability standards, as prescribed in appropriate datacenter SLAs, are achieved.

Reference Documentation

Schedule J.1 - Data Center Service Level Management

Schedule J.2 - Data Center Service Level Matrix

Schedule J.3 - Data Center SLA Definitions

	Requirements	**Describe Compliance**
1.	The Contractor must establish a formal Availability and SLA Management service. This service must include representatives from the Contractor and the Commonwealth for reviewing and approving the availability and SLA metrics. Contractor must publish the formal Availability and SLA Management plan based on a Service Catalog. This service must identify key Services and the associated level of availability or capacity as appropriate, identify the Services that will be measured by an SLA, and define the basis on which the SLA service levels will be monitored and obtained. The Contractor must obtain approval from the Commonwealth.	

2.	The Contractor must use Service Level Measurement Tools to measure and report Contractor's performance of the Services at a level of detail sufficient, as determined by the Commonwealth, to verify Contractor's compliance with those Service Levels described in **Schedule J.3 Data Center SLA Definitions.** The Contractor must review and update the required sections within Schedule J.3 Data Center SLA Definitions. The Contractor must complete the following sections in each of the Critical Service Levels and Key Measurements: • Collection Process – identify how the measurement data must be collected • Reporting Tools – identify any tools, automated or manual, that must be used • Raw Data Storage (Archives) – identify where data must be stored and accessible by the Commonwealth for further analysis. The Contractor is responsible for storing raw data used to generate SLA reports for the duration of the contract plus 3 years. The Contractor must make that raw data available to the Commonwealth via the Contractor hosted knowledge management portal for no-less than the most recent 13 months. Data older than the most recent 13 months must be provided on request in a format prescribed by the Commonwealth within 5 business days of the request. • Reporting Format/s – identify the proposed reporting format
3.	Contractor's Availability Management process must integrate Availability Management with other service management processes, such as SLA, Capacity Management, Problem Management and Service Desk.
4.	The Contractor must establish automated non-compliance indicators. The Contractor's process for managing Services performance must automatically e-mail the designated Commonwealth contact when SLA service parameters are not met. The Contractor must create email notification groups by major service. The Contractor must utilize this, or a similar process for outage notification.

5.	The Contractor must investigate all instances of non-compliance. The Contractor must notify the Commonwealth of an outage as defined in the CCPM. The Contractor must complete a root cause analysis (RCA) for all major outages, and provide a detailed report to the Commonwealth and impacted user. Completion of the Incident report must occur within 2 days of the incident and the RCA within 10 days of the incident.
6.	The Contractor must use integrated tools, methods, and activities for reporting service and component availability. The Contractor must ensure proactive measures to improve availability of Services are implemented whenever it is cost justified.
7.	The Contractor must integrate Agency Availability Management processes with SLA Management. On a monthly basis, the Contractor must consolidate all system SLA availability reports into a management operations report, summarizing availability, outages, and SLA compliance by platforms.
8.	The Contractor must develop and maintain a Portal/Website for agencies to view operational status, planned maintenance, and component level outages.
Deliverables	
Deliverables are defined in **Schedule K – Key Program Deliverables**	

3.2.1.3 Change & Release Management

Change & Release Management ensures that all changes within the datacenter environment are planned, executed, monitored, documented, and that the change produced the intended effect. The Contractor must establish the overall Change & Release Management function and manage the daily operations of the functions. This must ensure that all changes are processed in a uniform manner that required documentation, approvals, and notifications are completed before the change is implemented within each of the lower infrastructure environments and then moved into the production environment. Post implementation review and approval requires that all steps have been completed as documented, and within the time frame allotted. All change and release documentation must be maintained in a manner that facilitates random compliance auditing. On a yearly basis, random selections of changes must be audited for compliance purposes.

Reference Documentation

Schedule H - Commonwealth Computing Process and Procedures Manual

	Requirements	Describe Compliance
1.	The Contractor must establish a formal Change & Release Management function. This function must include representatives from the Contractor and Commonwealth to support the review and approval of all changes. Contractor must publish the formal Change & Release Management plan. The Contractor must identify key elements and roles; Request for Change Form & Process, Change Manager, Change Advisory Board, Emergency Change Advisory Board, Notification process, Change review process. The documentation and process must follow industry best practices. The Contractor must train appropriate Commonwealth staff on the process as requested by the Commonwealth. The Contractor's Change Management & Release management process must consider and integrate with the Commonwealth's individual change management policies and procedures, for example from January to May of each year, Department of Revenue (DOR) maintains a "no update policy" to DOR servers that have any production Tax-Related Applications running on them.	
2.	The Contractor must institute a Change Advisory Board (CAB).The CAB members must ensure that the requested changes are thoroughly checked and assessed from both a technical and business perspective.	

3.	The Contractor must test infrastructure related changes & releases before implementation. This includes Contractor managed hardware and any Contractor managed software. The Contractor must file a Pre-Change Test Plan, as part of the Change & Release request process, including results before final approval to proceed. The Contractor must create and maintain test environments where testing must be conducted and evaluated prior to implementing any change into production environments.
4.	The Contractor must establish and manage scheduled maintenance periods, and communicate the scheduled outages. The Contractor must create a notification process for maintenance, emergency, and unplanned outages. The Contractor must establish regular maintenance periods for each computing platform. Maintenance periods must be coordinated per agency due to different peak business requirements. The Contractor must create mechanism to notify clients of expected and unexpected outages. .
5.	The Contractor must notify affected Commonwealth agencies before and after any changes. The Contractor must provide Change & Release Notifications prior to implementation via a central web site and e-mail.
6.	The Contractor must Validate all changes after implementation. The Contractor must complete a post change review to validate the success or failure of the change or release, and post the information within the change record. Take follow up action as appropriate.
7.	The Contractor must prepare back out procedures for all changes. As part of the Change & Release process, the Contractor must file a back out plan as appropriate to remove the change and restore Services to the prior level.
8.	The Contractor must track all (successes / failures) changes and produce Change &

	Release management statistics. The Contractor must create and deliver a monthly Change & Release Management Report to the Commonwealth, detailing changes, implementation status, and outage time periods as compared to planned outage schedules.
Deliverables	
Deliverables are defined in **Schedule K – Key Program Deliverables**	

3.2.1.4 +Service Desk

As part of the Services, Contractor must provide telephone support (e.g., a "Service desk") to the Commonwealth to assist the appropriate end users in determining, tracking and resolving questions regarding the Services. Contractor must provide telephone support through such telephone support infrastructure maintained by the Contractor. This telephone service desk is to augment the required "online" Service Desk capabilities as set forth in the RFP.

The Service Desk must be the single point of contact for authorized Commonwealth users regarding incidents, which include events that cause or may cause an interruption or reduction of service, as well as requests for information, and requests for Services relating to all of the Services provided within the Contractor's catalog of Services. The Contractor's Service Desk must have processes for Service Delivery and Service Management that are ITIL-conformant. The Service Desk process includes Service Management processes: Incident Management, Problem Management, Change Management, Configuration Management and Service Request Management.

Currently most Commonwealth agencies provide a local Help Desk function to support staff's desktops, local printing systems, applications, and the general public users it serves. The majority of the agency Help Desks utilize the Commonwealth's Enterprise ITSM. A connection between the Commonwealth's Enterprise ITSM and the Contractor's Service Desk is required to keep Help Desk tools synchronized.

In addition, the Contractor must provide an Internet accessible KMP as a central repository for processes and procedures, communications plans, and other relevant documentation to be shared with the Commonwealth. Knowledge Management will be a function shared by the Commonwealth along with the Contractor. This must allow the Commonwealth to combine data from all Commonwealth agencies and the Contractor, reorganize it, make it understandable, and present it to the Commonwealth.

The Contractor must coordinate with the Commonwealth to provide feedback on the effectiveness and accuracy of KMP content. In addition, the Contractor must notify the Commonwealth when incorrect information is identified, reference material becomes outdated, or when the content is rendered inaccurate. At the Commonwealth's discretion, the Contractor may be required to develop content, as needed, including answers to frequently asked questions, reference/educational materials, and other documents to be added at the Commonwealth discretion.

The Contractor must create and keep current a CCPM that documents the processes, procedures and timelines used to meet the requirements of this contract. The CPPM must provide detailed process descriptions to support the computing needs of the Commonwealth utilizing best practices and be made available (via Contractor's Portal) to all Commonwealth agencies throughout the term of the contract.

Reference Documentation Schedule H - Commonwealth Computing Procedures Manual	
Requirements	
1.	The Contractor must provide an integrated Service Desk process with the other Service Management processes, including Incident Management, Problem Management, Change Management, Configuration Management and Service Request Management. The final Service Desk processes and procedures must consider current Commonwealth service management policies and procedures.
2.	The Contractor must provide a Service Desk with processes and tools for Service Delivery and Service Management that are ITIL-conformant.
3.	The Contractor must seamlessly integrate the Service Desk (including tools, technology and processes) with the Service/Help Desk(s) of other identified Agency Service Desks as required. The Contractor must coordinate the integration of the proposed Service Desk with the Commonwealth's Enterprise ITSM System. Integration with other agency ITSM systems is not required.
4.	The Contractor must analyze incident trends, and recommend and implement actions, with Commonwealth's approval, to reduce incidents.
5.	The Contractor must conduct random surveys of authorized users of the Service Desk in accordance with the Commonwealth each month.
6.	The Contractor must develop and document processes regarding interfaces, interaction, and responsibilities between Level 1 Support personnel, Level 2 Support personnel, and any other internal or external persons or entities that may either submit notice of an incident or receive notice of an incident.
7.	The Contractor must ensure staffing levels and work allocation remains appropriate to handle incident volumes and incident response targets.
8.	The Contractor must provide trained service desk personnel.
9.	The Contractor must ensure that the Service Desk is available at all times (i.e. 24 hours a day, 365 days a year).

10.	The Contractor must manage all Incidents and/or Service Requests from authorized users relating to Contracted Services.
11.	The Contractor must provide weekly reports to the Commonwealth on Service Desk activities, performance, and adherence to established SLAs. Service Desk reporting must include at a minimum: • Key issues relating to Service Desk processes, improvements, script development. • Status as to Service Desk staffing, training, and authorization. • Integration activities and issues with other Service Desks belonging to the Commonwealth. • Trend analysis must include (13) most recent months. If the Service has been in place less than thirteen months then trend analysis must include all months of Service. • Calculate metrics and provide monthly reports. • Number of Contacts, to include all interactions (Calls, phone calls, electronic, automated or otherwise). • Number of calls abandoned, average call duration, average time to answer, average time to abandon. • Number and percentage of Contacts resolved. • Number and percentage of Contacts passed to other Service Desks. • Other pertinent information regarding Service Desk operation and performance.
12.	The Contractor must enable a KMP accessible by all authorized users. Content for the KMP must be approved by the Commonwealth.
13.	The Contractor must record all incidents, problems, service requests, change requests, and configuration information in the software recording tool. All updates to the record, contacts with clients or vendors, and resolutions must be recorded in a real-time and consistent manner. This recording tool must house the KMP.
14.	The Contractor must monitor reporting system to ensure incidents and problems are being addressed to meet agreed SLAs.
15.	The Contractor must ensure alerts are transitioned successfully. Transition must include the transfer of system and application monitoring alerts with the ability to turn-off the problem alert process during maintenance windows and other scheduled outages.
16.	The Contractor must provide interim Support Desk Procedures to be used as the Commonwealth transitions from its current support architecture to the Contractor's

	Service Desk. The Contractor must provide Service Desk operation throughout the transition to the Contractor's fully managed service.
17.	Incident Management - The Contractor's Incident Management process must encompass Incident Management processes deployed across all Service Components that are designed to: restore service as quickly as possible, minimize disruption to the Commonwealth, aim for highest levels of availability and service quality, completely transparent and auditable delivery of service, and promote the highest level for user satisfaction.
18.	Problem Management - The Contractor's Problem Management Process must minimize the adverse effect on the business of Incidents and Problems caused by errors in the IT infrastructure, Applications, systems and supporting components, and proactively prevent the occurrence of Incidents and Problems by identifying and eliminating causes of failure.
Deliverables	
Deliverables are defined in **Schedule K – Key Program Deliverables**	

3.2.1.5 Technical Architecture

The Technical Architecture function will oversee the ongoing design of the various computing platforms that will support the Commonwealth's existing computing topologies, as well as plan for the approaching consolidation of the Commonwealth datacenters. The intent is to design an infrastructure which will ultimately utilize multiple datacenters for processing, tiered DR Services, and on-demand Services in a secure environment. At the conclusion of the design, and after approval by the Commonwealth, the Contractor must document the environment via a Service Catalog.

The Contractor must design the technical architecture of the computing systems based on current best practices, to support the evolving technologies and business needs of the Commonwealth. The volume of computing and storage will vary during the term of the contract due to applications development, testing, certification, the retirement of existing production environments, as well as cyclical processing demands such as the various tax seasons. The Contractor must be able to expand and contract service offerings based on Commonwealth needs

in a timely and cost effective manner.	
Reference Documentation N/A	
Requirements	
1.	The Contractor must create a Service Catalog. Define the Services and platforms to be offered. The Contractor must provide a detailed list of Services, via a common Service Catalog to be provided to the Commonwealth. The Contractor must utilize an industry standard software product to ensure the detailed service offering is recorded.
2.	The Contractor must design and build the IT architecture required to support the Services. The Contractor must design and build the IT technical architecture to support the Services selected by the Commonwealth. The Contractor must provide the design to the Commonwealth for review and approval prior to execution. All designs must be approved by the Commonwealth.
3.	The Contractor must design platform and support lifecycles. The Contractor must provide a technical support staff structure for the Services and platforms to be offered. Support must include all skills needed to plan, operate and support each technology platform.
4.	The Contractor must provide Technical Support Services. The Contractor must provide the skills of and the size of the support staff to plan,

	manage, and operate the various IT infrastructure platforms.
5.	Interoperability The Contractor must design architectures with system components that facilitate system data accessibility.
Deliverables	
Deliverables are defined in **Schedule K – Key Program Deliverables**	

3.2.1.5.1 Technology Refresh

Technology refresh is an ongoing activity required of the Contractor. The Contractor must prepare technology impact statements that address the key technologies planned for refresh or technologies identified to be of interest to the Commonwealth. These impact statements must provide a wide range of information, including the following matters applicable to the Contractor's environment:

- Technology trends
- IT Infrastructure Contractor releases and offerings
- IT Infrastructure Contractor retirement of older versions of products
- Proposed scheduling of Contractor releases into the datacenter environment
- Potential impact of the new releases on business applications in the datacenter infrastructure
- Potential impact of the new releases on deployment and operational processes
- Risk analyses with recommendations for mitigation of risks

The Commonwealth and the Contractor must review the impact statements. Based on these reviews, the Contractor must recommend a plan and schedule for technology refresh to the Commonwealth. Since the expected usable life of any hardware approved for the datacenter environment is about 36 months, the plan must project an 18-month window into the future, and include resource estimates for each recommended refresh activity. Software refresh will depend on software releases and the Contractor must ensure operational compatibility with existing Commonwealth applications and/or functionality or must provide upgrade alternatives and options. The Contractor must obtain Commonwealth approvals prior to implementing technology upgrades that will affect Commonwealth operations.

Reference Documentation

N/A

	Requirements	Describe Compliance
1.	The Contractor must document and update Technical Architecture approach and project plan including; Service Catalog, IT Architecture, and Technical support	
2.	The Contractor must review and refresh technology on a scheduled basis.	
3.	The Contractor must provide technical Architecture Staffing.	

Deliverables
Deliverables are defined in **Schedule K – Key Program Deliverables**

3.2.1.5.2 IT Service Continuity Architecture

The Contractor's IT Service Continuity Architecture must provide tiered DR capabilities and Services for applications that have been identified by the Commonwealth. The Contractor must provide a Service Continuity solution that includes DR computing, storage, networking systems and recovery processes and must be included in the overall Commonwealth architecture design. Only critical applications and associated equipment identified by the Commonwealth must be addressed with DR systems. Additional information regarding Tiered Service Delivery and Tiered DR can be found in referenced supporting exhibits.

The Commonwealth will lead the Business Continuity effort with assistance from the Contractor.

Reference Documentation

Schedule J.1 – Data Center Service Level Management

Schedule J.2 – Data Center Service Level Matrix

Schedule J.3 – Data Center SLA Definitions

Requirements	
1.	The Contractor's DR Architecture and Plan and Business Continuity Plan (COOP) must be documented by the Contractor and approved by the Commonwealth.
2.	IT Service Continuity Architecture and Plan - The Contractor must obtain Backup hardware and software and must be configured and available per an agreed to Service Level to process the identified critical applications. Where applicable, data must be electronically replicated (including disk-2-disk) to the backup systems (off site) to insure a successful recovery. Wherever data replication is not viable, backup tape data must be utilized.
3.	Recovery systems must be available via network access. Routing must be configured and tested during initial system architecture design. The Contractor must include the network requirements of the DR plan in the design

	of the network architecture.
4.	Recovery documentation for each identified system/ application must be required. Information must include the targeted backup hardware, software, networking changes, data location, restoration and access process, execution authorization, and notification to service owner when an application has been restored to service. The Contractor must create recovery documentation for each system / application identified as a critical system where DR is required.
5.	The Contractor mus creat a DR support plan. The Contractor's DR team must notify the Commonwealth when a recovery plan is to be put into action, and must manage questions and issues that may arise after implementation. The Contractor must create a DR team that manages the execution of the DR plan from declaration to recovery when required.
6.	For critical systems identified as having a current tested DR Plan within the DPH, the Contractor must update the associated DR test plans for the new target environment. Successful testing of each revised DR Plan is required prior to Commonwealth acceptance.
Deliverables	
Deliverables are defined in **Schedule K – Key Program Deliverables**	

3.2.1.6 Account Management

The Account Management function is responsible to provide each Commonwealth agency with oversight of the contracted Services and support required to satisfy the Commonwealth's computing needs. The Account Manager must provide direct interface with the Commonwealth agencies ensuring daily operations and needs are provided, and create monthly operational summaries reporting to both the agencies and the Commonwealth. This report must address all operational events and issues that occurred during the month that would have effected service level attainments, problems and incidents, and recommendations for changes needed to provide continuous, secure computing Services. Each Commonwealth agency will interact with its assigned Account Manager to discuss needs, issues, problems or costs.

Reference Documentation

Schedule G - Staffing Plan and Key Positions

Requirements		Describe Compliance
1.	The Contractor must assign an Account Manager to each identified agency. The Account Manager must be responsible for all Services provided, represent the Commonwealth agency's needs, and be the advocate for the agency throughout the Contractor's organization. Based on the size and application complexity of the Commonwealth agency, the Contractor must assign additional account management resources. Account Managers must understand agencies line of business and business trend analysis. The Contractor must assign a minimum of five (5) dedicated account managers.	
2.	Account Managers must meet with assigned agency contacts on a regular basis. This must be at minimum weekly during the initial program start and through transition.	
3.	The Contractor must meet with Commonwealth teams on a monthly basis. This must be at minimum weekly during the initial program start and transition to monthly meetings with the Commonwealth teams to address problems and assure continuous service improvements.	
4.	The Contractor must participate in agency-sponsored IT planning sessions on a quarterly basis. Contractor must schedule quarterly computing capacity reviews to ensure sufficient processing capacity, needs, and issues are being addressed. Suggest changes when necessary.	
5.	The Contractor must advocate for agency interests. Contractor's Account Management team must advocate for the Commonwealth's interests. For example, intervene with Service Desk personnel to resolve a major problem; problem escalation process, support root cause analyses process. Another example, coordinate with agency and service providers to ensure timing of technology refreshes have the least impact on the agency.	
6.	Monthly status reports - The Contractor must ensure The Commonwealth is aware of operational status and project update information on a monthly basis. The Contractor must create and deliver a monthly status report, summarizing operational metrics as defined in the CCPM, by service platform, including highlights and exceptions, and project status.	

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

3.2.1.7 Configuration Management

The Contractor's Configuration Management system must ensure complete and accurate recordkeeping relative to datacenter assets; hardware, operating system software, firmware, and network. The Contractor's Configuration Management Database (CMDB) system must be synchronized with the proposed datacenter Change and Release Management processes. Also included must be associations of infrastructure configuration items (CIs) and Agency application infrastructure to support application infrastructure related SLAs.

At the end of the contract the Contractor must provide the Commonwealth with a final electronic copy of the CMDB.

The following list identifies but does not limit the roles and responsibilities that the Contractor must perform:

- Define and document Configuration Management standards and procedures per ITIL v3 standards.
- Establish an electronic interface to the Commonwealth's CMDB(s) to keep current both the Commonwealth's CMDB and the Contractor's CMDB.
- Establish process for tracking configuration changes
- Establish process interfaces to Incident and Problem Management, Change Management, technical support, maintenance and asset management processes
- Establish appropriate authorization controls for modifying configuration items
- Establish configuration baselines as reference points for rebuilds, and providing ability to revert to stable configuration states
- Establish process for verifying the accuracy of configuration items, adherence to Configuration Management process, identify process deficiencies and recommend corrective actions

The Commonwealth must require online access to configuration related information and reports to satisfy application updates and audit requirements.

Reference Documentation

Schedule H - Commonwealth Computing Procedures Manual

Requirements		Describe Compliance
1.	The Contractor must provide a documented process to track configuration changes accordingly to ITIL V3 framework.	
2.	Per agency request, the Contractor must provide specific application related infrastructure component configuration information.	
3.	The Contractor must provide current configuration reports at an agency level by datacenter component.	
4.	The Contractor must perform continuous review and updates to the Contractor's and Commonwealth's CMDB to maintain accuracy of the CMDBs.	
5.	CMDB that constitutes the common repository created by the Contractor to include, but not be limited to, location information, service information, configuration information, application information, billing data, inventory data, and performance data. This data must be provided to the Commonwealth via electronic interface in a format approved by the Commonwealth.	

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

3.2.1.8 3rd Party License Management

Currently the Commonwealth manages over 2,000 business applications that require numerous software platforms and products. The Contractor's 3rd Party License Management service must ensure accurate inventory and licensing compliance for all Contractor provided infrastructure software products. The Contractor must be solely responsible for the management of all infrastructure software products provided through this contract.

The Contractor must coordinate with the Commonwealth to ensure compatibility between Commonwealth provided applications related software, and the Contractor provided infrastructure software. The Contractor must provide a method for tracking and reporting on both Contractor provided and Commonwealth provided software that must reside on the managed infrastructure.

The Contractor must provide the ability to purchase the Third Party Software listed in Exhibit B.4 - DPH - Third Party Software and additional third party software if required to provide the contracted services. The Contractor is responsible for the licensing and maintenance and support for the Third Party Software. The Commonwealth at its sole discretion may procure third party software from appropriate contracts.

The Contractor must provide the ability to purchase maintenance and support for the Third Party Software listed in Exhibit B.10 - DPH – Hybrid Third Party Software. The Contractor is responsible for the maintenance and support for the Third Party Software. The Commonwealth at its sole discretion may procure third party software maintenance and support from appropriate contracts.

Reference Documentation

Exhibit B.4 - DPH - Third Party Software

Exhibit B.10 - DPH – Hybrid Third Party Software

Requirements	
1.	The Contractor must provide, as requested, current software license reports for in scope infrastructure. For example specific OS version and patch levels per service instance.
2.	The Contractor must implement continuous service improvement process related to 3rd party software management to improve service quality, efficiency, and effectiveness.

3.	The Contractor must implement 3rd Party Software Management initiatives to achieve reduced costs of Services and to meet or exceeded ROI (Return on Investment) analysis projections.
Deliverables	
Deliverables are defined in **Schedule K – Key Program Deliverables**	

3.2.2 Technical Services

3.2.2.1 Transition Management (New Customer and/or Services)

The Transition Management service ensures the systematic planning, management, execution, and monitoring of major changes to the datacenter environment(s). This Services offering is to support new customers and/or new Services (i.e. remote file servers, remote databases, etc.). This service offering includes the phased migration of Commonwealth applications to the Contractor's managed service excluding initial transition.

Information and tasks pertaining to the transition of the initial Targeted Datacenters and Agencies can be found in Section 3.3 – Transition Services.

Reference Documentation

N/A

Requirements	
1.	Transition Management Office – The Contractor must create a Transition Management Office and team that must be responsible for the migration projects of hardware and applications from the Commonwealth's locations to the new target datacenter environments.
2.	The Contractor must create a computing environment; hardware, software, network systems, peripherals, and devices as required to migrate the Services from the Commonwealth.
3.	The Contractor must provide recommendations for the repurpose, replacement, or retirement of existing Commonwealth hardware, software, network systems, and peripheral devices as required after system migrations have been completed.
4.	Optimize Current Process and Procedures – The Contractor must coordinate with Commonwealth customer to review and plan for a transition of processes and procedures. The Contractor must implement a plan for optimization of the existing

	processes, procedures, tools, etc. to provide more efficient and effective Services.
5.	The Contractor must develop detailed plans to migrate Commonwealth applications, and associated infrastructure from Commonwealth datacenters to the Contractor's datacenters. On a monthly basis, the Contractor must create a report to detail the transition projects on the plan, status, risks, and the forecasted transition date.
6.	The Contractor must coordinate with Commonwealth applications project teams to plan and execute the application and infrastructure migration plans.
7.	The Contractor must revise datacenter disaster recovery plans on the occasion of major changes to the datacenter hardware, software, or network portfolio.
Continual Process Improvement	
8.	Related to the project management and contract management role, the Contractor must provide Continual Service Improvement to reduce service risks.
9.	The Contractor must provide Continual Service Improvement to improve service quality.
10.	The Contractor must provide Continual Service Improvement to improve client satisfaction.
11.	The Contractor must provide Continual Service Improvement to ensure service transparency.
12.	The Contractor must provide Continual Service Improvement to ensure service sustainability.
13.	The Contractor must provide Continual Service Improvement to improve/reduce costs.
Deliverables	
Deliverables are defined in **Schedule K – Key Program Deliverables**	

3.2.2.2 Infrastructure Architecture

The Infrastructure Architecture service will define and manage the scope and design of the infrastructure architecture for the computing systems to support the evolving needs of the Commonwealth. This range of Services includes design of the mainframe, mid-range, x86 servers, (both physical and virtual), Local Area Network (LAN), storage, backup systems, and the DR systems. The design will also need to detail how the most current data will be restored to the targeted DR system.

Efforts are underway to re-write many of the Commonwealth business applications. For example, some of the mainframe applications are being migrated to newer server based systems. The Contractor must consider the planned retirement of some of the mainframe workload, and at the same time consider the offsetting growth in other server platform environments.

At the direction of the Commonwealth, the Contractor must transition Commonwealth based computing infrastructure to one of the datacenters. The Contractor must work with the Commonwealth agencies to understand the systems involved, and the timeframe of these migrations. Working with the Commonwealth agencies, the Contractor must provide the design, project management, hardware and technical support required to test and migrate these systems to the new production environment. At its discretion, each agency must provide the applications staff to support the migrations.

The Infrastructure Architecture service will review and recommend hardware, software, and the technical configurations required to build the requested infrastructure environments. Prior to migrating each of the current application workloads to the new target infrastructure, the Contractor must work with each Commonwealth agency to develop a mutually agreed to Acceptance Test Plan that includes the testing of application infrastructure performance characteristics.

Reference Documentation

Schedule J.1 – Data Center Service Level Management

Schedule J.2 – Data Center Service Level Matrix

Schedule J.3 – Data Center SLA Definitions

Requirements

1.	Define the infrastructure technology Services to be offered. The Contractor must provide a detailed list of Services and computer platforms to be provided to the Commonwealth.
2.	The Contractor must design and build the IT infrastructure architecture to support the

	Services required by the Commonwealth. Design must provide as much interoperability and open standards as possible. All designs must be approved by the Commonwealth. The Contractor must provide the design in a Visio format to the Commonwealth for review and approval prior to execution. This diagram must be dated and maintained as Services are altered for the duration of the engagement.
3.	The Contractor must address CJIS and Criminal History Record Information Act (CHRIA) requirements for agency application infrastructure designs where required. Some agency application infrastructure designs (e.g. PSP) require additional security and encryption level requirements imposed by CJIS.
4.	SAP Infrastructure Design The Contractor's target infrastructure design for the Commonwealth's SAP environments must include a certified SAP sizing report prior to migration of the systems.
5.	Commonwealth Wide Area Net connectivity. The Contractor must implement initiatives to provide connectivity from the datacenter to the Commonwealth Network. Redundant network links are required. The Contractor must connect to and manage the requisite connections. The Contractor must provide ongoing network support Services to manage these links including the ability to increase capacity as needed to support changes in the application infrastructure requirements.
6.	Develop Acceptance Test Plan. Prior to migrating each of the current application workloads to the new target infrastructure, the Contractor must work with each Commonwealth Agency to develop a mutually agreed to Acceptance Test Plan that includes the testing of application infrastructure performance characteristics.
7.	Provide System Acceptance testing. The Contractor must conduct system acceptance testing, and provide the Commonwealth with written verification prior to declaring the system is fit for use. This acceptance test must include validation of infrastructure performance against system performance characteristics agreed to by both parties.
8.	Ready for use certification. The Contractor must provide the Commonwealth with written verification prior to

	declaring the Service is ready for use. The Service will not be considered ready for use until written acceptance is obtained from the Commonwealth.
9.	Support User Acceptance Testing. Contractor must support the Commonwealth's user acceptance testing. The Commonwealth must not be charged for Services until written acceptance is obtained from the Commonwealth.
10.	Provide Application Infrastructure environments. The Contractor must provide non-production and production environments for each of the application computing platforms. The non-production environments will be used for testing new technologies and applications, updates and upgrades, prior to production implementations. The Contractor must identify proposed solution to individual or consolidated non-production environments for agencies.
11.	Design service lifecycle. The Contractor must rovide the infrastructure design for the Services and platforms to be offered. The Contractor must provide ongoing evaluation and recommend new technologies to enhance, improve, and reduce the cost of Services.
12.	Define Technical Support functions. The Contractor must plan, manage, and operate the IT infrastructure, based on the various service levels offered.
Continual Service Improvement	
13.	Related to the project management and contract management role, the Contractor must provide Continual Service Improvement to reduce service risks.
14.	The Contractor must provide Continual Service Improvement to improve service quality.
15.	The Contractor must provide Continual Service Improvement to improve client satisfaction.
16.	The Contractor must provide Continual Service Improvement to ensure service transparency.
17.	The Contractor must provide Continual Service Improvement to ensure service sustainability.
18.	The Contractor must provide Continual Service Improvement to improve/reduce costs.

Deliverables
Deliverables are defined in **Schedule K - Key Program Deliverables**

3.2.2.3 Capacity Management

The Capacity Management activity focuses on the planning and scheduling of the Commonwealth's infrastructure capacity and growth. Capacity planning includes consideration of data communications, networking, processing, storage, and other environmental variables. The Contractor must issue periodic reports showing usage, trends, capacity forecasts, and recommendations for upgrades.

Processor capacity planning focuses on estimating, measuring, and reporting on the central processing unit (CPU) and memory usage, including peak usage and average usage over time.

Forecasting of each agency's application-based processor and memory usage must be determined using projected transaction and user volumes supplied by the Commonwealth. The Contractor must track application-based processor and memory usage and report the usage and trends to the Commonwealth. The Contractor must make periodic recommendations for upgrading existing server capacity.

Data storage capacity planning focuses on estimating, measuring, and reporting on data storage used per application over time.

Forecasting of application-based data storage usage will be provided by the Commonwealth. The Contractor must track current data storage usages and report the usage and trends to the Commonwealth. The Contractor must make periodic recommendations for upgrading existing data storage capacity.

New application infrastructure capacity planning focuses on estimating, measuring, and reporting on network, server, and data storage usage over time per application. New processing requirements must be established during testing in test environments. The Contractor must track application-based infrastructure usage. The Contractor must make monthly recommendations for upgrading existing infrastructure capacity.

The following list identifies but does not limit the roles and responsibilities that the Contractor must perform:

- Establish comprehensive Capacity Management planning process
- Identify future business Commonwealth requirements that will alter capacity requirements
- Assess capacity impacts when adding, removing or modifying applications
- Capture trending information and forecast future agency infrastructure capacity

requirements based on agency defined thresholds

- Recommend changes to capacity to improve service performance
- Assess impact/risk and any cost of capacity changes with agencies
- Maintain capacity levels to optimize use of existing IT resources and minimize agency costs
- Ensure adequate capacity exists within the IT environments

Reference Documentation

Schedule H - Commonwealth Computing Procedures Manual

	Requirements
1.	The Contractor must work with each agency, develop the initial Capacity Management Plan based on an inventory and review of each of the agency applications and associated managed infrastructure. The Contractor must develop the initial Capacity Management Plan and provide quarterly updates to the plan.
2.	The Contractor must meet with the Commonwealth and agency representatives on a monthly basis to assess the future datacenter resource requirements; processors, storage space, network (LAN & WAN), selected application transactions, and number of users, etc.
3.	The Contractor must produce an annual datacenter Capacity Plan and Trend Analysis.
4.	The Contractor must produce a monthly planned vs. actual resource usage report.
5.	The Contractor must recommend methods for reducing hardware "footprints", e.g., replacing server storage with network attached storage and aggressive server virtualization.
6.	The Contractor must allow emergency or temporary orders for additional Services or capacity without a minimum service commitment.
Continual Service Improvement	
7.	Related to the project management and contract management role, the Contractor must provide Continual Service Improvement to reduce service risks.
8.	The Contractor must provide Continual Service Improvement to improve service quality.

9.	The Contractor must implement initiatives to improve client satisfaction. The Contractor must provide Continual Service Improvement to improve client satisfaction.
10.	The Contractor must provide Continual Service Improvement to ensure service transparency.
11.	The Contractor must provide Continual Service Improvement to ensure service sustainability.
12.	The Contractor must provide Continual Service Improvement to improve/reduce costs.
Deliverables	
Deliverables are defined in **Schedule K – Key Program Deliverables**	

3.2.2.4 DR Planning & Testing

The DR Planning & Testing service ensures that the Contractor provides expert assistance in developing, documenting, deploying, and testing tiered datacenter recovery strategies that includes access for Commonwealth end users. This service must protect the identified applications processing at the datacenters, Commonwealth employees and constituents who utilize the application.

The Commonwealth will provide the Contractor with a list of agency applications that require a DR solution and related DR plan after contract is awarded. The Contractor is expected to provide DR Planning and Testing Services for agency applications that require DR Services. For Commonwealth agency applications that do not currently have DR plans, these Services must be provided in the event the Commonwealth elects to order DR services for these applications.

Reference Documentation

Schedule J.1 – Data Center Service Level Management

Schedule J.2 – Data Center Service Level Matrix

Schedule J.3 – Data Center SLA Definitions

	Requirements
1.	The Contractor must meet with the Commonwealth and agency representatives on an annual basis and upon request to assess its DR requirements. Post contract award, Contractor must document the Tiered DR plans in an online software program that must be available to Commonwealth and Contractor staff. The documented plans must be made available at the time each individual critical application is transitioned to the Contractor's managed Services.
2.	The Contractor must review and update Disaster Recovery Plans (DRPs) – The Contractor must review existing Disaster Recovery Plans (DRPs) to determine gaps in existing or future DR Services, within the first 120 days after the Effective Date. The Contractor must at least annually review and update the disaster recovery plans. The Contractor must assist the Commonwealth in identifying dependencies/limitations to DR testing due to non-Contractor infrastructure.
3.	The Contractor must provide the Commonwealth and agency representatives with access to an online DR planning tool.
4.	The Contractor must provide the Commonwealth and agency representatives with access to an automated emergency notification system. This would be invoked on the occasion of a disaster or other emergency.
5.	The Contractor must assist the Commonwealth and agency representatives as requested to review agency identified critical business applications and related IT applications and infrastructure.
6.	The Contractor must assist the Commonwealth and agency representatives as requested in developing, documenting, deploying, and exercising its tiered disaster recovery plans. The Contractor must perform a successful recovery test within 6

	months of transition to the Contractor's Managed Service.
7.	The Contractor must assist the Commonwealth and agency representatives as requested in coordinating disaster recovery exercises. Frequency of DR exercises will be at the discretion of the Commonwealth. The Contractor must every six (6) months test the operability of the disaster recovery plan then in effect.
8.	The Contractor must assist the Commonwealth and agency representatives as requested in developing, documenting, deploying, and exercising its continuity of operations (COOP) and continuity of government (COG) plans.
9.	The Contractor must assist the Commonwealth and agency representatives as requested in integrating its disaster recovery plans into its COOP and COG plans.
10.	As requested by the Commonwealth, the Contractor must evaluate the efficiency of business partner disaster recovery and/or business continuity plans.
11.	In concert with the Commonwealth and agency representatives, the Contractor must lead the recovery operations as requested in the event of a disaster or other major disruption.
12.	The Contractor must conduct disaster recovery planning and activities in accordance with the Business Continuity Institute Good Practice Guideline or similar standard.
13.	The Contractor must ensure DR Planning & Testing Services are documented in the Service Catalog.
Continual Service Improvement	
14.	Related to the project management and contract management role, the Contractor must provide Continual Service Improvement to reduce service risks.
15.	. The Contractor must provide Continual Service Improvement to improve service quality.
16.	. The Contractor must provide Continual Service Improvement to improve client satisfaction.
17.	. The Contractor must provide Continual Service Improvement to ensure service transparency.
18.	

	The Contractor must provide Continual Service Improvement to ensure service sustainability.
19.	The Contractor must provide Continual Service Improvement to validate business case for cost of service.
20.	The Contractor must provide Continual Service Improvement to improve/reduce costs.
Deliverables	
Deliverables are defined in **Schedule K – Key Program Deliverable**	

3.2.2.5 Security Management

The Security Management service must ensure the confidentiality, integrity and availability of Commonwealth information and infrastructure systems. All support and implementation activities must be conducted in accordance with, but not limited to, leading industry and Commonwealth standards, which include, but are not limited to, ISO 27001:2005 and ISO 27002:2005. The Contractor must support all related system audits at the Contractor's expense. The Contractor must maintain current security ISO 27001, ISO 9001 and ISO/IEC 20000 certifications.

The Contractor must comply with Commonwealth IT policies and directives as well as federal and Commonwealth laws, regulations and policies, including but not limited to the Criminal History Record Information Act (CHRIA), Health Insurance Portability and Accountability Act (HIPAA), Criminal Justice Information Services (CJIS) regulations, The United States Social Security Administration (SSA)regulations, IRS (Internal Revenue Service) Publications, Commonwealth Information Technology Bulletins (ITBs) and the Payment Card Industry (PCI) standards. The Contractor must work with each agency to understand and ensure compliance with all laws, regulations, and policies as they pertain to each individual agency.

Reference Documentation

Exhibit J.1 through J.3 - Commonwealth Security and Compliance Requirements

Exhibit G.6 - PSP - CJIS Security Policy

Exhibit G.9 - PSP – CCHRI

Exhibit G.7 - PSP - Summary of CJIS Requirements

Exhibit G.12 - PSP - CHRIA Handbook

Requirements

1.	The Contractor must develop an annual Security Management Plan.
2.	The Contractor must deploy complement of network security systems. The Contractor must implement at minimum: spam filtering, anti-virus, malware protection, firewall (web, application), intrusion prevention and detection, web content filtering, virtual private network, and data loss prevention systems.
3.	The Contractor must perform quarterly (at the Contractor's expense) Vulnerability Analyses (VA) and penetration testing to identify new or emerging information

	security threats. The Contractor must perform penetration testing (at the Contractor's expense) and present the results of each VA on a quarterly basis. Should exposures be identified, plan and remediate the exposure in accordance with Commonwealth IT policy guidelines. The Contractor must report results to the Commonwealth within the time set out in an applicable SLA. The above requirement is for all systems/subsystems that the Contractor is responsible for including managed servers/virtual servers, network devices, security devices including , but not limited to, the following: • Performing web application firewall administration and securing web applications behind it. • Ensuring and maintaining PCI level 1 compliance. • Implementing DLP for the data center server assets to avoid a breach. • Implementing Database Firewall to secure database assets from breach.
4.	The Contractor must review network and other security logs for evidence of attacks. The Contractor must utilize enterprise grade intrusion detection tool(s) to systematically identify, stop, and report security threats. The Contractor must produce a monthly Security Log Analysis as part of the monlthy status reports as described in RFP section IV-5 Reports and Project Control.

5.	Apply operating system and other security patches. The Contractor must implement a Patch Management Program to ensure the timely application of security updates on all infrastructure platforms in accordance with Commonwealth IT policy guidelines. The Patch Management Program must adhere to the Change Management process that includes Commonwealth approvals.
6.	The Contractor must restrict physical access to all network systems and equipment with biometric or other second factor access control systems.
7.	The Contractor must restrict access to all data in the Commonwealth network infrastructure. The Contractor must restrict and control all data access right, groups and special permissions based on the data security program designed by the Commonwealth security team and/or specified by the agencies. Access level changes and exceptions must be executed only when approved paperwork is complete and approved. A file of all access changes must be maintained by the Contractor for audit purposes. The Contractor must support Commonwealth initiated security audits.
8.	The Contractor must evaluate the security standing of network-connected subcontractors. The Contractor must conduct information security audits of prominent subcontractors on an annual basis.
Continual Service Improvement	
9.	**3.3** Related to the project management and contract management role, the Contractor must provide Continual Service Improvement to reduce service risks.
10.	The Contractor must provide Continual Service Improvement to improve service

	quality.
11.	The Contractor must provide Continual Service Improvement to improve client satisfaction.
12.	. The Contractor must provide Continual Service Improvement to ensure service transparency.
13.	The Contractor must provide Continual Service Improvement to ensure service sustainability.
14.	The Contractor must provide Continual Service Improvement to improve/reduce costs.
Deliverables	
Deliverables are defined in **Schedule K – Key Program Deliverables**	

3.3.1.1 Performance Monitoring & Management

The Performance Monitoring & Management Service of the infrastructure components, databases, and applications provide the critical input for meeting service level commitments. Performance monitoring is a proactive method to identify and respond to system database, processor utilization, or environmental problems that may affect the Services, or might negatively affect Services in the near future. The selected performance monitoring tools must also provide one of the key inputs for calculating SLAs, and the associated monthly evaluation and reporting needs.

The Contractor must collect performance information and report on infrastructure and application performance status on a daily basis using performance management and monitoring tools.

All tracked performance information must be reported daily, including processing performance, network (LAN / WAN) performance, and storage performance data. The Contractor must determine trends in conjunction with the Commonwealth, and all trends must be reported to address, if necessary, any changes from an established baseline. Forecasts of future usage must be determined based on expected growth in application transaction volume and expected deployment of future applications.

The Contractor must provide a base level of performance monitoring for key infrastructure components such as server, storage, network, and security. Additional Performance Monitoring Services such as database and application monitoring must be offered to the Commonwealth as an additional level of service.

Agency applications may require additional application level monitoring provided and managed by the Commonwealth Agencies. The Contractor must allow additional Commonwealth based monitors to be installed and managed by individual Commonwealth Agencies.

Reference Documentation

Schedule J.1 – Data Center Service Level Management

Schedule J.2 – Data Center Service Level Matrix

Schedule J.3 – Data Center SLA Definitions

Requirements

1.	The Contractor must use performance monitor software tool(s) to monitor selected infrastructure Services. The selected infrastructure service must be presented to the Commonwealth for approval.

2.	The Contractor must create and maintain performance monitoring procedures for each platform to ensure each system is monitored in a consistent manner. All identified systems must be monitored under the parameters established in the CCPM. •
3.	Performance information reporting - The Contractor must collect and report on the performance data on a monthly basis. The Contractor must utilize these reports to ensure SLA's are being achieved. A monthly report must be created to provide a review of how well the systems are performing. Also, the Contractor must provide daily reporting. The Contractor must recommend system changes to correct over and under system utilization, as well as system upgrades as appropriate. These reports and recommendations must be shared with the Commonwealth. The Contractor must provide daily performance reports summarizing incidents for the past 24-hours and immediate reports of incidents and routine status reports of incidents in progress for resolution such as a network or server outage that impacts Commonwealth Services. Examples of automated notifications include, but are not limited to, drive full (Warning, critical), unscheduled reboots, server instability, etc. and to be defined in the CCPM. Contractor must have to ability to provide performance information on a daily, weekly, and monthly basis.
4.	The Contractor must support the load testing of applications by providing additional targeted performance monitoring Services during the testing period. This service must be made available as an additional service. The Contractor must provide load-testing performance monitoring as an add-on service.
5.	Performance Monitoring training - The Contractor must provide the Commonwealth with training on the use of performance management tools and reporting.

6.	The Contractor must support for agency level monitors - agency applications may require additional application level monitoring to be provided and managed by the Commonwealth agencies. The Contractor must support synthetic transactions in applications to create a "dashboard" view that applications are working properly. The Contractor must allow additional agency based monitors to be installed and managed by individual Commonwealth Agencies.
Continual Service Improvement	
7.	Related to the project management and contract management role, the Contractor must provide Continual Service Improvement to reduce service risks.
8.	The Contractor must implement initiatives to improve service quality. The Contractor must provide Continual Service Improvement to improve service quality.
9.	The Contractor must provide Continual Service Improvement to improve client satisfaction.
10.	The Contractor must provide Continual Service Improvement to ensure service transparency.
11.	The Contractor must provide Continual Service Improvement to ensure service sustainability.
12.	The Contractor must provide Continual Service Improvement to improve/reduce costs.
Deliverables	
Deliverables are defined in **Schedule K – Key Program Deliverables**	

3.3.2 Facilities Management

3.3.2.1 Facilities Architecture / Maintenance

The Facilities Architecture and Maintenance service must provide and staff a minimum of two fully operational datacenter facilities in a multi datacenter mode. This service requires the integration and alignment of the non-core Services, including those relating to the premises, required to operate and maintain a datacenter that fully supports the core objectives of this project.

These datacenters must be geographically dispersed to provide protection from regional disruptions such as weather, power or other emergencies. The process of locating and managing these physical environments must include defining the physical site requirements, selecting appropriate facilities, and designing effective processes for monitoring and maintaining environmental Services and managing physical access. Effective management of the physical environment reduces the possibility of service interruptions due to unauthorized access and damage to computing equipment and personnel. Please review Exhibit D.7 - EDC Facility Summary for information regarding the EDC facilities.

Facilities Management includes all aspects of providing and managing the physical environment. For example; power and power distribution, cooling and ventilation, fire detection and suppression, building security and access control, and environmental monitoring are all required. Listed below are the basic Services required, but not inclusive of all Services needed, to manage an enterprise class datacenters required by the Commonwealth.

Reference Documentation

Exhibit D.7 - EDC Facility Summary

Requirements

1.	Safe and secure datacenter. Two layers of authentication and appropriate clearances ist be required. The Contractor must provide datacenter environments which are secured to ensure that only authorized personal have physical access to the buildings, systems and all levels of data. This includes data storage within networked storage devices, servers, tapes, diskettes, optical and paper formats. The Contractor must comply with the security requirements of the Commonwealth. The Contractor must immediately inform the Commonwealth of any vulnerability or weakness in the Services, and recommend a solution or mitigation. TheContractor must assess the EDC facilities and provide a report to the

	Commonwealth as it pertains to required security upgrades.
2.	The Contractor must provide fully redundant environmental Services. To include, but not limited to, HVAC, UPS conditioned power and distribution, generator backup, automated transfer switch, fire suppression system. The Contractor must integrate its Facilities Management process with Service Management processes, especially Change Management, Incident Management, Service Continuity Management and Availability Management. The Contractor must confirm its ability to provide, manage, maintain and operate multiple Tier 3 equivalent facilities. The Contractor must assess the EDC facilities and provide a report to the Commonwealth as it pertains to required HVAC and power upgrades.
3.	The Contractor must staff the datacenters with appropriate operational and management levels of personnel 24/7/365. Critical engineering and management staff must be available to the Commonwealth Monday through Friday, between 8am – 5pm Eastern time excluding Commonwealth observed holidays. Access to operational staff must be available 24/7/365. Video surveillance system must be utilized at all entry points and throughout the datacenter and tape storage areas. Datacenter Staff are required to adhere to the Commonwealth requirements for background checks and security clearances. The Contractor is required to monitor the status of staff and to take appropriate action for staff found to subsequently have violated prescribed legal or ethical standards as described in **Schedule G –Staffing Plan and Key Positions**. Such violations must be immediately reported and appropriate actions taken. Commonwealth verification of the requirements will be necessary prior to staff working on Commonwealth related systems.
4.	Procurement Planning - The Contractor must provide program and processes to alter the datacenter environment and to refresh the environmental Services at end-of-life, and as additional Services are needed.
5.	Physical Access to Facilities- The Contractor must coordinate with the Commonwealth to provide for physical access and facilitate inspections by government authorities (including the Commonwealth) for auditing the conduct of government business.

	The Contractor must assess the EDC facilities and provide a report to the Commonwealth as it pertains to required physical access to the EDC facility.
6.	SLA Reporting - The Contractor must identify and create environmental service level objectives in the form of SLAs, and report on the service availability, problems, and corrective actions on a monthly basis. The Contractor must assess the EDC facilities and provide a report to the Commonwealth as it pertains to monitoring, maintain and reporting on EDC SLAs.
7.	The facilities must be designed and operated with environmentally friendly equipment and techniques, and be SSAE 16 compliant. The Contractor must assess the EDC facilities and provide a report to the Commonwealth as it pertains to monitoring, maintaining and reporting on EDC SLAs.
8.	The Contractor must schedule (at its expense) a SSAE 16 audit of the EDC datacenter no more than 12 months after the effective date of the contract.
Continual Service Improvement	
9.	Related to the project management and contract management role, the Contractor must provide Continual Service Improvement to reduce service risks.
10.	The Contractor must provide Continual Service Improvement to improve service quality.
11.	The Contractor must provide Continual Service Improvement to improve client satisfaction.
12.	The Contractor must provide Continual Service Improvement to ensure service transparency.
13.	The Contractor must provide Continual Service Improvement to improve/reduce costs.

Deliverables	
Deliverables are defined in **Schedule K – Key Program Deliverables**	

3.3.2.2 Site Operations

The Site Operation service must provide datacenter operations staff and management to operate and monitor the IT computing equipment and Services being provided. The staff must interface with Commonwealth staff to institute best practice datacenter Services. Datacenter operations include, but are not limited to, management of the computing platforms, storage, local area networking, security firewall, tape backup, and offsite tape rotation systems.

Reference Documentation

N/A

	Requirements	Describe Compliance
1.	The Contractor must monitor and operate the various computer systems, network, network and local disk storage and firewall security systems. pThe Contractor must rovide datacenter operations staff to monitor the computer system platforms, associated disk systems, networking Services and firewall and security systems. The Contractor must ensure proper equipment operations, timely batch jobs processing and appropriate response to any abnormal end and error conditions. The Contractor must support application specific operations as determined by the application owner. This includes executing the troubleshooting procedures required by the application owners as detailed within the CCPM. This may include operational activities and initial troubleshooting steps, contact and escalation lists (aka "Run Book"). This information must be maintained by the Contractor on an application by application basis and must be hosted within the Knowledge Management Portal. A daily operations batch schedule report must be created and used to log normal / abnormal conditions. Abnormal conditions must be investigated for problem determination and rerun. Any abnormal condition that cannot be corrected must be referred to technical support staff for resolution. The Contractor must properly clean and maintain equipment to minimize problems and outages, at intervals established with the Commonwealth or in compliance with	

	stated and written specifications. The Contractor must assess the EDC facilities and provide a report to the Commonwealth as it pertains to monitoring, maintaining and operating the installed infrastructure.
2.	For the systems that utilize tape backup Services, the Contractor must provide a structured tape management approach. For systems that utilize disk-2-disk backup approach the Contractor must provide a structured disk-2-disk approach. The Contractor must manage and maintain the tape backup system and Services. The Contractor must rotate designated tapes to, and returned from approved offsite storage location. Maintain detailed audit log of tape movement. Some agency applications fall under additional CJIS and CCHRI security requirements for tape backups. The Contractor must provide datacenter operations staff to manage and maintain the tape management system. Tapes must be rotated to, and returned from an approved offsite vaulting subcontractor. An automated software process must be utilized to report the completion status of backup processing, with electronic notification of failures sent to Contractor technical support, and identified Commonwealth staff for follow up and corrective action. The Contractor must provide the facilities to Retrieve External Storage Media from on-site and off-site storage as requested by the Commonwealth or as required in an emergency. The Contractor must wipe or erase the data and configuration information resident on the media prior to disposal or re-use, and in accordance with Commonwealth standards. The Contractor must dispose of retired media in an environmentally sound manner after purging any Commonwealth data using Commonwealth, and/or Federal guidelines/policies prior to disposing of media. The Contractor must operate media libraries and library management systems as required to provide the Services. mhe Contractor must Maintain an existing inventory control system to properly manage External Storage Media in storage and prepare them for shipment to the

	contingency site. The Contractor must assess the EDC tape backup facilities and provide a report to the Commonwealth as it pertains to manage and operated the installed tape backup systems and media operations.
3.	The Contractor must monitor physical access and security of the datacenter. Video surveillance is required. The Contractor must staff the datacenter with appropriate level of staff and management 24/7/365. The Contractor must monitor physical access to the datacenter and respond to security incidents in a consistent and auditable manner. All breaches must be reported to the Commonwealth for review and follow up action as required. Monitoring of the video system for all entry points and throughout the datacenter and tape storage areas must be included in this responsibility. The Contractor is required to adhere to the Commonwealth requirements for background checks and security clearances. Commonwealth verification that the requirements have been met will be necessary prior to Contractor working on Commonwealth related systems.
4.	The Contractor must manage and maintain equipment configuration inventory system. The Contractor must provide staff to create and maintain a configuration record for all hardware and software components in the datacenter. This must be an accurate record of all software, computing, disk storage, tape, network, racking, cables, and environmental equipment.
5.	The Contractor must provide programs and processes to alter the operational environment, and to refresh the Services at asset end-of-life or implementation of new technology Services, as these Services are needed.
6.	The Contractor must identify and create service objectives for the site operational Services in the form of SLAs, and report on the service availability, problems, and corrective actions on a monthly basis.

Continual Service Improvement	
7.	Related to the project management and contract management role, the Contractor must provide Continual Service Improvement to reduce service risks.
8.	The Contractor must provide Continual Service Improvement to improve service quality.
9.	The Contractor must provide Continual Service Improvement to improve client satisfaction.
10.	The Contractor must provide Continual Service Improvement to ensure service transparency.
11.	The Contractor must integrate Continuous Improvement Program processes into Availability Management and Service Level Management.
12.	The Contractor must provide Continual Service Improvement to improve/reduce costs.
Deliverables	
Deliverables are defined in **Schedule K – Key Program Deliverables**	

3.3.3 Managed Hosting Services

For all Managed Hosting Services, the Contractor must actively monitor the daily operations of the infrastructure used to provide the services. The Contractor must execute the troubleshooting procedures required by the application owners as detailed within the CCPM. This may include operational activities and initial troubleshooting steps, contact and escalation lists (aka "Run Book"). This information must be maintained by the Contractor on an application by application basis and must be hosted within the Knowledge Management Portal.

3.3.3.1 Windows Support

This service must provide hosting, operations and support Services for Microsoft Windows based servers (physical and virtual) located at the central datacenters. Contractor must support various hardware systems and various versions of the Microsoft operating systems, and support service software. The Contractor must provide support for both physical and virtual servers. Currently the Commonwealth utilizes virtualization technology from VMware and Microsoft's Hyper-V. See attached Exhibits for hardware and software details. The number and level of support staff members required to perform the below listed tasks must be determined by the Contractor, based on number of Commonwealth clients, hardware, software, and operating systems being serviced.

Listed below are the basic Services required, but not inclusive of all Services needed, to manage an enterprise class datacenter required by the Commonwealth. The Contractor must include these Services within the base level of Services in this Offering. Change requests must be approved and authorized using the change management process.

Reference Documentation

N/A

	Requirements
1.	The Contractor must monitor local operations, troubleshoot and resolve operational issues. The Contractor must actively monitor the daily operations of all MS Windows servers. Maintain a log for each server detailing hardware / software configuration and critical service operations. The Contractor must review and document its review of system logs on a weekly basis to ensure critical system Services are processing without errors. The Contractor must complete weekly server log indicating which logs were reviewed, date and initial the log.

	•
2.	The Contractor must monitor system backup processing on a daily basis. The Contractor must review daily backup log for successful completion. Note failures, and correct the problems. The Contractor must create problem record for any abnormal condition and any repairs that have been made, re-execute as appropriate. An automated software process must be utilized to report the completion status of backup processing, with electronic notification of failures sent to Contractor technical support, and identified Commonwealth staff for follow up and corrective action.
3.	The Contractor must provide Microsoft Hyper-V and VMware trained staff holding manufacturer recognized certifications for hardware and software technical support. Post award; the Contractor must provide the Commonwealth a resume or CV for Key Positions assigned to this engagement. A copy must be maintained on Contractor file including verified background clearances as required.
4.	The Contractor must provide cost effective operational and technical support for the Windows computing platform. The Contractor must provide platform level operational and technical support for the computing platform. The Contractor must provide Level 2 and Level 3 Support to the Service Desk and/or Commonwealth Users. The Contractor must provide a tiered level of support Services (e.g. Gold, Silver, and Bronze). The Contractor must provide technical advice and support to the Application Development and Maintenance (ADM) and Database Administration (DBA) staffs, as required. Post award; The Contractor must provide Commonwealth with a resume or CV for Key Positions assigned to this engagement. A copy must be maintained on Contractor file.
5.	The Contractor must ensure network connectivity and consistent system response

	times. The Contractor must utilize automated system management tool(s) to ensure real-time monitoring and notification of server availability and response times. Stop / Start times of servers will be a source of input for SLA measurements. Identify tool set(s).
6.	The Contractor must ensure server operating systems are maintained with the current patch level, based on the Services provided by the server. The Contractor must analyze monthly service patches and determine which need to be applied, by server type. The Contractor must create a change record, log the update in the server log, install based on server maintenance schedule and update the server configuration record. The Contractor must notify impacted Commonwealth users immediately of any unscheduled service interruptions via email/web. The Contractor must be document normal work hours and holiday schedules with each agency to determine the contact method and escalation process of each Commonwealth agency.
7.	The Contractor must provide a review and analysis of system performance/capacity to determine if current performance/capacities are sufficient to support the needs of the stakeholders.
8.	User Account Management - phe Contractor must Provide certified operating system administration staff to create and maintain the registration of profiles, associated groups, and the security permissions required to service the approved client base of the operating systems.
9.	Procurement Planning The Contractor must provide program and processes to refresh the hardware at asset end-of-life, and as upgrades are needed to meet anticipated growth in utilization.
10.	SLA Reporting The Contractor must collect actual system availability, utilization and response time data. On a monthly basis, the Contractor must create a Service Level Agreement

	report for the Commonwealth team.
11.	Installation of Windows updates/patches must be coordinated by Agency. For IES, windows version upgrades must be SAP certified. The Contractor must coordinate at an agency level and account for any required patching as technology upgrades require.
12.	The Contractor must provide Software License Management.
Continual Service Improvement	
13.	Related to the project management and contract management role, the Contractor must provide Continual Service Improvement to reduce service risks.
14.	The Contractor must provide Continual Service Improvement to improve service quality.
15.	The Contractor must provide Continual Service Improvement to improve client satisfaction.
16.	The Contractor must provide Continual Service Improvement to ensure service transparency.
17.	The Contractor must provide Continual Service Improvement to improve/reduce costs.
Deliverables	
Deliverables are defined in **Schedule K – Key Program Deliverables**	

3.3.3.2 Storage Management

The Storage Management service must provide hosting and operational support Services for storage management systems. Storage management systems must be maintained at current support levels for optimal performance, recoverability, and secure operations. Systems must be located in the Contractor's datacenters. The Contractor must support the hardware and software components of these systems.

The proposed storage management service and solution must address adherence to multiple security and compliance requirements relating to the storage and management of multiple types of data assets (e.g. CHRIA law, criminal history).

Reference Documentation

N/A

	Requirements
1.	The Contractor must monitor local operations, troubleshoot and resolve operational issues. The Contractor must monitor system backup processing on a daily basis. The Contractor must actively monitor the daily operations of all storage units. The Contractor must maintain a log for each storage unit. The Contractor must complete weekly service logs indicating the frequency logs are reviewed, and the status of the daily backup process. The Contractor must create problem records for any abnormal condition and any repairs that have been made. •
2.	The Contractor must provide appropriately trained staff that hold current manufacturer certifications for hardware and software technical support (where available). Staff must interact with vendor support Services as needed. The Contractor must provide Commonwealth with a resume or CV for Key Positions assigned to this engagement. A copy must be maintained on Contractor file including required background checks and clearances as required.
3.	The Contractor must provide platform level operational and technical support for the computing platform. The Contractor must provide Level 2 and Level 3 Support to the Service Desk and/or

	Commonwealth Users. The Contractor must provide a tiered level of support Services (e.g. Gold, Silver, Bronze)
4.	The Contractor must monitor system backup processing on a daily basis. The Contractor must review daily backup log for successful completion. The Contractor must note failures, and correct the problem. The Contractor must create problem record for any abnormal condition and any repairs that have been made. An automated software process must be utilized to report the completion status of backup processing, with electronic notification of failures sent to identified Commonwealth staff and Contractor technical support for follow up and corrective action.
5.	The Contractor must ensure network connectivity, and consistent system response times. The Contractor must identify and use automated system management tool(s) to ensure storage system availability and expected response times. Stop / Start time records must be a source of input for SLA measurements.
6.	The Contractor must ensure storage device operating systems are maintained with the current system patch level, including firmware upgrades. The Contractor must analyze monthly service patches and determine which patches need to be applied. The Contractor must create a change record, log the update in the storage system log, and install based on maintenance schedule. The Contractor must notify impacted Commonwealth users immediately of any unscheduled service interruptions via email/web. The Contractor must document normal work hours and holiday schedules with each agency to determine the contact method and escalation process of each Commonwealth agency. The Contractor must coordinate at an agency level and account for any required patching as technology upgrades require.
7.	The Contractor must utilize data storage conservation techniques such as data de-duplication or other industry standards, to reduce the overall footprint of the data.

8.	The Contractor must propose options/solutions for self-provisioning or limited self-management of storage as a service.
Continual Service Improvement	
9.	. Related to the project management and contract management role, the Contractor must provide Continual Service Improvement to reduce service risks.
10.	The Contractor must provide Continual Service Improvement to improve service quality.
11.	The Contractor must provide Continual Service Improvement to improve client satisfaction.
12.	The Contractor must provide Continual Service Improvement to ensure service transparency.
13.	The Contractor must provide Continual Service Improvement to improve/reduce costs.
Deliverables	
Deliverables are defined in **Schedule K – Key Program Deliverables**	

3.3.3.3 ERP Hosting – SAP / Oracle

ERP Hosting – SAP service must provide hosting and operational support Services for two SAP-ERP systems that are currently located at the DPH. One system Services the General Accounting System application, and the other Services the Integrated Tax System application for the Department of Revenue. Each application has associated development and testing environments support on segregated equipment. Contractor must support various production and non-production versions of the applications and the associated hardware. The roles and the number of staff members required to perform the below listed tasks must be determined by the Contractor.

Due to the critical and complex nature of these SAP environments, the Commonwealth requires an experienced SAP hosting provider. The Contractor's proposed target infrastructure design for the Commonwealth's SAP environments must include a certified SAP sizing report prior to migration of the systems.

The ERP Hosting – Oracle service must provide hosting and operational support Services for the current Oracle Enterprise system utilized by the Pennsylvania Liquor Control Board (PLCB). The application has associated development and testing environments support on segregated equipment. Contractor must support various production and non-production versions of the applications and the associated hardware.

Reference Documentation

N/A

Requirements	
1.	The Contractor must provide ERP Hosting Services for SAP and Oracle based applications.
2.	The Contractor must monitor local system operations, troubleshoot and resolve operational issues. The Contractor must actively monitor the daily operations of all ERP systems. The Contractor must maintain a log for each server detailing hardware / software configuration and critical service operations. The Contractor must review and document its review of system logs on a weekly basis to ensure critical system Services are processing without errors. The Contractor must complete weekly server log indicating which logs were reviewed, date and initial the log.

	•
3.	The Contractor must monitor system backup processing on a daily basis. The Contractor must review daily backup log for successful completion. Note failures, and correct the problem. The Contractor must create problem record for any abnormal condition and any repairs that have been made. An automated software process must be utilized to report the completion status of backup processing, with electronic notification of failures sent to Contractor technical support, and identified Commonwealth staff for follow up and corrective action.
4.	The Contractor must provide IBM, SAP, and Oracle trained staff holding current manufacturer certifications for hardware and software technical support. Staff must interact with vendor support Services when needed. The Contractor must provide Commonwealth with a resume or CV for Key Positions assigned to this engagement. A copy must be maintained on Contractor file including required background checks and clearances as required.
5.	The Contractor must provide cost effective operational and technical support for the computing platform. The Contractor must provide Level 2 and Level 3 Support to the Service Desk and/or Commonwealth Users. The Contractor must provide a tiered level of support Services (e.g. Gold, Silver, and Bronze).
6.	The Contractor must ensure network connectivity, and consistent system response times. The Contractor must utilize automated system management tool(s) to ensure real-time monitoring and notification of server availability and response times. Stop / Start times of servers must be a source of input for SLA measurements. Identify tool set(s).
7.	The Contractor must ensure server operating systems are maintained with the current system patch level, based on the Services provided by the server. The Contractor must analyze monthly service patches and determine which patches need to be applied, by server type. The Contractor must create a change record, log the update in the server log, and install based on server maintenance schedule.

	The Contractor must implement a Patch Management Program to ensure the timely application of updates on all infrastructure platforms in accordance with Commonwealth IT policy guidelines.
8.	User Account Management The Contractor must provide certified system administration staff to create and maintain the registration of profiles, associated groups, and the security permissions required to service the approved client base of the system.
9.	Procurement Planning The Contractor must provide program and process to refresh the hardware at asset end-of-life, and when upgrades are needed to meet anticipated growth in utilization.
10.	SLA Reporting The Contractor must collect actual system availability, utilization and response time data. On a monthly basis, the Contractor must create a SLA report for the Commonwealth and Vendor Management teams.
Continual Service Improvement	
11.	Related to the project management and contract management role, the Contractor must provide Continual Service Improvement to reduce service risks.
12.	The Contractor must provide Continual Service Improvement to improve service quality.
13.	The Contractor must provide Continual Service Improvement to improve client satisfaction.
14.	The Contractor must provide Continual Service Improvement to ensure service

	transparency.
15.	The Contractor must provide Continual Service Improvement to improve/reduce costs.
Deliverables	
Deliverables are defined in **Schedule K – Key Program Deliverables**	

3.3.3.4 UNIX Support – AIX / Linux

The Unix Support – AIX / Linux service must provide hosting and operational support Services for AIX and Linux server systems. The systems must be located in the Contractor's datacenters. Contractor must support various versions of the AIX and Linux operating systems. The number of staff members required to perform the operational tasks listed below must be determined by the Contractor.

Reference Documentation

N/A

	Requirements
1.	The Contractor must onitor local operations, troubleshoot and resolve operational issues. The Contractor must actively monitor the daily operations of all AIX / Linux systems. The Contractor must assume responsibility for all master and subordinate console functions. The Contractor must issue operator commands to control all In-Scope platforms. The Contractor must Assume the responsibility for and perform all console operations. The Contractor must monitor the performance of online interactive traffic and take appropriate action to resolve online-system-related incidents and/or problems, including escalating (as appropriate) the incident and/or problem to the proper Level 2 Support group. The Contractor must monitor the transmission of files between the Commonwealth and any other parties as designated by Commonwealth. The Contractor must provide operational support for data transmission (send/receive), consistent with commercial or agency standards. The Contractor must manage, maintain, monitor, and control online and batch process, both scheduled and unscheduled (including on-request processing). The Contractor must maintain a log for each server detailing hardware / software configuration and critical service operations. The Contractor must review the system logs on a weekly basis to ensure critical system Services are processing without errors. The Contractor must review and document its review of system logs on a weekly basis to ensure critical system Services are processing without errors. The Contractor must complete weekly server log indicating which logs were reviewed, date and initial the log. The Contractor must maintain and update the operational documentation for all operations procedures and Services. •

2.	The Contractor must provide a review and analysis of UNIX system performance/capacity to determine if current performance/capacities are sufficient to support the needs of the UNIX stakeholders. The Contractor must perform an initial review and audit of the current UNIX usage, procedures and reports and provide an analysis of the current UNIX usage, processes and reports currently being supported. The Contractor must document its review and audit findings and recommendations.
3.	Production Control and Scheduling (including batch processing) The Contractor must schedule batch jobs within Commonwealth agency defined windows to achieve maximum performance as long as required batch completion times are met. A cross platform (e.g. Window, Unix, and Mainframe) system must be required. Where practicable, provide for automated scheduling of batch work and processes including backups. Commonwealth agencies have a number of applications that require scheduling software / batch processing software (i.e. $Universe, SAP certified, etc.), this software is heavily integrated into many of these systems. The Contractor must develop, maintain, and utilize an emergency contact list and escalation procedures to resolve abnormally ended jobs. The Contractor must resolve abnormally ended jobs caused by conditions external to production programs. The Contractor must repair abnormally ended jobs when possible and perform job restarts in accordance with the Service Management Manual. The Contractor must check job outputs and print queues, and change job priorities. The Contractor must notify Commonwealth agencies in accordance with the Contractor's proposed notification procedures in the event that applications do not execute properly.
4.	The Contractor must monitor system backup processing on a daily basis. The Contractor must review daily backup logs for successful completion. The Contractor must note failures, and correct the problem. The Contractor must create problem record for any abnormal condition and any repairs that have been made. An automated software process must be utilized to report the completion status of backup processing, with electronic notification of failures sent to Contractor technical

	support, and identified Commonwealth staff for follow up and corrective action.
5.	The Contractor must provide AIX and Linux trained staff that hold current manufacturer certifications for hardware and software technical support. The Contractor must provide technical advice and support to the Application Development and Maintenance (ADM) and Database Administration (DBA) staffs, as required. Post award; The Contractor must provide Commonwealth with a resume or CV for Key Positions assigned to this engagement. A copy must be maintained on Contractor file.
6.	The Contractor must provide cost effective operational and technical support for the computing platform. The Contractor must provide platform level operational and technical support for the computing platform. The Contractor must list the service levels for the various service tiers that can be provided. See Schedule J.1 Data Center Service Level Management for the definitions of the expected options. The Contractor must provide Level 2 and Level 3 Support to the Service Desk and/or Commonwealth Users.
7.	The Contractor must ensure network connectivity to COPANET, and consistent system response times. The Contractor must utilize automated system management tool(s) to ensure real-time monitoring and notification of server availability and response times. Stop / Start times of servers must be a source of input for SLA measurements.
8.	The Contractor must ensure server operating systems are maintained with the current system patch level, based on the Services provided by the server. The Contractor must analyze monthly service patches and determine which patches need to be applied, by server type. The Contractor must create a change record, log the update in the server log, and install based on server availability schedule. Change requests must be approved and authorized using the change management process. The Contractor must notify the Commonwealth of any scheduled or unscheduled service interruptions.

	The Contractor must implement a Patch Management Program to ensure the timely application of updates on all infrastructure platforms in accordance with Commonwealth IT policy guidelines.
9.	User Account Management The Contractor must provide certified system administration staff to create and maintain the registration of profiles, associated groups, and the security permissions required to service the approved client base of the system and application.
10.	Procurement Planning The Contractor must provide program and processes to refresh the hardware at asset end-of-life, and when upgrades are needed to meet anticipated growth in utilization.
11.	SLA Reporting The Contractor must collect actual system availability, utilization and response time data. On a monthly basis, the Contractor must create a Service Level Agreement report for the Commonwealth and Vendor Management teams.
12.	The Contractor must provide Software License Management.
Continual Process Improvement	
13.	Related to the project management and contract management role, the Contractor must provide Continual Service Improvement to reduce service risks.
14.	The Contractor must provide Continual Service Improvement to improve service quality.
15.	The Contractor must provide Continual Service Improvement to improve client satisfaction.

16.	The Contractor must provide Continual Service Improvement to ensure service transparency.
17.	The Contractor must provide Continual Service Improvement to improve/reduce costs.
Deliverables	
Deliverables are defined in **Schedule K – Key Program Deliverables**	

3.3.3.5 Mainframe Services

The Mainframe Services must provide hosting and operational support Services for both IBM and Unisys mainframe systems. These mainframe systems run several Logical Partitions (LPAR's) and Integrated Facility for Linux (IFL) partitions. The Contractor must support the mainframe operating systems and the management of the associated partitions. The number of support staff members required to perform the tasks listed below must be determined by the Contractor.

Listed below are the basic Services required to manage the Mainframe systems required by the Commonwealth. Contractor must include these Services in addition to the base level of Services in this Offering.

Reference Documentation

Schedule J.1 – Data Center Service Level Management

Schedule J.2 – Data Center Service Level Matrix

Schedule J.3 – Data Center SLA Definitions

Requirements	
1.	The Contractor must provide Mainframe systems and operations (Unisys, IBM). The Contractor must ability to purchase metered IBM & Unisys Million Instructions Per Second (MIPS). The Contractor must monitor local operations, troubleshoot and resolve operational

	issues. The Contractor must actively monitor the daily operations of all mainframe (current) systems. The Contractor must assume responsibility for all master and subordinate console functions. Issue operator commands to control all In-Scope platforms throughout the organization. The Contractor must provide all tools and apps that are currently being provided, for example MAPPER/APPMAP, browser based terminal emulation access, and middleware components (like OpenTI, IBM WBM & WMQ, etc.) that are critical to agency operations and application usage. The Contractor must assume the responsibility for and perform all console operations. The Contractor must monitor the performance of online interactive traffic and take appropriate action to resolve online-system-related incidents and/or problems, including escalating (as appropriate) the incident and/or problem to the proper Level 2 Support group. The Contractor must monitor the transmission of files between the Commonwealth and any other parties as designated by the Commonwealth. The Contractor must provide operational support for data transmission (send/receive), consistent with commercial or agency standards. The Contractor must manage, maintain, monitor, and control online and batch process, both scheduled and unscheduled (including on-request processing). The Contractor must maintain a log for each system detailing hardware / software configuration and critical service operations. The Contractor must review the system logs on a weekly basis to ensure critical system Services are processing without errors. The Contractor must maintain and update the operational documentation for all operations procedures and Services. •
2.	The Contractor must provide a review and analysis of mainframe usage to determine if current usage is required to support the needs of the mainframe stakeholders. The Contractor must perform an initial review and audit of the current mainframe usage, procedures and reports and provide an analysis of the current mainframe usage, processes and reports currently being supported. The Contractor must document its review and audit findings and recommendations.
3.	Production control and scheduling (including batch jobs) The Contractor must provide a process of scheduling batch jobs within

	Commonwealth agency defined windows to achieve maximum performance as long as required batch completion times are met. The Contractor must provide for automated scheduling of batch work and processes including backups. The Contractor must provide the capability for agencies to schedule and monitor batch processing. The Contractor must develop, maintain, and utilize an emergency contact list and escalation procedures to resolve abnormally ended jobs. The Contractor must resolve abnormally ended jobs caused by conditions external to production programs. The Contractor must repair abnormally ended jobs when possible and perform job restarts in accordance with the Service Management Manual. The Contractor must check job outputs and print queues, and change job priorities. The Contractor must notify Commonwealth agency customers in accordance with the notification procedures in the event that applications and batch processing do not execute properly.
4.	Batch Monitoring The Contractor must actively monitor batch operations on all mainframe systems on a daily basis. The Contractor must maintain a log for each batch system and review the system logs on a daily basis to ensure key batch Services are processing without errors. The Contractor must review and document its review of system logs on a daily basis to ensure critical batch Services are processing without errors. The Contractor must notify Commonwealth agencies in accordance with the notification procedures in the event that batch processing does not execute properly. The Contractor must provide online monitoring of batch processing by the Commonwealth.
5.	The Contractor must monitor system backup processing on a daily basis. The Contractor must provide a process to review daily backup log for successful completion. The Contractor must note any failures, initial and date the log, and correct the problem. The Contractor must create problem record for any abnormal condition and any repairs that have been made. Automated software process must be utilized to report the completion status of

	backup processing, with electronic notification of failures sent to Contractor technical support, and identified Commonwealth staff for follow up and corrective action.
6.	The Contractor must provide cost effective, operational, and technical support for the computing platform. The Contractor must provide platform level operational and technical support for computing platforms including Mainframe, Storage, AIX, LINUX, SAP, Oracle and Windows architects. The Contractor must provide Level 2 and Level 3 Support to the Service Desk and/or Commonwealth Users. The Contractor must provide technical advice and support to the Application Development and Maintenance (ADM) and Database Administration (DBA) staffs, as required. The Contractor must list the service levels for the various levels of service tiers that can be provided. See **Schedule J.1 Data Center Service Level Management** for the definitions of the expected options.
7.	The Contractor must ensure network connectivity to COPANET, and consistent system response times. The Contractor must utilize automated system management tool(s) to ensure real time monitoring and notification of system availability and response times. Stop / Start times of servers must be a source of input for SLA measurements
8.	The Contractor must ensure operating systems are maintained with the current system patch level, based on the Services provided by the server. The Contractor must analyze monthly service patches and determine which patches need to be applied. The Contractor must create a change record, log the update in the system log, and install based on system availability schedule. The Contractor must notify the Commonwealth of any scheduled or unscheduled service interruptions with consideration to Commonwealth scheduled holidays and standard workweek. The Contractor must implement a Patch Management Program to ensure the timely application of updates on all infrastructure platforms in accordance with

	Commonwealth IT policy guidelines.
9.	User Account Management The Contractor must provide certified system administration staff to create and maintain the registration of profiles, associated groups, and the security permissions (including password management) required to service the approved client base of the system and application.
10.	Procurement Planning The Contractor must provide a program and process to refresh the hardware at asset end-of-life, and when upgrades are needed to meet anticipated growth in utilization
11.	SLA Reporting The Contractor must collect actual system availability, utilization and response time data. The Contractor must create a SLA report on a monthly basis, for the Commonwealth and Contractor.
12.	The Contractor must provide Software License Management.
13.	The Contractor must coordinate at an agency level and account for any required patching as technology upgrades require.
Continual Service Improvement	
14.	Related to the project management and contract management role, the Contractor must provide Continual Service Improvement to reduce service risks.
15.	The Contractor must provide Continual Service Improvement to improve service quality. On a quarterly basis, the Contractor must make recommendations to the

	Commonwealth team any system changes that would be appropriate to maintain or improve SLA commitments.
16.	The Contractor must provide Continual Service Improvement to improve client satisfaction.
17.	The Contractor must provide Continual Service Improvement to ensure service transparency.
18.	The Contractor must provide Continual Service Improvement to improve/reduce costs.
Deliverables	
Deliverables are defined in **Schedule K – Key Program Deliverables**	

3.3.3.6 Security & Firewall

The Security & Firewall service must provide hosting and operational support Services for security products and firewalls located at the datacenters. These security devices and Services protect the equipment and applications in the datacenters from malicious attempts to penetrate the computing environment with worms, phishing, Trojan horse malware, and unlawful data access. The Contractor must install and maintain mainstream security hardware and software utilizing current industry best practices sufficient to protect the enterprise class datacenter environments with a significant volume of sensitive class data (e.g. HIPAA, CJIS, CHRIA, PCI, PII, etc.). The number of support staff members required to perform the tasks listed below must be determined by the Contractor.

Listed below are the basic Services required to manage the security & firewall systems required by the Commonwealth. The Contractor must include these Services in addition to the base level of Services in this Offering.

Reference Documentation

N/A

	Requirements	Describe Compliance
1.	The Contractor must monitor local security operations, troubleshoot and resolve operational issues. The Contractor must actively (normal daily process) monitor the operations of all security, firewall systems and security zones. The Contractor must maintain a log for each server/appliance/system and review the system logs on a daily basis to ensure key system Services are processing without errors. The Contractor must provide the ability to import data to agency SIEM or enterprise SIEM tool for correlation and reporting purposes. The Contractor must provide the ability for Commonwealth agencies to request security modifications (firewall changes) as documented in the CCPM. The Contractor must document review of the system security logs on a weekly basis to ensure critical system Services are processing without errors. The Contractor must complete weekly server log indicating which logs were reviewed, date and initial the log.	
2.	The Contractor must provide security training to Commonwealth personnel specific to the security Services being delivered. The Contractor must provide the Commonwealth with a resume or CV for Key Positions assigned to this engagement. The Contractor must comply with agency background checks and clearances as defined in Appendix A - Terms and Conditions.	
3.	The Contractor must achieve cost effective 24/7 security operational coverage for this critical system. The Contractor must provide dedicated security support staff onsite during scheduled business days, and automated log and notification systems to alert security team of possible intrusion events in real time mode.	

	The Contractor must provide Level 2 and Level 3 Support to the Service Desk and/or Commonwealth Users. Security staff must be available to respond and evaluate the severity of the event 24/7/365.
4.	The Contractor must ensure network connectivity, and ensure consistent system response times. The Contractor must utilize automated system management tool(s) to ensure real-time monitoring and notification of server availability and response times.
5.	The Contractor must ensure server/appliance operating systems are maintained with the current system patch level. The Contractor must implement a Patch Management Program to ensure the timely application of security updates on all infrastructure platforms in accordance with Commonwealth IT policy guidelines. The Contractor must ensure signature and threat analysis files are updated on a regular basis, and conform to industry best practices. The Contractor must analyze monthly service patches and determine which patches need to be applied, by server type. The Contractor must create a change record, log the update in the server log, and install based on server availability schedule. The Contractor must notify the Commonwealth of any scheduled or unscheduled service interruptions.
6.	The Contractor must provide active security operations, corrective action, and reporting by utilizing Contractor software to monitor inbound and outbound traffic for malicious patterns and content, and take appropriate protective measures. The ability to utilize security management software to detect threats and analyze firewall logs, to proactively detect and protect from malicious events. The Contractor must comply with agency specific security requirements. Comply with all agency and OA/OIT security policies and ITBs. On a quarterly schedule, the Contractor must run appropriate penetration testing, and report results to Commonwealth and Contractor. The Contractor must create monthly report on events, incidents and corrective activities. The Contractor must provide a report that indicates systems not in compliance with security standards.

	The Contractor must provide real time reporting of security breaches.
7.	The Contractor must provide SLA Reporting including but not limited to collecting actual system availability, utilization and response time data. che Contractor must Create a Service Level Agreement report for the Commonwealth and Contractor on a monthly basis.
8.	The Contractor must provide Software License Management.
Continual Process Improvement	
9.	Related to the project management and contract management role, the Contractor must provide Continual Service Improvement to reduce service risks.
10.	The Contractor must provide Continual Service Improvement to improve service quality. The Contractor must make recommendations to the Commonwealth team any system changes that would be appropriate to maintain or improve SLA commitments on a quarterly basis.
11.	The Contractor must provide Continual Service Improvement to improve client satisfaction.
12.	The Contractor must provide Continual Service Improvement to ensure service transparency.
13.	The Contractor must provide Continual Service Improvement to improve/reduce costs.

Deliverables
Deliverables are defined in **Schedule K – Key Program Deliverables**

3.3.3.7 Database Management Services

The Database Management Service must provide the Commonwealth with a "managed database" service offering. The service must include the database platform (Hardware/Software) and the ongoing database management administration Services. The Contractor must provide a multi-tiered level of service (e.g. Gold, Silver, and Bronze) across multiple database platforms. While the Commonwealth's application portfolio (over 2,000 applications) currently utilizes numerous database technologies, the majority of the applications that are utilizing database technologies are using Oracle, Microsoft SQL, IMS, Sybase, or DB2.

It is anticipated the Database Management Services will be an optional service that can be utilized by the Agencies beyond the basic infrastructure Services.

Reference Documentation

N/A

	Requirements
1.	The Contractor must design, manage, and administer database environments that support multiple business applications.
2.	The Contractor must provide Level 2 and Level 3 Support to the Service Desk and/or Commonwealth Users. ○
3.	The Contractor must monitor database backup and recovery processing on a daily basis. The Contractor must review daily backup log for successful completion. The Contractor must note any failures, initial and date the log, and correct the problem. The Contractor must create problem record for any abnormal condition and any repairs that have been made. Automated software process must be utilized to report the completion status of

	backup processing, with electronic notification of failures sent to Contractor technical support and identified Commonwealth staff for follow up and corrective action.
4.	The Contractor must provide a multi-tiered level of service (e.g. Platinum, Gold, Silver, Bronze, and Basic) for Oracle, Sybase, Microsoft SQL, IMS or DB2 database platforms. The Contractor must provide Level 2 and Level 3 Support to the Service Desk and/or Commonwealth Users.
5.	The Contractor must utilize the proposed service management Services (e.g. Incident, Service Request, Change, Configuration) to manage database management Services with multiple agency customers.
6.	The Contractor must provide a review and analysis of system performance/capacity to determine if current performance/capacities are sufficient to support the needs of the stakeholders.
7.	The Contractor must monitor system backup processing on a daily basis. The Contractor must review daily backup log for successful completion. The Contractor must note failures, and correct the problem. The Contractor must create problem record for any abnormal condition and any repairs that have been made. An automated software process must be utilized to report the completion status of backup processing, with electronic notification of failures sent to Contractor technical support, and identified Commonwealth staff for follow up and corrective action.
Continual Process Improvement	
8.	Related to the project management and contract management role, the Contractor must provide Continual Service Improvement to reduce service risks.
9.	The Contractor must provide Continual Service Improvement to improve service quality.

10.	The Contractor must provide Continual Service Improvement to improve client satisfaction.
11.	The Contractor must provide Continual Service Improvement to ensure service transparency.
12.	The Contractor must provide Continual Service Improvement to improve/reduce costs.

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

3.3.3.8 Limited-Use Colocation Services

While the Commonwealth's goal is to move to a fully managed infrastructure Services model, it is anticipated that there will be a need for the Contractor to provide some limited co-location Services within its proposed datacenter Services solution. Some examples of where colocation Services may be required are:

- Support for existing systems in the EDC prior to transformation to a fully managed service.
- 3rd Party Vendor Equipment that requires co-location with the primary systems for performance and/or security reasons.

The Contractor must provide datacenter co-location Services with the following options:

- Co-location Service Option 1: Datacenter Only (Rackspace, power, network connectivity, basic infrastructure Services)
- Co-location Service Option 2: Datacenter with Managed Services Option (Bronze, Silver, Gold Tiers) – Technology owned maintained by 3rd Party or Commonwealth
- Co-location Service Option 3: Remote Hands Support

Currently there are 3 areas within the Commonwealth EDC that are supporting co-location Services. EDC facility summary is provided as **Exhibit D.7**. While many of these systems will be migrated to a fully managed service over time, the Contractor must plan for co-location space in its Datacenter Architecture.

Reference Documentation Exhibit D.1 through D.15 Series - Enterprise Datacenter (EDC) Exhibits	
Requirements	
1.	The Contractor must provide colocation Services within each of the datacenters. One of those centers must be the Commonwealth EDC.
2.	The Contractor must provide Colocation Service Option 1: Datacenter Only (Rackspace, power, network connectivity, basic infrastructure Services)
3.	The Contractor must provide Co-location Service Option 2: Datacenter with Managed Services Option (Bronze, Silver, Gold Tiers) – Technology owned maintained by 3rd Party or Commonwealth
4.	The Contractor must provide Co-location Service Option 3: Remote Hands Support
Continual Process Improvement	
5.	Related to the project management and contract management role, the Contractor must provide Continual Service Improvement to reduce service risks.
6.	The Contractor must provide Continual Service Improvement to improve service quality.
7.	The Contractor must provide Continual Service Improvement to improve client satisfaction.
8.	The Contractor must provide Continual Service Improvement to ensure service transparency.
Deliverables	
Deliverables are defined in **Schedule K – Key Program Deliverables**	

3.3.4 Capacity on Demand Services

3.3.4.1 Server Capacity on Demand

The Server Capacity On Demand is an Infrastructure as a Service (IaaS) offering that ensures the ready availability of server and mainframe capacity to accommodate cyclical, and seasonal, processing requirements, sudden or unplanned production demands, and short-term application development needs. Server capacity may be physical or virtual as requested by the Commonwealth.

The Server Capacity On Demand would include support for the following system platforms:

- X86
  - Windows
  - Linux
- I Series
  - i5/OS
- P Series
  - Linux
  - AIX
- Mainframe
  - IBM
  - Unisys

Reference Documentation

N/A

Requirements

1.	The Contractor must provide a provisioning capability to support on-demand requests for server resource capacity. The Commonwealth will require access to additional capacity on demand for the following platforms: X86 • Windows • Linux IBM I Series • i5/OS IBM P Series • Linux • AIX

	Mainframe • IBM • Unisys
2.	The Contractor must maintain an adequate inventory of Windows/Linux, mid-range, and Mainframe server capacity that must be sufficient to satisfy forecasted informal, ad hoc, and cyclical Commonwealth requests.
3.	As a function of ongoing account management, the Contractor must meet with the Commonwealth/Agencies to assess future server requirements.
4.	The Contractor must encourage Commonwealth server conservation via server virtualization when appropriate.
5.	The Contractor must provide expedited service, when requested, to satisfy urgent requirements.
6.	The Contractor must provide a self-provisioning tool to be used by the agencies to order and configure servers.
Continual Process Improvement	
7.	Related to the project management and contract management role, the Contractor must provide Continual Service Improvement to reduce service risks.
8.	. The Contractor must provide Continual Service Improvement to improve service quality.
9.	The Contractor must provide Continual Service Improvement to improve client satisfaction.
10.	The Contractor must provide Continual Service Improvement to ensure service transparency.
11.	. The Contractor must provide Continual Service Improvement to ensure service sustainability.
12.	The Contractor must provide Continual Service Improvement to improve/reduce costs.

Deliverables
Deliverables are defined in **Schedule K – Key Program Deliverables**

3.3.4.2 Storage Capacity on Demand

The Storage Capacity On Demand service is an Infrastructure as a Service (IaaS) offering that ensures the ready availability of storage capacity to accommodate cyclical, or seasonal, storage requirements, sudden or unplanned production demands, short-term application development needs, and storage access for web enabled devices.

Reference Documentation

N/A

Requirements

1.	The Contractor must maintain an adequate access to, or supply of storage area equipment, to satisfy forecasted informal, ad hoc, and cyclical Commonwealth requests. ○
2.	The Contractor must meet with the Commonwealth on a annual basis, or as requested, to assess future storage requirements.
3.	The Contractor must encourage data storage conservation via data de-duplication, compression, and other industry techniques.
4.	The Contractor must provide expedited data storage service to satisfy urgent requirements, as requested.
5.	The Contractor must provide online storage capabilities (Centralized Private Cloud Storage), which includes web service, browser, and mobile device accessibility, that are fully secure, (compliant with ISO 27000, NIST 800-53, and Secure SDLC). This service must provide file-level encryption, multiple hierarchical permission levels, account level dynamic storage-sizing, and anti-virus capability.
6.	Storage solution must include the capability to make quick copies of databases (SNAPS, Flash copies). Storage backup proposals must include disk-2-disk solutions.

Continual Service Improvement	
7.	Related to the project management and contract management role, the Contractor must provide Continual Service Improvement to reduce service risks.
8.	The Contractor must provide Continual Service Improvement to improve service quality.
9.	The Contractor must provide Continual Service Improvement to improve client satisfaction.
10.	The Contractor must provide Continual Service Improvement to ensure service transparency.
11.	The Contractor must provide Continual Service Improvement to ensure service sustainability.
12.	The Contractor must provide Continual Service Improvement to improve/reduce costs.
Deliverables	
Deliverables are defined in **Schedule K – Key Program Deliverables**	

3.3.4.3 DR Infrastructure on Demand

The DR Infrastructure On Demand service is an infrastructure as a service (IaaS) offering that ensures the ready availability of DR infrastructure; servers, storage systems, networking capabilities, etc. This infrastructure must enable Commonwealth datacenters to recover critical business applications and data in the event of a disaster.

Reference Documentation

N/A

	Requirements
1.	The Contractor must maintain an adequate inventory of servers, storage systems, and networking capacity sufficient to satisfy forecasted informal, ad hoc, and cyclical Commonwealth requests. ○
2.	The Contractor must meet with the Commonwealth on a annual basis and as requested to assess its future DR requirements.
3.	The Contractor must revise datacenter and disaster recovery plans, upon request of the Commonwealth.
4.	The Contractor must provide support for the Commonwealth with identifying and establishing DR or Continuity of Government (CoG) capabilities and plans.
	Continual Process Improvement
5.	Related to the project management and contract management role, the Contractor must provide Continual Service Improvement to reduce service risks.
6.	The Contractor must provide Continual Service Improvement to improve service quality.

7.	The Contractor must provide Continual Service Improvement to improve client satisfaction.
8.	The Contractor must provide Continual Service Improvement to ensure service transparency.
9.	The Contractor must provide Continual Service Improvement to ensure service sustainability.
10.	The Contractor must provide Continual Service Improvement to improve/reduce costs.

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

3.3.4.4 Additional Technical Services

The Commonwealth may require additional technical support beyond the standard service level based infrastructure Services. The availability and access to skilled resources would complement the standard hosting offerings. The Contractor is expected to provide these additional resources for both short and longer-term engagements.

Reference Documentation

N/A

Requirements

1.	The Contractor must provide access to skilled technology resources. Additional technology support Services categories include but are not limited to: • Infrastructure (mainframe, mid-range and x86) Architects/Engineers • Performance Specialists

	• Database Architects • Database Analysts • Security Architects • Security Analysts • Unix (AIX, Linux) Administrators • Windows Server Administrators • Mainframe Systems Programmers • Batch Administrators • Microsoft Product Specialists (e.g. Exchange, SharePoint) • 3rd Party Software Product Specialists • Basis and SAP Oracle support
Deliverables	
Deliverables are defined in **Schedule K – Key Program Deliverables**	

3.4 Transition Services

3.4.1 Transition Services – Guiding Principals

At present, the Commonwealth's information technology Services are hosted at a variety of Commonwealth datacenters, including:

- Shared enterprise facilities - (EDC and DPH) and;
- Agency facilities, for example those managed and maintained by DPW, DOR, DOH, PSP and DLI.

The Commonwealth datacenter locations are identified in Exhibit S - Datacenter locations.

In an effort to reduce datacenter costs, simplify datacenter administration, and provide more robust and reliable information Services to the Commonwealth, the Commonwealth datacenter modernization initiative calls for the phased migration or transition of Commonwealth information Services to the newly-established Contractor managed multi datacenter environment.

The Guiding Principles associated with the transition to the new datacenter environment are:

- Transition approach must meet the milestone objectives as described in **Schedule D – Transition Milestones**.
    - Based on the Commonwealth's number of licenses, additional licenses may be needed for the transition of Services. The Contractor is responsible for any additional licenses needed for the transition of service.
    - The Commonwealth, at its sole discretion, may procure the software licenses through existing statewide contract.
- Initial transition approach of the Commonwealth's mainframe and SAP environments requires that the results be as close to the Commonwealth's current configuration as technically possible.
    - Any deviations from current environments must be approved by the Commonwealth.
- Customized approach developed to meet the needs of the Commonwealth
    - The selected Contractor's transition approach must account for Commonwealth specific needs such as the Transition Considerations and Critical Configuration Considerations as described in Exhibits R and T.
    - The selected Contractor must implement a discovery process during transition planning to acquire information required to develop a Detailed Transition Plan.
    - The selected Contractor must include application level transformation models. Transformation models must take into account the initial transition approach that the Commonwealth's mainframe and SAP environments must be as close to the Commonwealth's current configuration as possible.

- The Contractor must provide transformation project managers experienced in projects of similar size and complexity.

This project requires:

- Strong governance model, which includes:
    - Clearly defined roles and responsibilities
    - Jointly developed processes
    - Effective meetings and reporting framework to minimize resource requirements while achieving goals
    - Mechanisms in place to identify and address risks and issues
    - Compliance with applicable policies, standards, processes, and procedures
- Effective communication, which includes:
    - Consistent delivery of key messages through well-defined communication plans
    - Tailored communications to target audiences and stakeholders
    - Communications to meet the needs of the Commonwealth.
- Collaboration and teamwork, which includes:
    - Detailed upfront project planning and feedback
    - Agreement on status for reporting purposes

- Plans scaled to address Commonwealth agency differences in size and complexity
- Establishment and support for successful deliverable review process
- Feedback on deliverables throughout the life of the project.

3.4.2 Transition Planning/Governance

The Contractor's Transition Program Management Office (TPMO) must contain a dedicated consolidation specific program team. The team is responsible to jump-start the consolidation program by bringing respective stakeholders together for a series of transition workshops. The transition workshops must work to align the stakeholders, and produce the following deliverables:

- Overall transition approach and strategy for Server and Mainframe consolidation
- Transition and consolidation governance plan
- Transition risk assessment plan
- Consolidation cost/benefit analysis
- Consolidation stakeholder transition agreements
- Consolidation transition planning guidelines

The TPMO must provide program management Services to deliver architecture, transition plan integration, and organizational change management, as well as quality assurance, verification of testing, financial oversight, and operational readiness for the Mainframe and Server transition/consolidation program. The TPMO must exist under the overall Contractor's PMO office and must include a combination of resources dedicated to the effort full time, plus resources that participate in the program on an as needed basis. The program plan and architecture must be developed by the Contractor and approved by the Commonwealth. The Contractor must ensure processes and tools are implemented to support Transition change control, schedule, quality, communications, risk and issues management.

Proposed Transition Plan

The Commonwealth anticipates the following high-level sequence of transition activities. At minimum, the Contractor's Transition Plan must reference these activities and project timeframes.

Transition Activities

The high level transition milestones and deliverables are described in **Schedule D - Transition Milestones** and **Schedule K - Key Program Deliverables**.

Target Datacenter Transitions

The following table includes the target datacenter facilities that are to be initially transitioned by the Contractor. The target datacenter facilities are defined as the physical Commonwealth facilities that are selected to be transitioned to the Contractor's control and/or facilities. The Contractor must coordinate with each Commonwealth agency or datacenter representative to create a *Facility Specific Transition Plan* for each targeted facility. The Contractor must include target datacenter transitions in its Transition Timeline. The Contractor must include a "pilot"

transition approach to ensure successful transitions of Commonwealth applications and infrastructure. This approach must demonstrate to the agencies that Contractor's approach must be successful before moving forward with additional transition phases.

Contractor must establish a high-speed direct link (not via COPANet) with the current DPH location to enable "systems" connectivity that would facilitate the ability to effect smoother transition of data.

The selected Contractor must not charge the Commonwealth for completion of a Transition Milestone. All transition costs must be included in the selected Contractor's unit prices for the Services.

	Target Datacenter Facilities		Transition Requirement Notes
	Group1 Transitions		
1	**DPH** (All Agency Mainframe – Unisys/IBM; IES SAP, and all other Agency hosted environments)		• The DPH operation and all of its supported agency application workloads must be successfully migrated out of the current facility to the Contractor's Datacenter. • Operations support must be assumed by the Contractor once the workloads are successfully moved to the new provider's datacenter environment. • Key Transition Milestone(s): o Refer to **Schedule D - Transition Milestones**
1	**EDC**		• Contractor must assume operations support of the EDC datacenter • Key Transition Milestone(s): o Refer to **Schedule D - Transition Milestones**
Group 2 Transition			
2	**DLI**		• The DLI datacenter operations and all of its supported application workloads must be successfully migrated out of the DLI facility to the Contractor's Datacenter. • Key Transition Milestone(s): o Refer to **Schedule D - Transition Milestones**
Group 3 Transitions			
3	**DPW** – Rm. 105, 106 (Lower Environments, PACSES)		• The DPW Rooms 105, 106 datacenter operation and all supported application workloads must be successfully migrated out of the current DPW facility to the Contractor's Datacenter architecture. • Key Transition Milestone(s): Refer to **Schedule D - Transition Milestones**

	Target Datacenter Facilities		Transition Requirement Notes
3	**DOR**		• The DOR datacenter operation and all of its supported application workloads must be successfully migrated out of the current DOR facility to the Contractor's Datacenter architecture. • Key Transition Milestone(s): ○ Refer to **Schedule D - Transition Milestones**
3	**DOH**		• The DOH datacenter operation and all of its supported application workloads must be successfully migrated out of the current DOH facility to the Contractor's Datacenter architecture. • Key Transition Milestone(s): ○ Refer to **Schedule D - Transition Milestones**
3	**PSP**		• The PSP datacenter operation (Headquarters) and all of its supported application workloads must be successfully migrated out of the current PSP facilities to the Contractor's Datacenter architecture. • Key Transition Milestone(s): ○ Refer to **Schedule D - Transition Milestones**

3.4.2.1 Transition Program Management

The TPMO function ensures the non-disruptive migration of Commonwealth information Services from current Commonwealth host locations, to the Contractor provided multi datacenter environments.

The Contractor must establish a TPMO and develop the requisite transition plans.

A transition approach and detailed transition plan for each of the Commonwealth's existing Datacenters must be developed by the Contractor and approved by the Commonwealth. The Commonwealth has over 2,000 business applications with over 50% designated mission critical. The Contractor must work with each agency to determine its application environment within each facility. The Contractor's target datacenter environment must be configured and tested prior to migration of the application.

Reference Documentation

Schedule D - Transition Milestones

Requirements		Describe Compliance
1.	The Contractor must establish a TPMO to manage all information service transition activities. The Office must be jointly administered by Contractor and Commonwealth staff. The Contractor must provide a communication plan that must provide an information vehicle for all interested parties.	
2.	The Contractor must provide a functional organization chart for the TPMO, including an estimate of the type and number of full time Contractor resources that are required to ensure the successful transition of Services from current multiple datacenters to the Contractor's datacenter Services.	
3.	The Contractor must analyze applications and design the required computing architecture to migrate Commonwealth datacenters to Contractor datacenter environments. Hardware, software, network, etc. The Contractor must work with Commonwealth technical staff to ascertain the requirements to successfully migrate processing to Contractor datacenter environments	

4.	Optimize Current Process and Procedures – The Contractor must coordinate with Commonwealth agencies to review and plan for a transition of processes and procedures.
5.	The Contractor must revise datacenter DR plans on the occasion of major changes to the datacenter hardware, software, or network portfolio to reflect those major changes.
6.	The Contractor must establish an IT infrastructure that meets all application processing requirements. The Contractor must confirm that the target IT infrastructure meets or exceeds current computing requirements. The Contractor must work with Commonwealth technical staff to design and build the infrastructure required to support the applications being migrated to the Contractor multi datacenter environment.
7.	A multi-faceted Transition Strategy is required: • Comprehensive; • Non-disruptive; and • Compliant with Commonwealth requirements. The Strategy must address the transition of: • Shared infrastructure elements, as appropriate; and • Specific information Services. • Disparate Agency application architectures and impacts to move to the new environment(s) The Strategy must also address the following: • Cost/Benefit for the Agency • Risks and Risk Mitigation Plan The migration order of the Commonwealth datacenters must be provided by the Commonwealth.
8.	The Contractor must identify mandatory requirements and critical success factors that have a direct impact on developing a successful transition plan

9.	The Contractor must create a Transition Timeline that outlines the overall timeline starting at effective date and continues through delivering transition Services for each of the targeted datacenters.
10.	The Contractor must create a generic Infrastructure Element Transition Plan that may be readily adapted to accommodate specific infrastructure element transitions. The Contractor must create a prospective Infrastructure Element Transition Plan. Appropriate EDC, DPH and other Agency Datacenter hardware elements may be re-purposed wherever possible.
11.	The EDC Managed Services datacenter assets must be managed and maintained by the Contractor until they are transitioned to the Contractor's managed Services. The current maintenance contract for the EDC servers is scheduled to expire on June 30, 2014.
12.	The Contractor must create, manage and execute an application / infrastructure migration plan. The Contractor has the primary responsibility for planning and executing the transition of infrastructure elements, with support of Commonwealth technical and business support staff. The Contractor must provide adequate tools and techniques for moving and migrating Commonwealth data to the new target storage environment. The Contractor must ensure that critical applications are not decoupled from key infrastructure components causing system latency.
13.	The Contractor must create a generic Information Service Transition Plan that may be readily adapted to accommodate specific information service transitions.
14.	The Contractor must meet with Commonwealth to produce and execute specific Information Service Transition Plans. The Contractor must select cut over windows

	that minimize system unavailability and coordinate approval with the affected agency. The Contractor must communicate to the Commonwealth cut over date and times. The Contractor must setup a special call number and support staff to take calls concerning the migration, these Services must be made available to transitioned users until the transition is officially signed off as completed. .
15.	The Contractor must work with Commonwealth to create testing, business acceptance and fallback plans.
16.	Service Management Systems – Contractor must transition all agency system management platforms currently in place to the Contractor, consolidating all infrastructure system management responsibilities. The Contractor must make available within the Service Catalog all system management platforms and tools that are currently supporting the Commonwealth infrastructure.
17.	CMDB – The Contractor must work with the Commonwealth to acquire asset information to support the asset management system and configuration management system.
18.	Chargeback – The Contractor must work with the Commonwealth to interface with the Commonwealth's billing processing and validation ITSM system to provide a chargeback system for new and existing Services available on the Contractor's Service Catalog.
19.	Identify Options and Costs – The Contractor must list the appropriate different options that must satisfy the requirements of the transition scope. The Contractor must communicate options with the Commonwealth and obtain approval on selected option(s) to proceed.

20.	The Contractor must expand/reconfigure datacenter facilities to accommodate growth in Commonwealth information and information systems.
21.	The Contractor must produce weekly reports on the progress of the information service transition initiatives.
Deliverables	
Deliverables are defined in **Schedule K – Key Program Deliverables**	

3.4.2.2 Security Transition Activities

To maintain continuity of Services, the Contractor must provide training to Contractor's employees and subcontractors on security policies during initial phase of the Transition.

Reference Documentation

Schedule D - Transition Milestones

Requirements

1.	Baseline Security Risk and Vulnerability Assessment The Contractor must conduct a security risk assessment, which includes a penetration test on the In-Scope systems, an architecture review, and a vulnerability assessment. This assessment must result in a report with recommendations for meeting the Commonwealth's baseline security standard.
2.	Security Training The Contractor's security team must meet with the Commonwealth's Security teams (OA & Agency) to participate in creating a comprehensive Security Program strategy. The Contractor and the Commonwealth Security teams must develop security awareness training content consisting of the Contractor's Security Plan documentation, Commonwealth OA and agency security policy guidelines. Security training must be mandatory for employees, contractors and subcontractors assigned to work on the Commonwealth's Datacenter project. Appropriate levels of training must be designated and tracked for compliance based on the specific area the employee must be working in. Both an individual's current training status and overall attainment of group training goals must be tracked and reported in the security clearance database. These levels must range from general security awareness that all employees must participate in to task-specific security and governance requirements targeted at operations, specialist, Commonwealth agency specific regulations, or working rules needed for compliance with Commonwealth or federal mandates unique to certain Commonwealth agencies and programs. This training must be delivered both during the new hire process, and on a regular schedule to be determined during Transition as new updates become necessary.

3.	Initial Security Plan During the initial phase of the Transition the Contractor's security team must work with the Commonwealth's Security Team to create a Security Plan. Begin work on draft policy and procedure documents collectively known as the Security Plan during the start of the Transition Risk and Vulnerability Assessment, which must be completed one (1) month prior to Transition activities. The Contractor must use best practice security standards (as outlined in the Requirements section of the RFP) along with past engagement experience to provide an outline that must address but must not be limited to the following: security strategy and technology roadmaps, security operations procedures, standard hardware and software security configurations, physical security policies and procedures, security incident management, private and protected data use standards, and audit procedures and reporting standards. This set of documents must be used as the foundation of the Contractor's master security plan for Datacenter operations which must be reviewed and updated on an annual basis. ○
4.	On-boarding and off-boarding The Contractor must conduct required background checks for its employees working on the Commonwealth Datacenter project. Where appropriate, The Contractor must use identity management tools to manage access to the systems requiring access by its employees. For systems where the Contractor is unable to use its identity management system, assign staff to manage the access. The Contractor must train Contractor employees on his or her responsibilities within the contract. For logical and physical access to Commonwealth Co-location facilities and environments not managed by the Contractor, the Commonwealth's security access request process must be followed. For off-boarding, The Contractor must update security clearance database with the status of Contractor employee and concurrently update its identity management tool to ensure the access is revoked. The Contractor must provide a monthly report describing personnel actions including but not limited to; new hires, terminations, any change in employee status/duties, etc.,

5.	Complete DR Transition Activities The Contractor must conduct knowledge transfer during the initial phase of the Transition, including review of Commonwealth DR plans and review of Third Party DR contracts. The Contractor must also update the DR plan contact information and any changes made in the first six (6) months of Transition.
Deliverables	
Deliverables are defined in **Schedule K – Key Program Deliverables**	

Schedule G

Staffing Plan and Key Positions

1. Offeror Key Personnel

This schedule lists the Key Personnel. For the purposes of this schedule and the Contract, the following Offeror roles/titles have the following responsibilities:

a) **Engagement Executive -** The Engagement Executive is responsible for overall accountability of the Commonwealth business relationship and the success of the project. Serves as the primary contact for the management of the contract and assist Commonwealth customers with all facets of services, including assisting in building strong customer teaming relationships and delivering the highest level of customer service and satisfaction.

b) **Program Manager (Offeror Project Manager) -** The Program Manager has overall responsibility for delivery of the Services to the Commonwealth and exercises day-to-day supervision of the Program Management Office (PMO). The PMO Manager will manage the overall relationship ensuring that the Offeror fulfills all of its obligations under the Contract by working with the Commonwealth Management Committee to establish, manage, and meet commitments, requirements, and expectations to ensure operational compliance with the Contract. The PMO Manager will have a detailed knowledge and understanding of the Service Levels structure and credits, billing formats, hierarchies and credits, and Services being provided to ensure that Offeror fulfills its obligations under the Contract, including all obligations relating to deliverables. There will be one PMO Manager 100% dedicated to the Commonwealth for the Term. The PMO Manager will be located at the Offeror's Harrisburg, Pennsylvania location.

c) **PMO Transition Manager(s)** – The PMO Transition Manager provides technical expertise and leadership during the transition of the current state datacenter services to the steady state managed datacenter services (i.e. the Commonwealth's new datacenter structure and services to be provided by Offeror pursuant to the Contract), and provides continuing engineering support through the remainder of the Term. In conjunction with the Commonwealth, the PMO Transition Manager develops plan(s) (inclusive of a detailed schedule(s) for performing associated tasks) for Offeror's implementation and transition of the Commonwealth from its legacy providers, cooperating with the Commonwealth to obtain the Commonwealth's approval and acceptance of the Transition Plan, and identifying the Transition Plan roles, responsibilities, and performance contingencies.

There will be two (2) PMO Transition Managers 100% dedicated to the Commonwealth for the entire Ramp-up Period. After the Ramp-up Period, the number of Transition Managers is reduced to one for the Term. The Transition Managers will be located at the Offeror's Harrisburg, Pennsylvania location during transition period.

d) **Availability Manager** – The Availability Manager is responsible for the overall service level management program for all of the Datacenter Services delivered.

e) **Service Level Management Analyst** – The PMO Service Level Management Analyst will prepare and package mutually agreed to operational reports, SLA reports, maintains Operations Manual, and oversees the Governance performance reporting. The Service Level Management Analyst will be located at the Offeror's Harrisburg, Pennsylvania location.

f) **Sr. Enterprise Infrastructure Architect** – The Enterprise Infrastructure Architect is responsible for the overall technology management program for the Datacenter Services delivered. The Enterprise Architect will provide executive level technology oversight to the Program. The Enterprise Architect will provide leadership in the forecasting and outlook for new technologies and services to be added during the term of the Program. The Enterprise Architect must have deep understanding of infrastructure, application deployment, and web and software applications.

g) **Incident Management Manager** - The PMO Incident Manager will provide technical and operational escalations management and resolution by working with the help desk and Operations Centers to provide escalation oversight and back up support for Program Manager. The PMO Incident Manager will provide SLA review, compliance, and management; facilitate chronic issue management and resolution; and address operational and delivery issues and adherence to performance; assist with incidents, issues, and escalations; and provide root cause analysis and resolution.

h) **Change Manager and Change Analyst** – The Change Manager and Change Analyst will provide oversight and overall coordination of standard change management, process across products and services, and provide change management for future strategy and planning.

i) **Finance Manager and Finance Analyst** – The Finance Manager and Finance Analyst will provide billing support and facilitation of the consolidated billing process support for the one single invoice to the Commonwealth.

j) **Agency Account Managers** – Offeror will provide a minimum of five (5) dedicated Agency Account Managers responsible for understanding all of the services provided by Offeror and providing guidance to the agencies in understanding their datacenter business needs. Offeror must assign an Agency Account Manager to each agency that purchases services through the contract. Not all Agency Account Managers must be assigned to a single agency. Offerors shall identify the number of Agency Account Managers that will be assigned to this project as part of their proposal. Agency Account Managers will act as a liaison between Offeror and the agency; strengthen the strategic relationship between Offeror and the Commonwealth; maintain overall responsibility for sales, support, and operations; ensure that agreements are finalized and signed by all parties; provide periodic briefings to the Commonwealth on new services and technologies that may be of interest/use and provide the Commonwealth with pricing information on request. The Agency Account Managers will be located at the Offeror's Harrisburg, Pennsylvania location.

k) **Agency Infrastructure Architects (Service Area Leads)** - Offeror will provide a minimum of five (5) Infrastructure Architects responsible for the detailed design engineering of the Commonwealth's specific datacenter services designs and quotes and for coordinating Commonwealth related requests. There will be at least five (5) Infrastructure Architects dedicated to the Commonwealth for the Term.

l) **Security Manager** – Offeror will provide a Security Manager to oversee all aspects of the project to ensure compliance with all security standards and requirements.

2. Offeror Key Personnel Table

Role/Position	Name	Company
Engagement Executive	[redacted]	Unisys Corporation
Program Manager/Service Delivery	[redacted]	Unisys Corporation
PMO Transition Manager 1	[redacted]	Unisys Corporation
PMO Transition Manager 2	[redacted]	IBM Corporation
Security Manager	[redacted]	Unisys Corporation
Service Excellence Officer	[redacted]	Unisys Corporation
Sr. Enterprise Infrastructure Architect	[redacted]	Unisys Corporation
Incident Management Manager	[redacted]	Unisys Corporation
Availability Manager	[redacted]	IBM Corporation
Service Level Management Analyst	[redacted]	Unisys Corporation
Change Manager	[redacted]	Unisys Corporation
Change Analyst	[redacted]	Unisys Corporation
Agency Account Manager 1	[redacted]	Unisys Corporation
Agency Account Manager 2	[redacted]	Unisys Corporation
Agency Account Manager 3	[redacted]	Unisys Corporation
Agency Account Manager 4	[redacted]	IBM Corporation
Agency Account Manager 5	[redacted]	Unisys Corporation
Agency Infrastructure Architect 1	[redacted]	Unisys Corporation
Agency Infrastructure Architect 2	[redacted]	Unisys Corporation
Agency Infrastructure Architect 3	[redacted]	Unisys Corporation

Role/Position	Name	Company
Agency Infrastructure Architect 4	[redacted]	PCN
Agency Infrastructure Architect 5	[redacted]	IBM Corporation
Agency Infrastructure Architect 6	[redacted]	IBM Corporation
Finance Analyst	[redacted]	Unisys Corporation
Finance Manager	[redacted]	Unisys Corporation
IBM Project Executive	[redacted]	IBM
IBM Service Delivery Executive	[redacted]	IBM

SCHEDULE H

COMMONWEALTH COMPUTING PROCEDURES MANUAL

Contents

1 PURPOSE 3

1.1 Organizational Overview 3

1.2 Transition and Support Activities and Responsibilities 4

1.3 IT Service Management Procedures 5

1.4 Financial Management Procedures 12

1.5 Contract Management Procedures 14

1.6 Relationship Management Procedures 16

1.7 Offeror Operational Procedures 18

1.8 The Commonwealth Customer Operations Manuals 20

Content	Description
1 PURPOSE	The Offeror should describe the purpose of the Commonwealth Computing Procedures Manual. This section should address who should use the Manual, how the Manual is organized, how the initial version and updates will be distributed, version control procedures for the Manual, when updates will occur, and procedures for authorizing and implementing updates. It is intended that the structure of the Manual will require that the individual compliance requirements and business rules of each participating Commonwealth Customer are separately identified where applicable for each section or component part of the Manual.
1.1 Organizational Overview	
1. Offeror Governance Organization	Include organization charts, description of functions performed, contact information.
2. Offeror Management and Delivery Organization	Include organization charts, description of functions performed, contact information.
3. Key Contacts - Offeror	A list of contacts that are key users of the Services and/or perform a liaison function in regard to the Services (by Commonwealth and Commonwealth Agencies, by location).

Content	Description
4. Key Contacts – Third Parties	A list of key Third Parties (maintenance providers, software providers, telecom carriers, etc).
1.2 Transition and Support Activities and Responsibilities	
1. Overall Management and Reporting Process	A description of Offeror management structure, reporting, and review process associated with Transition Services and Transformation Services.
2. Critical Deliverables and Milestones	A list of Critical Deliverables, milestones and timeline for the Transition Services and Transformation Services periods.
3. Interim Performance Management Procedures	A description of interim procedures to monitor and coordinate Service delivery, including Problem Management, Change Management, Service Level monitoring and reporting, physical and Logical Security, project management, work authorization, etc. A description of the responsibilities of both Parties.

Content	Description
4. Interim Financial Management Procedures	A description of interim procedures for invoicing, invoice verification, charge back to the Commonwealth Customers, determining Resource Unit volume by Service Component, asset management, asset transfers, forecasting, Commonwealth Customer support, etc. A description of the responsibilities of both Parties.
5. Interim Contract Management Procedures	A description of interim procedures for managing and administering the Agreement including proposed changes to the Agreement, interpretation procedures, issue-escalation process, and disputes. A description of the responsibilities of both Parties.
6. Other Transition and Support Procedures and Responsibilities	Any other pertinent procedures and responsibilities.
1.3 IT Service Management Procedures	
1. Service Desk	The facilities, associated technologies, and fully trained staff who respond to Calls, coordinate all Incident Management, Problem Management and Request Management activities, and act as a single point of contact for Authorized Users in regard to the Services.

Content	Description
2. Incident Management	The use of people, processes and technology with the primary goal to restore normal Service operations as quickly as possible and minimize the adverse impact on business operations, thus ensuring that the best achievable levels of service quality and availability are maintained.
3. Problem Management	The process, software, techniques and procedures that aid in identification, tracking, communication, and resolution of Problems arising in Customer's IT Environment, and resolving those Problems arising from or related to the Services. The goal of Problem Management is to minimize the adverse impact of Incidents and Problems on the business that are caused by errors within the IT infrastructure, and to prevent recurrence of Incidents related to these errors. In order to achieve this goal, Problem Management seeks to get to the root cause of Incidents and then initiate actions to improve or correct the situation.
4. Change Management	The processes relating to planning and performing all changes in IT environment pertaining to the Services, including changes to individual components and coordination of changes across all components. The Change Management processes will support and include checkpoints to determine any potential or required Change Control Procedures and includes a process of controlling changes to the infrastructure or any aspect of Services, in a controlled manner, enabling approved changes with minimum disruption.

<table>
<tr><th>Content</th><th>Description</th></tr>
<tr><td>5. Configuration Management</td><td>The process of identifying and defining CIs in a system, recording and reporting the status of CIs and RFCs, and verifying the completeness and correctness of the CIs.

The following data fields are required as a minimum for Asset/Configuration Management (any number of these may require that auditing be enabled.):

<table>
<tr><th>Physical Attributes</th><th>Logical Attributes</th></tr>
<tr><td>CI Name</td><td>System Role</td></tr>
<tr><td>Serial Number</td><td>Primary Capability</td></tr>
<tr><td>Commonwealth Asset Tag</td><td>Capability</td></tr>
<tr><td>Owner</td><td>Complexity</td></tr>
<tr><td>Ownership Type</td><td>Priority</td></tr>
<tr><td>Funding Source</td><td>Storage (currently TPC tool)</td></tr>
<tr><td>Purchase Date</td><td>24 x 7 Access</td></tr>
</table>
</td></tr>
</table>

Content	Description	
	Life Cycle Dates	**OS Billing Platform**
	Status	**Operating System (OS)**
	Physical Location	**OS Version**
	Region	**OS Manufacturer**
	Product Name	**Last Scan Date**
	CI Type	**Audit Report**
	Model/Version	**Relationships**
	Manufacturer	**Applications**
	Supplier Name	**Application SW Info**
	Tier	**Disaster Recovery Priority**
	Asset Classification	**Customer Project Identification**
		Drivers and Version Numbers

Content	Description
	<table><tr><td>**Date of Last Inventory**</td><td>**Service Pack**</td></tr><tr><td></td><td>**Network Protocol**</td></tr><tr><td></td><td>**Assigned IP Address(s)**</td></tr><tr><td></td><td>**DNS Host Name**</td></tr><tr><td></td><td>**Domain**</td></tr><tr><td></td><td>**Physical or Virtual Identifier**</td></tr><tr><td></td><td>**Funding Source**</td></tr><tr><td></td><td>**Memory allocated**</td></tr><tr><td></td><td>**Installation date** **Related CIs**</td></tr></table>

Content	Description
6. Release Management	The process responsible for planning, scheduling and controlling the movement of Releases to Test and Live Environments. The primary objective of Release Management is to ensure that the integrity of the Live Environment is protected and that the correct Components are released. Release Management works closely with Configuration Management and Change Management.
7. Request Management and Fulfillment	The process responsible for managing the lifecycle of all Service Requests.
8. Availability Management	The process responsible for defining, analyzing, Planning, measuring and improving all aspects of the Availability of IT services. Availability Management is responsible for ensuring that all IT Infrastructure, Processes, tools, roles etc. are appropriate for the agreed Service Level targets for Availability.
9. Capacity Management	The process responsible for ensuring that the Capacity of IT Services and the IT Infrastructure are able to deliver agreed Service Level targets in a cost effective and timely manner. Capacity Management considers all Resources required to deliver the IT Service, and plans for short, medium and long term business requirements.

Content	Description
10. Service Level Management (SLM)	The process responsible for negotiating SLAs, and ensuring that these are met. SLM is responsible for ensuring that all IT Service Management Processes, OLAs, and Underpinning Contracts, are appropriate for the agreed Service Level targets. SLM monitors and reports on Service Levels, facilitates Service Delivery Failure actions with the appropriate Governance Committee and holds regular Commonwealth Customer reviews.
11. IT Service Continuity Management (ITSCM)	The process responsible for managing risks that could seriously impact IT Services. ITSCM ensures that the IT Offeror can Always provide minimum agreed Service Levels, by reducing the risk to an acceptable level and Planning for the recovery of IT Services. ITSCM should be designed to support Business Continuity Management.
12. IT Financial Management	The process responsible for managing the Budgeting, Accounting, Invoicing and Chargeback requirements).
13. Information Security Management	The process that ensures the confidentiality, integrity and Availability of an organization's Assets, information, data and IT Services. Information Security Management usually has a wider scope than the Offeror. It normally includes handling of paper, building access, phone calls etc., for the entire organization.

Content	Description
14. Project Management and Support	Project Management and Support will align projects to Commonwealth requirements and deliver projects from request through end-to-end solutioning including turnover to the Commonwealth Customers and validation that project requirements were met in terms of timing, quality, and cost.
15. Service Catalog	A database or structured Document with information about select Services, including those available for Deployment. The Service Catalog is the only part of the Service portfolio published to Commonwealth Customers, and is used to support the request and delivery of select Services. The Service Catalog may include information about Deliverables, prices, contact points, ordering and request processes.
1.4 Financial Management Procedures	
1. Invoicing	The Offeror should describe procedures for invoicing. The content should include procedures for calculating Resource Unit volumes for pricing (per Service Component, as applicable), invoicing of Projects, etc. The content should include procedures regarding disputed invoice amounts.

Content	Description
2. Chargeback	The Offeror should describe procedures for charge back of costs related to the Services and the overall Agreement to the Commonwealth Customers (to include responsibilities and support by both the Offeror and the Commonwealth).
3. Budgeting	The Offeror should describe how it would assist the Commonwealth with the annual budgeting cycle. Process should include estimation of Resource Unit volumes (by Service Component and Commonwealth Customer as appropriate), potential Projects, review cycle, etc. The content should include the responsibilities of Offeror, the Commonwealth, and Commonwealth Agencies.
4. Forecasting	The Offeror should describe procedures for forecasting cost versus budget.
5. Procurement	The Offeror should describe procedures for procurement Services (where Offeror performs procurement on behalf of the Commonwealth, as applicable). The content should include responsibilities and process for both the Commonwealth staff and Offeror.

Content	Description
6. Service Level Credits and Earnback	The Offeror should describe procedures for calculating Service Level Credits on invoices and Earnback calculations.
1.5 Contract Management Procedures	
1. Contract Change Control	The Offeror should describe procedures regarding changes to the Agreement, including changes to any Exhibit or Attachment. Content should include procedures to classify services as a New Service, and resulting process to change the Agreement (including pricing). Content should include notification period and process, authority levels, and escalation procedures for changes to the Agreement.
2. Reporting	The Offeror should describe procedures and activities regarding key standard Reports and requests for ad hoc reports from the Commonwealth and The Commonwealth Agencies.
3. New Service Levels	The Offeror should describe procedures for determining new Service Levels (based on continuous improvement and/or Commonwealth request).

Content	Description
4. Benchmarking	The Offeror should describe procedures for Benchmarking exercises, including determination and agreement of benchmark firm, sample peer group and process used for benchmark, payment for benchmark, review of results, and potential outcome. Content should include dispute resolution process.
5. Auditing	The Offeror should describe procedures for operational and/or financial audits (as required by the Commonwealth auditing and/or regulatory agencies). The Offeror should describe notification process and procedures to resolve audit findings.
6. Offeror Key Personnel and Subcontractors	The Offeror should describe procedures for Commonwealth approval regarding replacement or removal of Offeror Key Personnel and major Subcontractors to Offeror.
7. Dispute Resolution	The Offeror should describe procedures regarding formal dispute resolution process.

Content	Description
1.6 Relationship Management Procedures	
1. Customer Satisfaction Surveys	The Offeror should describe the process to be used for conducting customer satisfaction surveys. Content should include procedures regarding action items and attempts to resolve customer issues.
2. Commonwealth Agencies	The Offeror should describe procedures and responsibilities regarding the relationship between the Commonwealth, the Commonwealth Agencies and the Offeror. Content should include procedures regarding communication and coordination regarding work requests, Service delivery issues, budgeting and financial issues, etc.
3. Authorized Users	The Offeror should describe procedures and responsibilities regarding responding to Authorized Users (including listing of Authorized Users) problems, requests, and questions.

Content	Description
4. Third Party Vendors	Offeror to describe procedures for relationship regarding Third Party Vendors which may provide services, Equipment, and/or Software that are ancillary to (or support) the overall delivery of Services. Procedures and coordination with key Third Party Vendors should be documented.
5. Other Third Parties	The Offeror should describe procedures for any other contact or requests from other Third Parties in regard to the Agreement.

Content	Description
1.7 Offeror Operational Procedures	
1. Operating Level Agreements (OLA)	OLAs are internal "back-to-back" agreements that define how two different Service Component Providers will work together to support the delivery of defined IT Services to the Commonwealth and Commonwealth agencies. The OLAs will define how Service Component Providers will work together to meet the Service Requirements documented in SOWs and Service Level Requirements documented in formal SLAs for the DCS initiative. The OLAs are a set of operational processes that supplements the IT Service Management section of the Commonwealth Computing Procedures Manual providing the second level detail required for individual Service Components to interoperate. Simply stated, the OLA "bolts" multiple Service Components together operationally.
2. Operational Procedures (by Service Component, as applicable)	The Offeror should describe the activities that the Offeror proposes to undertake in order to provide the Services, including those directions, supervision, monitoring, staffing, reporting, Planning and oversight activities normally undertaken by the Offeror which shall be consistent with those Offeror activities used to provide services similar to the Services.

Content	Description
3. Service Responsibility Matrix (SRM)	A map of the Functional Service Areas which potentially overlap Offeror responsibility and Commonwealth responsibility required to deliver business solutions to the business units. A Service Responsibility Matrix will be developed for each such area to delineate which party is responsible for performing select service elements and/or providing assistance or input.

Content	Description
1.8 The Commonwealth Customer Operations Manuals	
1. Individual Commonwealth Customer Operations Manual	The Commonwealth Computing Procedures Manual will also contain specific sections dedicated to operational procedures for Services provided to individual The Commonwealth Customers (each a "**The Commonwealth Customer Operations Manual**"). Each The Commonwealth Customer Operations Manual will address unique operational requirements of the respective The Commonwealth Customer, including operational areas such as the following: • Runbooks • Data safeguarding, use and release restrictions • Data security policies • Disaster Recovery requirements • Notification levels and procedures (e.g. problems and initial Severity Level procedures)

SCHEDULE I

INTENTIONALLY OMITTED

Schedule J.1

Data Center Service Level Management

Table of Contents

1 GENERAL 3
2 SERVICE LEVEL MEASUREMENT DESCRIPTIONS 3
3 REPORTING 4
4 NOTICE REQUIREMENTS FOR ADDITIONS, DELETIONS & MODIFICATIONS 5
5 SERVICE LEVEL CREDITS 5
6 EARN-BACK 7
7 ADDITIONS, MODIFICATIONS, AND DELETIONS OF SERVICE LEVELS 7
8 SERVICE DELIVERY FAILURE 9
9 COMMENCEMENT OF OBLIGATIONS 10
10 IMPROVEMENT PLAN FOR KEY MEASUREMENTS 10
11 MEASURING TOOLS 10
12 TIMES 11
13 SINGLE INCIDENT/MULTIPLE DEFAULTS 11
14 EXCLUSIONS 12
15 PERCENTAGE OBJECTIVES 12

1 General

The Commonwealth has adopted the ITIL framework and has established Service Level Management to maintain and improve IT Service quality, through a constant cycle of agreeing, monitoring, measuring, and reporting upon IT Service achievements and the instigation of actions to eradicate poor service.

The Service Level Performance Measures and their targets that are described in this Schedule J.1 have been specifically designed to support the Service Level Agreements set forth in Schedule J.2.

The methodology set out in this Schedule J.1 supports the Service Level Management cycle of agreeing, monitoring, measuring, reporting and improving the delivery of the services to the Commonwealth.

Effective on the Service Commencement Date, the Contractor will perform the Service to which Service Levels apply, so that the Service Level Performance will, in each month of the Term, meet or exceed, the Service Levels.

New Service Levels (Critical Measurements, Key Measurements) may be added or substituted by the Commonwealth as specified in this Schedule J.1 during the Term. For example, such additions or substitutions may occur in conjunction with changes to the environment and the introduction of new Equipment or Software to support a new or additional catalog service. However, where such Equipment or Software or such means of Service delivery is a replacement or upgrade of existing technology to support an existing catalog service, there shall be a presumption of equivalent or improved performance.

The achievement of the Service Levels by the Contractor may require the coordinated, collaborative effort of the Contractor with other third party contractors. The Contractor shall provide a single point of contact for the prompt resolution of all Service Level Defaults and all failures to provide high quality Services to the Commonwealth, regardless of whether the reason for such Service Level Defaults, or failure to provide high quality Services to the Commonwealth, was caused by the Contractor.

2 Service Level Measurement Descriptions

2.1 Application Infrastructure Availability

The Service Level for "Application Infrastructure Availability" measures the percentage of time all or a portion the application infrastructure is Available and not in a Degraded Condition.

Application Infrastructure Availability will be determined based on whether a component of the infrastructure assigned to an application in the CMDB meets the Service Level Performance Measure set out in Schedule J.2. Each associated processing environment (e.g. production, test, development, etc.), is a separate application and has its own SLA.

If Contractor monitoring indicates that any component of the application infrastructure has an issue, i.e. is unavailable and/or has a performance issue, Contractor will notify Commonwealth of the issue. If any application associated with the component has been impacted by the issue, an incident will be reported in accordance with the incident

management procedure defined in the Commonwealth Compute Procedures Manual (CCPM), which may include whether the application is available or in a Degraded Condition. If the Commonwealth notifies the Contractor that the application has been impacted, then a Service Level Default will have occurred, if a Service Level Performance Measure as set out in Schedule J.2 has not been met and a Service Level Credit will be applied consistent with section 5.1 of this Schedule J.1, unless Unisys provides root cause analysis to indicate that the impact to the application was not caused by the component issue. If the Commonwealth cannot identify an application impact then the Service Level Credit will apply only to the component of the application infrastructure which was not available.

If the Commonwealth identifies an impact to an application, prior to Unisys notifying the Commonwealth of component unavailability, the Commonwealth will report an incident in accordance with the Incident Management procedure defined in the CCPM. Unisys will investigate and determine the status of associated infrastructure components as defined in the CMDB, and if any infrastructure components are unavailable or have a performance issue, then a Service Level Default will have occurred, if a Service Level Performance Measure as set out in Schedule J.2 has not been met and a Service Level Credit will be applied consistent with section 5.1 of this Schedule J.1, unless Unisys provides root cause analysis to indicate that the impact to the application was not caused by a component failure.

2.2 Measuring Incident and Problem Resolution

The Service Level for "Incident and Problem Resolution" measures the percentage of Incident events with resolution times (commonly known as "Mean-Time-To-Resolve" – MTTR) within the limits specified within the appropriate Commonwealth Compute Procedures Manual based on the Incident Priority/Severity. These incidents are either user reports or monitoring system generated events indicating a service issue.

2.3 Measuring Other Service Management and Service Delivery

The Service Level for "Other Service Management and Service Delivery" measure the percentage of projects or solution requests, Backups, recoveries, and proposals that are delivered within the limits specified within the appropriate Commonwealth Compute Procedures Manual based on the request.

3 Reporting

Unless otherwise specified in this Schedule J.1, each Service Level (Critical Measurement, Key Measurement), Deliverable, and Transition Milestone shall be measured and reported on a monthly basis. The format, layout and content of such monthly report shall be as directed by the Commonwealth. The Contractor's monthly performance reports are due by the 5th Business day of each month and shall include a set of soft-copy reports such that the Commonwealth is able to verify the Contractor's performance and compliance with the Service Level (Critical Measurement, Key Measurement), Deliverable (until all Deliverables are received and approved by the Commonwealth), and Transition Milestone.

The Contractor shall provide detailed supporting information for each report to the Commonwealth in a format suitable for use on a personal computer. The data and detailed supporting information

shall include the methodology used by Contractor to calculate the service level performance based on the data measured and reported by the measurement tool such that the Commonwealth is able to reproduce the calculations made by Contractor and validate the results reported in the monthly Service Level Performance reports. All detailed supporting information shall be the Commonwealth's Confidential Information, and the Commonwealth may access such information online and in real-time, where feasible, at any time during the Term. In addition, Contractor shall provide the Commonwealth with direct, unaltered access to review and audit all raw data collection related to Service Levels.

The Contractor will create, maintain, and provide to the Commonwealth detailed procedure documentation of its Service Level measurement process used to collect Service Level data and calculate Service Level attainment. The process documentation must include quality assurance reviews and verification procedures. The measurement process must be automated to the extent possible, and any manual data collection steps must be clearly documented, verified and auditable. All methods, codes and automated programs must be documented and provided to the Commonwealth for validation and approval. The Contractor must ensure it tests and validates the accuracy and currency of the documentation and measurement process on a quarterly basis.

4 Notice Requirements for Additions, Deletions & Modifications

Subject to *Section 27* (Change Control) of the Contract , the Commonwealth will send notice to the Contractor at least ninety (90) days prior to the date that additions or deletions to Performance Categories, or additions or deletions to Service Levels (which include the movement of Critical Measurements to Key Measurements and Key Measurements to Critical Measurements), or modifications to Service Level Pool Percentage Allocation for any Critical Measurements or additions or deletions to Deliverables are to be effective. The Commonwealth may send only one such notice (which notice may contain multiple changes) each calendar quarter. Movement of Critical Measurements to Key Measurements and Key Measurements to Critical Measurements does not constitute creation of new service levels.

5 Service Level Credits

In the event of a Service Level Default, the Contractor shall provide the Commonwealth credits as defined below:

5.1 Schedule J.2 and Schedule J.3 set forth the information required to calculate whether the Service Level has met a Service Level Default level and how the Service Level is calculated and reported. For each Service Level Default, the Contractor shall provide credits to the Commonwealth, subject to Section 6 below, a Service Level Credit that will be computed in accordance with the following formula:

Service Level Credit = 100% of the effected month's invoicing for the service(s) that experienced a Service Level Default, unless otherwise identified in Schedule J.2, to a maximum credit not to exceed the At-Risk Amount as defined in **Schedule A - Defined Terms**

For example, assume that the Contractor fails to meet a Critical Measurement Service Level. If an infrastructure component fails and has no impact to an application then the Service Level Credit for the month totals the amount of the infrastructure component that was invoiced for that particular month. If an infrastructure component fails which has an

impact to an application, then the Service Level Credit for the month totals the amount of the fee for all infrastructure components associated with an impacted application as invoiced in the month that the application was impacted. If the Contractor's Monthly Invoice Amount for the infrastructure components for the month in which the Service Level Default occurred was $100,000, the credit would be $100,000.

If the event occurs where the total monthly credit amount exceeds the At-Risk Amount, each Service Level Default will be calculated based on the percentage of the total credit Amount and applied to the At-Risk Amount. An Example is if the At-Risk Amount is $100,000 and there are three Service Level Defaults (#1 = $50,000, #2=30,000 and #3=$80,000 for a total of $160,000) then the credit for Defaults would be calculated as follows:

Default 1		Default 2		Default 3		Total Credits Due
$50,000	+	$30,000	+	$80,000	=	$160,000

Default 1		Total Credits Due		Default 1Proration
$50,000	/	$160,000	=	31.25%

At-Risk Amount		Default 1 Proration		Credit Due for Default 1
$100,000	X	31.25%	=	$31,250

If more than one Service Level Default has occurred in a single month, the sum of the corresponding Service Level Credits shall be credited to the Commonwealth.

5.2 In no event shall the amount of Service Level Credits credited to the Commonwealth with respect to all Service Level Defaults occurring in a single month exceed, in total, the At-Risk Amount.

5.3 The Contractor shall notify the Commonwealth in writing if the Commonwealth becomes entitled to a Service Level Credit, which notice shall be included in the standard monthly reporting for Critical Measurements and Key Measurements as described in Section 3 above. The monthly reports shall also describe any failure to meet Key Measurements for the month.

5.4 The total amount of Service Level Credits that the Contractor will be obligated to pay to the Commonwealth, with respect to Service Level Defaults occurring each month, shall be credited on the invoice that contains charges for the month during which the Service Level Default(s) giving rise to such credit(s) occurred. For example, the amount of Service Level Credits payable with respect to Service Level Defaults occurring in August shall be set forth in the invoice for the August Monthly Invoice Amount issued in September.

5.5 Subject to , *Section 23* (Service Levels) of the Contract, the Contractor acknowledges and agrees that the Service Level Credits shall not be deemed or construed to be liquidated damages or a sole and exclusive remedy or in derogation of any other rights and remedies the Commonwealth has hereunder or under the Contract.

6 Earn-Back

The Contractor shall have Earn-Back opportunities with respect to Service Level Credits as follows:

6.1 The Service Level must be identified as Earn-Back Eligible per Schedule J.2 with a "Y" in the column titled "Earn-Back Eligible"

6.2 Within fifteen (15) days after the Earn-Back period as shown in Schedule J.2, the Contractor shall provide a report to the Commonwealth that will include, with respect to each Critical Measurement for which there was a Service Level Default, the following:

6.2.1 Statistics on the Contractor's average monthly performance during the Earn-Back period

6.2.2 The amount of Service Level Credit imposed for Service Level Default

6.2.3 The total amount of Service Level Credits imposed for Service Level Defaults

6.3 If the Contractor fails to meet the "Earn-Back Minimum" objective, Service Level Credits will be calculated and applied on the next billing cycle.

6.3.1 Earn-Back WILL NOT be available to the Contractor if it fails to meet the "Earn-Back Minimum" objective (Credit applied on the next billing cycle).

6.4 If the Contractor fails to meet the "Required" objective, Service Level Credits will be calculated and applied to the invoice following the Earn-Back period as shown in Schedule J.2 if an Earn-Back is not earned or immediately upon failure of a "Required" objective.

6.4.1 Earn-Back WILL be available to the Contractor if it fails to meet the "Required" objective and Earn-Back is available. If the Contractor meets the "Required" objective for the following Earn-Back period as shown in Schedule J.2, the Contractor will not be required to issue the credit.

6.4.2 If, during the Earn-Back period, the Commonwealth deletes the Critical Measurement (including demotion of a Critical Measurement to a Key Measurement) that corresponds to the Service Level Default giving rise to such Earn-Back review period, Contractor shall continue to track its performance for such former Critical Measurement and shall be entitled to an Earn-Back if and to the extent, and at the time, it would have otherwise been entitled to such Earn-Back in accordance with the procedures described in Section 6.4.1 above had the Critical Measurement not been so deleted or demoted to a Key Measurement during such Earn-Back review period.

6.5 If the Contract is terminated for default all service credits are due upon notice of termination.

7 Additions, Modifications, and Deletions of Service Levels

The Commonwealth may add, modify or delete Critical Measurements or Key Measurements as described below by sending written notice in accordance with Section 4 above.

7.1 Additions

The Commonwealth may add Service Levels in accordance with this Section 7.1 and by providing written notice in accordance with Section 4. Service Level commitments associated with added Service Levels will be computed as follows:

7.1.1 Where at least nine (9) consecutive months of verifiable service measurements exist for a particular Service that is being provided by the Contractor, the Parties agree that the Service Level shall be defined as the average for the Nine-Month Measurement Window however the target will not equal 100%, or

7.1.2 Where no measurements exist for a particular Service that is being provided by the Contractor, the Parties shall attempt in good faith to agree on a Service Level commitment using industry standard measures or third party advisory services (for example, Gartner Group, Yankee Group, etc.), or

7.1.3 Where less than nine (9) months or no measurements exist for a particular Service that is being provided by the Contractor, and the Parties fail to agree on a Required Service Level and an Earn-Back Minimum Service Level commitment using industry-standard measures as described in Item 2 of Section 7.1 of this Schedule, the Parties shall do the following:

7.1.3.1 The Contractor shall begin providing monthly measurements within ninety (90) days after the Contractor's receipt of the Commonwealth's written request and subject to agreement on such measurements in accordance with the *Section 27* (Change Control Procedures).

7.1.3.2 After nine (9) or more actual Service Level attainments have been measured (or should have been measured per Section 7.1.3.1 of this Schedule J.1 and if not so measured; constructed as described in Section 7.1.3.2.1 of this Schedule J.1), the Commonwealth may at any time in writing request that Section 7.1.1 above be used to establish the Service Level commitments:

7.1.3.2.1 If the Contractor is responsible for measuring actual service level attainments for nine (9) consecutive months and fails to provide one (1) or more measurements during the Six-Month Measurement Window such that nine (9) consecutive measurements are not available, the missing measurement(s) shall be constructed according to the following:

(i) if one measurement is missing, the missing measurement shall be constructed by using the highest of the eight (8) actual measurements, or

(ii) if two (2) or more measurements are missing, the first missing measurement shall be constructed by using the highest of the actual measurements and adding to that measurement twenty percent (20%) of the difference between that measurement and one hundred percent (100%) and each of the remaining missing measurements shall be constructed by using the highest of the actual measurements and

adding to that measurement thirty-five percent (35%) of the difference between that measurement and one hundred percent (100%).

For example, if there were four measurements for a particular Service, and the highest of the four measurements were 95%, then the measurements for the missing two months would be deemed to be 96.00% (representing 95.00% plus (20% of 5%)) and 96.75% (representing 95.00% plus 35% of 5%)), respectively.

7.1.3.2.2 If the Contractor has provided twenty-four (24) actual Service Level attainment measurements for any particular Service provided by the Contractor, and the Commonwealth has not used Item 1 of Section 7.1 of this Schedule to establish Service Level commitments, then continued provision of actual Service Level attainment measurements shall be subject to the Parties' mutual agreement in accordance with the *Section 27* (Change Control Procedures).

7.2 Deletions

The Commonwealth may delete Critical Measurements or Key Measurements by sending written notice in accordance with Section 4 herein.

8 Service Delivery Failure

If either (i) three (3) Service Level Defaults occur in any six (6) month period, or (ii) the Problem Management Process, as defined in the Commonwealth Computing Procedures Manual (CCPM), has identified a major recurring Problem not directly reflected in SLA performance and there is no formal Chronic Problem issue project underway to address such Problem (each a "Service Delivery Failure" or “SDF”) , then within thirty (30) days of the occurrence of such Service Delivery Failure, Contractor will provide the Commonwealth with a written plan (the "SD (Service Delivery) Service Improvement Plan") for improving the Contractor's performance to address the Service Delivery Failure, which plan will include a specific implementation timetable. The SD Service Improvement Plan will be subject to the Commonwealth's approval. Within 30 days of the Commonwealth's approval, or such other timeframe agreed to by the Commonwealth, Contractor will implement the SD Service Improvement Plan, which will include making timely and appropriate investments in people, processes and technology. In addition, the Contractor will demonstrate to the Commonwealth's reasonable satisfaction, that the changes implemented by Contractor have been made in normal operational processes to sustain compliant performance results in the future.

If Contractor fails to implement the SD Service Improvement Plan in the specified timetable, or if after the implementation of the SD Service Improvement Plan performance has not consistently improved, Contractor will be liable for a Service Level Credit in an amount equal to 10 percent (10%) of the then-current monthly invoice (the "SDF Credit"). The SDF Credit will be applied to the monthly invoice until such time as Contractor has demonstrated, for three (3) consecutive months, effective Service delivery, as evidenced by satisfying the criteria specified in the Problem Management RCA process related to the Service and/or no reoccurrence of the Service Level Defaults which triggered the applicable Service Delivery Failure. The SDF Credit will not be subject to Earn-Back. Under no circumstances shall the imposition of the SDF Credit described

above or the Commonwealth's exercise of any other rights hereunder be construed as the Commonwealth's sole or exclusive remedy for any failures described hereunder. SDF Credits are not to be considered a part of the At-Risk Amount calculation in relation or Service Levels and are a separate commitment from the Contractor indicating the Contractor's commitment to delivering service.

Further, the Contractor will work with the Commonwealth to define and document a repeatable Chronic Service Issue Resolution process in the Problem Management section of the Service Management Manual to be effective on the Effective Date. At a minimum, the process should address:

8.1 Establishment of a project team to drive and manage the process improvement

8.2 Approach to development of an Improvement Plan which will include milestones, resources and dependencies

8.3 Approach to Program Management of Plan implementation including integration of improvements/changes into daily operational processes

8.4 Implementation of Progress Reporting within the Contractors management structure, the Commonwealth and the Commonwealth Customers

8.5 Closure process to transition solution into normal operations including alignment of processes defined in the Service Management Manual

9 Commencement of Obligations

The obligations set forth herein shall commence on the first full month of service delivery in accordance with provisions set forth in Section 7.1 above.

10 Improvement Plan for Key Measurements

If the Contractor fails to satisfy any Key Measurement for three (3) months in any rolling six (6) month period, the Contractor shall provide the Commonwealth with a written plan for improving the Contractor's performance to satisfy the Key Measurement within thirty (30) days of the third (3rd) failure to meet the Service Level for the Key Measurement. At Contractor's sole cost and expense, the Contractor shall promptly implement such plan. If Contractor fails to implement the plan in the specified timetable, or if after ninety (90) days after any such implementation of the plan, the Key Measurement has not consistently improved, then the Commonwealth may at its option declare that such failure will constitute a Service Delivery Failure and Contractor will comply with the requirements of Section 8 above.

11 Measuring Tools

As of the Effective Date, the measuring tools and methodologies set forth in Schedule J.3 represent acceptable measuring tools and methodologies for the Critical Measurements and Key Measurements designated.

If there are any Critical Measurement Service Levels for which the measuring tools and methodologies have not been agreed upon by the Commonwealth and the Contractor and for which measuring tools are not included in Schedule J.3, and the Contractor fails to propose a measuring

tool for such Critical Measurement that is acceptable to the Commonwealth prior to the date upon which the Contractor shall be responsible for Service Level performance and Service Level Credits due for Service Level Default, such failure shall be deemed a Service Level Default for the Critical Measurement until the Contractor proposes and implements such acceptable measuring tool. The Commonwealth will not unreasonably withhold approval for the Contractor's recommendation for an alternate tool.

Tools for new Critical Measurement Service Levels will be implemented according to the *Section 27* (Change Control Procedures). Upon the Commonwealth's written notice approving a proposed alternate or new measurement tool, such tool shall be deemed automatically incorporated into Schedule J.3 as of the date for completion of implementation set forth in the Commonwealth's notification without requirement for an additional written amendment of this Agreement.

If, after the Effective Date or the implementation of tools for new Critical Measurements, the Contractor desires to use a different measuring tool for a Critical Measurement, the Contractor shall provide written notice to the Commonwealth, in which event the Parties will reasonably adjust the measurements as necessary to account for any increased or decreased sensitivity in the new measuring tools; provided that, if the Parties cannot agree on the required adjustment, the Contractor will continue to use the measuring tool that had been initially agreed to by the Parties.

It is not anticipated that changes in the measuring tools will drive changes in Service Levels; rather, the need to collect and accurately reflect the performance data should drive the development or change in performance monitoring tools. Contractor will configure all measuring tools to create an auditable record of each user access to the tool and any actions taken with respect to the data measured by or residing within the tool. All proposed measuring tools must include functionality enabling such creation of an auditable record for all accesses to the tool.

12 Times

Unless otherwise set forth herein, all references in this Schedule to Times shall refer to definition as described in **Schedule A – Defined Terms**.

13 Single Incident/Multiple Defaults

If a single incident results in the failure of the Contractor to meet more than one Service Level and the Service Level Credits are calculated in the same way, the Contractor shall issue Service Level Credits for every failure not to exceed the invoice amount of the impacted services and not to exceed the At-Risk Amount.

An example would be if a network component experienced a failure that denies access to ten subscribed services ("Application Infrastructure Availability" in this example). The CMDB would identify the impacted services and Service Level Credits would be due on all ten services to a maximum credit of the invoice amount for the ten services not to exceed the At-Risk Amount.

If a single incident results in the failure of the Contractor to meet more than one Service Level, and the Service Level Credits are not calculated in the same way, the Contractor shall issue Service Level Credits for the highest Service Level Credit not to exceed the At-Risk Amount.

An example would be if a subscribed service invoice is $500 per month and one Service Level Credit is defined as the "Monthly Invoice Amount for Impacted Service" ($500 in this example)

and one Service Level Credit is defined as $5,000. The credit would be calculated at the higher amount ($5,000 in this example).

14 Exclusions

For purposes of calculating Available Time and Availability, the Scheduled Uptime and Downtime shall not include any period of Downtime that is the result of scheduled time required to perform system maintenance (for example, preventive maintenance, system upgrades, etc.), provided that such time has been mutually agreed between the Parties and is scheduled so as to minimize the impact to the Commonwealth's business. The Contractor shall maintain Availability during such periods to the extent reasonably practicable. In addition, Service Level failures shall be relieved to the extent caused by the Commonwealth.

15 Percentage Objectives

Both parties understand that certain Service Levels may not be measured against an objective of one hundred percent (100%), for example, Time (days, hours, etc.), defects, etc. where zero (0) hours/days and zero percent (0%), respectively, are the appropriate objectives. The calculations described in this Section will be modified when appropriate to reflect these objectives. For example, if the Service Level involved defects in lines of code where zero percent (0%) is the objective, lowest would be changed to highest in Item 1 of Section 7.1 herein, highest would be changed to lowest in Item 3.2.1 of Section 7.1 herein and one hundred percent (100%) would be changed to zero percent (0%) in Item 3 of Section 7.1.

Schedule J.2

Data Center Service Level Matrix

Description of Schedule

This Schedule J.2 sets forth the following:

1. For Critical Measurements (CMs)

- the numeric measurements for Minimum Service Levels and expected Service Levels;
- the timing regarding the commencement of obligations for each critical Service Level
- a cross-reference to Schedule J.3 where the qualitative description of the performance category and the associated critical Service Level can be found

2. For Key Measurements (KMs)

- the numeric measurements for minimum Service Levels and expected Service Levels;

Service Level Matrix

Ref [a]	Service Level Categories	Required	Earnback Minimum	Earnback Eligible	Earnback Period (Consecutive Months)	Measurement Window	SLA Class[b]	Default Remedy Type[c]
SL01	Application Infrastructure Availability Platinum	99.999%	99.999%	N	NA	Monthly	CM	As described in Schedule J.1 Section 2.1
SL02	Application Infrastructure Availability - Gold	99.990%	99.990%	N	NA	Monthly	CM	As described in Schedule J.1 Section 2.1
SL03	Application Infrastructure Availability - Silver	99.900%	99.400%	Y	12 mos	Monthly	CM	As described in Schedule J.1 Section 2.1
SL04	Application Infrastructure Availability -Bronze	99.400%	99.200%	Y	12 mos	Monthly	CM	As described in Schedule J.1 Section 2.1
SL05	Application Infrastructure Availability -Basic	98.500%	98.500%	N	NA	Monthly	CM	As described in Schedule J.1 Section 2.1
SL06	Resolution Time - Severity Level 1 Incidents	97.500%	96.000%	Y	12 mos	Monthly	CM	Monthly invoice amount for impacted Service
SL07	Resolution Time - Severity Level 2	97.500%	96.000%	Y	12 mos	Monthly	CM	Monthly invoice amount for impacted Service
SL08	Resolution Time - Severity Level 3/4	97.500%	96.000%	Y	12 mos	Monthly	CM	Monthly invoice amount for impacted Service
SL09	Solution Request Fulfillment	95.000%	90.000%	Y	12 mos	Monthly	CM	Monthly invoice amount for impacted Service calculated quarterly
SL10	Standard Service Request Fulfillment	95.000%	90.000%	Y	6 mos	Monthly	CM	Total ordered amount for impacted Service
SL11	Completion of Project/Solution Phase	95.000%	90.000%	Y	6 mos	Monthly	CM	Monthly invoice amount for impacted Service
SL12	Solution and Procurement Proposals Delivered	95.000%	90.000%	Y	6 mos	Monthly	CM	Monthly invoice amount for impacted Service
SL13	CMDB Content Accuracy and Timeliness	98.000%	95.000%	Y	6 mos	Monthly	CM	$10,000.00 Credit on invoice
SL14	Software License Renewal Timeliness	99.900%	99.500%	Y	6 mos	Monthly	CM	$5,000.00 Credit on invoice
SL15	Successful Backups	97.000%	96.000%	Y	6 mos	Monthly	CM	Monthly invoice amount for impacted Service
SL16	Successful Recoveries	99.000%	98.000%	Y	12 mos	Monthly	CM	Monthly invoice amount for impacted Service calculated quarterly
SL17	Security Incident Notification Timeliness	99.900%	99.900%	N	NA	Monthly	CM	$5,000.00 Credit on invoice
SL18	Security Update Timeliness	97.500%	96.000%	N	6 mos	Monthly	CM	$5,000.00 Credit on invoice

Ref [a]	Service Level Categories	Required	Earnback Minimum	Earnback Eligible	Earnback Period (Consecutive Months)	Measurement Window	SLA Class[b]	Default Remedy Type[c]
SL19	Incident Management Communication – for Severity 1 Incidents	95.000%	90.000%	Y	6 mos	Monthly	KM	Monthly invoice amount for impacted Service
SL20	Root Cause Analysis Delivery	98.000%	96.000%	Y	6 mos	Monthly	KM	Monthly invoice amount for impacted Service
SL21	Chronic Problems	1.000%	2.000%	Y	6 mos	Monthly	KM	Monthly invoice amount for impacted Service
SL22	High Risk Security Patch Updates Timeliness	99.999%	99.900%	Y	12 mos	Monthly	KM	$50,000.00 Credit on invoice
SL23	Change Management Effectiveness	96.800%	93.750%	Y	6 mos	Monthly	KM	$5,000.00 Credit on invoice
SL24	Service Desk – Call Answer Time	< 27 Sec	< 30 Sec	Y	12 mos	Monthly	KM	$5,000.00 Credit on invoice
SL25	Service Desk – Abandon Rate	3.000%	4.000%	Y	12 mos	Monthly	KM	$5,000.00 Credit on invoice
SL26	Incident Ticket Quality	97.000%	95.000%	Y	6 mos	Monthly	KM	$5,000.00 Credit on invoice
SL27	Service Desk – Customer Satisfaction	4.2	3.9	Y	6 mos	Monthly	KM	$5,000.00 Credit on invoice
SL28	Batch Scheduling Launched on Time	99.500%	99.000%	Y	6 mos	Monthly	KM	Monthly invoice amount for impacted Service
SL29	Batch Processing Completed Successfully	99.900%	99.500%	Y	6 mos	Monthly	KM	Monthly invoice amount for impacted Service
SL30	Reports Delivered On Time	98%	95.00%	Y	6 mos	Monthly	KM	$10,000.00 Credit on invoice
SL31	Off-Site Media Management	95.000%	90.000%	Y	6 mos	Monthly	KM	Monthly invoice amount for impacted Service

Notes:

(a) Ref- See Schedule J.3 for detailed description of the Service Level metrics.

(b) SLA Class as defined in Schedule J.1.

(c) Amount listed for Key Measurements to be used in the event the Key Measurement becomes a Critical Measurement through Change Management. While the Service Level remains a Key Measurement no Default Remedies are due.

Schedule J.3

Data Center SLA Definitions

CONTENTS

1. CONTRACTOR GUIDELINES....4

1.1. Service Level Class Definitions....4

2. SERVICE LEVEL DETAILS....4

SL01 Application Infrastructure Availability – Platinum....5

SL02 Application Infrastructure Availability – Gold....6

SL03 Application Infrastructure Availability – Silver....7

SL04 Application Infrastructure Availability – Bronze....8

SL05 Application Infrastructure Availability – Basic....9

SL06 Resolution Time - Severity Level 1 Incidents....10

SL07 Resolution Time - Severity Level 2....11

SL08 Resolution Time - Severity Level 3/4....12

SL09 Solution Request Fulfillment....13

SL10 Standard Service Request Fulfillment....14

SL11 Completion of Project/Solution Phase....15

SL12 Solution and Procurement Proposals Delivered....16

SL13 CMDB Content Accuracy and Timeliness....17

SL14 Software License Renewal Timeliness....19

SL15 Successful Backups....20

SL16 Successful Recoveries....21

SL17 Security Incident Notification Timeliness....22

SL18 Security Update Timeliness....23

SL19 Incident Management Communication – for Severity Level 1 Incidents....24

SL20 Root Cause Analysis Delivery....26

SL21 Chronic Problems....27

Service Category....27

Incident & Problem Resolution....27

SL22 High Risk Security Patch Updates....28

SL23 Change Management Effectiveness....29

SL24 Service Desk – Call Answer Time....30

SL25 Service Desk – Abandon Rate....31
SL26 Incident Ticket Quality....32
SL27 Service Desk – Customer Satisfaction....33
SL28 Batch Scheduling Launched on Time....34
SL29 Batch Processing Completed Successfully....35
SL30 Reports Delivered On Time....36
SL31 Off-Site Media Management....37
SLXX Name (Template)....38
3. NOTES....39

1. Contractor Guidelines

This Schedule contains specific service level requirements that the Contractor must meet in order to perform the requested Services.

1.1. Service Level Class Definitions

There are two classes of Service Level performance metrics used, Critical Measurements (CMs) and Key Measurements (KMs).

- **Critical Measurements (CMs)** are performance measurements defined for the most important service areas. CMs will have associated fees, e.g. Service Level Credits, payable by the Contractor to Commonwealth for missed CMs according to the terms of the negotiated contract.

- **Key Measurements (KMs)** are performance target measurements for non-critical service areas. KMs are not eligible for Service Level Credits. Key Measures cover less critical service deliverables, sub processes or interim activities that are related to CM performance, and are reflective of overall effective and efficient service performance management. Based on periodic contractual SLA reviews, adjustments may be negotiable and KMs may be promoted to CMs.

Service Level measurement and reporting normally begins immediately following the Service Commencement Date. However, to allow for stabilization where appropriate, application of Service Level Credits may be reduced or waived for some period of time (to be negotiated) after the Service Commencement Date.

2. Service Level Details

The following pages describe each Service Level, its calculation, and other details relevant to the Service Level.

SL01 Application Infrastructure Availability – Platinum

Service Level Reference	Description
Application Infrastructure Availability – Platinum	
Service Category	Availability
Metric Description	This Service Level measures the percentage of time all or a portion of the application infrastructure is Available and not in a Degraded Condition during the applicable Measurement Window.
Metric Inclusions	Server instances and related CIs supporting targeted applications are identified in the CMDB. Scheduled hours of operations and maintenance windows for each infrastructure element related to the targeted applications will be maintained in the Commonwealth Computing Procedures Manual.
Metric Exclusions	• All items defined in Hold Time and Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** The Service Level calculation for targeted Applications Infrastructure Availability is the sum of actual Available Time for the individual applications divided by the sum of expected, scheduled Available Time for the applications, with the result expressed as a percentage. • = 1 – ((Sum of minutes the application infrastructure component is not Available or in a Degraded Condition) / ((1440 minutes per day) X (calendar days in month))) expressed as a percentage
Service Level Reporting Window	Monthly

SL02 Application Infrastructure Availability – Gold

Service Level Reference	Description
Application Infrastructure Availability – Gold	
Service Category	Availability
Metric Description	This Service Level measures the percentage of time all or a portion of the application infrastructure is Available and not in a Degraded Condition during the applicable Measurement Window.
Metric Inclusions	Server instances and related CIs supporting targeted applications are identified in the CMDB. Scheduled hours of operations and maintenance windows for each infrastructure element related to the targeted applications will be maintained in the Commonwealth Computing Procedures Manual.
Metric Exclusions	• All items defined in Hold Time and Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** The Service Level calculation for targeted Applications Infrastructure Availability is the sum of actual Available Time for the individual applications divided by the sum of expected, scheduled Available Time for the applications, with the result expressed as a percentage. • = 1 – ((Sum of minutes the application infrastructure component is not Available or in a Degraded Condition) / ((1440 minutes per day) X (calendar days in month))) expressed as a percentage
Service Level Reporting Window	Monthly

SL03 Application Infrastructure Availability – Silver

Service Level Reference	Description
Application Infrastructure Availability – Silver	
Service Category	Availability
Metric Description	This Service Level measures the percentage of time all or a portion of the application infrastructure is Available and not in a Degraded Condition during the applicable Measurement Window.
Metric Inclusions	Server instances and related CIs supporting targeted applications are identified in the CMDB. Scheduled hours of operations and maintenance windows for each infrastructure element related to the targeted applications will be maintained in the Commonwealth Computing Procedures Manual.
Metric Exclusions	• All items defined in Hold Time and Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** The Service Level calculation for Targeted Applications Infrastructure Availability is the sum of actual Available Time for the individual applications divided by the sum of expected, scheduled Available Time for the applications, with the result expressed as a percentage. • = 1 – ((Sum of minutes the application infrastructure component is not Available or in a Degraded Condition) / ((1440 minutes per day) X (calendar days in month))) expressed as a percentage
Service Level Reporting Window	Monthly

SL04 Application Infrastructure Availability – Bronze

Service Level Reference	Description
Application Infrastructure Availability – Bronze	
Service Category	Availability
Metric Description	This Service Level measures the percentage of time all or a portion of the application infrastructure is Available and not in a Degraded Condition during the applicable Measurement Window.
Metric Inclusions	Server instances and related CIs supporting targeted applications are identified in the CMDB. Scheduled hours of operations and maintenance windows for each infrastructure element related to the targeted applications will be maintained in the Commonwealth Computing Procedures Manual.
Metric Exclusions	• All items defined in Hold Time and Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** The Service Level calculation for targeted Applications Infrastructure Availability is the sum of actual Available Time for the individual applications divided by the sum of expected, scheduled Available Time for the applications, with the result expressed as a percentage. • = 1 – ((Sum of minutes the application infrastructure component is not Available or in a Degraded Condition) / ((1440 minutes per day) X (calendar days in month))) expressed as a percentage
Service Level Reporting Window	Monthly

SL05 Application Infrastructure Availability – Basic

Service Level Reference	Description
Application Infrastructure Availability – Basic	
Service Category	Availability
Metric Description	This Service Level measures the percentage of time all or a portion of the application infrastructure is Available and not in a Degraded Condition during the applicable Measurement Window.
Metric Inclusions	Server instances and related CIs supporting targeted applications are identified in the CMDB. Scheduled hours of operations and maintenance windows for each infrastructure element related to the targeted applications will be maintained in the Commonwealth Computing Procedures Manual.
Metric Exclusions	• All items defined in Hold Time and Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** The Service Level calculation for targeted Applications Infrastructure Availability is the sum of actual Available Time for the individual applications divided by the sum of expected, scheduled Available Time for the applications, with the result expressed as a percentage. • = 1 – ((Sum of minutes the application infrastructure component is not Available or in a Degraded Condition) / ((1440 minutes per day) X (calendar days in month))) expressed as a percentage
Service Level Reporting Window	Monthly

SL06 Resolution Time - Severity Level 1 Incidents

Service Level Reference	Description
Resolution Time - Severity Level 1 Incidents	
Service Category	Incident and Problem Resolution
Metric Description	This Service Level measures the percentage of time Contractor resolves Severity Level 1 events within the applicable time period. Also known as Mean Time To Resolve (MTTR) for Severity Level 1 Incidents.
Metric Inclusions	Includes all Applications Infrastructure components as defined by the CMDB and Severity Level 1 events that are assigned to the appropriate Service Level. The time limits for the resolution of each are as listed below. Time frame for resolution shall be based on the tier designation for the highest mainframe, server or instance associated with the respective incident. For incidents not associated with a specific mainframe, server, or instance, the resolution timeframe shall be measured as a Silver tier. Platinum < 90 minutes Gold < 120 minutes Silver < 180 minutes Bronze < 240 Minutes
Metric Exclusions	• All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** The Service Level calculation for Resolution Time – Severity Level 1 is the total number of Incidents that are or become Severity Level 1 that are Resolved within the relevant Resolution Time specified, divided by the total number of Incidents that are or become Severity Level 1 during the applicable Measurement Window, with the result expressed as a percentage. • = (Number of Severity Level 1 Incidents Resolved within Limit) / (Total Number of Severity Level 1 Incidents) expressed as a percentage
Service Level Reporting Window	Monthly

SL07 Resolution Time - Severity Level 2

Service Level Reference	Description
Resolution Time - Severity Level 2	
Service Category	Incident and Problem Resolution
Metric Description	This Service Level measures the percentage of time Contractor resolves Problems within the applicable time periods. Also known as Mean Time To Resolve (MTTR) for Severity Level 2 Incidents.
Metric Inclusions	Includes all mainframes, servers, and instances associated with targeted applications and other Severity Level 2 events not associated with servers or instances. The time limits for the resolution of each mainframe, server or instance are as listed below. Time frame for resolution shall be based on the tier designation for the highest mainframe, server or instance associated with the respective incident. For incidents not associated with a mainframe, server, or instance, resolution shall be measured as Silver tier (< 360 minutes). Platinum < 90 minutes Gold < 180 minutes Silver < 360 minutes Bronze < 960 Minutes
Metric Exclusions	• All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** The Service Level calculation for Resolution Time – Severity Level 2 is the total number of Incidents that are or become Severity Level 2 that are Resolved within the relevant Resolution Time specified, divided by the total number of Incidents that are or become Severity Level 2 during the applicable Measurement Window, with the result expressed as a percentage. • = (Number of Severity Level 2 Incidents Resolved within Limit) / (Total Number of Severity Level 2 Incidents) expressed as a percentage
Service Level Reporting Window	Monthly

SL08 Resolution Time - Severity Level 3/4

Service Level Reference	Description
Resolution Time - Severity Level 3/4	
Service Category	Incident and Problem Resolution
Metric Description	This Service Level measures the percentage of time Contractor resolves Incidents within the applicable time periods. Also known as Mean Time To Resolve (MTTR) for Severity Level 3 and Severity Level 4 Incidents.
Metric Inclusions	Severity Level 3 - For all Severity Level 3 Incidents , the incident shall be resolved within 3,780 business minutes (i.e. 63 hours) Severity Level 4 - For all Severity Level 4 Incidents, the incident shall be resolved within 4,860 business minutes (i.e. 81 hours or 9 business days) Total business minutes shall be measured during only those minutes between 8:00 AM and 5:00 PM inclusive, Monday through Friday inclusive (1 Business day = 9 Business hours = 540 Business minutes); (1 business minutes = 2,700 minutes)
Metric Exclusions	• All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	8:00AM – 5:00 PM
Days of Measurement	Monday through Friday
Calculation	• **Summary:** The Service Level calculation for Resolution Time – Severity Level 3/4 is the total number of Incidents that are or become Severity Level 3 or 4 that are Resolved within the relevant Resolution Time specified, divided by the total number of Incidents that are or become Severity Level 3 or 4 during the applicable Measurement Window, with the result expressed as a percentage. • = ((Number of Severity Level 3 Incidents Resolved within Limit) +(Number of Severity Level 4 Incidents Resolved within Limit)) / ((Total Number of Severity Level 3 Incidents) + (Total Number of Severity Level 4 Incidents)) expressed as a percentage
Service Level Reporting Window	Monthly

SL09 Solution Request Fulfillment

Service Level Reference	Description
Solution Request Fulfillment	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the percentage of time Contractor successfully implements a solution request within the timeframe committed to the requester as measured in the applicable Measurement Window. All phases of the solution implementation process from the Commonwealth Customer approval of the solution proposal through implementation and the Commonwealth Customer acceptance into production are included in this measure.
Metric Inclusions	For purposes of calculating this Service Level, only those requests which require a solution proposal that has been accepted by the Commonwealth will be included in the calculation. Solution requests without a production date established by the time the order is received will be counted as a missed expectation.
Metric Exclusions	None
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is the total number of projects that are successfully completed during the applicable Measurement Window on or before the due date specified in the applicable solution proposal and/or a subsequent project plan, divided by the total number of projects that should have been completed during the applicable Measurement Window, with the result expressed as a percentage. • = (Number of solution requests completed within limit during the measurement window) / (Total number of solution requests due within the measurement window) expressed as a percentage
Service Level Reporting Window	Monthly

SL10 Standard Service Request Fulfillment

Service Level Reference	Description
Standard Service Request Fulfillment	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the percentage of time Contractor successfully completes Standard Service Requests that do not require a solution proposal to be approved by the Commonwealth. Specific target timeframes are either established in the CCPM or a specific commitment date outside of the standard timeframe may be established at the Commonwealth's discretion.
Metric Inclusions	Included as Standard Service Requests shall be an agreed upon set of service requests as specified in the Commonwealth Computing Procedures Manual.
Metric Exclusions	• Elapsed time waiting for the Commonwealth or a Commonwealth Customer's required approval or hold shall be excluded. • All items defined in Note 2 at the bottom of this Schedule J.3 • Exception: An Agency unplanned Standard Services Request for more than 10% above the Agency's most recent approved demand forecast. The Contractor must notify the Commonwealth of the need to order Equipment within two business days of receipt of the order, the Contractor provides the Commonwealth with an acceptable estimated time to deliver the Equipment, and the Equipment is delivered within the time specified. •
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is the total number of Standard Service Requests successfully completed by Contractor during the applicable Measurement Window and within the required timeframes specified in Commonwealth Compute Procedure Manual (CCPM) or other agreed to date, divided by the number of Standard Service Requests that should have been completed by Contractor during the applicable Measurement Window, with the result expressed as a percentage. • = (Number of Standard Requests completed within limit) / (Total Number of Standard Requests due within the measurement window) expressed as a percentage •
Service Level Reporting Window	Monthly

SL11 Completion of Project/Solution Phase

Service Level Reference	Description
Completion of Project/Solution Phase	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the percentage of time Contractor successfully completes a phase (e.g. procurement, floor prep, network prep, physical install, turn-up and test, production) milestone no later than the committed timeframe. All phases of the solution implementation process following the Commonwealth Customer approval of the solution proposal through implementation and the Commonwealth Customer acceptance into production are included in this measure.
Metric Inclusions	For purposes of calculating this Service Level, only those requests which require a solution proposal or project plan that has been accepted by the Commonwealth and a production date established will be included in the calculation. If a milestone is missed, the rescheduled milestone will also be included in the measurement
Metric Exclusions	All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is the total number of project or solution requests successfully completed by Contractor during the applicable Measurement Window and within the required timeframes specified in Commonwealth Compute Procedure Manual (CCPM) or other agreed to date, divided by the number of Project and solution requests that should have been completed by Contractor during the applicable Measurement Window, with the result expressed as a percentage • = (Number of project/solution requests completed within Limit) / (Total Number of project/solution requests due within the measurement window) expressed as a percentage
Service Level Reporting Window	Monthly

SL12 Solution and Procurement Proposals Delivered

Service Level Reference	Description
Solution and Procurement Proposals Delivered	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the percentage of time Contractor provides a viable proposal to the Commonwealth, in response to a solution or procurement request, within the timeframe established in the Commonwealth Computing Procedures Manual for commodity and standard requests or a jointly agreed to commitment date for custom requests.
Metric Inclusions	Each proposal submitted to the Commonwealth will be considered a measurable event. If there are multiple proposals for one request due to requirements changes then subsequent iterations will be counted as another event. Each will count as an event and an opportunity to succeed or fail.
Metric Exclusions	• All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is the total number of viable proposals submitted to the Commonwealth during the applicable Measurement Window on or before the due date determined from the Commonwealth Computing Procedures Manual for Standard and Commodity Requests or jointly agreed for custom requests, divided by the total number of proposals that should have been submitted during the applicable Measurement Window, with the result expressed as a percentage. • = (Number of solution and procurement proposal requests completed within interval during the measurement window) / (Total number of solution and procurement proposal requests due with the measurement window) expressed as a percentage
Service Level Reporting Window	Monthly

SL13 CMDB Content Accuracy and Timeliness

Service Level Reference	Description
CMDB Content Accuracy and Timeliness	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the percentage of an audited statistically valid sample of Inventory Records (as defined below) during the Measurement Window that is determined to be Accurate (as defined below) by such audits.
Metric Inclusions	The audited sample for this Service Level must contain a number of randomly selected CMDB Inventory Records that is reasonably acceptable to the Commonwealth. The random selection shall be a statistically significant stratified random sampling representing all Commonwealth Customers each month. **Definitions for purposes of this Service Level:** Accurate means all Critical Inventory Attributes are correctly and completely populated in the CMDB Inventory of Record. Critical Inventory Attributes means those database fields in an Inventory Record that are essential for Contractor's successful delivery of Service and necessary for Commonwealth's successful performance of retained responsibilities, including architecture, IT planning, and reconciliation of invoices. Critical Inventory Attributes that must be audited are set out in CCPM and may be modified over time in accordance with the CCPM. CMDB Inventory of Record means the inventory of CIs, including all Equipment and Software, to be created and maintained by Contractor in accordance with the CCPM. Inventory Record means the record for a single item of Equipment or Software in the Inventory of Record, including all of the Critical Inventory Attributes for that item.
Metric Exclusions	• All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is the total number of CMDB Inventory Records that are audited during the applicable Measurement Window and that are Accurate, divided by the total number of Inventory Records that are audited during the applicable Measurement Window, with the result expressed as a percentage. • = ((Number of valid records found) / (Total Number of Records Audited)) expressed as a percentage

Service Level Reporting Window	Monthly

SL14 Software License Renewal Timeliness

Service Level Reference	Description
Software License Renewal Timeliness	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the timeliness of all license and maintenance renewals for software managed by Contractor.
Metric Inclusions	This SLA includes the renewal of software licenses included in the Agreement and hardware maintenance agreements included in hardware service charges (HSC) to a the Commonwealth Customer (e.g. renewal of SSL certificates, application utility software, custom solution hardware (covered by a maintenance agreement) charged to the Commonwealth Customer through the HSC).
Metric Exclusions	• Renewals for software or maintenance purchased outside of this contract by the Commonwealth or the Commonwealth Customers and not included in Contractor's charges to the Commonwealth are excluded. • All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	This Service Level measures the timeliness of all license and maintenance renewals for software managed by Contractor.
Days of Measurement	N/A
Calculation	• **Summary:** Renewals are routinely expected to be installed ten (10) or more business days prior to the renewal due date for the item or service. (Renewal due date is the date when the current license or maintenance contract expires.) The Service Level calculation for Software License Renewal Timeliness is a percentage derived from the total number of all renewals processed divided by the total number due for the month that were renewed before the renewal expiration date without disruption in service. • = ((Successful Software Renewals implemented within Time Frame) / (Total Software License Renewals Completed)) expressed as a percentage
Service Level Reporting Window	Monthly

SL15 Successful Backups

Service Level Reference	Description
Successful Backups	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the percentage of time Contractor completes backup jobs successfully during the applicable Measurement Window in accordance with the relevant criteria specified in the Commonwealth Computing Procedures Manual.
Metric Inclusions	Backup jobs include all registered backup clients (including but not limited to all file systems, databases, application files, operating systems, applications and respective Data).
Metric Exclusions	• If there is an appropriate tool available and in use that captures open files, then the backup of open files are included as part of the backup. If there is not an appropriate tool available and in use for the capture of open files, then open files are skipped and not counted against this Service Level. Any batch jobs related to infrastructure backups, or other functionality exclusively for Contractor would be excluded. • All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level is the sum of the number of times Contractor completes backup jobs successfully and complete on time during the applicable Measurement Window divided by the of the sum of the number of times Contractor began or should have begun backup jobs within the applicable measurement window, with the result expressed as a percentage. • = ((Number of Successful Backups) / (Total Number of Backups Attempted)) expressed as a percentage
Service Level Reporting Window	Monthly

SL16 Successful Recoveries

Service Level Reference	Description
Successful Recoveries	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the percentage of time Contractor completes data recoveries successfully and on time during the applicable Measurement Window in accordance with the relevant criteria specified in the Commonwealth Computing Procedures Manual.
Metric Inclusions	Recoveries include all registered recovery clients (including but not limited to all file systems, databases, application files, operating systems, applications and respective Data).
Metric Exclusions	• Any batch jobs related to infrastructure recoveries, or other functionality exclusive for the Contractor would be excluded. • All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is the total number of data recovery jobs that are completed successfully and on time in accordance with the relevant criteria set forth in the Commonwealth Computing Procedures Manual during the applicable Measurement Window, divided by the total number of data recovery jobs that were attempted or scheduled to be completed during the applicable Measurement Window, with the result expressed as a percentage. • = ((Number of Successful Recoveries) / (Total Number of recoveries attempted)) expressed as a percentage
Service Level Reporting Window	Monthly

SL17 Security Incident Notification Timeliness

Service Level Reference	Description
Security Incident Notification Timeliness	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the percentage of time Contractor completes identifying and notifying CoPA of detected security incidents in accordance with ITB-SEC024.
Metric Inclusions	Time required receiving and analyzing reactive and/or proactive incidents from any and all managed sources including, but not limited to, firewalls, intrusion detection/prevention devices, VPN appliances, switches, routers, and all other equipment over which Commonwealth traffic traverses. Time required contacting CoPA and reporting the incident in accordance with ITB-SEC024.
Metric Exclusions	• All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is the total number of Security Incidents reported in accordance with ITB SEC-024 using the procedure set forth in the Commonwealth Computing Procedures Manual, divided by the total number of detected security incidents, with the result expressed as a percentage. • = [(number of incidents reported in accordance with ITB SEC-024) / number of detected incidents)] expressed as a percentage
Service Level Reporting Window	Monthly

SL18 Security Update Timeliness

Service Level Reference	Description
Security Update Timeliness	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the percentage of time Contractor completes Security Updates successfully and on time during the applicable Measurement Window in accordance with the relevant criteria specified in the Commonwealth Computing Procedures Manual.
Metric Inclusions	Security Updates include all updates and changes designated as a Security Update at the time or request/order. These updates includes, but are not limited to, Security Patches, Firewall configuration changes, proxy updates and changes, and Identity Management changes.
Metric Exclusions	• Any batch jobs related to infrastructure recoveries, or other functionality exclusive for the Contractor would be excluded. • All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is the total number of Security update requests that are completed successfully and on time in accordance with the relevant criteria set forth in the Commonwealth Computing Procedures Manual during the applicable Measurement Window, divided by the total number of Security update requests that were requested to be completed during the applicable Measurement Window, with the result expressed as a percentage. • = ((Number of Security Updates) / (Total Number of Requested Security Updates)) expressed as a percentage
Service Level Reporting Window	Monthly

SL19 Incident Management Communication – for Severity Level 1 Incidents

Service Level Reference	Description
Incident Management Communication – for Severity Level 1 Incidents	
Service Category	Incident & Problem Resolution
Metric Description	This Service Level measures the percentage of time the Contractor provides the notices to the applicable users within the following timeframes with respect to Incidents that are or become Severity Level 1 Incidents and that are not Resolved in less than one (1) hour from the Start Time for such Incident. • First notice: Within one hour of incident ticket creation • Subsequent notices: every 30 minutes A notice is defined as : • Verbal communication to user, as documented in the ticket • Bridge call including user, as documented in the ticket • Email to user, as documented in the ticket Such notices shall not be deemed to have been provided unless (a) the user that reported the Incident has been contacted by the Contractor and such notice of status has been provided or (b) Contractor has left a voice mail (or if not possible because the user does not have a voice mail box, sent an email or attempted some other reasonable means of communication) for the user.
Metric Inclusions	Includes all Severity Level 1 Incidents
Metric Exclusions	• Severity Level 2, 3 and 4 Incidents • Duplicate Incident reports for the incident • All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is the total number of Incidents that are or become Severity Level 1 Incidents, that have Start Times during the applicable Measurement Window, that have actual Resolution Times of greater than one (1) hour and for which Contractor provided the applicable user the required notice(s) within the required timeframe(s) as set forth in this Section, divided by the total number of Incidents that are or become Severity Level 1 Incidents, that have Start Times during the applicable Measurement Window and that have actual Resolution Times of greater than one (1) hour, with the result expressed as a percentage. • = ((Number of Incidents with Communications within established intervals) / (Total Number of

	Severity Level 1 Incidents)) expressed as a percentage
Service Level Reporting Window	Monthly

SL20 Root Cause Analysis Delivery

Service Level Reference	Description
Root Cause Analysis Delivery	
Service Category	Incident & Problem Resolution
Metric Description	This Service Level measures the percentage of time Contractor reports the results of a Formal Root Cause Analyses for Service Restoral Incidents within the timeframes below during the Measurement Window: • RCA's due within ten (10) Business Days from the request of the RCA.
Metric Inclusions	An user may request a Formal RCA for incidents that require more in-depth analysis than required with the normal Root Cause Analysis process. The Formal RCA is documented and tracked within the Problem Management process, and upon completion, is presented by the Contractor Problem Management Team to the affected the Commonwealth Customer and the Commonwealth for review and approval. Contractor shall perform a Formal Root Cause Analysis with respect to any Service Restoral Incident, if requested by the Commonwealth, and that has a Start Time during the applicable Measurement Window.
Metric Exclusions	• Those Service Restoral Incidents for which the Commonwealth or the Commonwealth's Customer does not request a Formal Root Cause Analysis. • Duplicate Requests • All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is the total number of written Formal Root Cause Analyses that are delivered to the Commonwealth within the timeframes specified in this Section during the applicable Measurement Window, divided by the total number of written Formal Root Cause Analyses that should have been delivered to the Commonwealth during the applicable Measurement Window, with the result expressed as a percentage. • = ((Number of Formal Root Cause Analyses Delivered within established interval) / (Total Number of Formal Root Cause Analyses Due)) expressed as a percentage
Service Level Reporting Window	Monthly

SL21 Chronic Problems

Service Level Reference	Description
Chronic Problems	
Service Category	Incident & Problem Resolution
Metric Description	A Chronic Problem means a problem which meets any of the following criteria: 1. The existence two or more incidents with the same root cause for the same software, service, process, or hardware for which Contractor, the Commonwealth, or the Commonwealth Customer, have designated as a problem requiring a Root Cause Analysis with a corrective action plan. 2. The existence of three or more service failures or outages for the same software, service, process, or hardware within the same month for any two (2) months within any rolling six (6) months. 3. The existence of three (3) or more service failures or outages for the same software, service, process, or hardware within any rolling six (6) month period for which no root cause has been determined. Multiple Incidents that are opened contemporaneously for the same software, service, process, or hardware due to the same root cause shall be deemed to be a single incident for purposes of this Service Level.
Metric Inclusions	All incidents and Problem Investigation reports for all services covered by any service level metric.
Metric Exclusions	• Problems which have a published Root Cause Analysis with an associated action plan approved by the Commonwealth Customers and which has all agreed corrective actions on schedule (not exceeding their completion dates) and have had no reoccurrences of the same failure may be excluded at the Contractor's request and the Commonwealth's approval. • All items defined in Note 2 at the bottom of this Schedule J.3 • Duplicate Incident reports for the same Incident
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** Contractor's performance shall be measured by determining the total number of Problems that are or become Chronic Problem(s) during the applicable Measurement Window. • ((the number of Chronic Problems) / (the total number of problems)) expressed as a percentage
Service Level Reporting Window	Monthly

SL22 High Risk Security Patch Updates

Service Level Reference	Description
High Risk Security Patch Updates	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the timeliness in which high-risk security patches are applied. All high risk security patches must be applied within five (5) business days from the date the software vendor or applicable industry guiding entity provides notice to the Contractor or other date as agreed to by the Commonwealth or the Commonwealth Customer.
Metric Inclusions	Includes those security patches for which the vendor or applicable industry guiding entity indicates is high risk.
Metric Exclusions	• Excludes low and medium risk patches • All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is the total number of high risk security patches released five (5) business days prior to the beginning and end of the measurement window that were installed within five (5) business days divided by the total number of high risk security patches released five (5) business days prior to the beginning and end of the measurement window, with the result expressed as a percentage. • = ((Number of high risk intrusion protection updates installed within established interval) / (Total Number of high risk intrusion protection updates installed)) expressed as a percentage
Service Level Reporting Window	Monthly

SL23 Change Management Effectiveness

Service Level Reference	Description
Change Management Effectiveness	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the percentage of time Contractor successfully implements Changes to the Services.
Metric Inclusions	Changes are not successfully implemented if they: (i) do not comply with the Change Management procedures (including the Change Control Process), (ii) do not comply with the Change Management procedures detailed within the Commonwealth Computing Procedures Manual, (iii) cause Severity Level 1 Incidents or Severity Level 2 Incidents, within 168 hours of implementing the change, (iv) exceeds the reserved implementation or maintenance window as approved within the ITSM Change Request, or (v) are backed out.
Metric Exclusions	• Severity Level 1 and Severity Level 2 incidents that occur during the implementation window for the change and are resolved before the Implementation or Maintenance window ends. • All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is the number of changes that are successfully implemented by Contractor during the applicable Measurement Window, divided by the number of changes that should have been implemented by Contractor during the applicable Measurement Window, with the result expressed as a percentage. • = ((Number of Successful Change Management Requests) / (Total Number of Change Management Requests Scheduled during the period)) expressed as a percentage
Service Level Reporting Window	Monthly

SL24 Service Desk – Call Answer Time

Service Level Reference	Description
Service Desk – Call Answer Time	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the elapsed time an user is placed on hold after leaving the interactive voice response or Automatic Call Distribution System to the time the phone call is answered by a live support technician.
Metric Inclusions	All phone calls to the Service Desk shall be included in the calculation of this Service Level with no exceptions for phone calls to the Service Desk during any period of Downtime.
Metric Exclusions	• All items defined in Note 2 at the bottom of this Schedule J.3 • Excludes the time a caller is listening to a Menu of choices before being routed to a helpdesk agent.
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is the total number of seconds, for all phone calls to the Service Desk during the applicable Measurement Window, between the time the phone caller first selects a menu option on the IVR or Automatic Call Distribution System for assistance by a live support technician to the time the phone call is verbally answered by a live support technician ready to start working on the phone call, divided by the total number of all phone calls to the Service Desk during the applicable Measurement Window. • = (Average Time a Call takes to be answered by Service Desk Agent) expressed in seconds
Service Level Reporting Window	Monthly

SL25 Service Desk – Abandon Rate

Service Level Reference	Description
Service Desk – Abandon Rate	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the percentage of phone calls to the Service Desk that are abandoned by the user after the user selected a service option and prior to a live support technician answering the phone call.
Metric Inclusions	All phone calls to the Service Desk shall be included in the calculation of this Service Level with no exceptions for phone calls to the Service Desk during any period of Downtime.
Metric Exclusions	• Calls disconnected prior to an automated voice response system completing the Menu of choices for callers are not counted as abandoned. • All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is the total number of phone calls to the Service Desk during the applicable Measurement Window that are abandoned by the user (prior to an automated voice response system answers), divided by the total number of phone calls to the Service Desk during the applicable Measurement Window, with the result expressed as a percentage. • = ((Number Of Abandoned Telephone Calls) / (Total Number Of Telephone Calls)) expressed as a percentage
Service Level Reporting Window	Monthly

SL26 Incident Ticket Quality

<table>
<tr><th>Service Level Reference</th><th>Description</th></tr>
<tr><td>Incident Ticket Quality</td><td></td></tr>
<tr><td>Service Category</td><td>Other Service Management and Delivery</td></tr>
<tr><td>Metric Description</td><td>This Service Level measures the quality and timeliness of the Contractor’s incident management and communication of incident management activities (as defined in the Commonwealth Computing Procedures Manual Commonwealth Computing Procedures Manual). Contractor must update the incident tickets at a minimum on the following frequencies:
<table>
<tr><th><u>Service Restorals</u></th><th><u>Service Requests</u></th></tr>
<tr><td>P1: every 15 minutes</td><td>P1: Daily</td></tr>
<tr><td>P2: 30 minutes</td><td>P2: Weekly</td></tr>
<tr><td>P3: daily</td><td>P3: every 2 weeks</td></tr>
<tr><td>P4: weekly</td><td>P4: Monthly</td></tr>
</table></td></tr>
<tr><td>Metric Inclusions</td><td>Includes a statistically valid random sample of Service Restorals and Service Requests closed during the Measurement Window, all priorities.</td></tr>
<tr><td>Metric Exclusions</td><td>• Excludes Change Requests (CRQ), solution requests (REQ), and Problem Management (PBI)
• All items defined in Note 2 at the bottom of this Schedule J.3</td></tr>
<tr><td>Hours of Measurement</td><td>24x7</td></tr>
<tr><td>Days of Measurement</td><td>365</td></tr>
<tr><td>Calculation</td><td>• Summary: This Service Level calculation is the number of sampled tickets in the Measurement Window which meet the defined quality and communication frequency criteria divided by the total number of sampled tickets in the Measurement Window, with the result expressed as a percentage.
• ((Number of service restorals and requests that met the interval) / (the total number of service restorals and requests)) expressed as a percentage</td></tr>
<tr><td>Service Level Reporting Window</td><td>Monthly</td></tr>
</table>

SL27 Service Desk – Customer Satisfaction

Service Level Reference	Description
Service Desk – Customer Satisfaction	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the average scores of the customer satisfaction surveys taken on a random statistical sample of customers that had a service contact with the Contractor during the measurement period. The surveys will be conducted in accordance with the Commonwealth Computing Procedures Manual.
Metric Inclusions	Survey responses shall be on a five (5) point scale (with five (5) being the most satisfied) or shall reflect such other satisfaction criteria established pursuant to the survey design process.
Metric Exclusions	• All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** At the Commencement Date, This Service Level calculation is the sum of all scores for each response (question answered) for the surveys that are returned during the applicable Measurement Window, divided by the total number of responses for all surveys that are returned during the applicable Measurement Window. • = (Average Score of Surveys)
Service Level Reporting Window	Monthly

SL28 Batch Scheduling Launched on Time

Service Level Reference	Description
Batch Scheduling Launched on Time	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the percentage of time Contractor starts the Batch job schedules defined in the standard scheduling tool or manually scheduled at the established start time associated with such schedules specified in the Commonwealth Computing Procedures Manual. Established start time is defined for this Service Level as the first Batch job, which is started after 12:00 noon eastern time, starts within five (5) minutes of its scheduled time as detailed the CCPM.
Metric Inclusions	Scheduled Batch jobs include normally scheduled and recurring production jobs, as well as production jobs that are run on an as-needed basis.
Metric Exclusions	• Any batch jobs related to infrastructure backups, or other functionality exclusive for Contractor would be excluded. • All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is the total number of Batch job schedules defined in the standard scheduling tool that are started during the applicable Measurement Window at the established start time associated with such schedules as set forth in the Commonwealth Computing Procedures Manual, divided by the total number of Batch job schedules that should have been started during the applicable Measurement Window, with the result expressed as a percentage. • = (Number Of Batches Launched On Time) / (Total Number Of Batches Scheduled) expressed as a percentage
Service Level Reporting Window	Monthly

SL29 Batch Processing Completed Successfully

Service Level Reference	Description
Batch Processing Completed Successfully	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the percentage of time Contractor completes Batch jobs successfully and on time during the applicable Measurement Window in accordance with the relevant specifications located in the Commonwealth Computing Procedures Manual.
Metric Inclusions	Batch jobs include normally scheduled and recurring production jobs, as well as production jobs that are run on an as-needed basis. To be considered Successful the Batch must complete within the schedule window for that particular Batch Job.
Metric Exclusions	• Any batch jobs related to infrastructure backups, or other functionality exclusive for Contractor would be excluded. • All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is the total number of Batch jobs that are completed successfully and on time in accordance with the relevant criteria set forth in the Online CCPM repository during the applicable Measurement Window, divided by the total number of Batch jobs that should have been completed during the applicable Measurement Window, with the result expressed as a percentage. • = ((Number of successful batches) / (Total number of batches scheduled)) expressed as a percentage
Service Level Reporting Window	Monthly

SL30 Reports Delivered On Time

Service Level Reference	Description
Reports Delivered On Time	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level for reports delivered on time as outlined in Schedule K reports measures the percentage of time Contractor delivers the reports on time in accordance with the requirements. Each Report provided with respect to a Critical Service Level or Key Measurement shall be deemed an individual Report for the purposes of calculating this Service Level.
Metric Inclusions	Schedules as set forth in the Commonwealth Computing Procedures Manual.
Metric Exclusions	• Any reports identified as Critical Monthly reports in the Commonwealth Computing Procedures Manual and measured in Critical Service Levels. • All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is a count of the total number of reports that were not successfully delivered (i.e. on time and in compliance with content and format requirements) during the applicable Measurement Window. • = ((Number of reports delivered on time) / (Total number of reports scheduled to be delivered)) expressed as a percentage
Service Level Reporting Window	Monthly

SL31 Off-Site Media Management

Service Level Reference	Description
Off-Site Media Management	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the accuracy of the Contractor's management of off-site media, specifically the physical location and electronic tracking accuracy of off-site media. The measure is intended to sample one-twelfth of the universe of off-site media such that each the Commonwealth Customer's complete environment is sampled at least once per year.
Metric Inclusions	All media for which Contractor receives an off-site storage resource unit charge.
Metric Exclusions	• Virtual tapes and tapes retained in locations designated within Schedule E. • All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	N/A
Days of Measurement	N/A
Calculation	• **Summary:** This Service Level calculation is based on a statistically valid random sample representing one-twelfth of the universe of off-site media and is the sum of the number of times a tape is either physically in the correct location or electronically listed in the correct location divided by the total number of tapes in the random sample, with the result expressed as a percentage. • = ((Number of correct audits) / (Total number of audits))expressed as a percentage
Service Level Reporting Window	Monthly

SLXX Name (Template)

Service Level Reference	Description
SLA Name (Template)	
Service Category	
Metric Description	
Metric Inclusions	
Metric Exclusions	
Hours of Measurement	
Days of Measurement	
Calculation	
Collection Process	
Reporting Tools / Data Source(s)	
Data Storage (Archives)	
Reporting Format/s	
Service Level Reporting Window	

3. Notes

Note 1: Contractor's failure to achieve any Service Level will not constitute a Service Level Default or accrue toward a Service Level Termination Event to the extent such failure is directly attributable to any Force Majeure events as (as defined in Paragraph 65 of the Contract.

Note 2: Contractor's failure to achieve any Service Level will not constitute a Service Level Default or accrue toward a Service Level Termination Event to the extent such failure is directly attributable to any of the following:

(i) the failure or unavailability of equipment or other resources for which the Commonwealth is operationally and managerially responsible pursuant to the Contract,

(ii) changes made to the environment by the Commonwealth that were not communicated in accordance with the Change Control Procedure or other method agreed upon by the Parties, and

(iii) scheduled and approved maintenance windows.

Schedule K

Key Program Deliverables

Table of Contents

INTRODUCTION –PROGRAM DELIVERABLES 3
KEY PROGRAM DELIVERABLES 3
D-01 Datacenter Architecture Plan and Roadmap 3
D-02 Commonwealth Computing Procedures Manual (CCPM) 5
D-03 Technology Architecture and Refresh Approach 15
D-04 IT Service Continuity Architecture and Plan 17
D-05 Transition Management Plan 18
D-06 Agency Level DR Plan(s) 20
D-07 Security Management Plan 20
D-08 Facilities Management Plan 22
D-09 Security Risk and Vulnerability Assessment Report 23
D-10 Gap Analysis Report 23
D-11 Contract Management Plan 24
D-12 Schedule C.2 - Service Descriptions Initial Completion 24
DELIVERABLE ACCEPTANCE CRITERIA MATRIX 26
EXAMPLE - DELIVERABLE ACCEPTANCE MATRIX 28

Introduction –Program Deliverables

This Schedule sets forth certain obligations of Offeror regarding Program Deliverables. The Offeror must deliver to the Commonwealth any Key Program Deliverables as described below, in format and content acceptable to the Commonwealth.

As specified below, Offeror shall provide each Key Program Deliverable on or before the date specified in this Schedule. The Key Program Deliverable Acceptance Criteria and the Commonwealth Sign-off Matrix will be developed prior to the Effective Date and will be in the format referenced below in this document.

Key Program Deliverables

D-01 Datacenter Architecture Plan and Roadmap

The Datacenter Architecture Plan and Roadmap will include the Offeror's proposed Datacenter Architecture that will be utilized to support the Project. The Datacenter Architecture Plan and Roadmap should include at minimum sections that support the following:

- 2+ Datacenter Architecture (with EDC) - describes the overall Datacenter Architecture used in the delivery of the Offeror's Enterprise Datacenter Services. This should include details on datacenter specifications, location, physical security, and capacity. The architecture will show how the Commonwealth's Enterprise Data Center (EDC) will be incorporated into the Offeror's overall datacenter capacity.

- Datacenter Network Architecture - describes the required network connectivity between each of the datacenters. Included are connection requirements to the Commonwealth's network COPANET. The Offeror will also describe its Internet connection to the proposed Datacenter(s).

- Datacenter Security Architecture - describes the security architecture used to ensure the confidentiality, integrity and availability of Commonwealth information and infrastructure systems. The Security Architecture will describe the security technology components such as firewalls, intrusion detection devices, virus detection, etc. that will be utilized in the Offerors solution. Datacenter Security implementation activities must be conducted in accordance with, but not limited to, leading industry and Commonwealth standards such as ISO 27001:2005 and ISO 27002:2005.

- Datacenter Technology Environment - describes the Datacenter technology used in the delivery of the Offeror's Enterprise Datacenter Services. A summary of the planned allocation of platforms within each of the proposed datacenters should be included. Note: more detailed technology specifications shall be provided in the *D-03 Technology Architecture and Refresh Approach* deliverable.

- Datacenter Implementation Roadmap – presents the detailed implementation plan for the enablement of the overall Datacenter Architecture. The Datacenter Implementation Roadmap shall Reference roles and responsibilities, as well as critical dates and timelines.

EDC Assessment		
D-01.01	Effective Date + 45 days	Offeror must assess the EDC facilities and provide a report to the Commonwealth as it pertains to: • Required security upgrades • Required HVAC and power upgrades • Required physical access to the EDC facility • Monitoring, maintain and reporting on EDC SLAs • Monitoring, maintaining and operating the installed infrastructure
Multi Datacenter Environment (2+ Architecture)		
D-01.02	Effective Date + 60 days – with quarterly updates	*Datacenter Architecture Plan and Roadmap* Datacenter Architecture Plan and Roadmap includes: • 2+ datacenter architecture (with/plus EDC) • Datacenter Network Architecture • Datacenter Security Architecture • Datacenter Technology Environment • Datacenter Implementation Roadmap Offeror must publish quarterly updates to the Datacenter Architecture Plan and Roadmap to include proposed updates to the technical architecture and implementation plan
Network and Security Architecture		
D-01.03	Effective Date + 60 days – with quarterly updates	*Datacenter Architecture Plan and Roadmap – Network and Security Architecture* The Network and Security Architecture - describes the network and security architecture to support the 2+ datacenter architecture.
Datacenter Architecture and Technology		
D-01.04	Effective Date +60 days– with quarterly updates	*Datacenter Architecture Plan and Roadmap* – Datacenter Technology The Datacenter Technology describes the technology used in the delivery of the Offeror's Enterprise Datacenter Services.
D-01.05	Effective Date +90 days – with quarterly updates	*Datacenter Architecture Plan and Roadmap* – Datacenter Technology Roadmap The Datacenter Technology Roadmap will identify specific, short-term steps and schedules for project of changes with estimated timings and cost impact to Commonwealth datacenter customers.

D-01.06	Effective Date + 180 days	*Datacenter Architecture Plan and Roadmap – Configuration Item Reconciliation* *The Configuration Item Reconciliation is the validation and update of the CMDB of record with the Offeror's configuration information including the EDC assets and CI's.*
Limited-Use Colocation Services		
D-01.07	Effective Date + 30 days	*Datacenter Architecture Plan and Roadmap*

D-02 Commonwealth Computing Procedures Manual (CCPM)

Offeror will develop documentation in accordance with the requirements in **Schedule H** - **Commonwealth Computing Procedures Manual (CCPM)**. This comprehensive services management manual will include, but not be limited to, the following sections as described in **Schedule H**:

- Organizational Overview
- Transition and Support Activities and Responsibilities
- IT Service Management Procedures
- Financial Management Procedures
- Contract Management Procedures
- Relationship Management Procedures
- Offeror Operational Procedures
- Commonwealth Customer Operations Manuals

Additional Planning Services		
D-02.01	Effective Date + 14 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide the initial version of the Commonwealth Computing Procedures Manual (CCPM) (see Schedule H CCPM Commonwealth Computing Procedures Manual) that includes Offeror's overall program and service management processes and procedures. The comprehensive manual includes the following sections: • Organizational Overview • Transition and Support Activities and Responsibilities • IT Service Management Procedures • Financial Management Procedures • Contract Management Procedures • Relationship Management Procedures • Offeror Operational Procedures • The Commonwealth Customer Operations Manuals PMO & Contract Management will focus on the bolded sections of the CCPM.

D-02.02	As needed during transition	After review and approval from the Commonwealth, Offeror must provide ongoing updates to the CCPM during the startup and transition phase
D-02.03	Yearly or as required	Offeror must provide CCPM updates as required as new services are added and yearly after the transition phase.
Availability/SLA Management		
D-02.04	Effective Date + 30 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must document the Availability and SLA Management approach and providing updates to the CCPM.
D-02.05	Effective Date +45 days	*Commonwealth Computing Procedures Manual (CCPM)* After review and approval from the Commonwealth, Offeror must review the Availability and SLA Management approach and project plan with Commonwealth stakeholders.
D-02.06	Monthly	*Commonwealth Computing Procedures Manual (CCPM)* SLA Achievement Report, detailing system availability, SLA attainment, and reason for outages.
D-02.07	As Needed	*Commonwealth Computing Procedures Manual (CCPM)* Root Cause Analysis (RCA) report for all major outages within SLA (e.g. hours/days of outage).
D-02.08	As requested	*Commonwealth Computing Procedures Manual (CCPM)* Ad hoc – Availability and SLA Reports
Change & Release Management		
D-02.09	Effective Date + 30 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must document the Change and Release Management approach and project plan updating appropriate sections to the CCPM.
D-02.10	Effective Date +45 days	*Commonwealth Computing Procedures Manual (CCPM)* After review and approval from the Commonwealth, Offeror must review the Change and Release Management approach and project plan with Commonwealth stakeholders.
D-02.11	Weekly	*Commonwealth Computing Procedures Manual (CCPM)* Weekly Change Management Meeting with the Change Advisory Board
D-02.12	Monthly	*Commonwealth Computing Procedures Manual (CCPM)* Monthly Change & Release Management summary report containing the number of changes, by platform, by Commonwealth organization, and status.

D-02.13	Yearly	*Commonwealth Computing Procedures Manual (CCPM)* On a yearly basis, randomly select completed Changes & Releases for detail auditing to determine compliance to policies. Create a summary report of the finding and make recommendations for improvements where appropriate.
D-02.14	Per Change Event	*Commonwealth Computing Procedures Manual (CCPM)* Complete Change Control & Release Management process for each change event adhering to the letter and spirit of the policy and process. Maintain a complete copy of the change / release for possible future audit.
Service Desk		
D-02.15	Effective Date + 30 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must document the Service Desk approach, organization, schedule and project plan.
D-02.16	Effective Date +45 days	*Commonwealth Computing Procedures Manual (CCPM)* After review and approval from the Commonwealth, Offeror must review the Service Desk approach and project plan with Commonwealth stakeholders
D-02.17	Effective Date + 60 days	*Knowledge Management Portal (KMP)* Offeror must provide a Knowledge/Service Management portal that describes the Offeror's contract information, pricing schedules, service offerings and operating procedures (operational, service delivery processes, SLAs, service ordering, etc.)
D-02.18	Effective Date +60 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide Commonwealth Computing Procedures Manual (CCPM) including but not limited to the following: Datacenter Operations, Change Management, Service Desk Operations, Security Management, Backup Management, Disaster Recovery, Performance Management, Asset Management, Service Level Management and Configuration Management. The Offeror must make the CCPM available on the Offeror's Knowledge/Service portal. See Schedule H Commonwealth Computing Procedures Manual (CCPM) for additional detail.
D-02.19	Effective Date +180 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must describe the process to keep separate and current specific sections of the CCPM dedicated to the operations of individual Commonwealth customers.
D-02.20	Effective Date +90 days	Knowledge Management Portal Offeror must provide Knowledge/Service portal training to authorized Commonwealth stakeholders

D-02.21	Weekly	*Commonwealth Computing Procedures Manual (CCPM)* Weekly summary report containing the type of incidents and problems being reported to the Service Desk. Identify measures being taken to reduce or eliminate stated incidents and problems.
D-02.22	Monthly	*Commonwealth Computing Procedures Manual (CCPM)* Monthly summary report containing the type of incidents and problems being reported to the Service Desk. Identify measures being taken to reduce or eliminate stated incidents and problems.
Account Management		
D-02.23	Effective Date + 30 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must document their Account Management approach and project plan.
D-02.24	Effective Date +45 days	*Commonwealth Computing Procedures Manual (CCPM)* After review and approval from the Commonwealth, Offeror must review the Account Management approach and project plan with Commonwealth stakeholders
D-02.25	Monthly	Monthly summary report containing the operational availability report on all systems in service, events and issues that occurred during the month. Report shall contain operational metrics by service platform, highlights and exceptions, and project status updates.
Configuration Management		
D-02.26	Effective Date + 30 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must document their Configuration Management approach, tool(s) and project plan.
D-02.27	Effective Date +45 days	*Commonwealth Computing Procedures Manual (CCPM)* After review and approval from the Commonwealth, Offeror must review the Configuration Management approach, tool(s) and project plan with Commonwealth stakeholders
D-02.28	As Requested	Offeror must provide Agency / Commonwealth level Configuration Management Reports
3rd Party License Management		
D-02.29	Effective Date + 30 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must document their 3rd Party License Management approach, tool(s) and project plan.

D-02.30	Effective Date +45 days	*Commonwealth Computing Procedures Manual (CCPM)* After review and approval from the Commonwealth, Offeror must review the 3rd Party License Management approach, tool(s) and project plan with Commonwealth stakeholders
D-02.31	Per request	Offeror must provide Software License Reports
Capacity Management		
D-02.32	Effective Date + 30 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must document their Capacity Management approach, tool(s) and project plan.
D-02.33	Effective Date +45 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must review the Capacity Management approach, tool(s) and project plan with Commonwealth stakeholders
D-02.34	Effective Date + 240 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must present the baseline Capacity Management Plan
D-02.35	Monthly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must issue periodic reports showing usage, trends, capacity forecasts, and recommendations for upgrades.
D-02.36	Annual	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide technology usage report (i.e. MIPS, vcpu, storage, etc.) by stakeholder and overall usage by the Commonwealth. The report must show monthly technology growth patterns by stakeholder.
Windows Support		
D-02.37	Effective Date + 30 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must present their roadmap and project plan to address the Windows Operations and Management including but not limited to the following; windows servers, backups, network connectivity, technical support, staffing, etc.
D-02.38	Effective Date + 45 days	*Commonwealth Computing Procedures Manual (CCPM)* After review and approval from the Commonwealth, Offeror must present plan to address the assessment recommendations identified in the Windows Operations and Management project plan.
D-02.39	Effective Date +60 days	*Commonwealth Computing Procedures Manual (CCPM)* Present a report describing the methodology the Offeror will follow to perform a Windows backups audit finding and recommendation to the Commonwealth Stakeholders, the audit report will include findings, recommendations, project plan and cost estimates.

D-02.40	Monthly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide SLA report(s). Provide a report detailing system availability, SLA attainment, reason for outages, and recommendations for improvements.
D-02.41	Quarterly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide Continuous Improvement Report. Provide a report detailing system availability and SLA attainment. Recommend system and cost improvements as appropriate.
Storage Management		
D-02.42	Effective Date + 30 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must present their roadmap and project plan to address Storage Management including but not limited to the following; data storage, backups, network connectivity, technical support, staffing, etc.
D-02.43	Effective Date + 45 days	*Commonwealth Computing Procedures Manual (CCPM)* After review and approval from the Commonwealth, Offeror must present plan to address the assessment recommendations identified in the Storage Management project plan.
D-02.44	Effective Date +60 days	*Commonwealth Computing Procedures Manual (CCPM)* Present a report describing the methodology the Offeror will follow to perform a system backups audit finding and recommendation to the Commonwealth Stakeholders, the audit report will include findings, recommendations, project plan and cost estimates.
D-02.45	Monthly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide SLA report(s). Provide a report detailing system availability, SLA attainment, reason for outages, and recommendations for improvements.
D-02.46	Quarterly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide Continuous Improvement report(s). Provide a report detailing system availability and SLA attainment. Recommend system and cost improvements as appropriate.
ERP Hosting – SAP / Oracle		
D-02.47	Effective Date + 30 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must present their roadmap and project plan to address ERP Hosting including but not limited to the following; data storage, backups, network connectivity, technical support, staffing, etc.

D-02.48	Effective Date + 45 days	*Commonwealth Computing Procedures Manual (CCPM)* After review and approval from the Commonwealth, Offeror must present plan to address the assessment recommendations identified in the ERP Hosting project plan.
D-02.49	Effective Date +60 days	*Commonwealth Computing Procedures Manual (CCPM)* Present a report describing the methodology the Offeror will follow to perform a system backup audit finding and recommendation to the Commonwealth Stakeholders, the audit report will include findings, recommendations, project plan and cost estimates.
D-02.50	Monthly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide SLA report(s). Provide a report detailing system availability, SLA attainment, reason for outages, and recommendations for improvements.
D-02.51	Quarterly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide Continuous Improvement report(s). Provide a report detailing system availability and SLA attainment. Recommend system and cost improvements as appropriate.
UNIX Support – AIX / Linux		
D-02.52	Effective Date + 30 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must present their roadmap and project plan to address UNIX Support including but not limited to the following; data storage, backups, network connectivity, technical support, staffing, etc.
D-02.53	Effective Date + 45 days	*Commonwealth Computing Procedures Manual (CCPM)* After review and approval from the Commonwealth, Offeror must present plan to address the assessment recommendations identified in the UNIX Support project plan.
D-02.54	Effective Date +60 days	*Commonwealth Computing Procedures Manual (CCPM)* Present UNIX audit finding and recommendation to the Commonwealth Stakeholders, the report will include findings, recommendations, project plan and cost estimates.
D-02.55	Monthly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide SLA report(s). Provide a report detailing system availability, SLA attainment, reason for outages, and recommendations for improvements.
D-02.56	Quarterly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide Continuous Improvement report(s). Provide a report detailing system availability and SLA attainment. Recommend system and cost improvements as appropriate.

Mainframe Services		
D-02.57	Effective Date + 30 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must present their roadmap and project plan to address Mainframe Support (IBM & Unisys) including but not limited to the following; data storage, backups, network connectivity, technical support, staffing, etc.
D-02.58	Effective Date + 45 days	*Commonwealth Computing Procedures Manual (CCPM)* After review and approval from the Commonwealth, Offeror must present project plan to address the assessment recommendations identified in the Mainframe Support (IBM & Unisys) plan.
D-02.59	Effective Date +60 days	*Commonwealth Computing Procedures Manual (CCPM)* Present mainframe audit finding and recommendation to the Commonwealth Stakeholders, the report will include findings, recommendations, project plan and cost estimates.
D-02.60	Monthly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide SLA report(s). Provide a report detailing system availability, SLA attainment, reason for outages, and recommendations for improvements.
D-02.61	Quarterly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide Continuous Improvement report(s). Provide a report detailing system availability and SLA attainment. Recommend system and cost improvements as appropriate.
Database Management Services		
D-02.62	Effective Date + 30 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must document their Database Management approach, tool(s) and project plan.
D-02.63	Effective Date +45 days	*Commonwealth Computing Procedures Manual (CCPM)* After review and approval from the Commonwealth, Offeror must review the Database Management approach, tool(s) and project plan with Commonwealth stakeholders
D-02.64	Effective Date +60 days	*Commonwealth Computing Procedures Manual (CCPM)* Present backup audit finding and recommendation to the Commonwealth Stakeholders, the report will include findings, recommendations, project plan and cost estimates.
D-02.65	Effective Date	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide Database Management Service Architecture document (Oracle, Sybase, and MS SQL).

D-02.66	Monthly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide Database Management Service Usage Reports
Server Capacity on Demand		
D-02.67	Effective Date + 30 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must document their Server Capacity on Demand approach, tool(s) and project plan.
D-02.68	Effective Date +45 days	*Commonwealth Computing Procedures Manual (CCPM)* After review and approval from the Commonwealth, Offeror must review the Server Capacity on Demand approach, tool(s) and project plan with Commonwealth stakeholders
D-02.69	Quarterly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must host a quarterly meeting with the Commonwealth to review current server utilization on all managed server platforms and locations, and forecast future quarter's server processing requirements. Recommendations to increase capacities will be made, when approved by the Commonwealth; the additional equipment will be scheduled for deployment.
Storage Capacity on Demand		
D-02.70	Effective Date + 30 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must document their Storage Capacity on Demand approach, tool(s) and project plan.
D-02.71	Effective Date +45 days	*Commonwealth Computing Procedures Manual (CCPM)* After review and approval from the Commonwealth, Offeror must review the Storage Capacity on Demand approach, tool(s) and project plan with Commonwealth stakeholders
D-02.72	Quarterly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must host a quarterly meeting with the Commonwealth to review current SAN storage utilization on all managed SAN platforms and locations, and forecast future quarter's SAN storage requirements. Recommendations to increase capacities will be made, when approved by the Commonwealth; the additional equipment will be scheduled for deployment.
DR Infrastructure on Demand		
D-02.73	Quarterly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must host a quarterly meeting with the Commonwealth to review current disaster recovery service and capabilities, and forecast future quarter's disaster recovery requirements. Recommendations to increase capacities will be made, when approved by the Commonwealth, the additional equipment and services will be scheduled for deployment.

Additional Technical Services		
D-02.74	Monthly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide a monthly report on technical support services usage by Commonwealth datacenter customer.
Limited-Use Colocation Services		
D-02.75	Effective Date + 30 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must document their approach, tool(s) and project plan for supporting Limited-Use Colocation Services.
D-02.76	Effective Date +45 days	*Commonwealth Computing Procedures Manual (CCPM)* After review and approval from the Commonwealth, Offeror must review the Limited-Use Colocation Services approach, tool(s) and project plan with Commonwealth stakeholders
D-02.77	Effective Date +60 days	*Commonwealth Computing Procedures Manual (CCPM)* Present backup audit finding and recommendation to the Commonwealth Stakeholders, the report will include findings, recommendations, project plan and cost estimates.
D-02.78	Monthly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide Limited-Use Colocation Services Usage Reports
Performance Monitoring & Management		
D-02.79	Monthly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide monthly summary report containing the performance level achieved for each system being monitored. This report will be reviewed with the Commonwealth and plans will be made to address system utilization as appropriate.
D-02.80	Daily	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide daily reports containing the performance level achieved for each system being monitored. Daily reports summarizing incidents for the past 24-hours and immediate reports of incidents and routine status reports of incidents in progress for resolution such as a network or server outage that impacts a facility and our business. These reports will be reviewed with the Commonwealth and plans will be made to address system utilization as appropriate.

Transition Program Management		
D-02.81	Effective Date + 60 days	*Commonwealth Computing Procedures Manual (CCPM)* Establish Interim Contract Management Procedures during the transition of datacenter services. Offeror must describe an interim procedure to monitor and manage service delivery including but not limited to the following; Problem Management, Change Management, Service Level monitoring and reporting, physical and logical security, project management, etc. while the service is transitioned from the Commonwealth to the Offeror.
D-02.82	Weekly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide Transition Status reports, including any schedule variance that cannot be remediated will trigger the escalation procedures outlined in the Transition Plan/Agreement, which will be developed during Transition.
Security & Firewall		
D-02.83	Quarterly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide Continuous Improvement report. Provide a report detailing system availability and SLA attainment. Recommend system and cost improvements as appropriate.

D-03 Technology Architecture and Refresh Approach

The Technology Architecture and Refresh Approach will include the Offeror's proposed the Technology that will be utilized to support the architecture and delivery of services across all platform and services. The Technology Architecture and Refresh Approach should include at minimum sections that support the following:

- Datacenter Technology - describes the technology used in the delivery of the Offeror's Enterprise Datacenter Services. The technology descriptions should include hardware, software that will be included in the overall solution delivery. The technology should also include a complete list of those Service Level measurement and monitoring tools that will be used to measure and report Offeror's performance of the Services at a level of detail sufficient, as determined by the Commonwealth, to verify Offeror's compliance with those Service Levels described in **Schedule J.1 Datacenter Service Level Management** as of the Effective Date.

- Datacenter Technology Roadmap - will identify specific, short and long term steps and schedules for planned and proposed future changes with estimated timings and cost impact to Commonwealth datacenter customers. This should be the basis for generation of technology roadmaps which will include schedules, dependencies and requirements for introduction of new technology changes as well as acquisition, support, and retirement of current software/hardware.

- Configuration Item Reconciliation - is the validation and update of the CMDB of record with the Offerors configuration information including the EDC assets and Configuration Items (CI's).

Technology Refresh		
D-03.01	Effective Date + 30 days	*Technology Architecture and Refresh Approach* Offeror must document the following Technical Architecture approach and project plan including; Service Catalog, IT Architecture, and Technical support
D-03.02	Effective Date +45 days	*Technology Architecture and Refresh Approach* After review and approval from the Commonwealth, Offeror must review the Technical Architecture approach and project plan with Commonwealth stakeholders
D-03.03	Effective Date + 60 days	Offeror must identify the technical architecture organization and staff.
Infrastructure Architecture		
D-03.04	Effective Date + 45 days	*Technology Architecture and Refresh Approach* Offeror must document the approach and project plan for the computing infrastructure architecture and review with Commonwealth Stakeholders
D-03.05	Effective Date + 45 days	*Technology Architecture and Refresh Approach* After review and approval from the Commonwealth, Offeror must document the approach and project plan for the network architecture to connect Offeror's datacenter(s), review with Commonwealth Stakeholders
D-03.06	As requested by Commonwealth Stakeholders	*Technology Architecture and Refresh Approach* Offeror must describe the process to request a review new technologies evaluations by Commonwealth datacenter customers.
D-03.07	Per request – prior to a new application infrastructure service	*Technology Architecture and Refresh Approach* Offeror must provide Infrastructure Architecture Design Reports
Performance Monitoring & Management		
D-03.08	Effective Date + 30 days	*Technology Architecture and Refresh Approach* Offeror must document their Performance Monitoring and Management approach, tool(s) and project plan.

D-03.09	Effective Date +45 days	*Technology Architecture and Refresh Approach* After review and approval from the Commonwealth, Offeror must review the Performance Monitoring and Management approach, tool(s) and project plan with Commonwealth stakeholders

D-04 IT Service Continuity Architecture and Plan

The IT Service Continuity Architecture and Plan will include the Offeror's proposed Disaster Recovery (DR) solution architecture. The DR solution architecture will describe how the Offeror will deliver multiple tiers of disaster recovery services. The IT Service Continuity Architecture and Plan will also describe the Offeror's approach to reviewing the Commonwealth's current DR Plans and the updating of those plans in coordination with the Commonwealth.

IT Service Continuity Architecture		
D-04.01	Effective Date + 30 days	*IT Service Continuity Architecture and Plan* Offeror must describe their methodology for reviewing and refreshing technology on a scheduled basis.
D-04.02	Effective Date + 30 days	*IT Service Continuity Architecture and Plan* Offeror must provide an IT Service Continuity Architecture and Plan to Implement DR solution
D-04.03	30 days prior to transition of each critical application	*IT Service Continuity Architecture and Plan* Offeror must describe their approach to providing Develop/Update Agency Application DR and Business Recovery Plan(s)
D-04.04	Depending on DR Tier Solution • Current DR • Tier 0 • Tier 1 • Tier 2 • Tier 3 • Tier 4	*IT Service Continuity Architecture and Plan* Offeror must develop a plan to transition agencies to Tiered DR Solution • Currently have DR (DPH) – at time of transition • Tier 0 – Transition + 90 days • Tier 1 – Transition + 60 days • Tier 2 – Transition + 30 days • Tier 3 – at time of transition • Tier 4 – at time of transition
DR Planning & Testing		
D-04.05	Effective Date + 30 days	*IT Service Continuity Architecture and Plan* Offeror must document their Tiered Disaster Recovery approach, tool(s) and project plan.

D-04.06	Effective Date +45 days	*IT Service Continuity Architecture and Plan* After review and approval from the Commonwealth, Offeror must review their Tiered Disaster Recovery approach, tool(s) and project plan with Commonwealth stakeholders
D-04.07	Monthly	*IT Service Continuity Architecture and Plan* Offeror must provide report(s) describing schedule of stakeholder participation in DR solution

D-05 Transition Management Plan

The Transition Management Plan will provide a detailed overview of the Offeror's transition management approach, process and procedures. The Transition Management Plan will describe the enablement of the Transition Project Management Office (TPMO) and also provide a detailed implementation schedule of transition activities and milestones. The Transition Management Plan should include at minimum sections that support the following:

- Transition Management Approach
- Transition Project Management Office (TPMO) Organization and Responsibilities
- Transition Management Communications Plan
- Transition Schedule

Transition Management (New Customer and/or Services)		
D-05.01	Effective Date + 60 days	*Transition Management Plan* Offeror must create a Transition Roadmap with major milestones and present it to the Commonwealth for review
D-05.02	Effective Date + 90 days	*Transition Management Plan* After review and approval from the Commonwealth, Offeror must create a Detailed Transition Project Plan with major milestones and present it to the Commonwealth for review
D-05.03	Weekly	*Transition Management Plan* Offeror must create a report for the Commonwealth detailing the transition projects on the plan, status, schedule, risks, and the forecasted transition date.

Transition Program Management		
D-05.04	Effective Date + 60 days	*Transition Management Plan* Offeror must present their approach to transition Commonwealth computing assets. The approach must include a roadmap and project plan to successfully transition Commonwealth computing assets using the schedule identified in the RFP
D-05.05	Effective Date + 90 days	*Transition Management Plan* Present and review the transition roadmap and plan to Commonwealth stakeholders.
D-05.06	Effective Date + 60 days	*Transition Management Plan* Establish Interim Contract Management Procedures during the transition of datacenter services. Offeror must describe an interim procedure to monitor and manage service delivery including but not limited to the following; Problem Management, Change Management, Service Level monitoring and reporting, physical and logical security, project management, etc. while the service is transitioned from the Commonwealth to the Offeror.
D-05.07	Effective Date + 60 days	*Transition Management Plan* EDC / Legacy Datacenter Infrastructure Maintenance Strategy – Offeror must document their strategy as it related to providing a solution to the infrastructure maintenance expiration issue at the EDC and any other datacenter that has the same or similar issue.
D-05.08	Effective Date + 60 days	*Transition Management Plan* Offeror must provide the procedure to standup their Transition Management Office
D-05.09	Weekly during transition	*Transition Management Plan* Offeror must provide Transition Status reports, including any schedule variance that cannot be remediated will trigger the escalation procedures outlined in the Transition Plan/Agreement, which will be developed during Transition.
Security Transition Activities		
D-05.10	Effective Date + 60 days	*Transition Management Plan* Offeror must provide their Security Transition Plan
D-05.11	Weekly updates during transition	*Transition Management Plan* Offeror must provide their Security Transition Status Report(s)

D-06 Agency Level DR Plan(s)

The Offeror is required to assist the Commonwealth Agencies with updates to or development of their current DR Plans (DRPs). These Agency Level DR Plans will reflect the Offeror's DR approach and solution for DR testing. The following describes the Offeror's responsibilities regarding the updating of Agency Level DRPs:

- Within six (6) months after the Effective Date, Offeror shall complete the update all existing Agency-specific Disaster Recovery Plans and technical recovery guides to reflect all changes implemented to the Services infrastructure prior to or during the performance of Transition Services.
- For Applications lacking tested Disaster Recovery Plans, Offeror shall work with Commonwealth Agencies to complete a gap analysis of the current Disaster Recovery Plans and technical recovery guides compared to the requested recovery time objective, as specified in **Schedule J.1 Datacenter Service Level Management**, and update the Disaster Recovery Plans with the results within forty-eight (48) months after the Effective Date.
- For Agencies without a Disaster Recovery Plan, the Offeror shall work with Agencies to develop a basic Disaster Recovery Plan and technical recovery guides within eighteen (18) months after the Effective Date.

DR Planning & Testing		
D-06.01	Monthly	*Agency Level DR Plan* Offeror must provide report(s) describing the schedule of DR test being performed by stakeholders
D-06.02	Monthly	*Agency Level DR Plan* Offeror must provide report(s) describing the results of stakeholder DR test
D-06.03	As requested– Per Agency Critical Application	*Agency Level DR Plan* Offeror must provide DR Test Plans as required

D-07 Security Management Plan

The Security Management Plan will address the overall security management for the planned facility security implementation for the EDC, the Offeror Facilities, software and equipment deployment specifically for data and online security, annual security assessments and other standard security concepts for ensuring the safety, security and confidentiality of Commonwealth Data.

The Security Management Plan shall include a complete description of the personnel security management program. It shall comply with background check requirements specified in the Terms and Conditions and shall provide a methodology for ongoing evaluation and reporting of any change in status of Offeror personnel that would negatively impact their ability to continue to meet Commonwealth or Agency security requirements.

Security Management		
D-07.01	Effective Date + 30 days	*Security Management Plan* Offeror must document their Security Management approach, tool(s) and project plan.
D-07.02	Effective Date +45 days	*Security Management Plan* After review and approval from the Commonwealth, Offeror must review their Security Management approach, tool(s) and project plan with Commonwealth stakeholders.
D-07.03	Quarterly	*Security Management Plan* Offeror must provide the Commonwealth with a report containing the detailed results of the Vulnerability Analyses testing. Include any remediation activities that are required.
D-07.04	Monthly	*Security Management Plan* Offeror must provide the Commonwealth with the detailed monthly Security Log Analysis report. Include any remediation activities that are required.
D-07.05	Ongoing	*Security Management Plan* Offeror must maintain a hardcopy file of all security access changes. The copy will contain the date, time, file changes, access rights applied and the name of the security officer completing the access request.
Security & Firewall		
D-07.06	Effective Date + 30 days	*Security Management Plan* Offeror must document their Security and Firewall approach, tool(s) and project plan.
D-07.07	Effective Date +45 days	*Security Management Plan* After review and approval from the Commonwealth, Offeror must review the Security and Firewall approach, tool(s) and project plan with Commonwealth stakeholders
D-07.08	Monthly	*Security Management Plan* Threat Assessment and Analysis Report. Provide a monthly report detailing the threat assessments, volume and major types of malware detected, volume of SPAM rejected, corrective actions, and recommendations that would improvement security of Commonwealth systems.
D-07.09	Monthly	*Security Management Plan* Offeror must provide SLA reports. Provide a report detailing system availability, SLA attainment, reason for outages, and recommendations for improvements, security incident notification, and security change request intervals and results.

D-07.10	Monthly	*Security Training and On-boarding Status Report* Offeror must provide a monthly Security Training and On-boarding Status Report detailing security training, changes to project personnel, and background check status and results.

D-08 Facilities Management Plan

The Facilities Management Plan will address management for both the EDC facility and the proposed Offeror's facility(s). The Facilities Management Plan should describe the Offeror's plan for providing and managing the physical environment. For example; power and power distribution, cooling and ventilation, fire detection and suppression, building security and access control, and environmental monitoring. Provide an approach for yearly review and self-verification that the datacenters will be managed, maintained and operated at the equivalent of Uptime Institute of Tier 3 rating. The plan should also address how the Offeror will support SSAE-16 compliance audits.

Facilities Architecture / Maintenance		
D-08.01	Effective Date + 60 days	*Facilities Management Plan* Offeror must present their assessment of the EDC and any required facility changes/modification required to upgrade the facility to meet service level objectives. The assessment must include a roadmap and project plan to make any required facility modifications.
D-08.02	On the July 31st following the Commonwealth's acceptance of Milestone M-14	*Facilities Management Plan* Present results of the SSAE 16 audit of the EDC. The audit period is to cover the period from Transition completion through the following June 30th
D-08.03	Monthly	*Facilities Management Plan* Offeror must provide monthly Facilities SLA Report, detailing environmental equipment availability, SLA attainment, and reason for outages.
D-08.04	Quarterly	*Facilities Management Plan* Offeror must provide quarterly Facility service improvement report. Report changes and improvements to the facility or the maintenance of the facilities.
D-08.05	Annual	*Facilities Management Plan* Offeror must provide annual SSAE 16 audit reports for each datacenter facility being used to support the Commonwealth. The Audit Report for the EDC must be provided on the anniversary of the Audit Report described in Deliverable D-08.02.

Site Operations		
D-08.06	Effective Date + 60 days	*Facilities Management Plan* Offeror must present their assessment of the EDC monitoring and staffing changes/modification required to upgrade the facility to meet Commonwealth service level objectives. The assessment must include a roadmap and project plan to make any required monitoring and staffing modifications.
D-08.07	Effective Date + 90 days	*Facilities Management Plan* Present plan to address the assessment recommendations identified in the EDC monitoring, project plan and staffing report.
D-08.08	Daily, Monthly	*Facilities Management Plan* Offeror must provide daily and monthly SLA report(s), detailing environmental equipment availability, SLA attainment, and reason for outages.
D-08.09	Quarterly	*Facilities Management Plan* Offeror must provide quarterly site operations improvement report. Identify changes or improvements to the site operations that would assist the Offeror in meeting the agreed facility SLAs.

D-09 Security Risk and Vulnerability Assessment Report

The Offeror will execute a Baseline Security Risk and Vulnerability Assessment. The assessment report must include a roadmap and project plan to make any required security modifications prior to final transition of services.

Security Transition Activities		
D-09.01	Effective Date + 60 days	*Security Risk and Vulnerability Assessment Report* Offeror must execute a Baseline Security Risk and Vulnerability Assessment. The assessment must include a roadmap and project plan to make any required security modifications.
D-09.02	Effective Date + 90 days	*Security Risk and Vulnerability Assessment Report* Present results of the Security Risk and Vulnerability assessment along with a Roadmap and Project Plan to address the recommendation identified in the assessment.

D-10 Gap Analysis Report

The Offeror will execute a Data Center Gap Analysis. The analysis report must identify gaps in the current data centers and the Offeror's recommendations and corrective approach.

Gap Analysis Activities		
D-10.01	Effective Date + 120 days	*Gap Analysis Report* Offeror must execute a Data Center Gap Analysis. The analysis must include gaps identified and a roadmap and project plan to institute any recommendations and corrective actions.
D-10.02	Effective Date + 150 days	*Gap Analysis Report* Present results of the Data Center Gap Analysis along with a Roadmap and Project Plan to address the recommendations identified in the analysis.

D-11 Contract Management Plan

The Contract Management Plan will address management for the overall contract. The Contract Management Plan should describe the Offeror's plan to ensure it is adhering to the terms and conditions of the contract and providing the services/products that meet the requirements of the project. The Contract Management Plan must identify the activities to be performed or initiated to manage, track, amend, and close the contract. The Contract Management Plan must include but is not limited to: participants roles and responsibilities, task accomplishment plan, status reports, deliverable management, contact performance management, risk management, and contract closeout.

Contract Management Plan		
D-11.01	Effective Date + 45 days	*Contract Management Plan* Offeror must document its Contract Management approach, tool(s) and project plan.
D-11.02	Effective Date + 60 days	*Contract Management Plan* After review and approval from the Commonwealth, Offeror must review its Contract Management approach, tool(s) and project plan with Commonwealth stakeholders.

D-12 Schedule C.2 - Service Descriptions Initial Completion

Schedule C.2 (Service Descriptions) is a description of the Services that are orderable by the Commonwealth from the Catalog of Services contained within Schedule C.1. Schedule C.2 must include enough detail to allow an authorized Commonwealth employee to have a brief understanding of the service referenced within the document. A template has been provided as part of the executed Contract and is the basis for this deliverable.

Schedule C.2 – Service Descriptions Initial Completion		
D-12.01	Effective Date + 30 days	*Schedule C.2 – Service Descriptions Initial Completion* Contractor must document and provide to the Commonwealth, a completed Schedule C.2 containing all Services listed and priced within Schedule C.1 – Catalog of Services using the template included within Schedule C.2 of this Contract at the time of execution.

Deliverable Acceptance Criteria Matrix

This section is provided for the Offeror to understand the process the Commonwealth will use for acceptance of Deliverables/Milestones that are committed to in the RFP. The Matrix provided below is an example of the template that will be used to capture Deliverables/Milestones and other information related to the acceptance process.

It is critical to the success of the Data Center Computing Services project that the deliverable acceptance process is thorough and that any deficiencies are addressed as early as possible to minimize impacts to the Services. Designated Commonwealth working teams will be reviewing the Deliverables/Milestones throughout the phases of development. The Offeror will solicit input from the Commonwealth team members as the items are developed with the goal of understanding expectations in advance so as to obtain acceptance upon delivery. Feedback and suggestions received from the Commonwealth must be incorporated into the Deliverables/Milestones. The Commonwealth will identify the individuals authorized to provide formal Acceptance Approval / Nonconformance notification to the Offeror for the Deliverables/Milestones. The deliverable acceptance process will comply with the following guidelines and be formally documented in the Commonwealth Computing Procedures Manual (CCPM).

1. The Offeror will give written notice to the Commonwealth that a Deliverable / Milestone is complete.
2. A walk-through review of the Deliverable and/or Milestone will be scheduled by the Offeror seven (7) days following the issuance of the written notice to the Commonwealth. The purpose of the walk-through is to provide a forum for discussion and review of the Transition Deliverable / Milestone with the approver/s. If additional review, physical inspection, on-line access or backup information is required, the Commonwealth will notify the Offeror at this time.
3. The Commonwealth will provide the Offeror with notice that the Deliverable / Milestone is Accepted or notice of Noncompliance no later than seven (7) days after the walk-through, fourteen (14) days after notice of completion.
4. If the Commonwealth does not provide notice to the Offeror of their Acceptance or Nonconformance within fourteen (14) days of notice of completion, the Offeror will give the Commonwealth written notice that the request was not received and the Acceptance Review Period will be extended an additional seven (7) days.
5. The Enterprise Datacenter Services Transition Management Committee will review all Deliverable / Milestones which have not received written notice of Acceptance or Noncompliance within fourteen (14) days after notice of completion. The Enterprise Datacenter Services Transition Management Committee's goal is to determine and document the Commonwealth and Offeror actions necessary to complete the review minimizing any potential delays to the project and addressing any substantive issues.
6. For any Deliverables / Milestones which are found to be Noncompliant, the Offeror will address the nonconformity (and any other problems of which it has knowledge) and redeliver the item to the Commonwealth using the process outlined above.

The status of each Deliverable and any associated issues will be managed through a monthly deliverables review meeting between the Commonwealth and the Offeror. The objective of the meeting is to review the status of all deliverables, communicate deliverable owners and

deliverable recipients for upcoming deliverables, review rejected deliverables and remediation plans for those deliverables.

Example - Deliverable Acceptance Matrix

Reference #	Deliverable / Milestone Name	Due Date	Acceptance Criteria	Monthly Credit
D-01	Datacenter Architecture Plan and Roadmap		•	
D-02	Commonwealth Computing Procedures Manual (CCPM)		•	
D-03	Technology Architecture and Refresh Approach		•	
D-04	IT Service Continuity Architecture and Plan		•	
D-05	Transition Management Plan		•	
D-06	Agency Level DR Plan(s)		•	
D-07	Security Management Plan		•	
D-08	Facilities Management Plan		•	
D-09	Security Risk and Vulnerability Assessment Report		•	
D-10	Gap Analysis Report		•	
D-11	Contract Management Plan		•	
D-12	Service Descriptions Initial Completion		•	

SCHEDULE L

APPROVED SUBCONTRACTORS

IBM Corporation

International Business Machines Corp.
New Orchard Road,
Armonk, New York 10504
914-499-1900

Deloitte LLP

300 Corporate Center
Suite 601
Camp Hill, PA 17011-1762
717-695-5200

Acclaim Systems, Inc.

Rakesh Khetawat
110 E. Pennsylvania Blvd.
Feasterville, PA 19053
215-354-1422

American Personnel Managers & Consultants, Inc.

2226 Gettysburg Road
Camp Hill, PA 17011
717-303-0229

Credo Technology Solutions, Inc.

110 Sunset Avenue
Harrisburg, PA 17112
717-657-7017

Domino Technologies, Inc.

Governor's Plaza South - Building No. 3, Suite 334
2001 North Front Street #334
Harrisburg, PA 17102
717-730.6265
Mailing Address
6211 Lookout Drive
Mechanicsburg, PA 17050

e&e IT Consulting Services, Inc.

5026 Arthur Ave,
Mechanicsburg, PA 17050
717-975-1664

Info-Matrix Corporation

Brenda S. Orth
650 North 12th Street
Lemoyne, PA 17043
717-260-9860

Innovative Business Concepts, Inc.

Jennifer Briggs
209 Hamilton Street
Harrisburg, PA 17102
717-221-1125

PC Network, Inc.

PCN
The Philadelphia Building
1315 Walnut Street, Suite 1402
Philadelphia, PA 19107
267-236-0015

SCHEDULE M

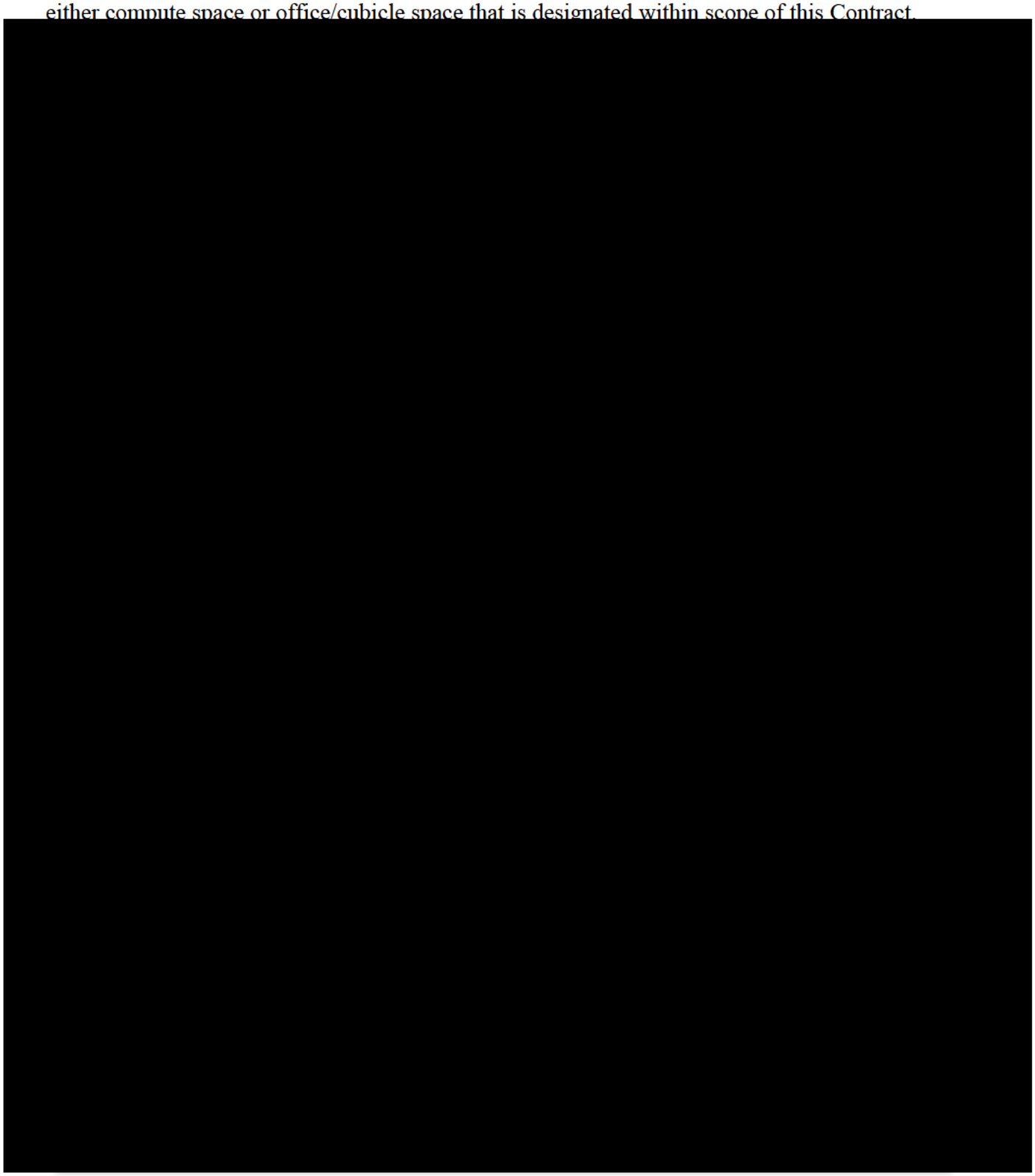
DETAILED TRANSITION PLAN

SCHEDULE N

ENTERPRISE DATA CENTER FLOOR PLAN

EDC Floor Plan

The following is the Floor Plan for 1 Technology Drive, Harrisburg, PA. The shaded areas are either compute space or office/cubicle space that is designated within scope of this Contract.



SCHEDULE O

COMMONWEALTH DATA CENTERS TO BE TRANSITIONED

[redacted]

Unisys Response to

Commonwealth of Pennsylvania

Office of Administration

Office for Information Technology

[redacted]

Request for Proposal (RFP)
RFP 6100022698

Technical Submittal

[redacted]

September 20, 2013

This proposal has been reproduced on recycled paper

J. Edward Coleman
Chairman & Chief Executive Officer

Unisys Corporation
801 Lakeview Drive
Blue Bell, PA 19422

Telephone
(215) 986-6100 (Office)

UNISYS

September 20, 2013

Bureau of IT Procurement
c/o Commonwealth Mail Processing Center
2 Technology Park (rear)
Attn: IT Procurement 506 Finance
Harrisburg, PA 17110
Attn: Janis Brown

RE: **BAFO Request for Proposal (RFP Number 6100022698) for the Commonwealth of Pennsylvania Data Center Computing Services**

Dear Ms. Brown:

Thank you for selecting Unisys to participate in the "Best and Final Offers" (BAFO) phase of the evaluation process. We reviewed the BAFO request and we are pleased to submit our improvements to our Technical, Cost, and SDB submittals.

Our two primary production Datacenters (Commonwealth's EDC and the Unisys Ashburn facility) were selected to enable High Availability and, by design, are less than 90 miles apart. We welcome the opportunity to better explain and clarify how the Unisys proposed Datacenter Model was designed to support High Availability configurations between two physical production Datacenters and easily supports Production Servers in one physical Datacenter and lower server environments (DEV and Test Servers) in the other physical Datacenter. **Please find the Unisys answers to the 2+ Datacenter Architecture BAFO questions in Tab 1.**

As part of Orals, the Commonwealth provided Unisys with written questions that were addressed during our presentation and asked a number of additional questions at the end of our Presentation. When analyzing and categorizing the types of questions asked, Unisys discovered that most of the questions were related to our proposed Security Offering.

Protecting citizen data has always been important to the Commonwealth. Security becomes even more important as the Commonwealth transitions to the proposed on-demand compute environment; quite simply the agencies must have the confidence in the security of the new environment to meet their diverse regulatory requirements such as CHRIA, FERPA, HIPAA/HITECH, IRS 1095, PCI and CJIS during transition, and steady state operations. The Unisys team understands this is fundamental to the success of the initiative and is committed to a successful transition and operation of the new environment.

We leverage our teaming partner - Deloitte's robust public sector security risk framework that integrates several regulatory requirements, as the foundation of our security management plan. This readily available catalog of rationalized regulatory requirements and controls will help us appropriately address the people, process and technology aspects of our security solution. **Please find the details on our Security improvements and clarifications in Tab 2.**

Also during the Orals, the Unisys Team received several questions around our x86 Technical Infrastructure. As a result, we have made several revisions and enhancements to our Technical Submittal focused on clarifying our x86 Technical Infrastructure offering. **Please find the details on our Technical Infrastructure improvements and clarifications in Tab 3.**

Finally, we proposed a small number of technical changes that improve both transition and operations while providing efficiencies. **A summary of major improvements are listed below and the details for all of our operational efficiencies are in Tab 4.**

- As part of an effort to continue to refine the Transition Plan and enable an earlier migration out of the DPH while limiting overall operational risk, the Unisys Team's overall timeline for Transition is now 18 months. The Unisys Team continues to plan to complete the EDC's Transition by Month 6 and now plans to complete the DPH migration by Month 12. If the new contract effective date is before December 31, 2013, the reduced DPH transition timeline will allow the Commonwealth to avoid a DPH contract extension.

- The Unisys Team refined the 2+ Data Center architecture approach by adjusting the functions provided by the Unisys Eagan data center and its network connectivity. This modification simplifies the planning and migration activities for the DPH and agency individual data centers during Transition while maintaining the flexibility to meet changing business needs.

Should you have any questions about this BAFO response or need additional information, please continue to contact Dean R. Shaner.

We appreciate this opportunity to provide improvements and clarification to our proposal in support of your mission.

Sincerely,

[redacted]

[redacted]. Edward Coleman
[redacted]Chairman and CEO

Table of Contents

Transmittal Letter

Table of Contents

1.0 BAFO Datacenter Questions 1-1

2.0 Security Offering Improvements 2-1

02b-UIS-CoPA-F.3.1.2 Network and Security Architecture

02c-UIS-CoPA-F.3.2.2.5 Security Management

02d-UIS-CoPA-F.3.2.4.6 Security and Firewall

Exhibit A–Attachment-Datacenter Security Management Plan Sample Plan

3.0 Technical Infrastructure 3-1

03b-UIS-CoPA-F.3.2.2.2 Infrastructure Architecture

4.0 Operational Efficiency Revisions 4-1

04b-UIS-CoPA-3.0_Work_Plan

04c-UIS-CoPA-2.0 Management Summary

04d-UIS-CoPA-F.3.3.2.1 Transition Program Management

04e-UIS-CoPA-A9-6100022698 - ScheMule M - Transition Plan

04f-UIS-CoPA-F.3.1.1 Multi Datacenter Environment

04g-UIS-CoPA-3.2.1.5.2 IT Service Continuity Architecture

04h-UIS-CoPA-F.3.2.4.2 Storage Management

04i-UIS-CoPA-F.3.2.4.7 Database Management Services

5.0 Appendix A Modifications 5-1

This page intentionally left blank.

1. BAFO Datacenter Questions

No.	BAFO Question
1	*Describe how Unisys's proposed 2+ Data Center Architecture will support a High Availability configuration between multiple physical data centers with equal parts of an application distributed between physical data centers?*

A key design feature of the Unisys Data Center Architecture is to support high availability configurations and applications running across multiple physical data centers. This design requires a set of fundamental components or capabilities to enable effective communications between applications and support movement of applications between sites, thus enabling the placement of applications on physical or virtual server workloads across multiple data centers. These components or capabilities are:

- **Location of Physical Data Centers**- Distance between data centers is a major consideration when architecting a high availability configuration. Separation of greater than 90 miles can cause latency problems which in turn can be expensive to remedy. Unisys strategically selected the [redacted] site to complement the EDC. Distance between these sites is 90 miles.
- **Storage** – In a high availability environment with applications divided between multiple data centers, a robust storage architecture must be deployed across the data centers to easily move data across application components. Furthermore, due to the tight coupling of many Commonwealth applications, the production, development, test, QA, or disaster recovery workloads will be no more than 90 miles apart between the EDC and Unisys [redacted] data centers after transition is completed. The short distance between the sites allows for large amounts of data to be replicated quickly between the applications so application fail-over and API calls can occur rapidly; this is a key architectural approach in any high availability environment for applications that are in clusters or in multiple data centers.

  Unisys will be supporting both IBM and EMC storage systems along with various replication products that are in the existing environment today supporting current application needs. Servers will be connected to storage systems through a Storage Area Network (SAN) allowing the servers to load their operating system and application components via the SAN, thereby allowing the servers to connect to any operating system or application workload whether production, development, test, QA, or disaster recovery; equally any sever can switch out a workload for another with automation scripting or manual intervention. All storage products will have the same architecture between EDC, Unisys [redacted] and Unisys [redacted]

- **Latency Elimination** - In high availability environments where applications are tightly coupled and distributed between two or more data centers, like the Commonwealth, latency elimination becomes critical, so intercommunication between the applications is not impacted. Upon completion of transition, the production, development, test, QA and disaster recovery workloads will be within 90 miles. Both data centers are essentially on an extended high speed low latency Ethernet LAN segment, much in the same way they are today between the EDC and the DPH. Being on a low latency link is critically important so that there is no disruption of API calls between application components in different data centers; the further the distance between distributed application components, the more likely there will be errors or a performance degradation.
- **Networking** – A logically flat, robust network architecture needs to be the same across sites to simplify rules and performance management of routers and LAN switches providing predictable performance characteristics between distributed applications. To facilitate this, Unisys will be utilizing Cisco networking products within the EDC, Unisys [redacted] and Unisys [redacted] Consequently, the way an application traverses a network in one data center will be the same as the other center(s), thereby eliminating conditions that may impact performance between applications in multiple centers.
- **Security** – A key component in any high availability environment is the security architecture and it must be robust to deal with the distributed nature of applications located across multiple centers. When locating application components across data centers, firewall provisioning and management is essential between sites so there are no inconsistencies between the sites. This is crucial to maintain adherence to security regulations such as HIPPA, FTI, CJIS, PCI, CHRIA and Commonwealth policies. For further information on the revised and enhanced Unisys Security Management Plan,please refer to Section 3.2.2.5.

  To facilitate this, Unisys will be standardizing on Juniper firewalls for the capability to create virtual firewalls, and ability to provision between sites and integrate with automation software for the self-provisioning of virtual server workloads between data centers. The value of Juniper firewalls is its policy management engine and virtual firewall capability to turn-up and down like firewalls in multiple data center in a high availability environment.

  As an additional security measure for applications between sites, Unisys will be deploying Imperva application firewalls along with McAfee Data Loss Protection appliances. These appliances will secure application workloads and communications between centers. Between the deployment of Juniper and Imperva firewalls, Unisys will be able to effectively manage and secure communications of applications across multiple data centers.

- **Load Balancing** – Splitting web and application servers between data centers for high availability requires load balancers that have geographic balancing capabilities; therefore, Unisys will be standardizing on F5 load balancers to manage and route

incoming requests for Windows, Linux, and AIX hosted applications that are located across multiple data centers.

- **Configuration Management Database** – High availability of applications across data centers is only possible with a properly populated Configuration Management Database (CMDB) that has the association of infrastructure components to application components so one can effectively manage the complexity of a distributed application architecture. The CMDB is critical to understanding the location of application components and how they are interrelated to the infrastructure, especially if the application is split between data centers. For this reason, a robust CMDB is needed to track the configuration of infrastructure and application components to assure they are properly configured and to aid in assuring successful API communications between applications as well as supporting application workload movement between clusters or data centers.

  In addition, automation software is highly dependent on the CMDB to provision and move workloads between applications in separate data centers. More importantly, if a change is taking place in one center it must be reflected in the other center(s); therefore, change impact management is critically important to be integrated into the CMDB so that it will alert you in the change process if a component needs to be changed in another center.

  To support the above configuration management activities, Unisys will be using BMC Atrium Discovery and Dependency Mapping (ADDM) product to auto discover application infrastructure components in the multiple data centers including their associated relationships. These Configuration Items (CI) will then be populated into the BMC Remedy Atrium CMDB that will be replicated to the Commonwealth's IT Service Management platform.

With the above in place as a foundation to place equal parts of an application in multiple data centers, we can now focus on how the servers will layer on top to facilitate high availability for applications between centers. The Commonwealth's applications run on either a physical or virtual host that are comprised of a variety of operating systems such as MVS, zVM, zOS, zLinux, OS2200, MCP, AIX, Linux, or Windows. To simplify the response, Unisys categorized these operating systems into four system types: Mainframe, AIX, Linux and Windows. Further we defined them as Virtual or Physical since there are differences. These systems enable an application to be split between multiple data centers as follows:

- **Mainframe Systems (MVS, zVM, zOS, zLinux, OS2200, and MCP)** – Upon successful transition Unisys will have placed mainframe systems across Unisys [redacted] and the EDC to host production, development, test, QA, and disaster recovery workloads. The initial configuration of the Unisys and IBM mainframes will be in an active/passive configuration. If a production workload is in the Unisys [redacted] data center and requires disaster recovery for an application, then the passive (disaster recovery) workload would be located in the EDC. The active environment will replicate data to the passive site where the two sites applications

components are kept in sync so, in the event that there is a disruption at the active site, the passive application workload can be turned up within a specified amount of time; optionally, the application can be configured to be active-active across the centers so that there is little delay in disruption of an application workload.

- **Virtual Hosts for AIX, Linux, and Windows** - Given that a significant number of Commonwealth's applications are tightly coupled and spread across multiple operating systems such as AIX, Linux, and Windows, it is architecturally important to consolidate them to a common hardware platform. Doing so when placing application workloads in separate datacenters simplifies management, provisioning and the movement of application workloads from one cluster within or between sites. To overcome this architectural challenge there is no other provider in the marketplace that supports mixed workloads on one common consolidated platform for AIX, iSeries, Linux, and Windows other than IBM Flex Systems. Therefore IBM Flex Systems is the standard platform that Unisys will utilize in all centers for all AIX, iSeries, Linux, and Windows environments. IBM Flex Systems are not constrained by a single fixed storage vendor that then limits scale and cost efficiency; in fact, IBM Flex Systems allow for the integration of a variety of industry leading storage systems, including existing storage systems that are currently hosting applications. Unisys approach mitigates a costly storage migration to new storage platforms and minimizes downtime. To learn more about IBM Flex Systems please refer to Section F 3.2.2.2.

  The IBM Flex Systems virtual servers will connect to the SAN and will load their operating systems and application components from the storage environment via the SAN. This will also allow a virtual server to switch out an application workload between production, development, test, QA, or disaster recovery is the ability to automatically failover the workloads.

  Key to placing equal parts of an application split between physical data centers is being able to move them from cluster to cluster or across datacenters. IBM Flex Systems using the Flex Systems Manager, in conjunction with VMware vCenter and other management tools has the ability to automate the movement of mixed workloads and simplifying the failover process for applications between clusters or across datacenters. Another advantage of the IBM Flex Systems is being able to balance or move application workloads between data centers; consequently, you can readily move production, development, test, or QA workloads between data centers to support changes in business needs or to support various usage patterns.

- **Physical AIX, Linux, and Windows** – The only difference in the AIX and Wintel physical server environment over the virtual environment is that it will be allocated a complete server within the IBM Flex Systems Blade Chassis. All other attributes are the same as indicated above for a virtual server.

The Unisys proposed 2+ Data Center Architecture will not only support a high availability configuration between multiple physical data centers with equal parts of an application

distributed between physical data centers, but also minimize any potential application performance issues when moving the Commonwealth's tightly coupled applications to a new center by limiting the distance separation between the applications to 90 miles, thereby minimizing any potential chance for latency propagation. The further the distance between application nodes, the greater the performance impact due to network latency delay between sites.

Network latency can have a large impact on the performance of application APIs, because at times application components can have timing sequences in their code waiting for the return of information within a given amount of time. If the information isn't received within the expected duration, a time out error will occur impacting the performance and operation of the application. So when splitting applications between two centers for high availability, you want to keep them as close together as possible to achieve the least amount of latency propagation to eliminate any application performance issues. This is exactly what the Unisys solution does, thereby, saving the Commonwealth costly application testing efforts and rewrites in application code.

No.	*BAFO Question*
2	*Describe how Unisys's proposed 2+ Data Center Architecture will support a configuration where the production environment is in one physical datacenter and the lower environments (e.g. development, system test, user acceptance testing) are in another physical datacenter and the lower environments are designated as the DR solution for the production environment. In support of this information, please include details addressing the following:* *a. Identify each datacenter that will be used in the 2+ Data Center Architecture and the Commonwealth workload that will be supported in each datacenter.* *b. In addition to the datacenters that will support the Commonwealth as identified in Unisys's proposal, explain how Unisys will leverage capacity from the other datacenter resources within its provider network if required.*

To support the Commonwealth's mission critical applications, it is essential that the robust architecture that Unisys provides the Commonwealth has the ability to swap out environments within and across multiple data centers. Therefore in a mainframe or open systems environment to accomplish the swap a of production environment in one location with lower environments in another center for disaster recovery Unisys will store all server and application workloads as images on the SAN. By storing images and booting operating systems from the SAN we create a many-to-one relationship of workload images to servers where one server can pull an image from a pool, therefore, allowing the swap out of a lower environment for a production environment in the event of a disaster. In fact the process of swapping workloads out can be automated if desired.

To enable this functionality to take place you need the same robust architecture across centers. Therefore that is an integral part of our architectural design. The robust architecture that Unisys will use is described in the answer above for high availability for

applications in separate data centers. Within this architecture to execute the swap out of environments between production and lower environments for disaster recovery we will use automation scripts in the mainframe environment, and for open systems the IBM Flex Systems Manager, in conjunction with VMware vCenter and other management tools, which can have automation scripts applied. Furthermore a benefit of the IBM Flex Systems over its competition is it has the ability to swap out or move mixed workloads, meaning AIX, ISeries, Linux, and Windows as one unit within or across centers, which is critically important when you have tightly coupled applications. The core of our architecture was designed from the beginning to swap and move workloads and environments within and across data centers.

Unisys will use three data centers in the proposed 2+ Data Center Architecture, the EDC, Unisys [redacted] and Unisys [redacted] Within any of these three centers the Commonwealth can place production, development, test, QA, or disaster recovery workloads; as well Capacity-on-Demand services will be available within all three centers.

To complement these three centers Unisys is extending to the Commonwealth services from our provider network from IBM, Deloitte, and Microsoft. Between these three providers coupled with Unisys services there is an extensive amount of services and resources that we will bring to the Commonwealth. For a sample of these services please refer to **Figure 1-1**.

Service Type	EDC	Unisys Data Centers	IBM Data Centers	Microsoft Azure	Deloitte
Unisys Mainframe	●	●			
IBM Mainframe	●	●	●		
AIX	●	●	●		
Windows	●	●	●	●	
Linux	●	●	●	●	
zLinux	●	●	●		
Storage	●	●	●		
Microsoft SQL	●	●	●	●	●
Oracle	●	●	●	●	●
SAP Services			●		●
Security Services	●	●	●		●

Figure 1-1. Platforms and Services by Provider

Existing agency workload placement will be between the EDC and Unisys [redacted] to mitigate risk and performance issues given the Commonwealth's tightly coupled applications. Unisys [redacted] and our providers' network will be available for additional

services for Capacity-on-Demand and disaster recovery workloads. For recommended agency mapping of workloads refer to **Figure 1-2**. During transition planning, workloads can be re-located to another center if desired, given our architecture fully supports the movement of workloads between centers as described above.

Agency	EDC	Unisys [redacted]	Unisys [redacted]
Aging			
Agriculture			
Banking and Security Commission			
Civil Service Commission			
Corrections			
DCED			
DCNR			
Education			
Environmental Protection			
Ethics			
General Counsel			
General Services			
Governor's Office			
Health			
IES			
Inspector General			
Insurance			
Labor and Industry			
Liquor Control Board			
Lieutenant Governor			
Military and Veterans Affairs			
Milk Marketing Board			
Office of Administration			
Office of Budget			
Patient Safety Authority			
PCCD			
PEMA			
Pennvest			
PHMC			
Probation and Parole			
Public Welfare			
PUC			
Revenue			
State			
State Police			
STEB			
Transportation			

• Production • Test • Development • Capacity On Demand • Disaster Recovery • Future Disaster Recovery

Figure 1-2. Initial Commonwealth Workload Recommendations

This page intentionally left blank.

2. Security Offering Improvements

Security Offering Clarification

As part of Orals, the Commonwealth provided Unisys with written questions that Unisys responded to in writing and also addressed during our presentation. In addition the Commonwealth asked a number of additional questions at the end of our Orals Presentation. When analyzing and categorizing the types of questions asked, Unisys discovered that most of the questions were related to our Security Offering or our x86 Technical Infrastructure.

As a result, we have made significant enhancements to our Technical Submittal focused on improving and clarifying our Security and x86 offerings.

In this section, the Unisys Team has refined the following Security and Network sections to clarify the security services which are used to support establishing, implementing, and maintaining functions to comply with the appropriate Commonwealth security guidelines, including CHRIA, OA/OIT guidelines and ITBs; Agency security requirements; and federal and industry guidelines and regulations (HIPPA/HITECH, FTI, CJIS, and PCI). In addition, a new Sample Security Management Plan has been included. This sample document covers the full format of the plan and is now specific to the security needs of the Commonwealth.

Our revised responses for the identified Requirements in the Schedules or Sections listed below are included in this tab.

Tab	Schedule or Section	Requirements
2	Schedule F Section 3.1.2 Network and Security Architecture	1A, 2A, 4A, 5A, 6A, 6B, 7A
2	Schedule F Section 3.2.2.5 Security Management	Introduction, 1, 2 (A,B,C),4A, 6A, 7A
2	Schedule F Section 3.2.4.6 Security and Firewall	Introduction, 1B, 1D, 1E, 3A, 3C, 4A, 5, 6A, 6B, 6D, 6E, 6F

This page intentionally left blank.

3.1.2 Network and Security Architecture

Secure and robust network connections are critical to the overall data center architecture. Connections between the data centers and access to the Commonwealth's network must be planned, established, and tested prior to the transitioning of Services. All Offeror data centers and locations must coordinate connections between the Offeror's network and the Commonwealth's fiber network (COPANET).

Reference Documentation

Exhibit A - Commonwealth Network Environment

Exhibit P – Enterprise Internet Bandwidth Utilization

	Requirements	Describe Compliance
1.	All proposed datacenter locations will connect to and provide access from COPANET.	Offeror must describe its approach to connect to COPANET.
2.	Dual network termination points to connect to COPANET.	Offeror must describe its networking capability and the ability to support dual termination points in the proposed datacenters environments.
3.	Provide network security via firewall and security devices.	Offeror must describe its network security and access control solution.
4.	All proposed Offeror's datacenter facilities will have secure Internet access capabilities. Internet access must provide virus and intrusion protection systems with reporting capabilities.	Offeror must describe its approach to providing secure access from Commonwealth authorized users via the Internet. The Offeror must describe its approach to providing virus and intrusion protection and reporting.
5.	Multiple security zones must be configured within each datacenter to support specific agency requirements. For example: access, web, application, and data zones. The specific configuration and number of individual zones may be different per agency and application.	Offeror must describe its ability to support the configuration of multiple security zones within its datacenter architecture.

6.	Secure connections are required for traffic that may traverse between Datacenters and between Datacenters and Commonwealth. Encryption shall be a minimum of 128-bit and must be FIPS 140-2 certified to meet Criminal Justice Information Services (CJIS) requirements. (Refer to Pennsylvania State Police (PSP) Summary of CJIS Requirements and CJIS Security Policy.)	Offeror must describe its ability to provide secure network connectivity that meets the standards outlined in the requirement.
7.	Remote access to datacenters supporting CJIS systems must meet minimum security requirements identified in CJIS Security Policy. These requirements include but are not limited to identifying remote user's identity, IP address and connection must be FIPS 140-2 certified with a minimum of 128-bit encryption.	Offeror must describe its ability to comply with the security policies described in this requirement,

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

1 COPANET

1.A All proposed datacenter locations will connect to and provide access from COPANET.

Offeror must describe its approach to connect to COPANET.

As **Figure 3.1.2-1** below illustrates, the Unisys Team will be meeting the current COPANET connectivity requirements by connecting locally at [redacted] via 10 Gb Ethernet and via 1 x 1 Gb Ethernet connections to an alternate COPANET location from the [redacted] data center. Should direct connectivity to the Verizon PIP network be required, Unisys can terminate Commonwealth provided PIP circuits on Unisys owned and managed equipment at the Unisys Data Centers.

In addition to the [redacted] two new data centers will be utilized – [redacted] and [redacted]. In the [redacted] a new connection to the existing COPANET node will be built using two 10 Gb fiber connections within the [redacted]. Since the distance to connect [redacted] to COPANET is so short, these connections do not require a WAN circuit to be installed, thus saving cost. The [redacted] connectivity is shown on the left diagram of **Figure 3.1.2-1** below:

On the right side of the **Figure 3.1.2-1** above, the COPANET connection to [redacted] is shown. Based on predicted future usage, the [redacted] Data Center will be connected to COPANET via a 1 Gb circuit. To prevent a single point of failure in the connection to COPANET, the COPANET circuit from [redacted] will terminate in a different physical facility than the connection from the [redacted] The locations being considered to terminate the Data Center circuit are [redacted] or [redacted].

It should be noted that the circled number 4 in **Figure 3.1.2-1** indicates a logical circuit number assigned to the circuit being proposed for the Commonwealth, which will be explained in more detail in the next section. The point-to-point circuit4 above will terminate on [redacted] routers in [redacted]. On the COPANET side, the circuits will terminate on existing [redacted] switch line cards, which currently form the edge connection point into COPANET.

In the [redacted] the two 10 Gb fiber connections will terminate directly on the new [redacted] core switches, while the other end of the connection will also terminate on existing [redacted] switch line cards. Unisys will be providing the necessary equipment to terminate these 10 Gb connections. The Commonwealth will be required to provide ports or line card availability on the COPANET nodes (PEs). Any additional PE equipment (line cards or SFPs) would be provided by Unisys.

2 Dual network termination points to connect to COPANET

2.A Offeror must describe its networking capability and the ability to support dual termination points in the proposed datacenters environments.

The new Commonwealth network's proposed design will have the following characteristics:

- The use of the current [redacted] Data Center;
- A [redacted] Data Center;
- A [redacted] Data Center;
- An [redacted] Data Center, if the Commonwealth elects to continue with the current [redacted] approach (using existing the existing Verizon PIP connectivity);
- Diverse connectivity into existing COPANET nodes from the [redacted] and [redacted] (described in detail in the previous section);
- Internet VPN tunnels (site to site) from the [redacted] and [redacted] to [redacted] to

support Capacity on Demand and disaster recovery services;

- Internet access for Unisys employees and Unisys 3rd parties will be provided at the [redacted] using the site's current Internet access, and [redacted] to support Unisys management and tools traffic;
- The Unisys network design addresses both bandwidth and latency concerns;
- The Unisys network design includes both circuit and data center redundancy.

Figure 3.1.2-2 below shows an overview of the 4 new circuits that will be put in place to support the network design. The numbers are grouped together by color, with numbers 1 and 2 (yellow) used for high-speed backbone data center connectivity, 3 (green) for Unisys Internet tools connectivity, and 4 (purple) for COPANET connectivity. The dashed green lines represent the encrypted VPN tunnels from the [redacted] and [redacted] to Unisys [redacted]

Figure 3.1.2-2 – WAN Overview

At the heart of the new design is a high speed, fully redundant, low latency wide area network (WAN). This new backbone WAN will connect the [redacted] and the [redacted] sites together using two separate 10 Gb redundant paths between each site. Using standard [redacted] WAN load balancing across the links (per-destination load balancing), up to 20 Gb of bandwidth will be available between the [redacted] and [redacted]. The [redacted] site will be connected using Internet VPN tunnels to the [redacted] and [redacted].

Figure 3.1.2-3 is a diagram that breaks out the 2 circuits that will be installed in support of this new backbone WAN network. The Unisys Team is confident this WAN design is the appropriate network solution to support the data transformation needs of the Commonwealth, given the amount of data that will likely need to traverse the network from the existing Commonwealth Data Centers to the new Unisys Data Centers. After the data center transition and transformation phases of the project are completed, a bandwidth analysis will be done to evaluate the circuit bandwidth. It

is anticipated that less bandwidth will be needed in the steady state environment than during the transition and transformation stages.

Figure 3.1.2-3 – Data Center Connectivity

As shown in the **Figure 3.1.2-3** above, the fiber acquired from the telecommunication provider(s) will terminate directly on core switches, allowing the deployment of technology between the and . Using a Layer 2 multipath network will be built without the Spanning Tree Protocol (STP) being deployed. This new network design is particularly suitable for large virtualization deployments, private clouds, and high-performance computing environments. When deployed across multiple creates a flat data center switching fabric with:

- High switching capacity
- High cross-sectional bandwidth
- Low predictable latency

To address specific latency concerns regarding physical distance between the data centers, point-to-point telecommunication circuits will be deployed. Based on the fact that it takes approximately 1 millisecond (ms) for light to travel 100 miles, Unisys is estimating that round trip latency between the and sites should be less than 5ms. The reason the latency is not less than 5ms is because additional latency (i.e., non-distance related) is added by the physical telecommunication equipment at either end of the circuit. Point-to-point circuits offer the lowest latency versus traditional network "cloud" or "star" topologies, as the distance the light needs to travel is considerably less.

In addition to (mentioned above) for steady state operations between the and Data Centers, the new Commonwealth network will also be utilizing technology during the transition in situations where the same IP subnets need to be maintained. Unisys experience is that IP addresses often need to be maintained either permanently or temporarily because of the number of servers being moved (servers in the same IP subnet cannot all be moved or relocated at the same time) or the hard coding of IP addresses in applications not allowing new IP addresses to be assigned. In either case, and platforms is a technology that significantly simplifies extending Layer 2 networks across distributed data centers without getting into complicated and unreliable tunneling technologies that were used in the past.

Unisys successfully utilized technology recently on a similarly sized project when moving a large production data center between (approximately 400 miles)

and where no IP readdressing was allowed by our customer. In that project it was necessary to maintain the same Layer 2 subnet across geographically large distances (high latency environment) and [redacted] performed as designed. When all the servers were migrated successfully, [redacted] was turned off.

Figure 3.1.2-4 – [redacted] Overview

As **Figure 3.1.2-4** above shows, [redacted] provides the Commonwealth with the ability to deploy virtual computing resources and clusters across geographically distributed data centers, delivering:

- Transparent workload mobility
- Business resiliency
- Superior computing resource efficiencies

At the [redacted] and [redacted] locations, a completely new [redacted] LAN network will be built for the Commonwealth using state of the art [redacted] devices at the core, distribution, and access layers. Servers will have the ability to be connected to the network in either 10 Gb, 1 Gb, or 100 Mb configurations, with the network itself supporting high availability redundant uplinks, as shown in **Figure 3.1.2-5** above.

At the [redacted] the new [redacted] LAN will also connect to the existing [redacted] core network. By connecting the new [redacted] equipment in the [redacted] to the existing [redacted] equipment the Commonwealth will leverage the benefits of using existing infrastructure to reduce costs, as well as introducing new technology to significantly update the network with the latest equipment. The new [redacted] network for our data centers will include [redacted] network ports and [redacted] network ports.

Figure 3.1.2-6 below shows a more detailed LAN design for the [redacted] and [redacted] Data Centers.

Figure 3.1.2-6 – LAN Detail

4 Secure Internet access

4.A All proposed Offeror's datacenter facilities will have secure Internet access capabilities.

Offeror must describe its approach to providing secure access from Commonwealth authorized users via the Internet.

The VPN clients enable secure Internet access capabilities for Unisys employees and Unisys 3rd parties. The Internet bandwidth Unisys is installing at will be used for Unisys specific Internet facing management tools, such as Unisys understands that the current Internet facing Commonwealth servers that are running today are going over Verizon managed circuits and that this solution will remain unchanged. The current Verizon management and support of the Commonwealth's VPN firewalls will also remain unchanged.

will be connected to the Commonwealth networks using Internet VPN tunnels from th and as shown in the following figure. These tunnels will terminate on FIPS 140-2 complaint network infrastructure in each site.

New Internet bandwidth of will be provided at , as shown in **Figure 3.1.2-7** below. Existing Internet connectivity is already provided out of the and sites. The and sites can quickly be upgraded to , if necessary.

Figure 3.1.2-7 – Internet Connectivity

5 Security Zones

5.A Multiple security zones must be configured within each datacenter to support specific agency requirements. For example: access, web, application, and data zones. The specific configuration and number of individual zones may be different per agency and application.

Offeror must describe its ability to support the configuration of multiple security zones within its datacenter architecture.

The Commonwealth network will be protected through a combination of network and security devices from several "best in class" vendors. The firewall vendor will be [redacted] The [redacted] devices will consist of a combination of devices. Protecting the [redacted] will be [redacted] firewalls; protecting the front end Internet connections will be another set of [redacted] firewalls. The enterprise [redacted] firewalls will also have built in IPS sensors.

The [redacted] box is designed around the concept of multiple security zones. The [redacted] device supports various types of security zones, with the understanding that different agencies may have different requirements. From a Unisys perspective, security zones represent virtual sections of the network, segmented into logical areas. Security zones can be assigned to a physical interface or to a virtual system. When assigned to a virtual system, multiple zones can share a single physical interface.

Figure 3.1.2-8 – Security Zones

Following the multi-zone network architecture, focused on Web, Application, and Database zones, presented above in **Figure 3.1.2-8**, [redacted] offers comprehensive, flexible, and robust security solutions that are ideally tailored for the requirements of the Commonwealth's new data centers. Unisys understands the Commonwealth's need for agencies and applications to be separated with firewalls and the [redacted] enterprise solution best meets this need.

[redacted] offers an unparalleled combination of features addressing these fundamental requirements:

- **Scale:** [redacted] solutions offer the processing scalability required to combat today's sophisticated threats. With the [redacted] offers firewalls that scale, both in terms of throughput and in the number of concurrent sessions, so they can accommodate the intensive security and bandwidth requirements of the next-generation data center.
- **Fabric architecture support:** [redacted] provides switches for fabric architectures, and is leading the way in delivering cohesive security integration in these environments. The [redacted] product line is designed to work with the scalable [redacted] fabric, ensuring optimal flexibility, scalability, and security in these emerging environments.
- **Visibility:** [redacted] security solutions can incorporate the required context, in real time, to provide effective, continuous policy enforcement. With [redacted] provides a deep understanding and visibility into application behaviors and weaknesses to prevent application-borne threats that are otherwise difficult to detect, let alone stop. In addition, [redacted] allows organizations to integrate user identities into their security policies. [redacted] also offers hypervisor integration that enables security teams to incorporate visibility into virtualized components in their security mechanisms.

- **Intelligent enforcement:** Finally, [redacted] offers solutions that can be deployed both on physical devices and in the hypervisor, enabling policy management and enforcement across the entire next-generation data center. As result, organizations realize stronger overall security, and security teams can implement faster configuration changes and reduce the errors that can create security exposures.

6 Secure Network Connectivity

6.A Secure connections are required for traffic that may traverse between Datacenters and between Datacenters and Commonwealth.

The requirement for secure connections is addressed through the use of dedicated point-to-point private connections with appropriate access and routing controls. If the security requirements of the Commonwealth dictate, Unisys will encrypt selected traffic between the data centers using the FIPS compliant [redacted] firewalls and additionally offers the Unisys [redacted] product as an optional Enterprise Services Catalog item to provide a more secure connection if selected. All Commonwealth agency to agency traffic will be encrypted, where required, using the [redacted] Firewalls with 128 bit encryption or higher. The VPN tunnels to [redacted] are established using FIPS140-2 compliant infrastructure.

6.B Encryption shall be a minimum of 128-bit and must be FIPS 140-2 certified to meet Criminal Justice Information Services (CJIS) requirements. (Refer to Pennsylvania State Police (PSP) Summary of CJIS Requirements and CJIS Security Policy.)

Offeror must describe its ability to provide secure network connectivity that meets the standards outlined in the requirement.

Unisys will coordinate with the Commonwealth as part of transition in determining the necessary encryption requirements, like PSP's CJIS Requirements and CJIS Security Policies. Where encryption is required, our solution will provide a minimum of 128-bit encryption that meets FIPS 140-2 certification and meets CJIS requirements. FIPS compliant [redacted] firewalls are capable of 128 bit encryption or higher. Beyond meeting this specific requirement for FIPS 14.2 certified 128bit encryption, Unisys is offering the additional protection of our [redacted] product as an option. Where necessary, Unisys will provide tunnel/VPN termination points for all traffic coming in over the Internet. The tunnels will be able to support 128 bit encryption or higher. These tunnels will terminate on the [redacted] equipment.

7 Remote Access

7.A Remote access to datacenters supporting CJIS systems must meet minimum security requirements identified in CJIS Security Policy. These requirements include but are not limited to identifying remote user's identity, IP address and connection must be FIPS 140-2 certified with a minimum of 128-bit encryption.

Offeror must describe its ability to comply with the security policies described in this requirement.

The Unisys Team understands the importance of protecting data and managing remote access to the Commonwealth systems, especially those systems supporting CJIS and CHRIA controlled data.

The Unisys solution includes an architecture for remote access for system administration of the Commonwealth systems which includes FIPS 140-2 validated VPN infrastructure using a minimum of 128-bit encryption, two factor authentication, role based authentication and tools privilege access, as well as privileged user access control and password vaults. Each of the components within this architecture will be connected with our logging and security infrastructure to support identifying remote user identities, IP addresses and privileged user activity. By using this remote administration architecture, the Unisys Team provides a secure access method to support the Commonwealth's environment and meet the requirements of the Commonwealth policies and applicable regulations including CJIS, FTI, HIPPA/HITECH, and PCI.

Figure 3.1.2-9 is an example of the remote administration access architecture.

Figure 3.1.2-9 – Security Zones

3.2.2.5 Security Management

The Security Management service must ensure the confidentiality, integrity and availability of Commonwealth information and infrastructure systems. All support and implementation activities must be conducted in accordance with, but not limited to, leading industry and Commonwealth standards, which include, but are not limited to, ISO 27001:2005 and ISO 27002:2005. The Offeror must support all related system audits at the Offeror's expense. The Offeror must maintain current security ISO 27001, ISO 9001 and ISO/IEC 20000 certifications.

The Offeror must comply with Commonwealth IT policies and directives as well as federal and Commonwealth laws, regulations and policies, including but not limited to the Criminal History Record Information Act (CHRIA), Health Insurance Portability and Accountability Act (HIPAA), Criminal Justice Information Services (CJIS) regulations, The United States Social Security Administration (SSA)regulations, IRS (Internal Revenue Service) Publications, Commonwealth Information Technology Bulletins (ITBs) and the Payment Card Industry (PCI) standards. The Offeror must work with each agency to understand and ensure compliance with all laws, regulations, and policies as they pertain to each individual agency.

Reference Documentation

Exhibit J.1 through J.3 - Commonwealth Security and Compliance Requirements

Exhibit G.6 - PSP - CJIS Security Policy

Exhibit G.9 - PSP – CCHRI

Exhibit G.7 - PSP - Summary of CJIS Requirements

Exhibit G.12 - PSP - CHRIA Handbook

	Requirements	Describe Compliance
1.	Develop an annual Security Management Plan.	Offeror must describe its approach to Security Management and provide a sample of a Security Management Plan. Highlight how stated security objectives align with Commonwealth business goals, IT policies, and regulatory requirements.
2.	Deploy complement of network security	Offeror must describe its proposed

	systems. Implement at minimum: spam filtering, anti-virus, malware protection, firewall (web, application), intrusion prevention and detection, web content filtering, virtual private network, and data loss prevention systems.	solution including the following: • Processes and Procedures • Tools / Applications • End User Reports o Standard o Custom • Escalation Procedures Offeror must describe its prior experience relative to providing datacenter management and support of CJIS, CCHRI, HIPAA and PCI systems.
3.	Perform quarterly (at the Offeror's expense) Vulnerability Analyses (VA) and penetration testing to identify new or emerging information security threats. Perform penetration testing (at the Offeror's expense) and present the results of each VA on a quarterly basis. Should exposures be identified, plan and remediate the exposure in accordance with Commonwealth IT policy guidelines. Report results to the Commonwealth within the time set out in an applicable SLA. The above requirement will be for all systems/subsystems that the Offeror is responsible for including managed servers/virtual servers, network devices, security devices including , but not limited to, the following: • Performing web application firewall administration and securing web applications behind it. • Ensuring and maintaining PCI level 1 compliance.	Offeror must describe its capabilities and approach to performing vulnerability analysis and penetrating testing on a quarterly basis. Provide sample reports for each.

	• Implementing DLP for the data center server assets to avoid a breach. • Implementing Database Firewall to secure database assets from breach.	
4.	Review network and other security logs for evidence of attacks. Utilize enterprise grade intrusion detection tool(s) to systematically identify, stop, and report security threats. Produce a monthly Security Log Analysis as part of the monthly status reports as described in RFP section IV-5 Reports and Project Control.	Offeror must describe its solution and approach.
5.	Apply operating system and other security patches. Implement a Patch Management Program to ensure the timely application of security updates on all infrastructure platforms in accordance with Commonwealth IT policy guidelines. The Patch Management Program must adhere to the Change Management process that includes Commonwealth approvals.	Offeror must describe its proposed Patch Management program.
6.	Restrict physical access to all network systems and equipment with biometric or other second factor access control systems.	Offeror must describe solution and approach to meet this requirement.
7.	Restrict access to all data in the Commonwealth network infrastructure. Restrict and control all data access right, groups and special permissions based on the data security program designed by the	Offeror must describe solution and approach to meet this requirement.

	Commonwealth security team and/or specified by the agencies. Access level changes and exceptions will be executed only when approved paperwork is complete and approved. A file of all access changes will be maintained by the Offeror for audit purposes. Offeror must support Commonwealth initiated security audits.	
8.	Evaluate the security standing of network-connected subcontractors. Conduct information security audits of prominent subcontractors on an annual basis.	Offeror must describe solution and approach to meet this requirement.
Continual Service Improvement		
9.	Reduce service risks.	Relative to the service in question, Offeror must provide examples of previous Offeror initiatives aimed at eliminating or mitigating service risks.
10.	Improve service quality.	Offeror must provide examples of previous Offeror initiatives aimed at improving service quality.
11.	Improve client satisfaction.	Offeror must provide examples of previous Offeror initiatives aimed at continually improving client satisfaction.
12.	Provide service transparency.	Offeror must provide examples of previous Offeror initiatives aimed at providing service transparency; in particular, visibility into the service execution process.
13.	Ensure service sustainability.	Offeror must provide examples of previous Offeror initiatives aimed at ensuring service sustainability; in

		particular, efforts targeted at cost containment and cost reductions.
14.	Improve/reduce cost of service.	Offeror will provide examples of Security Management initiatives that have been implemented or can be utilized to achieve reduced costs of Services and to meet or exceeded ROI (Return on Investment) analysis projections.

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

Introduction

We understand that maintaining the confidentiality, integrity and availability of citizen data has always been important to the Commonwealth. Security becomes vital as the Commonwealth transitions to the proposed on-demand compute environment and the agencies must have the confidence in the security of the new datacenter to meet their diverse regulatory requirements including CHRIA, FERPA, HIPAA/HITECH, IRS 1095, PCI and CJIS during transition, and ongoing operations. The Unisys team understands this is fundamental to the success of the initiative and is committed to a successful transition and operation of the new environment.

Consequently, we take a holistic approach to security. We leverage our teaming partner - Deloitte's robust public sector security risk framework that integrates several regulatory requirements, as the foundation of our security management plan. This readily available catalog of rationalized regulatory requirements and controls (the security risk framework) will help us appropriately address the people, process and technology aspects of our security solution.

As illustrated in **Figure 3.2.2.5-1**, the Commonwealth ITBs, policies and agency regulatory requirements drive the Security Management Plan, which in turn becomes the implementation blueprint of our datacenter security solution.

Figure 3.2.2.5-1 – A Holistic Datacenter Security Solution Driven by Security Regulations

The Unisys Team will work with each agency to understand their compliance requirements and use our security management plan to define, establish, implement and monitor appropriate safeguards. The Unisys team's security functions will be led by Michael Sheketoff who brings more than 38 years of technical and management experience.

To better support the various objectives of the Commonwealth, the Unisys security team's security function will be organized as depicted in **Figure 3.2.2.5-2**. The figure below also includes the key responsibilities of our security functions.

Figure 3.2.2.5-2 – Unisys Team's Security Functions and Key Responsibilities

Our process begins with establishing the Security Management Plan (Initial Security Plan). The compute environment's security management plan is driven by Deloitte's demonstrated public sector security framework - containing over 3,500 individual regulatory requirements mapped to almost 300 unique integrated requirements that include NIST SP800-53 rev4, CJIS v5.1, CHRIA, HIPAA/HITECH, PCI DSS v2/3, SSA and IRS 1075 rev8-2010. This framework is flexible to add additional controls and regulations as agencies face the need to comply with new regulations and controls.

During transition we use the security risk framework as the foundation, validate the agency requirements, systems security architecture and classify data, and develop and establish the security management plan. The initial security plan, established prior to the start of data center transition will provide the guiding principles (policies and standards) to establish safeguards, maintain a Personally Identifiable Information (PII) inventory and an IT asset inventory, driven by applicable key regulatory requirements.

Using the security management plan as the blueprint, the Unisys security solution is designed - taking in to consideration the people, process and technology. The solution is implemented consistently across the data centers. We have explained our security team's role in supporting datacenter transition as part of Section *3.3.2.2 Security Transition Activities* of this RFP Response. In addition,we have described the security approach to maintain ongoing compliance of the datacenter and safeguard Commonwealth data in section 3.2.4.6 of this RFP response. In addition, the Unisys team uses appropriate encryption solutions to encrypt data at rest and establish segregated network zones to

maintain a multi-layered defense-in-depth approach to safeguard Commonwealth data.

The Unisys team brings in leading industry solutions, to maintain a defense-in-depth security solution, and uses centralized audit log monitoring to safeguard Commonwealth's data and systems. We have illustrated our security technology stack and processes involved in audit log analysis to detect and report security incidents in Figure 3.2.2.5-3 below.

Figure 3.2.2.5-3 – Unisys Team's Security Technology Stack and Audit Log Monitoring Process

Additionally, we implement and operate the security technologies using processes rooted in the ITIL framework. The security governance is carried out with transparency – by sharing the alerts, risks and issues with the Commonwealth's Chief Information Security Officer (CISO) and agency security officers.

Our approach to meet the Commonwealth's *3.2.2.5 Security Management* requirements is detailed below.

1 Security Management Plan, Sample (example)

Develop an annual Security Management Plan. Offeror must describe its approach to Security Management. Provide a sample of a Security Management Plan. Highlight how stated security objectives align with Commonwealth business goals, IT policies, and regulatory requirements.

The Unisys team understands the importance of information security and regulations/standards mandated through the Commonwealth Information Technology Bulletins (ITBs), Commonwealth agency standards/polcies and Federal agencies. The Unisys team has envisioned a six step approach to establish a risk aware data center that

addresses several regulatory requirements such as:

- Health Insurance Portability and Accountability Act (HIPAA)
- Criminal Justice Information Services (CJIS) regulations
- The United States Social Security Administration (SSA) regulations
- Internal Revenue Services (IRS) Publication 1075
- Commonwealth Information Technology Bulletins (ITBs)
- Criminal History Record Information Act (CHRIA)
- Payment Card Industry (PCI) Data Security Standards(DSS).

We have illustrated our six step process to establish a regulatory compliant data center in the figure below. Our approach has been developed by our teaming partner Deloitte, through their extensive experience facilitating regulatory compliance, enables the use of regulations as a driving factor to proactively assess, identify and mitigate gaps. Throughout this process, the Unisys team will collaborate with the Commonwealth stakeholders to review gaps identified, help prioritize mitigation steps and monitor remediation steps. Note that the collaboration with Commonwealth agencies is required as some of the gaps with the regulatory requirements documented may be with the applications not in Unisys control.

Figure 3.2.2.5-4 – The Unisys Team Collaborates with the Commonwealth, Using Our Six-Step Process, To Establish A Risk Aware Datacenter.

- **Deloitte's public sector security risk framework:** The Unisys team uses its teaming partner, Deloitte's demonstrated public sector security risk framework to identify, assess and document the appropriate data protection controls to secure Commonwealth data. Our approach to use an integrated security risk framework is an innovative method to "assess once, comply and report many regulations".
- Deloitte's public sector security risk framework contains over 3,500 individual regulatory requirements mapped to almost 300 unique integrated requirements primarily driven by NIST SP800-53 rev3 (moderate level). This detailed Microsoft Excel-based framework contains the regulatory requirements and their integrated controls. This technology agnostic approach to manage risks is still a pioneer in state governments.
- **Our related experience:** Our teaming partner, Deloitte has established the security risk framework at over 10 states to help the states integrate and assess security regulatory requirements as part of systems development efforts and conduct integrated enterprise level security assessemnts. Our selected experience includes
  - Commonwealth of Pennsylavania – Department of Public Welfare (DPW)
  - State of Indiana
  - State of Delaware and
  - State of Washington.

Unique and *Distinguishing* Factors

Benefits from the Unisys teaming partner, Deloitte's public sector security risk framework

- Contains authoritative sources from more than 30 regulations & standards
- Provides a core set of risk & compliance management solutions
- Allows for consistent comparison, prioritization & aggregation of risk and compliance across the Commonwealth's agencies
- Allows the team to "hit the ground running"
- Provides pre-configured reportsfor key individual regulations.

For example, the Commonwealth of Pennsylvania DPW's security risk framework rationalizes more than 4,000 individual regulatory requirements into 350 unique integrated requirements, including:

- Commonwealth security ITBs
- DPW security policies and standards
- IRS 1075
- SSA
- HIPAA
- Family EducationalRights Protection Act (FEPRA)
- NIST SP800-53 rev 3 and
- ISO 27001:2005.

Additionally, Deloitte's efforts at the state of Delaware included integration of CJIS and PCI DSS v2. Our teaming partner, Deloitte has also established security risk frameworks at several of our commercial clients including very large Banking & Securities, Life Sciences & Health Care, Retail and Oil & Gas firms. The current version of the framework does not include CHRIA requirements and Deloitte will include them as part of the initial security plan activities.

Reporting for regulatory requirements: The data center's current security posture will be documented as part of the initial security plan and also within the data center's security risk framework. When a Commonwealth agency requires a report on the data center's current measures to meet the agency's corresponding regulatory requirements, the data center security manager will use the pre-existing reporting capability of the security framework to extract reports specific to individual regulations such as IRS 1075, SSA, CJIS and PCI DSS.

Our approach to address the Commonwealth selected seven individual security regulatory requirements: As discussed above, we use our risk framework driven approach to address the Commonwelath selected seven key regualtions, through our six step process. The table below illustrates the key components of our approach to establish a Commonwealth data center that meets the Commonwealth identified security regulations and policies/standards.

Regulation/Policy /Standard	Step1: Used to classify Common-wealth data	Step 2: Integrated with the data center risk framework	Step 3: Considered in data center initial security plan	Step 4: Used to perform baseline risk & vulnerability assessment	Step 5:Used to develop and monitor corrective action plan	Step 6: Used to perform an annual security risk assessment & security plan update	Provides ability to generate individual regulatory reports
Commonwealth ITBs	✓	✓	✓	✓	✓	✓	✓
IRS 1075	✓	✓	✓	✓	✓	✓	✓
CJIS	✓	✓	✓	✓	✓	✓	✓
PA CHRIA	✓	✓	✓	✓	✓	✓	✓
SSA	✓	✓	✓	✓	✓	✓	✓
HIPAA	✓	✓	✓	✓	✓	✓	✓
PCI DSS	✓	✓	✓	✓	✓	✓	✓

Each of the six steps are described below:

Step 1: Data identification process and sensitivity classification

As part of the initial security plan the Unisys team will work with the Commonwealth stakeholders to establish a data classification standard data sensitivity levels and establish a data classification based on applicable regulations and leading practices such as NIST SP800-122 (Guide to protecting the confidentiality of PII).

Perform Commonwealth data classification: The Unisys team will conduct workshops with the Commonwealth stakeholders to define a data classification standard for the Commonwewalth Personally Identifiable Information (PII) based on data sensitivity levels. For example, some of the categories include

- Special handling PII (that contains SSN, driver license number, FEIN, and Medicare ID)
- Protected Health Information
- Federal Taxpayer Information (FTI)
- US Social Security Administration (SSA)
- Criminal Justice Information (CJI), including Pennsylvania's Criminal History Records Information Act (CHRIA)
- Sensitive PII (such as racial/ethnic origin, religious/philosophical beliefs, Trade-union membership and criminal convictions).

From our experience of working with the Commonwealth and several public sector clients, Unisys team understands Commonwealth's regulatory landscape. In the table below, we illustrate our understanding of a sample of Federal and Commonwealth regulations that impact the data used by the Commonwealth data center IT infrastructure.

Type of Data	Regulatory impact
Personal Health Information (PHI) **Electronic Health Records (EHR)**	
Child welfare data	

	□ □□□□

Identify presence of PII within the Commonwealth IT infrastructure: In addition to the above illustrated data classification, Unisys team will conduct a one time data discovery assessment. During development of the initial security plan, we perform a data discovery using the McAfee Data Loss Prevention (DLP) solution's data discovery tool. This assessement supports the Unisys team to identify the presence of PII at rest within the current Commonwealth data center IT infrastructure.

The data collected will be documented as part of the IT asset inventory. This information will be used during the data center transition to establish appropriate data protection controls based on the data sensitivity and regulatory requirements (using the Commonwealth data center security risk framework).

Step 2: Gain an understanding of Commonwealth agency's individual regulatory requirements and define the data center security risk framework

From our experience of working with the Commonwealth and several public sector clients, Unisys team understands Commonwealth's regulatory landscape. We will conduct workshops with the Commonwealth agencies as part of the transition planning to identify the applicable regulations, standards and industry leading practices for the data managed by the data center. We will use this information to integrate each agency's individual regulatory requirements as part of the Commonwealth data center security risk framework and to develop the initial security plan (discussed in step 4). The figure below illustrates a sample of the regulations, standards and industry practices that Unisys team uses to define the Commonwealth data center security framework.

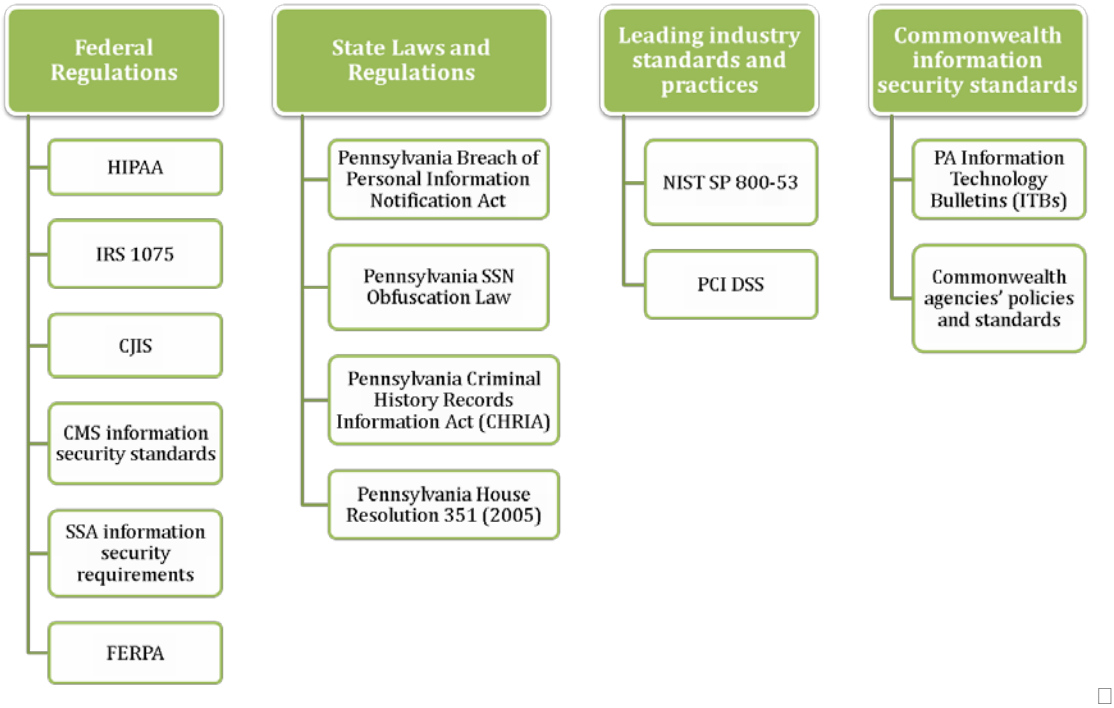


Figure 3.2.2.5-5 – Sample List of Regulations, Industry Standards and Leading Industry Practices Applicable to the Commonwealth

Establish the Commonwealth data center security risk framework

The Unisys team will establish the Commonwealth data center security risk framework. This framework is a broad library of the applicable security and privacy requirements. These requirements are integrated from the relevant Commonwealth ITBs, industry standards, State and Federal regulations. As part of transition and during the ongoing operations, the Unisys team uses this security risk framework to help document data protection controls that meets the relevant regulations and business requirements.

We bring a pre-configured security risk framework to "hit the ground running": We use Deloitte's pre-configured and highly customizable public sector security risk framework to "hit" the ground running and reduce costs. Deloitte, has developed this framework based on more than 12 yers of security and privacy experience within the Commonwelath and the public sector marketplace.

The existing Unisys team's public sector security risk framework provides an integration of regulatory requirments from the following:

- Internal Revenue Services (IRS) publication 1075
- United States Social Security Administration (SSA)
- Health Information Portability and Accountability Act (HIPAA)
- Criminal Justice Information Services (CJIS)

- Payment Card Industry (PCI) Data Security Standard (DSS) v2.0
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 rev 3.

The screenshot below illustrates the Unisys Team's public sector security risk framework showcasing a sample integration of above described regulatory requirements.

Figure 3.2.2.5-6. Sample Integration of Regulatory Requirements available in our pre-configured Public Sector Security Risk Framework.

As described above, we will conduct workshops with the Commonwealth agencies to identify each agency's regulatory requirements such as Commonwealth ITBs, Commonwealth agency policy/standards and PA Criminal History Records Information Act (CHRIA). The Unisys team will extend the Unisys Team's public sector security risk framework to integrate additional regulations to establish the Commonwealth data center security risk framework.

Once developed, the Unisys team estimates that the data center's security risk framework will contain over 4,000 individual regulatory requirements mapped to over 300 integrated/baseline controls, primarily driven by NIST SP800-53 rev 4 as the primary baseline control. As necessary, we will extend the baseline controls with additional leading industry standards to accommodate selected regulatory requirements that may not integrate with NIST SP800-53. The figure below illustrates our demonstrated approach to extend our public sector security risk framework with additional Commonwealth data center regulatory and policy requirements.

Figure 3.2.2.5-7 – The Unisys Team's Approach to Integrate Data Protection Requirements Using the Commonwealth Data Center Security Risk Framework

The Unisys team uses the security risk framework shown in Figure 3.2.2.5-7 above to identify current state and document the initial security plan (described in Step 3). In addition, we used the security risk framework to perform the baseline security risk assessment (described in Step 4).

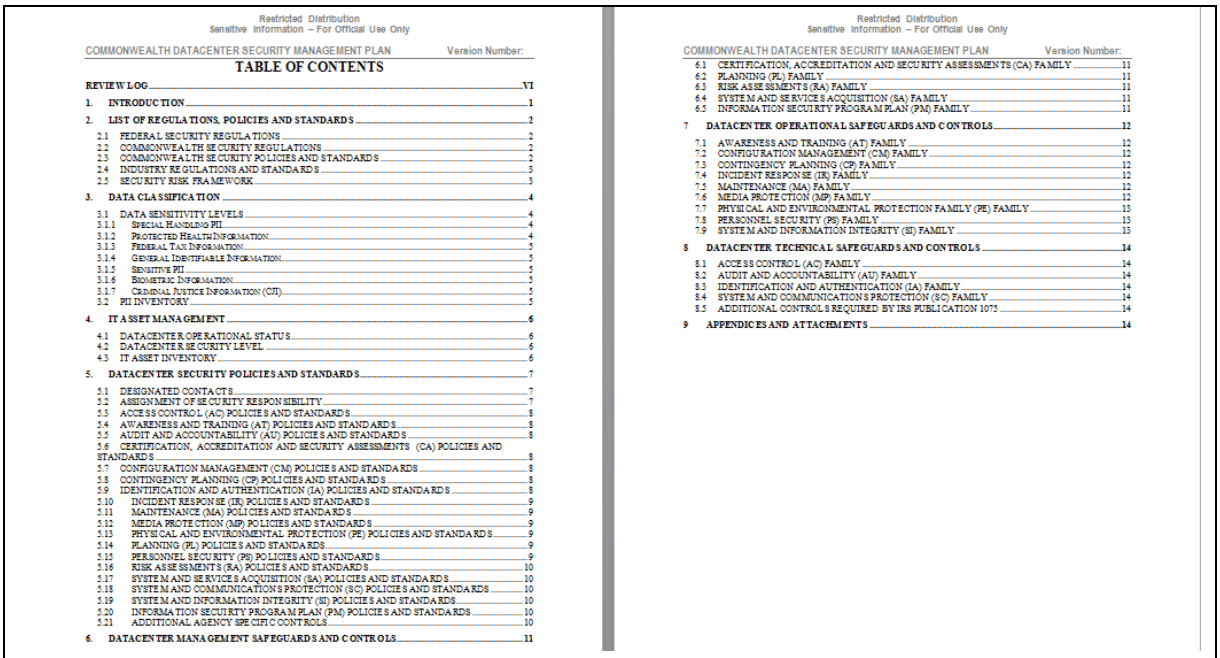
As part of ongoing data center transition and maintenance, we use the established security risk framework to identify relevant data protection requirements to help implement appropriate controls to protect Commonwealth data.

Step 3: Document Initial Security Plan (security management plan) and support Commonwealth's need to develop reports based on regulations

We will establish the Commonwealth data center security plan using guidelines provided by leading industry standards: NIST SP800-18 (RFP requirement specified by Q50 of round 1 part 2) and control guidelines established by NIST SP800-53 rev 4. To develop this plan, the Unisys team uses the Centers for Medicare and Medicaid Services (CMS) Systems Security Plan (SSP) template to define and maintain the appropriate security controls.

A copy of a revised and improved sample security plan is attached to this section within this tab of the BaFO submission.

The figure below illustrates the table of contents of the Sample Commonwealth data center initial security plan.



Restricted Distribution
Sensitive Information – For Official Use Only

COMMONWEALTH DATACENTER SECURITY MANAGEMENT PLAN Version Number:

TABLE OF CONTENTS

REVIEW LOG VI
1. INTRODUCTION 1
2. LIST OF REGULATIONS, POLICIES AND STANDARDS 2
2.1 FEDERAL SECURITY REGULATIONS 2
2.2 COMMONWEALTH SECURITY REGULATIONS 2
2.3 COMMONWEALTH SECURITY POLICIES AND STANDARDS 2
2.4 INDUSTRY REGULATIONS AND STANDARDS 3
2.5 SECURITY RISK FRAMEWORK 3
3. DATA CLASSIFICATION 4
3.1 DATA SENSITIVITY LEVELS 4
3.1.1 SPECIAL HANDLING PII 4
3.1.2 PROTECTED HEALTH INFORMATION 4
3.1.3 FEDERAL TAX INFORMATION 5
3.1.4 GENERAL IDENTIFIABLE INFORMATION 5
3.1.5 SENSITIVE PII 5
3.1.6 BIOMETRIC INFORMATION 5
3.1.7 CRIMINAL JUSTICE INFORMATION (CJI) 5
3.2 PII INVENTORY 5
4. IT ASSET MANAGEMENT 6
4.1 DATACENTER OPERATIONAL STATUS 6
4.2 DATACENTER SECURITY LEVEL 6
4.3 IT ASSET INVENTORY 6
5. DATACENTER SECURITY POLICIES AND STANDARDS 7
5.1 DESIGNATED CONTACTS 7
5.2 ASSIGNMENT OF SECURITY RESPONSIBILITY 7
5.3 ACCESS CONTROL (AC) POLICIES AND STANDARDS 8
5.4 AWARENESS AND TRAINING (AT) POLICIES AND STANDARDS 8
5.5 AUDIT AND ACCOUNTABILITY (AU) POLICIES AND STANDARDS 8
5.6 CERTIFICATION, ACCREDITATION AND SECURITY ASSESSMENTS (CA) POLICIES AND STANDARDS 8
5.7 CONFIGURATION MANAGEMENT (CM) POLICIES AND STANDARDS 8
5.8 CONTINGENCY PLANNING (CP) POLICIES AND STANDARDS 8
5.9 IDENTIFICATION AND AUTHENTICATION (IA) POLICIES AND STANDARDS 8
5.10 INCIDENT RESPONSE (IR) POLICIES AND STANDARDS 9
5.11 MAINTENANCE (MA) POLICIES AND STANDARDS 9
5.12 MEDIA PROTECTION (MP) POLICIES AND STANDARDS 9
5.13 PHYSICAL AND ENVIRONMENTAL PROTECTION (PE) POLICIES AND STANDARDS 9
5.14 PLANNING (PL) POLICIES AND STANDARDS 9
5.15 PERSONNEL SECURITY (PS) POLICIES AND STANDARDS 9
5.16 RISK ASSESSMENTS (RA) POLICIES AND STANDARDS 10
5.17 SYSTEM AND SERVICES ACQUISITION (SA) POLICIES AND STANDARDS 10
5.18 SYSTEM AND COMMUNICATIONS PROTECTION (SC) POLICIES AND STANDARDS 10
5.19 SYSTEM AND INFORMATION INTEGRITY (SI) POLICIES AND STANDARDS 10
5.20 INFORMATION SECURITY PROGRAM PLAN (PM) POLICIES AND STANDARDS 10
5.21 ADDITIONAL AGENCY SPECIFIC CONTROLS 10
6. DATACENTER MANAGEMENT SAFEGUARDS AND CONTROLS 11
6.1 CERTIFICATION, ACCREDITATION AND SECURITY ASSESSMENTS (CA) FAMILY 11
6.2 PLANNING (PL) FAMILY 11
6.3 RISK ASSESSMENTS (RA) FAMILY 11
6.4 SYSTEM AND SERVICES ACQUISITION (SA) FAMILY 11
6.5 INFORMATION SECURITY PROGRAM PLAN (PM) FAMILY 11
7 DATACENTER OPERATIONAL SAFEGUARDS AND CONTROLS 12
7.1 AWARENESS AND TRAINING (AT) FAMILY 12
7.2 CONFIGURATION MANAGEMENT (CM) FAMILY 12
7.3 CONTINGENCY PLANNING (CP) FAMILY 12
7.4 INCIDENT RESPONSE (IR) FAMILY 12
7.5 MAINTENANCE (MA) FAMILY 12
7.6 MEDIA PROTECTION (MP) FAMILY 12
7.7 PHYSICAL AND ENVIRONMENTAL PROTECTION FAMILY (PE) FAMILY 13
7.8 PERSONNEL SECURITY (PS) FAMILY 13
7.9 SYSTEM AND INFORMATION INTEGRITY (SI) FAMILY 13
8 DATACENTER TECHNICAL SAFEGUARDS AND CONTROLS 14
8.1 ACCESS CONTROL (AC) FAMILY 14
8.2 AUDIT AND ACCOUNTABILITY (AU) FAMILY 14
8.3 IDENTIFICATION AND AUTHENTICATION (IA) FAMILY 14
8.4 SYSTEM AND COMMUNICATIONS PROTECTION (SC) FAMILY 14
8.5 ADDITIONAL CONTROLS REQUIRED BY IRS PUBLICATION 1075 14
9 APPENDICES AND ATTACHMENTS 14

Figure 3.2.2.5-8 – Sample Commonwealth data center initial security plan – Proposed Table of Contents.

Step 4: Conduct baseline security risk and vulnerability assessment

The Unisys team performs the baseline security risk and vulnerability assessment to identify gaps within the current Commonwealth data center infrastructure. The Unisys team will work with the Commonwealth to establish a corrective action plan and prioritize mitigation efforts. We have illustrated our steps to perform the baseline security risk and vulnerability assessment in the table below.

Steps	Activities
Scope and Plan	• [illegible] • [illegible] • [illegible]
Conduct Vulnerability Assessment	• [illegible] • [illegible] • [illegible] • [illegible] • [illegible] • [illegible] • [illegible]

Perform Risk Assessment and Security Architecture Review	
Perform Security Configuration Risk Review	
Reporting	

Step 5: Establish Corrective Action Plan

The Unisys team will work with the Commonwealth stakeholders to review the gaps identified by the baseline security risk and vulnerability assessment for establishing the corrective action plan, determining milestones and prioritizing remediation measures. The Unisys team will work with the Commonwealth to update the corrective action plan based on milestones, results from the annual risk assessment and the quarterly vulnerability assessments. The figure below illustrates a sample corrective action plan process, based on CMS guidelines:

Figure 3.2.2.5-9 – The Unisys Team Works with the Commonwealth Stakeholders To Establish a Corrective Action Plan.

Figure 3.2.2.5-10 illustrates a sample Corrective Action Plan template based on CMS guidelines.

Weakness Identifier	Security Control No.	Weakness Description	POC	Resources Required (One-time)	Scheduled Completion Date	Milestones With Completion Dates
State Defined-x	(i.e. AC-2(2))	[Selected Risk Description from final SAR]	[Name, Office/Org]	[man-hours or costs, indicate resource requirement (i.e. new, reallocated or current)]	[field cannot be changed once negotiated and agreed upon]	[include expected completion date with each milestone]
[System Acronym]-1 (ex.)	CP-3 (2)	BCP training has not been conducted.	John Doe - OCISO	(48 Total Man-hours) 40 man-hours - current	6/30/2013 (This should ONLY contain a date - no additional information)	(CP-3 (2)) Employ automated mechanisms to provide a more thorough and realistic training environment. (06/15/2013) (Ensure you put the completion date just as shown above for EACH milestone.)

Changes to Milestones Date	Completion Date	Weakness Status	Risk Level	Weakness Severity	Exception or Waiver	Comments
[When a corrective action is not completed as originally scheduled indicate new date.]	[MM/DD/YY (Completed means weakness has been fully resolved and tested)]	[Completed/Closed, Delayed or Ongoing/Open]	[High, Medium, Low]	[Significant Deficiency, Reportable Condition, Weakness]	[Provide reason, date and signatory for exception or waiver]	[Add additional detail for any previous entries]
N/A	6/29/2013	Completed/Closed	Medium	Weakness	N/A	

Figure 3.2.2.5-10 – Sample Corrective Action Plan Template

Step 6: Perform an annual review and update of the data center security management plan and security risk framework

The Unisys team will perform an annual review and update of data center security plan and the security risk framework. Unisys team performs the following steps to update and submit the security management plan.

Steps	Activities
Scope and Plan	[illegible]
Update IT asset inventory	[illegible]
Update Security Risk Framework	[illegible]

Perform Security Risk Assessment	
Update and Submit the Security Management Plan	

Our approach to maintain and address individual regulatory requirements specified by the Commonwealth

The Unisys team uses the risk framework driven approach to address individual requirements specified for the regulations as identified above.

Risk framework provides an integrated view of the regulatory requirements: The data center's security risk framework provides an integrated view of the regulatory requirements and provides a unified approach to document the data center's security plan. Each regulatory requirement within the data center risk framework is integrated with a baseline control, that integrates similar requirements. This baseline control is based on NIST SP800-53 rev 4. In addition, NIST SP800-53 is considered as the base of several federal regulations such as CJIS and IRS 1075.

The data center risk framework provides pre-existing reports to generate individual regulatory compliance reports: The Unisys team understands that the Commonwealth agencies have individual regulatory requirements and require reports corresponding to their regulatory requirement. The Unisys team risk framework provides pre-configured reports for the following regulatory requirements:

- Internal Revenue Services (IRS) publication 1075
- Payment Card Industry (PCI) Data Security Standards (DSS)
- Health Informaiton Portability and Accountability Act (HIPAA)
- Criminal Justice Information Services (CJIS) and
- United States Social Security Administration (SSA).

In addition to the above pre-configured reports, the Unisys team will configure the risk framework to generate reports for PA CHRIA and the Commonwealth ITBs.

Within the security risk framework, each regulatory requirement is reviewed and mapped to a baseline/integrated control (based on NIST SP800-53). Each of the baseline controls are associated a framework control number. The data center's current security posture will be documented as part of the initial security management plan (initial security plan) and also within the data center's security risk framework.

The data center security manager uses the pre-existing reporting capability of the framework to extract reports specific to regulations.For example, if a Commonwealth agency requires a report that describes the data center's security controls to meet IRS 1075, the security manger generates a report that provides the following information

- Security Frameword Identifier (ID)
- NIST SP800-53 Security (control) Domain
- Regulation
- Regualtory reference
- Regulatory Requirement Description
- Established control
- Last assessment date
- Weakness identied
- Mitigation status
- Plan of Action
- Milestone.

These readily available reports will help the Commonwealth agencies to analyze the regulatory posture and submit as part of periodic reports submitted to regulatory agencies.

Sample risk framework report for IRS1075: The figure below illustrates a sample of the risk framework's pre-configured report that will be used to describe the data center's security posture for IRS1075 regulation.

Figure 3.2.2.5-11 – The Unisys Team's Security Risk Framework Provides a Regulatory Report Customized to Commonwealth Agency Requirements (Example of IRS 1075).

Sample risk framework report for PCI DSS: The figure below illustrates a sample of the risk framework's pre-configured report that will be used to describe the data center's security posture for PCI DSS industry regulation.

Figure 3.2.2.5-12 – The Unisys Team's Security Risk Framework Provides a Regulatory Report Customized to Commonwealth agency Requirements (example of PCI DSS).

Through the data center consolidation effort, the Commonwealth is embarking on a path of integration within and beyond the enterprise. We understand this evolution requires a comprehensive security and privacy strategy and approach that are critical to its operation. The Unisys team brings to the Commonwealth a strong mix of industry leading regulatory risk management practices, experienced team members, related Commonwealth and public sector experiences that add value to establish and maintain a regulatory compliant data center. We believe that these qualifications, combined with our technology strategy and implementation capabilities, uniquely position us to collaborate with the Commonwealth to help effectively evolve and mature the data center's security regulatory posture.

2 Network Security System Architecture, Experience

2.A Implement at minimum: spam filtering, anti-virus, malware protection, firewall (web, application), intrusion prevention and detection, web content filtering, virtual private network, and data loss prevention systems.

2.B Offeror must describe its proposed solution including the following:
Processes and Procedures
Tools / Applications
End User Reports
Standard
Custom
Escalation Procedures

The Commonwealth will be protected through the deployment of the following devices at all Internet ingress points: Web & Application Firewall, Anti-Malware, IPS, Content Filter,

VPN Concentrator and DLP, Processes and Procedures to address Acceptable Use, Physical & Logical Access Reviews and the applicable Commonwealth ITBs.

Web and database application firewalls will use the Imperva SecureSphere platform for proactive, real-time alerting and blocking of potential application threats. Imperva offers adaptable security protection for web threats and meets the Payment Card Industry Data Security Standard (PCI DSS) 6.6 requirement for web application firewalls.

Network based Data loss prevention (DLP), anti-virus, anti-malware, and spam filtering will be provided by McAfee Endpoint Protection security , platforms. McAfee DLP Discover allows discovery and verification of sensitive data, while DLP Prevent ensures that sensitive data being transmitted can be encrypted, redirected, quarantined, or even block the data transmission in question.

Traditional network firewall, virtual private network (VPN), and Intrusion Prevention Services (IPS) services will utilize the Juniper SRX enterprise platform, with separate instances for each service to reduce maintenance downtime and impact.

All firewalls will be implemented using the least privilege policy per agency, blocking all traffic by default. Unisys will work with the Commonwealth CISO during Transition to define a set of recommended security zone templates that will be made available to the agencies. The actual security zones for each application will then be defined to include one or more zones such as the following: 1) web/application production zones 2) database production zone 3) testing zone and 4) development zone. Each security zone is logically separated from one another and using the least privilege policy by blocking all traffic between zones by default.

Modification to the policy is accomplished via the change management process and requires agency approval. Unisys initially uses vendor standard security policies/configurations on the anti-virus and DLP platforms and works with the agencies and OA's Security Office to modify these as appropriate to meet Commonwealth security requirements.

Reporting will be provided from the individual tools, in addition to an aggregate view from the enterprise SIEM system. Examples of standard reports include: anti-virus compliance and auditing per system, dropped and suspicious firewall events, overall top enterprise threats from the SIEM, threat trending per month/quarter/etc. Custom reports may also be requested via the Enterprise Services Catalog and will be developed by working with the Commonwealth security staff to identify required information, trending, formatting, etc. from the individual tools as well as the enterprise SIEM.

There are well established and tested escalation processes in place to address incidents. Escalation processes are described in Schedule F, Section 3.2.1.4 "Service Desk". For security incidents, Commonwealth IT Security Incident Reporting Policy will also be followed.

2.C Offeror must describe its prior experience relative to providing datacenter management and support of CJIS, CCHRI, HIPAA and PCI systems.

Unisys currently supports agencies such as the Department of Public Welfare, Liquor Control Board, Department of Revenue, the Department of Health, and the Pennsylvania State Police in the DPH required to adhere to and be audited on the security standards of

CJIS, CCHRI, HIPAA, PCI, NIST, FISMA and IRS. As required, Unisys supports Commonwealth agencies in complying with these stated security requirements by ensuring the appropriate complement of network security devices are implemented for each agency. The Unisys Team also has provided data at rest encryption capabilities and updated training for the support staff as regulations change and audit based remediation activities require changes in the environment.

The Unisys Team has provided data center management in support of other government agencies in support of CJIS, CCHRI, HIPAA, and PCI systems. As an example, Unisys designed a data and records management system for the Alabama Criminal Justice Information Center that meets CJIS and CHRIA requirements. The Alabama Criminal Justice Information Center (ACJIC) is a state agency providing local, state, and federal criminal justice agencies with the information needed to provide citizen safety. ACJIC realized that gaps in its information technology were hindering communications and business continuity. It needed to more efficiently deliver critical information from its network and systems. ACJIC explored several solutions and solution providers before choosing Unisys to help establish an IT infrastructure specifically designed to address the agency's requirements.

4 Security Attack and Threat Assessment

4.A Review network and other security logs for evidence of attack. Utilize enterprise grade intrusion detection tool(s) to systematically identify, stop, and report security threats. Produce a monthly Security Log Analysis as part of the monthly status reports as described in RFP section IV-5 Reports and Project Control.Offeror must describe its solution and approach

Review Network and Other Security Logs

Unisys will implement a security information and event management (SIEM) system that allows for proactive analysis of security logs from all security, network and system platforms. The SIEM collects, aggregates, analyzes, and correlates system logs to identify suspected security incidents and confirms that the full path of attack is identified. These logs include network switches, routers, firewalls, load balancers, intrusion prevention systems, and active directory domain controllers among others. The Unisys SIEM reviews logs from all sources and identifies immediate threats as well as has the ability to perform historical analysis on previous events for trending and lower severity or persistent attacks. Millions of events can be searched quickly and easily, and logs will be normalized and stored in the CEF (Common Event Format) for easy export to the Commonwealth SIEM platform.

Suspected risks and threats immediately go through the incident management process for remediation, and follow up reporting are provided in standard formatting, with custom reporting also available.

The Juniper intrusion prevention system (IPS) sends its logs to the SIEM for real time analysis and correlation with other device logs to determine possible malicious activity. This is accomplished with a signature based system capable of protocol and traffic anomaly detection, zero day protection, and application awareness. Suspected intrusions are blocked based upon the vendor recommended security rating and continually tuned for more accurate detection and less false positives.

The Commonwealth will receive a monthly security report detailing all security incidents, which will be provided to appropriate agency and OA security administration. See item 3 above for additional details on reports.

6 Network Physical Access Restrictions

6.A Restrict physical access to all network systems and equipment with biometric or other second factor access control systems. Offeror must describe solution and approach to meet this requirement

Unisys takes a layered approach to security. Each facility has both physical and logical security in place. Managing access to systems starts with physically securing all network systems and equipment to prevent unauthorized personnel from gaining access. Given the differences in the facilities, however, we will discuss the facilities' physical access controls separately.

For the Unisys [redacted] facility; perimeter security is maintained by camera and an active physical security presence. A guard controls access to interior spaces 24x7x365; the guards are employees of the building owner, not contractors. Access control systems include access to and within the facility. Access control is achieved through three factors of authentication tools, namely keycard, keypad and biometric devices, across up to seven entry points (entry to lobby, two in the mantrap from lobby to main offices, two in the mantrap from offices to vault hallway, from hallway to the Commonwealth Datacenter vault, from the vault into the optional cages). Additional rack-based keypad or keycard controls are included in the Catalog to further restrict physical access to one or more of any agency's racks at the option of the agency.

For the EDC, building perimeter security is maintained by camera. A guard will control access to interior spaces during business hours. During off hours, access is not normally available to personnel who do not have predefined access (e.g., visitors, deliveries), when access to the CTC-1 building is also restricted. Access control systems include access to and within the facility. Unisys will use the existing badge reader systems and biometric access control systems in a double-entry configuration. Additional keypad or keycard controls are available through a change order to further restrict physical access to one or more of any agency's cages or racks at the option of the agency.

Unisys Security Operations Center (SOC) is comprised of security support staff and a suite of automated tools that provide comprehensive 24x7x365 monitoring, alerting, and response to security events.

7. Network Data Access Restrictions

7.A Restrict access to all data in the Commonwealth network infrastructure. Restrict and control all data access right, groups and special permissions based on the data security program designed by the Commonwealth security team and/or specified by the agencies. Access level changes and exceptions will be executed only when approved paperwork is complete and approved. A file of all access changes will be maintained by the Offeror for audit purposes. Offeror must support Commonwealth initiated security audits. Offeror must describe solution and approach to meet this requirement

Unisys will implement a "need to know" and "least privilege" policy in accordance with

Commonwealth logical and data access policies. System administrators will set up user accounts with appropriate levels of data access to restrict and control the access rights of system users based on their role and group designations as specified by the Commonwealth or specific Commonwealth agencies. The Unisys security team will use a privileged identity management suite to manage and monitor the access of privileged users to Commonwealth systems. Additionally, access activity logs produced by Commonwealth systems and management tools are sent to the SIEM for aggregate analysis and reporting. Changes and exceptions will only be made by Unisys upon the receipt of approved documentation from the Commonwealth or Commonwealth agency management. Unisys will perform monthly reviews of logical access changes and will support and fully participate in all Commonwealth initiated security audits. Unisys will maintain a log of all access changes for audit and review at the Commonwealth's request.

This page intentionally left blank.

3.2.4.6 Security & Firewall

The Security & Firewall service will provide hosting and operational support Services for security products and firewalls located at the data centers. These security devices and Services protect the equipment and applications in the data centers from malicious attempts to penetrate the computing environment with worms, phishing, Trojan horse malware, and unlawful data access. Offeror must install and maintain mainstream security hardware and software utilizing current industry best practices sufficient to protect the enterprise class data center environments with a significant volume of sensitive class data (e.g. HIPAA, CJIS, CHRIA, PCI, PII, etc.). The number of support staff members required to perform the tasks listed below will be determined by the Offeror.

Listed below are the basic Services required to manage the security & firewall systems required by the Commonwealth. Offeror must include these Services in addition to the base level of Services in this Offering.

Reference Documentation

Exhibit A - Commonwealth Network Environment

Exhibit J.1 through J.3 - Commonwealth Security and Compliance Requirement

Exhibit G.6 - PSP - CJIS Security Policy

Exhibit G.9 - PSP - CCHRI

Exhibit G.7 - PSP - Summary of CJIS Requirements

Exhibit G.12 - PSP - CHRIA Handbook

	Requirements	Describe Compliance

1.	Monitor local security operations, troubleshoot and resolve operational issues.
	
	Actively (normal daily process) monitor the operations of all security, firewall systems and security zones.
	
	Maintain a log for each server/appliance/system and review the system logs on a daily basis to ensure key system Services are processing without errors.
		Offeror must describe its approach to supporting the needs of the Commonwealth including the following:
		
		• Processes & Procedures
		• Tools / Applications
		• End User Reports
		  o Standard
		  o Custom
		• Tiered Service/Support Levels

	Provide the ability to import data to agency SIEM or enterprise SIEM tool for correlation and reporting purposes. Provide the ability for Commonwealth agencies to request security modifications (firewall changes) as documented in the CCPM. Document review of the system security logs on a weekly basis to ensure critical system Services are processing without errors. Complete weekly server log indicating which logs were reviewed, date and initial the log.	• Escalation Procedures Offeror must describe prior experience relative to providing datacenter management and support of CJIS, CCHRI, HIPAA and PCI compliant systems.
2.	Provide security training to Commonwealth personnel specific to the security Services being delivered. Provide the Commonwealth with a resume or CV for each operational staff member assigned to this engagement. Comply with agency background checks and clearances as defined in Appendix A - Terms and Conditions.	Offeror must describe its approach to supporting the needs of the Commonwealth. Offeror must submit a representative sample of staff resumes typically provided for these positions and describe the process to ensure compliance of background checks and clearances.
3.	Achieve cost effective 24/7 security operational coverage for this critical system. Provide dedicated security support staff onsite during scheduled business days, and automated log and notification systems to alert security team of possible intrusion events in real time mode. Provide Level 2 and Level 3 Support to the Service Desk and/or Commonwealth Users. Security staff must be available to respond and evaluate the severity of the event	Offeror must describe its security operations coverage and how it will be applied.

	24/7/365.	
4.	Ensure network connectivity, and ensure consistent system response times. Utilize automated system management tool(s) to ensure real-time monitoring and notification of server availability and response times.	Offeror must describe its real-time monitoring approach and toolset to provide and maintain network availability and performance. Offeror must identify tools it uses to support network availability and performance.
5.	Ensure server/appliance operating systems are maintained with the current system patch level. Implement a Patch Management Program to ensure the timely application of security updates on all infrastructure platforms in accordance with Commonwealth IT policy guidelines. Ensure signature and threat analysis files are updated on a regular basis, and conform to industry best practices. Analyze monthly service patches and determine which patches need to be applied, by server type. Create a change record, log the update in the server log, and install based on server availability schedule. Notify the Commonwealth of any scheduled or unscheduled service interruptions.	Offeror must describe its approach to supporting the needs of the Commonwealth. Offeror must describe its approach for testing and validating updates to the OS and 3rd Party software that it supports. Offeror must describe its approach to communicating unscheduled and scheduled outages, including escalation process.
6.	Provide active security operations, corrective action, and reporting by utilizing Offeror software to monitor inbound and outbound traffic for malicious patterns and content, and take appropriate protective measures. The ability to utilize security management software to detect threats	Offeror must describe its Security Operations Process and how it will be applied.

	and analyze firewall logs, to proactively detect and protect from malicious events. Comply with agency specific security requirements. Comply with all agency and OA/OIT security policies and ITBs. On a quarterly schedule, run appropriate penetration testing, and report results to Commonwealth and Offeror. Create monthly report on events, incidents and corrective activities. Report that indicates systems not in compliance with security standards. Real time reporting of security breaches.	
7.	SLA Reporting including but not limited to collecting actual system availability, utilization and response time data. Create a Service Level Agreement report for the Commonwealth and Offeror on a monthly basis.	Offeror must describe its approach to supporting the needs of the Commonwealth.
8.	Software License Management	Refer to 3rd Party Software Management service.
Continual Process Improvement		
9.	Reduce service risks.	Offer methods to eliminate or mitigate service risks.
10.	Improve service quality. Make recommendations to the Commonwealth team any system changes that would be appropriate to maintain or improve SLA commitments	Offeror must describe its approach to supporting the needs of the Commonwealth.

	on a quarterly basis.	
11.	Improve client satisfaction.	Offeror must provide examples of previous Offeror initiatives aimed at continually improving client satisfaction.
12.	Ensure service transparency using documentation methods to ensure service transparency, by providing visibility into service execution.	Offeror must describe its approach to supporting the needs of the Commonwealth.
13.	Improve/reduce cost of service.	Offeror must provide examples of Security and Firewall Support initiatives that have been implemented or can be utilized to achieve reduced costs of Services and to meet or exceeded ROI (Return on Investment) analysis projections.

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

Introduction

Unisys understands the importance of the critical need for the Commonwealth to protect its equipment, applications, and data in compliance with regulations such as HIPAA, PCI, PII, CJIS, and CHRIA, and to protect its computing infrastructure from malicious and unlawful attempts to cause harm. Unisys will leverage its experience with industry leading security and firewall products to provide hosting and operational support services for the Commonwealth.

1 Security Operations Approach, Experience

1.B Actively (normal daily process) monitor the operations of all security, firewall systems and security zones.

The Unisys SIEM platform integrated with the Remedy Incident platform will provide automated and customizable log reviews and incident escalation to dedicated, on-site security operations staff during the scheduled business day's review of critical system processes and components.

The Unisys Team's SNMP monitoring tools also process events on the operational status of the security and firewall platforms. By forwarding the event alerts generated by both the SIEM and the monitoring tools, the event correlation system identifies the actual event and auto-generates incident tickets with ITSM. The network and security support team uses the information from the incident ticket and the details from the SIEM and the monitoring tools to resolve the associated incidents.

1.D Provide the ability to import data to agency SIEM or enterprise SIEM tool for correlation and reporting purposes.

The Unisys Team provides support to export data from the SIEM and central logging tools via CEF (Common Event Format) and CSV (Comma Separated Value) files that can be imported into the Commonwealth SIEM. Requests to provide exported data or integrate with an Agency or enterprise SIEM are supported through the service request process.

1.E Provide the ability for Commonwealth agencies to request security modifications (firewall changes) as documented in the CCPM.

The Commonwealth will be able to request security modifications through the Change Management Process documented in the CCPM. All changes to firewall policy for a specific agency must be approved by the entitled change approver for that agency.

3 Service Desk, Tiered Support, Operational Coverage

3.A Achieve cost effective 24/7 security operational coverage for this critical system.

Offeror must describe its security operations coverage and how it will be applied.

Provide dedicated security support staff onsite during scheduled business days, and automated log and notification systems to alert security team of possible intrusion events in real time mode.

Unisys will provide dedicated network/security support staff onsite during scheduled business days, coupled with automated tools that provide real time notification of suspected security intrusion events. The Unisys Security Operations Center (SOC) is comprised of these security support staff and a suite of automated tools that provide comprehensive 24x7x365 monitoring, alerting, and response to security events. Please refer to Schedule F, Section 3.2.2.5 – Security Management, for more details. Personnel follow specific instructions to mitigate issues according to the Security Incident Procedure (SIP) policy.

3.C Security staff must be available to respond and evaluate the severity of the event 24/7/365.

The Unisys Team uses an integrated series of manual and automated procedures to monitor, respond, evaluate and manage security events. These procedures include a basis to determine the severity of the events and support the appropriate response to resolve the incident.

The Unisys Team also uses an integrated set of tools to monitor and manage the security infrastructure within the data centers. The central security monitoring component is the [redacted] platform which collects, prioritizes, and forwards significant security events to the [redacted]. Network and security events are correlated with other events within BPPM and used to auto-generate incident tickets with the ITSM platform for network, security and other system events. ITSM provides automatic ntofications for Unisys support including the network and security teams, security manager, and Commonwealth stakeholders.

In addition to the security monitoring described above, the Unisys Service Desk (Level 1) supports the security staff as the point of contact for authorized users to call in events and incidents. The Service Desk also provides regular status updates on active events.

Events will be escalated to senior Unisys network/security support resources (Level 3) and/or the OEM as needed to resolve the incident.

4 Monitor network Connectivity, Toolset

4.A Ensure network connectivity, and ensure consistent system response times.

Unisys will provide event management solutions to help confirm network connectivity and consistent system response times. Proactive monitoring tools will be used that monitor excessive delay and latency in the network via ICMP and SNMP. Network monitoring systems [redacted]) will measure and record interface errors, discards, uptime, etc. for real time alerting and historical analysis.

Refer to Schedule F Section 3.1.2 Network Architecture for further details on network connectivity.

5 Patch Management

Ensure server/appliance operating systems are maintained with the current system patch level.

Offeror must describe its approach to supporting the needs of the Commonwealth.

Implement a Patch Management Program to ensure the timely application of security updates on all infrastructure platforms in accordance with Commonwealth IT policy guidelines.

Offeror must describe its approach for testing and validating updates to the OS and 3rd Party software that it supports.

Ensure signature and threat analysis files are updated on a regular basis, and conform to industry best practices.

Analyze monthly service patches and determine which patches need to be applied, by server type.

Create a change record, log the update in the server log, and install based on server availability schedule.

Notify the Commonwealth of any scheduled or unscheduled service interruptions.

Offeror must describe its approach to communicating unscheduled and scheduled outages, including escalation process.

The Unisys technical support team will patch based on Commonwealth /Agency policies as defined in the ITBs. The patch program will address policies, processes, procedures for the following:

- Sources of patches (how to obtain them from the OEM's)
- Toolsets that will be used to stage patches for possible deployment

- Change management procedures supporting the Change Management Process to identify, approve and manage deployment of patches
- Compliance procedures to include utilization of the toolsets to run compliance audits and identify out of compliance CI's with patch policies and approved changes
- Process and procedures to bring out of compliance CI's back into compliance

Unisys will follow the Change Management Process for applying patches to all IT infrastructure CI's. This process will maintain the change record in the [redacted] platform and also update the CMDB configuration management file after completion of the patch release and deployment process. The BMC ITSM change record will be related to the CI's in the CMDB as an audit trail for patch changes upon the completion of the Release and Deployment Process.

The distributed IT infrastructure toolset to support the automation of patch release and deployment is [redacted] Unisys will maintain in this toolset the appropriate patch policies for determining patch deployment and compliance. The [redacted] will be maintained with all the current patches supplied by the OEM's and will be used to manage the production state of patch deployment in the windows environment.

Unisys approach to testing and validating updates to the all CI's is to follow the release and deployment process for all changes into all production environments. The release process includes:

- Change ticket approvals
- Test planning and accepted test results
- Release and deployment planning including release back out plans
- Release testing for risky deployments
- Early life cycle support to help provide a successful deployment
- Release back out for failed releases

The Unisys technical support team will work with the Commonwealth/Agencies to determine patch policies for which patches should be applied to the server/appliance environment. Policies will be implemented to govern changes to the server/appliance environment as it pertains to HIPAA, SOX, CIS, etc. and to conform to the Commonwealth policies.

Unisys will follow the Change Management Process for applying patches to the production environment. This process will maintain the change record in the [redacted] platform and also update the CMDB configuration management file upon deployment for the server/appliance Configuration Item (CI). The Change Record will be related to the CI in the CMDB as an audit trail for changes to servers.

The toolset to support the automation of patch release and deployment is [redacted]. Unisys will maintain in this toolset the appropriate patch policies for determining patch deployment and compliance. The [redacted] will be updated with all the current patches supplied by the infrastructure OEM's and will be used to manage the production state of patch deployment in the infrastructure environment. Unisys will use [redacted] to support:

- Policies for the server/appliance environment
- Software distribution and server/appliance patching
- Compliance management of patches required for security policies

The anti-virus, malware and intrusion detection tools also monitor and update the related signature and threat analysis files within the server, network and security infrastructure using the regular updates provided by the vendors. Antivirus and other signature updates which are automatically pushed to the infrastructure will be processed as part of the tools configurations. Other update files will be loaded during an approved change window and use the change approval process.

Unisys standard maintenance notification and escalation process will be followed, as defined in Schedule F, Section 3.2.3.2 Site Operations.

6 Security Operations

6A Provide active security operations, corrective action, and reporting by utilizing Offeror software to monitor inbound and outbound traffic for malicious patterns and content, and take appropriate protective measures.

Offeror must describe its Security Operations Process and how it will be applied.

The ability to utilize security management software to detect threats and analyze firewall logs, to proactively detect and protect from malicious events.

Unisys will use a combination of intrusion prevention and SIEM (Security Incident and Event Management) software to monitor all inbound and outbound traffic for malicious content in real-time. Unisys will follow the incident and problem management process to expeditiously report and act on all suspected security events, which may include network based blocking of traffic. Firewall logs will be analyzed by both a standardized syslog platform and a SIEM that will correlate with other device logs (e.g. IPS, server, etc.).

Refer to Schedule F Section 3.2.2.5 Security Management for detail on the Unisys Team's Security Operations process.

Refer to questions 1B, 2C and 3C above for details on the security management tools and log analysis to proactively detect and protect from malicious events.

6.B Comply with agency specific security requirements.

Comply with all agency and OA/OIT security policies and ITBs.

The Unisys Team uses the Security Management Plan as the basis to analyze, understand, and document the security, regulatory, and policy requirements for each agency, including OA/OIT security policies and ITBs. The security team uses this information to define, update and maintain the configurations of the security platforms, tools, and monitoring systems to maintain compliance with the related policies.

6.D Report that indicates systems not in compliance with security standards.

The Unisys Team uses the automated management tools ([redacted]) to monitor for compliance for the network, security, and other systems. These tools include configuration templates which are used during automated regular checks on the systems to confirm the configurations continue to comply with the security standards. If a system is identified as not being in compliance, an incident ticket is generated and will be closed after the configuration is returned to a compliant state. The templates are updated through change management to reflect modifications from the Security Management Plan, new or updated OA/OIT policies and ITBs.

Compliance reports are made available through the Services Portal's dashboard.

6.E Create monthly report on events, incidents and corrective activities.

The ITSM system described in Section 3.2.3.2 supports the tracking and reporting on all incidents and the related resolutions. The ITSM system's reporting functionality will be used to generate the monthly reports on security related events, incidents and resolutions. This report is available through the Services Portal dashboard.

6.F Real time reporting of security breaches.

The Unisys Team uses the SIEM to monitor and forward events which are caused by security breaches. Incident tickets are auto-generated in ITSM based on the events and include email notifications to the Unisys security team, security manager, and Commonwealth stakeholders. The SIEM will analyze the incident; and when a security breach is suspected, Unisys will report it as a priority 1 incident using the incident management process as defined in the CCPM, including real time reporting and establishing management conference bridges. Updates on the incidents are available through contacting the Service Desk, participating in status update bridges when available and on the Services Portal.

Restricted Distribution or Use
Sensitive Information – For Official Use Only

Commonwealth Datacenter Security Management Plan – Sample Plan

Version 1.0

August, 2013

TABLE OF CONTENTS

REVIEW LOG ..... **V**

1. INTRODUCTION **1**

2. LIST OF REGULATIONS, POLICIES AND STANDARDS **2**

2.1 FEDERAL SECURITY REGULATIONS 2
2.2 COMMONWEALTH SECURITY REGULATIONS 2
2.3 COMMONWEALTH SECURITY POLICIES AND STANDARDS 2
2.4 INDUSTRY REGULATIONS AND STANDARDS 3
2.5 SECURITY RISK FRAMEWORK 3

3. DATA CLASSIFICATION **4**

3.1 DATA SENSITIVITY LEVELS 4
3.1.1 SPECIAL HANDLING PII 4
3.1.2 PROTECTED HEALTH INFORMATION 4
3.1.3 FEDERAL TAX INFORMATION 5
3.1.4 GENERAL IDENTIFIABLE INFORMATION 5
3.1.5 SENSITIVE PII 5
3.1.6 BIOMETRIC INFORMATION 5
3.1.7 CRIMINAL JUSTICE INFORMATION (CJI) 5
3.2 PII INVENTORY 5

4. IT ASSET MANAGEMENT **6**

4.1 DATACENTER OPERATIONAL STATUS 6
4.2 DATACENTER SECURITY LEVEL 6
4.3 IT ASSET INVENTORY 6

5. DATACENTER SECURITY POLICIES AND STANDARDS **7**

5.1 DESIGNATED CONTACTS 7
5.2 ASSIGNMENT OF SECURITY RESPONSIBILITY 7
5.3 ACCESS CONTROL (AC) POLICIES AND STANDARDS 8
5.4 AWARENESS AND TRAINING (AT) POLICIES AND STANDARDS 8
5.5 AUDIT AND ACCOUNTABILITY (AU) POLICIES AND STANDARDS 8
5.6 CERTIFICATION, ACCREDITATION AND SECURITY ASSESSMENTS (CA) POLICIES AND STANDARDS 8
5.7 CONFIGURATION MANAGEMENT (CM) POLICIES AND STANDARDS 8
5.8 CONTINGENCY PLANNING (CP) POLICIES AND STANDARDS 8
5.9 IDENTIFICATION AND AUTHENTICATION (IA) POLICIES AND STANDARDS 8
5.10 INCIDENT RESPONSE (IR) POLICIES AND STANDARDS 9
5.11 MAINTENANCE (MA) POLICIES AND STANDARDS 9
5.12 MEDIA PROTECTION (MP) POLICIES AND STANDARDS 9
5.13 PHYSICAL AND ENVIRONMENTAL PROTECTION (PE) POLICIES AND STANDARDS 9
5.14 PLANNING (PL) POLICIES AND STANDARDS 9
5.15 PERSONNEL SECURITY (PS) POLICIES AND STANDARDS 9
5.16 RISK ASSESSMENTS (RA) POLICIES AND STANDARDS 10
5.17 SYSTEM AND SERVICES ACQUISITION (SA) POLICIES AND STANDARDS 10
5.18 SYSTEM AND COMMUNICATIONS PROTECTION (SC) POLICIES AND STANDARDS 10
5.19 SYSTEM AND INFORMATION INTEGRITY (SI) POLICIES AND STANDARDS 10
5.20 INFORMATION SECUIRTY PROGRAM PLAN (PM) POLICIES AND STANDARDS 10
5.21 ADDITIONAL AGENCY SPECIFIC CONTROLS 10

6. DATACENTER MANAGEMENT SAFEGUARDS AND CONTROLS **11**

6.1 CERTIFICATION, ACCREDITATION AND SECURITY ASSESSMENTS (CA) 11
6.2 PLANNING (PL) 11
6.3 RISK ASSESSMENTS (RA) 11
6.4 SYSTEM AND SERVICES ACQUISITION (SA) 11
6.5 INFORMATION SECUIRTY PROGRAM PLAN (PM) 11

7 DATACENTER OPERATIONAL SAFEGUARDS AND CONTROLS 12

7.1 AWARENESS AND TRAINING (AT) 12
7.2 CONFIGURATION MANAGEMENT (CM) 12
7.3 CONTINGENCY PLANNING (CP) 12
7.4 INCIDENT RESPONSE (IR) 12
7.5 MAINTENANCE (MA) FAMILY 28
7.6 MEDIA PROTECTION (MP) 28
7.7 PHYSICAL AND ENVIRONMENTAL PROTECTION FAMILY (PE) 28
7.8 PERSONNEL SECURITY (PS) 28
7.9 SYSTEM AND INFORMATION INTEGRITY (SI) 28

8 DATACENTER TECHNICAL SAFEGUARDS AND CONTROLS 29

8.1 ACCESS CONTROL (AC) 29
8.2 AUDIT AND ACCOUNTABILITY (AU) 29
8.3 IDENTIFICATION AND AUTHENTICATION (IA) 29
8.4 SYSTEM AND COMMUNICATIONS PROTECTION (SC) 29

9 APPENDICES AND ATTACHMENTS 30

REVIEW LOG

This Review Log is maintained to record the reviews that have taken place for this system.
The review log should be completed by entering the data from each column in the appropriate row.

Author	Response Data
Name:	
Title:	
Organization:	
Address:	
Mail stop:	
City, State, Zip:	
E-mail:	
Phone Number:	

Date of Review.	Staff Name of Reviewer	Commonwealth Approval

1. INTRODUCTION

The SSP documents the current level of existing security controls within the System that protect the confidentiality, integrity and availability (CIA) of the system and its information.

2. LIST OF REGULATIONS, POLICIES AND STANDARDS

2.1 FEDERAL SECURITY REGULATIONS

[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]

2.2 COMMONWEALTH SECURITY REGULATIONS

[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]

2.3 COMMONWEALTH SECURITY POLICIES AND STANDARDS

[illegible]	[illegible]
[illegible]	[illegible]

[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]

2.4 INDUSTRY REGULATIONS AND STANDARDS

[illegible]	[illegible]
[illegible]	[illegible]

2.5 SECURITY RISK FRAMEWORK

3. DATA CLASSIFICATION

3.1 DATA SENSITIVITY LEVELS

- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]

[illegible]

3.1.1 Special Handling PII

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

3.1.2 Protected Health Information

[illegible]

[illegible]

3.1.3 Federal Tax Information

3.1.4 General Identifiable Information

3.1.5 Sensitive PII

3.1.6 Biometric Information

3.1.7 Criminal Justice Information (CJI)

3.2 PII INVENTORY

4. IT ASSET MANAGEMENT

4.1 DATACENTER OPERATIONAL STATUS

Datacenter	Operational Status
Datacenter 1	
Datacenter 2	

4.2 DATACENTER SECURITY LEVEL

Datacenter 1 Description	Response Data
Security Level:	
Information Type:	

Datacenter 2 Description	Response Data
Security Level:	
Information Type:	

4.3 IT ASSET INVENTORY

5. DATACENTER SECURITY POLICIES AND STANDARDS

5.1 DESIGNATED CONTACTS

5.2 ASSIGNMENT OF SECURITY RESPONSIBILITY

Individual[s] Responsible for Security	Response Data
Name:	
Title:	
Organization:	
Address:	
Mail stop:	
City, State, Zip:	
E-mail:	
Phone Number:	
Emergency Contact (daytime): (name, phone & email)	

Component ISSO	Response Data
Name:	
Title:	
Organization:	
Address:	
Mail stop:	
City, State, Zip:	
E-mail:	
Phone Number:	
Emergency Contact (daytime): (name, phone & email)	

5.3 ACCESS CONTROL (AC) POLICIES AND STANDARDS

5.4 AWARENESS AND TRAINING (AT) POLICIES AND STANDARDS

5.5 AUDIT AND ACCOUNTABILITY (AU) POLICIES AND STANDARDS

5.6 CERTIFICATION, ACCREDITATION AND SECURITY ASSESSMENTS (CA) POLICIES AND STANDARDS

5.7 CONFIGURATION MANAGEMENT (CM) POLICIES AND STANDARDS

5.8 CONTINGENCY PLANNING (CP) POLICIES AND STANDARDS

5.9 IDENTIFICATION AND AUTHENTICATION (IA) POLICIES AND STANDARDS

5.10 INCIDENT RESPONSE (IR) POLICIES AND STANDARDS

5.11 MAINTENANCE (MA) POLICIES AND STANDARDS

5.12 MEDIA PROTECTION (MP) POLICIES AND STANDARDS

5.13 PHYSICAL AND ENVIRONMENTAL PROTECTION (PE) POLICIES AND STANDARDS

5.14 PLANNING (PL) POLICIES AND STANDARDS

5.15 PERSONNEL SECURITY (PS) POLICIES AND STANDARDS

5.16 RISK ASSESSMENTS (RA) POLICIES AND STANDARDS

5.17 SYSTEM AND SERVICES ACQUISITION (SA) POLICIES AND STANDARDS

5.18 SYSTEM AND COMMUNICATIONS PROTECTION (SC) POLICIES AND STANDARDS

5.19 SYSTEM AND INFORMATION INTEGRITY (SI) POLICIES AND STANDARDS

5.20 INFORMATION SECUIRTY PROGRAM PLAN (PM) POLICIES AND STANDARDS

5.21 ADDITIONAL AGENCY SPECIFIC CONTROLS

6. DATACENTER MANAGEMENT SAFEGUARDS AND CONTROLS

6.1 CERTIFICATION, ACCREDITATION AND SECURITY ASSESSMENTS (CA)

The description of datacenter's CA process and technology solutions

6.2 PLANNING (PL)

The description of datacenter's PL process and technology solutions

6.3 RISK ASSESSMENTS (RA)

The description of datacenter's RA process and technology solutions

6.4 SYSTEM AND SERVICES ACQUISITION (SA)

The description of datacenter's SA process and technology solutions

6.5 INFORMATION SECUIRTY PROGRAM PLAN (PM)

The description of datacenter's PM process and technology solutions

7 DATACENTER OPERATIONAL SAFEGUARDS AND CONTROLS

7.1 AWARENESS AND TRAINING (AT)

The description of datacenter's AT process and technology solutions

7.2 CONFIGURATION MANAGEMENT (CM)

The description of datacenter's CM process and technology solutions

7.3 CONTINGENCY PLANNING (CP)

The description of datacenter's CP process and technology solutions

7.4 INCIDENT RESPONSE (IR)

<Sample Incident Response Control Descriptions>

IR-1 – Incident Response Policy and Procedures

Control Requirements

NIST SP800-53 rev3:

IRS 1075 rev2010:

CJIS v5.1:

HIPAA:

PA CHRIA:

state ITB:

PCI DSS:

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation**
Status: Implemented	

COMMONWEALTH DATACENTER SECURITY MANAGEMENT PLAN	Version Number:
• [illegible] • [illegible] • [illegible] [illegible] [illegible] • [illegible] • [illegible] • [illegible] • [illegible] • [illegible] • [illegible] • [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible]	

IR-2 – Incident Response Training (Moderate)

Control

NIST SP800-53 rev3:

IRS 1075 rev2010:

Supplemental Guidance

CJIS v5.1:

HIPAA:

PA CHRIA:

state ITB:

PCI DSS: 12.9.4

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation**
Status: Implemented	

IR-3 – Incident Response Testing and Exercises (Moderate)

Control

NIST SP800-53 rev3:

IRS 1075 rev2010:

Supplemental Guidance

CJIS v5.1:

HIPAA:

PA CHRIA:

state ITB:

PCI DSS **12.9.2**

12.9.6

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation**
Status: Implemented	

IR-4 – Incident Handling (Moderate)

Control

NIST SP800-53 rev3:

Implementation Standard(s)

IRS 1075 rev2010:

CJIS v5.1:

HIPAA:

PA CHRIA:

state ITB:

Security Incident Category 1 (Critical/High)	

	[illegible]
[illegible] [illegible]	[illegible] A [illegible]
[illegible] [illegible] [illegible] [illegible]	[illegible]

Security Incident Category 2 (Medium)	
[illegible] [illegible]	[illegible]
[illegible] [illegible] [illegible]	[illegible] A [illegible]
[illegible] [illegible] [illegible] [illegible]	[illegible]

Security Incident Category 3 (Low)	
[illegible] [illegible]	[illegible]
[illegible] [illegible] [illegible]	[illegible] A [illegible]
[illegible] [illegible] [illegible] [illegible]	[illegible]

Security Incident Category (Unknown/Other)	
[illegible] [illegible]	[illegible]
[illegible] [illegible] [illegible]	[illegible] A [illegible]
[illegible] [illegible] [illegible] [illegible]	[illegible]

[illegible]	[illegible]

PCI DSS: [illegible]

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation**
Status: Implemented [illegible] A[illegible] • [illegible] • [illegible] • [illegible] • [illegible] • [illegible] • [illegible] • [illegible] • [illegible]	[illegible]

IR-5 – Incident Monitoring (Moderate)

Control

NIST SP800-53 rev3:

IRS 1075 rev2010:

CJIS v5.1:

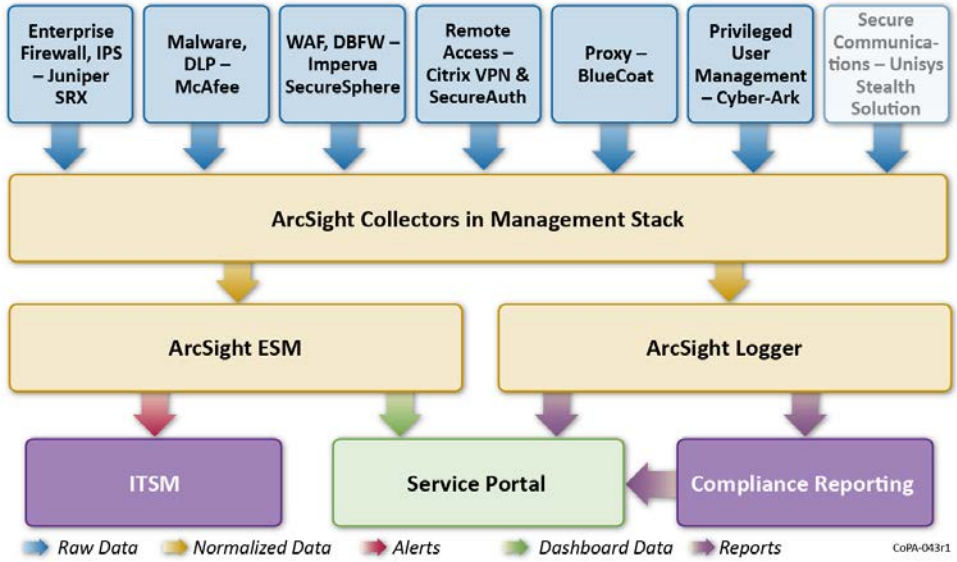
HIPAA:

PA CHRIA:

state ITB:

PCI DSS: 12.9.5

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation**
Status: Implemented	


Enterprise Firewall, IPS – Juniper SRX
Malware, DLP – McAfee
WAF, DBFW – Imperva SecureSphere
Remote Access – Citrix VPN & SecureAuth
Proxy – BlueCoat
Privileged User Management – Cyber-Ark
Secure Communica-tions – Unisys Stealth Solution
ArcSight Collectors in Management Stack
ArcSight ESM
ArcSight Logger
ITSM
Service Portal
Compliance Reporting
Raw Data
Normalized Data
Alerts
Dashboard Data
Reports
CoPA-043r1

IR-6 – Incident Reporting (Moderate)

Control

NIST SP800-53 rev3:

IRS 1075 rev2010:

CJIS v5.1:

HIPAA:

PA CHRIA:

state ITB:

PCI DSS:

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation**
Status: Implemented	

Agency Name	**Data type**	**Contact Information**	**Reporting Timeframe**
			500 records or

			more
			Less than 500 records
			Low Level

	[illegible]	[illegible]	**Incident [illegible]** [illegible] **Medium Level Incident [illegible]** [illegible] **High Level Incident [illegible]** [illegible]	

IR-7 – Incident Response Assistance (Moderate)	
Control **NIST SP800-53 rev3:** **IRS 1075 rev2010:** **CJIS v5.1:** **HIPAA:** **PA CHRIA:** **state ITB:** **PCI DSS: 12.9.3**	
Fully explain control implementation *(or fully explain why control requirement is not applicable)* **Status: Implemented**	**Responsible for Control Implementation**

IR-8 – Incident Response Plan (Moderate)

Control
NIST SP800-53 rev3:

IRS 1075 rev2010:

CJIS v5.1:

HIPAA:

PA CHRIA:

state ITB:

PCI DSS: 12.9.1

-
-
-
-
-
-
-

12.9.2

12.5.3

Fully explain control implementation *(or fully explain why control requirement is not applicable)* **Status: Implemented**	**Responsible for Control Implementation**

A	

7.5 MAINTENANCE (MA) FAMILY

The description of datacenter's MA process and technology solutions

7.6 MEDIA PROTECTION (MP)

The description of datacenter's MP process and technology solutions

7.7 PHYSICAL AND ENVIRONMENTAL PROTECTION FAMILY (PE)

The description of datacenter's PE process and technology solutions

7.8 PERSONNEL SECURITY (PS)

The description of datacenter's PS process and technology solutions

7.9 SYSTEM AND INFORMATION INTEGRITY (SI)

The description of datacenter's SI process and technology solutions

8 DATACENTER TECHNICAL SAFEGUARDS AND CONTROLS

8.1 ACCESS CONTROL (AC)

The description of datacenter's AC process and technology solutions

8.2 AUDIT AND ACCOUNTABILITY (AU)

The description of datacenter's AU process and technology solutions

8.3 IDENTIFICATION AND AUTHENTICATION (IA)

The description of datacenter's IA process and technology solutions.

8.4 SYSTEM AND COMMUNICATIONS PROTECTION (SC)

The description of datacenter's SC process and technology solutions

9 APPENDICES AND ATTACHMENTS

End of Document

3. Technical Infrastructure

Technical Infrastructure Clarification

During the Orals phase, the Unisys Team received several questions around our x86 Technical Infrastructure. As a result, we have made several revisions and enhancements to our Technical Submittal focused on clarifying our x86 Technical Infrastructure offering. The Unisys team has updated our proposal with additional information on the IBM Flex System which is a core component of the x86 (Windows and Linux), iSeries and AIX infrastructures.

Unisys is an authorized reseller of VCE's VBlock Technology. Based on the Commonwealth's complete datacenter and technology requirements in this RFP, Unisys performed a detailed analysis between the IBM x86 Flex systems blade technologies and VCE's VBlock Technology. After reviewing the results, we selected the IBM Flex systems as their technology was deemed superior in meeting the requirements of this RFP. The details of our analysis and clarifications on our x86 technology offering is found in this Tab.

In addition, the Unisys Team has updated the IBM storage and tape references to the IBM DS8800 disk storage system and TS7700/TS3500 tape library system.

Our revised responses for the identified Requirements in the Schedules or Sections listed below are included in this tab.

Tab	Schedule or Section	Requirements
3	Schedule F Section 3.2.2.2 Infrastructure Architecture	1A and 1B

This page intentionally left blank.

3.2.2.2 Infrastructure Architecture

The Infrastructure Architecture service will define and manage the scope and design of the infrastructure architecture for the computing systems to support the evolving needs of the Commonwealth. This range of Services includes design of the mainframe, mid-range, x86 servers, (both physical and virtual), Local Area Network (LAN), storage, backup systems, and the DR systems. The design will also need to detail how the most current data will be restored to the targeted DR system.

Efforts are underway to re-write many of the Commonwealth business applications. For example, some of the mainframe applications are being migrated to newer server-based systems. The Offeror must consider the planned retirement of some of the mainframe workload, and at the same time consider the offsetting growth in other server platform environments.

At the direction of the Commonwealth, the Offeror must transition Commonwealth-based computing infrastructure to one of the datacenters. The Offeror must work with the Commonwealth agencies to understand the systems involved, and the timeframe of these migrations. Working with the Commonwealth agencies, the Offeror must provide the design, project management, hardware and technical support required to test and migrate these systems to the new production environment. At its discretion, each agency will provide the applications staff to support the migrations.

The Infrastructure Architecture service will review and recommend hardware, software, and the technical configurations required to build the requested infrastructure environments. Prior to migrating each of the current application workloads to the new target infrastructure, the Offeror must work with each Commonwealth agency to develop a mutually agreed to Acceptance Test Plan that includes the testing of application infrastructure performance characteristics.

Reference Documentation

Exhibit A - Commonwealth Network Environment

Exhibit(s) B.1 through B.6 - Data PowerHouse (DPH) Exhibits

Exhibit(s) C.1 through C.13 - Department of Public Welfare (DPW) Exhibits

Exhibit(s) D.1 through D.15 - Enterprise Datacenter (EDC) Exhibits

Exhibit(s) E.1 through E.43 - Department of Labor & Industry (DLI) Exhibits

Exhibit(s) F.1 through F.4 - Department of Health (DOH) Exhibits

Exhibit(s) G.1 through G.16 - PA State Police (PSP) Exhibits

Exhibit(s) H.1 through H.8 - Department of Revenue (DOR) Exhibits

Exhibit(s) I.1 through I.13 - Commonwealth SAP Environment - Integrated Enterprise Services (IES) Exhibits

Exhibit L - Master Application Inventory

Schedule J.1 - Datacenter Service Level Management

Exhibit(s) M.1 through M.7 - Department of Corrections (DOC) and Pennsylvania Board of Probation and Parole (PBPP) Exhibits

Exhibit(s) N.1 through N.2 - PennDOT Exhibits

	Requirements	**Describe Compliance**
1.	Define the infrastructure technology Services to be offered. Provide a detailed list of Services and computer platforms to be provided to the Commonwealth.	Offeror must describe its ability to provide infrastructure technical Services across multiple computing platforms (mainframe, mid-range and x86). Include explanation of different service tiers (e.g. gold, silver and bronze).
2.	Design and build the IT infrastructure architecture to support the Services required by the Commonwealth. Design will provide as much interoperability and open standards as possible. All designs must be approved by the Commonwealth. Provide the design in a Visio format to the Commonwealth for review and approval prior to execution. This diagram will be dated and maintained as Services are altered for the duration of the engagement.	Offeror must describe its methodology and approach to infrastructure architecture design Services. Offeror must describe the documentation requirements, timelines for both normal requests and emergency situations. Offeror must provide representative sample of infrastructure design documentation.
3.	Address CJIS and Criminal History Record Information Act (CHRIA) requirements for agency application infrastructure designs where required. Some agency application infrastructure designs (e.g. PSP) require additional security and encryption level requirements imposed by CJIS.	Offeror must provide examples of its experience in designing infrastructures that adhere to CJIS and CHRIA requirements.
4.	SAP Infrastructure Design The Offeror's proposed target	Offeror must provide examples of its experience in sizing and design of SAP

	infrastructure design for the Commonwealth's SAP environments must include a certified SAP sizing report prior to migration of the systems.	infrastructures. All designs must be approved by the Commonwealth.
5.	Commonwealth Wide Area Net connectivity. Provide connectivity from the datacenter to the Commonwealth Network. Redundant network links are required.	Offeror must describe its capabilities to connect to and manage the requisite connections. Explain ongoing network support Services to manage these links including the ability to increase capacity as needed to support changes in the application infrastructure requirements.
6.	Develop Acceptance Test Plan. Prior to migrating each of the current application workloads to the new target infrastructure, the Offeror will work with each Commonwealth Agency to develop a mutually agreed to Acceptance Test Plan that includes the testing of application infrastructure performance characteristics.	Offeror must discuss its proposed approach to systems acceptance testing and include the approach to performance testing.
7.	Provide System Acceptance testing. The Offeror must conduct system acceptance testing, and provide the Commonwealth with written verification prior to declaring the system is fit for use. This acceptance test must include validation of infrastructure performance against system performance characteristics agreed to by both parties.	Offeror must discuss its proposed approach to systems acceptance testing.
8.	Ready for use certification	Offeror must provide the Commonwealth with written verification prior to declaring the Service is ready for use. The Service will not be considered ready for use until written acceptance is obtained from the

		Commonwealth.
9.	Support User Acceptance Testing.	Offeror must support the Commonwealth's user acceptance testing. The Commonwealth shall not be charged for Services until written acceptance is obtained from the Commonwealth.
10.	Provide Application Infrastructure environments. Provide non-production and production environments for each of the application computing platforms. The non-production environments will be used for testing new technologies and applications, updates and upgrades, prior to production implementations.	Offeror must describe its approach to the design and management of multiple application infrastructures. Identify proposed solution to individual or consolidated non-production environments for agencies.
11.	Design service lifecycle. Provide the infrastructure design for the Services and platforms to be offered. Provide ongoing evaluation and recommend new technologies to enhance, improve, and reduce the cost of Services.	Offeror must describe its approach to provide service lifecycle design for all Commonwealth computing platforms and associated infrastructures. Offeror must provide the Commonwealth and its agencies the ability to request new technologies to be available.
12.	Define Technical Support functions.	Offeror must list Offeror's support staff levels required to plan, manage, and operate the IT infrastructure, based on the various service levels offered.
Continual Service Improvement		
13.	Reduce service risks.	Relative to the service in question, Offeror must provide examples of previous Offeror initiatives aimed at eliminating or mitigating service risks.
14.	Improve service quality.	Offeror must provide examples of previous Offeror initiatives aimed at improving service quality.

15.	Improve client satisfaction.	Offeror must provide examples of previous Offeror initiatives aimed at continually improving client satisfaction.
16.	Provide service transparency.	Offeror must provide examples of previous Offeror initiatives aimed at providing service transparency; in particular, visibility into the service execution process.
17.	Ensure service sustainability.	Offeror must provide examples of previous Offeror initiatives aimed at ensuring service sustainability; in particular, efforts targeted at cost containment and cost reductions.
18.	Improve/reduce cost of service	Offeror must provide examples of previous technology initiatives implemented by Offeror that achieved reduced costs of Services and that met or exceeded ROI (Return on Investment) analysis projections.

Deliverables

Deliverables are defined in **Schedule K - Key Program Deliverables**

Offeror Response

1 Infrastructure Service Tiers

1.A Define the infrastructure technology Services to be offered.

The Unisys Team offers a solution that provides these managed infrastructure technology services:

- Unisys OS2200
- Unisys Libra
- IBM zSeries
- IBM iSeries
- Network
- Security
- Server/Midrange
- Storage
- Backup
- Disaster Recovery
- IaaS Services
- Data center Facilities

1.B Provide a detailed list of Services and computer platforms to be provided to the Commonwealth.

Figure 3.2.2.2-1 below shows the computer platforms the Unisys team will deploy as part of the Infrastructure Architecture services. Following, there is a description of each of the technologies, and overview of how the Unisys team will utilize those solutions. For your convenience, we also provide references to other sections of proposal if additional information is required.

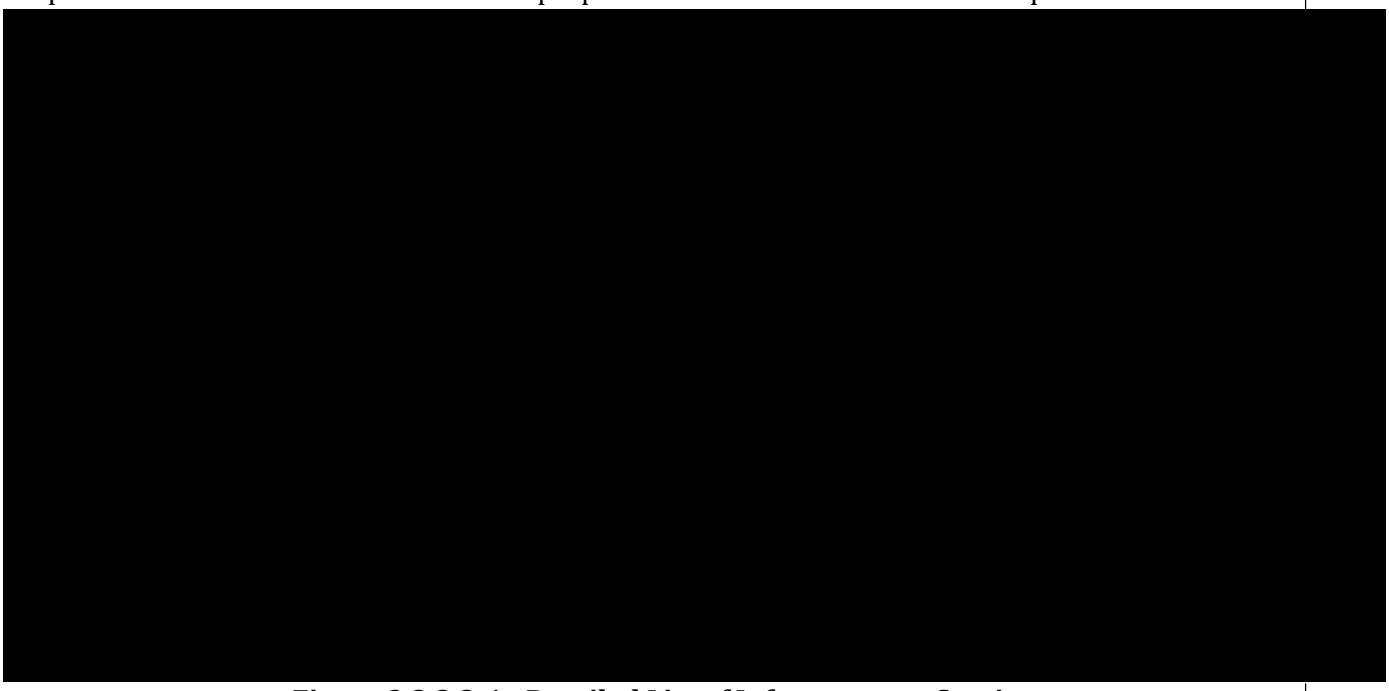


Figure 3.2.2.2-1 - Detailed List of Infrastructure Services

- [redacted] – The [redacted] blade technologies will be utilized by the Unisys team to provide all x86 server services to the Commonwealth. The Unisys team evaluated several platforms for hosting the Commonwealth's server infrastructure, including VCE's VBlock Technology. Unisys found that the [redacted] infrastructure was superior in every significant area of comparison, as detailed below.

A high level comparison chart between [redacted] and [redacted] is shown in **Table 3.2.2.2-1**.

Table 3.2.2.2-1 – [redacted]

Comparison At A Glance	IBM Flex Systems	VCE VBlock
Supports Microsoft Windows	✓	✓
Supports Linux	✓	✓
Supports IBM AIX	✓	

Supports IBM iSeries	✓	
Supports VMWare	✓	✓
Supports Microsoft HyperV	✓	
Supports KVM	✓	
Supports IBM PowerVM	✓	
Supports East/West Traffic For Reduced Network Latency	✓	
Supports Trusted Compute Base and Trusted Platform Module	✓	

- Flexibility and expandability – [redacted] can host AIX, IBM I series, Linux and Windows servers, both virtualized and physical. Additionally, a higher blade density means 1/3 less data center floor space for equivelant CPU counts. Expanding the Flex System is easier because the system is not locked down, thus storage, network and compute node can be expanded separately, as opposed to VBlock, which requires all three to be upgraded at once. Lastly, [redacted] allows for components to apply updates and patches separately, meaning less impact to users. VBlock updates and patching are locked down, and are required to be applied all at once, and only after VCE releases them, meaning all systems are upgraded, whether the underlying workloads are ready for them or not. This increases the risk of critical security and system patches being delayed and greater user impact.

- Performance – [redacted] blades do not have to route traffic to top of rack switches to communicate with other blades. Utilizing east/west communications, Flex Systems significantly reduces communication latency between compute nodes.

- Compute Power – SPECint benchmark testing data shows that [redacted] compute nodes are 9% faster than equivalent VBlock compute nodes. SAP SMP benchmark testing also shows that [redacted] AIX blades can support 10,000 users, as opposed to 6,500 for VCE VBlock.

- Virtualization Support – [redacted] support all major virtualization platforms the Commonwealth lists in this RFP (VMware, Microsoft's HyperV and IBM's AIX based PowerVM) as opposed to the homogenous VMWare environment of the VBlock platform.

- Security – [redacted] utilizes the Trusted Computing Base and Trusted Platform Module to prevent access to system level resources and system controllers, blocking these resources as a means to access operating systems and hypervisors. Additionally, all intra-chassis, east/west communications are

encrypted.

- o Ease of Management – [redacted] is a highly integrated management tool that can manage the entire [redacted] infrastructure, from low level components such as fans and power supplies through the hypervisor to the storage, compute and network components, the [redacted] provides single pane of glass management of AIX, Linux, IBM iSeries and Windows workloads, both physical and virtual, increasing value and cost savings to the Commonwealth.

The [redacted] form the infrastructure for both virtualization and physical servers. Utilization of this technology provides the Commonwealth with increased power, agility, and performance at a lower cost, able to meet the compute needs of the Commonwealth now and into the future. For more information on how the Unisys team will utilize [redacted] please refer to Schedule F, Sections 3.2.4.1, Windows Support; 3.2.5.1, Server Capacity on Demand, and the Linux section of 3.2.4.4 Unix Support.

- [redacted] is an AIX variant of the [redacted] line of blade servers. The Unisys team will deliver all AIX services referenced in this RFP on this platform. Combined with the x86 Flex System blades, the Unisys team brings to the Commonwealth the unique ability to co-locate AIX, Linux and Windows workloads in the same blade chassis, driving down management and deployment costs for the Commonwealth. For more information on the use of the [redacted], please see Schedule F, Section 3.2.4.4 Unix Support.

- [redacted] is a CMOS processor based mainframe which the Unisys team will utilize to deliver Unisys mainframe services to the Commonwealth. Please see Schedule F, Section 3.2.4.5 Mainframe Support for more information.

- [redacted] is an x86 processor based mainframe which the Unisys team will utilize to deliver Unisys mainframe services to the Commonwealth. Please see Schedule F, Section 3.2.4.5 Mainframe Support for more information.

- [redacted] is the mainframe on which the Unisys team will deliver both IBM mainframe and zLinux services to the Commonwealth. Please see Schedule F, Section 3.2.4.5 Mainframe Support for more information.

- [redacted] designed for high performance, reliability, and flexibility and will be utilized by the Unisys team to provide storage to the [redacted] mainframe. Please see Schedule F, Section 3.2.4.5 Mainframe Support for more information.

- [redacted] is a high-end disk storage system designed to provide consistent performance, high availability and simple usability. The [redacted] will be one of the storage platforms the Unisys team will utilize to deliver storage services to the Commonwealth. Please see Schedule F, Section 3.2.4.2 Storage Management for more information.

- [redacted] provides storage virtualization by presenting itself to server hosts as a storage device, and to storage devices

as a server host. Utilization of the [redacted] brings power and agility to the Commonwealth at the storage layer, and compliments the virtualization at the server layer. Please see Schedule F, Section 3.2.4.2 Storage Management for more information.

- [redacted] is a virtualization engine (virtual tape library) for [redacted] mainframes that uses disk drives for cache to accelerate backup operations. The design is intended to protect data while having shorter backup windows. End-to-end encryption protects data in motion, on cache hard drives and on tape. Please see Schedule F, Section 3.2.4.2 Storage Management for more information.

- [redacted] system is an enterprise class storage system, used by the Unisys team to deliver storage to open systems and [redacted] mainframes. Please see Schedule F, Section 3.2.4.2 Storage Management for more information.

- [redacted] storage devices provide both file and block storage services. The Unisys team will utilize the [redacted] as one of the storage options available to the Commonwealth through the Enterprise Services Catalog. Please see Schedule F, Section 3.2.4.2 Storage Management for more information.

- [redacted] – The Unisys team will utilize [redacted] as one of the options to provide the Commonwealth tape based backup and recovery services. Please see Schedule F, Section 3.2.4.2 Storage Management for more information.

- [redacted] will be used by the Unisys team to deliver [redacted] services for the [redacted] mainframes. Please see Schedule F, Section 3.2.4.2 Storage Management for more information.

- [redacted] is equivalent in many ways to the IBM SAN Volume Controller, capable of storage virtualization and replication of data and virtual machines across data centers. The Unisys team will use [redacted] as one of the storage service options for the Commonwealth. Please see Schedule F, Section 3.2.4.2 Storage Management for more information.

- [redacted] is a continuous data protection solution offered by [redacted] which supports asynchronous and synchronous data replication of block based storage. Please see Schedule F, Section 3.2.4.2 Storage Management for more information.

- [redacted] – The Unisys team will utilize [redacted] to perform de-duplication of disk based backup. Please see Schedule F, Section 3.2.4.2 Storage Management for more information.

- [redacted] will be utilized by the Unisys team to provide tape based backup and recovery services to the Commonwealth. Please see Schedule F, Section 3.2.4.2 Storage Management for more information.

- [redacted] will be utilized by the Unisys team to provide tape based backup and recovery services to the Commonwealth. Please see Schedule F, Section 3.2.4.2 Storage Management for more information.

- [redacted] – [redacted] will be utilized by the Unisys team to provide tape based backup and recovery services to the Commonwealth. Please see Schedule F, Section 3.2.4.2 Storage Management for more information.

- [redacted] – [redacted] a web-filtering, content caching internet perimeter security device for large enterprises. The Unisys team will deploy Blue Coat Proxy to provide internet security and content filtering to the Commonwealth. Please see Schedule F, Section 3.1.2 Network and Security Architecture.

- [redacted] – [redacted] is a distributed sniffer system. The Unisys team will utilize [redacted] to quickly analyze problems on the network or to isolate problems specific to an application. Please see Schedule F, Section 3.1.2 Network and Security Architecture.

- [redacted] – Long recognized as a leader in data center networking, the Unisys team will utilize [redacted] routers and switches to provide the Commonwealth LAN and WAN services. Please see Schedule F, Section 3.1.2 Network and Security Architecture.

- [redacted] – The Unisys team will deliver network firewall services to the Commonwealth using Juniper Firewalls. The [redacted] firewalls chosen by the Unisys team allow advanced functionality at the firewall layer. Please see Schedule F, Section 3.1.2 Network and Security Architecture.

- [redacted] – The [redacted] deployed by the Unisys team will offer the Commonwealth ubiquitous load balancing of applications across data centers. Please see Schedule F, Section 3.1.2 Network and Security Architecture.

4. Operational Efficiency Revisions

We are also proposing a number of technical changes that improve operations while providing efficiencies. These Technical improvements and clarifications are summarized below.

Transition

As part of an effort to continue to refine the Transition Plan we were able to accelerate the migration from the DPH to the new data center to 12 months without a measurable increase in risk. With this revised timeline, we will now eliminate a DPH contract extension if the transition can begin prior to January 2014. We were hopeful before submission of our proposal that such an aggressive timeline could be met but the extra time for the BAFO process allowed us to confirm acceleration was achievable with limited additional risk. We also were able to reevaluate the other data center transitions as well and now are committing to their full transition by Month 18. In summary, the EDC will be completely transitioned within 6 months. DPH would be fully transitioned in 12 months; all agency data centers within 18 months. The details on the changes for the Transition Plan are provided within the Work Plan, Section 3.0 and related updates are located in the following indicated sections.

Our revised responses for the identified Requirements in the Schedules or Sections listed below are included in this tab.

Tab	Schedule or Section	Requirements
4	Section 3.0 Work Plan	3.1.2, and 3.2-3.2.2
4	Section 2 Management Summary	2.5
4	Schedule F Section 3.3.2.1 Transition Program Management	3A, 6C, 7B, 9A
4	Schedule M - Transition Plan	Transition Schedule and Detailed transition plan

2+ Data Center Architecture

The Unisys Team refined the 2+ Data Center architecture approach by redefining the services provided by the Unisys [redacted] data center and its network connectivity. This modification simplifies the planning and migration activities for the DPH and individual agency data centers during Transition while maintaining the flexibility to meet changing business needs. As a result of these modifications, the sections in the table below have been updated to reflect that production, Capacity on Demand, and disaster recovery services are available from the [redacted] and EDC Data Centers.

The EDC in Harrisburg, PA is the designated disaster recovery site for Unisys and IBM mainframe services, should the Unisys [redacted] facility become unavailable. Unisys' [redacted] data center remains available for Capacity on Demand services and to further enhance disaster recovery services if the Commonwealth's business or policy needs change or there

is a need for greater than 90 miles of geographic separation. In addition, the IBM Sterling Forest disaster recovery subscription service for the IBM Mainframe is also available through a service request. Therefore there is a full menu of additional services available should the Commonwealth's need change or a horrific event cause a broader disaster recovery response. Details about the changes to disaster recovery are provided in the following sections.

Our revised responses for the identified Requirements in the Schedules or Sections listed below are included in this tab.

Tab	Schedule or Section	Requirements
4	Schedule F Section F.3.1.1 Multi-Datacenter Environment	4A, 7A
4	Schedule F Section 3.2.1.5.2 IT Service Continuity Architecture	3A

Data Loss Prevention

The Unisys Team has decided to use McAfee Data Loss Prevention in place of Symantec Data Loss Prevention. Post submission of our proposal we re-examined our selection against the Commonwealth's goal of integrating new products with existing Commonwealth products to provide the benefits of full integration, reduced risk and lower costs. The McAfee DLP met all of these criteria and therefore we decided to make this our product of choice. Now McAfee DLP will integrate with the Commonwealth's antivirus and malware management tools, as well as reduce risk and operating costs. **All references to Symantec security products, such as DLP, Antivirus, or Malware in the Unisys RFP response are considered changed to the related McAfee product.**

Backup Software

The Unisys Team has also changed its product for backup services. The new product being proposed is EMC Networker. It replaces Commvault Simpana. EMC Networker is a proven solution at the Commonwealth and has been leveraged at the EDC since its inception. We see value keeping a product that has been used successfully by the Commonwealth for many years. Using the EMC product should help reduce risk during transition and provide operational efficiencies longer term. A detailed explanation of EMC Networker is included in the attached Schedule F Section F.3.2.4.2 (Storage Management). **Any references to Commvault, Simpana or Commvault Simpana in the Unisys RFP response are now considered EMC Networker.**

Our revised responses for the identified Requirements in the Schedules or Sections listed below are included in this tab.

Tab	Schedule or Section	Requirements
4	Section 3.2.4.2 Storage Management	Introduction, 1B, 4B, 4G, 7A, 13A, Benefits to Commonwealth
4	Section 3.2.4.7 Database Management Services	1A, 2A

3.0 Work Plan

3. WORK PLAN (RFP REQUIREMENT II-3) 3-3

3.1 WORK PLAN OVERVIEW 3-3
3.1.2 Work Plan Description 3-3
3.2 DETAILED TASK PLAN 3-9
3.2.1 Transition Services 3-10
3.2.1.1 Account Organization 3-11
3.2.1.2 Enterprise Data Center (EDC) to Managed Services Model 3-12
3.2.1.3 Tools Implementation 3-13
3.2.2 Application Workload Migrations 3-13
3.2.2.1 Operational Readiness 3-14
3.2.2.2 Agency Application Workload Migrations 3-15

This page intentionally left blank.

3. Work Plan (RFP Requirement II-3)

RFP	*Requirement*
II-3	*Work Plan. Describe in narrative form your technical plan for accomplishing the work. Use the task descriptions in Part IV of this RFP and Schedule F as your reference point. Modifications of the task descriptions are permitted; however, reasons for changes should be fully explained. Indicate the number of person hours allocated to each task. Include a Program Evaluation and Review Technique (PERT) or similar type display, time related, showing each event. If more than one approach is apparent, comment on why you chose this approach.*

3.1 Work Plan Overview

3.1.2 Work Plan Description

The program activities have been designed in three primary parts or phases: (1) Transition, (2) Migration, and (3) Steady State Operations, which is expected to be achieved by Month 18 of the program schedule. The overall program is supported by a program management framework which includes detailed planning, effective communication, and status tracking. This section includes a high level narrative of our proposed work plan along with selected pictures of the detailed work plan which is included in Attachment 9 to Section 3.0 – Schedule M. This section also includes details on the Unisys methodology that was used to design our proposed program plan and will be used to refine it based on Commonwealth feedback.

Transition activities build the foundation that the steady state organization needs to function including development of the final organizational plan, the communications plan, the financial management plan, and the development of policies and procedures, which will govern and guide the program's steady state operation. This activity sets plans and executes the transition from the current steady state operations model to the new operating model.

Transition consists of projects and tasks that will be executed to support the implementation of the resources, processes, procedures, and tools required to effectively deliver steady state data center compute services to the Commonwealth. In other words, we will create the IT service management infrastructure to support the new environment's hardware and software infrastructure. Transition will be broken further into smaller projects such as Tools Implementation, Transition of Services, and Service Desk Implementation. Examples of these types of activities include the enhancement to support the expanded scope for the BMC Remedy system, implementation of revisions to Service Management processes like change management, hiring and training of transition PMO staff, and knowledge transfer for implementation of Managed Services. In this phase, we will leverage our significant knowledge and broad experience with the Commonwealth to speed this process.

Migration activities focus on the relocation and provisioning of both the physical infrastructure and planned movement of applications to the target platforms. The re-envisioning of the current DPH, EDC, and incorporation of agencies currently outside the managed services contract will be planned, focused teams will be established to address each migration, and they will execute the individual actions required to accomplish the migration.

Migration will be comprised of activities that prepare the receiving data centers for the migration of applications, often called Infrastructure Readiness, as well as projects that will migrate applications and their data from Commonwealth Data Centers to Unisys facilities. The projects will be organized around migrating applications from each data center and be broken into manageable sizes. For example, the DPH Data Center will be broken into approximately nine smaller projects with scope based on inter-application dependencies, number of servers, and applications.

Transition Program Management activities consist of tasks that the Transition Program Office will execute to improve each project's performance in quality and performance to schedule. This will include tasks such as quality reviews; gathering and distribution of lessons learned, status meetings, and reports; and oversight of the project schedule rollup. Key attributes of these tasks are consistency, sharing, adjustments, and oversight.

As the incumbent vendor, Unisys will continue to provide outstanding service to the Commonwealth's mission-critical application infrastructure hosted in the DPH and staff augmentation services to the operations in the EDC until each location is fully transitioned to the new model. Our incumbency provides us with the uncommon ability to seed the

transition and migration teams with knowledgeable resources who understand the Commonwealth infrastructure, considerably reducing ramp-up time training staff on basic infrastructure support and each agency's priorities and nuances. It is during this time that we will accelerate our focus on reforming our organizational structure and work processes to meet the new model's changing requirements.

Once the transition activities conclude, **Steady State Operations** begins using the new operating model, which is developed during the Transition and Migration phases. Continuous Service Improvement activity commences during this phase providing opportunities to assess, design, and implement changes to the program processes to increase the value of the services to Commonwealth.

Table 3-1 below shows a projection of the work effort required to complete the transition by major activity.

Table 3-1. Transition Work Effort by Major Activity

Task Activity	Total Person Hours Allocated
Transition Project Management	42,705
Transition of Services	157,186
Tools Implementation Project	18,784
Infrastructure Readiness Project	45,869
Application Workload Migrations	56,998

The following Gantt chart shown in **Figure 3-2** provides a very high-level view of the timelines for the overall activities of this program.

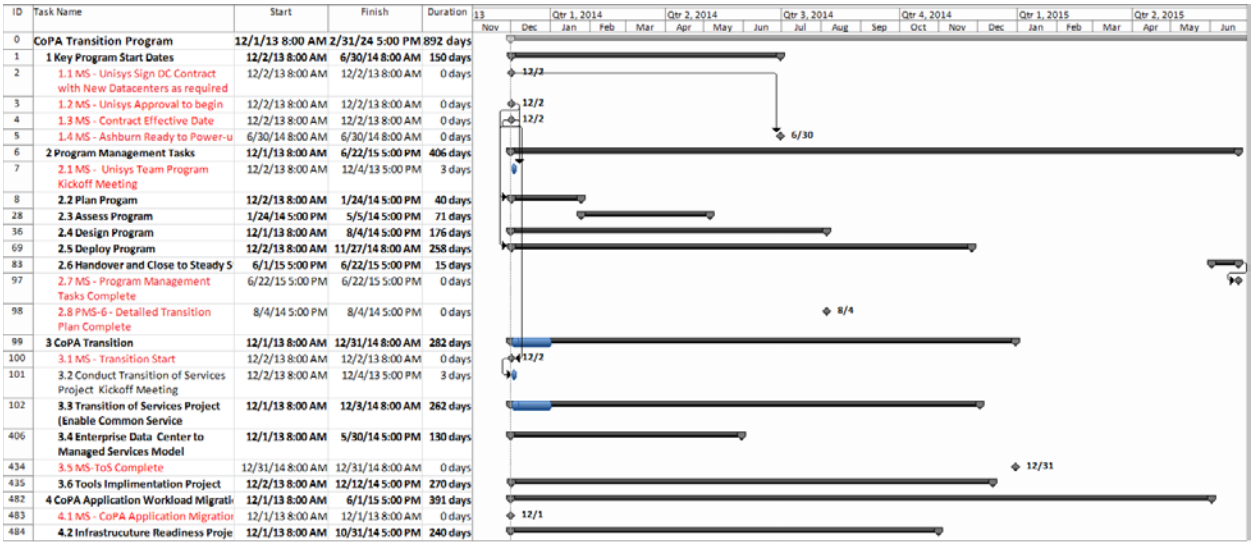


Figure 3-2. High-level Schedule of the Commonwealth's Transition Program

Transition Program Management Office – Project Start up

During **Month 1** of the program, much focus will be placed on program startup and long lead-time activities such as placing orders for the establishment of the telecommunications infrastructure. Executive planning sessions will be held to confirm a common understanding of scope, priorities, and timing. The Unisys Team will work with the Commonwealth to begin reviews and joint planning sessions for the Transition of Services, Tools Implementation, and Operational Readiness, which are critical to the EDC's transition to a Managed Services model. Unisys, IBM, and Deloitte are in the exceptional position to be able to leverage existing knowledge to expedite the turnover to the Unisys Team. Also, our account architecture team will create the architecture deliverables and review them with the Commonwealth to allow for long lead-time items such as circuits, core network equipment and storage, x86, AIX, and mainframe 'seed' equipment to be ordered.

During **Month 1** we bring key personnel on board to support the new contract starting with our Engagement Executive, [redacted] our Transition Executive, [redacted] our second Transition Manager, [redacted] and our Senior Enterprise Infrastructure Architect, [redacted] We will backfill positions currently held by Ann and Dave on the DPH contract.This team will lead all aspects of the transition efforts. We will also bring on our Service Excellence Officer, [redacted] to build our Service Excellence Office that will initially reform workflows of existing ITIL V3-aligned processes to meet the new services model requirements.

Transition Assessment and Data Gathering

Months 2 and 3 will contain many design and data gathering activities. We will begin the Tools Implementation tasks. The data center migration teams will begin analyzing the data collected from the BMC Atrium Discovery and Dependency Mapping (ADDM) tool to create move packages. Move Packages are defined as a group of dependent applications and data across several infrastructure components. We will conduct initial planning sessions with the Commonwealth stakeholders to solidify the order and timing of data center migrations. During this period, our key personnel will acclimate, and our Transition Program Management Office (TPMO) will be taking shape. As we move into Month 2, a team will begin detailed planning on the EDC's transition to quickly facilitate the transition to the Managed Services model.

It is also during **Months 2 and 3** that our executive leadership will work with Commonwealth executive leadership to solidify our approach to governance, communication, and reporting for steady state ongoing services, which will begin from the day an application is migrated to a Unisys Data Center, or workload in the EDC transitions to the managed services model. As dates are assigned to move packages, we will finalize the specific staff transition timeline for moving existing staff with Commonwealth knowledge to the new contract and we will start infusing our teams on both sides with new resources from IBM, Deloitte, and our SDB partners. We will on-board our Agency Account

Managers to acclimate the agencies to the changes in procedure and the support organization between the existing contract and the new model.

Transition Program Development – Process/Tool Refinement and Implementation

Many contract milestones will be completed in **Months 4 through 8.** To accomplish these milestones, we will complete the implementation and integration of the ITSM System with the Commonwealth ITSM system along with drafting of the CCPM. The ITIL V3 processes will be finalized and rolled out to the team. The Unisys Data Center core infrastructures will be installed, tested, and connected to COPANET, which will result in operational readiness. Early in this period, the Data Center Migration Teams will begin detailed planning on the DPH migration to facilitate complete migration within 12 months. The Unisys Team will initiate training of the Commonwealth stakeholders that will cover many aspects of the contract, operational procedures, and review of strategy and plans aligned with program key deliverables.

At this time, the Unisys Team will complete the transition of the Enterprise Data Center from the current staff augmentation model to the new managed services model. Existing Unisys Team members augmented with additional staff will completely assume the site's management responsibilities. After the Enterprise Data Center is operating in the steady state, agencies with applications hosted in the EDC can order additional services through the Enterprise Services Catalog and change order processes, and the Unisys Team will be accountable for Service Level Agreements (SLAs) within the EDC under the new contract.

DPH, DOR and DLI Application Workload Migration

Months 6 through 12 will focus almost exclusively on detailed planning and executing the DPH migration. To achieve this, Unisys, IBM, and the Commonwealth will work closely to plan the migration projects. The Unisys Team will be augmented with additional project management and technical resources that will perform migration tasks directly, or backfilling DPH team members who will be reassigned to provide a strong foundation of knowledge and experience to the DPH migration effort. The Commonwealth will verify the move packages that were identified by the Migration Team, develop and refine test plans for each application, and participate alongside the Unisys Team throughout the project to deliver a successful move. During this period, the Migration Team will put a strong communications strategy in place and plan to enable all stakeholders to have access to schedules and project plans. Unisys will develop a communications cadence of notifying affected users 30, 7, and again 2 days before any significant events such as re-IP events (if necessary) and move events.

Because the DPH will be migrated in at least nine separate move packages, an agency could have application infrastructure managed at the Willow Oak Data Center and the Unisys Data Center concurrently. As the migration move packages are relocated to the Unisys Data Center and the application infrastructure for each application is operating in the steady state, agencies with applications hosted in the Unisys Data Center can order

additional services through the Enterprise Services Catalog and Change Order processes, and the Unisys Team will be accountable for SLAs under the new contract. For all application infrastructures that remain at the Willow Oak Data Center, the Unisys Team will be accountable for SLAs under the current DPH contract until the infrastructure is relocated to the Unisys Data Center. By **Month 12**, the Unisys Team will complete the migration of the Data PowerHouse agency application infrastructure from the Willow Oak Data Center to the Unisys Data Centers.

The Department of Revenue (DOR) Data Center Migration is also included in this wave to avoid over allocation of DOR resources during its busy personal tax season.

DLI was chosen for this wave due to its size and complexity. The planning and execution of this move will complete by **Month 16**. IBM will take the lead on this migration because of its knowledge and experience with the Department of Labor & Industry (DLI).

At the end of **Month 12**, the DPH contract will officially expire, and all relevant staff supporting the existing DPH and EDC workloads will have transitioned to the new contract.

Agency Application Workload Migration – PSP, DOH, DPW

In **Months 13 through 18,** the migration team will plan and relocate the applications within the Pennsylvania State Police (PSP) ,Department of Health (DOH) and Department of Public Welfare (DPW) Data Centers. Again, we took the time of year into account for the PSP Data Center migration. This wave is intended to begin planning in December of 2014 and complete in May 2015, which will avoid busy summer and year-end holiday months.

As each agency application migration completes, the Unisys Team will officially assume responsibility for providing managed services to the agency from the Unisys Data Center, and when operational in steady state, the Unisys Team will be accountable for the achievement of service level commitments.

As Unisys and the Commonwealth conduct detailed Migration Planning the order and combinations of data centers by wave may change as we continue to refine the planning and movement of the various agencies' infrastructure.

After transition and migration are complete, our fully populated steady state organization, processes and tools will be fully deployed and operating in the new environment. New capabilities of capacity on demand, self provisioning, an expanded Service Desk capability, and ITIL V3 processes will be available and in use by this time. Further details of the transition from the current state to the new state of the Commonwealth's compute environment can be found in the following sections; a thorough discussion of the topic is provided in **Schedule M.**

3.2 Detailed Task Plan

The Unisys Work Plan is focused on the accomplishment of transition, migration, and steady state. Transition begins with a series of projects, tasks, and activities. Transition includes the required steps to implement a managed services model. Our Team will work closely to design and implement the processes, tools, and organizational structures required to deliver continuous services to the Commonwealth and stakeholders. The work products from these services will support the PMO and the rest of the team during execution of ongoing operations. A key element of the transition is transfer and implementation of the Unisys standard management toolset. This includes BMC Remedy ITSM, (Nagios) for monitoring, and BMC's Atrium Discovery and Dependency Mapping (ADDM) tool.

Our team will work with the Commonwealth to identify a technology refresh plan for existing hardware in the EDC during the EDC transition. Unisys will work with the Commonwealth to address a continuance of hardware maintenance until the infrastructure is replaced.

The daily TPMO operations will be tightly aligned with the PMO operations. [redacted] and her executive leadership team will drive effective handoffs of transition projects to the steady state. For transition architecture strategy and support, the TPMO will interface directly with the Senior Enterprise Infrastructure Architect, [redacted] and his team of Agency Infrastructure Architects.

Figure 3-3 shows the proposed Level 2 schedule for the Commonwealth's Transition Program.

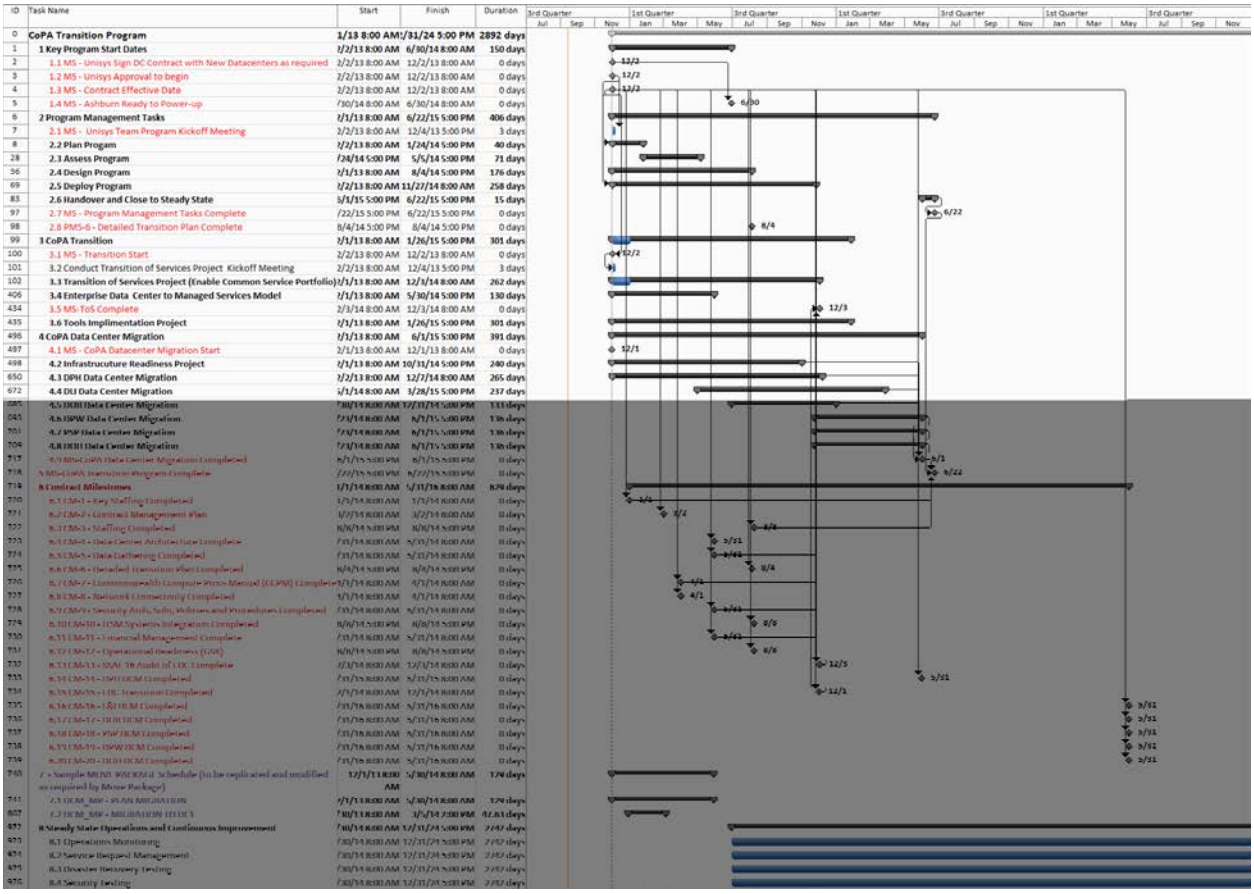


Figure 3-3. Level 2 Schedule of the Commonwealth's Transition Program

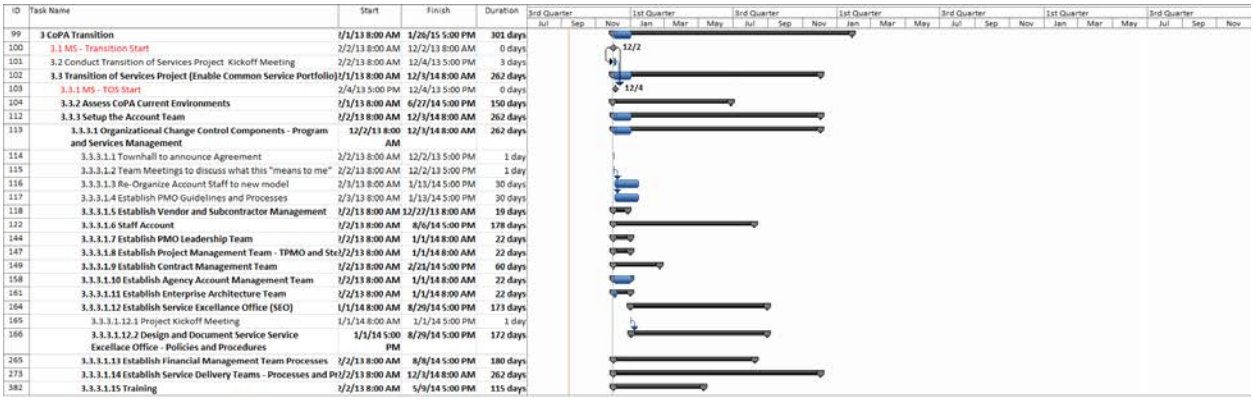
Our approach on transition timing was developed with the Commonwealth's goals in mind. Our initial focus is on transition of the EDC to a managed services model followed by data center migrations to move agency applications from the Willow Oak Data Center to a Unisys Data Center. These priorities will enable the Commonwealth to transition all obligations under the current DPH contract to the new data center compute services contract. In parallel, we are focusing on the accomplishment of key program deliverables within specified time frames. Remaining agency migrations will then take place between Months 6 and 18 with fewer constraints and priority than those for the DPH and EDC migrations.

3.2.1 Transition Services

Transition Services are the cornerstone of a successful relationship between the Commonwealth and the Unisys Team. In the Transition Services projects, tasks, and activities, the Commonwealth and the Unisys Team will work closely to design and implement the processes, tools, and organizations that are necessary to provide excellent services continuously to the Commonwealth and your stakeholders. The outputs from

these services will assist the PMO and the rest of the entire team in executing the program's ongoing operations.

Among the important outcomes from the Transition Services projects will be deliverables such as the Commonwealth Computing Procedures Manual (CCPM), which will provide both the Commonwealth and the Unisys Team with a defined set of expectations. Along with the CCPM, these projects will establish the Program Management Office and the tools and processes they need to successfully deliver services to the Commonwealth. These tools and processes will include those that are needed to effectively support the ITIL V3 framework, provide the Commonwealth transparency into the billing, and establish the Service Desk. **Figure 3-4** below shows the Transition phase of the project.



ID	Task Name	Start	Finish	Duration
99	3 CoPA Transition	1/1/13 8:00 AM	1/26/15 5:00 PM	301 days
100	3.1 MS - Transition Start	2/2/13 8:00 AM	12/2/13 8:00 AM	0 days
101	3.2 Conduct Transition of Services Project Kickoff Meeting	2/2/13 8:00 AM	12/4/13 5:00 PM	3 days
102	3.3 Transition of Services Project (Enable Common Service Portfolio)	1/1/13 8:00 AM	12/3/14 8:00 AM	262 days
103	3.3.1 MS - TOS Start	2/4/13 5:00 PM	12/4/13 5:00 PM	0 days
104	3.3.2 Assess CoPA Current Environments	1/1/13 8:00 AM	6/27/14 5:00 PM	150 days
112	3.3.3 Setup the Account Team	1/2/13 8:00 AM	12/3/14 8:00 AM	262 days
113	3.3.3.1 Organizational Change Control Components - Program and Services Management	12/2/13 8:00 AM	12/3/14 8:00 AM	262 days
114	3.3.3.1.1 Townhall to announce Agreement	2/2/13 8:00 AM	12/2/13 5:00 PM	1 day
115	3.3.3.1.2 Team Meetings to discuss what this "means to me"	2/2/13 8:00 AM	12/2/13 5:00 PM	1 day
116	3.3.3.1.3 Re-Organize Account Staff to new model	2/3/13 8:00 AM	1/13/14 5:00 PM	30 days
117	3.3.3.1.4 Establish PMO Guidelines and Processes	2/3/13 8:00 AM	1/13/14 5:00 PM	30 days
118	3.3.3.1.5 Establish Vendor and Subcontractor Management	1/2/13 8:00 AM	12/27/13 8:00 AM	19 days
122	3.3.3.1.6 Staff Account	1/2/13 8:00 AM	8/6/14 5:00 PM	178 days
144	3.3.3.1.7 Establish PMO Leadership Team	1/2/13 8:00 AM	1/1/14 8:00 AM	22 days
147	3.3.3.1.8 Establish Project Management Team - TPMO and Ste	1/2/13 8:00 AM	1/1/14 8:00 AM	22 days
149	3.3.3.1.9 Establish Contract Management Team	1/2/13 8:00 AM	2/21/14 5:00 PM	60 days
158	3.3.3.1.10 Establish Agency Account Management Team	1/2/13 8:00 AM	1/1/14 8:00 AM	22 days
161	3.3.3.1.11 Establish Enterprise Architecture Team	1/2/13 8:00 AM	1/1/14 8:00 AM	22 days
164	3.3.3.1.12 Establish Service Excellance Office (SEO)	1/1/14 8:00 AM	8/29/14 5:00 PM	173 days
165	3.3.3.1.12.1 Project Kickoff Meeting	1/1/14 8:00 AM	1/1/14 5:00 PM	1 day
166	3.3.3.1.12.2 Design and Document Service Service Excellace Office - Policies and Procedures	1/1/14 5:00 PM	8/29/14 5:00 PM	172 days
265	3.3.3.1.13 Establish Financial Management Team Processes	1/2/13 8:00 AM	8/8/14 5:00 PM	180 days
273	3.3.3.1.14 Establish Service Delivery Teams - Processes and Pr	1/2/13 8:00 AM	12/3/14 8:00 AM	262 days
382	3.3.3.1.15 Training	1/2/13 8:00 AM	5/9/14 5:00 PM	115 days

Figure 3-4. Initial Organization Set Up and EDC Transition

3.2.1.1 Account Organization

Unisys understands we are only as strong as our team. Early in the transition process, we will focus on training existing staff on changes brought on by the new contract; acquiring outstanding supplemental resources to deliver services; and providing the tools, processes, and work environment to enable them to be successful.

The activities for Account Organization will provide the framework to establish an effective Program Management Office.

3.2.1.1.1 Establish PMO Guidelines and Processes

Establishing the PMO guidelines and processes will include developing the interim Contract Management procedures as necessary, developing the vendor and Subcontractor Management policies and procedures, and modifying the existing Billing processes.

3.2.1.1.2 Organize Account Personnel

Organize Account Personnel will include tasks supporting talent acquisition and staff training, providing work space, and implementing standard work processes.

The Unisys Team identified individuals who will fill key positions as required by the Commonwealth. During these activities, Unisys will move individuals to these key roles by identifying and training them to assume the new roles. We will also identify other roles that are required early to lead organizations through the transition period.

Staffing plans for the technical and support teams will be reviewed and revised during the PMO's formation, including the PMO leadership team and the Project Management team, including the Transition Project Management team, the Enterprise Architecture team, and the Service Excellence team. Unisys will develop this plan to assign resources to the appropriate roles during the transition. We will engage Small Diverse Business partners to supply services and staffing requiring the establishment of processes for interaction among partners.

Contract, role, and industry-specific training will be planned and provided as appropriate to the staff as they move to their roles. This training includes CCPM, billing, Advanced ITIL V3, PMP, ITIL Foundation, and others as necessary. Unisys will partner with Harrisburg University to coordinate and deliver training.

Establishment of the Service Excellence Office will enable and drive the reformation of existing ITIL V3 processes, the drafting of the Commonwealth Compute Procedures Manual, and the implementation of quality processes and policies.

3.2.1.2 Enterprise Data Center (EDC) to Managed Services Model

The EDC will transition to a Managed Services model. Key to this project is knowledge transfer and implementation of the Unisys standard management toolset. Unisys is uncommonly positioned to enable this transition quickly, using our current team that supports the EDC. This team is very knowledgeable of the Commonwealth's current environment, which will enable an expeditious knowledge transfer process. This project will depend on the implementation and customization of the BMC Remedy ITSM Toolset, Nagios for monitoring, and BMC's Atrium Discovery and Dependency Mapping (ADDM) tool. During the EDC's transition, Unisys will work with the Commonwealth to identify a technology refresh plan for existing hardware in the EDC. Until the infrastructure is replaced, Unisys will work with the Commonwealth to include continuance of hardware maintenance.

3.2.1.3 Tools Implementation

ID	Task Name	Start	Finish	Duration
435	**3.6 Tools Implimentation Project**	**12/2/13 8:00 AM**	**12/12/14 5:00 PM**	**270 days**
436	3.6.1 MS - Tools Implementation Project St	7/22/14 8:00 AM	7/22/14 8:00 AM	0 days
437	**3.6.2 Install BMC ITSM**			
438	3.6.2.1 Prep Foundation Data	1/6/14 8:00 AM	2/21/14 5:00 PM	35 days
439	3.6.2.2 Configure CFG Mgt	12/2/13 8:00 AM	1/31/14 5:00 PM	45 days
440	3.6.2.3 Configure Release Mgt	12/2/13 8:00 AM	1/24/14 5:00 PM	40 days
441	3.6.2.4 Configure Service Level Mgt	12/16/13 8:00 AM	1/24/14 5:00 PM	30 days
442	3.6.2.5 ITSM Configured & Tested	1/27/14 8:00 AM	3/28/14 5:00 PM	5 days
443	**3.6.2.6 CCPM Approach & Reviews with**	**12/2/13 8:00 AM**	**3/3/14 5:00 PM**	**66 days**
444	3.6.2.6.1 Prep SD,SLM,CHG&Release, Performance & Capacity Mgt,	12/2/13 8:00 AM	12/30/13 5:00 PM	21 days
445	3.6.2.6.2 Review SD,SLM,CHG & Release, Performance & Capacity	2/11/14 8:00 AM	2/11/14 8:00 AM	0 days
446	3.6.2.6.3 Change and Asset Mgt Proce	2/11/14 8:00 AM	3/3/14 5:00 PM	15 days
447	3.6.3 Configure DSO - Remedy Synch	1/27/14 8:00 AM	3/28/14 5:00 PM	45 days
448	3.6.4 Install & Configure KM	2/3/14 8:00 AM	2/14/14 5:00 PM	10 days
449	3.6.5 Load KM ITSM Procedures, SC, Contra	2/19/14 8:00 AM	3/4/14 5:00 PM	10 days
450	3.6.6 KM Loaded	3/5/14 8:00 AM	3/5/14 8:00 AM	0 days
451	3.6.7 Install & Configure EDC & DPH ADDM	12/2/13 8:00 AM	2/21/14 5:00 PM	60 days
452	3.6.8 Install & Configure DOR ADDM Discov	12/2/13 8:00 AM	2/21/14 5:00 PM	60 days
453	3.6.9 Install&Configure DLI ADDM Discover	12/2/13 8:00 AM	2/21/14 5:00 PM	60 days
454	3.6.10 Install & Configure DOH ADDM Disco	12/2/13 8:00 AM	2/21/14 5:00 PM	60 days
455	3.6.11 Install & Configure PSP ADDM Discov	12/2/13 8:00 AM	2/21/14 5:00 PM	60 days
456	3.6.12 Install & Configure DPW Discovery	12/2/13 8:00 AM	2/21/14 5:00 PM	60 days
457	3.6.13 Install BPPM/BEM/SIM Monitoring &	12/2/13 8:00 AM	2/21/14 5:00 PM	60 days
458	3.6.14 Configure Availability Management	1/20/14 8:00 AM	4/11/14 5:00 PM	60 days
459	3.6.15 Configure Capacity Management	2/10/14 8:00 AM	4/11/14 5:00 PM	45 days
460	3.6.16 Install & Configure Bladelogic for Se	2/3/14 8:00 AM	4/4/14 5:00 PM	45 days
461	3.6.17 Configure Standard Reporting BMC	2/24/14 8:00 AM	4/4/14 5:00 PM	30 days
462	3.6.18 Configure Pureshare Dashboards	3/17/14 8:00 AM	4/25/14 5:00 PM	30 days
463	3.6.19 ITSM Configured for Operations	4/25/14 5:00 PM	4/25/14 5:00 PM	0 days
464	**3.6.20 Security Tools**	**12/2/13 8:00 AM**	**12/12/14 5:00 PM**	**270 days**
465	**3.6.20.1 Data Loss Prevention**	**12/2/13 8:00 AM**	**12/12/14 5:00 PM**	**270 days**
470	**3.6.20.2 Database Firewall (DBFW)**	**1/6/14 8:00 AM**	**12/12/14 5:00 PM**	**245 days**
475	**3.6.20.3 Web Application Firewall (WAF**	**1/6/14 8:00 AM**	**12/12/14 5:00 PM**	**245 days**
480	3.6.21 MS - Tools Implimentation Project C	12/12/14 5:00 PM	12/12/14 5:00 PM	0 days
481	3.6.22 MS - CoPA Transition of Services Cor	12/12/14 5:00 PM	12/12/14 5:00 PM	0 days

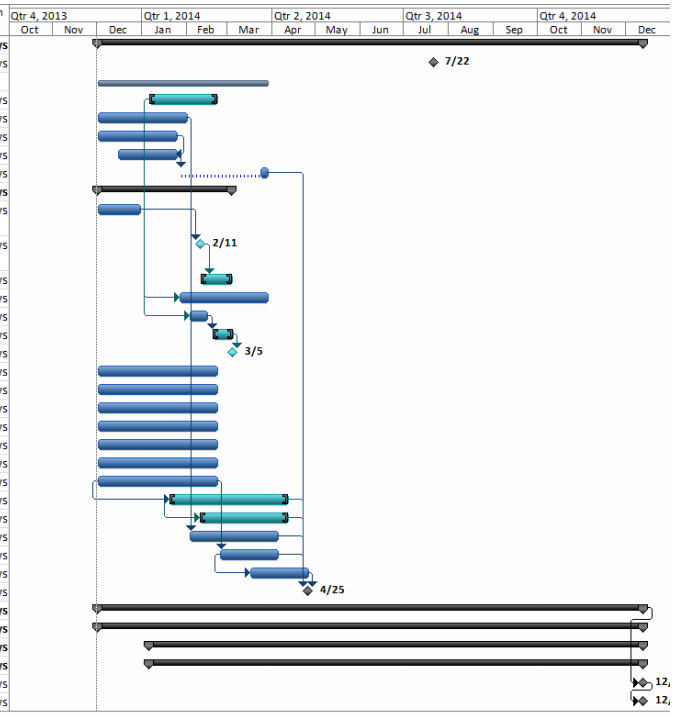


Figure 3-5. Tools Implementation Project Activities and Timeline

Unisys developed a technical architecture to support a multi-data center environment, network and security, and data center support architecture. The tools implementation project (**Figure 3–5**) is the precursor and basis for many other activities in the transition of services. Unisys will implement tools such as BMC's Remedy Suite for ITSM, PMG for Services Catalog and billing data, SolarWinds and Nagios for monitoring, BladeLogic for provisioning, and PureShare for dashboards along with other tools to form the architecture, which will be wrapped by processes and performed by Unisys, IBM, and Deloitte. The PMG Services Catalog is unique in the industry because it provides an active service catalog and workflow that can begin at the customer's request. Much of the industry focuses the service catalog on self-provisioning and other IT tasks. The Real-time Dashboard is also unique because it provides an active CIO dashboard that can be set up with much of the report data while also sharing the data at the right level of detail for a variety of management levels and uses.

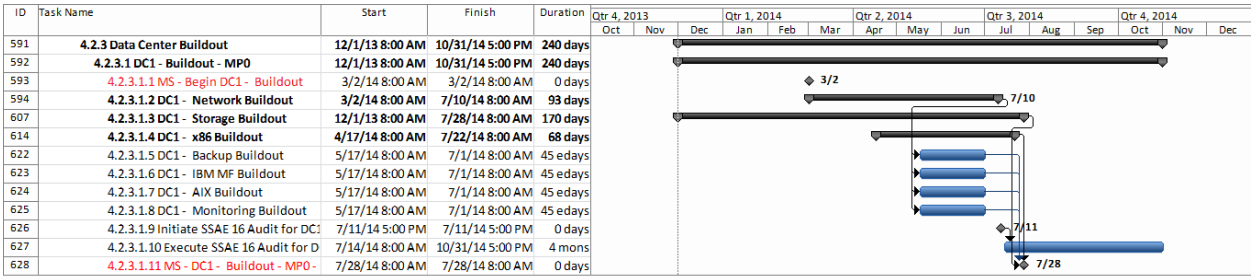
3.2.2 Application Workload Migrations

At Unisys, we believe the term Data Center Migration is a misnomer. The focus is and should be on the applications. The processes the team will follow require much input and participation from the Commonwealth application owners. Automated tools such as ADDM alongside traditional tools are used to minimize the dependency on customer input and

maximize accuracy. Each migration project will last about 3 months. On the project, technical teams and applications teams will work closely to define the exact scope, plan tasks, identify risks, develop solutions, and identify optimum times for outages that will minimize the impact on the end users. In the 3-month project, much of the effort is spent on planning, verifying, and re-planning, all with the goal of a successful migration.

But before any applications can be moved, the receiving data center must be made operationally ready. This includes implementing the infrastructure components required to meet or exceed the service levels required.

3.2.2.1 Operational Readiness

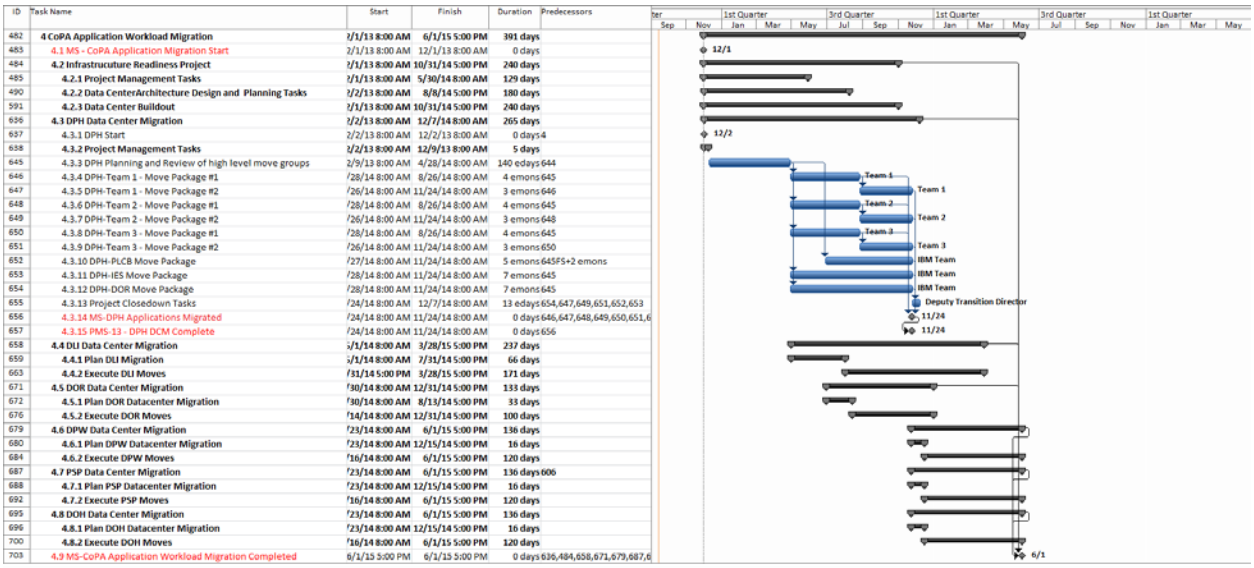


ID	Task Name	Start	Finish	Duration
591	**4.2.3 Data Center Buildout**	**12/1/13 8:00 AM**	**10/31/14 5:00 PM**	**240 days**
592	**4.2.3.1 DC1 - Buildout - MP0**	**12/1/13 8:00 AM**	**10/31/14 5:00 PM**	**240 days**
593	4.2.3.1.1 MS - Begin DC1 - Buildout	3/2/14 8:00 AM	3/2/14 8:00 AM	0 days
594	**4.2.3.1.2 DC1 - Network Buildout**	**3/2/14 8:00 AM**	**7/10/14 8:00 AM**	**93 days**
607	**4.2.3.1.3 DC1 - Storage Buildout**	**12/1/13 8:00 AM**	**7/28/14 8:00 AM**	**170 days**
614	**4.2.3.1.4 DC1 - x86 Buildout**	**4/17/14 8:00 AM**	**7/22/14 8:00 AM**	**68 days**
622	4.2.3.1.5 DC1 - Backup Buildout	5/17/14 8:00 AM	7/1/14 8:00 AM	45 edays
623	4.2.3.1.6 DC1 - IBM MF Buildout	5/17/14 8:00 AM	7/1/14 8:00 AM	45 edays
624	4.2.3.1.7 DC1 - AIX Buildout	5/17/14 8:00 AM	7/1/14 8:00 AM	45 edays
625	4.2.3.1.8 DC1 - Monitoring Buildout	5/17/14 8:00 AM	7/1/14 8:00 AM	45 edays
626	4.2.3.1.9 Initiate SSAE 16 Audit for DC1	7/11/14 5:00 PM	7/11/14 5:00 PM	0 days
627	4.2.3.1.10 Execute SSAE 16 Audit for D	7/14/14 8:00 AM	10/31/14 5:00 PM	4 mons
628	4.2.3.1.11 MS - DC1 - Buildout - MP0 -	7/28/14 8:00 AM	7/28/14 8:00 AM	0 days

Figure 3-6. Operational Readiness Timeline

To achieve operational readiness, the data center must be prepared by connecting the data center to COPANET and have a local area network designed, built, tested and operational, including data security devices such as firewalls and intrusion detection and prevention. Tools such as Remedy by BMC must be enhanced to support the expanded scope to support ITIL V3 processes for incident, problem, change, release, asset, configuration, and service level management. Supporting tools such as PMG for billing and service catalog, ADDM for automated discovery, BladeLogic for provisioning and automated patching, PureShare for dashboards, and Nagios for monitoring must also be operational. Infrastructure such as storage, virtual servers, physical servers, monitoring, and backup must be in place. Operational Readiness activities and timeline are shown in **Figure 3–6.**

3.2.2.2 Agency Application Workload Migrations



ID	Task Name	Start	Finish	Duration	Predecessors
482	4 CoPA Application Workload Migration	7/1/13 8:00 AM	6/1/15 5:00 PM	391 days	
483	4.1 MS - CoPA Application Migration Start	2/1/13 8:00 AM	12/1/13 8:00 AM	0 days	
484	4.2 Infrastrucuture Readiness Project	7/1/13 8:00 AM	10/31/14 5:00 PM	240 days	
485	4.2.1 Project Management Tasks	7/1/13 8:00 AM	5/30/14 8:00 AM	129 days	
490	4.2.2 Data CenterArchitecture Design and Planning Tasks	7/2/13 8:00 AM	8/8/14 5:00 PM	180 days	
591	4.2.3 Data Center Buildout	7/1/13 8:00 AM	10/31/14 5:00 PM	240 days	
636	4.3 DPH Data Center Migration	7/2/13 8:00 AM	12/7/14 8:00 AM	265 days	
637	4.3.1 DPH Start	2/2/13 8:00 AM	12/2/13 8:00 AM	0 days	4
638	4.3.2 Project Management Tasks	7/2/13 8:00 AM	12/9/13 8:00 AM	5 days	
645	4.3.3 DPH Planning and Review of high level move groups	2/9/13 8:00 AM	4/28/14 8:00 AM	140 edays	644
646	4.3.4 DPH-Team 1 - Move Package #1	7/28/14 8:00 AM	8/26/14 8:00 AM	4 emons	645
647	4.3.5 DPH-Team 1 - Move Package #2	7/26/14 8:00 AM	11/24/14 8:00 AM	3 emons	646
648	4.3.6 DPH-Team 2 - Move Package #1	7/28/14 8:00 AM	8/26/14 8:00 AM	4 emons	645
649	4.3.7 DPH-Team 2 - Move Package #2	7/26/14 8:00 AM	11/24/14 8:00 AM	3 emons	648
650	4.3.8 DPH-Team 3 - Move Package #1	7/28/14 8:00 AM	8/26/14 8:00 AM	4 emons	645
651	4.3.9 DPH-Team 3 - Move Package #2	7/26/14 8:00 AM	11/24/14 8:00 AM	3 emons	650
652	4.3.10 DPH-PLCB Move Package	7/27/14 8:00 AM	11/24/14 8:00 AM	5 emons	645FS+2 emons
653	4.3.11 DPH-IES Move Package	7/28/14 8:00 AM	11/24/14 8:00 AM	7 emons	645
654	4.3.12 DPH-DOR Move Package	7/28/14 8:00 AM	11/24/14 8:00 AM	7 emons	645
655	4.3.13 Project Closedown Tasks	7/24/14 8:00 AM	12/7/14 8:00 AM	13 edays	654,647,649,651,652,653
656	4.3.14 MS-DPH Applications Migrated	7/24/14 8:00 AM	11/24/14 8:00 AM	0 days	646,647,648,649,650,651,6
657	4.3.15 PMS-13 - DPH DCM Complete	7/24/14 8:00 AM	11/24/14 8:00 AM	0 days	656
658	4.4 DLI Data Center Migration	5/1/14 8:00 AM	3/28/15 5:00 PM	237 days	
659	4.4.1 Plan DLI Migration	5/1/14 8:00 AM	7/31/14 5:00 PM	66 days	
663	4.4.2 Execute DLI Moves	7/31/14 5:00 PM	3/28/15 5:00 PM	171 days	
671	4.5 DOR Data Center Migration	7/30/14 8:00 AM	12/31/14 5:00 PM	133 days	
672	4.5.1 Plan DOR Datacenter Migration	7/30/14 8:00 AM	8/13/14 5:00 PM	33 days	
676	4.5.2 Execute DOR Moves	7/14/14 8:00 AM	12/31/14 5:00 PM	100 days	
679	4.6 DPW Data Center Migration	7/23/14 8:00 AM	6/1/15 5:00 PM	136 days	
680	4.6.1 Plan DPW Datacenter Migration	7/23/14 8:00 AM	12/15/14 5:00 PM	16 days	
684	4.6.2 Execute DPW Moves	7/16/14 8:00 AM	6/1/15 5:00 PM	120 days	
687	4.7 PSP Data Center Migration	7/23/14 8:00 AM	6/1/15 5:00 PM	136 days	606
688	4.7.1 Plan PSP Datacenter Migration	7/23/14 8:00 AM	12/15/14 5:00 PM	16 days	
692	4.7.2 Execute PSP Moves	7/16/14 8:00 AM	6/1/15 5:00 PM	120 days	
695	4.8 DOH Data Center Migration	7/23/14 8:00 AM	6/1/15 5:00 PM	136 days	
696	4.8.1 Plan DOH Datacenter Migration	7/23/14 8:00 AM	12/15/14 5:00 PM	16 days	
700	4.8.2 Execute DOH Moves	7/16/14 8:00 AM	6/1/15 5:00 PM	120 days	
703	4.9 MS-CoPA Application Workload Migration Completed	6/1/15 5:00 PM	6/1/15 5:00 PM	0 days	636,484,658,671,679,687,6

Figure 3-7. Agency Application Workload Phased Migrations

The application workloads supported in the agency data centers are planned to be moved in three phases, as shown in **Figure 3–7.** The first phase is focused on the Data PowerHouse Data Center, the Department of Labor & Industry, and Department of Revenue. Application workloads supported in the Pennsylvania State Police, Department of Public Welfare and Department of Health data centers will move last in the final phase. Unisys determined the order of agency migrations based on lower periods of activities, but also recognize that due to in-flight projects and other activities, these priorities may change. Each of these agency data centers will be divided into multiple projects based on size, complexity, and number of applications. Each project includes a similar set of tasks including documenting the application scope and supporting infrastructure, determining the move strategy for each component, such as "over the wire" or "lift-n-shift", and order of application migrations. This activity is followed by detailed planning; identification of hardware in the receiving data center; remediation of hardcoded IP addresses in the application; test plan creation; data transfer, which will be planned to avoid peak work periods, and finally testing.

The Unisys plan includes over-the-wire transfer of data and when appropriate, operating systems and applications. This approach will minimize risk that may occur during reinstallation activities by using the current operating system and application setting and minimize outages by synchronizing periodically throughout the weeks leading to the migrating events, and can be more easily scheduled around peak work times for the agencies.

Each plan will include notifications to Commonwealth stakeholders 30, 7, and 2 days before events. Application owners will be expected to verify each application successfully migrated through appropriate testing activity.

2.0 Management Summary

2. MANAGEMENT SUMMARY 2-3

2.1 THE PATH FORWARD 2-3
2.2 THE UNISYS TEAM 2-4
2.3 OUR EXECUTIVE LEADERSHIP TEAM 2-7
2.4 UNISYS SOLUTION 2-14
2.4.1 Unisys Tenets 2-14
2.5 THE PROPOSED SOLUTION 2-14

"As a Pennsylvania-based corporation, Unisys and many of our employees depend on the critical services the Commonwealth will provide through this initiative. That is added incentive for our team to succeed and meet your expectations. As a demonstration of our commitment to the Commonwealth I will personally serve as the executive sponsor to ensure the highest levels of service and satisfaction."

Commonwealth Executive Sponsor
Chairman and CEO
Unisys

This page intentionally left blank.

2. Management Summary

RFP	*Requirement*
II-2	*Management Summary. Include a narrative description of the proposed effort and a list of the items to be delivered or services to be provided.*

This RFP is much broader and far more significant than consolidating infrastructure. The essence of this opportunity is optimized "compute services," supporting the Commonwealth's applications by providing the right service in the right capacity when it is needed and in a way that is cost effective, transparent, and secure. When the transition is complete and the benefits are realized, the industry will recognize this initiative for what it is—a paradigm shift in service delivery for state government.

2.1 The Path Forward

This engagement is an innovation effort to transform information technology (IT) at the Commonwealth to a robust yet flexible offering that supports current and future capacity and service levels that evolve, expand, and contract with the flow of changes in the Commonwealth's business and operating environment. No longer is it acceptable to carry fixed costs that burden the Commonwealth financially when changes in the economy, government funding, or government needs occur. IT at the Commonwealth must be an enabler of these changes to optimize your operating environment going forward.

The Commonwealth is seeking a fundamental shift in the way it acquires and operates IT by implementing a fully consumptive, secure private cloud services utility model. The model is based on an IT Service Management platform that leverages ITIL V3 best practices and Lean Six Sigma methods to create an "optimization framework" for an enterprise-centric IT infrastructure.

Ultimately, the Commonwealth and its chosen service provider will move the current Commonwealth applications to an Infrastructure as a Service (IaaS) operating model in which agencies can scale transactions and compute capacity based on need, therefore optimizing the cost of supporting these applications. **That is much different from today's contract which features fixed pricing for most services, limited transparency, and little flexibility to scale according to changing needs. The new model will provide the opportunity to lower costs of service and the means to tailor services to specific needs. As your current service provider, we welcome these changes.**

2.2 The Unisys Team

To be successful and to mitigate risk to the greatest degree possible, this innovative effort must start with a world-class team delivering specific and proven experience with the Commonwealth of Pennsylvania. Unisys, as the prime contractor, will be totally responsible for successfully delivering the compute services in this RFP's scope. As a Pennsylvania-based company with approximately 23,000 employees worldwide, Unisys has a long and successful record of accomplishment of working with you and other prestigious organizations on similar innovative efforts.

Innovation - Flexible Pricing Models

Unisys Experience with:

- *Defense Information Systems Agency (DISA)*
- *Internal Revenue Service (IRS)*
- *City of Minneapolis*
- *American Red Cross*
- *California State University System(CSU)*

For this engagement, we will bring forward many local IT experts—currently more than 150—who support the Commonwealth today and we build on that core group with new staff and skills to actively pursue robust new programs for continuous innovation and improvement. We again have partnered with **IBM** and others you know but also have engaged several new partners, including **Deloitte Consulting** (Deloitte). All have been carefully selected for their unique skills, knowledge or resources to enable success of this engagement, to deliver on time and on budget, and to meet the Commonwealth's high expectations for flexibility, service quality, and client satisfaction. We are blending resources most experienced with your applications and systems with new skills and new ideas to drive ongoing innovation and efficiencies.

Stability and reliability of your compute services environment will be our top priority. We estimate that our team – The Unisys Team – currently manages approximately 75 percent of your in-scope compute capacity. That level of knowledge and experience is a key differentiator between the Unisys Team and others that claim they have the credentials necessary to transition the Commonwealth's most important systems.

IBM and Deloitte are exclusive partners to the Unisys Team. Both are premier companies and experienced providers of services and technology to the Commonwealth. As illustrated in **Figure 2-1,** we considered many factors when we selected IBM and Deloitte for our core, "best of breed" team to deliver compute services to the Commonwealth.

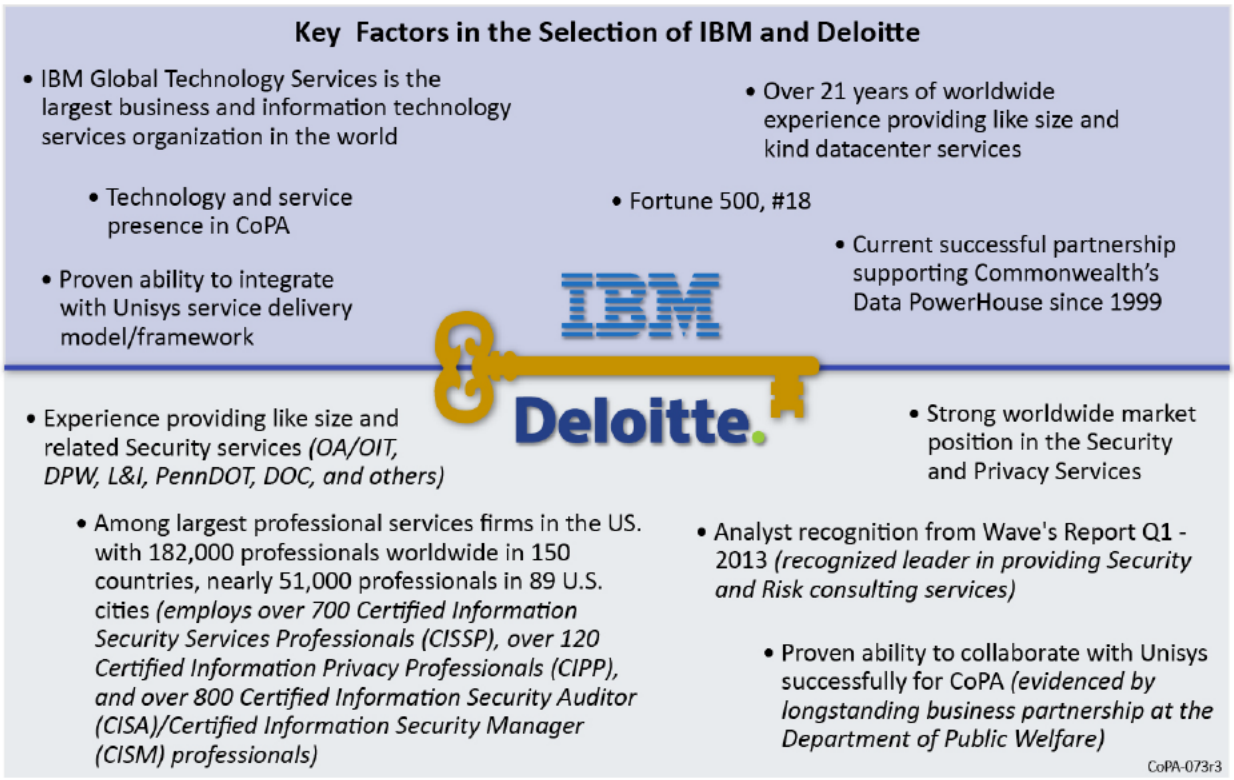


Figure 2-1. Key Factors

Figure 2-2 highlights the entire Unisys Team and each team member's role. Recognizing the value of the Commonwealth's approach with its own staff augmentation contract, Unisys assembled a large pool of Small Diverse Businesses (SDBs) to improve our ability to source the best technical resources at the best value while helping the local, small and diverse business community. Those SDB firms include **American Personnel Managers, Acclaim Systems, Credo Technology Solutions, Domino Technologies, e & e IT Consulting Systems, Info-Matrix Corporation, Innovative Business Concepts,** and **PCN.** We also selected **Pierson Computing Connection Incorporated** to provide certain technology components of our solution, and **Latus Commercial Realty** to provide commercial real estate services. In addition, we have added **Harrisburg University of Science and Technology** to provide educational and training support.

With added focus on innovation and emerging technologies, our team also includes BMC, Cisco, EMC, Microsoft, PMG, PureShare, Juniper, and VMware. These companies are on the leading edge of new technologies that can transform the way we operate and in turn deliver significant efficiencies. Section 4 of our proposal provides a detailed perspective of Unisys qualifications and additional details on the members of our team.

Figure 2-2. The Unisys Team

This consortium is world class. It includes the two primary inventors and suppliers—Unisys and IBM—of the technology infrastructure and system software running nearly all of the Commonwealth's business application systems. Therefore, the Unisys Team will have a direct line to software developers and technical support experts worldwide for issues that require around-the-clock problem solving.

We know success revolves around the Commonwealth's business application systems and keeping them fully operational. Unisys and IBM together offer more than 100 years of working knowledge of the Commonwealth's business application systems. Further, we augmented our team with Deloitte, the largest, most experienced applications integrator, developer, and application maintenance provider in support of the Commonwealth's business application systems. Deloitte also provides a variety of mission-critical IT

Committed to the Commonwealth

Local Knowledgeable Resources

*In **Pennsylvania**, Unisys, IBM, and Deloitte Consulting **employ 6,962 people** with more than **900 people** in the **metropolitan Harrisburg** area.*

security services to the Commonwealth. Our team will leverage Deloitte's application knowledge and security capabilities extensively, further promoting success overall.

The Unisys Team has unsurpassed collective knowledge of your applications, business, history, nuances, people, policies, processes and systems. The Unisys Team has an unmatched – unrivaled record of accomplishment in the managed infrastructure services, security, and application services space for the Commonwealth. For example:

- We have consistently met high levels of availability and met or exceeded service level requirements
  - Specifically:
    - **Achieved overall 99.9915 percent availability** in the DPH since 2008
    - **Achieved greater than 99 percent of all SLAs** since 2008
- We have had no security breaches in the DPH
- We successfully completed a number of innovative initiatives, including:
  - Implementation of the enterprise shared infrastructure
  - Inclusion of tiered service levels and rate card
  - Piloting of self-provisioning
  - Near 100 percent ITIL V3 Foundation certification of all Unisys DPH and [redacted] delivery staff

Bottom line—we have assembled a team with by far the most experience and knowledge specific to the Commonwealth supplemented by a global network of experts to assist, as necessary. This team comprises experienced staff—many of whom you already know—starting with our executive leadership.

2.3 Our Executive Leadership Team

Because of this engagement's importance and our commitment to the Commonwealth of Pennsylvania, [redacted], Unisys Chairman and CEO, has chosen to serve as Executive Sponsor and will personally ensure our company's complete commitment to its success.

In addition to [redacted] role as Executive Sponsor, Unisys established an Executive Leadership Committee to support the efforts of our Harrisburg-based service delivery leadership team. This committee, which consists of senior business and service delivery executives from Unisys, IBM and Deloitte, was established to provide direct visibility into our respective organizations to

"We have an excellent service delivery team assigned to this initiative. [redacted] are some of the very best in service delivery. I trust their judgment and have empowered them to make the necessary decisions locally to keep the project on schedule and meet your expectations. Their team is complemented by a Unisys Executive Leadership Committee focused on providing whatever additional corporate resources and support are necessary to succeed."

—[redacted]
Commonwealth Executive Sponsor
Chairman & CEO

enable us to meet our commitments to the Commonwealth during transition and steady state operations. This committee also will be tasked to resolve issues that may arise but cannot be resolved locally. The committee will provide executive leadership, support, and direction throughout the engagement's entire life and will be a vital component of the transition and steady state governance model. **Figure 2-3** identifies the members of our Executive Leadership Committee.

Figure 2-3. Unisys Executive Leadership Committee

Our Service Delivery Team

The Harrisburg-based Unisys leadership team, depicted in **Figure 2-4,** will be led by [redacted]. As Engagement Executive, [redacted] has worked closely with key Commonwealth executives to manage many aspects of the current Data PowerHouse (DPH) Program over the past five years. On joining Unisys, [redacted] oversaw the successful transition to shared services in 2008. This transformed service delivery and saved the Commonwealth $240 million.

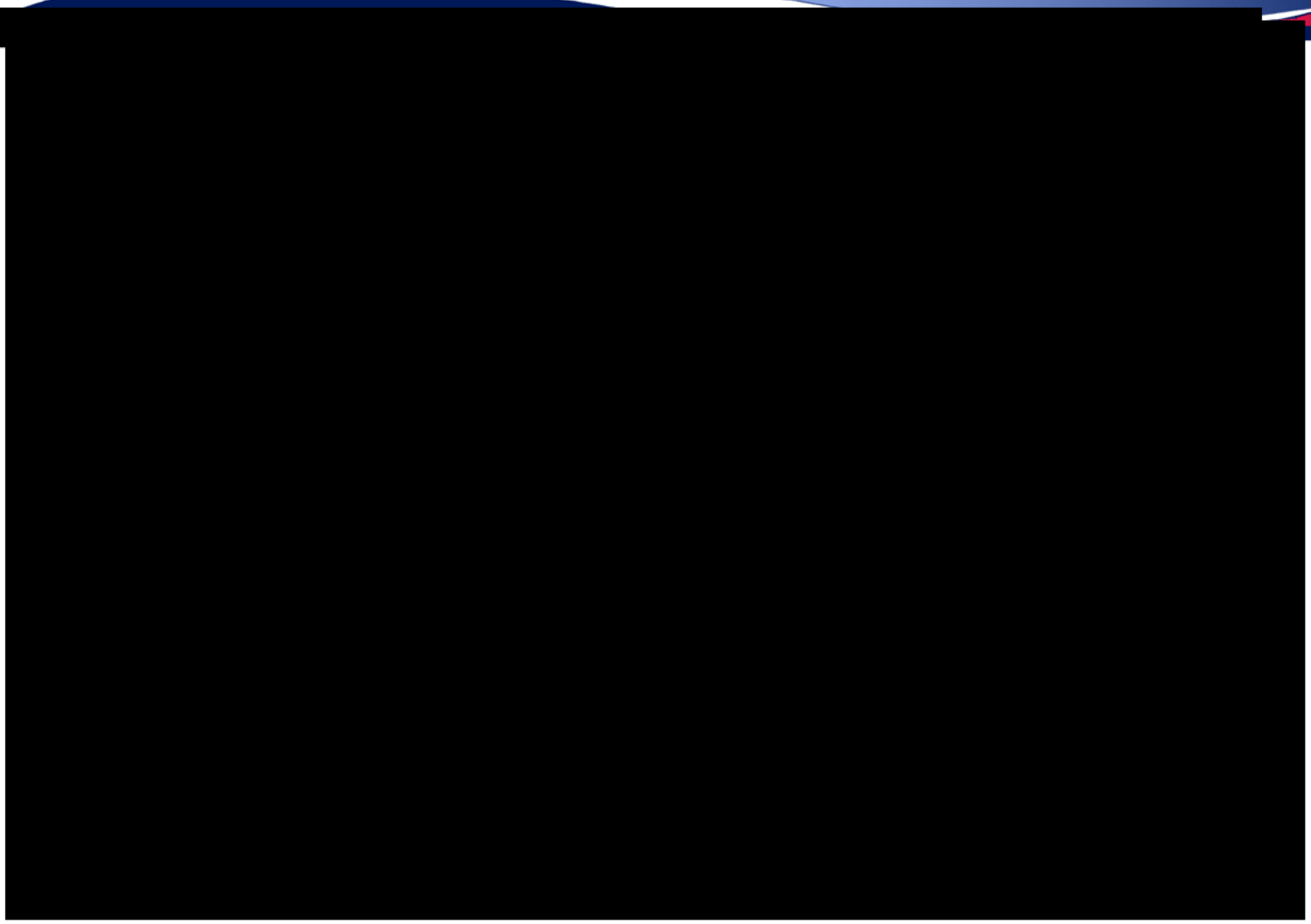


Figure 2-4. Unisys Harrisburg Service Delivery Team

During her tenure with Unisys, [redacted] spearheaded a number of innovative technology solutions, including server virtualization that reduced costs for the Commonwealth. She also fostered the evolution of the DPH architecture to new technology concepts, including disk-based backup solutions and flexible service offerings. [redacted] has demonstrated great sensitivity when it comes to customer satisfaction by implementing a number of in-depth survey processes designed to take the customer's pulse at many different levels on all aspects of service. She has held her team accountable to document issues and follow-up actions in collaboration with the agencies. These activities improved customer satisfaction significantly. [redacted] Certifications – ITIL V3 Foundation.

[redacted] was presented with the 2012 Outstanding Leadership and Innovation ("Ollie") award from former Commonwealth CIO George White for his efforts at OA-Information Technology (OIT) to support the Pennsylvania State Police. The "Ollie" award is sponsored by the Office of Administration's Office for Information Technology and Government Technology magazine.

[redacted] will serve the Commonwealth as lead Agency Account Manager. [redacted] is a 23-year Unisys employee who has worked at the Commonwealth of Pennsylvania since 2002 in a variety of Project Management and Client Services Management roles supporting numerous Commonwealth organizations. Since 2005, he has worked on site at the Commonwealth Technology Center in very close collaboration with the Commonwealth CTO, CISO, Client Management, Enterprise Data Center, Enterprise Networking and Security, Enterprise Services, GIS, PMO, and many agencies. Certifications—ITIL V3 Foundation and PMP.

[redacted] will serve the Commonwealth as the Service Delivery Executive (Program Manager). [redacted] brings 14 years of experience leading large Service Delivery organizations, most recently supporting outsourced engagements for Computer Sciences Corporation (CSC). [redacted] will leverage his experience with leading large-scale data center delivery teams, including a team at Textron, where he directed the consolidation of 10 sites with multiple mainframes and more than 800 open systems servers and then managed an ongoing Service Delivery team of 500 employees. Certification—ITIL V3 Foundation.

[redacted] will serve the Commonwealth as PMO Transition Manager. [redacted] brings 27 years of IT delivery experience working for large IT outsourcing firms before joining Unisys at the beginning of this year. As a Transition Management leader working for Dell Services (formerly Perot Systems), [redacted] led multiple large-scale data center transitions, migrations, and system upgrades during his 5-year tenure. [redacted] managed Perot Systems' Healthcare Business Unit portfolio of transitions and data center migrations. Certifications—ITIL V3 Foundation and PMP.

[redacted] will serve the Commonwealth as the Senior Enterprise Architect under the new contract. He has 16 years of IT industry experience working for IBM in several architect roles before joining Unisys in 2011 as the Lead Client Architect managing the Unisys North American Client Architect team, which includes oversight of the Client Architects supporting the Commonwealth. While working for IBM, [redacted] served as Transformation Integration Architect, leading a large team of architects to develop technical components to build a multitenant data center to support the State of Georgia's strategic consolidation plans. Certifications—ITIL V3 Foundation, Open Group Master IT Architect, and IBM IT Architect Certifications.

[redacted] will serve the Commonwealth as the Chief Security Manager. [redacted] brings more than 38 years of technical and management experience, working with a number of federal and state government agencies, including the Pennsylvania State Police (PSP), for which he managed security for the new Commonwealth Law Enforcement Assistance Network (CLEAN). He also collaborated with JNET to provide access to CLEAN by JNET users without requiring additional authentication and assisted Office of Administration/Office for Information Technology (OA/OIT) leadership with creating Security ITBs. [redacted] efforts enabled deployment of the new Megan's Law application to its full user base much faster than would have been achievable otherwise, enabling PSP to meet its legislatively mandated deadline. Certifications—CISSP (Certified Information Systems Professional) and SANS GSEC (Global Information Assurance Certification Security Essentials Certification).

[redacted] will serve the Commonwealth as the Service Excellence Officer. [redacted] is currently the Operations Director for Unisys in North America responsible for all Unisys customers; [redacted] will be 100 percent dedicated to the Commonwealth. A 32-year employee with Unisys, [redacted] brings considerable successful experience across our client base. In his current role, he led a number of key initiatives under our ITIL V3 and Lean Six Sigma-based Continual Service Improvement Program. [redacted] led several service improvement initiatives for the Commonwealth, including multiple Kaizen Process Optimization workshops with the Unisys Team supporting the Commonwealth of Pennsylvania. One of these workshops laid the groundwork to transition the DPH contract from an antiquated Remedy system to the current ITSM 7.6 Remedy system. Certifications—Six Sigma Lean Black Belt and ITIL V3 Foundation.

Section 5 of our proposal provides a detailed description of the entire Unisys staffing plan, including other key personnel on the Unisys Team.

Our team is organized around your needs and largely based in Harrisburg -- close to you. That will help facilitate more effective coordination and communications. **Figure 2-5** is a high-level description of the functions of each of our seven core teams.

Figure 2-5. Seven Functional Teams

To illustrate the interaction between our team and the Commonwealth team, we present **Figure 2-6.** It is a high-level graphical depiction of the coordination and flow of communications between our respective organizations. Having significant experience with the Commonwealth, Unisys understands that it is not as simple as one Unisys point of contact to a single Commonwealth counterpart. The Commonwealth organization is multidimensional; each agency has its own management structure and IT support team, and the OA manages the contract on behalf of the agencies.

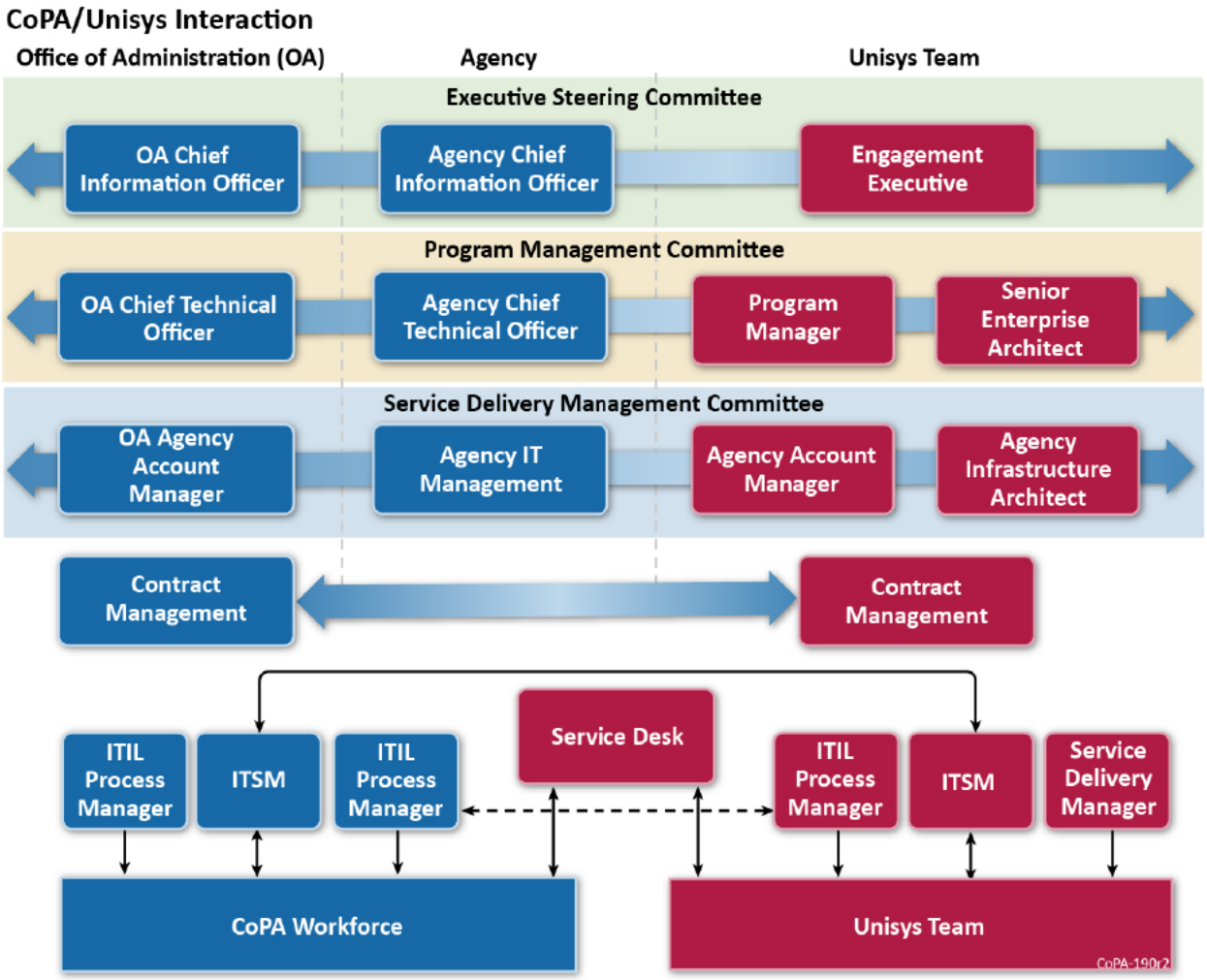


Figure 2-6. Commonwealth and Unisys Communication and Interaction Flow

As part of our deliverables, Unisys will develop, with you, a comprehensive stakeholder communications plan involving our leadership team in addition to our project and service delivery staff. That will enable those affected but not included above to have the necessary information on each stage of the transition.

Now that you have been introduced to the Unisys Team and our key leadership staff, the sections that follow highlight the solution strategy we followed to meet the Commonwealth's requirements as well as an overview of our proposed solution.

2.4 Unisys Solution

2.4.1 Unisys Tenets

Given our knowledge of the Commonwealth, and a detailed review of the RFP's requirements, we carefully selected our consortium partners, and designed a solution based on the following tenets:

- **"Do no harm" –** Every aspect of the engagement must be performed without any unplanned interruption of services
- **"Align compute services with the business" –** Our proposed solution must provide a transparent and flexible compute services environment aligned with the business needs of the agencies
- **"Achieve success together" –** Work closely with Commonwealth staff, understand and address their individual issues, and provide needed training to facilitate knowledge transfer and adoption of best practices
- **"Focus on moving software applications rather than moving hardware" –** This is about moving software applications that support the most important functions of Pennsylvania state government
- **"Managing change is key to success" –** We must implement strong change management practices, a solid training plan, and effective communications when transforming the Commonwealth to its future model
- **"Recognize and respect differences among individual agencies" –** We must recognize that agencies will have their autonomy to execute their business goals while assisting the Office of Administration with achieving its enterprise objectives
- **"Innovation is a must" –** In all aspects of our solution, we must look ahead…not back
- **"Security is paramount" –** We must encapsulate everything we do with a strong security framework that protects all Commonwealth data and IT resources.

2.5 The Proposed Solution

Our proposed solution is designed to eliminate any application latency risks to the Commonwealth's applications while providing an ongoing cost-effective solution to meet the Commonwealth's security, operational, and financial objectives. To deliver the required services and meet the RFP's requirements, we carefully architected two key components: the **Data Center Infrastructures** that will underpin the services delivered through a **Component-based Operating Model,** both of which are described below.

Data Center Infrastructures

As depicted in **Figure 2-7,** Unisys will provide a network of Tier 3 data centers interconnected to provide the optimum data center environment. This network improves resiliency and largely mitigates any application latency issues with the move of the DPH

and other agency data centers to the new compute environment. In addition to the [redacted] our data center approach will be to leverage two additional compute facilities in [redacted]. A contributing reason we chose the [redacted] facility as a primary production site is its location, which is within a [redacted] an important metric relative to the reduction of any potential latency issues with moving the Commonwealth's applications to a new location. Also, there is a robust telecommunications infrastructure in the [redacted] area to locate the workloads that currently exist in the DPH. Remaining agency data centers will be located in either the [redacted] or [redacted] facilities. During data gathering, we will study network latency and other factors with the productions applications in the agency data centers to determine the best location for the workloads based on potential latency issues that need to be mitigated. An important consideration in the selection of [redacted] as a data center is to provide Capacity on Demand services and geographical separation for disaster recovery workloads to better protect the Commonwealth in the event of a natural disaster occurring on the East Coast. Today, Commonwealth disaster recovery workloads are greater than 50 miles apart, but they are in the same geographical zone which poses a risk to the Commonwealth. [redacted] provides the ability to locate disaster workloads in the [redacted] or vice versa if geological separation is desired.

We plan to leave the [redacted] "as is" during migration to mitigate risk and to focus on other transition activities. Unisys will establish the IT Service Management (ITSM) infrastructure for the Commonwealth in the [redacted] initially and then a redundant copy in [redacted] to provide the compute services outlined in this proposal and to accommodate existing applications.

Unisys will deploy a network-operating environment that is fully fault tolerant and provides the scalability and flexibility needed going forward while reducing network-operating costs. Furthermore, this network will be integrated into COPANET to interconnect the compute facilities in **Figure 2-7**.

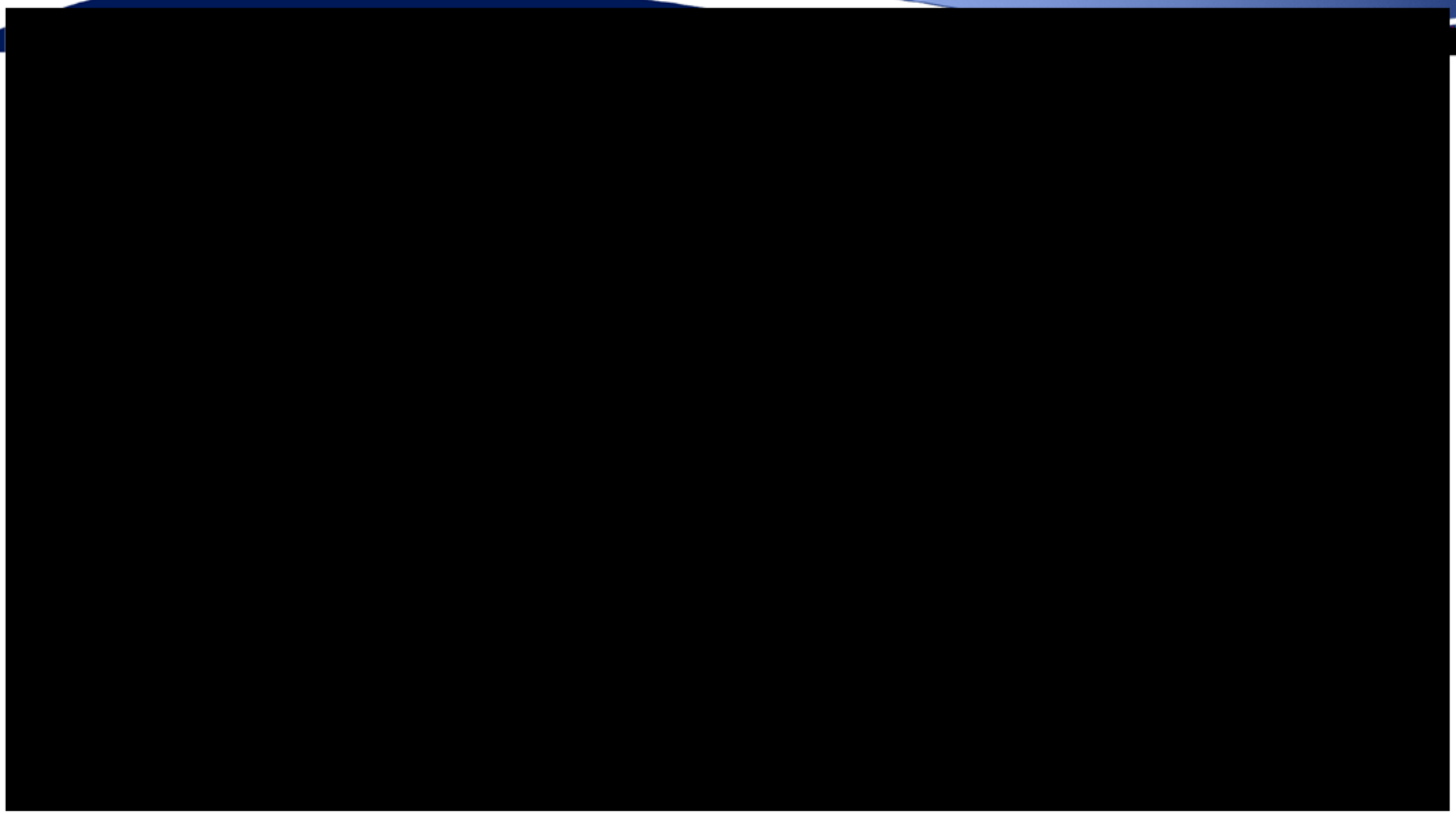


Figure 2-7. Proposed Data Center Architecture

Unisys also will deliver a modern disaster recovery plan and framework that leverages the use of Capacity-on-Demand computing to have the right amount of compute resources when needed eliminating the expense of having dedicated systems sitting idle. The Unisys approach to disaster recovery is based on systems as workloads that can be located in any facility that in turn can leverage capacity-on-demand models to make disaster recovery cost-effective moving forward.

While our compute centers are geographically dispersed to provide the maximum protection (risk reduction), flexibility and cost efficiencies, their operations will be integrated through the Component Based Operating Model depicted in **Figure 2-9**. The primary support center that will operate this model will be in the Harrisburg area, thereby providing not only convenient access by Commonwealth staff but also the opportunity to base the vast majority of our delivery and support team in Harrisburg avoiding the typical phone support only model provided by others.

Common Infrastructure Architecture

Within each of the data centers is a common infrastructure architecture to support the Managed Hosting and Capacity-on-Demand Services. It is important to note there is no difference in the infrastructure platform to support Managed Hosting or Capacity-on-Demand thereby simplifying the management and provisioning efforts which enables the

ability to optimize and scale of workloads, leading to cost efficiencies. The components that make up the infrastructure architecture are depicted in **Figure 2-8** below.

Figure 2-8. Common Infrastructure Architecture

Component Based Operating Model

To achieve the RFP's requirements, Unisys developed a component-based operating model as depicted in **Figure 2-9.** This model encompasses the requirements in the RFP and reflects a logical view that the Commonwealth can easily visualize. This compute services model illustrates the main deliverables and services and will sit on top of all compute data center facilities in **Figure 2-7** that Unisys provides for Commonwealth workloads, whether production or disaster recovery based.

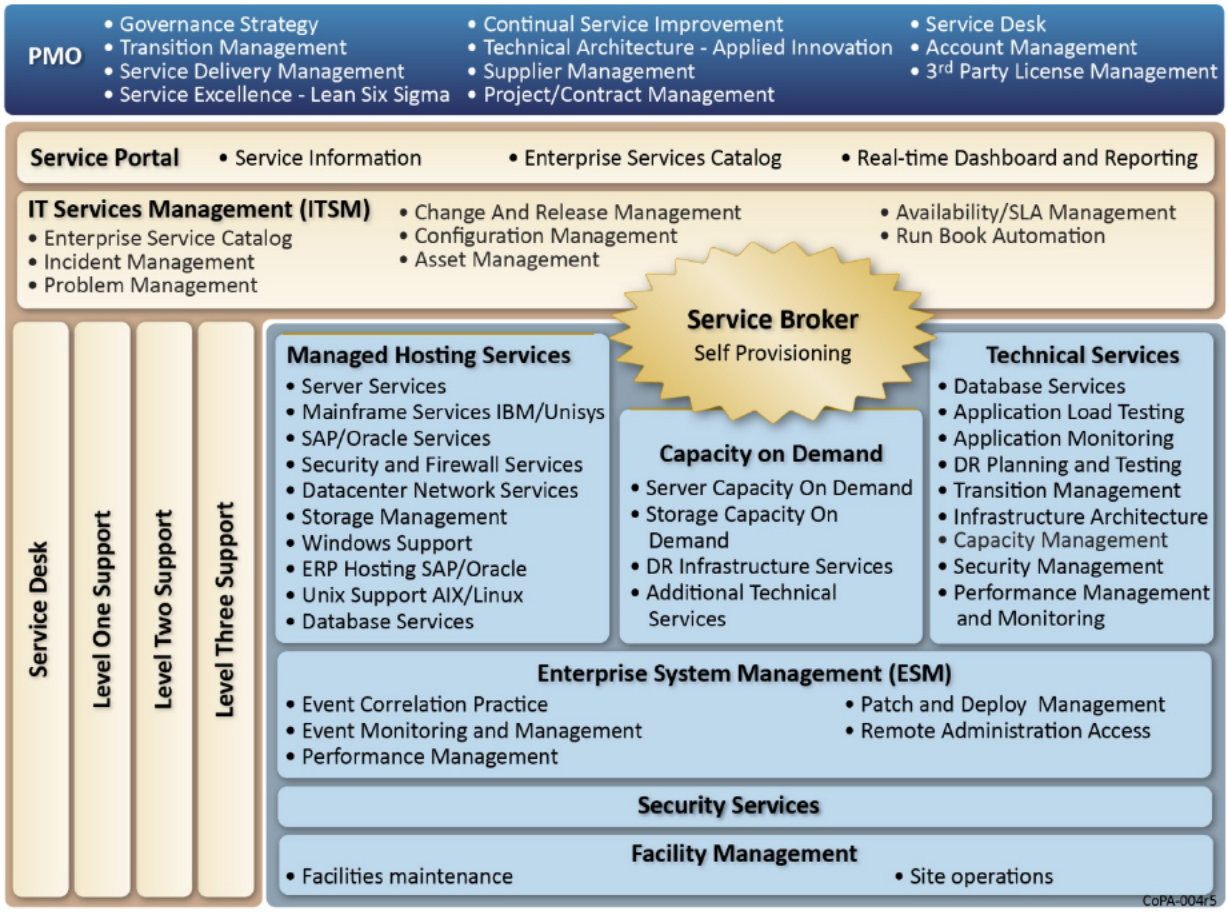


Figure 2-9. Component Based Operating Model

The Component Based Operating Model is broken down into the following components to support the requirements within the RFP:

1. **Program Management Office –** Establish a local and dedicated Program Management and Service Excellence Office that provides a focus on governance, a drive toward continued value, and cost savings by deploying Lean Six Sigma practices based on studies of cycle time and defect analysis from events that are extracted from the IT Service Management platform. By removing cycle time waste and defects of the operating environment, Unisys will provide the Commonwealth with continued cost savings and a higher quality IT compute environment. This same office is responsible for the ongoing governance of driving continuous service improvement and innovation.

2. **Service Portal –** Create an enterprise services portal, enterprise services catalog, and real-time dashboard to provide a single interface to all agencies to interact, provision, and be able to determine the performance of the IT operating environment in near real time. Each agency will have the ability to develop its own

personality with its service portal. Agencies will be able to configure their portals to develop their own "look and feel," determine the services they want to publish or offer, provision, and report on, in near real time, while still having access to the overall view of the enterprise as appropriate.

3. **IT Service Management –** Deliver an enterprise IT Service Management platform based on ITIL V3 best practices and Lean Six Sigma methods that drive the maturity of the IT operating model with a goal of achieving an efficiency gain of 5 percent year over year. Of significant importance is the development of an enterprise wide Configuration Management Database (CMDB) that defines the service that IT delivers to the Commonwealth. The creation of services in the CMDB will allow the Commonwealth to proactively determine business impact by determining a fault before it occurs and allowing maximum use of IT resources to reduce ongoing cost. Each agency will have its own instance in the service management environment to provide operating autonomy. Unisys will provide a federated service management environment to the OA so it has the overall view of the total IT operating environment at the Commonwealth. The Commonwealth can be comfortable knowing that Unisys supports a multitude of IT Service Management Systems, including BMC Remedy and ServiceNow. Our Component-based Operating model can be enabled with any one of the named IT Service Management Platforms.

4. **Managed Hosting Services and Capacity on Demand –** Enable an adaptive, flexible, and secure hardware compute environment that is based on a consumptive utility model with a "no volume commit" attribute that provides the agencies with the autonomy to perform their IT functions and meet their business requirements. In the Unisys compute model, there is fundamentally no difference between Managed Hosting Services and Capacity on Demand because they are served from the same hardware platforms and managed by the same ITSM management platform. As an innovation effort and to make sure the Commonwealth is aligned with market trends, the Unisys Team includes optional Virtual Private Cloud offerings from Microsoft and VMware in the Catalog of Services. From Microsoft, we included Azure, Office 365, and Dynamics as optional services. From VMware, we included its new offering in the marketplace for virtual private cloud capacity for Windows as an optional service.

5. **Service Broker –** Unisys will provide the Commonwealth with a consolidated, optimized, and centralized multitenant compute environment in which the agencies will not have to compromise their control by being able to self-provision workloads through the use of an enterprise service portal and catalog. Once ordered from the service catalog, the request will be processed through ITSM for change approval. When the request is approved, the Service Broker will invoke an automated runbook to execute the provisioning effort. Once the provisioning effort is complete, the runbook will update the Configuration Management Database. Agencies will be able to maintain a very real level of control over their compute environment required to meet the business need. As an innovation effort, the Service Catalog and

Service Broker will be an integrated pair to provision not only capacity from the private cloud environment we are providing the Commonwealth, but also all services from partners such as IBM, Microsoft, and VMware. Our vision for the Service Catalog and Service Broker is you can provision any service from any provider at any time with "no commit" that is then managed by the Component Based Compute Model provided in this RFP. One provisioning model and one management model will unify the compute model for the Commonwealth and provide the business flexibility and optimized compute environment the Commonwealth is looking for.

6. **Technical Services –** Unisys will provide a set of selectable services that can be procured from the services catalog to manage given applications in the Commonwealth agencies. These technical services can be people- or management-based services and can be procured in a consumption-based approach.

7. **Security Services –** Achieve and maintain a robust and comprehensive security environment that meets the IT Security policies set forth by the Commonwealth and enable agencies to meet their regulatory compliance requirements. The data center security environment will be established with the assistance of Deloitte, which has over 10 years of experience working with the Commonwealth to create, implement, and manage security policies and using Deloitte's demonstrated security framework to help the agencies meet diverse regulatory requirements.

8. **Facility Management –** Provide the ongoing management for all data centers whether Unisys or Commonwealth owned facilities.

9. **Service Desk –** The Service Desk will take calls from IT support staff to log incidents that were not automatically generated from the event monitoring system. The Service Desk will use knowledge management to try to resolve an event within an agreed time. If the event cannot be resolved in the agreed time, it will be escalated to Level One Support.

10. **Level One Support –** Level One Support manages all events that are automatically generated from the hardware and application environments as well as resolving incidents that are received from the Service Desk. Level One will use various tools, runbooks, and knowledge management to resolve incidents. If the incident is not resolved within a given time, it will be escalated to Level Two Support.

11. **Level Two Support –** Level Two Support is a team of very knowledgeable resources who can solve a wide array of Commonwealth compute issues. This team largely knows the individuals in the agencies and has an ongoing relationship with them. When Level Two Support believes it cannot resolve the incident in a timely way, it will pull in Level Three Support resources.

12. **Level Three Support –** Level Three Support is a team of architecture experts that deeply understands the compute architecture that supports the Commonwealth

applications. This team is also an integral part of driving continuous improvement plan by identifying inefficiencies in the compute architecture.

Because of the Component Based Operating Model already described and the innovative approach to provisioning compute services, Commonwealth IT professionals may ask questions about how to provision workloads, how to manage and report on the workloads, and how to drive continuous improvement. To answer those expected questions, we provide brief summaries below.

"How do I provision workloads?"

The process will begin with logging onto the services portal that will be configured with a look and feel for each agency. In accordance with the agency and personal login credentials, users will be presented with the services they may provision. Provisioning a service will be an "Amazon-like" experience in which a user will select services from the catalog and provide quantity and key information to order the service. Once the "shopping cart" is filled, the order will be submitted and provisioned using the Service Broker. Each order processed by the ITSM system will have to be preapproved or approved when submitted. No runbook will be generated until a change is approved. Once a change is approved, the runbook will be executed to provision the desired service. Equally important, the CMDB will be automatically updated with the configuration information and the up- and downstream relationships as part of the runbook's execution.

"How do I manage and report in near real time the performance of those workloads?"

With the move to "IT as a business," it is imperative to be able to report in near real time the active performance, health, and quality of the IT services being provided to the Commonwealth. Unisys will provide real-time dashboards that are configurable by user preferences, meaning there are base profiles created for views for a CIO, CTO, Program Manager, and IT professional that enable these users to select the items they want to view on the dashboard. **Figure 2-10** is a representative example of a real-time dashboard.

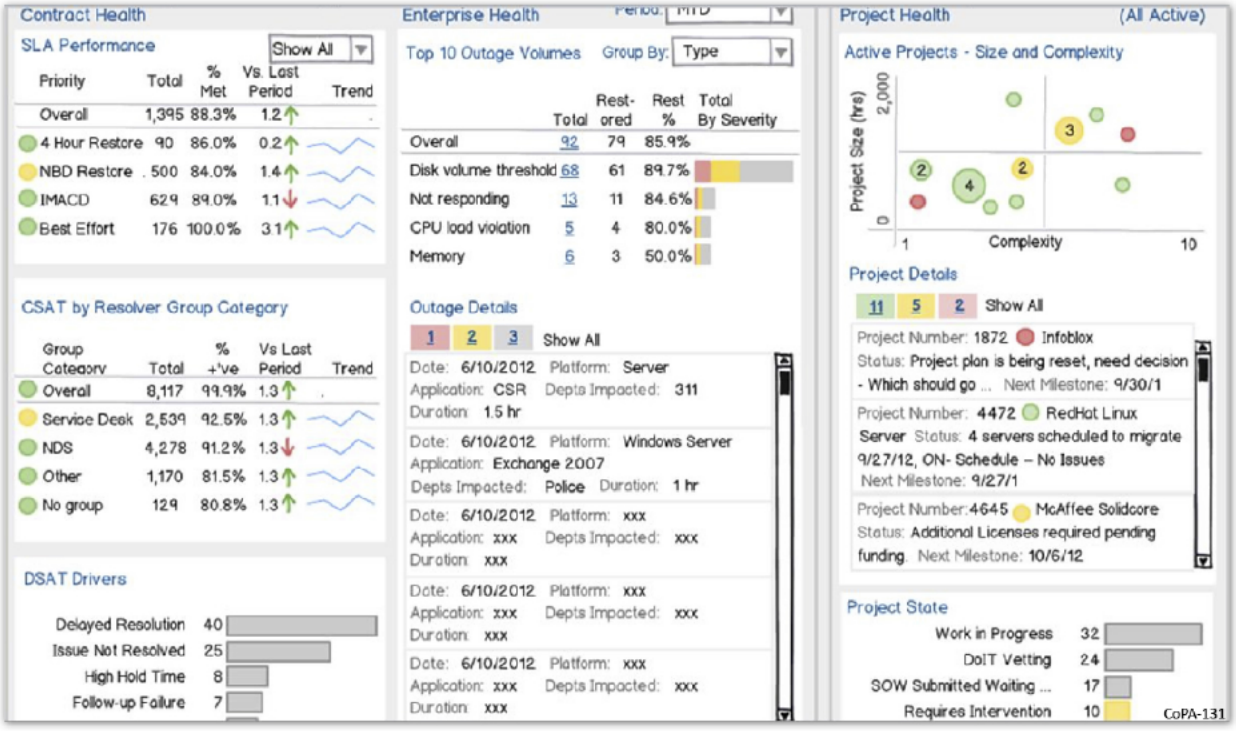


Figure 2-10. Real-time Dashboard

"How do I drive continuous improvement to drive greater value and cost containment?"

The Unisys team will provide a fulltime, dedicated Service Excellence Office. The office is responsible for driving Continuous Service Improvement to the Commonwealth throughout the entire ITIL V3 life cycle, across all Commonwealth Agencies, IT domains, and applications infrastructures. Unisys will apply Lean Six Sigma methodologies to analyze current and trending cycle times and defects collected from industry leading measurement tools. The Service Excellence Office will proactively eliminate anomalies to improve the operating environment from the time services are automatically provisioned through transition, implementation, and the ongoing IT Service Management. This will provide the Commonwealth with reduced costs, drive greater value, and increases quality while providing the Commonwealth with the highest client satisfaction experience.

To deliver and fully realize these solution's benefits, Unisys will develop and execute a comprehensive and reasonable work plan that focuses on the work effort to:

1. **Transition –** implement the component based operating model depicted in **Figure 2-9** across all future state data centers

2. **Migrate applications –** migrate the Commonwealth's applications to the new secure compute environment and immediately adopt the service reference architecture

3. **Implement Continual Service Improvement and Innovation Program (CSIIP) –** implement a continuous improvement program that drives out costs, generates additional value, and improves ongoing quality and client satisfaction.

Work Plan Overview – Simplified, Low Risk, and Based on Experience

> ***Work Plan** – Low Risk and Based on Experience*
>
> *Our competition may know the outsourcing business, but they do not know the Commonwealth to the degree of the Unisys Team. That is a critical distinction.*

Because of the critical nature of the Commonwealth's business systems, you cannot afford to have a service provider that needs to learn on the job. Unisys and our partners fully understand that the Commonwealth's critical business systems cannot be put at risk and that no unexpected downtime is acceptable. In building our proposed work plan, Unisys leveraged our knowledge and experience with the Commonwealth's infrastructure and business systems.

Our plan is realistic and achievable. During the first 18 months, the Commonwealth and our team will drive significant change. The realism of the Transition Work Plan is key to minimizing risk to the Commonwealth while we transform your current delivery processes and organization, implement new processes and organizations, and migrate applications from existing data centers to new locations.

On contract approval, Unisys will immediately initiate several actions. For example, the Unisys Team will mobilize in Harrisburg to begin the process of planning and initiating the transition. We will do this quickly because many of the identified resources are already on site and available to assist. Another action will be to formally stand up various governance teams and begin the flow of information. Some of our technical staff will prepare the various data center sites for migration and begin to install the network connections to COPANET. Concurrently, discussions will begin immediately to plan the [redacted] transition and DPH migration.

During this period and continuing through transition, our main responsibility will be confirming the current production systems are fully operable. Some of our current experts on these systems will actively engage with key members of the project teams; while others will maintain their focus on providing the high levels of service the Commonwealth has come to expect from our team. These experts will come together in the steady state to continue to provide and improve services that will meet or exceed all contractual commitments. **Figure 2-11** depicts the timeline for the various activities in the program.

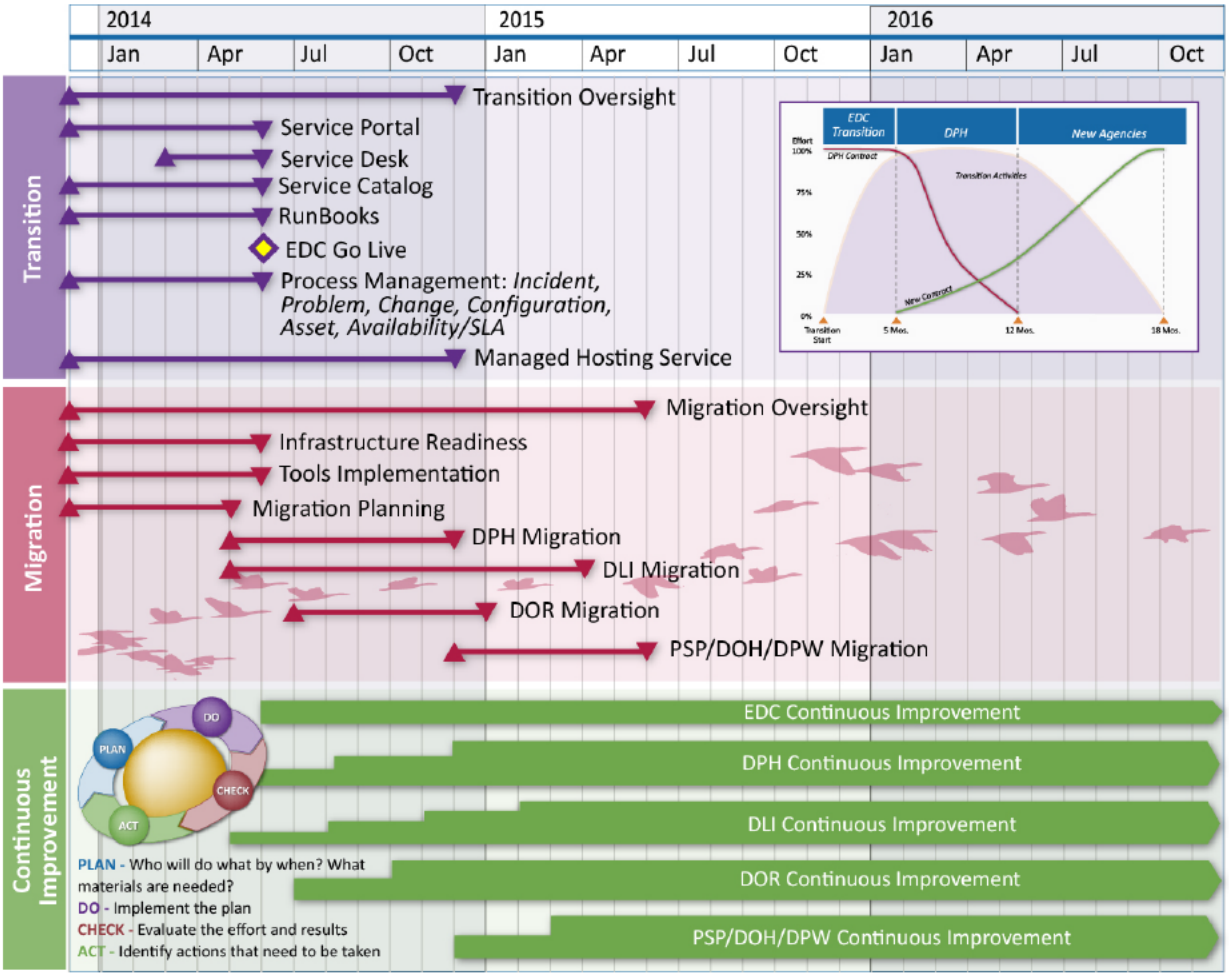


Figure 2-11. Work Plan Timeline

Transition

A major transition from the current operating model is required to achieve the objectives outlined in this RFP. Our approach to transition embodies our tenet of "Do No Harm." Therefore, we will use our detailed knowledge of the Commonwealth systems and lessons learned from prior transitions to mitigate risk. These include finalizing an aggressive but realistic transition plan with significant input from and approval of OA/OIT and the affected agencies.

Transition activities center on People (our team and your team), Process (policies, methodologies and procedures), and Technology (tools)—all required to successfully deliver the new component based operating model. One of the first tasks will be standing up our Program Management Office because it will play a key role throughout transition, transformation, and beyond.

At the core of our service delivery model is an IT Service Management Platform that supports the new processes and tools being implemented. This platform facilitates high-quality service delivery as well as improved sharing of information among all the new data centers, including the [redacted] However, achieving the new model differs, depending on where current applications are hosted. The major difference is that the [redacted] will not be moving; therefore, all the tasks for a physical move of IT infrastructure and applications will be unnecessary for the [redacted] An advantage for the Unisys Team is that we currently have significant technical resources helping to manage the [redacted] Also, one of our partners, Domino, manages the PennDOT systems in the [redacted] Together, we have knowledge of nearly all the technology. Therefore, we are very confident that we can methodically transfer total responsibility to our team in 6 months and very quickly the [redacted] will begin realizing the new model's benefits.

Transition and transformation of the DPH and the other agency data centers will require a complete relocation of applications and adoption of the new component based operating model. To accelerate the benefits of the new model to the Commonwealth, we architected the transition so that as applications are transferred to the new facility, they are operating in the transformed environment. That means you will receive value more quickly, and at the end of the transition, all systems will be transformed, in the steady state, and ready for a program of continuous improvement.

Application Migration

To migrate applications to the new data centers, the Unisys Team will be required to prepare the new data centers. These activities include establishing connectivity between COPANET and the data centers; establishing Commonwealth-specific infrastructure such as core LAN services; and implementing the infrastructure to support tools and shared infrastructure devices such as firewalls, backup, and monitoring. This project, Infrastructure Readiness, combined with the transition activities described above together will achieve the Operational Readiness milestone defined by the Commonwealth.

We will start with the DPH and then generally repeat the process (transition, infrastructure readiness, and so forth) above, incorporating additional lessons learned as we proceed. Again, a "Do no harm" strategy will be used to mitigate the risk of unplanned outages for all transitions and migrations.

In the Application Migration activities, there are three major focus areas:

- The first is **Operational Readiness,** which will provide the infrastructure and processes required to host applications. In these tasks, our team will create detailed designs and implement the Wide Area Network (WAN), Local Area Network (LAN), Storage and Backup infrastructure, Monitoring, Tools, Server Management, Dashboard, and Information Technology Service (ITSM) infrastructures.
- The second major focus area is the **Application Migration (AP) Planning,** which runs in parallel with Operational Readiness. In the planning framework, the AP team

will analyze application affinity information gathered electronically as well as in meetings with the agencies and their application owners to determine application move groups. Draft application move group packages based on the information gathered will be created, results of the analysis will show which applications are related to share infrastructure with potential latency dependencies, schedule restrictions, size, complexity, or relate to and depend on other applications. A typical move package will not exceed 125 servers, instances, or images, including Wintel, Linux, or AIX instances and mainframe images. Applications will be targeted to the facility that provides the most benefits, but the Commonwealth will be the final approving authority of any plan.

- The last is the **execution of the migration plan** that overall will move thousands of agency applications in manageable phases. This by far will be the most intensive and most important of all the activities. Even though our team has significant knowledge of the various applications, this must be a collaborative effort with agencies to prevent unexpected interruption of the business of government. The Unisys Team will work closely with the OA/OIT and the agencies to develop detailed plans for each application to be migrated. These plans will include an Hour-by-Hour (HxH) plan, which will detail the step-by-step plans for the test, re-IP, and move events, which will include all precautions required to provide the appropriate level of security needed, fallback plans, testing and acceptance criteria, which will be used to determine the event's success.

As illustrated in **Figure 2-11**, the [redacted] transition and transformation are planned to occur within 6 months, DPH within 12 months, and all agency data centers within 18 months. This schedule exceeds the requirements of the RFP and we believe is reasonable.

To oversee all these transition and migration activities is Unisys Transition and Program/Project Management. The Transition Executive, Scott Lorah, will provide a collaborative, transparent, and candid process for the development and management of the plans, adherence to the plans through verified accomplishments, risk management, issue management, quality deliverables, and process improvement. The emphasis of our approach is to provide clear analysis of progress, identify opportunities for improvements, review lessons learned, and implement best practices for each project.

The Unisys Program Management Office (PMO) will have overall responsibility for meeting the contract requirements. Also, guiding and overseeing the Transition Program will be a Program Steering Committee comprising members from OA, agencies, Unisys, and our partner IBM. Also, Project Steering Committees will be used to guide and oversee each of the agency-focused projects.

"Security is Paramount"

Protecting citizen data has always been extremely important to the Commonwealth. Security becomes even more important as the Commonwealth transitions to the proposed on-demand compute environment; quite simply the agencies must have the confidence in the security of the new environment to meet their diverse regulatory requirements such as

CHRIA, FERPA, HIPAA/HITECH, IRS 1095, PCI and CJIS during transition, and steady state operations. The Unisys team understands this is fundamental to the success of the initiative and is committed to a successful transition and operation of the new environment with security being paramount in all decision making.

Consequently, we take a holistic approach to security. We leverage our teaming partner - Deloitte's robust public sector security risk framework that integrates several regulatory requirements, as the foundation of our security management plan. This readily available catalog of rationalized regulatory requirements and controls will help us appropriately address the people, process and technology aspects of our security solution. Also, the Unisys Team has very experienced, nationally recognized security experts that we will engage when preparing and executing our security specific security management plan for the Commonwealth.

As illustrated in Figure 2-12 below, the Commonwealth ITBs, policies and agency regulatory requirements drive the Security Management Plan, which in turn becomes the implementation blueprint of our datacenter security solution.

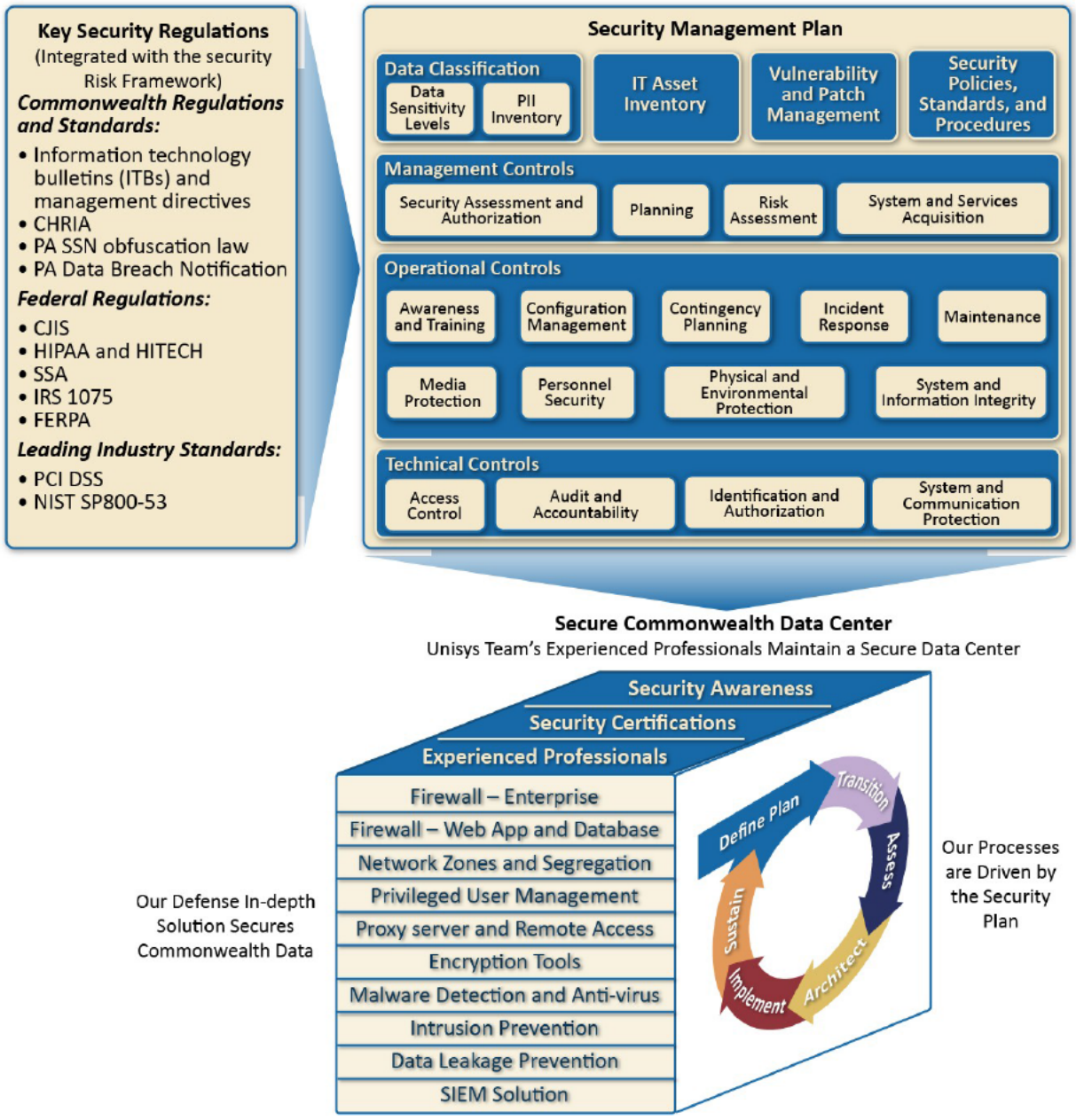


Figure 2-12. Our Holistic Datacenter Security Solution is Driven By the Security Regulations

Security Management Plan. The compute environment's security management plan is driven by Deloitte's demonstrated public sector security framework - containing over 3,500 individual regulatory requirements mapped to almost 300 unique integrated requirements that include NIST SP800-53 rev4, CJIS v5.1, CHRIA, HIPAA/HITECH, PCI DSS v2/3, SSA and IRS 1075 rev8-2010. This framework is flexible to add additional controls and regulations as agencies face the need to comply with new regulations and controls. The success of the security framework, particularly the flexibility it provides to "assess once and comply with many regulations", is demonstrated in its use in over 10 states - where the security framework is used to integrate and

assess security regulatory requirements in systems development efforts and conduct integrated enterprise security assessments.

During transition we use the security risk framework as the foundation, validate the agency requirements, systems security architecture and classify data, and develop and establish the security management plan. The plan describes how the integrated controls are implemented consistently across the compute facilities

We will perform an annual review and update of the security management plan to keep the Commonwealth abreast of their emerging security needs. Schedule F, section 3.2.2.5 Security Management Section provides more detailed description of the security management plan, and how agencies will be able to obtain their individual regulatory requirement views to meet their regulatory and compliance needs.

Security Solution. Using the security management plan as the blueprint, the Unisys security solution is designed - taking into consideration the people, process and technology. The solution is implemented consistently across the data centers.

Security Technologies: The data center security solution is designed and implemented during the transition along with established processes for continual improvement during ongoing operations. We have selected leading security technologies to provide defense in depth protection that includes:

Security Processes: We implement and operate the security technologies using processes rooted in the ITIL framework. The security governance is carried out with transparency – by sharing the alerts, risks and issues with the Commonwealth's Chief Information Security Officer (CISO) and agency security officers. The service portal provides customizable dash boards for the CISO and agencies for them to see relevant security metrics and allow for collaborative and transparent management processes to help effectively manage the security risks and issues.

Security Team: We have a proposed a world class security team, led by Mike Sheketoff and supported by our teaming partner Deloitte, who play a significant role during transition by performing the baseline security assessments, security architecture reviews and developing the security management plan. Again, all our efforts will be coordinated with the Commonwealth's security team to ensure we are meeting all expectations and leveraging their vast knowledge of the Commonwealth's security landscape. Deloitte's large pool of qualified specialists, helps us implement security technologies like data loss prevention and database firewall solution, perform quarterly vulnerability tests and annual updates to the security management plan. The Unisys team operates the security environment with trained professionals, following the ITIL process foundation. We provide more details of our proposed security operations and solutions in Schedule F, Section 3.2.4.6.

On-going Security Thought Leadership: The Commonwealth enterprise must secure a significant amount of extremely sensitive and confidential data. Internal and external threats continuously test the security measures that protect this data. These threats are ever increasing and are dynamic. Concurrently government budgets are becoming smaller while the need for enhanced security is growing much larger. To meet this need Unisys proposes two additional enhancements to our security proposal.

The first would be to conduct regular security educational seminars with agency leadership to provide greater visibility and understanding about the need and value of a comprehensive security program. The seminars would also provide updated information on threats and what agencies can and should do to mitigate these threats. Unisys proposes that these seminars would be a joint effort between the Unisys Security Team and the Commonwealth CISO.

The second enhancement is Unisys developing and supporting an ongoing Cyber-Security Research and Development Initiative to identify best practices, as well as new security processes and tools, and then test new products and processes in a controlled environment.

The recomended home for this initiative would be Harrisburg University since they have a comprehensive security curriculum, availability to faculty and students as needed, and lastly security topics that directly impact government could be featured at the Government Technology Institute's Innovation Center. The knowledge coming from the Center could be integrated into educational programs such as the Certified Government CIO (CGCIO) and Government IT Managers (GITM) programs. That would ensure this valuable information becomes an integral part of professional development for current and aspiring government IT leaders. Again, decisions related to the initiative and its operations would be guided by the Commonwealth CISO.

Collectively these enhancements to our proposal restate our commitment to security and recognize the need for the Commonwealth to have all of the tools it needs to combat the increasing threat of cyber-crime.In summary, we understand the importance of meeting the diverse agency security requirements through meticulous planning, and implementation of a robust security solution. We have assembled a team of world class specialists with demonstrated success at the Commonwealth, to implement the next generation security that is critical for the new compute environment. **Our solution and our people will closely couple with the Commonwealth's security requirements and their security experts. The blending of our respective expertise and experiences will provide a comprehensive approach during and after the transition of the Commonwealth's most sensitive data and computing resources.**

Continuous Improvement

Unisys will establish a dedicated Service Excellence Office that proactively manages continuous service improvement, ITIL V3 process management, quality, and customer satisfaction through a comprehensive Quality Plan. This quality plan will focus on continuous service improvement, reducing risk, improving service quality, client satisfaction, and transparency, while reducing overall IT costs. We believe this is a key differentiator in our partnership with the Commonwealth. Unisys will develop, implement, manage and govern two detailed Quality Plans. The initial Quality Plan will be a Transition Quality Plan to make sure that quality is a primary focus in the critical Transition of the

Commonwealth agencies to the new IT Services contract. Unisys will then develop and manage the IT Services Management Quality Plan, for steady state ongoing operations.

As applications are migrated to the new data centers, they will operate using the new tools and processes, thereby realizing the benefits of the new compute services model. Once applications and systems are transformed, they will reach the steady state. The future steady state model will leverage disciplined processes aligned with ITIL V3 best practices and accountability to deliver against stringent SLAs across more than 30 categories. This evolution from the current state to the future state will leverage state-of-the-art technology and tools coupled with the component based operating model as defined in **Figure 2-9**, and up-to-the-minute statistical reporting across the enterprise displayed on high-tech dashboards at the fingertips of Commonwealth agencies.

To keep these systems optimized, we propose an active and ongoing program to continually find new technologies or new processes that improve performance or lower the cost of operations. We call this our Continual Service Improvement and Innovation Program (CSIIP).

To optimize performance for the Commonwealth during steady state operations, Unisys will implement an ongoing program of Continual Improvement, as depicted in **Figure 2-12**. We developed and use a methodology that has worked well for our clients worldwide, and we will implement it at the Commonwealth. Collaboration is the main premise, and we know from experience that the Commonwealth wants to actively participate in bringing positive change to its compute operations. This program will be led and sponsored by the Service Excellence Office on the Unisys Team.

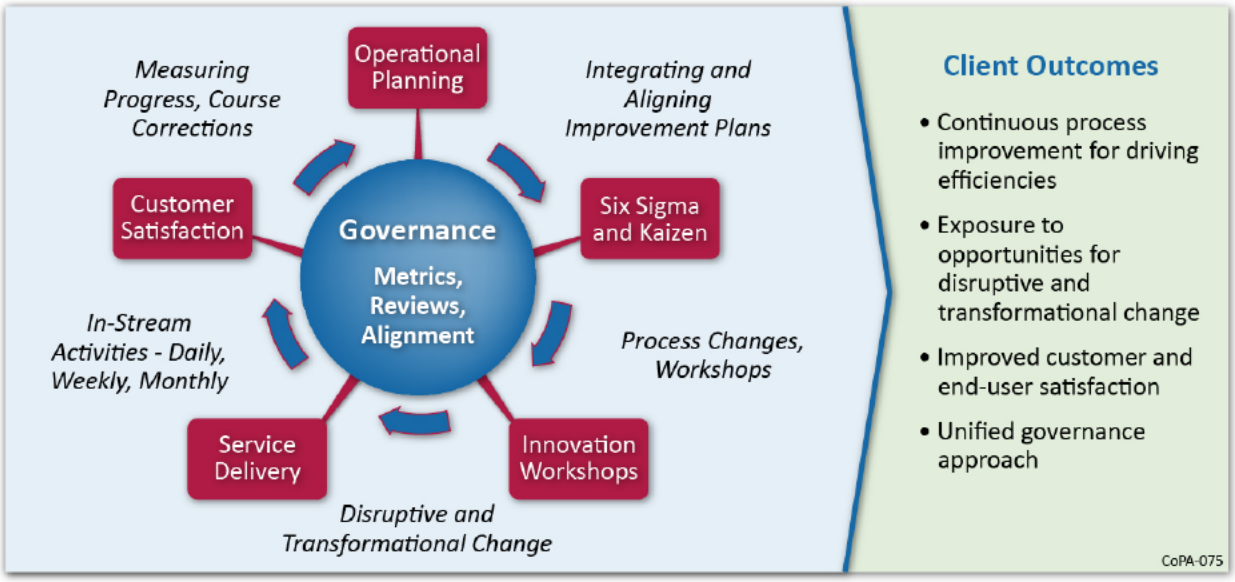


Figure 2-12. Continual Service Improvement and Innovation Program (CSIIP)

Rather than an ad hoc compilation of capabilities, tools, and methods, the CSIIP provides Unisys with a continuous and systematic way to deliver improvement and innovative outcomes for the Commonwealth by leveraging a highly structured yet flexible approach depicted in **Figure 2-12**. Two key elements include our CSIIP and Innovation Workshops.

"The Commonwealth has been a valued Unisys customer for many years. Together, we successfully completed major projects that have provided significant innovations and value like the DPH. I am confident that, if entrusted with this most important engagement, our team will raise the bar even higher for the Commonwealth and its citizens."

[redacted]
Commonwealth Executive Sponsor
Chairman & CEO

The CSIIP process includes two types of workshops, Improvement/Kaizen or Innovation Workshops. We will use a global pool of trained facilitators who have conducted workshops across a wide range of industries worldwide.

Improvement/Kaizen workshops are joint sessions between the Commonwealth and Unisys, which focus on identifying opportunities for improvements and categorizing, prioritizing, and developing high-level business cases and implementation roadmaps for the most promising opportunities. Opportunities are governed on a SharePoint portal to provide agencies with visibility and transparency to the continual improvement process.

One of the CSIIP's major features is the ability to consolidate and analyze the many inputs required to effectively develop an innovation and improvement plan. This will provide the Commonwealth with the necessary information to make informed decisions based on relative cost/benefit, alignment with strategy, and ROI for various actions of varying scale from incremental through to truly "breakthrough" initiatives.

Unisys will also collaborate with the Commonwealth by hosting innovation workshops to drive continuous innovation. These workshops will focus on opportunity identification, categorization, prioritization of innovation opportunities, and then on the development of high-level business cases and implementation roadmaps for the most promising opportunities identified.

Innovation is what drives businesses and organizations to excel and is required to meet the ever increasing need for 'faster-better-cheaper.' Unisys' approach looks at all aspects of innovation (strategy, people, process and technology). All are required to be aligned for a program to be successful and impactful. Unisys will work with the Commonwealth and its agencies to clearly understand their strategic IT vision and then work with the each to provide a programmatic approach to innovation. Unisys will work with the Commonwealth to implement a "high-yield innovation pipeline" process to identify and incorporate new innovations into the Commonwealth Agency's IT and infrastructure for the Pennsylvania citizens receiving services.

The work plan we identified will provide a thoughtful, realistic, and achievable roadmap to meet the RFP's requirements, and just as important your high expectations for delivering a solution that will make the Commonwealth a leader in enterprise compute services.

Innovation Workshops

Unisys Innovation Workshops are collaborative workshops with the Commonwealth designed to explore opportunities for disruptive and transformational change. We will expose the Commonwealth to the latest disruptive technologies and trends and collaboratively examine opportunities for strategic business benefit.

Why the Commonwealth Should Choose the Unisys Team?

All critical services delivered by Commonwealth agencies will depend on this engagement's success. Therefore, it is vital to identify and mitigate all risks so the transition to a new operating model can happen without unplanned outages or reduction in service levels. The consequences of failure are immense and frankly unthinkable.

The Unisys Team of premier technology and service companies has the most experience and knowledge specific to the Commonwealth. As the Unisys Team has been the sole provider of managed DPH services to the Commonwealth, no other offerer can claim this level of expertise. Our experience includes a 13-year track record—measured and reported monthly—that no other team can claim. We have vast knowledge of the existing infrastructure, thousands of agency applications, and Commonwealth processes and business environment. This experience and knowledge will be essential to mitigate risk associated with this innovative endeavor and ultimately meet your high expectations.

And because we are your current service provider, we have greater flexibility and offer more opportunities to customize the work plan to further mitigate risk and meet individual needs of the many agencies that depend on these services. The challenge of the DPH contract's termination on December 31, 2014 will become much less of an issue.

In 1999, we accepted the challenge of consolidating the Commonwealth's 17 data centers and succeeded. In 2008, we accepted the challenge of reinventing Commonwealth operations to shared services, saved $240 million and succeeded. Now in 2013 and beyond, we are totally committed to accept this new challenge and successfully deliver the results expected by this RFP.

This page intentionally left blank.

3.3.2.1 Transition Program Management

The TPMO function confirms the non-disruptive migration of Commonwealth information Services from current Commonwealth host locations, to the Offeror provided multi datacenter environments.

The Offeror must establish a TPMO and develop the requisite transition plans.

A transition approach and detailed transition plan for each of the Commonwealth's existing Datacenters must be developed by the Offeror and approved by the Commonwealth. The Commonwealth has over 2,000 business applications with over 50% designated mission critical. The Offeror must work with each agency to determine its application environment within each facility. The Offeror's target datacenter environment must be configured and tested prior to migration of the application.

Reference Documentation

Schedule D - Transition Milestones

Exhibit D.7 - EDC - Facility Summary

Exhibit A - Commonwealth Network Environment

Exhibit(s) B.1 through B.6 - Data PowerHouse (DPH) Exhibits

Exhibit(s) C.1 through C.13 - Department of Public Welfare (DPW) Exhibits

Exhibit(s) D.1 through D.15 - Enterprise Datacenter (EDC) Exhibits

Exhibit(s) E.1 through E.43 - Department of Labor & Industry (DLI) Exhibits

Exhibit(s) F.1 through F.4 - Department of Health (DOH) Exhibits

Exhibit(s) G.1 through G.16 - PA State Police (PSP) Exhibits

Exhibit(s) H.1 through H.8 - Department of Revenue (DOR) Exhibits

Exhibit(s) I.1 through I.13 - Commonwealth SAP Environment - Integrated Enterprise Services (IES) Exhibits

Exhibit L - Commonwealth Master Application Inventory

Exhibit(s) M.1 through M.7 Department of Corrections (DOC) and Pennsylvania Board of Probation and Parole (PBPP) Exhibits

Exhibit(s) N.1 through N.2 - PennDOT Exhibits

Requirements		Describe Compliance
1.	Establish a TPMO to manage all	Offeror must describe the proposed TPMO,

	information service transition activities. The Office will be jointly administered by Offeror and Commonwealth staff. Provide a communication plan that will provide an information vehicle for all interested parties.	and discuss the mission, goals and objectives, and the roles and responsibilities of the Offeror. Offeror must provide at least one sample where Offeror has successfully created an office similar to the required TPMO.
2.	Provide a functional organization chart for the TPMO, including an estimate of the type and number of full time Offeror resources that will be required to ensure the successful transition of Services from current multiple datacenters to the Offeror's datacenter Services.	Offeror must describe the TPMO structure including but not limited to the number of full time resources and the role of the TPMO in the transition.
3.	Analyze applications and design the required computing architecture to migrate Commonwealth datacenters to Offeror datacenter environments. Hardware, software, network, etc. Work with Commonwealth technical staff to ascertain the requirements to successfully migrate processing to Offeror datacenter environments	Offeror must describe solution and approach to meet this requirement. Offeror must provide at least one relevant example from a prior engagement, in which it was engaged, that is similar to the needs of the Commonwealth.
4.	Optimize Current Process and Procedures – Coordinate with Commonwealth agencies to review and plan for a transition of processes and procedures.	Offeror must describe its overall plan for optimization of the existing processes, procedures, tools, etc. to provide more efficient and effective Services. The description must include approach, plan, and methodologies.
5.	Revise datacenter DR plans on the occasion of major changes to the datacenter hardware, software, or network portfolio to reflect those major changes.	Offeror must describe solution and approach to meet this requirement.

6.	Establish an IT infrastructure that meets all application processing requirements. The Offeror must confirm that the target IT infrastructure meets or exceeds current computing requirements. Work with Commonwealth technical staff to design and build the infrastructure required to support the applications being migrated to the Offeror multi datacenter environment.	Offeror must describe solution and approach to meet this requirement. Offeror must provide at least one relevant example from a prior engagement, in which it was engaged, that is similar to the needs of the Commonwealth.
7.	A multi-faceted Transition Strategy will be required: • Comprehensive; • Non-disruptive; and • Compliant with Commonwealth requirements. The Strategy will address the transition of: • Shared infrastructure elements, as appropriate; and • Specific information Services. • Disparate Agency application architectures and impacts to move to the new environment(s) The Strategy must also address the following: • Cost/Benefit for the Agency • Risks and Risk Mitigation Plan The migration order of the Commonwealth datacenters will be provided by the Commonwealth.	Offeror must describe the transition (interim and steady state strategies) and transition plans that it has employed during other similar size engagements.

8.	Identify mandatory requirements and critical success factors that will have a direct impact on developing a successful transition plan	Offeror must describe the 3-5 characteristics, conditions, or variables it believes will have a direct and critical impact on the effectiveness, efficiency, and viability of the Offeror's solution. Offeror must describe its approach to mitigating risks and ensuring these critical factors are successfully addressed.
9.	Create a Transition Timeline that outlines the overall timeline starting at effective date and continues through delivering transition Services for each of the targeted datacenters.	Offeror must describe the overall timeline from the start of pre-Transition activities through the point at which the Offeror expects it will be delivering predictable, repeatable Managed Service Results that meet the requirements of the RFP. The schedule must include a description of the critical milestones related to Transition efforts for each targeted Commonwealth datacenter. Any critical milestones identified must be included in the Transition Project Plan.
10.	Create a generic Infrastructure Element Transition Plan that may be readily adapted to accommodate specific infrastructure element transitions. Create a prospective Infrastructure Element Transition Plan. Appropriate EDC, DPH and other Agency Datacenter hardware elements may be re-purposed wherever possible.	Offeror must describe a realistic Transition Project Plan to transition the Commonwealth's datacenters to the proposed architecture.

11.	The EDC Managed Services datacenter assets must be managed and maintained by the Offeror until they are transitioned to the Offeror's managed Services. The current maintenance contract for the EDC servers is scheduled to expire on June 30, 2014.	Offeror must describe its transition approach to address the transition of operations and management of the EDC infrastructure from the Commonwealth to the Offeror's support Services and how it intends to address the server maintenance expiration issue.
12.	Create, manage and execute an application / infrastructure migration plan. The Offeror has the primary responsibility for planning and executing the transition of infrastructure elements, with support of Commonwealth technical and business support staff. The Offeror must provide adequate tools and techniques for moving and migrating Commonwealth data to the new target storage environment. The Offeror must ensure that critical applications are not decoupled from key infrastructure components causing system latency.	Offeror must describe solution and approach to meet this requirement. Offeror must provide at least one sample where it has successfully migrated application and hardware. Offeror must describe its proposed tools and techniques for moving and migrating Commonwealth data to the new target storage environment.
13.	Create a generic Information Service Transition Plan that may be readily adapted to accommodate specific information service transitions.	Offeror must outline a prospective Information Service Transition Plan to take over support of migrated Commonwealth systems and applications. Offeror must provide at least one sample where it has successfully completed application and hardware migrated.
14.	Meet with Commonwealth to produce and execute specific Information Service Transition Plans. Select cut over windows that minimize system unavailability and coordinate approval with the affected agency.	Offeror must describe solution and approach to meet this requirement. Offeror must provide at least one relevant example from a prior engagement, in which it was engaged, that is similar to the needs of the Commonwealth.

	Communicate to the Commonwealth cut over date and times. Setup a special call number and support staff to take calls concerning the migration, these Services must be made available to transitioned users until the transition is officially signed off as completed. .	
15.	Work with Commonwealth to create testing, business acceptance and fallback plans.	Offeror must describe solution and approach to meet this requirement. Offeror must provide at least one relevant example from a prior engagement, in which it was engaged, that is similar to the needs of the Commonwealth.
16.	Service Management Systems – Offeror must transition all agency system management platforms currently in place to the Offeror, consolidating all system management responsibilities. The Offeror must make available all system management platforms and tools that are currently supporting the Commonwealth infrastructure.	Offeror must describe solution and approach to meet this requirement.
17.	CMDB – Work with the Commonwealth to acquire asset information to support the asset management system and configuration management system.	Offeror must describe its approach to capturing, validating and storing all configuration information required to perform the Services within 120 days of the Effective Date of the Contract. In particular, the Offeror must address how it will identify and relate critical associations (e.g. Application to Server, Server Tier to Application, Application to Disaster Recovery Time Objective, software to server, etc.) for the enterprise. Offeror must describe its approach to transitioning the data and related processes from the existing CMDB or equivalent

		system/database to the Offeror's solution and how the Offeror must ensure accuracy of data across Service Management areas to ensure accurate and timely invoicing and chargeback to the Commonwealth.
18.	Chargeback – Work with the Commonwealth to interface with the Commonwealth's billing processing and validation ITSM system to provide a chargeback system for new and existing Services available on the Offeror's Service Catalog.	Offeror must describe its transition approach to Chargeback Management. Offeror must describe its approach to assisting the Commonwealth in transitioning Commonwealth customers from the existing Chargeback system. The description must include an expected analysis of the current billing system environment, expected termination assistance, communications plans, strategy for testing and major milestones.
19.	Identify Options and Costs – List the appropriate different options that will satisfy the requirements of the transition scope. Communicate options with the Commonwealth and obtain approval on selected option(s) to proceed.	Offeror must describe proposed approach.
20.	Expand/reconfigure datacenter facilities to accommodate growth in Commonwealth information and information systems.	Offeror must discuss its approach; the expansion/reconfiguration plans must include the EDC.
21.	Produce weekly reports on the progress of the information service transition initiatives.	Offeror must describe its proposed approach to providing weekly transition progress reports.
Deliverables		
Deliverables are defined in **Schedule K – Key Program Deliverables**		

Offeror Response

3 Requirements Analysis Approach

3.A Analyze applications and design the required computing architecture to migrate Commonwealth datacenters to Offeror datacenter environments. Hardware, software, network, etc.

Offeror must describe solution and approach to meet this requirement.

The Commonwealth benefits from the 13+ years of experience the Unisys Team has supporting the Commonwealth of Pennsylvania and its key applications residing in the Data PowerHouse and Enterprise Data Center. The Transition and Data Center Methodology utilized by Unisys keeps the applications at the center of focus.

The first step in planning the Transition is to understand the applications supported within each data center. The Unisys Team will accomplish this during the Data Gathering phase leveraging [redacted] tool to understand all applications running in the environment and their relationship to each other and to the infrastructure. Additionally the Commonwealth may choose to request two additional tools through a service request in situations where the application owners may need additional help to identify technical requirements. [redacted] the industry leading asset analytics tool, gathers detailed infrastructure information to provide the appropriate future-state infrastructure environment for each application/component. The application owners will also have at their disposal a process developed by Unisys Team members called Application Performance Impact Assessment that takes a top-down approach to identify those applications that are critical and require a deep dive. The process is supported by tools and software utilized for latency issue detection and validation.

Once the information gathering and documentation is complete, the Unisys Team will generate a draft move package grouping based on the application dependencies, the number of applications, and the number of servers. The move package groupings are reviewed at an application grouping level with representatives from the Commonwealth prior to creating the initial project schedules. The project team and application owners will provide a detailed review and input into the detailed project schedules. This input will include a review of the scope of each application, confirmation of related applications as well as input into the appropriate day, date and time of day that reduces the impact to the stakeholders who utilize the application(s).

During the project, additional attention is paid to each application to provide a smooth migration. These tasks include reviewing the applications for hard coded IP addresses, firewall rules, and other issues that may occur during the migration. Based on the information gathered and the analysis of application requirements, the required computing architecture at the target data center environment will be reviewed and validated accordingly. Development and execution of detailed test plans both before and immediately after the migration is required to verify the application will execute as expected. Lastly, each migration project is not completed until the application owner has confirmed the application executes as expected.

6.C Work with Commonwealth technical staff to design and build the infrastructure required to support the applications being migrated to the Offeror multi datacenter environment.

Unisys will provide a network of data centers that supports relocation of Commonwealth applications. All Unisys data centers other than the EDC are Uptime Institute Tier 3 equivalent facilities.

The EDC workload will remain untouched except for provision of metering for the computer room. Updates to the facility infrastructure including BMS, UPS, generators, and air conditioning will be presented for Commonwealth approval.

7 Multi Faceted Transition Strategy

7.B The migration order of the Commonwealth datacenters will be provided by the Commonwealth.

The Migration Strategy will address the transition of: Shared infrastructure elements, as appropriate; and Specific information Services. Disparate Agency application architectures and impacts to move to the new environment(s)

Unisys proposes a phased and comprehensive approach in assessing and implementing data center migrations and consolidations. This approach focuses on several key areas. First, we identify risk and risk mitigation. Unisys treats these moves like a controlled disaster recovery – every action is planned, tested, and validated with documented, rehearsed back-out and contingency plans. Second, is the business and application centric approach, we take the time to detail business requirements and understand application interdependencies disruption to the business. Finally, we use a thorough and comprehensive program management methodology to making the data center migration as smooth and non-disruptive as possible and will not short-cut planning activities.

Phase 1, Data Gathering and Analysis, will concentrate on developing a complete understanding of the current application and infrastructure inventory. Based on this information Unisys will be able to identify the requirements that will be used as inputs to the overall migration plan. A master migration plan will be negotiated with business stakeholders strives to minimize potential impacts to normal business operations. Phase 1 will concentrate on the following key areas:

- Project and resource planning
- Application inventory and physical asset inventory
- System and Application Mapping including dependencies and interdependencies
- Identification of either assets or application that will be retired, moved or consolidated
- Identification of requirements such as outage windows, change control process, validation needs, site availability and capacity constraints
- Aligning the applications and systems into move groups or migration bundles
- Selecting migration strategies and technical requirements for each application
  - Based upon Application RTO and RPO
  - Physical moves, data migrations to new “seed” equipment at the target site are two examples of migration strategies
- Building of a Master Migration Schedule

The overall goals of Phase 1 are to discover the assets to be moved and gain consensus on a migration schedule.

Phase 2 is the detailed site planning that establishes target site readiness to host the moved assets. Design of the new storage assets, verification of network and facilities plans, and a rollout plan for new assets are completed at this time. Key goals for this period include:

- Validate that target site build-out plans will meet the time and infrastructure needs for the asset migration
- Validate that new storage infrastructure is designed appropriately and in order
- Validate that new server roll-outs are timed appropriately to meet migration schedule
- Finalize all scheduling for transportation and OEM re-certification of assets

At the conclusion of Phase 2, Unisys and the Commonwealth will agree to initiate migration activities.

Phase 3 is the execution of the move plans. For each of the move groups, Unisys creates detailed task level runbooks that choreograph every action during the move. These plans are tested via table top exercises; the actual moves are coordinated by the Unisys Team and tested by the application support teams. Key activities include:

- Finalizing detailed night of move project plans
- Completing migration workbooks containing detailed procedures for application shutdown, server power-off/power-on, and other key technical activities
- Testing and rehearsal of move activities
- Final site visits to confirm target site is ready for asset move
- Disassembly, packaging, transportation and re-assembly of all assets
- Verification of proper functionality at target site

Phase 3 concludes with the Commonwealth's acceptance of the Data Center migration.

Unisys Data Center migration methodology has been successful in dozens of large data center moves. Key to our success is a disciplined quality assurance program. Unisys will assign a subject matter expert not directly involved in the engagement to review the project at pre-determined points in time known as "QA Gates." The QA reviewer will look for issues that create risk in several areas with an emphasis on those that may jeopardize the migration timelines or pose a threat to maintaining normal business operations. The QA reviewer will meet with a set of Client stakeholders and project sponsors to review how well Unisys is meeting expectations. Chart in **Figure 3.3.2.1-5** summarizes the steps in the methodology and the estimated QA Gate timing.

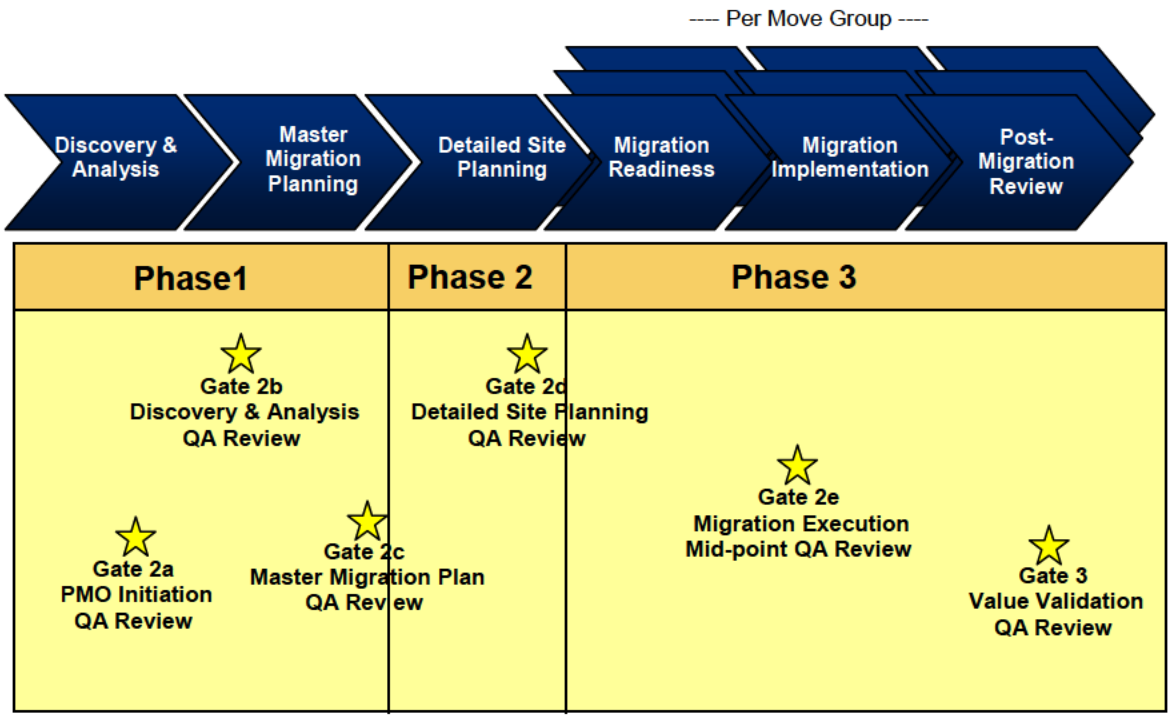


Figure 3.3.2.1-5 – Migration Phases

Once move groups are established the data center migrations will be accomplished using a variety of tools and techniques. The type of migration will be suggested by the Unisys Team but in all cases reviewed and agreed upon by the application owners.

The primary methods will be:

- Over-the-Wire – This is also known as P2P, V2V or Seed. This option will minimize the duration of the application outage required. For over-the-wire moves, seed hardware is first located in the receiving site and made production ready. A small application is placed on each server in the sending site to replicate the OS, application and application data onto the specific drives at the receiving site. Installation of the application is done during a monthly planned outage. An initial copy is executed soon after installation and sync copies are periodically executed leading up to the move event. During the move event, a final sync copy is taken after the application is shut down to verify all data and updates have been received in the new data center. Once the final sync is completed, the hardware in the sending data center is shut down and the application in the receiving data center is brought up. Once fully started, the application support team will execute the test plan created during the planning process. After a successful test, the test, the application owner will sign-off that it is ready for turnover to the end users. Using this option requires a shorter application outage. This method has low to moderate risk and a lower cost profile when utilized on assets with less than one year of expected life. As the age of the equipment increases so does the risk but the cost profile decreases due to the expectation of replacing the aging hardware.
- Lift and Shift –This option requires the applications to be shut down by the application support team, the supporting infrastructure will then be shut down and taken out of the racks, placed in shipping containers and transported to the new site via a dedicated professional moving partner. For applications that utilize shared storage, in most cases,

the data will be migrated over the wire using a data pre-application tool prior to the start of the event. In some cases, the project team may choose to ship data via tape. Once at the new site, the servers will be re-racked, cabled, and powered up according to the processes provided by the application support team. Once fully started, the application support team will be expected to execute the test plan created during the planning process. Once the team has successfully executed the test, the application owner will sign-off that it is ready for turnover to the end users. Using this option requires a longer application outage. This method has low to moderate risk and a low cost profile when utilized on assets with greater than one year of expected life. As the age of the equipment increases so does the risk and cost profile.

A third option exists which is a variation of the Over-the-Wire option.

- Seed with Greenfield – In this option, seed hardware is installed in the receiving data center, the operating system is installed directly on the hardware, the Application is installed and then the application's data is copied. Once fully started, the application support team will execute the test plan created during the planning process. Once the team has successfully executed the test, the application owner will sign-off that it is ready for turnover to the end users. Using this option requires a shorter application outage but presents a high risk profile and a higher cost profile.

In all cases, minimal changes are made to the environment to minimize the risk and expedite resolution of any incidents discovered during the migration events.

Early in the planning process, the Project Managers will work with the Application Owners to identify and agree on the migration method for each infrastructure device supporting an application being migrated. In most cases, shared services infrastructure devices such as Storage and Virtual Machines (VM) will be migrated over-the-wire to allow for flexibility in move package creation.

9 Transition Timeline

9.A Create a Transition Timeline that outlines the overall timeline starting at effective date and continues through delivering transition Services for each of the targeted datacenters.

Any critical milestones identified must be included in the Transition Project Plan.

Figure 3.3.2.1-7 below shows a high level timeline of projects and activities as compared to the Commonwealth's Milestones. The Unisys Team is uniquely able to accomplish this accelerated timeline as a result of the close relationship our team has delivering current and prior projects with the Commonwealth. We save time on the DPH and EDC migrations by skipping over the major learning curve of a vendor that is not currently supporting Commonwealth environments.

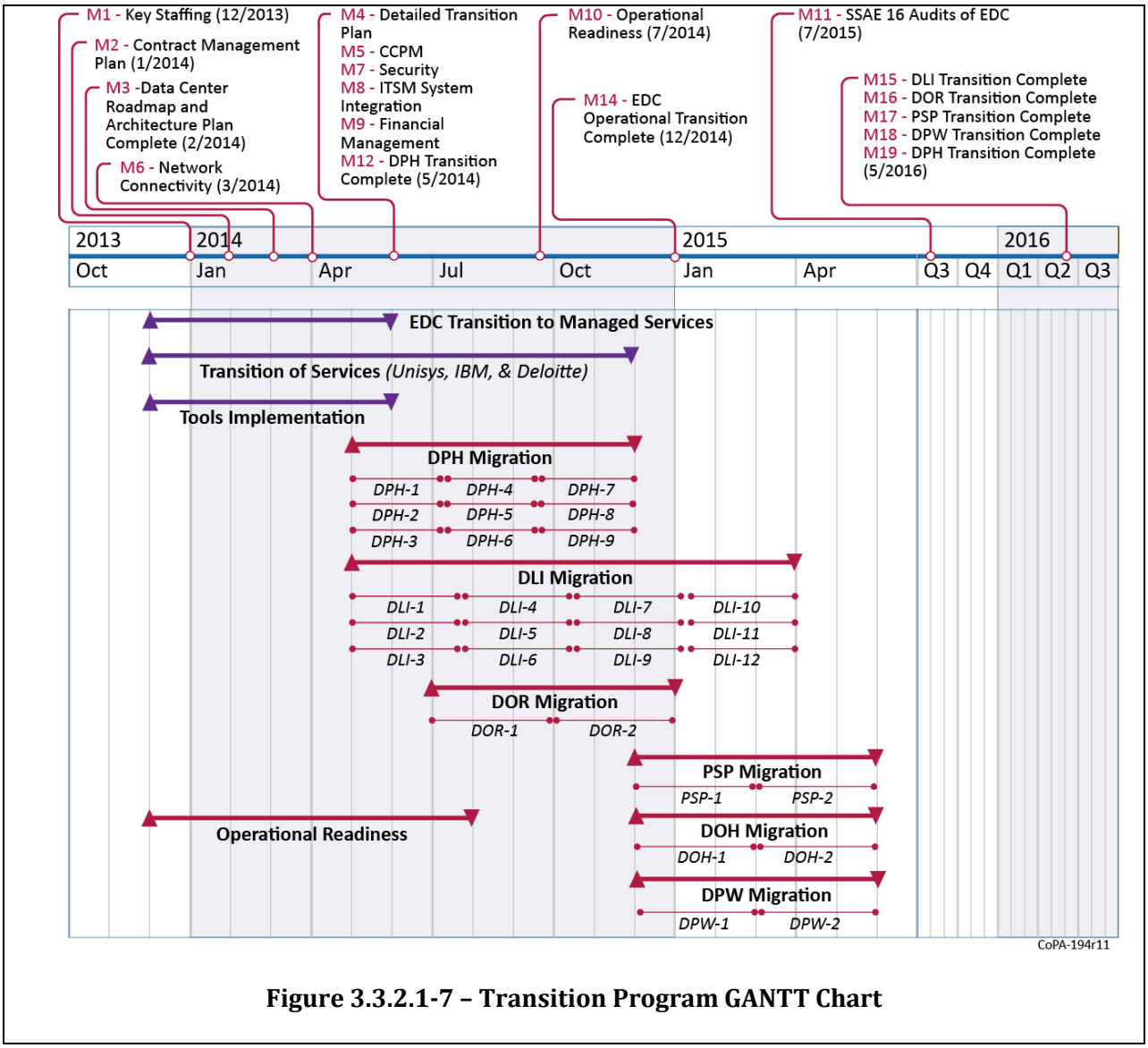


Figure 3.3.2.1-7 – Transition Program GANTT Chart

This page intentionally left blank.

Request for Proposal

RFP # 6100022698

Commonwealth of Pennsylvania

Office of Administration

Office for Information Technology

Data Center Computing Services

SCHEDULE M

DETAILED TRANSITION PLAN

(Offeror to provide Offeror's Detailed Transition Plan within the Schedule)

UNISYS RESPONSE: Transition Plan

Transition Schedule

Data center transition is not a destination; it is a journey that requires thoughtful planning. Unisys views transition as the process through which the Commonwealth Data Centers are prepared for the next generation. The transition does not happen overnight. However, Unisys experience with data center transformation enables us to use best practices and proven tools that accelerate the process and convert time to value. Our Transition Schedule is displayed in **Figure M-9.**

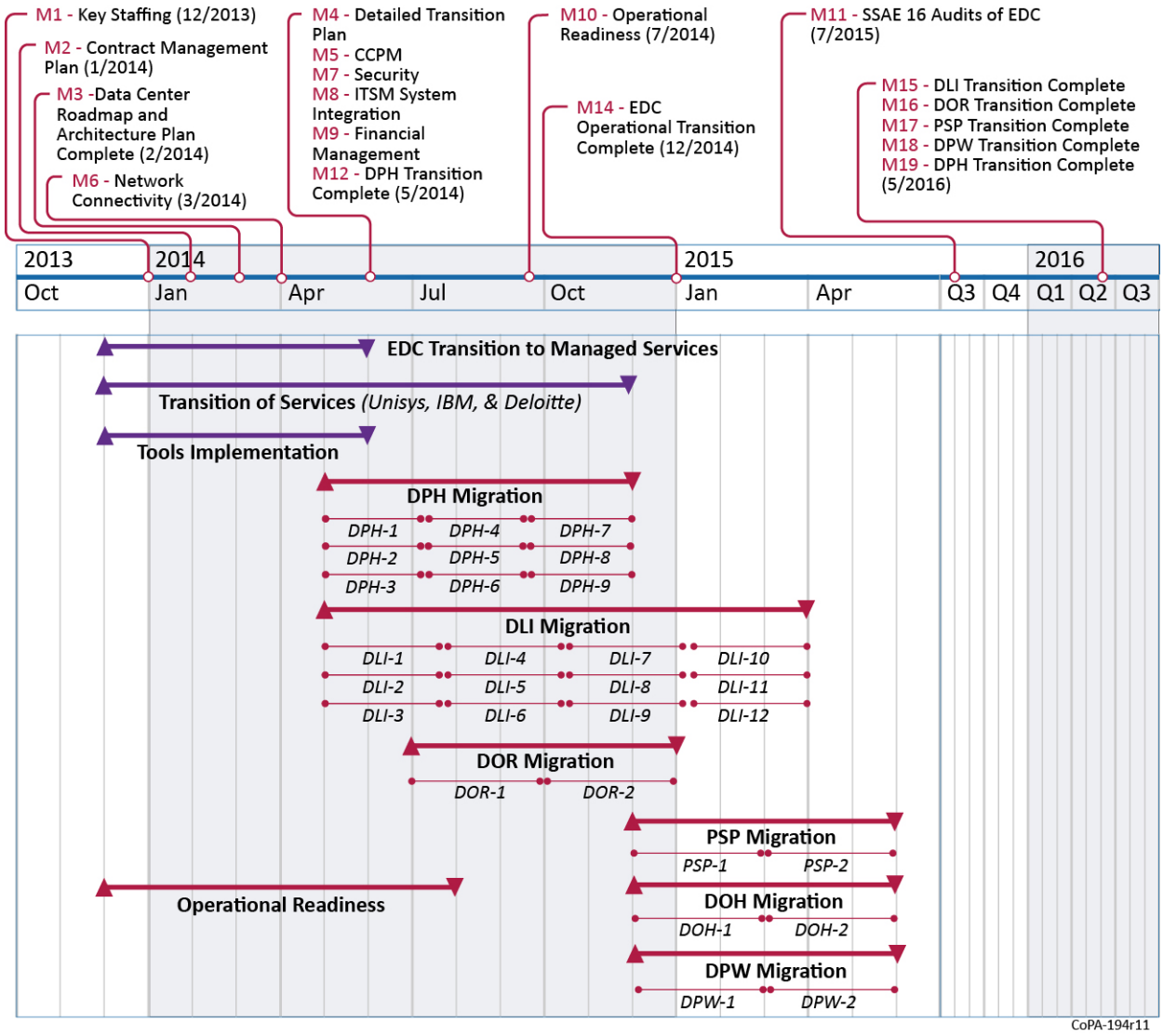


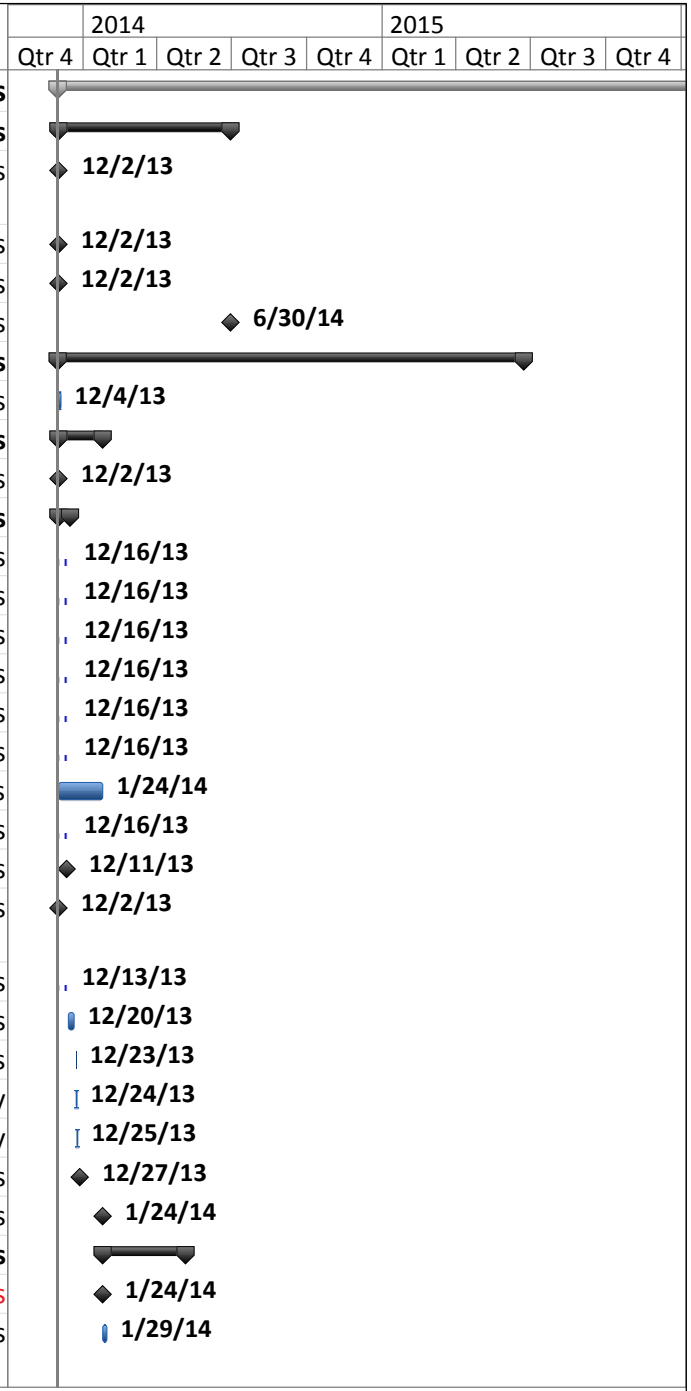
Figure M-9. Transition Schedule

Detailed Transition Plan

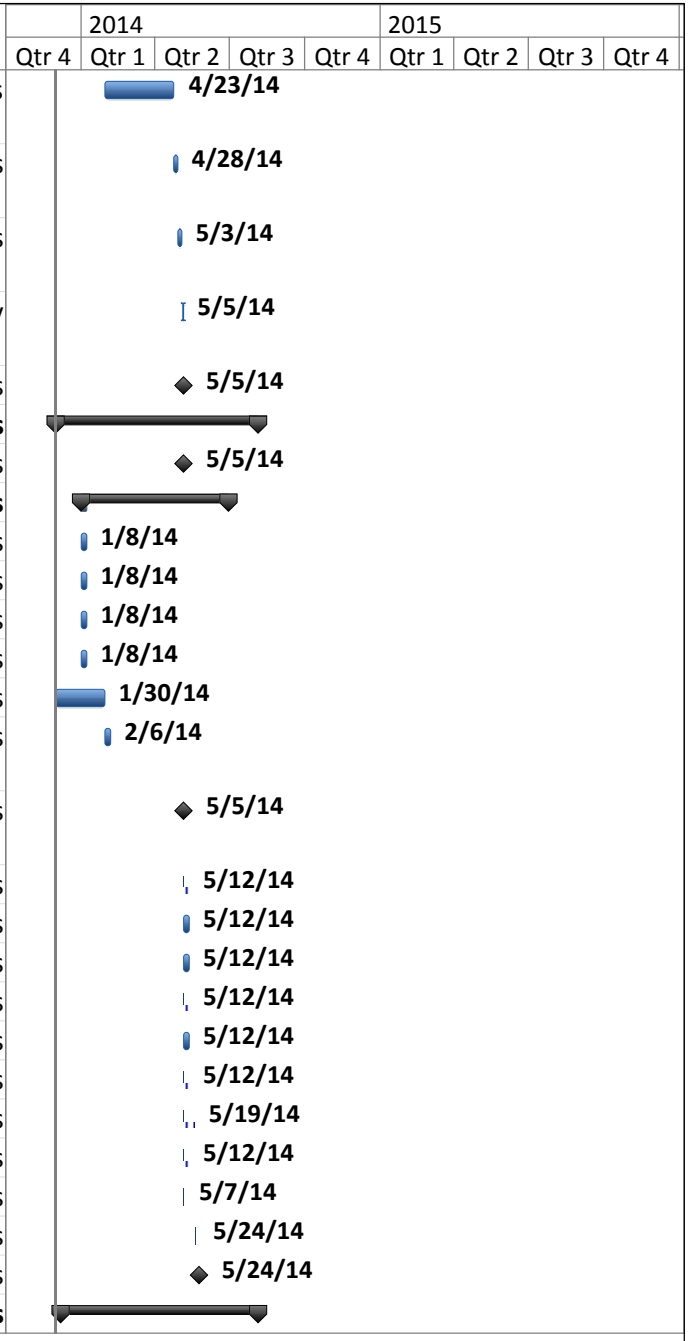
On the following pages, Unisys includes our Detailed Transition Plan for Commonwealth review.

This page intentionally left blank.

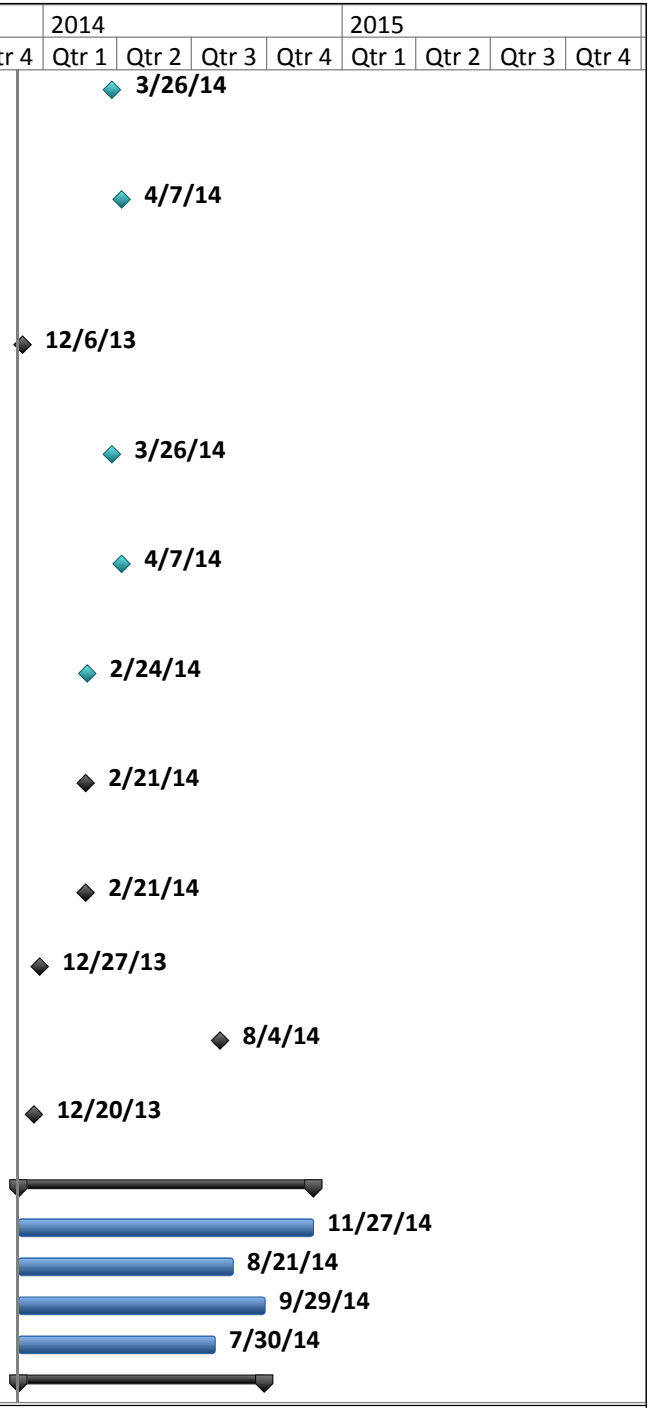
ID	Task Name	Start	Finish	Duration
0	**CoPA Transition Program**	**12/1/13**	**12/31/24**	**2892 days**
1	**1 Key Program Start Dates**	**12/2/13**	**6/30/14**	**150 days**
2	1.1 MS - Unisys Sign DC Contract with New Datacenters as required	12/2/13	12/2/13	0 days
3	1.2 MS - Unisys Approval to begin	12/2/13	12/2/13	0 days
4	1.3 MS - Contract Effective Date	12/2/13	12/2/13	0 days
5	1.4 MS - [redacted] Ready to Power-up	6/30/14	6/30/14	0 days
6	**2 Program Management Tasks**	**12/1/13**	**6/22/15**	**406 days**
7	2.1 MS - Unisys Team Program Kickoff Meeting	12/2/13	12/4/13	3 days
8	**2.2 Plan Progam**	**12/2/13**	**1/24/14**	**40 days**
9	2.2.1 Plan Tasks Started	12/2/13	12/2/13	0 days
10	**2.2.2 Update Project Plans**	**12/2/13**	**12/16/13**	**10 days**
11	2.2.2.1 Update Transition Governance Plan	12/2/13	12/16/13	14 edays
12	2.2.2.2 Update the Initial Transition MPP	12/2/13	12/16/13	14 edays
13	2.2.2.3 Update the Transition Communications Plan	12/2/13	12/16/13	14 edays
14	2.2.2.4 Develop Project Logs (RAID)	12/2/13	12/16/13	14 edays
15	2.2.2.5 Plan Change and Quality Management	12/2/13	12/16/13	14 edays
16	2.2.2.6 Plan Acceptance Criteria	12/2/13	12/16/13	14 edays
17	2.2.3 Setup Transition QA Program	12/2/13	1/24/14	2 mons
18	2.2.4 Obtain the Transition Logistics	12/2/13	12/16/13	14 edays
19	2.2.5 Conduct Internal Transition Kickoff Meetings	12/11/13	12/11/13	0 days
20	2.2.6 Complete Pursuit to Transition Handover and Knowledge Transfer	12/2/13	12/2/13	0 days
21	2.2.7 Schedule and Hold CoPA Kickoff Sessions	12/2/13	12/13/13	10 days
22	2.2.8 Baseline the Transition MPP	12/13/13	12/20/13	7 edays
23	2.2.9 Conduct Checkpoint Quality Review	12/23/13	12/23/13	4 hrs
24	2.2.10 Update Project Logs (RAID)	12/23/13	12/24/13	1 day
25	2.2.11 Perform Internal Status Requirements	12/24/13	12/25/13	1 day
26	2.2.12 PMS-5 - Detailed Transition Plan Completed	12/27/13	12/27/13	0 days
27	2.2.13 MS - Plan Tasks Completed	1/24/14	1/24/14	0 days
28	**2.3 Assess Program**	**1/24/14**	**5/5/14**	**71 days**
29	2.3.1 MS - Start Assess Tasks	1/24/14	1/24/14	0 days
30	2.3.2 Coordinate Assessment Process Review Meeting with Client	1/24/14	1/29/14	5 edays



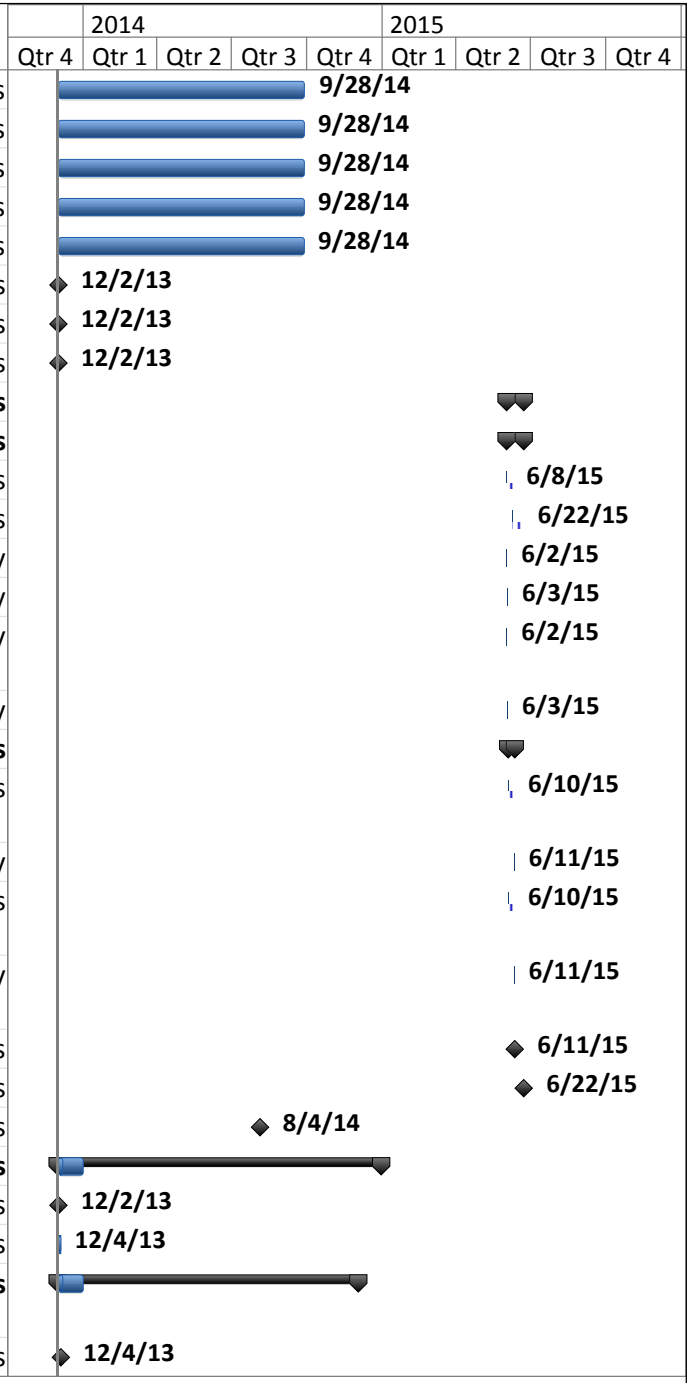
ID	Task Name	Start	Finish	Duration
31	2.3.3 Conduct Customer Assessment Meeting and Data Gathering	1/30/14	4/23/14	3 mons
32	2.3.4 Conduct Internal Review of Workstream Assessment Package	4/23/14	4/28/14	5 edays
33	2.3.5 Gain Client Agreement on Mitigation Plan for Assessment Gaps	4/28/14	5/3/14	5 edays
34	2.3.6 Obtain Workstream Assessment Package Sign Off from Client	5/5/14	5/5/14	1 day
35	2.3.7 Assess Tasks Completed	5/5/14	5/5/14	0 days
36	**2.4 Design Program**	**12/1/13**	**8/4/14**	**176 days**
37	2.4.1 MS - Start Design Tasks	5/5/14	5/5/14	0 days
38	**2.4.2 Develop Program Master Plan**	**1/1/14**	**6/30/14**	**180 edays**
39	2.4.2.1 Goverance Plan	1/1/14	1/8/14	7 edays
40	2.4.2.2 Risk Plan	1/1/14	1/8/14	7 edays
41	2.4.2.3 Data Gathering	1/1/14	1/8/14	7 edays
42	2.4.2.4 Operational Readiness Plan	1/1/14	1/8/14	7 edays
43	2.4.3 Complete Transition Program Schedule	12/1/13	1/30/14	60 edays
44	2.4.4 Review and Gain Approval of Program Schedule from Commonwealth	1/30/14	2/6/14	7 edays
45	2.4.5 Complete Solution Design Documents (SDD) for Each Workstream	5/5/14	5/5/14	0 days
46	2.4.6 Refine the Customer Communication Plan	5/5/14	5/12/14	7 edays
47	2.4.7 Gain Client Agreement on Design Gap Mitigation	5/5/14	5/12/14	7 edays
48	2.4.8 Conduct Internal Program Plan Review	5/5/14	5/12/14	7 edays
49	2.4.9 Review Transition Status Report Templates with Client	5/5/14	5/12/14	7 edays
50	2.4.10 Finalize ITSM Operating Processes and Procedures	5/5/14	5/12/14	7 edays
51	2.4.11 Address Procurement	5/5/14	5/12/14	7 edays
52	2.4.12 Develop Procedures For Each Workstream	5/5/14	5/19/14	14 edays
53	2.4.13 Develop the Program Performance Reporting Plan	5/5/14	5/12/14	7 edays
54	2.4.14 Perform Internal Design Review	5/5/14	5/7/14	2 edays
55	2.4.15 Complete the Customer Design Review	5/19/14	5/24/14	5 edays
56	2.4.16 Complete Design Tasks	5/24/14	5/24/14	0 days
57	**2.4.17 D-05 - Transition Management Plan**	**12/6/13**	**8/4/14**	**171 days**



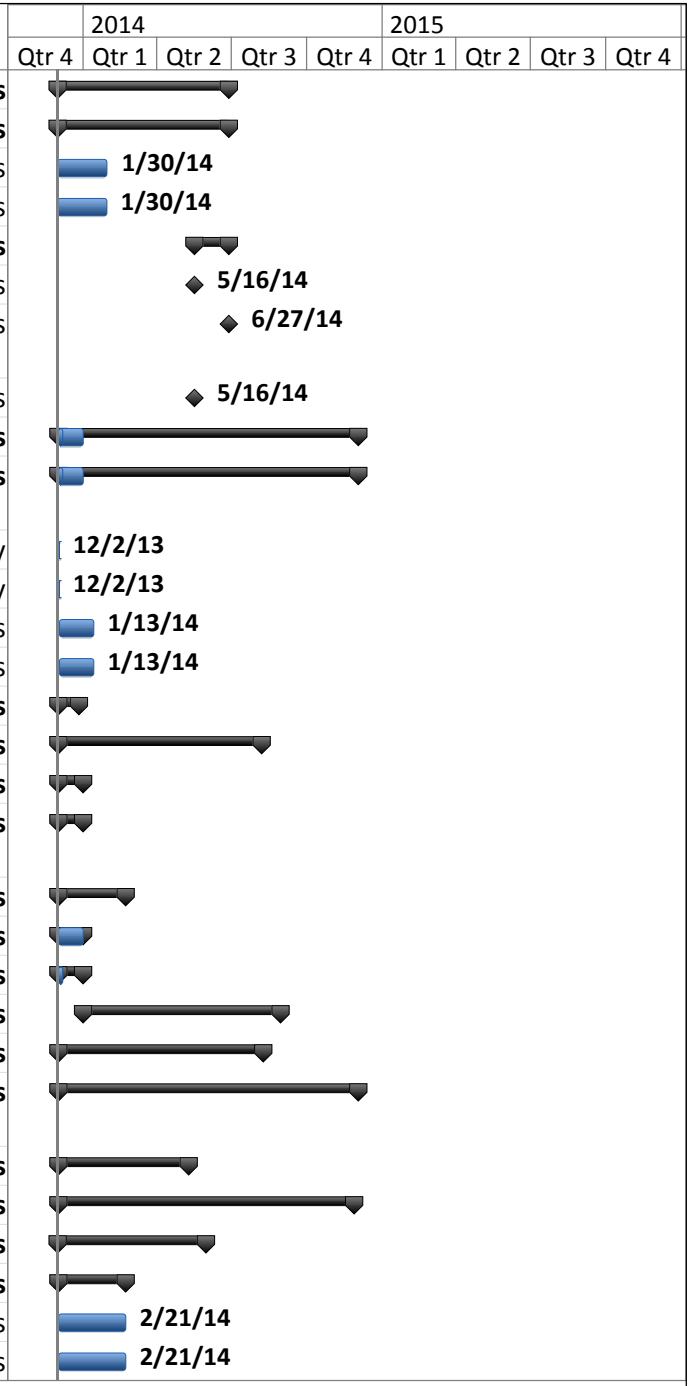
ID	Task Name	Start	Finish	Duration
58	2.4.17.1 D-05.01 - Transition Management Plan - New Customer/Service - Create Transition Roadmap with major milestones and present to the Commonwealth	3/26/14	3/26/14	0 days
59	2.4.17.2 D-05.02 - Transtion Managemetn Plan - New Customer/Service - Create a Detailed Transition Project Plan with major milestones and persent it to the Commonwealth	4/7/14	4/7/14	0 days
60	2.4.17.3 D-05.03 - Transition Management Plan - New Customer/Service First of weekly Transition Status Report	12/6/13	12/6/13	0 days
61	2.4.17.4 D-05.04 - Transition Management Plan - Present approach to transition Commonwealth computing assets. Includes Roadmap and project plans	3/26/14	3/26/14	0 days
62	2.4.17.5 D-05.05 - Transtion Managemetn Plan - Present transition roadmap and plan to Commonwealth stakeholders	4/7/14	4/7/14	0 days
63	2.4.17.6 D-05.06 - Transition Management Plan - Establish Intermim Contract Management Procedures during the transition of datacenter services	2/24/14	2/24/14	0 days
64	2.4.17.7 D-05.07 - Transition Management Plan - Document EDC/Legacy Datacenter Infrastructure Maintenance Strategy	2/21/14	2/21/14	0 days
65	2.4.17.8 D-05.08 - Transition Management Plan - Document prodecure to standup the Transion	2/21/14	2/21/14	0 days
66	2.4.17.9 D-05.09 - Transition Management Plan - Provide the first of the weekly Transition Status Reports	12/27/13	12/27/13	0 days
67	2.4.17.10 D-05.10 - Security Transition Activities - Provide Security Transition Plan	8/4/14	8/4/14	0 days
68	2.4.17.11 D-05.11 - Transition Management Plan - Provide the first of the weekly Security Transition Status Reports	12/20/13	12/20/13	0 days
69	**2.5 Deploy Program**	**12/2/13**	**11/27/14**	**258 days**
70	2.5.1 Start Deploy Tasks	12/2/13	11/27/14	12 emons
71	2.5.2 Manage Transition of Services	12/2/13	8/21/14	262 edays
72	2.5.3 Manage Tools Implementation Project	12/2/13	9/29/14	301 edays
73	2.5.4 Manage Operational Readiness Project	12/2/13	7/30/14	240 edays
74	**2.5.5 Manage DPH Migration**	**12/2/13**	**9/28/14**	**215 days**



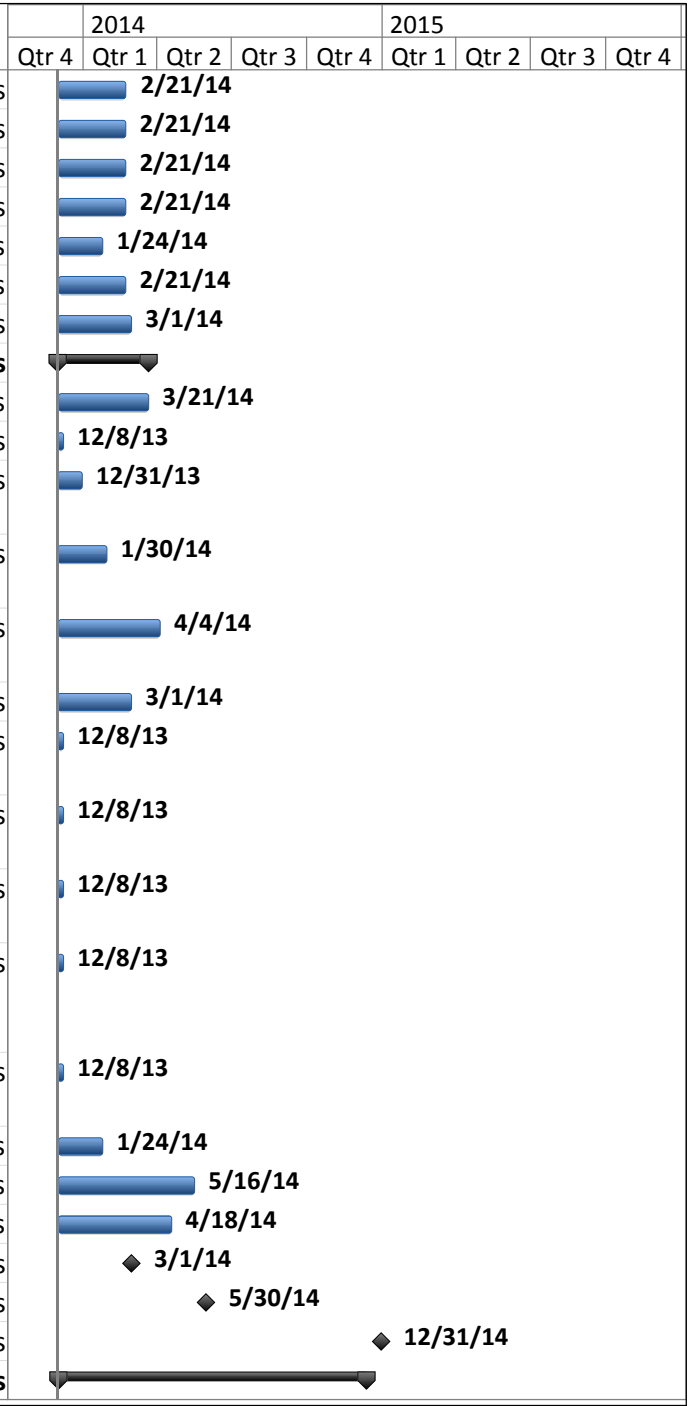
ID	Task Name	Start	Finish	Duration
75	2.5.5.1 Manage DPH Move Group 1	12/2/13	9/28/14	10 emons
76	2.5.5.2 Manage DPH Move Group 2	12/2/13	9/28/14	10 emons
77	2.5.5.3 Manage DPH Move Group 3	12/2/13	9/28/14	10 emons
78	2.5.5.4 Manage DPH Move Group 4	12/2/13	9/28/14	10 emons
79	2.5.5.5 Manage DPH Move Group 5	12/2/13	9/28/14	10 emons
80	2.5.6 Conduct Deployment Checkpoint Review	12/2/13	12/2/13	0 days
81	2.5.7 Hold the Services Operational Readiness Review (ORR)	12/2/13	12/2/13	0 days
82	2.5.8 Final Go-Live (Cutover)	12/2/13	12/2/13	0 days
83	**2.6 Handover and Close to Steady State**	**6/1/15**	**6/22/15**	**15 days**
84	**2.6.1 Transition Feedback**	**6/1/15**	**6/22/15**	**15 days**
85	2.6.1.1 Prepare to Seek Transition Feedback	6/1/15	6/8/15	7 edays
86	2.6.1.2 Gather and Submit Transition Feedback	6/8/15	6/22/15	14 edays
87	2.6.2 Review Initial Operational Reports with Client	6/1/15	6/2/15	1 eday
88	2.6.3 Customer Close-Out Transition	6/2/15	6/3/15	1 eday
89	2.6.4 Hand Off Out of Scope Opportunities to Account Project Office	6/1/15	6/2/15	1 eday
90	2.6.5 Handover to Service Delivery	6/2/15	6/3/15	1 eday
91	**2.6.6 Finalize and Manage Lessons Learned**	**6/3/15**	**6/11/15**	**6 days**
92	2.6.6.1 Finalize and Submit Transition Management Phase Lessons Learned	6/3/15	6/10/15	7 edays
93	2.6.6.2 Identify Vital Few Deals and Communicate Accordin	6/10/15	6/11/15	1 eday
94	2.6.6.3 Prepare for Lessons Learned Review for Transition Management Phase	6/3/15	6/10/15	7 edays
95	2.6.6.4 Schedule and Conduct Lessons Learned Review Transition Management Phase	6/10/15	6/11/15	1 eday
96	2.6.6.5 Drive Lessons Learned Action Items	6/11/15	6/11/15	0 hrs
97	2.7 MS - Program Management Tasks Complete	6/22/15	6/22/15	0 days
98	2.8 PMS-6 - Detailed Transition Plan Complete	8/4/14	8/4/14	0 days
99	**3 CoPA Transition**	**12/1/13**	**12/31/14**	**282 days**
100	3.1 MS - Transition Start	12/2/13	12/2/13	0 days
101	3.2 Conduct Transition of Services Project Kickoff Meeting	12/2/13	12/4/13	3 days
102	**3.3 Transition of Services Project (Enable Common Service Portfolio)**	**12/1/13**	**12/3/14**	**262 days**
103	3.3.1 MS - TOS Start	12/4/13	12/4/13	0 days



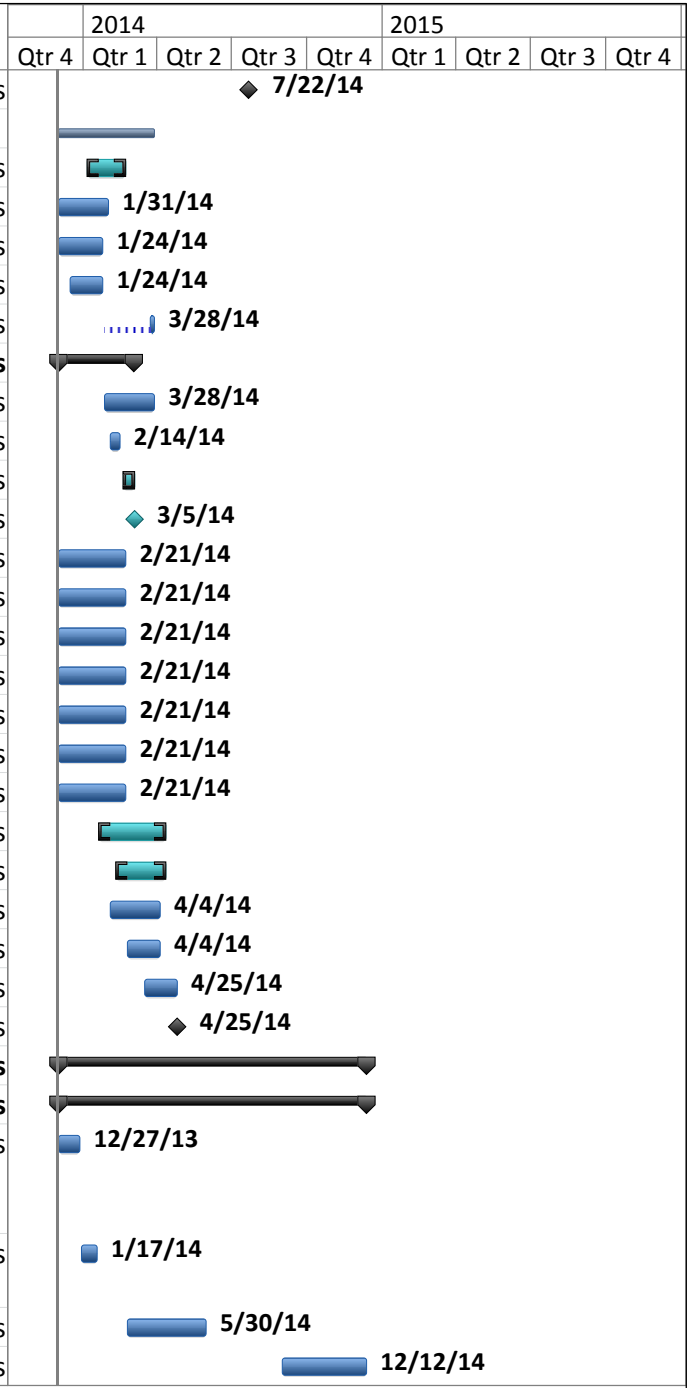
ID	Task Name	Start	Finish	Duration
104	**3.3.2 Assess CoPA Current Environments**	**12/1/13**	**6/27/14**	**150 days**
105	**3.3.2.1 Knowledge Transfer activities**	**12/1/13**	**6/27/14**	**150 days**
106	3.3.2.1.1 Review ADDM Results EDC and DPH	12/1/13	1/30/14	60 edays
107	3.3.2.1.2 Review ADDM results DOR, DLI, DPW, DOH, PSI	12/1/13	1/30/14	60 edays
108	**3.3.2.1.3 D-10 - Gap Analysis Report**	**5/16/14**	**6/27/14**	**30 days**
109	3.3.2.1.3.1 D-10.01 - Gap Analysis Report	5/16/14	5/16/14	0 days
110	3.3.2.1.3.2 D-10.02 - Gap Analysis Report - Present results and roadmap	6/27/14	6/27/14	0 days
111	3.3.2.2 PMS-5 - Data Gathering	5/16/14	5/16/14	0 days
112	**3.3.3 Setup the Account Team**	**12/2/13**	**12/3/14**	**262 days**
113	**3.3.3.1 Organizational Change Control Components - Program and Services Management**	**12/2/13**	**12/3/14**	**262 days**
114	3.3.3.1.1 Townhall to announce Agreement	12/2/13	12/2/13	1 day
115	3.3.3.1.2 Team Meetings to discuss what this "means to	12/2/13	12/2/13	1 day
116	3.3.3.1.3 Re-Organize Account Staff to new model	12/3/13	1/13/14	30 days
117	3.3.3.1.4 Establish PMO Guidelines and Processes	12/3/13	1/13/14	30 days
118	**3.3.3.1.5 Establish Vendor and Subcontractor Manager**	**12/2/13**	**12/27/13**	**19 days**
122	**3.3.3.1.6 Staff Account**	**12/2/13**	**8/6/14**	**178 days**
144	**3.3.3.1.7 Establish PMO Leadership Team**	**12/2/13**	**1/1/14**	**22 days**
147	**3.3.3.1.8 Establish Project Management Team - TPMO and Steady State**	**12/2/13**	**1/1/14**	**22 days**
149	**3.3.3.1.9 Establish Contract Management Team**	**12/2/13**	**2/21/14**	**60 days**
158	**3.3.3.1.10 Establish Agency Account Management Tean**	**12/2/13**	**1/1/14**	**22 days**
161	**3.3.3.1.11 Establish Enterprise Architecture Team**	**12/2/13**	**1/1/14**	**22 days**
164	**3.3.3.1.12 Establish Service Excellance Office (SEO)**	**1/1/14**	**8/29/14**	**173 days**
265	**3.3.3.1.13 Establish Financial Management Team Proce**	**12/2/13**	**8/8/14**	**180 days**
273	**3.3.3.1.14 Establish Service Delivery Teams - Processes and Procedures**	**12/2/13**	**12/3/14**	**262 days**
382	**3.3.3.1.15 Training**	**12/2/13**	**5/9/14**	**115 days**
399	**3.3.3.1.16 Relocate Account Team**	**12/2/13**	**11/28/14**	**259 days**
406	**3.4 Enterprise Data Center to Managed Services Model**	**12/1/13**	**5/30/14**	**130 days**
407	**3.4.1 Perform EDC Assessment**	**12/2/13**	**2/21/14**	**60 days**
408	3.4.1.1 Identify Required Security Updates/Upgrades	12/2/13	2/21/14	60 days
409	3.4.1.2 Identify HVAC and power upgrades	12/2/13	2/21/14	60 days



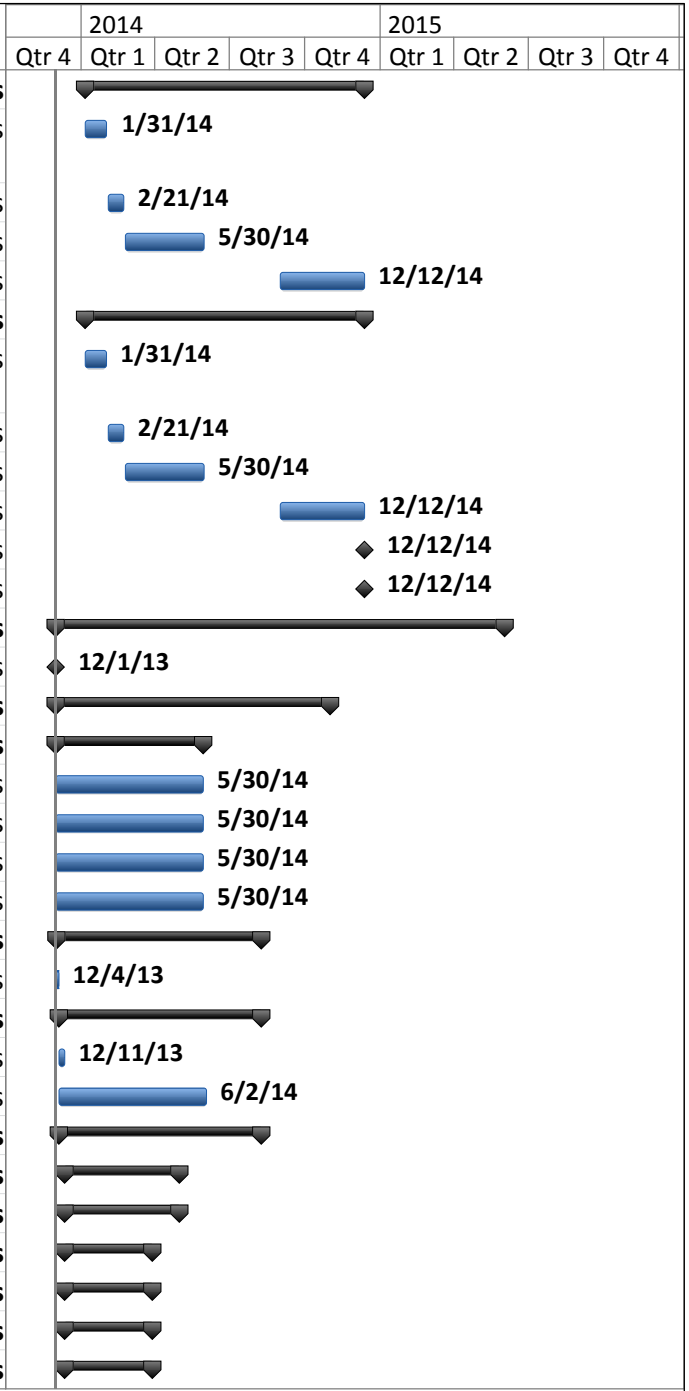
ID	Task Name	Start	Finish	Duration
410	3.4.1.3 Identify physical access required for facility	12/2/13	2/21/14	60 days
411	3.4.1.4 Review BMS System quality and information	12/2/13	2/21/14	60 days
412	3.4.2 Integrate Building Management System to BMC BEM	12/2/13	2/21/14	60 days
413	3.4.3 Integrate DCIMI to BMC BEM	12/2/13	2/21/14	60 days
414	3.4.4 Implement Rackwise	12/2/13	1/24/14	2 mons
415	3.4.5 Install Electrical SubMetering	12/2/13	2/21/14	3 mons
416	3.4.6 SSAE 16 Audit of EDC	12/1/13	3/1/14	90 edays
417	**3.4.7 Knowledge Transfer activities**	**12/1/13**	**3/21/14**	**80 days**
418	3.4.7.1 Create/update Runbooks	12/2/13	3/21/14	4 mons
419	3.4.7.2 Verify CMDB contains EDC assets and Cis	12/1/13	12/8/13	7 edays
420	3.4.7.3 Document current Service Catalogs, processes and procedures are transitioned	12/1/13	12/31/13	30 edays
421	3.4.8 Multi-environments/instances are available for identified systems	12/1/13	1/30/14	60 edays
422	3.4.9 Verify High Availability, backup and DR are operational for identified systems	12/2/13	4/4/14	90 days
423	3.4.10 Verify specific details for CCPM are in KMP	12/1/13	3/1/14	90 edays
424	3.4.11 Verify Operational dashboards are in place to report on status and alerts	12/1/13	12/8/13	7 edays
425	3.4.12 Verify Service Level agreements have been identified and supporting metrics are in place	12/1/13	12/8/13	7 edays
426	3.4.13 Verify system is Operational for scheduling and tracking of ticket-based tasks and incidents (ITSM/Remedy)	12/1/13	12/8/13	7 edays
427	3.4.14 Verify system is is operational to begin data collection in order to produce Configuration, monitoring and management status reports	12/1/13	12/8/13	7 edays
428	3.4.15 Verify all Transition Orders are completed and accepted by the Commonwealth	12/1/13	12/8/13	7 edays
429	3.4.16 Implement ITIL Processes	12/2/13	1/24/14	2 mons
430	3.4.17 Complete Staffing	12/2/13	5/16/14	6 mons
431	3.4.18 Implement Tools	12/2/13	4/18/14	5 mons
432	3.4.19 PMS-13 - SSAE 16 Audit of EDC Completed	3/1/14	3/1/14	0 days
433	3.4.20 PMS-15 - EDC Transition Completed	5/30/14	5/30/14	0 days
434	3.5 MS-ToS Complete	12/31/14	12/31/14	0 days
435	**3.6 Tools Implimentation Project**	**12/2/13**	**12/12/14**	**270 days**



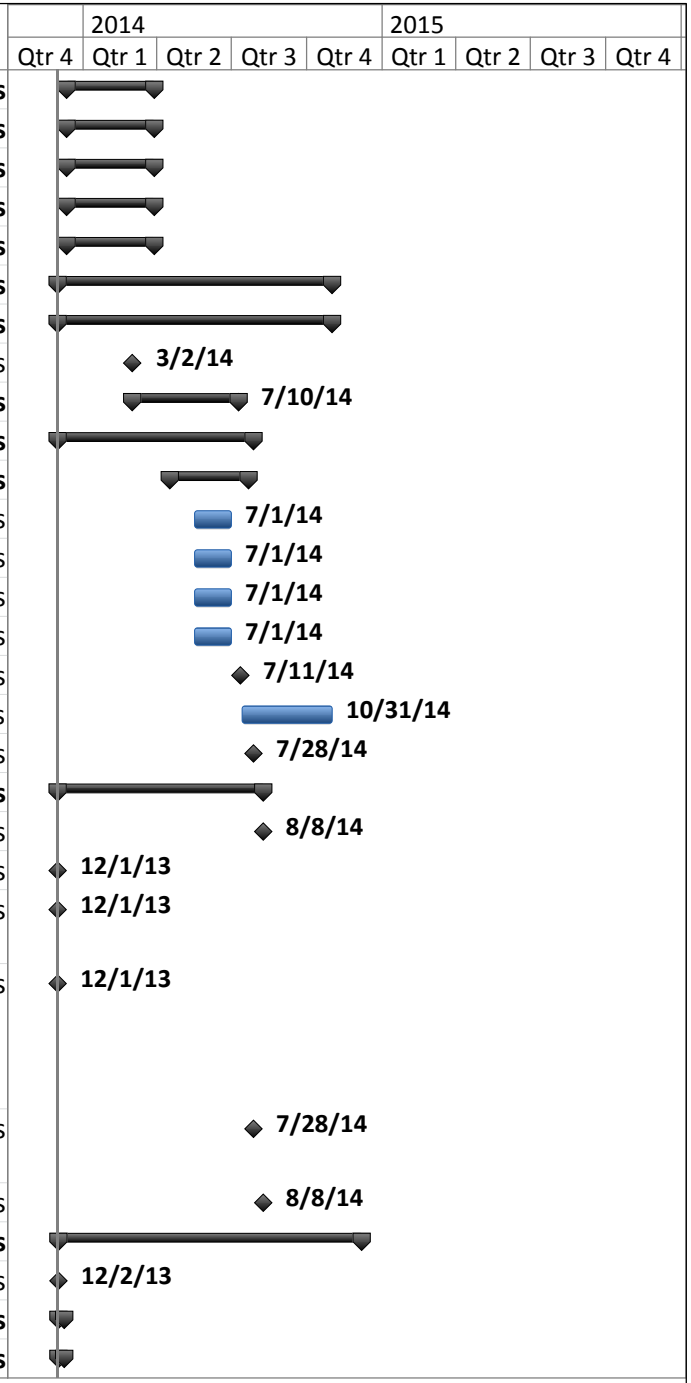
ID	Task Name	Start	Finish	Duration
436	3.6.1 MS - Tools Implementation Project Start	7/22/14	7/22/14	0 days
437	**3.6.2 Install BMC ITSM**			
438	3.6.2.1 Prep Foundation Data	1/6/14	2/21/14	35 days
439	3.6.2.2 Configure CFG Mgt	12/2/13	1/31/14	45 days
440	3.6.2.3 Configure Release Mgt	12/2/13	1/24/14	40 days
441	3.6.2.4 Configure Service Level Mgt	12/16/13	1/24/14	30 days
442	3.6.2.5 ITSM Configured & Tested	1/27/14	3/28/14	5 days
443	**3.6.2.6 CCPM Approach & Reviews with COPA**	**12/2/13**	**3/3/14**	**66 days**
447	3.6.3 Configure DSO - Remedy Synch	1/27/14	3/28/14	45 days
448	3.6.4 Install & Configure KM	2/3/14	2/14/14	10 days
449	3.6.5 Load KM ITSM Procedures, SC, Contract Pricing	2/19/14	3/4/14	10 days
450	3.6.6 KM Loaded	3/5/14	3/5/14	0 days
451	3.6.7 Install & Configure EDC & DPH ADDM Discovery	12/2/13	2/21/14	60 days
452	3.6.8 Install & Configure DOR ADDM Discovery	12/2/13	2/21/14	60 days
453	3.6.9 Install&Configure DLI ADDM Discovery	12/2/13	2/21/14	60 days
454	3.6.10 Install & Configure DOH ADDM Discovery	12/2/13	2/21/14	60 days
455	3.6.11 Install & Configure PSP ADDM Discovery	12/2/13	2/21/14	60 days
456	3.6.12 Install & Configure DPW Discovery	12/2/13	2/21/14	60 days
457	3.6.13 Install BPPM/BEM/SIM Monitoring & Integration	12/2/13	2/21/14	60 days
458	3.6.14 Configure Availability Management	1/20/14	4/11/14	60 days
459	3.6.15 Configure Capacity Management	2/10/14	4/11/14	45 days
460	3.6.16 Install & Configure Bladelogic for Servers (EDC	2/3/14	4/4/14	45 days
461	3.6.17 Configure Standard Reporting BMC	2/24/14	4/4/14	30 days
462	3.6.18 Configure Pureshare Dashboards	3/17/14	4/25/14	30 days
463	3.6.19 ITSM Configured for Operations	4/25/14	4/25/14	0 days
464	**3.6.20 Security Tools**	**12/2/13**	**12/12/14**	**270 days**
465	**3.6.20.1 Data Loss Prevention**	**12/2/13**	**12/12/14**	**270 days**
466	3.6.20.1.1 Perform requirements gathering and design the data center DLP solution to monitor the datacenter egress points	12/2/13	12/27/13	20 days
467	3.6.20.1.2 Implement pilot solution and configure DLP policy on one egress point	12/30/13	1/17/14	15 days
468	3.6.20.1.3 Implement DLP solution for DCM Phase 1	2/24/14	5/30/14	70 days
469	3.6.20.1.4 Implement DLP solution for DCM Phase 2	9/1/14	12/12/14	75 days



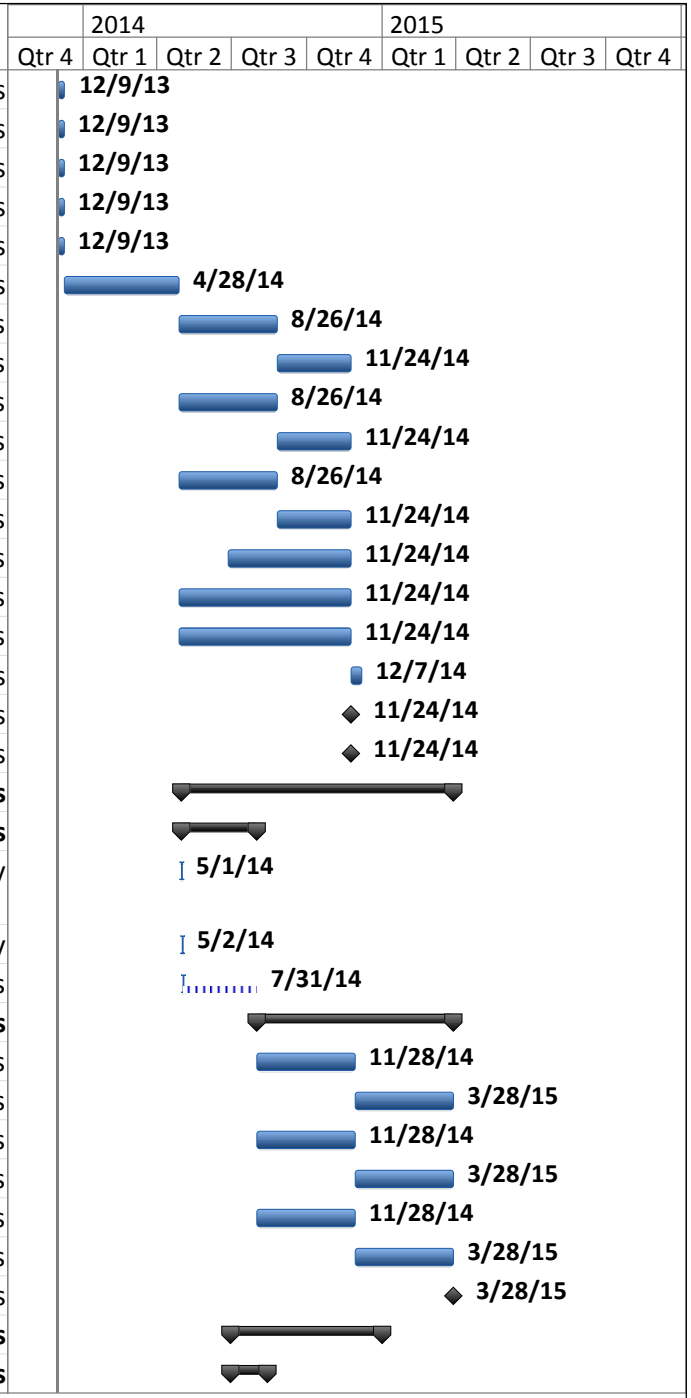
ID	Task Name	Start	Finish	Duration
470	**3.6.20.2 Database Firewall (DBFW)**	**1/6/14**	**12/12/14**	**245 days**
471	3.6.20.2.1 Perform requirements gathering and design the data center DBFW	1/6/14	1/31/14	20 days
472	3.6.20.2.2 Implement pilot solution and configure DBFW	2/3/14	2/21/14	15 days
473	3.6.20.2.3 Implement DBFW solution for DCM Phase 1	2/24/14	5/30/14	70 days
474	3.6.20.2.4 Implement DBFW solution for DCM Phase 2	9/1/14	12/12/14	75 days
475	**3.6.20.3 Web Application Firewall (WAF)**	**1/6/14**	**12/12/14**	**245 days**
476	3.6.20.3.1 Perform requirements gathering and design the data center WAF	1/6/14	1/31/14	20 days
477	3.6.20.3.2 Implement pilot solution and configure WAF	2/3/14	2/21/14	15 days
478	3.6.20.3.3 Implement DBFW solution for WAF Phase 1	2/24/14	5/30/14	70 days
479	3.6.20.3.4 Implement DBFW solution for WAF Phase 2	9/1/14	12/12/14	75 days
480	3.6.21 MS - Tools Implimentation Project Complete	12/12/14	12/12/14	0 days
481	3.6.22 MS - CoPA Transition of Services Complete	12/12/14	12/12/14	0 days
482	**4 CoPA Application Workload Migration**	**12/1/13**	**6/1/15**	**391 days**
483	4.1 MS - CoPA Application Migration Start	12/1/13	12/1/13	0 days
484	**4.2 Infrastrucuture Readiness Project**	**12/1/13**	**10/31/14**	**240 days**
485	**4.2.1 Project Management Tasks**	**12/1/13**	**5/30/14**	**129 days**
486	4.2.1.1 Refine Goverance Plan	12/1/13	5/30/14	180 edays
487	4.2.1.2 Develop and maintain Risk Plan (RAID)	12/1/13	5/30/14	180 edays
488	4.2.1.3 Validate Data Gathering Timeline	12/1/13	5/30/14	180 edays
489	4.2.1.4 Develop Configuration/Test Plan	12/1/13	5/30/14	180 edays
490	**4.2.2 Data CenterArchitecture Design and Planning Tasks**	**12/2/13**	**8/8/14**	**180 days**
491	4.2.2.1 Data Center Planning Kickoff Meeting	12/2/13	12/4/13	3 days
492	**4.2.2.2 Refine Data Center Plan**	**12/4/13**	**8/8/14**	**177 days**
493	4.2.2.2.1 Finalize DC Seed and Critical Gear plan	12/5/13	12/11/13	5 days
494	4.2.2.2.2 Develop Operational Readiness Plan	12/4/13	6/2/14	180 edays
495	**4.2.2.2.3 Create Architecture Diagrams**	**12/4/13**	**8/8/14**	**177 days**
539	**4.2.2.3 Order Long Lead/Seed Items**	**12/11/13**	**4/30/14**	**100 days**
540	**4.2.2.3.1 WAN**	**12/11/13**	**4/30/14**	**100 days**
546	**4.2.2.3.2 LAN**	**12/11/13**	**3/28/14**	**77 days**
551	**4.2.2.3.3 x86 Seed**	**12/11/13**	**3/28/14**	**77 days**
556	**4.2.2.3.4 x86 ITSM Environment**	**12/11/13**	**3/28/14**	**77 days**
561	**4.2.2.3.5 Storage Seed**	**12/11/13**	**3/28/14**	**77 days**



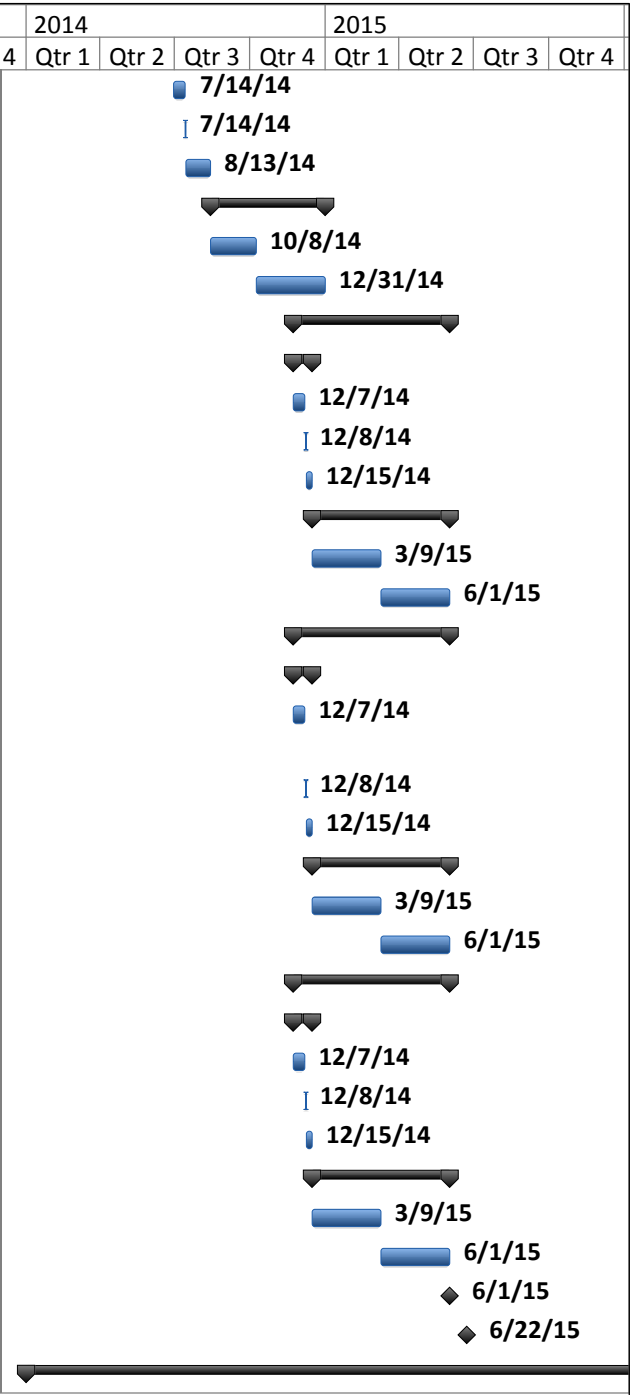
ID	Task Name	Start	Finish	Duration
566	**4.2.2.3.6 Storage ITSM**	**12/11/13**	**3/28/14**	**77 days**
571	**4.2.2.3.7 IBM MF**	**12/11/13**	**3/28/14**	**77 days**
576	**4.2.2.3.8 Unisys MF**	**12/11/13**	**3/28/14**	**77 days**
581	**4.2.2.3.9 IBM P-Series**	**12/11/13**	**3/28/14**	**77 days**
586	**4.2.2.3.10 IBM AIX**	**12/11/13**	**3/28/14**	**77 days**
591	**4.2.3 Data Center Buildout**	**12/1/13**	**10/31/14**	**240 days**
592	**4.2.3.1 DC1 - Buildout - MP0**	**12/1/13**	**10/31/14**	**240 days**
593	4.2.3.1.1 MS - Begin DC1 - Buildout	3/2/14	3/2/14	0 days
594	**4.2.3.1.2 DC1 - Network Buildout**	**3/2/14**	**7/10/14**	**93 days**
607	**4.2.3.1.3 DC1 - Storage Buildout**	**12/1/13**	**7/28/14**	**170 days**
614	**4.2.3.1.4 DC1 - x86 Buildout**	**4/17/14**	**7/22/14**	**68 days**
622	4.2.3.1.5 DC1 - Backup Buildout	5/17/14	7/1/14	45 edays
623	4.2.3.1.6 DC1 - IBM MF Buildout	5/17/14	7/1/14	45 edays
624	4.2.3.1.7 DC1 - AIX Buildout	5/17/14	7/1/14	45 edays
625	4.2.3.1.8 DC1 - Monitoring Buildout	5/17/14	7/1/14	45 edays
626	4.2.3.1.9 Initiate SSAE 16 Audit for DC1	7/11/14	7/11/14	0 days
627	4.2.3.1.10 Execute SSAE 16 Audit for DC1	7/14/14	10/31/14	4 mons
628	4.2.3.1.11 MS - DC1 - Buildout - MP0 - COMPLETED	7/28/14	7/28/14	0 days
629	**4.2.3.2 Prepare Operational Readiness Report**	**12/1/13**	**8/8/14**	**180 days**
630	4.2.3.2.1 Deliverables D-01 (01,02, 03,04,05,06,07) Com	8/8/14	8/8/14	0 days
631	4.2.3.2.2 Transition Project Office established	12/1/13	12/1/13	0 days
632	4.2.3.2.3 Transition Program Plan and architecture developed and approved	12/1/13	12/1/13	0 days
633	4.2.3.2.4 Processes and tools implemented to support the transition change control, schedule, quality, communications, risk and issues management (Project Logs established)	12/1/13	12/1/13	0 days
634	4.2.3.2.5 Datacenter environment configured, tested and accepted	7/28/14	7/28/14	0 days
635	4.2.3.3 PMS-12 - Operational Readiness	8/8/14	8/8/14	0 days
636	**4.3 DPH Data Center Migration**	**12/2/13**	**12/7/14**	**265 days**
637	4.3.1 DPH Start	12/2/13	12/2/13	0 days
638	**4.3.2 Project Management Tasks**	**12/2/13**	**12/9/13**	**5 days**
639	**4.3.2.1 Develop Agency centric plans**	**12/2/13**	**12/9/13**	**5 days**



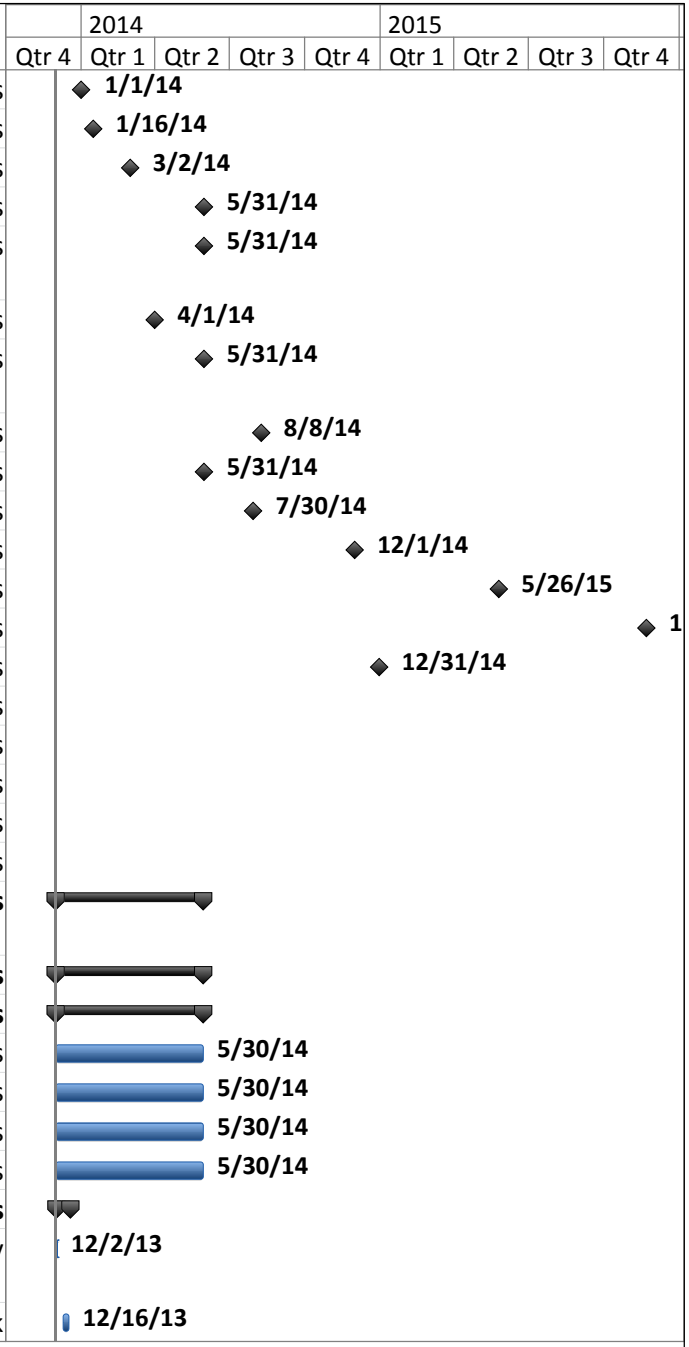
ID	Task Name	Start	Finish	Duration
640	4.3.2.1.1 Goverance Plan	12/2/13	12/9/13	7 edays
641	4.3.2.1.2 Risk Plan	12/2/13	12/9/13	7 edays
642	4.3.2.1.3 Validate Data Gathering Timeline	12/2/13	12/9/13	7 edays
643	4.3.2.1.4 Configuration/Test Plan	12/2/13	12/9/13	7 edays
644	4.3.2.1.5 Operational Readiness Plan	12/2/13	12/9/13	7 edays
645	4.3.3 DPH Planning and Review of high level move groups	12/9/13	4/28/14	140 edays
646	4.3.4 DPH-Team 1 - Move Package #1	4/28/14	8/26/14	4 emons
647	4.3.5 DPH-Team 1 - Move Package #2	8/26/14	11/24/14	3 emons
648	4.3.6 DPH-Team 2 - Move Package #1	4/28/14	8/26/14	4 emons
649	4.3.7 DPH-Team 2 - Move Package #2	8/26/14	11/24/14	3 emons
650	4.3.8 DPH-Team 3 - Move Package #1	4/28/14	8/26/14	4 emons
651	4.3.9 DPH-Team 3 - Move Package #2	8/26/14	11/24/14	3 emons
652	4.3.10 DPH-PLCB Move Package	6/27/14	11/24/14	5 emons
653	4.3.11 DPH-IES Move Package	4/28/14	11/24/14	7 emons
654	4.3.12 DPH-DOR Move Package	4/28/14	11/24/14	7 emons
655	4.3.13 Project Closedown Tasks	11/24/14	12/7/14	13 edays
656	4.3.14 MS-DPH Applications Migrated	11/24/14	11/24/14	0 days
657	4.3.15 PMS-13 - DPH DCM Complete	11/24/14	11/24/14	0 days
658	**4.4 DLI Data Center Migration**	**5/1/14**	**3/28/15**	**237 days**
659	**4.4.1 Plan DLI Migration**	**5/1/14**	**7/31/14**	**66 days**
660	4.4.1.1 Send Application Questionairres to Application Ownwers	5/1/14	5/1/14	1 day
661	4.4.1.2 Kickoff Meeting - L&I Data Center Migration	5/2/14	5/2/14	1 day
662	4.4.1.3 Perform Detailed planning of Move Package	5/2/14	7/31/14	3 emons
663	**4.4.2 Execute DLI Moves**	**7/31/14**	**3/28/15**	**171 days**
664	4.4.2.1 DLI -1 Move Package	7/31/14	11/28/14	4 emons
665	4.4.2.2 DLI -2 Move Package	11/28/14	3/28/15	4 emons
666	4.4.2.3 DLI -4 Move Package	7/31/14	11/28/14	4 emons
667	4.4.2.4 DLI -5 Move Package	11/28/14	3/28/15	4 emons
668	4.4.2.5 DLI -7 Move Package	7/31/14	11/28/14	4 emons
669	4.4.2.6 DLI -8 Move Package	11/28/14	3/28/15	4 emons
670	4.4.2.7 MS-DLI Data Center Migration Complete	3/28/15	3/28/15	0 days
671	**4.5 DOR Data Center Migration**	**6/30/14**	**12/31/14**	**133 days**
672	**4.5.1 Plan DOR Datacenter Migration**	**6/30/14**	**8/13/14**	**33 days**



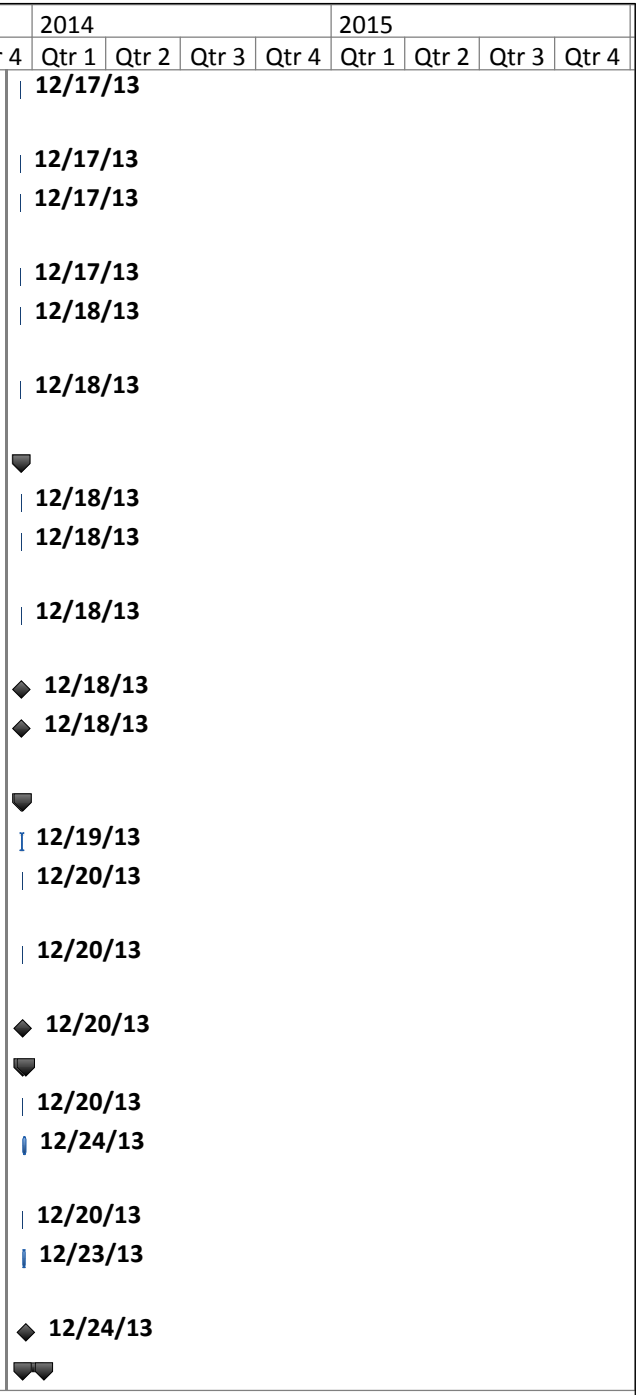
ID	Task Name	Start	Finish	Duration
673	4.5.1.1 Send Application Questionairres to Application Owr	6/30/14	7/14/14	14 edays
674	4.5.1.2 Kickoff Meeting - DOR Data Center Migration	7/14/14	7/14/14	1 day
675	4.5.1.3 Perform Detailed planning of Move Package	7/14/14	8/13/14	1 emon
676	**4.5.2 Execute DOR Moves**	**8/14/14**	**12/31/14**	**100 days**
677	4.5.2.1 Execute DOR Move Group 1	8/14/14	10/8/14	2 mons
678	4.5.2.2 Execute DOR Move Group 2	10/9/14	12/31/14	3 mons
679	**4.6 DPW Data Center Migration**	**11/23/14**	**6/1/15**	**136 days**
680	**4.6.1 Plan DPW Datacenter Migration**	**11/23/14**	**12/15/14**	**16 days**
681	4.6.1.1 Send Application Questionairres to Application Owr	11/23/14	12/7/14	14 edays
682	4.6.1.2 Kickoff Meeting - DPW Data Center Migration	12/8/14	12/8/14	1 day
683	4.6.1.3 Perform Detailed planning of Move Package	12/8/14	12/15/14	7 edays
684	**4.6.2 Execute DPW Moves**	**12/16/14**	**6/1/15**	**120 days**
685	4.6.2.1 Execute DPW Move Group 1	12/16/14	3/9/15	3 mons
686	4.6.2.2 Execute DPW Move Group 2	3/10/15	6/1/15	3 mons
687	**4.7 PSP Data Center Migration**	**11/23/14**	**6/1/15**	**136 days**
688	**4.7.1 Plan PSP Datacenter Migration**	**11/23/14**	**12/15/14**	**16 days**
689	4.7.1.1 Send Application Questionairres to Application Ownwers	11/23/14	12/7/14	14 edays
690	4.7.1.2 Kickoff Meeting - PSP Data Center Migration	12/8/14	12/8/14	1 day
691	4.7.1.3 Perform Detailed planning of Move Package	12/8/14	12/15/14	7 edays
692	**4.7.2 Execute PSP Moves**	**12/16/14**	**6/1/15**	**120 days**
693	4.7.2.1 Execute PSP Move Group 1	12/16/14	3/9/15	3 mons
694	4.7.2.2 Execute PSP Move Group 2	3/10/15	6/1/15	3 mons
695	**4.8 DOH Data Center Migration**	**11/23/14**	**6/1/15**	**136 days**
696	**4.8.1 Plan DOH Datacenter Migration**	**11/23/14**	**12/15/14**	**16 days**
697	4.8.1.1 Send Application Questionairres to Application Owr	11/23/14	12/7/14	14 edays
698	4.8.1.2 Kickoff Meeting - DOH Data Center Migration	12/8/14	12/8/14	1 day
699	4.8.1.3 Perform Detailed planning of Move Package	12/8/14	12/15/14	7 edays
700	**4.8.2 Execute DOH Moves**	**12/16/14**	**6/1/15**	**120 days**
701	4.8.2.1 Execute DOH Move Group 1	12/16/14	3/9/15	3 mons
702	4.8.2.2 Execute DOH Move Group 2	3/10/15	6/1/15	3 mons
703	4.9 MS-CoPA Application Workload Migration Completed	6/1/15	6/1/15	0 days
704	5 MS-CoPA Transition Program Complete	6/22/15	6/22/15	0 days
705	**6 Contract Milestones**	**1/1/14**	**5/31/16**	**629 days**



ID	Task Name	Start	Finish	Duration
706	6.1 CM-1 - Key Staffing Completed	1/1/14	1/1/14	0 days
707	6.2 CM-2 - Contract Management Plan	1/16/14	1/16/14	0 days
708	6.3 CM-3 - Data Center Architecture Complete	3/2/14	3/2/14	0 days
709	6.4 CM-4 - Detailed Transition Plan Completed	5/31/14	5/31/14	0 days
710	6.5 CM-5 - Commonwealth Compute Procs Manual (CCPM) Completed	5/31/14	5/31/14	0 days
711	6.6 CM-6 - Network Connectivity Completed	4/1/14	4/1/14	0 days
712	6.7 CM-7 - Security Arch, Soln, Policies and Procedures Completed	5/31/14	5/31/14	0 days
713	6.8 CM-8 - ITSM Systems Integration Completed	8/8/14	8/8/14	0 days
714	6.9 CM-9 - Financial Management Complete	5/31/14	5/31/14	0 days
715	6.10 CM-10 - Operational Readiness (GSK)	7/30/14	7/30/14	0 days
716	6.11 CM-11 - SSAE 16 Audit of EDC Complete	12/1/14	12/1/14	0 days
717	6.12 CM-12 - DPH DCM Completed	5/26/15	5/26/15	0 days
718	6.13 CM-13 - DPH DCM Completed - Escalated Penalty	11/22/15	11/22/15	0 days
719	6.14 CM-14 - EDC Transition Completed	12/31/14	12/31/14	0 days
720	6.15 CM-15 - L&I DCM Completed	5/31/16	5/31/16	0 days
721	6.16 CM-16 - DOR DCM Completed	5/31/16	5/31/16	0 days
722	6.17 CM-17 - PSP DCM Completed	5/31/16	5/31/16	0 days
723	6.18 CM-18 - DPW DCM Completed	5/31/16	5/31/16	0 days
724	6.19 CM-19 - DOH DCM Completed	5/31/16	5/31/16	0 days
725	**7 - Sample MOVE PACKAGE Schedule (to be replicated and modified as required by Move Package)**	**12/1/13**	**5/30/14**	**129 days**
726	**7.1 DCM_MP - PLAN MIGRATION**	**12/1/13**	**5/30/14**	**129 days**
727	**7.1.1 Project Management Tasks**	**12/1/13**	**5/30/14**	**129 days**
728	7.1.1.1 Goverance Plan	12/1/13	5/30/14	180 edays
729	7.1.1.2 Risk Plan	12/1/13	5/30/14	180 edays
730	7.1.1.3 Validate Data Gathering Timeline	12/1/13	5/30/14	180 edays
731	7.1.1.4 Configuration/Test Plan	12/1/13	5/30/14	180 edays
732	**7.1.2 DCM_MP - MOVE STRATEGY/IDENTIFY SERVERS**	**12/2/13**	**12/18/13**	**13 days**
733	7.1.2.1 Schedule Individual Application Meetings and Distribute Questionairre	12/2/13	12/2/13	1 day
734	7.1.2.2 Conduct One-on-One Application Owner Meetings	12/10/13	12/16/13	1 wk

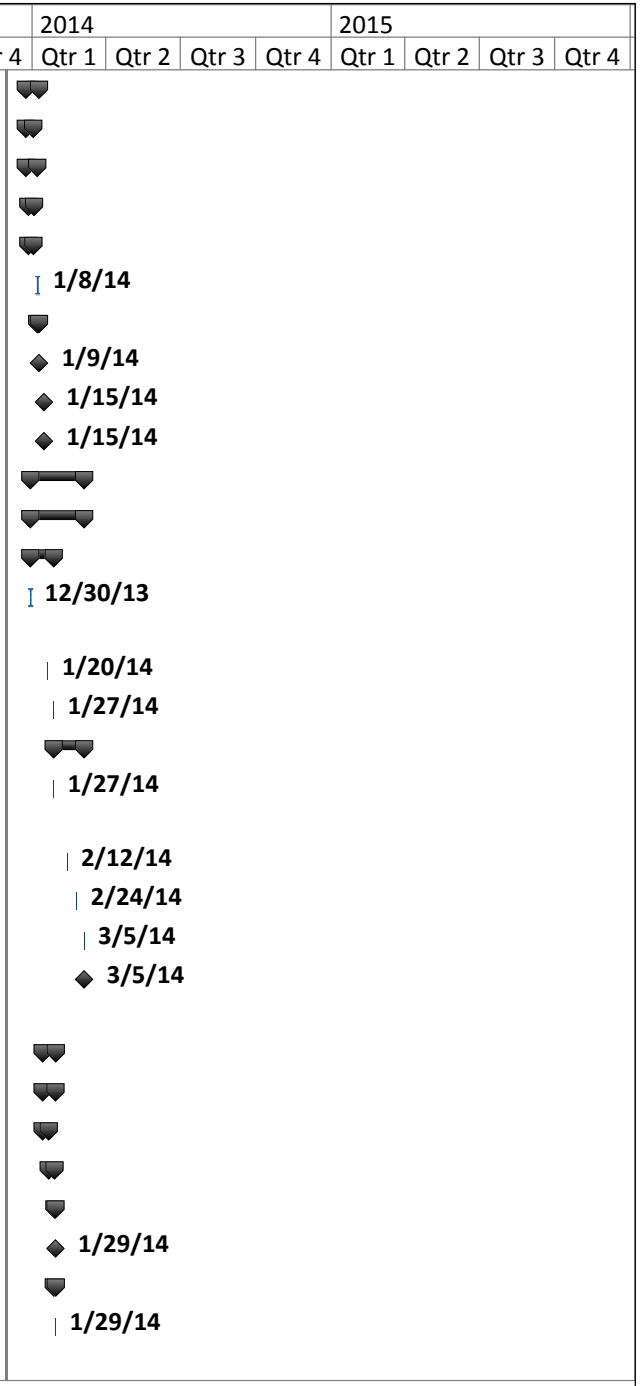


ID	Task Name	Start	Finish	Duration
735	7.1.2.3 Conduct Internal Planning Meeting/Review Overall Approach	12/17/13	12/17/13	2 hrs
736	7.1.2.4 Identify In-Scope P2P, V2V, Forklift Server/Applicati	12/17/13	12/17/13	4 hrs
737	7.1.2.5 Validate Move Strategy & Initial Logistics Assessment (Virtual & Forklift)	12/17/13	12/17/13	4 hrs
738	7.1.2.6 Validate Out-of-Warranty Servers	12/17/13	12/17/13	4 hrs
739	7.1.2.7 Determine HA, backup and DR requirements for each application	12/18/13	12/18/13	4 hrs
740	7.1.2.8 Refine MP Move Baseline (Unix and Intel) with DCM Team Review	12/18/13	12/18/13	4 hrs
741	**7.1.2.9 DCM_MP - CODE FREEZE**	**12/18/13**	**12/18/13**	**0.5 days**
742	7.1.2.9.1 Initiate MP Server Baseline Inventory Freeze	12/18/13	12/18/13	0.5 hrs
743	7.1.2.9.2 Initiate MP Code Freeze for all the Related Applications	12/18/13	12/18/13	0.5 hrs
744	7.1.2.9.3 Remove any remaining hard coded IP s from the applications	12/18/13	12/18/13	4 hrs
745	7.1.2.9.4 COMPLETED: DCM_MP - CODE FREEZE	12/18/13	12/18/13	0 days
746	7.1.2.10 COMPLETED: DCM_MP - MOVE STRATEGY / IDENTIFY SERVERS	12/18/13	12/18/13	0 days
747	**7.1.3 DCM_MP - MOVE STRATEGY SIGNOFF**	**12/19/13**	**12/20/13**	**1.5 days**
748	7.1.3.1 Review Move Package Contents and Strategy with	12/19/13	12/19/13	1 day
749	7.1.3.2 Provide Move Package Contents and Strategy to for Approval	12/20/13	12/20/13	2 hrs
750	7.1.3.3 Receive Move Package Content and Strategy Approval to Proceed from	12/20/13	12/20/13	2 hrs
751	7.1.3.4 COMPLETED: MP - MOVE PACKAGE STRATEGY SIGN	12/20/13	12/20/13	0 days
752	**7.1.4 DCM_MP - DUE DILIGENCE PLANNING**	**12/20/13**	**12/24/13**	**1.63 days**
753	7.1.4.1 Schedule, Prepare, Perform MP Kickoff Meeting	12/20/13	12/20/13	1 hr
754	7.1.4.2 Establish Weekly Meetings with App Owners and Technical Team	12/20/13	12/24/13	1.5 days
755	7.1.4.3 Schedule WAN Analysis (optional)	12/20/13	12/20/13	0.06 days
756	7.1.4.4 Check if WAN Analysis is completed & remediation implemented (optional)	12/20/13	12/23/13	0.5 days
757	7.1.4.5 COMPLETED: DCM_MP - DUE DILIGENCE PLANNING	12/24/13	12/24/13	0 days
758	**7.1.5 DCM_MP - CREATE WORKBOOK**	**12/20/13**	**1/15/14**	**18 days**

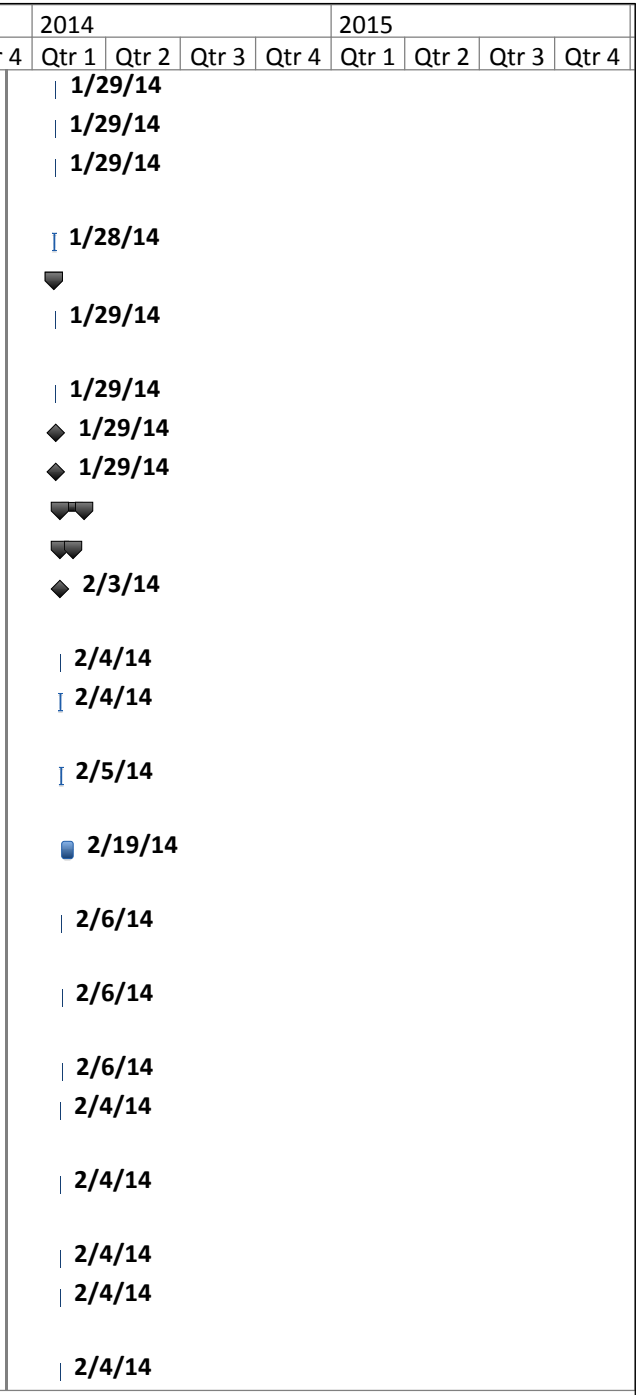


ID	Task Name	Start	Finish	Duration
759	7.1.5.1 Initiate Workbook for Move	12/20/13	12/27/13	1 wk
760	7.1.5.2 Assess MP in-flight projects, determine status and establish a plan for completion	12/27/13	12/30/13	1 day
761	**7.1.5.3 DCM_MP - DEVELOP RISK MANAGEMENT PLAN FOR MOVE**	**12/27/13**	**1/2/14**	**4 days**
762	**7.1.5.3.1 MP_RISK - RISK MITIGATION**	**12/27/13**	**12/30/13**	**1 day**
763	7.1.5.3.1.1 Review Standard Move Package Risks for Applicability	12/27/13	12/27/13	0.5 days
764	7.1.5.3.1.2 Document Move Package Risks and Mitigat	12/30/13	12/30/13	0.5 days
765	**7.1.5.3.2 MP_RISK - CONTINGENCY PLANNING**	**12/27/13**	**1/2/14**	**4 days**
766	7.1.5.3.2.1 Identify / Review Requirements for Contin	12/27/13	12/30/13	1 day
767	7.1.5.3.2.2 Review Options for Contingency	12/30/13	12/31/13	1 day
768	7.1.5.3.2.3 Review Options with to Obtain Agreement on Contingency Strategy	12/31/13	1/1/14	1 day
769	7.1.5.3.2.4 Finalize Contingency Plan	1/1/14	1/2/14	1 day
770	7.1.5.3.2.5 COMPLETED: MP_RISK - CONTINGENCY PL	1/2/14	1/2/14	0 days
771	7.1.5.3.3 COMPLETED: DCM_MP_PM - DEVELOP RISK MANAGEMENT PLAN FOR MOVE	1/2/14	1/2/14	0 days
772	**7.1.5.4 MP_APPS - DEVELOP TEST PLANS**	**12/27/13**	**1/15/14**	**13 days**
773	7.1.5.4.1 Review Initial Test Plan Template with the Application Test Lead	12/27/13	12/27/13	4 hrs
774	7.1.5.4.2 Identify Applications to be Tested	12/30/13	12/31/13	16 hrs
775	7.1.5.4.3 Identify Application Testers	1/1/14	1/2/14	16 hrs
776	7.1.5.4.4 Commit to Re-IP Planned Outage Window + Receive Email Approval from App Owners	1/3/14	1/3/14	8 hrs
777	7.1.5.4.5 Work with Application Test Lead to Create the Test Plan	12/30/13	12/30/13	8 hrs
778	7.1.5.4.6 Develop the High Level Test Plan (HLTP)	12/31/13	1/1/14	16 hrs
779	7.1.5.4.7 Create Test Cases / Scripts	1/3/14	1/9/14	5 days
780	7.1.5.4.8 Finalize Test Plan	1/10/14	1/10/14	8 hrs
781	7.1.5.4.9 Execute Dry Run of Test Cases and Scripts (Base	1/13/14	1/13/14	8 hrs
782	7.1.5.4.10 Establish Success Criteria Statement for DCM	1/14/14	1/14/14	4 hrs
783	7.1.5.4.11 Receive Written Approval of Test Plan and Success Criteria from	1/14/14	1/15/14	1 day
784	7.1.5.4.12 COMPLETED: MP_APPS - DEVELOP TEST PLAN	1/15/14	1/15/14	0 days

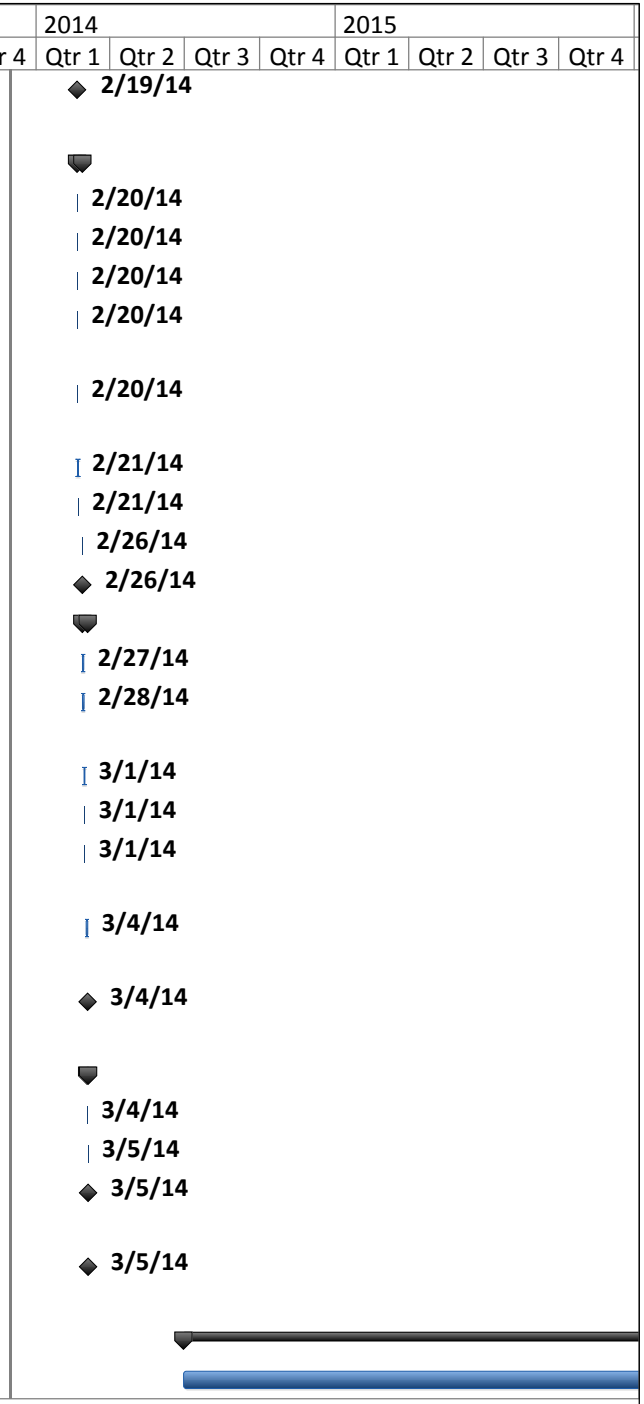
ID	Task Name	Start	Finish	Duration
785	**7.1.5.5 DCM_MP - SITE PREPARATION**	**12/24/13**	**1/9/14**	**12.13 days**
786	**7.1.5.5.1 DCM_MP_SP - SERVER IP REQUIREMENTS**	**12/24/13**	**1/2/14**	**7.25 days**
796	**7.1.5.5.2 DCM_MP_SP - FIREWALL RULE REQUIREMENT**	**12/24/13**	**1/7/14**	**10 days**
803	**7.1.5.5.3 DCM_MP_SP - WINTEL SERVICE REQUESTS**	**12/27/13**	**1/3/14**	**4.38 days**
816	**7.1.5.5.4 DCM_MP_SP - UNIX SERVICE REQUESTS**	**12/27/13**	**1/2/14**	**3.75 days**
841	7.1.5.5.5 DCM_MP_SP - Confirm SAN Setup	1/7/14	1/8/14	1 day
842	**7.1.5.5.6 MP_APPS - FIREWALL SERVICE REQUEST**	**1/7/14**	**1/9/14**	**2.13 days**
849	7.1.5.5.7 COMPLETED: DCM_MP_SP - SITE PREPARATIO	1/9/14	1/9/14	0 days
850	7.1.5.6 COMPLETED: DCM_MP - CREATE WORKBOOK	1/15/14	1/15/14	0 days
851	7.1.6 COMPLETED: DCM_MP - PLAN MIGRATION	1/15/14	1/15/14	0 days
852	**7.2 DCM_MP - MIGRATION TO DC1**	**12/30/13**	**3/5/14**	**47.63 days**
853	**7.2.1 DCM_MP - REVIEW AUDITS AND DCM NOTIFICATIONS**	**12/30/13**	**3/5/14**	**47.63 days**
854	**7.2.1.1 Pre-Re-IP Notifications**	**12/30/13**	**1/27/14**	**20.5 days**
855	7.2.1.1.1 Prepare & Send 30 Day Pre-Re-IP Planned Outage Notice	12/30/13	12/30/13	4 hrs
856	7.2.1.1.2 Prepare & Send 7 Day Pre-Re-IP Planned Outag	1/20/14	1/20/14	0.5 days
857	7.2.1.1.3 Prepare & Send 2 Day Pre-Re-IP Planned Outag	1/27/14	1/27/14	4 hrs
858	**7.2.1.2 Pre-DCM Notifications**	**1/27/14**	**3/5/14**	**27.25 days**
859	7.2.1.2.1 Prepare & Send 30 Day Pre-DCM Planned Outage Notice	1/27/14	1/27/14	4 hrs
860	7.2.1.2.2 Prepare & Send 7 Day Pre-DCM Planned Outag	2/12/14	2/12/14	4 hrs
861	7.2.1.2.3 Prepare & Send 2 Day Pre-DCM Planned Outag	2/24/14	2/24/14	4 hrs
862	7.2.1.2.4 Completion Notification (3 days post-move)	3/5/14	3/5/14	2 hrs
863	7.2.1.3 COMPLETED: DCM_MP REVIEW AUDITS AND DCM NOTIFICATIONS	3/5/14	3/5/14	0 days
864	**7.2.2 DCM_MP - Re-IP/Mock Move EVENT**	**1/14/14**	**1/29/14**	**12 days**
865	**7.2.2.1 DCM_MP_Re-IP - EXECUTION**	**1/14/14**	**1/29/14**	**11.5 days**
866	**7.2.2.1.1 MP_Re-IP - PREPARE APPLICATIONS**	**1/14/14**	**1/21/14**	**5.25 days**
884	**7.2.2.1.2 MP_Re-IP - GO/NO-GO DECISION**	**1/21/14**	**1/28/14**	**5.25 days**
893	**7.2.2.1.3 MP_Re-IP - EXECUTE Re-IP EVENT**	**1/28/14**	**1/29/14**	**1 day**
898	7.2.2.1.4 COMPLETED: DCM_MP_Re-IP - EXECUTION	1/29/14	1/29/14	0 days
899	**7.2.2.2 DCM_MP_Re-IP - POST RE-IP ACTIVITIES**	**1/27/14**	**1/29/14**	**2.25 days**
900	7.2.2.2.1 Update/Verify new IP Addresses for All Servers in Baseline	1/29/14	1/29/14	4 hrs



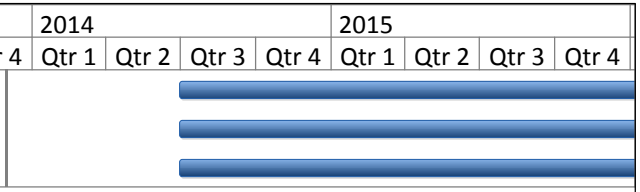
ID	Task Name	Start	Finish	Duration
901	7.2.2.2.2 Commit to Move Package Planned Outage Win	1/29/14	1/29/14	2 hrs
902	7.2.2.2.3 Make Initial Move Logistics Arrangements	1/29/14	1/29/14	2 hrs
903	7.2.2.2.4 Install any required data transfer hardware or software agents (optional)	1/29/14	1/29/14	2 hrs
904	7.2.2.2.5 Develop/Distribute Move Hr-By-Hr Plan (Draft)	1/27/14	1/28/14	7 hrs
905	**7.2.2.2.6 Submit CRQ Numbers to PM for Move**	**1/27/14**	**1/27/14**	**0.13 days**
914	7.2.2.2.7 Reserve War Room (Conference Rooms) for Move event	1/29/14	1/29/14	2 hrs
915	7.2.2.2.8 Arrange Site Access for Move Event	1/29/14	1/29/14	2 hrs
916	7.2.2.2.9 COMPLETED: DCM_MP_Re-IP - POST RE-IP ACT	1/29/14	1/29/14	0 days
917	7.2.2.3 COMPLETED: DCM_MP - Re-IP EVENT	1/29/14	1/29/14	0 days
918	**7.2.3 DCM_MP - MOVE PACKAGE MIGRATION EVENT**	**2/3/14**	**3/5/14**	**21.63 days**
919	**7.2.3.1 DCM_MP_MOVE - PERFORM FINAL LOGISTICS TAS**	**2/3/14**	**2/19/14**	**12 days**
920	7.2.3.1.1 Submit Final Logistics Request Form to Logistics Manager	2/3/14	2/3/14	0 days
921	7.2.3.1.2 Request ISSA Approval to ship systems	2/4/14	2/4/14	0.5 hrs
922	7.2.3.1.3 Provide Logisitics Quote & Shipping Plan to Project Manager for Approval	2/4/14	2/4/14	1 day
923	7.2.3.1.4 Receive Approved Logistics Quote & Shipping Plan from Project Manager	2/5/14	2/5/14	1 day
924	7.2.3.1.5 Initiate Logistics Plan & Coordinate with Shipping Vendors	2/6/14	2/19/14	10 days
925	7.2.3.1.6 Confirm DC Physical Security Arrangements (Guards are Notified)	2/6/14	2/6/14	2 hrs
926	7.2.3.1.7 Confirm security access arrangements for source locations	2/6/14	2/6/14	2 hrs
927	7.2.3.1.8 Submit Change Request for Move Event	2/6/14	2/6/14	1 hr
928	7.2.3.1.9 AC-Verify CCPM contains specific details for apps within Move Package	2/4/14	2/4/14	4 hrs
929	7.2.3.1.10 AC-Validate Monitoring is in place for Move Package Apps - will appear on dashboards	2/4/14	2/4/14	1 hr
930	7.2.3.1.11 AC-Confirm SLAs are in place for Move Packag	2/4/14	2/4/14	0.13 days
931	7.2.3.1.12 AC-Confirm ITSM ready to receive information regarding Move Package Apps	2/4/14	2/4/14	0.13 days
932	7.2.3.1.13 AC-Verify DR plans and test scheduled as appr	2/4/14	2/4/14	0.13 days



ID	Task Name	Start	Finish	Duration
933	7.2.3.1.14 COMPLETED: DCM_MP_MOVE - PERFORM FINAL LOGISTICS TASKS	2/19/14	2/19/14	0 days
934	**7.2.3.2 DCM_MP_MOVE - GO/NO-GO DECISION**	**2/20/14**	**2/26/14**	**4.38 days**
935	7.2.3.2.1 Finalize the Move Hr-By-Hr Plan Schedule	2/20/14	2/20/14	2 hrs
936	7.2.3.2.2 Prepare for Move GO/NO-GO Conference Call	2/20/14	2/20/14	2 hrs
937	7.2.3.2.3 Review Final Move Package Risks with	2/20/14	2/20/14	1 hr
938	7.2.3.2.4 Validate and Approve Move Package Success Criteria with	2/20/14	2/20/14	1 hr
939	7.2.3.2.5 Submit Supplemental CMDB Updates for Migration (if needed)	2/20/14	2/20/14	1 hr
940	7.2.3.2.6 Final Receiving Site(s) Walk-Thru Inspection	2/20/14	2/21/14	2 hrs
941	7.2.3.2.7 Conduct Internal Move GO/NO-GO Decision	2/21/14	2/21/14	1 hr
942	7.2.3.2.8 Conduct Formal Move GO/NO-GO Decision	2/26/14	2/26/14	1 hr
943	7.2.3.2.9 COMPLETED: DCM_MP_MOVE - GO/NO-GO DI	2/26/14	2/26/14	0 days
944	**7.2.3.3 DCM_MP_MOVE - EXECUTE MOVE EVENT ACTIVIT**	**2/26/14**	**3/4/14**	**4.63 days**
945	7.2.3.3.1 Relocate Equipment (Forklift)	2/26/14	2/27/14	30 ehrs
946	7.2.3.3.2 Migration Activities (See Move Hr-By-Hr Plan for Full Details)	2/26/14	2/28/14	2 edays
947	7.2.3.3.3 Conduct Move Application Testing	2/28/14	3/1/14	1 eday
948	7.2.3.3.4 Final Conf Call and Verbal approvals	3/1/14	3/1/14	1 ehr
949	7.2.3.3.5 AC-Provide MP Completion Documentation to Steady State and receive signoff	3/1/14	3/1/14	2 ehrs
950	7.2.3.3.6 AC-Received Approved MP Completion Documentation from App Owners	3/3/14	3/4/14	2 days
951	7.2.3.3.7 COMPLETED: DCM_MP_MOVE - EXECUTE MOVE EVENT ACTIVITIES	3/4/14	3/4/14	0 days
952	**7.2.3.4 DCM_MP_POST-MOVE LESSONS LEARNED**	**3/4/14**	**3/5/14**	**1.25 days**
953	7.2.3.4.1 MP_Post- Move Lessons Learned - Internal Tea	3/4/14	3/4/14	1 hr
954	7.2.3.4.2 MP_Post- Move Lessons Learned - Full Team	3/5/14	3/5/14	1 hr
955	7.2.3.4.3 COMPLETED: DCM_MP_POST-MOVE LESSONS LEARNED	3/5/14	3/5/14	0 days
956	7.2.3.5 COMPLETED: DCM_MP - MOVE PACKAGE MIGRATION EVENT	3/5/14	3/5/14	0 days
957	**8 Steady State Operations and Continuous Improvement**	**6/30/14**	**12/31/24**	**2742 days**
958	8.1 Operations Monitoring	6/30/14	12/31/24	2742 days



ID	Task Name	Start	Finish	Duration
959	8.2 Service Request Management	6/30/14	12/31/24	2742 days
960	8.3 Disaster Recovery Testing	6/30/14	12/31/24	2742 days
961	8.4 Security Testing	6/30/14	12/31/24	2742 days



3.1.1 Multi Datacenter Environment (2+ Architecture)

The Offeror must provide a multi datacenter environment. All datacenters will be managed and maintained by the Offeror, including the Commonwealth's EDC and may be either a standalone facility, or integrated into existing qualified facilities. The multi datacenter environment is to facilitate high availability, capacity on demand, and the recovery of applications and Services that are deemed critical to the Commonwealth. The multi datacenter requirement is to provide a minimum of two datacenters. The Offeror may propose additional capacity and Services utilizing additional facilities beyond the two required datacenters.

Reference Documentation

Schedule E – Datacenter Locations

Exhibit A - Commonwealth Network Environment

Exhibit(s) D.1 through D.15 – Enterprise Datacenter (EDC) Exhibits

	Requirements	Describe Compliance
1.	The Offeror's datacenter architecture must consist of multiple geographically disbursed datacenters. Any datacenters being used in a back-up function must be at least 50 miles apart from the associated primary location for the service.	Offeror must describe the process of establishing a multi datacenter environment, including facility management, resource sharing, operational coordination, and inter-datacenter communications. Provide proposed datacenter architecture and locations. Using **Schedule E – Datacenter locations**, the Offeror must list the address of all proposed Datacenter locations that will host the Commonwealth's applications and data.
2.	Tier III equivalent datacenter facilities proposed by the Offeror must have had consistent availability of 99.99% in the past six months as of December 31, 2011.	Offeror must provide current availability reports of its proposed datacenter(s) with its submittal.

3.	The EDC assets will be managed and maintained by the Offeror. The current maintenance contract for the EDC servers is scheduled to expire on June 30, 2014.	Offeror must describe its approach to transition operations and management of the EDC infrastructure from the Commonwealth to the Offeror's support Services and how it intend to address the server maintenance expiration issue.
4.	Each datacenters will have the capability to provide DR for the other, for identified critical applications.	Offeror must describe the process of providing DR for critical applications from one datacenter to the other. Also, describe additional DR Services if included in the overall proposed offering.
5.	Datacenter sustainability.	Offeror must describe its methods of achieving datacenter sustainability, such as realizing a low Power Usage Effectiveness (PUE) ratio.
6.	Robust physical security, including biometric access control, video surveillance, and routine security officer patrols.	Offeror must describe its security methods and techniques that will be used to protect Commonwealth computing assets and ensure compliance with Commonwealth security requirements.
7.	In a datacenter environment that hosts both Commonwealth and non-Commonwealth clients, segregation of Commonwealth data, and computing resources from other clients' data and computing resources. The Offeror is required to provide system and data segregation between different agency application environments. Note: The Offeror may not use the EDC to provide services to Non-Commonwealth clients. The Commonwealth may permit the Offeror to provide services to COSTARS members if written permission is granted by the Commonwealth.	Offeror must describe its approach to provide Services in the event a datacenter will be shared with a non-Commonwealth client, describe how segregation of resources will be achieved and maintained. Offeror must describe how systems and data segregation can be maintained between different agency application infrastructure environments.

8.	Elastic datacenter infrastructures to accommodate variable workloads.	Offeror must describe its computing and networking capabilities that will accommodate the growth or contraction of workloads.
9.	24/7/365 staffing.	Offeror must describe the staffing model used to provide 24/7/365 staffing. Operations staff, technical support staff, security staff, and management. Offeror must address how it plan to manage security/background checks, monitoring and reporting on employees and how it will coordinate those requirements with Criminal Justice agencies.
10.	Common work and meeting space.	Offeror must describe its capabilities to accommodate meeting and workspace for Commonwealth and Offeror IT staff and management.

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

4 DR Services

4.A Each datacenters will have the capability to provide DR for the other, for identified critical applications.

The Unisys data center architecture provides an operational model that supports a strategic intent of maturing the Commonwealth's disaster recovery posture. Unisys selection of sites was from its team's portfolio of sites and beyond. The selection criteria included criteria based on the Commonwealth's IT Strategic Plan published in late 2011 for operational characteristics that are required in facilities supporting the Commonwealth. The evaluation of sites over the last 18+ months has always included a mutual DR characteristic. With the [redacted] sites, Unisys has sites that can back each other up. Each has similar facilities infrastructure designed to provide a site ready to operate for the other where applications require.

Examples where this is the case appear throughout the solution such as the placement of the production Unisys mainframe in [redacted] with a DR peer in the [redacted] In fact, where [redacted] was once a cold and warm DR site, now those application

environments are in the [redacted] and [redacted].

In addition, Unisys is able to adjust and widen its DR approach where cost or design dictate. An example is the incorporation of the existing use of the [redacted] facility into the data center fabric as a continuing cold site option for the IBM mainframes. The [redacted] facility is also available to support geographic separation for disaster recovery as the Commonwealth's business or policies change.

While these stand as options, Unisys decisions on how production, test, development, and DR systems are deployed are not assumed. Agency use, including the use of the [redacted] as a participant in the architecture, will be a result of collaboration between the Unisys team and the agency in determining the best deployment for the best cost that meets an application's operating needs.

For example, the Department of Labor and Industry's application DR solutions may be migrated to the data centers in a number of ways, all of which Unisys will call on DLI for review and approval. In this case, specifically, the Unisys migration team along with its architecture, facility and space management teams will work to gain DLI's insight and counsel to collaborate on the best solution for DLI.

For more information and greater detail on the Unisys disaster recovery services please see Schedule F, Sections 3.2.1.5.2 "IT Service Continuity Architecture", 3.2.2.4 "DR Planning and Testing" and 3.2.5.3 "DR Infrastructure on Demand".

7 System and Data Segregation

7.A "In a datacenter environment that hosts both Commonwealth and non-Commonwealth clients, segregation of Commonwealth data, and computing resources from other clients' data and computing resources.

Offeror must describe its approach to provide Services in the event a datacenter will be shared with a non-Commonwealth client, describe how segregation of resources will be achieved and maintained."

Unisys data center architecture provides for secure physical and logical separation from any adjacent facility or campus occupants, including an ability to provide similar segregation within the Commonwealth's IT services area. The Commonwealth's IT environment is secure physically and logically from other potential occupants of the facilities supporting it.

At the [redacted] facility, the Commonwealth environment will occupy an entire "data center vault" at the facility and have its own secure entrance and facility infrastructure. No other facility customers from the other data center vaults are able to access the Unisys Commonwealth data center vault. Additionally, within the vault, 12 ft. tall cage mesh partitions can be used to separate different environments and systems as required.

At [redacted] the Commonwealth of Pennsylvania environment takes a secure data center area with security access controls and power and cooling infrastructure. In addition, the Commonwealth may select to install security caging with "slab-to-slab" steel wire-mesh fencing using the cages listed within the Enterprise Services Catalog or to a custom size via a service request.

3.2.1.5.2 IT Service Continuity Architecture

The Offeror's IT Service Continuity Architecture will provide tiered DR capabilities and Services for applications that have been identified by the Commonwealth. The Offeror must provide a Service Continuity solution that includes DR computing, storage, networking systems and recovery processes and will be included in the overall Commonwealth architecture design. Only critical applications and associated equipment identified by the Commonwealth will be addressed with DR systems. Additional information regarding Tiered Service Delivery and Tiered DR can be found in referenced supporting exhibits.

The Commonwealth will lead the Business Continuity effort with assistance from the Offeror.

Reference Documentation

Schedule J.1 - Datacenter Service Level Management

Requirements		Describe Compliance
1.	DR Architecture and Plan will be documented by the Offeror and approved by the Commonwealth.	Offeror must describe its infrastructure and service offering for a DR and Business Continuity Plan.
2.	IT Service Continuity Architecture and Plan - Backup hardware and software will be obtained, configured and available per an agreed to Service Level to process the identified critical applications. Where applicable, data will be electronically replicated (including disk-2-disk) to the backup systems (off site) to insure a successful recovery. Wherever data replication is not viable, backup tape data will be utilized.	Offeror must describe the design of its Tiered DR plan in the design of the Commonwealth technical architecture. Offeror must provide at least one relevant example from a prior engagement, in which it was engaged, that is similar to the needs of the Commonwealth. Offeror must describe its process for modifying the scope/service level for DR coverage.
3.	Recovery systems must be available via network access. Routing must be configured and tested during initial system architecture design. Include the network requirements of the DR plan in the design of the network architecture.	Offeror must describe the network requirements of its DR plan in its proposed design of the network architecture.

4.	Recovery documentation for each identified system/ application will be required. Information will include the targeted backup hardware, software, networking changes, data location, restoration and access process, execution authorization, and notification to service owner when an application has been restored to service. Offeror must create recovery documentation for each system / application identified as a critical system where DR is required.	Offeror must provide at least one relevant example from a prior engagement, in which it was engaged, that is similar to the tiered DR needs of the Commonwealth.
5.	A DR support plan must be created. The DR team must notify the Commonwealth when a recovery plan will be put into action, and must manage questions and issues that may arise after implementation. Create a DR team that will manage the execution of the DR plan from declaration to recovery when required.	Offeror must provide at least one relevant example from a prior engagement, in which it was engaged, that is similar to the DR needs of the Commonwealth.
6.	For critical systems identified as having a current tested DR Plan within the DPH, the Offeror will update the associated DR test plans for the new target environment. Successful testing of each revised DR Plan is required prior to Commonwealth acceptance.	Offeror must provide its approach to creating and testing DR Plans.
Deliverables		
Deliverables are defined in **Schedule K – Key Program Deliverables**		
Offeror Response		

3 DR, Recovery Systems

3.A Recovery systems must be available via network access. Routing must be configured and tested during initial system architecture design.

Include the network requirements of the DR plan in the design of the network architecture.

Offeror must describe the network requirements of its DR plan in its proposed design of the network architecture.

The Unisys solution leverages the same network for DR as it does for Production applications. The Unisys solution meets the COPANET connectivity requirements by connecting locally at EDC via 2x 10Gb Ethernet and via 1 x 1G Ethernet connections to one of several possible COPANET locations; the exact COPANET location in Harrisburg will be determined during the data gathering activities.

In addition to utilizing the EDC, a new data center will be utilized – [redacted]. In the [redacted] a new connection to the existing COPANET node will be built, as described above, using two 10Gb fiber connections within the Commonwealth Technology Center [redacted] Since the distance to connect the EDC to COPANET is so short, these connections will not require a WAN circuit to be installed, thus saving cost. The 1 Tech Park connectivity is shown on the far left in the diagram below (**Figure 3.2.1.5.2-1**)

[redacted]

Figure 3.2.1.5.2-1 – Commonwealth Network Architecture

On the right side of the diagram above, the COPANET connection to [redacted] is shown. Based on predicted future usage, the [redacted] data center will be connected to COPANET via a 1 Gb circuit. To prevent a single point of failure in the connection to COPANET, the two (2) 10G WAN circuits that run between the EDC and [redacted] will be used to reroute any COPANET traffic should there be a telco link failure. The locations being considered to terminate the [redacted] circuit are 555 [redacted]

[redacted] is connected to the Commonwealth using an Internet VPN tunnel terminated in both EDC and [redacted]. [redacted] has a large amount of commercial Internet bandwidth available from multiple telco providers. Should direct connectivity to the Verizon PIP network be required, Unisys will terminate Commonwealth provided PIP circuits on Unisys owned and managed equipment at the data centers.

A deeper technical description is provided in section F.3.1.2 Network and Security Architecture.

This page intentionally left blank.

3.2.4.2 Storage Management

The Storage Management service will provide hosting and operational support Services for storage management systems. Storage management systems must be maintained at current support levels for optimal performance, recoverability, and secure operations. Systems will be located in the Offeror's datacenters. The Offeror must support the hardware and software components of these systems.

The proposed storage management service and solution must address adherence to multiple security and compliance requirements relating to the storage and management of multiple types of data assets (e.g. CHRIA law, criminal history).

Reference Documentation

Exhibit B.1 - DPH - Asset List

Exhibit B.2 - DPH - Commonwealth Owned DPH IT Assets

Exhibit C.1 - DPW - Room 105 and CAO Servers – Storage

Exhibit D.1 - EDC - Server Inventory

Exhibit D.2 - EDC - Switch Summary

Exhibit D.3 - EDC - Storage Summary

Exhibit D.5 - EDC - DOT Datacenter Inventory

Exhibit E.1 - DLI - Datacenter Inventory Template

Exhibit F.1 - DOH - Datacenter Inventory Template

Exhibit F.2 - DOH - DPH Asset List

Exhibit F.3 - DOH - DPH COPA Software Asset IBM

Exhibit F.4 – DOH – Physical Servers

Exhibit G.1 - PSP - Datacenter HW Inventory

Exhibit G.3 - PSP - DPH Asset List

Exhibit G.12 - PSP - CHRIA Handbook

Exhibit H.1 - DOR - Datacenter Inventory

Exhibit H.2 - DOR - DPH Asset List

Exhibit H.4 - DOR - SAP TRM System

Exhibit I.1 - IES - DPH COPA Owned IT Assets

Requirements		Describe Compliance
1.	Monitor local operations, troubleshoot and resolve operational issues. Monitor system backup processing on a daily basis. Actively monitor the daily operations of all storage units. Maintain a log for each storage unit. Complete weekly service logs indicating the frequency logs are reviewed, and the status of the daily backup process. Create problem records for any abnormal condition and any repairs that have been made.	Offeror must describe proposed storage management Services. Offeror must identify tools it uses to support data backups including the following: • Processes and Procedures • Tools / Applications • End User Reports o Standard o Custom • Tiered Service/Support Levels • Escalation Procedures
2.	Provide appropriately trained staff that hold current manufacturer certifications for hardware and software technical support (where available). Staff will interact with vendor support Services as needed. Provide Commonwealth with a resume or CV for each operational staff member assigned to this engagement. A copy will be maintained on Offeror file including required background checks and clearances as required.	Offeror must submit a representative sample of staff resumes typically provided for these positions detailing their experience, education, and certifications.
3.	Provide platform level operational and technical support for the computing platform. Provide Level 2 and Level 3 Support to the Service Desk and/or Commonwealth Users. Provide a tiered level of support Services (e.g. Gold, Silver, Bronze)	Offeror must describe its approach to providing and maintaining different tiered levels of support. Offeror must provide a representative sample of available tiered service support Services.

4.	Monitor system backup processing on a daily basis. Review daily backup log for successful completion. Note failures, and correct the problem. Create problem record for any abnormal condition and any repairs that have been made. An automated software process will be utilized to report the completion status of backup processing, with electronic notification of failures sent to identified Commonwealth staff and Offeror technical support for follow up and corrective action.	Offeror must describe its approach to perform an initial review and audit of the backup policies, procedures and reports, to ensure the accuracy of the backup schedules, retention periods, target directories, and recovery point objectives. Offeror must describe its approach to identifying gaps and potential risks, and how those gaps and risks will be resolved.
5.	Ensure network connectivity, and consistent system response times. Identify automated system management tool(s) to ensure storage system availability and expected response times. Stop / Start time records will be a source of input for SLA measurements. Identify tool set(s).	Offeror must describe its real-time monitoring approach and toolset to provide and maintain network availability and performance. Offeror must identify tools it uses to support network availability and performance.
6.	Ensure storage device operating systems are maintained with the current system patch level, including firmware upgrades. Analyze monthly service patches and determine which patches need to be applied. Create a change record, log the update in the storage system log, and install based on maintenance schedule. Notify impacted Commonwealth users immediately of any unscheduled service interruptions via email/web.	Offeror must describe its approach to patch management. Offeror must identify tools used to manage system patches. Offeror must describe its approach for testing and validating updates to the OS and 3rd Party software that it supports. Offeror must describe its approach to communicating unscheduled and scheduled outages, including escalation process.

	The Offeror must document normal work hours and holiday schedules with each agency to determine the contact method and escalation process of each Commonwealth agency. Coordinate at an agency level and account for any required patching as technology upgrades require.	
7.	Utilize data storage conservation techniques such as data de-duplication or other industry standards, to reduce the overall footprint of the data.	Offeror must describe approach and toolset to meet this requirement. Offeror must describe data retention options/Services to store data for extended periods.
8.	Propose options/solutions for self-provisioning or limited self-management of storage as a service.	Offeror must describe approach and toolset to meet this requirement.
Continual Service Improvement		
9.	Reduce service risks.	Offeror must provide methods to eliminate or mitigate service risks.
10.	Improve service quality.	On a quarterly basis, Offeror must also recommend to the Commonwealth team any system changes that would be appropriate to maintain or improve SLA commitments.
11.	Improve client satisfaction.	Offeror must provide examples of previous Offeror initiatives aimed at continually improving client satisfaction.
12.	Ensure service transparency.	Offeror must provide methods and practices to ensure service transparency, providing visibility into service execution.
13.	Improve/reduce cost of service.	Offeror must provide examples of Storage Management initiatives that have been implemented or can be utilized to achieve reduced costs of Services and to meet or

		exceeded ROI (Return on Investment) analysis projections.

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

Introduction

The Unisys solution provides Storage Management through both EMC and IBM storage tools as well as Mainframe-based tools for storage dedicated to the Mainframes. These tools provide Unisys with the means to monitor and manage storage to the Commonwealth's requirements.

The Unisys solution builds upon the EMC storage tools by relying upon the [redacted] backup software suite as well as the [redacted] storage management and monitoring software suite. [redacted] manages the daily data protection processes. [redacted] provides administration dashboards for the underlying data protection infrastructure including backup servers, storage devices, tape libraries, fibre channel switches, replication processes, virtual server instances, as well as MS SQL and Oracle.

The combination of [redacted] and [redacted] will provide the Commonwealth with a comprehensive set of data protection capabilities that stretch across multi-data center infrastructures. [redacted] centralize the management of diverse locations while delivering NAS, SAN, DAS, and WAN backup options. The product set completes the integration of tape-based and disk-based backups including client-based software that optimizes the use of the solution's [redacted] infrastructure by reducing traffic load on the network.

Unisys challenged its partner EMC to match a new market approach to providing unlimited access to backup software that uses a subscription based on the amount of data protected rather than the legacy model of selling software licenses based on the complexity of the backup infrastructure. In support of the Commonwealth's goal of achieving cost savings for quality services and to continue [redacted] long-term support of the Commonwealth, [redacted] responded with an extremely cost competitive model.

1 Storage Management Services

1.B Offeror must identify tools it uses to support data backups including the following:

Processes and Procedures,

Tools / Applications,

End User Reports (standard and custom), and

Tiered Service/Support Levels

The Unisys solution includes the [redacted] software to automate the data backup services and the [redacted] to monitor and manage to data protection policies. The

tools are integrated into the Unisys Nagios collectors within the ITSM Services so that abnormal events and backup failures result in incident tickets which are managed to resolution.

The [redacted] tool also produces detailed dashboards reporting metrics on data backup activity and correlates these to delivery of critical service level requirements for application protection. This reporting mechanism is integrated to the Real-time Dashboard maintained and managed by ITSM Services. This integration provides deep-level backup reporting to the Services Portals available to Commonwealth service managers and staff who can access these dashboards for up-to-date reporting on the Service Level metrics that roll up into the Commonwealth SLAs for Backups and Restores.

The Unisys solution manages Backup services within the Infrastructure Architecture framework described in F.3.2.2.2 (Infrastructure Architecture).

The available ITSM Capacity, Tiered Service Levels, Tools, and End User Reports that are integrated into the Backup Service components are described in detail in Section 1 of Schedule F, Section 3.2.3.2 (Site Operations).

These are the additional tools provided in the Enterprise Services Catalog for replication services within and between data center locations.

[redacted]

The diagram below illustrates a feature available in the Enterprise Services Catalog that is alluded to in the Commonwealth's Disaster Recovery and Business Continuity requirements: the ability to have 3 copies of synchronized data across various data centers. The Unisys solution assumes that the platinum application availability is achieved by building upon application-based data replication that the application can manage to failover in clustered configurations.

The [redacted] product is proposed to manage the requirements for triple data copies. This configuration shown in **Figure 3.2.4.2-1** can be ordered from the Enterprise Services Catalog and then tested to the Commonwealth's most critical application's failover requirements.

The [redacted] can already provide seamless failovers at the server/host layer for Windows and Linux servers running on VMware. As the Commonwealth might expect EMC puts a high priority on integration testing with all of the product lines from its subsidiary VMware and this strategic partnership remains part of the EMC's long-term strategy of providing increased value in the server and application layers.

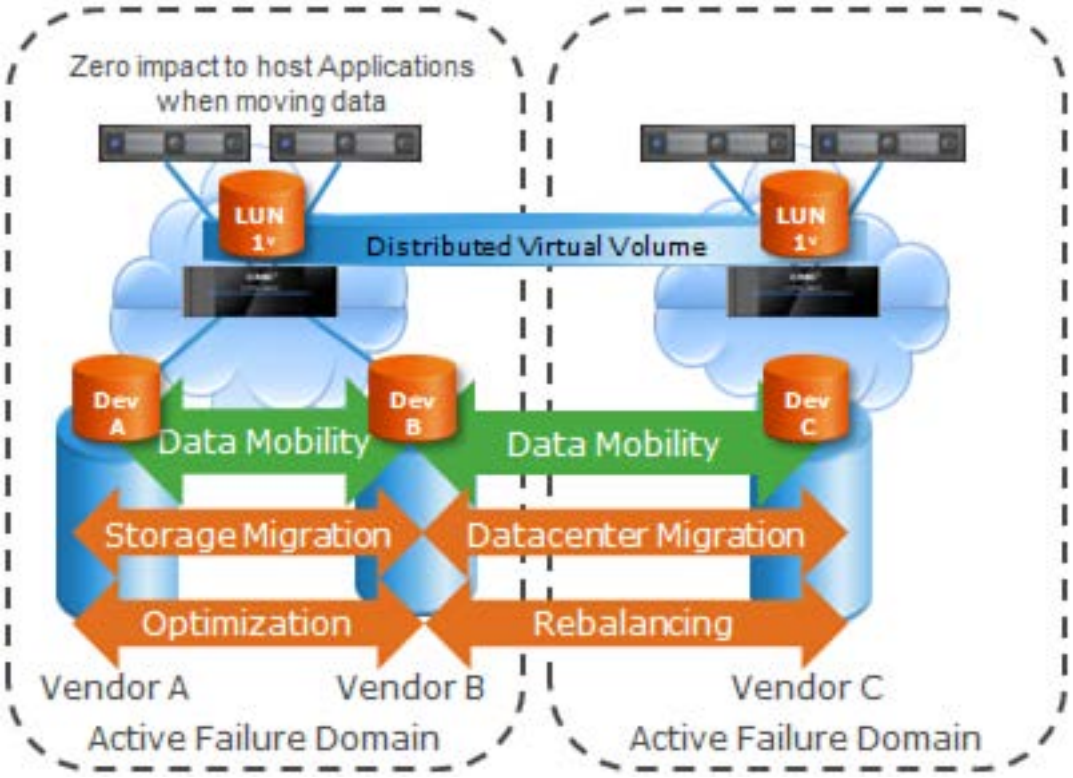


Figure 3.2.4.2-1 - [redacted]

[redacted]: Storage Virtualization and Data Protection

Figure 3.2.4.2-2 illustrates how the EMC's product will allow the Unisys Team to provide value across heterogeneous storage environments. The Commonwealth can select the [redacted] solution in the Enterprise Services Catalog as well as the R[redacted]t solution so that Agencies can migrate data into the Unisys-managed data centers and leverage existing storage assets until the end of their service life.

The V[redacted] configuration is also the means by which Unisys is able to offer the very fast Recover Time Objectives as well as Recovery Point Objectives that can offer near-zero data loss in the event of a disaster. These offerings are summarized below in Section 5.B as the Tier 5 and Tier 6 Disaster Recovery service offerings.

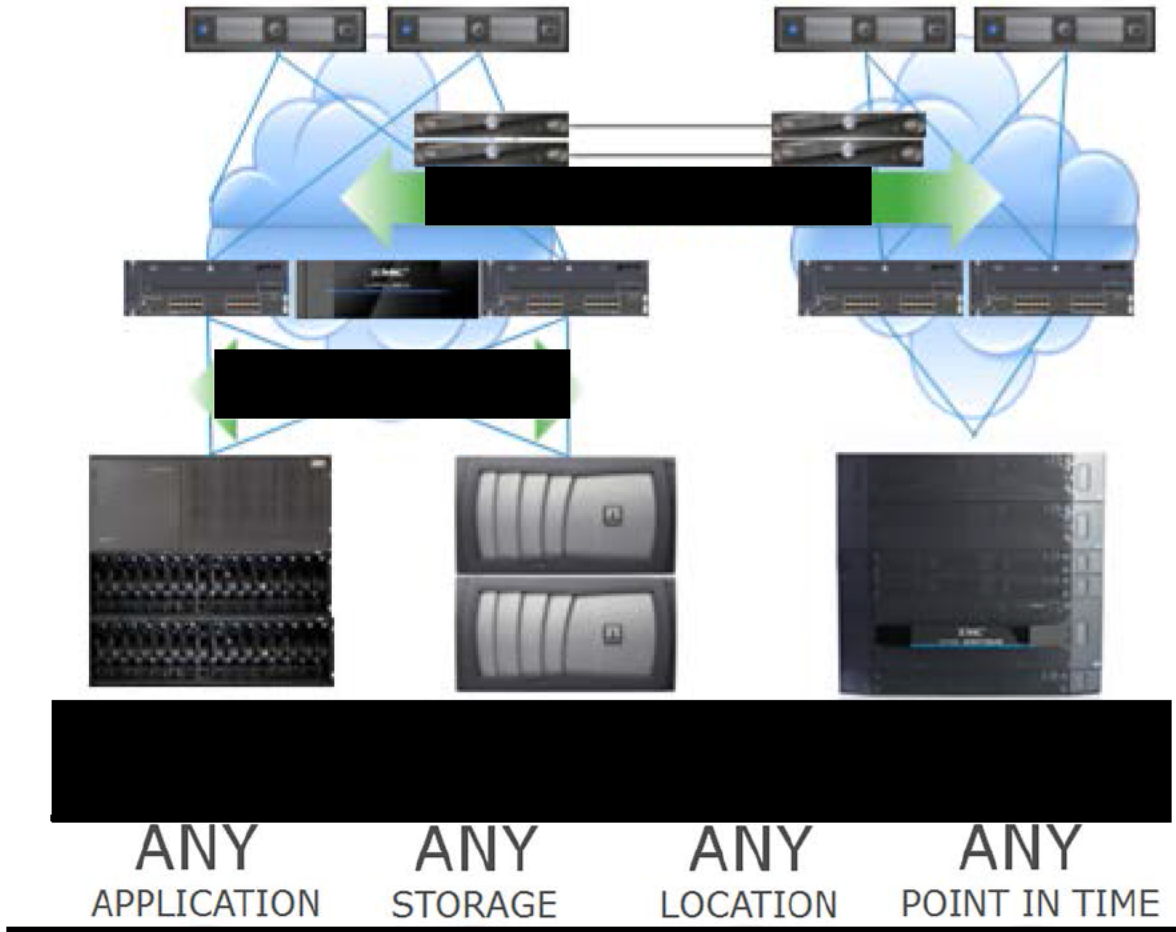


Figure 3.2.4.2-2

Figure 3.2.4.2-3 below shows the failover capabilities of the storage platform in the Unisys solution. The modular frames in the Unisys N+1 architecture can be configured in pairs to further increase the reliability and resiliency of the underlying Storage infrastructure.

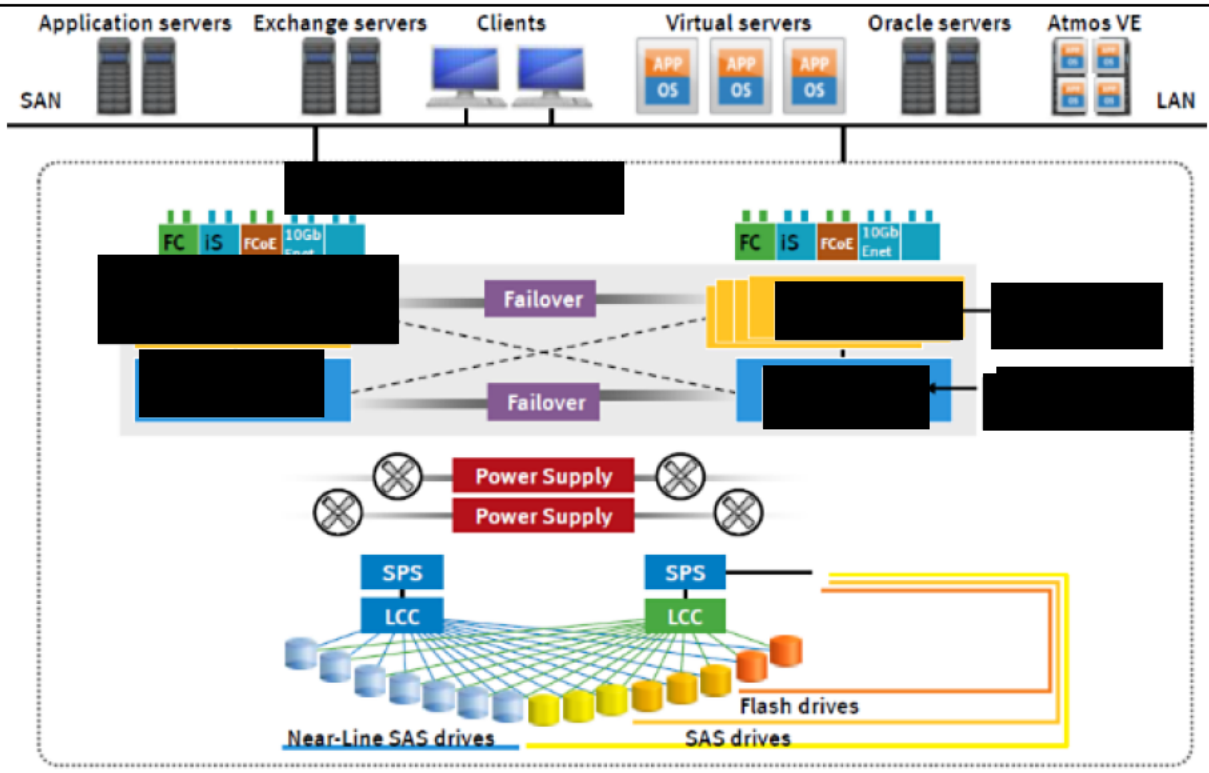


Figure 3.2.4.2-3 - [redacted]

The primary storage trends over the last two decades have reflected the increasing feature sets of mid-tier modular frames. Thus feature sets that customers paid a high premium for in Mainframe-class monolithic storage frames are, over time, refined and offered in the mid-tier frames. No company has been more successful in this storage trend than EMC, and this accounts for its majority market share in the industry. The [redacted] product series takes advantage of the [redacted] software, offered within the Unisys solution, to manage communications between servers and storage. This replicates the process that occurs in the storage controllers of large storage frames and allows a pair of separate [redacted] storage frames to appear as a single entity to the servers through [redacted].

[redacted]

The [redacted] in **Figure 3.2.4.2-4** provides a cost-effective way of integrating diverse storage frames from different vendors and from different frame models from a single vendor and virtualize the storage in a manner that servers are unaware of the storage hardware beneath the [redacted] layer.

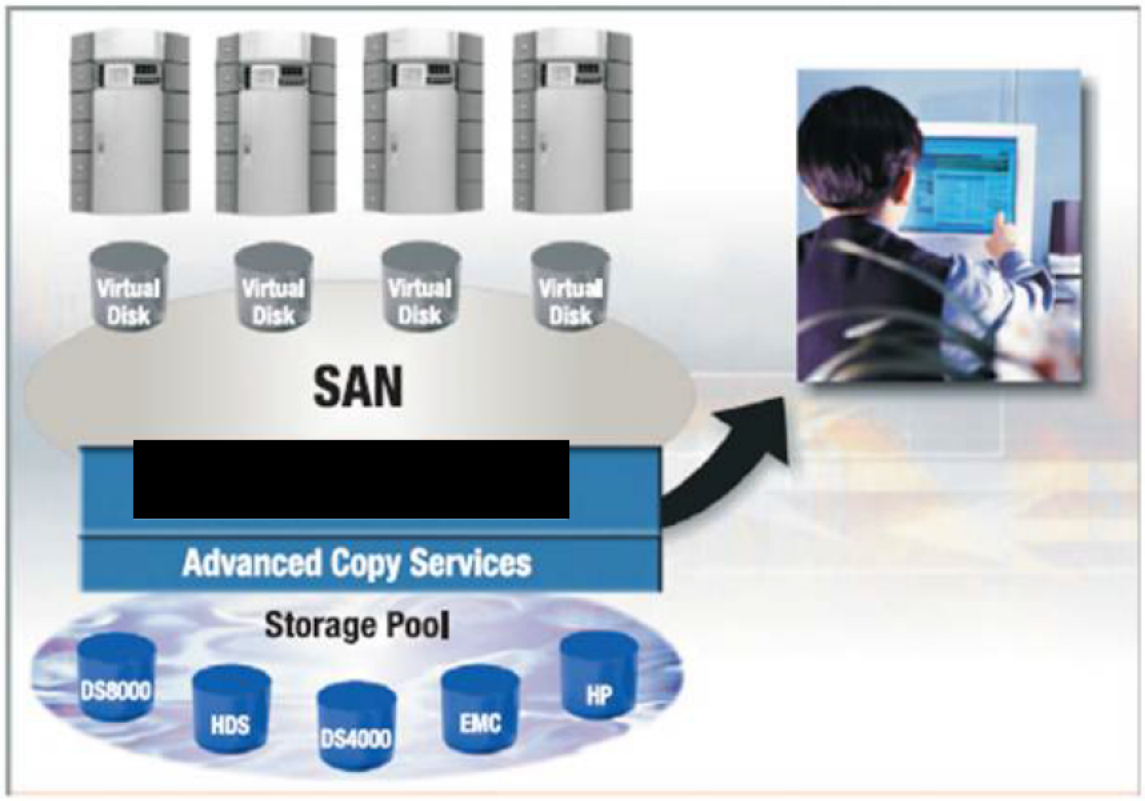


Figure 3.2.4.2-4 - [redacted]

[redacted] is designed to help increase the amount of storage capacity that is available to host applications. By pooling the capacity from multiple disk systems within the SAN, it helps enable storage administrators to reach beyond traditional islands of SAN storage and deploy storage in ways that can help best meet the needs of host applications.

Because the SVC hides the physical characteristics of storage from host systems, [redacted] is designed to help insulate host applications from physical changes to the storage pool. This ability can help applications continue to run without disruption as Unisys makes changes to the storage infrastructure. This will increase availability of Commonwealth services because a hardware refresh of storage frames can be conducted without disruption to the Commonwealth's servers providing access to data even when the replaced storage frame has been evacuated of data and unplugged.

End User Reports

- Standard Reports are summarized in 3.3.2.
- Custom Reports are offered by Unisys via the Enterprise Services Catalog

Tiered Service/Support Levels

The Commonwealth of Pennsylvania has indicated in Schedule J.2 - Datacenter Service Level Matrix the desired service tiers/support levels. In the design of the Services and the infrastructure needed to deliver those Service to the Commonwealth, the Unisys Team defined the Service Tiers to align to those requirements. A fuller explanation and representative sample

of all the Services provided in this structure can be found in the response to Section 3.2.1.5 sub-requirement 1.

4 System Backup Review and Audit, Gap Assessment

4.B Offeror must describe its approach to identifying gaps and potential risks, and how those gaps and risks will be resolved.

During transition and transformation, the Unisys solution includes an extended onsite presence of an [redacted] technical manager who aids the Unisys Team in the search for existing gaps and risks, along with potential improvements to the backup systems during the transition phase of the solution. This technical expert has extensive experience in implementations and in identifying value-add opportunities. The skills of this technical expert are married to the Unisys Team's extensive expertise around current backup operations. Jointly they lead the transition to the more cost effective [redacted] backup infrastructure. The Unisys Team, also working with the [redacted] technical manager, manages the review and audit of backup clients that move from the legacy system into the [redacted] system. During transition a like-to-like set of backup policies, procedures, reports, schedules, retention periods, target directories, and recovery point objectives are built out. The Unisys Team can then present the Commonwealth opportunities to further optimize the infrastructure to improve the quality of services or provide better cost efficiencies for the same services.

The Unisys Backup team is also able to compare the Backup inventory of clients and policies to the CMDB inventory to locate "negative" gaps in case a server or critical data set is introduced into the Fully Managed environment and, through unlikely process failures, was not protected with sufficient backup resources. The Unisys governance processes and the processes generated by the Unisys solution's Enterprise Services Catalog are designed to remove such failures. Additionally, a compare of Backup infrastructure inventory from the backup tools perspective with the CMDB can locate a gap should one occur as an additional level of protection The activities to perform the gap analysis are described in F.3.2.4.2, Requirement 4.

4.G An automated software process will be utilized to report the completion status of backup processing, with electronic notification of failures sent to identified Commonwealth staff and Offeror technical support for follow up and corrective action.

This is included as part of the [redacted] tools as described above in Section 4.D/E.

7 Data Storage Approach and Toolset

7.A Utilize data storage conservation techniques such as data de-duplication or other industry standards, to reduce the overall footprint of the data.

Offeror must describe approach and toolset to meet this requirement.

Offeror must describe data retention options/Services to store data for extended periods.

Unisys offers the Commonwealth the [redacted] platform and the [redacted] of backup software to achieve data de-duplication. [redacted] offers the Commonwealth a means to utilize de-duplication not only at the target backup media to reduce capacity but also

de-duplication at the source of the data the Commonwealth server that is backed up. This latter capacity reduces network load due to backups and speeds up the backup process by using hashed handshakes between backed-up server and the backup server.

Figure 3.2.4.2-5 below shows the basic concepts of [redacted] client and target based deduplication.

The [redacted] integration will now allow large servers that support Commonwealth applications to be backed up by using the very fast Fibre Channel (FC) to write directly to the [redacted] disk target. In some cases where very little has changed on a server, almost no data will be transferred because the [redacted] already has the unchanged blocks on disk. This will speed up the backups for the Commonwealth's most critical database application servers.

Within the Unisys solution, the large database infrastructures will [redacted]" to deduplicate data at the client side to avoid any network transfer at all for blocks of data that were sent in previous backups.

The tight integration of [redacted] reduces the bandwidth required on the IP data network, as well as the disk capacity required. And, because this support offers both client-side deduplication and support of the Fibre Channel protocol using a backup-to-disk workflow, the old VTL 'tape-based' management can be reduced to only appropriate point solutions. This means greater reliability and less complexity. This support also enables all the features that [redacted] and [redacted] offer, including virtual synthetic full backups, clone controlled replication, and global deduplication.

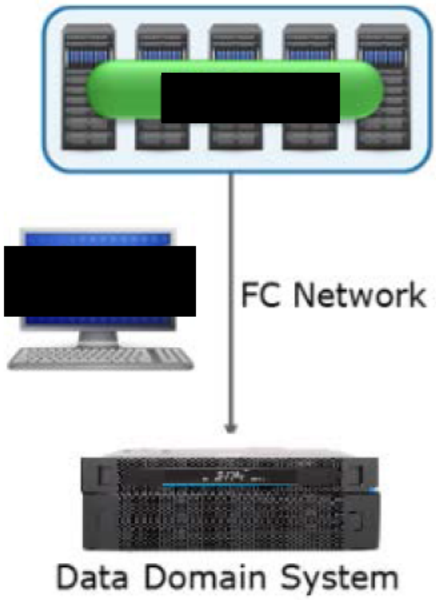


Figure 3.2.4.2-5 – [redacted] Deduplication

Unisys also considered the option of implementing Thin Provisioning for the Commonwealth because this is an industry-standard tool used to reduce storage foot print although it is not widely used. Thin Provisioning would allow a vendor to report that 2 TBs of storage had been allocated to a server but the server would only be provided with a stub or an IOU that would be filled only as the server began to fill up the space with actual data. However Thin Provisioning also brings with it significant risk of performance impacts. Basically if a vendor has "thin provisioned" 1,000 TBs but has only provided 100TBs of actual disk to meet data requests then the I/O demand on the actual disk provisioned is 10 times greater than if the 100TBs had actually landed on 1,000 TBs of actual disk. Unisys would like to caution the Commonwealth to consider both the billing and performance implications of any solutions that represent "Thin Provisioning" as a significant cost saver: That savings comes with a high I/O performance penalty and removes transparency by disconnecting billing statements based on Thin Provisioned storage from the actual storage hardware and software that provide capacity-based performance.

13 CI Reduce Cost of Service

13.A Improve/reduce cost of service.

Offeror must provide examples of Storage Management initiatives that have been implemented or can be utilized to achieve reduced costs of Services and to meet or exceeded ROI (Return on Investment) analysis projections.

The Service Excellence Office will proactively manages quality, continuous service improvement, ITIL process management, and customer satisfaction through a comprehensive quality plan that specifically addresses all of these areas. We believe this is a key differentiator in our partnership with the Commonwealth. Through this new organization and these quality plans, Unisys will drive best in class services and the highest customer satisfaction experience, while reducing overall costs to the Commonwealth.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

A few examples of Storage Management Continuous Service Improvement that have been implemented or can be utilized to achieve reduced costs of Services and to meet or exceeded ROI (Return on Investment) analysis projections are outlined below:

Storage Management

The DPH has implemented Distributed File Systems (DFS) to replicate our DPH File Server down to [redacted] In the event of a true disaster, files to perform our duties during and after the DR will be available. Data replication occurs in real time and is de-duplicated over the wire thus saving bandwidth on the WAN link. This confirms that our documentation, recovery scripts and procedures are current and accessible at all times to support Commonwealth agencies during disaster recovery drill and in the event of an actual disaster. By avoiding having to ship tapes containing this information to [redacted] and having to restore them, Unisys has improved the recovery time objective for disaster drills and disaster events.

Storage Management

As part of the DPH's continuing improvements in its backup infrastructure, the DPH has improved the successful recovery an 8TB database archive for IES from 10.7 hours down to nearly 4 hours by improving the bandwidth from .75Tb/hour to 2TB/hour. The DPH

accomplished this by bypassing the AIX VIO Shared Ethernet Adapter (SEA) built in restrictions and optimizing throughput between the media servers and the [redacted]

Storage Reporting - Service Level and Other Reports:

Throughout the contact, Unisys has provided a vast amount of contractual reporting to the Commonwealth. The reports include, but are not limited to Monthly Performance Reporting for each supported agency/bureau, Major reporting improvements include, Quarterly Vulnerability Reporting, Monthly XIV Storage Reporting for IES and DOR physical hosts, Monthly Storage Reports for PLCB, Monthly VMAX Storage Reports for DPW.

Storage SAN Advances:

Through advanced configuration and deployment of an Avamar grid the DPH is capable of replicating deployments of virtual servers between data centers. This capability is also leveraged for several disaster recovery scenarios including initial DR deployments and annual disaster recovery drills.

Storage Replication for DR:

Storage replication solutions have been implemented for several agencies using the latest disk to disk replication technology. These solutions have enabled a reduced dependency on tape media and drives for backup while providing a disk to disk update to offsite data supporting both data backup as well as disaster recovery requirements. Ongoing research and trials are conducted in conjunction with product support organizations to provide proper configuration and optimal performance for the technology supporting this critical managed service.

Disk-based Backup Strategy:

The Unisys solution leverages [redacted] products to facilitate disk-based backups and data replication to an offsite location. This eliminates cost and unreliability associated with tape media and significantly expedites recovery time in the event of a disaster. The implementation of a disk to disk with data de-duplication strategy for IES resulted in a significant reduction in backup and restore times for the extremely large, rapidly growing SAP data store. At the time that IES migrated to the DPH, the data store in SAP was 5 TB. This data store had previously been backed up across 32 tape drives taking close to five hours to back up. This left IES exposed to issues with tape media that would prevent the ability to restore effectively. Since their implementation, the size of the SAP data store peaked at 9 TB with performance on the disk-based backup solution enabling completion of backups in less than four hours.

Benefits to the Commonwealth

The Unisys Backup Service provides significant costs savings over those offered by competitors. The Unisys solution relies upon [redacted] and IBM technologies. Unisys challenged [redacted] to provide its premium backup infrastructure at more cost effective rates. During the Unisys BAFO efforts [redacted] provided substantial discounts in support of the Commonwealth's goal of reducing costs for critical services.

The Unisys solution for Storage Management provides interoperable, innovative automation

and integration between the Unisys ITSM monitoring and management and the standard management tool suites offered by EMC and IBM. This innovation allows the Unisys ITSM technical support staff to remove costly labor-based monitoring and escalation and provide the Commonwealth with more cost effective solutions.

The Unisys integration of ITSM monitoring and management tools with logging and alert features provided by [redacted] and IBM also provides a higher quality of services for the Commonwealth by automating incident ticket creations to engage technical staff proactively. The ITSM monitoring of event logs within Infrastructure components can create incident tickets on an initial logged event before the event cascades into a service disruption.

This page intentionally left blank.

3.2.4.7 Database Management Services

The Database Management Service will provide the Commonwealth with a "managed database" service offering. The service must include the database platform (Hardware/Software) and the ongoing database management administration Services. The Offeror must provide a multi-tiered level of service (e.g. Gold, Silver, and Bronze) across multiple database platforms. While the Commonwealth's application portfolio (over 2,000 applications) currently utilizes numerous database technologies, the majority of the applications that are utilizing database technologies are using Oracle, Microsoft SQL, IMS, Sybase, or DB2.

It is anticipated the Database Management Services will be an optional service that can be utilized by the Agencies beyond the basic infrastructure Services.

Reference Documentation

N/A

Requirements		Describe Compliance
1.	Design, manage, and administer database environments that support multiple business applications.	Offeror must describe proposed approach to designing and supporting enterprise level database platforms and Services that support multiple agency business applications.
2.	Provide Level 2 and Level 3 Support to the Service Desk and/or Commonwealth Users.	Offeror must describe its approach to supporting the needs of the Commonwealth including the following: • Processes & Procedures • Tiered Service/Support Levels • Tools / Applications • Escalation Procedures • End User Reports o Standard o Custom
3.	Monitor database backup and recovery processing on a daily basis.	Offeror must describe its approach to perform an initial review and audit of the backup and recovery policies, procedures

	Review daily backup log for successful completion. Note any failures, initial and date the log, and correct the problem. Create problem record for any abnormal condition and any repairs that have been made. Automated software process will be utilized to report the completion status of backup processing, with electronic notification of failures sent to Offeror technical support and identified Commonwealth staff for follow up and corrective action.	and reports, to ensure the accuracy of the backup schedules, retention periods, target directories, and recovery point objectives. Offeror must describe its approach to identifying gaps and potential risks, and how those gaps and risks will be resolved.
4.	Provide a multi-tiered level of service (e.g. Platinum, Gold, Silver, Bronze, and Basic) for Oracle, Sybase, Microsoft SQL, IMS or DB2 database platforms. Provide Level 2 and Level 3 Support to the Service Desk and/or Commonwealth Users.	Offeror must describe its approach to providing multi-tiered Services level.
5.	Utilize the proposed service management Services (e.g. Incident, Service Request, Change, Configuration) to manage database management Services with multiple agency customers.	Offeror must describe how its proposed database management Services will support multiple agency service requests.
6.	Provide a review and analysis of system performance/capacity to determine if current performance/capacities are sufficient to support the needs of the stakeholders.	Offeror must perform an initial review and audit of the current usage, procedures and reports and provide an analysis of the current usage, processes and reports currently being supported. Offeror must document its review and audit findings and recommendations.
7.	Monitor system backup processing on a daily basis. Review daily backup log for	Offeror must describe it approach to performing an initial review and audit of the backup policies, procedures and reports, to ensure the accuracy of the backup schedules, retention periods, target directories, and

	successful completion. Note failures, and correct the problem. Create problem record for any abnormal condition and any repairs that have been made. An automated software process will be utilized to report the completion status of backup processing, with electronic notification of failures sent to Offeror technical support, and identified Commonwealth staff for follow up and corrective action.	recovery point objectives. Offeror must describe its approach to identifying gaps and potential risks, and how those gaps and risks will be resolved.
Continual Process Improvement		
8.	Reduce service risks.	Offeror must provide methods to eliminate or mitigate service risks.
9.	Improve service quality.	On a quarterly basis, Offeror must also recommend to the Commonwealth team any system changes that would be appropriate to maintain or improve SLA commitments.
10.	Improve client satisfaction.	Offeror must provide examples of previous Offeror initiatives aimed at continually improving client satisfaction.
11.	Ensure service transparency.	Offeror must provide methods and practices to ensure service transparency, providing visibility into service execution.
12.	Improve/reduce cost of service.	Offeror must provide examples of Database Management Support initiatives that have been implemented or can be utilized to achieve reduced costs of Services and to meet or exceeded ROI (Return on Investment) analysis projections.
Deliverables		
Deliverables are defined in **Schedule K – Key Program Deliverables**		
Offeror Response		

1 Infrastructure, Database Environment

1.A Design, manage, and administer database environments that support multiple business applications.

Offeror must describe proposed approach to designing and supporting enterprise level database platforms and Services that support multiple agency business applications.

As requested, the Database Management Service is available on a time-and-materials basis through the technical resources provided in the Additional Technical Services section of the proposal. The indicated functions below are provided by the database management technical resources.

The Unisys Team provides services to effectively design, manage and administer database environments that support multiple business applications. Our team is uniquely positioned to provide the Commonwealth with the Database Management services as it brings highly specialized staff and deep experience in supporting a highly available and performing infrastructure.

The Unisys Team provides the Commonwealth with 24x7 support to manage database administration, operations and availability. The following represents the Enterprise Services Catalog of Database Management Services that highlights the available services to design, manage and administer your Enterprise database solution:

Database Management Service	Description
Database Design	• Design multiple agency business application database environments • Design the database server and storage platform topologies • Design high availability and scalable solutions
Database Creation / Management	• Install and patch database software • Create and maintain shell database instance sized appropriately based on supplied requirements • Create high availability/clustered configurations where requested
Backup Management	• Create and establish database backups integrated with the larger system backup strategy • Monitor and verify successful execution, retention and storage of backups
Database Recovery	• Configure and test database recovery solutions from backup or archive log • Support Disaster Recovery planning, rehearsal and execution
Application Release Management	• Support deployment management through various test

	environments per defined work plans • Execute physical deployment of application objects within the database
Data Management and Reporting	• Refresh data from backup/export periodically • Create and execute data alteration / extract solutions periodically via supplied requirements • Standard or custom reports as requested
Proactive Database Performance Analysis	• Proactively monitor and report on database health and performance • Provide periodic reports highlighting performance trends and consumption patterns
Proactive SQL Analysis / Tuning Recommendations	• Proactively monitor and report on database SQL performance in the production environment • Provide monthly reports highlighting performance trends and a list of SQL tuning opportunities • Development of tuning options for identified performance opportunities
Provide Level 2/3 Technical Help Desk Support	• Support triage and resolution of calls from the Level 1 Help Desk • Collect and report metrics, solutions and outcomes of said support

The Unisys Team currently supports multiple agencies and applications within the Commonwealth. We have demonstrated experience successfully managing complex system topologies that support multiple applications within distinct program offices and departments. Our approach on delivering successful projects across multiple agencies requires mature project management disciplines, clearly defined service offerings and efficient and timely communication and partnership with our clients.

2 Service Desk, Tiered Support, Level 2/3 Approach

2.A Provide Level 2 and Level 3 Support to the Service Desk and/or Commonwealth Users.

Offeror must describe its approach to supporting the needs of the Commonwealth including the following:

Processes & Procedures

Tiered Service/Support Levels

Tools / Applications

Escalation Procedures

End User Reports (Standard and Custom)

The Unisys Team provides Level 2 and Level 3 Support to Service Desk and/or Commonwealth Users. The Unisys Team offers multiple levels of database support services to provide timely and efficient handling of service requests, streamlined communications and premium customer service. We provide resources with excellent communication and client service skills to effectively interact with the Service Desk as well as Commonwealth Users to manage database issues/requests.

Our Level 2 technical support provides assistance with basic functionality of the database product, such as availability confirmation, overall performance verification, credential management, authorization and authentication as well as data management services. It is anticipated that Level 2 requests are of limited complexity and usually require limited time to resolve.

The Unisys Team Level 3 technical support includes more specialized and complex services such as targeted performance tuning, database availability and recovery, liaison between application teams and product vendors, overall database configuration, high availability and redundancy management, etc. Level 3 support questions often take more than a single session to resolve, or longer than a single day of engineer time.

The following highlights our approach toward Service Desk and Commonwealth User service/problem requests:

- **Processes and Procedures** – As service requests are identified by clients, the support team logs, triages, investigates and responds to end-user problems or requests. Our team follows a documented problem and incident management process based on the ITIL methodology. Processes and procedures are documented for streamline staff integration as well as facilitating consistent service delivery and expectations. Lastly, our team will focus on timely, clear and targeted communications to effectively manage and close requests with mutual satisfaction.
- **Tiered Service and Support Levels** – The Unisys Team provides tiered services and support levels to provide Commonwealth agencies the ability to customize their support needs. Services are available through the service request process for the tiered support structure highlighted below.

Tiered Support Level	Description
Platinum	Full time resources proactively monitoring database backups. Available 24x7x365 (on-site coverage averages 96 hrs. / week) with responsiveness SLA's. Resources are vendor certified (where applicable) with over 10 years of experience
Gold	Full time resources proactively monitoring database backups. Available 24x7x365 (on-site coverage averages 80 hrs. / week) with responsiveness SLA's. Resources are vendor certified (where applicable) with over 8 years of experience

Silver	□□ Full time resources proactively monitoring providing operational status. Available 24x7x365 on-site coverage averages 60 hrs. / week) with responsiveness SLA's. □□ Resources have over 6 years of qualified experience
Bronze	□□ Shared resources proactively monitoring providing operational status. Available 24x7x365 on-site coverage averages 40 hrs. / week) with responsiveness SLA's. □□ Resources are available from a pool of qualified DBA's with over 4 years of experience
Basic	□□ Shared resources available to support requested execution of listed services. Available 8x5x365 with responsiveness SLA's. □□ Resources are available from a pool of qualified DBA's with over 2 years of experience

- □ **Tools or Applications** – In addition to standard desktop software (Office, etc.) the Unisys Team will leverage enterprise class tools to manage database access, inquiry and management. Examples include TOAD, Erwin, Enterprise Manager, Microsoft Management Studio, etc. Licensing changes for these tools may apply and, if required, the tools can be added to the Enterprise Services Catalog. In addition to the database management tools, the Unisys Team will using the enterprise system management tools described in Schedule F, Section 3.2.3.2.
- □ **Escalation Procedures** –The Unisys Team follows a standard ITIL process flow for service request escalation procedures. The Escalation approach is described in Schedule F, Section 3.2.3.2.
- □ **End User Reports (Standard and Custom)** – The Unisys Team brings highly experienced DBAs that provide not only the support in managing databases and resolving issues, but also assisting with the development of end user reports that help with the management of critical Commonwealth applications. Data Management and Reporting is a service included in our Enterprise Services Catalog and governed by the tiered support listed above.

The overall approach for providing daily operations including Processes and Procedures, Tools and Applications, End User Reports, Tiered Service / Support Levels and Escalation Procedures is described in Schedule F, Section 3.2.3.2.

This page intentionally left blank.

5. Appendix A Modifications

Appendix A modifications

As per the RFP instructions, areas of concern were included within Section 8 of our original response. As part of our BAFO response and in addition to our original proposal, Section 8, Objections and Additions to Contract Terms and Conditions, Unisys submits the following additional term and condition that Unisys would like to negotitate with the Commonwealth.

32. TERMINATION

(a) For Convenience

(1) The Commonwealth may terminate this Contract without cause by giving Contractor thirty (30) calendar days prior written notice (Notice of Termination) whenever the Commonwealth shall determine that such termination is in the best interest of the Commonwealth (Termination for Convenience). Any such termination shall be effected by delivery to the Contractor of a Notice of Termination specifying the extent to which performance under this Contract is terminated either in whole or in part and the date on which such termination becomes effective.

In the event of termination for convenience, Contractor shall receive a termination for convenience fee ("Termination for Convenience Fee").

The Termination for Convenience Fee shall equal the applicable amount set out in Tab #6 of Schedule I (Termination Fees) minus the value of all Services performed by the Contractor consistent with the terms of the Contract prior to the effective date of termination.

Comment [DRS1]: Contractor proposes further discussion on the calculation of appropriate termination fees and related formula, including a termination fee for years 4 through 7

Comment [DRS2]: Contractor also proposes that wind down costs and unrecovered investments should be recoverable for certain other types of termination events similar to our existing contract with the Commonwealth

This page intentionally left blank.

Unisys Response to

Commonwealth of Pennsylvania

Office of Administration

Office for Information Technology

[redacted]

Request for Proposal (RFP)
RFP 6100022698

Small Diverse Business Participation Submittal
Best and Final Offer (BAFO)

September 20, 2013

This proposal has been reproduced on recycled paper

UNISYS

Table of Contents

SMALL DIVERSE BUSINESS (SDB) PARTICIPATION SUBMITTAL (RFP REQUIREMENT II-9) 2

1.1 INTRODUCTION 2

1.2 A – PROOF OF SDB QUALIFYING DATA 3

1.2.1 Small Diverse Business Bureau of Small Business Opportunities (BSBO) Verifications 5

1.2.1.1 Acclaim Systems, Inc. – BSBO Verification Letter 5

1.2.1.2 American Personnel Managers and Consultants, Inc.—BSBO Verification Letter 6

1.2.1.3 Atrion Corporation 7

1.2.1.4 Credo Technology Solutions, Inc. – BSBO Verification Letter 8

1.2.1.5 Domino Technologies, Inc.—BSBO Verification Letter 9

1.2.1.6 e & e IT Consulting Services, Inc.—BSBO Verification Letter 10

1.2.1.7 Info-Matrix Corporation—BSBO Verification Letter 11

1.2.1.8 Innovative Business Concepts, Inc.—BSBO Verification Letter 12

1.2.1.9 Latus Commercial Reality—BSBO Verification Letter 13

1.2.1.10 The Metropolitan Technology Services Group LLC—BSBO Verification Letter 14

1.2.1.11 PC Network, Inc.—BSBO Verification Letter 15

1.2.1.12 Pierson Computing Connection, Inc.—BSBO Verification Letter 16

1.2.1.13 Source IT Technologies—BSBO Verification Letter 17

1.3 B – SMALL DIVERSE BUSINESS PARTICIPATION 18

1.3.1 Numerical Percentage of Work Performed by the Small Diverse Businesses 18

1.3.1.1 (a) Percentage of Dollar Amount – Each Subcontract Commitment to Small Diverse Business 19

1.3.1.2 (b) Identified Small Diverse Business Entity 19

1.3.1.3 (c) Services or Supplies and Timeframe Provided By Each Small Diverse Business 20

1.3.1.4 (d) Location Where Each Small Diverse Business Will Provide Services or Supplies 21

1.3.1.5 (e) Timeframe for Each Small Diverse Business to Provide or Deliver Goods or Services 21

1.3.1.6 (f) Letters of Intent 22

1.3.1.7 (g) Small Diverse Businesses – Primary Person Contact Information 36

1.3.1.8 Total Percentages and SDB Subcontractor Commitment Contractual Obligation 37

1.3.1.9 Offeror's Project Person for Small Diverse Business information - Contact Information 37

Small Diverse Business (SDB) Participation Submittal (RFP Requirement II-9)

This Small Diverse Business (SDB) Participation Submittal dated September 20, 2013 in response to the Commonwealth of Pennsylvania Request for Proposal (RFP# 6100022698) is a complete replacement for the Unisys submission on June 19, 2013. This document has been updated and should be considered for evaluation as part of the Unisys Corporation Best and Final Offer.

1.1 Introduction

Unisys carefully considered all available certified Small Diverse Businesses (SDB) in the Commonwealth of Pennsylvania that both complimented and extended Unisys' capabilities and operations providing CoPA with a strong and qualified team (Figure 1). These selected SDBs have these requirements in addition to their experience in the required area of support and their dedication to quality.

In addition to managing and coordinating SDB support requirements, Unisys is committed to mentoring SDB leadership and fostering their growth. The intention is to provide opportunities for them to excel and to provide feedback and dialog that improves and strengthens the SDBs' performance. This philosophy strengthens CoPA's SDBs workforce for this current CoPA project and future projects as well.

Figure 1. Unisys and Small Diverse Businesses (SDB) Provide a Synchronized Team. *Unisys and the SDBs combined functionality provide CoPA with a fully coordinated team.*

1.2 A – Proof of SDB Qualifying Data

RFP	*Requirement*
II-9 A	*To receive credit for being a Small Diverse Business or for subcontracting with a Small Diverse Business (including purchasing supplies and/or services through a purchase agreement), an Offeror must include proof of Small Diverse Business qualification in the Small Diverse Business participation submittal of the proposal, as indicated below:* • *A Small Diverse Business verified by BSBO as a Small Diverse Business must provide a photocopy of their verification letter.*

Unisys has partnered with 13 subcontractors and suppliers that qualify as Pennsylvania Small Diverse Businesses (SDB). Each is currently verified by the Pennsylvania Department of General Services Bureau of Small Business Opportunities (BSBO). Table 1 summarizes proof of the qualifying data. Copies of BSBO verification letters follow this table.

Table 1. Proof of Small Diverse Business Qualification

Subcontractor (SDB) Name	**Vendor Type**	**Certification**
Acclaim Systems, Inc.	MBE	BSBO Verification Letter
American Personnel Managers & Consultants, Inc.	WBE	BSBO Verification Letter
Atrion Corporation	VBE	BSBO Verification Letter
Credo Technology Solutions, Inc.	MBE	BSBO Verification Letter
Domino Technologies, Inc.	MBE	BSBO Verification Letter
E & E IT Consulting Services, Inc.	WBE	BSBO Verification Letter
Info-Matrix Corp	WBE	BSBO Verification Letter
Innovative Business Concepts, Inc.	WBE	BSBO Verification Letter
Latus Capital Advisors Inc.	WBE	BSBO Verification Letter
Metropolitan Services Technology Group LLC	WBE	BSBO Verification Letter
PC Network, Inc.	WBE	BSBO Verification Letter
Pierson Computing Connection, Inc.	WBE	BSBO Verification Letter
Source IT Technologies	WBE	BSBO Verification Letter

1.2.1 Small Diverse Business Bureau of Small Business Opportunities (BSBO) Verifications

1.2.1.1 Acclaim Systems, Inc. – BSBO Verification Letter

NOTICE OF SMALL BUSINESS SELF-CERTIFICATION
AND SMALL DIVERSE BUSINESS VERIFICATION

pennsylvania
DEPARTMENT OF GENERAL SERVICES

The Department is pleased to announce that

ACCLAIM SYSTEMS INC

has successfully completed the Pennsylvania Department of General Services' process for self-certification as a small business under the Commonwealth's Small Business Procurement Initiative as established by Executive Order No. 2011-09, and is verified as a Small Diverse Business with the following designation(s):

BUSINESS TYPE(s): **Information Technology**

CERTIFICATION NUMBER: **163086-2012-07-SB-MBE**

ISSUE DATE: **07/31/2012** EXPIRATION DATE: **07/31/2014**

RECERTIFIED DATE: **7/19/2013**

[redacted]

Sheri Phillips, Secretary
Department of General Services
Commonwealth of Pennsylvania

1.2.1.2 American Personnel Managers and Consultants, Inc.—BSBO Verification Letter

NOTICE OF SMALL BUSINESS SELF-CERTIFICATION
AND SMALL DIVERSE BUSINESS VERIFICATION

pennsylvania
DEPARTMENT OF GENERAL SERVICES

The Department is pleased to announce that

AMERICAN PERSONNEL MANAGERS &

has successfully completed the Pennsylvania Department of General Services' process for self-certification as a small business under the Commonwealth's Small Business Procurement Initiative as established by Executive Order No. 2011-09, and is verified as a Small Diverse Business with the following designation(s):

BUSINESS TYPE(s): **Procurement Services, Procurement Goods, Information Technology**

CERTIFICATION NUMBER: **137157-2012-09-SB-WBE**

ISSUE DATE: **09/08/2012** EXPIRATION DATE: **09/08/2015**

RECERTIFIED DATE: **9/6/2013**

[redacted]

Sheri Phillips, Secretary
Department of General Services
Commonwealth of Pennsylvania

1.2.1.3 Atrion Corporation

pennsylvania
DEPARTMENT OF GENERAL SERVICES

July 29, 2013

Pasquale Grillo
Atrion Communication Resources Inc
185-i Industrial Parkway
Branchburg, NJ 08876

Certification Number: **365173-2013-06-SB-VBE**
Expiration Date: **June 21, 2014**
Business Types: **Information Technology**

Dear Pasquale Grillo:

The Bureau of Small Business Opportunities has reviewed your request for verification along with your supporting documents. I am pleased to inform you that the Commonwealth has verified your company as a Small Diverse Business, Veteran Business Enterprise (VBE). An automatic email was generated with a copy of your new certificate designating your Small Diverse Business status. If you need to obtain a copy of your Small Diverse Business certificate it can be reprinted on Step 5 within the Small Business Procurement Initiative (SBPI).

Please understand that the information you provided for verification was represented as being true and correct. Please know that the Commonwealth shall treat any misstatement as fraudulent concealment of the true facts punishable as a crime under Section 4904 of the Pennsylvania Crime Code, Title 18, of Pa. Consolidation Statutes relating to unsworn falsification to authorities

Your verification is valid until the expiration date noted above. For additional information or assistance, please contact Bureau staff at (717) 705-2398 or (717) 346-8105 or by email at ra-bsboverification@pa.gov. Best wishes in your business endeavors.

Sincerely,

[redacted]
DeShawn A. Lewis, Director
Bureau of Small Business Opportunities (BSBO)

Bureau of Small Business Opportunities
401 North Street | Room 611 | North Office Building | Harrisburg, PA 17120

1.2.1.4 Credo Technology Solutions, Inc. – BSBO Verification Letter

NOTICE OF SMALL BUSINESS SELF-CERTIFICATION

pennsylvania
DEPARTMENT OF GENERAL SERVICES

The Department is pleased to announce that

CREDO TECHNOLOGY SOLUTIONS INC

has successfully completed the Pennsylvania Department of General Services' process for self-certification as a small business under the Commonwealth's Small Business Procurement Initiative as established by Executive Order No. 2011-09, with the following designation:

BUSINESS TYPE(s): **Procurement Services, Information Technology**

CERTIFICATION NUMBER: **378902-2012-09-SB**

ISSUE DATE: **09/14/2012** EXPIRATION DATE: **09/14/2014**

RECERTIFIED DATE: **9/18/2013**

[redacted]

Sheri Phillips, Secretary
Department of General Services
Commonwealth of Pennsylvania

1.2.1.5 Domino Technologies, Inc.—BSBO Verification Letter

pennsylvania
DEPARTMENT OF GENERAL SERVICES

October, 19 2012

Swami Nathan Balagopal
Domino Technologies Inc
6211 Lookout Drive
Mechanicsburg, PA 17050

CERTIFICATIO NO: **176163-2012-10-S**
EXPIRATION DATE: **October 3, 2013**

The Bureau of Small Business Opportunities has reviewed your Recertification Application together with supporting documents. I am pleased to inform you that your company has been approved based on your certification application and your small business self-certification registration through the Small Business Procurement Initiative (SBPI). The Commonwealth now recognizes your company as a Small Business and a Small Diverse Business.

Through the application process, you have presented documentation that your company is engaged in providing certain products and/or services. Information regarding these products and/or services for which you have been certified has been electronically listed in the DGS database for use by all Commonwealth agencies. Please understand that your certification is a tool that you can use to market your goods or services to Commonwealth agencies.

Your certification is valid until the expiration date noted above. For additional information or assistance, please contact Bureau staff at (717) 783-3119 or by email at gs-bsbo@pa.gov. Best wishes in your business endeavors.

Sincerely,

[redacted]

Curtis Burwell
Equal Opportunity Manager

Bureau of Small Business Opportunities
401 North Street | Room 611 | North Office Building | Harrisburg, PA 17120

1.2.1.6 e & e IT Consulting Services, Inc.—BSBO Verification Letter

NOTICE OF SMALL BUSINESS SELF-CERTIFICATION

pennsylvania
DEPARTMENT OF GENERAL SERVICES

The Department is pleased to announce that

E & E IT CONSULTING SERVICES INC

has successfully completed the Pennsylvania Department of General Services' process for self-certification as a small business under the Commonwealth's Small Business Procurement Initiative as established by Executive Order No. 2011-09, with the following designation:

BUSINESS TYPE(s): **Information Technology**

CERTIFICATION NUMBER: **202218-2012-08-SB**

ISSUE DATE: **08/16/2012** EXPIRATION DATE: **08/16/2014**

RECERTIFIED DATE: **7/30/2013**

[redacted]

Sheri Phillips, Secretary
Department of General Services
Commonwealth of Pennsylvania

1.2.1.7 Info-Matrix Corporation—BSBO Verification Letter

NOTICE OF SMALL BUSINESS SELF-CERTIFICATION
AND SMALL DIVERSE BUSINESS VERIFICATION

pennsylvania
DEPARTMENT OF GENERAL SERVICES

The Department is pleased to announce that

INFO MATRIX CORPORATION

has successfully completed the Pennsylvania Department of General Services' process for self-certification as a small business under the Commonwealth's Small Business Procurement Initiative as established by Executive Order No. 2011-09, and is verified as a Small Diverse Business with the following designation(s):

BUSINESS TYPE(s): **Information Technology**

CERTIFICATION NUMBER: **156374-2012-07-SB-WBE**

ISSUE DATE: **07/26/2012** EXPIRATION DATE: **07/26/2014**

RECERTIFIED DATE: **7/8/2013**

[redacted]

Sheri Phillips, Secretary
Department of General Services
Commonwealth of Pennsylvania

1.2.1.8 Innovative Business Concepts, Inc.—BSBO Verification Letter

pennsylvania
DEPARTMENT OF GENERAL SERVICES

July 24, 2013

Jennifer P Briggs
Innovative Business Concepts
209 Hamilton Street
Harrisburg, PA 17102

Certification Number: **129749-2012-07-SB-WBE**
Expiration Date: **July 27, 2014**
Business Types: **Procurement Services, Information Technology**

Dear Jennifer Briggs:

The Bureau of Small Business Opportunities has reviewed your request for verification along with your supporting documents. I am pleased to inform you that your company has been verified as a Woman Business Enterprise (WBE). The Commonwealth recognizes your company as a Small Diverse Business (WBE). An automatic email was generated with a copy of your new certificate designating your Small Diverse Business status. If you need to obtain a copy of your Small Diverse Business certificate it can be reprinted on Step 5 with the Small Business Procurement Initiative (SBPI).

Please understand that the information that you provided for verification was represented as being true and correct. Please know that the Commonwealth shall treat any misstatement as fraudulent concealment of the true facts punishable as a crime under Section 4904 of the Pennsylvania Crime Code, Title 18, of Pa. Consolidation Statutes relating to unsworn falsification to authorities

Your verification is valid until the expiration date noted above. For additional information or assistance, please contact Bureau staff at (717) 705-2398 or (717) 346-8105 or by email at ra-bsboverification@pa.gov. Best wishes in your business endeavors.

Sincerely,

[redacted]

DeShawn A. Lewis, Director
Bureau of Small Business Opportunities (BSBO)

Bureau of Small Business Opportunities
401 North Street | Room 611 | North Office Building | Harrisburg, PA 17120

1.2.1.9 Latus Commercial Reality—BSBO Verification Letter

NOTICE OF SMALL BUSINESS SELF-CERTIFICATION

pennsylvania
DEPARTMENT OF GENERAL SERVICES

The Department is pleased to announce that

LATUS CAPITAL ADVISORS, INC.

has successfully completed the Pennsylvania Department of General Services' process for self-certification as a small business under the Commonwealth's Small Business Procurement Initiative as established by Executive Order No. 2011-09, with the following designation:

BUSINESS TYPE(s): **Procurement Services**

CERTIFICATION NUMBER: **368740-2012-10-SB**

ISSUE DATE: **10/02/2012** EXPIRATION DATE: **10/02/2014**

RECERTIFIED DATE: **9/18/2013**

[redacted]

Sheri Phillips, Secretary
Department of General Services
Commonwealth of Pennsylvania

1.2.1.10 The Metropolitan Technology Services Group LLC—BSBO Verification Letter

pennsylvania
DEPARTMENT OF GENERAL SERVICES

June 4, 2013

Jennifer Connolly
President
The Metropolitan Technology Services Group LLC
22 Wagner Farm Lane
Millstone, NJ 08535

Certification Number: **370936-2013-05-S**
Expiration Date: **May 10, 2014**
Business Types: **Information Technology**

Dear Jennifer Connolly:

The Bureau of Small Business Opportunities has reviewed your request for verification along with your supporting documents. I am pleased to inform you that your company has been verified as a Woman Business Enterprise (WBE) based on your certification with the Women's Business Enterprise National Council (WBENC) and your small business self-certification registration through the Small Business Procurement Initiative (SBPI). The Commonwealth now recognizes your company as a Small Diverse Business (WBE).

Please understand that the information that you provided for verification was represented as being true and correct. Please know that the Commonwealth shall treat any misstatement as fraudulent concealment of the true facts punishable as a crime under Section 4904 of the Pennsylvania Crime Code, Title 18, of Pa. Consolidation Statutes relating to unsworn falsification to authorities

Your verification is valid until the expiration date noted above. For additional information or assistance, please contact Bureau staff at (717) 783-3119 or by email at ra-bsboverification@pa.gov. Best wishes in your business endeavors.

Sincerely,

[redacted]

DeShawn A. Lewis, Director
Bureau of Small Business Opportunities (BSBO)

Bureau of Small Business Opportunities
401 North Street | Room 611 | North Office Building | Harrisburg, PA 17120

1.2.1.11 PC Network, Inc.—BSBO Verification Letter

NOTICE OF SMALL BUSINESS SELF-CERTIFICATION

pennsylvania
DEPARTMENT OF GENERAL SERVICES

The Department is pleased to announce that

PC NETWORK INC

has successfully completed the Pennsylvania Department of General Services' process for self-certification as a small business under the Commonwealth's Small Business Procurement Initiative as established by Executive Order No. 2011-09, with the following designation:

BUSINESS TYPE(s): **Information Technology**

CERTIFICATION NUMBER: **116258-2012-10-S**

ISSUE DATE: **10/24/2012** EXPIRATION DATE: **10/24/2013**

[redacted]

Sheri Phillips, Secretary
Department of General Services
Commonwealth of Pennsylvania

1.2.1.12 Pierson Computing Connection, Inc.—BSBO Verification Letter

pennsylvania
DEPARTMENT OF GENERAL SERVICES

July 11, 2013

Debra Pierson
President
Pierson Computing Connection
10 Long Lane, Suite 100
Mechanicsburg, PA 17050

Certification Number: **154433-2012-07-S**
Expiration Date: **July 23, 2014**
Business Types: **Information Technology**

Dear Debra Pierson:

The Bureau of Small Business Opportunities has reviewed your request for verification along with your supporting documents. I am pleased to inform you that your company has been verified as a Woman Business Enterprise (WBE) based on your certifications with the Pennsylvania Unified Certification Program (UCP) and the Women's Business Enterprise National Council (WBENC) and your small business self-certification registration through the Small Business Procurement Initiative (SBPI). The Commonwealth now recognizes your company as a Small Diverse Business (WBE).

Please understand that the information that you provided for verification was represented as being true and correct. Please know that the Commonwealth shall treat any misstatement as fraudulent concealment of the true facts punishable as a crime under Section 4904 of the Pennsylvania Crime Code, Title 18, of Pa. Consolidation Statutes relating to unsworn falsification to authorities

Your verification is valid until the expiration date noted above. For additional information or assistance, please contact Bureau staff at (717) 783-3119 or by email at ra-bsboverification@pa.gov. Best wishes in your business endeavors.

Sincerely

[redacted]

DeShawn A. Lewis, Director
Bureau of Small Business Opportunities (BSBO)

Bureau of Small Business Opportunities
401 North Street | Room 611 | North Office Building | Harrisburg, PA 17120

1.2.1.13 Source IT Technologies—BSBO Verification Letter

NOTICE OF SMALL BUSINESS SELF-CERTIFICATION

pennsylvania
DEPARTMENT OF GENERAL SERVICES

The Department is pleased to announce that

SOURCE IT TECHNOLOGIES LLC

has successfully completed the Pennsylvania Department of General Services' process for self-certification as a small business under the Commonwealth's Small Business Procurement Initiative as established by Executive Order No. 2011-09, with the following designation:

BUSINESS TYPE(s): **Information Technology**

CERTIFICATION NUMBER: **408368-2013-09-SB**

ISSUE DATE: **09/09/2013** EXPIRATION DATE: **09/09/2014**

[redacted]

Sheri Phillips, Secretary
Department of General Services
Commonwealth of Pennsylvania

1.3 B – Small Diverse Business Participation

RFP	*Requirement*
II-9 B	*In addition to the above verification letter, the Offeror must include in the Small Diverse Business participation submittal of the proposal the following information:* *1. Offerors must include a numerical percentage which represents the total percentage of the work (as a percentage of the total amount paid to the Offeror under the contract) that the Offeror commits to paying to Small Diverse Businesses (SDBs) as subcontractors. To support its total percentage SDB subcontractor commitment, Offeror must also include:* *a) The percentage of each subcontract commitment to a Small Diverse Business.* *b) The name of each Small Diverse Business. The Offeror will not receive credit for stating that after the contract is awarded it will find a Small Diverse Business.* *c) The services or supplies each Small Diverse Business will provide, including the timeframe for providing the services or supplies.* *d) The location where each Small Diverse Business will perform services.* *e) The timeframe for each Small Diverse Business to provide or deliver the goods or services.* *f) A completed and signed letter of intent, in the format set forth in Appendix J - SDB Letter of Intent, for each Small Diverse Business.* *g) The name, address and telephone number of the primary contact person for each Small Diverse Business.* *2. The total percentages and each SDB subcontractor commitment will become contractual obligations once the contract is fully executed.* *3. The name and telephone number of the Offeror's project (contact) person for the Small Diverse Business information.*

Our partners were selected based on their experience in providing quality goods and services to Unisys and the Commonwealth. Each firm selected participated in a bidding process with the Unisys Procurement organization to ensure requirements were clearly communicated and the best value for the Commonwealth was obtained through a competitive RFP with our suppliers. The firms listed below were allocated a specific percentage of the Total Contract Value based upon Unisys' evaluation of their capabilities to supply quality IT resources, hardware products, and office facility leasing/administration.

1.3.1 Numerical Percentage of Work Performed by the Small Diverse Businesses

RFP	*Requirement*
II-9 B 1	*In addition to the above verification letter, the Offeror must include in the Small Diverse Business participation submittal of the proposal the following information:* *1. Offerors must include a numerical percentage which represents the total percentage of the work (as a percentage of the total amount paid to the Offeror under the contract) that the Offeror commits to paying to Small Diverse Businesses (SDBs) as subcontractors.*

Unisys commits to paying the selected Small Diverse Businesses (SDBs), as subcontractors and/or suppliers, a numerical total percentage of **29.95%** based on the percentage of the Total Contract Value that represents the total percentage of the total cost submitted in the Cost Volume.

1.3.1.1 (a) Percentage of Dollar Amount – Each Subcontract Commitment to Small Diverse Business

RFP	*Requirement*
II-9 B 1a	*To support its total percentage SDB subcontractor commitment, Offeror must also include:* *a) The percentage of each subcontract commitment to a Small Diverse Business.*

Small Diverse Business	Percentage Each SDB Subcontractor
Acclaim Systems, Inc.	0.67%
American Personnel Managers & Consultants, Inc.	0.67%
Atrion Corporation	3.32%
Credo Technology Solutions, Inc.	1.03%
Domino Technologies, Inc.	1.63%
E & E IT Consulting Services, Inc.	1.39%
Info-Matrix Corporation	4.57%
Innovative Business Concepts, Inc.	0.75%
Latus Capital Advisors Inc.	0.55%
Metropolitan Technology Services Group, LLC	7.50%
PC Network, Inc.	1.08%
Pierson Computing Connection, Inc.	5.25%
Source IT Technologies, LLC	1.54%
Total	**29.95%**

1.3.1.2 (b) Identified Small Diverse Business Entity

RFP	*Requirement*
II-9 B 1b	*To support its total percentage SDB subcontractor commitment, Offeror must also include:* *b) The name of each Small Diverse Business. The Offeror will not receive credit for stating that after the contract is awarded it will find a Small Diverse Business.*

1. Acclaim Systems, Inc.
2. American Personnel Managers & Consultant, Inc. (APMC)

3. Atrion Corporation
4. Credo Technology Solutions, Inc.
5. Domino Technologies, Inc.
6. E & E IT Consulting Services, Inc.
7. Info-Matrix Corporation
8. Innovative Business Concepts, Inc.
9. Latus Capital Advisors Inc.
10. Metropolitan Technology Services Group, LLC
11. PC Network, Inc.
12. Pierson Computing Connection, Inc.
13. Source IT Technologies, LLC

1.3.1.3 (c) Services or Supplies and Timeframe Provided By Each Small Diverse Business

RFP	*Requirement*
II-9 B 1c	*To support its total percentage SDB subcontractor commitment, Offeror must also include:* *c) The services or supplies each Small Diverse Business will provide, including the timeframe for providing the services or supplies.*

Small Diverse Business	Service or Supply	Timeframe
Acclaim Systems, Inc.	Technical services labor	Full contract term
American Personnel Managers & Consultants, Inc.	Technical services labor	Full contract term
Computer hardware and maintenance services	Computer hardware and maintenance services	Full contract term
Credo Technology Solutions, Inc.	Technical services labor	Full contract term
Domino Technologies, Inc.	Technical services labor	Full contract term
E & E IT Consulting Services, Inc.	Technical services labor	Full contract term
Info-Matrix Corporation	Technical services labor	Full contract term
Innovative Business Concepts, Inc.	Technical services labor Computer hardware and maintenance services	Full contract term
Latus Capital Advisors Inc.	Real estate and facility management services	Full contract term
Metropolitan Technology Services Group, LLC	Computer hardware and maintenance services	Full contract term
PC Network, Inc.	Technical services labor	Full contract term
Pierson Computing Connection, Inc.	Computer hardware and maintenance services	Full contract term
Source IT Technologies, LLC	Computer hardware and maintenance services	Full contract term

1.3.1.4 (d) Location Where Each Small Diverse Business Will Provide Services or Supplies

RFP	*Requirement*
II-9 B 1d	*To support its total percentage SDB subcontractor commitment, Offeror must also include:* *d) The location where each Small Diverse Business will perform services.*

Small Diverse Business	Services Location - Address
Acclaim Systems, Inc.	Harrisburg, PA
American Personnel Managers & Consultants, Inc.	Ashburn, VA, Harrisburg, PA
Atrion Corporation	Harrisburg, PA
Credo Technology Solutions, Inc.	Harrisburg, PA
Domino Technologies, Inc.	Harrisburg, PA
E & E IT Consulting Services, Inc.	Harrisburg, PA
Info-Matrix Corporation	Harrisburg, PA
Innovative Business Concepts, Inc.	Harrisburg, PA
Latus Capital Advisors Inc.	Harrisburg, PA
Metropolitan Technology Services Group, LLC	Harrisburg, PA
PC Network, Inc.	Harrisburg, PA
Pierson Computing Connection, Inc.	Harrisburg, PA
Source IT Technologies, LLC	Harrisburg, PA

1.3.1.5 (e) Timeframe for Each Small Diverse Business to Provide or Deliver Goods or Services

RFP	*Requirement*
II-9 B 1e	*To support its total percentage SDB subcontractor commitment, Offeror must also include:* *e) The timeframe for each Small Diverse Business to provide or deliver the goods or services..*

Small Diverse Business	Timeframe to Provide or Deliver
Acclaim Systems, Inc.	Full contract term
American Personnel Managers & Consultants, Inc.	Full contract term
Atrion Corporation	Full contract term
Credo Technology Solutions, Inc.	Full contract term
Domino Technologies, Inc.	Full contract term
E & E IT Consulting Services, Inc.	Full contract term
Info-Matrix Corporation	Full contract term

Small Diverse Business	Timeframe to Provide or Deliver
Innovative Business Concepts, Inc.	Full contract term
Latus Capital Advisors Inc.	Full contract term
Metropolitan Technology Services Group, LLC	Full contract term
PC Network, Inc.	Full contract term
Pierson Computing Connection, Inc.	Full contract term
Source IT Technologies, LLC	Full contract term

1.3.1.6 (f) Letters of Intent

RFP	*Requirement*
II-9 B 1f	*To support its total percentage SDB subcontractor commitment, Offeror must also include:* *f) A completed and signed letter of intent, in the format set forth in Appendix J - SDB Letter of Intent, for each Small Diverse Business.*

Unisys has included Letters of Intent for each Small Diverse Business that identifies the specific work, goods or services to be performed and how this effort relates to the project.

Small Diverse Business Letters of Intent are included in the following pages for these partner firms:

1. Acclaim Systems, Inc.
2. American Personnel Managers & Consultants, Inc. (APMC)
3. Atrion Corporation
4. Credo Technology Solutions, Inc.
5. Domino Technologies, Inc.
6. E & E IT Consulting Services, Inc.
7. Info-Matrix Corporation
8. Innovative Business Concepts, Inc.
9. Latus Capital Advisors, Inc.
10. Metropolitan Technology Services Group LLC
11. PC Network, Inc.
12. Pierson Computing Connection, Inc.
13. Source IT Technologies, LLC

Technology Solutions to Support Your Enterprise

acclaim SYSTEMS
SOFTWARE SOLUTIONS PARTNER

September 12, 2013

Rakesh Khetawat
Director
Acclaim Systems Inc.
110 E Pennsylvania Blvd.
Feasterville, PA 19053

Dear Mr. Khetawat:

This letter serves as confirmation of the intent of Unisys Corporation to utilize Acclaim Systems Inc. on RFP 6100022698 (Data Center Computing Services) issued by the Commonwealth of Pennsylvania Office of Administration/Office for Technology.

If Unisys Corporation is the successful vendor, Acclaim Systems shall provide technical services labor for the duration of the contract term and renewal periods.

These services represent 0.67 % of the total amount Unisys Corporation will be paid under the initial term of the contract. The dollar value that the fixed percentage commitment represents will depend on the final negotiated contract pricing and actual contract usage or volume.

Acclaim Systems represents that it meets the small diverse business requirements set forth in the RFP and all required documentation has been provided to Unisys Corporation for its SDB submission.

We look forward to the opportunity to serve the Office of Administration/Office for Technology on this project. If you have any questions concerning our small diverse business commitment, please feel free to contact me at the number below.

Sincerely,

[redacted]

Beth Derr
Procurement Manager
Unisys Corporation
215-986-6552

Acknowledged,

[redacted]

Rakesh Khetawat
Director
Acclaim Systems Inc.
215-354-1422

September 12, 2013

Patricia M. Gingrich
President/CEO
American Personnel Managers & Consultants, Inc. (APMC)
2226 Gettysburg Road
Camp Hill, PA 17011

Dear Ms. Gingrich:

This letter serves as confirmation of the intent of Unisys Corporation to utilize American Personnel Managers & Consultants, Inc. (APMC) on RFP 6100022698 (Data Center Computing Services) issued by the Commonwealth of Pennsylvania Office of Administration/Office for Technology.

If Unisys Corporation is the successful vendor, APMC shall provide technical services labor and computer products and maintenance for the duration of the contract term and the renewal periods.

These services represent 0.67% of the total amount Unisys Corporation will be paid under the initial term of the contract. The dollar value that the fixed percentage commitment represents will depend on the final negotiated contract pricing and actual contract usage or volume.

APMC represents that it meets the small diverse business requirements set forth in the RFP and all required documentation has been provided to Unisys Corporation for its SDB submission.

We look forward to the opportunity to serve the Office of Administration/Office for Technology on this project. If you have any questions concerning our small diverse business commitment, please feel free to contact me at the number below.

Sincerely,

[redacted]

Beth Derr
Procurement Manager
Unisys Corporation
215-986-6552

Acknowledged,

[redacted]

Patricia M. Gingrich
President/CEO
American Personnel Managers and Consultants, Inc
717-303-0229

UNISYS

September 12, 2013

Richard Dietz
General Manager
Atrion Communication Resources
185 Industrial Parkway
Branchburg, NJ 08876

Dear Mr. Dietz:

This letter serves as confirmation of the intent of Unisys Corporation to utilize Atrion Communication Resources on RFP 6100022698 (Data Center Computing Services) issued by the Commonwealth of Pennsylvania Office of Administration/Office for Technology.

If Unisys Corporation is the successful vendor, Atrion Communication Resources shall provide Computer products and maintenance for the duration of the contract term and renewal periods.

These services represent 3.32% of the total amount Unisys Corporation will be paid under the initial term of the contract. The dollar value that the fixed percentage commitment represents will depend on the final negotiated contract pricing and actual contract usage or volume.

Atrion Communication Resources represents that it meets the small diverse business requirements set forth in the RFP and all required documentation has been provided to Unisys Corporation for its SDB submission.

We look forward to the opportunity to serve the Office of Administration/Office for Technology on this project. If you have any questions concerning our small diverse business commitment, please feel free to contact me at the number below.

Sincerely,

[redacted]

Beth Derr
Procurement Manager
Unisys Corporation
215-986-6552

Acknowledged,

[redacted]

Richard Dietz
General Manager
Atrion Communication Resources
908-231-7777 Ext 118

UNISYS

September 12, 2013

Jogendra Daita
President & CEO
Credo Technology Solutions, Inc.
110 Sunset Ave.
Harrisburg, PA 17112

Dear Mr. Daita:

This letter serves as confirmation of the intent of Unisys Corporation to utilize Credo Technology Solutions, Inc. on RFP 6100022698 (Data Center Computing Services) issued by the Commonwealth of Pennsylvania Office of Administration/Office for Technology.

If Unisys Corporation is the successful vendor, Credo Technology Solutions shall provide Technical Services Labor for the duration of the contract term and the renewal periods.

These services represent 1.03% of the total amount Unisys Corporation will be paid under the initial term of the contract. The dollar value that the fixed percentage commitment represents will depend on the final negotiated contract pricing and actual contract usage or volume.

Credo Technology Solutions represents that it meets the small diverse business requirements set forth in the RFP and all required documentation has been provided to Unisys Corporation for its SDB submission.

We look forward to the opportunity to serve the Office of Administration/Office for Technology on this project. If you have any questions concerning our small diverse business commitment, please feel free to contact me at the number below.

Sincerely,

[redacted]

Beth Derr
Procurement Manager
Unisys Corporation
215-986-6552

Acknowledged

[redacted]

Jogendra Daita
President & CEO
Credo Technology Solutions, Inc.
717-540-9730

September 12, 2013

Nathan Balagopal
President
Domino Technologies, Inc.
Governor's Plaza South
2001 N. Front Street, Suite 334
Harrisburg, PA 17102

Dear Mr. Balagopal:

This letter serves as confirmation of the intent of Unisys Corporation to utilize Domino Technologies, Inc. on RFP 6100022698 (Data Center Computing Services) issued by the Commonwealth of Pennsylvania Office of Administration/Office for Technology.

If Unisys Corporation is the successful vendor, Domino Technologies shall provide Technical Services Labor for the duration of the contract term and the renewal periods.

These services represent 1.63% of the total amount Unisys Corporation will be paid under the initial term of the contract. The dollar value that the fixed percentage commitment represents will depend on the final negotiated contract pricing and actual contract usage or volume.

Domino Technologies represents that it meets the small diverse business requirements set forth in the RFP and all required documentation has been provided to Unisys Corporation for its SDB submission.

We look forward to the opportunity to serve the Office of Administration/Office for Technology on this project. If you have any questions concerning our small diverse business commitment, please feel free to contact me at the number below.

Sincerely,

[redacted]

Beth Derr
Procurement Manager
Unisys Corporation
215-986-6552

Acknowledged,

[redacted]

Nathan Balagopal
President
Domino Technologies, Inc.
717-579-1601

September 12, 2013

Linda K. Etter
President
E & E IT Consulting Services, Inc.
5026 Arthur Avenue
Mechanicsburg, PA 17050

Dear Ms. Etter:

This letter serves as confirmation of the intent of Unisys Corporation to utilize E & E IT Consulting Services, Inc. on RFP 6100022698 (Data Center Computing Services) issued by the Commonwealth of Pennsylvania Office of Administration/Office for Technology.

If Unisys Corporation is the successful vendor, E & E IT Consulting Services shall provide Technical services labor for the duration of the contract term and renewal periods.

These services represent 1.39% of the total amount Unisys Corporation will be paid under the initial term of the contract. The dollar value that the fixed percentage commitment represents will depend on the final negotiated contract pricing and actual contract usage or volume.

E & E IT Consulting Services represents that it meets the small diverse business requirements set forth in the RFP and all required documentation has been provided to Unisys Corporation for its SDB submission.

We look forward to the opportunity to serve the Office of Administration/Office for Technology on this project. If you have any questions concerning our small diverse business commitment, please feel free to contact me at the number below.

Sincerely,

[redacted]

Beth Derr
Procurement Manager
Unisys Corporation
215-986-6552

Acknowledged,

[redacted]

Linda K. Etter
President
E & E IT Consulting Services, Inc.
717-975-1664

September 12, 2013

Brenda S. Orth
President/CEO
Info-Matrix Corp.
650 North 12th Street
Lemoyne, PA 17043

Dear Ms. Orth:

This letter serves as confirmation of the intent of Unisys Corporation to utilize Info-Matrix Corp. on RFP 6100022698 (Data Center Computing Services) issued by the Commonwealth of Pennsylvania Office of Administration/Office for Technology.

If Unisys Corporation is the successful vendor, Info-Matrix shall provide technical services labor and computer products and maintenance for the duration of the contract term and renewal periods.

These services represent 4.57% of the total amount Unisys Corporation will be paid under the initial term of the contract. The dollar value that the fixed percentage commitment represents will depend on the final negotiated contract pricing and actual contract usage or volume.

Info-Matrix represents that it meets the small diverse business requirements set forth in the RFP and all required documentation has been provided to Unisys Corporation for its SDB submission.

We look forward to the opportunity to serve the Office of Administration/Office for Technology on this project. If you have any questions concerning our small diverse business commitment, please feel free to contact me at the number below.

Sincerely,

[redacted]

Beth Derr
Procurement Manager
Unisys Corporation
215-986-6552

Acknowledged,

[redacted]

Brenda S. Orth
President/CEO
Info-Matrix Corp.
717-260-9850

September 12, 2013

Jennifer Briggs
President
Innovative Business Concepts, Inc.
209 Hamilton Street
Harrisburg, PA 17102

Dear Ms. Briggs:

This letter serves as confirmation of the intent of Unisys Corporation to utilize Innovative Business Concepts, Inc. on RFP 6100022698 (Data Center Computing Services) issued by the Commonwealth of Pennsylvania Office of Administration/Office for Technology.

If Unisys Corporation is the successful vendor, Innovative Business Concepts shall provide technical services labor and computer products and maintenance for the duration of the contract term and renewal periods.

These services represent 0.75% of the total amount Unisys Corporation will be paid under the initial term of the contract. The dollar value that the fixed percentage commitment represents will depend on the final negotiated contract pricing and actual contract usage or volume.

Innovative Business Concepts represents that it meets the small diverse business requirements set forth in the RFP and all required documentation has been provided to Unisys Corporation for its SDB submission.

We look forward to the opportunity to serve the Office of Administration/Office for Technology on this project. If you have any questions concerning our small diverse business commitment, please feel free to contact me at the number below.

Sincerely,

[redacted]

Beth Derr
Procurement Manager
Unisys Corporation
215-986-6552

Acknowledged:

[redacted]

Jennifer Briggs
President
Innovative Business Concepts, Inc.
717-221-1125

UNISYS

September 12, 2013

Laura Martin
CPM/Broker/Owner
Latus Capital Advisors Inc.
1100 Bent Creek Blvd., 2nd Floor
Mechanicsburg, PA 17050

Dear Ms. Martin:

This letter serves as confirmation of the intent of Unisys Corporation to utilize Latus Capital Advisors Inc. on RFP 6100022698 (Data Center Computing Services) issued by the Commonwealth of Pennsylvania Office of Administration/Office for Technology.

If Unisys Corporation is the successful vendor, Latus Capital Advisors Inc. shall provide Real estate and facility management services for the duration of the contract term and the renewal periods.

These services represent 0.55% of the total amount Unisys Corporation will be paid under the initial term of the contract. The dollar value that the fixed percentage commitment represents will depend on the final negotiated contract pricing and actual contract usage or volume.

Latus Capital Advisors Inc. represents that it meets the small diverse business requirements set forth in the RFP and all required documentation has been provided to Unisys Corporation for its SDB submission.

We look forward to the opportunity to serve the Office of Administration/Office for Technology on this project. If you have any questions concerning our small diverse business commitment, please feel free to contact me at the number below.

Sincerely,

[redacted]

Beth Derr
Procurement Manager
Unisys Corporation
215-986-6552

Acknowledged,

[redacted]

Laura Martin
CPM/Broker/Owner
Latus Capital Advisors Inc.
717-795-6102 - x101

UNISYS

September 12, 2013

Jim Cafferky
Account Executive
Metropolitan Technology Services Group LLC
4400 Route 9 South, Suite 1000
Freehold, NJ 07728

Dear Mr. Cafferky:

This letter serves as confirmation of the intent of Unisys Corporation to utilize Metropolitan Technology Services Group LLC on RFP 6100022698 (Data Center Computing Services) issued by the Commonwealth of Pennsylvania Office of Administration/Office for Technology.

If Unisys Corporation is the successful vendor, Metropolitan Technology Services Group LLC shall provide computer products and maintenance for the duration of the contract term and the renewal periods.

These services represent 7.50% of the total amount Unisys Corporation will be paid under the initial term of the contract. The dollar value that the fixed percentage commitment represents will depend on the final negotiated contract pricing and actual contract usage or volume.

Metropolitan Technology Services Group LLC represents that it meets the small diverse business requirements set forth in the RFP and all required documentation has been provided to Unisys Corporation for its SDB submission.

We look forward to the opportunity to serve the Office of Administration/Office for Technology on this project. If you have any questions concerning our small diverse business commitment, please feel free to contact me at the number below.

Sincerely,

[redacted]

Beth Derr
Procurement Manager
Unisys Corporation
215-986-6552

Acknowledged,

[redacted]

Jim Cafferky
Account Executive
Metropolitan Technology Services Group
732-786-1705

UNISYS

September 12, 2013

Katrin Hillner
President & CEO
PC Network Inc.
1315 Walnut Street, Suite 1402
Philadelphia, PA 19107

Dear Ms. Hillner:

This letter serves as confirmation of the intent of Unisys Corporation to utilize PC Network Inc. on RFP 6100022698 (Data Center Computing Services) issued by the Commonwealth of Pennsylvania Office of Administration/Office for Technology.

If Unisys Corporation is the successful vendor, PC Network shall provide Technical services labor for the duration of the contract term and renewal periods.

These services represent 1.08% of the total amount Unisys Corporation will be paid under the initial term of the contract. The dollar value that the fixed percentage commitment represents will depend on the final negotiated contract pricing and actual contract usage or volume.

PC Network represents that it meets the small diverse business requirements set forth in the RFP and all required documentation has been provided to Unisys Corporation for its SDB submission.

We look forward to the opportunity to serve the Office of Administration/Office for Technology on this project. If you have any questions concerning our small diverse business commitment, please feel free to contact me at the number below.

Sincerely,

[redacted]

Beth Deff
Procurement Manager
Unisys Corporation
215-986-6552

Acknowledged,

[redacted]

Katrin Hillner
President & CEO
PC Network Inc.
267-236-0152

UNISYS

September 13, 2013

Debra Pierson
President
Pierson Computing Connection, Inc.
10 Long Lane, Suite 103
Mechanicsburg, PA 17050

Dear Ms Pierson:

This letter serves as confirmation of the intent of Unisys Corporation to utilize Pierson Computing Connection, Inc. on RFP 6100022698 (Data Center Computing Services) issued by the Commonwealth of Pennsylvania Office of Administration/Office for Technology.

If Unisys Corporation is the successful vendor, Pierson Computing Connection shall provide computer products and maintenance for the duration of the contract term and the renewal periods.

These services represent 5.25 % of the total amount Unisys Corporation will be paid under the initial term of the contract. The dollar value that the fixed percentage commitment represents will depend on the final negotiated contract pricing and actual contract usage or volume.

Pierson Computing Connection represents that it meets the small diverse business requirements set forth in the RFP and all required documentation has been provided to Unisys Corporation for its SDB submission.

We look forward to the opportunity to serve the Office of Administration/Office for Technology on this project. If you have any questions concerning our small diverse business commitment, please feel free to contact me at the number below.

Sincerely,

[redacted]

Beth Derr
Procurement Manager
Unisys Corporation
215-986-6552

Acknowledged,

[redacted]

Debra Pierson
President
Pierson Computing Connection, Inc.
717-796-0493

UNISYS

September 12, 2013

John F. Homan
Vice President of Sales
Source IT Technologies, LLC
24 East Avenue, Suite 244
New Canaan, CT 06840

Dear Mr. Homan:

This letter serves as confirmation of the intent of Unisys Corporation to utilize Source IT Technologies, LLC on RFP 6100022698 (Data Center Computing Services) issued by the Commonwealth of Pennsylvania Office of Administration/Office for Technology.

If Unisys Corporation is the successful vendor, Source IT Technologies, LLC shall provide computer products and maintenance for the duration of the contract term and renewal periods.

These services represent 154% of the total amount Unisys Corporation will be paid under the initial term of the contract. The dollar value that the fixed percentage commitment represents will depend on the final negotiated contract pricing and actual contract usage or volume.

Source IT Technologies, LLC represents that it meets the small diverse business requirements set forth in the RFP and all required documentation has been provided to Unisys Corporation for its SDB submission.

We look forward to the opportunity to serve the Office of Administration/Office for Technology on this project. If you have any questions concerning our small diverse business commitment, please feel free to contact me at the number below.

Sincerely,

[redacted]

Beth Derr
Procurement Manager
Unisys Corporation
215-986-6552

Acknowledged,

[redacted]

John F. Homan
Vice President of Sales
Source IT Technologies, LLC
203-252-0410

1.3.1.7 (g) Small Diverse Businesses – Primary Person Contact Information

RFP	*Requirement*
II-9 B 1g	*To support its total percentage SDB subcontractor commitment, Offeror must also include:* *g) The name, address and telephone number of the primary contact person for each Small Diverse Business.*

Small Diverse Business	Primary SDB Contacts - Contact Information
Acclaim Systems, Inc.	[redacted] 110 E. Pennsylvania Blvd, Feasterville, PA 19053 **Phone:** 215-354-1422, **Fx:** 215-354-0488, **Email:** [redacted]@acclaimsystems.com
American Personnel Managers & Consultants, Inc.	[redacted] 2226, Gettysburg Road, Camp Hill, PA 17011 **Phone:** 717-303-0229, **Fx**: 717-737-4934, **Email:** [redacted]@aol.com
Atrion Communication Resources	[redacted] 185 Industrial Parkway, Branchburg, NJ 08876 **Phone:** 908-231-7777 Ext 118, **Email:** [redacted]@atrioncomm.com
Credo Technology Solutions, Inc.	[redacted], 110 Sunset Ave,Harrisburg,PA17112 **Phone:** 717.540.9730, **Email:** [redacted]@credotsinc.com
Domino Technologies, Inc.	[redacted] Governor's Plaza South, 2001 N. Front Street, Suite 334, Harrisburg, PA 17102 **Phone:** 717-579-1601, **Email:** [redacted]@dominotech.net
E & E IT Consulting Services, Inc.	[redacted] 5026 Arthur Avenue, Mechanicsburg, PA 17050 **Phone:** 717-975-1664, **Fx:** 717-975-1665, **Email:** [redacted]@ene-it-consulting.com
Info-Matrix Corporation	[redacted] 650 North 12th Street, Lemoyne, PA 17043 **Phone:** 717-260-9850, **Fx:** 717-260-9863, **Email:** [redacted]@info-matrix.com
Innovative Business Concepts, Inc.	[redacted] 209 Hamilton Street, Harrisburg, PA 17102 **Phone:** 717-221-1125, **Fx:** 717-774-3380, **Email:** [redacted]@innovative-bc.com
Latus Capital Advisors Inc.	[redacted] 1100 Bent Creek Blvd., 2nd Floor, Mechanicsburg, PA 17050 **Phone:** (O) 717-795-6102 - x101, (M) 717-919-7888, **Email:** lmartin@latusrealty.com
Metropolitan Technology Services Group LLC	[redacted] 22 Wagner Farm Lane, Millstone, NJ 08535 **Phone:** (O) 732-786-1705, (M) 732-616-4950, **Email:** [redacted]@metrotsg.com
PC Network, Inc.	[redacted] 1315 Walnut Street, Suite 1402, Philadelphia, PA 19107 **Phone:** (O) 267-236-0152, **Email:** [redacted]@pcn-inc.com
Pierson Computing Connection, Inc.	[redacted] 10 Long Lane, Suite 100, Mechanicsburg, PA 17050 PO Box 206, New Kingstown, PA 17072 **Phone:** 717-796-0493, **Email:** [redacted]piersoncci.com
Source IT Technologies	[redacted] 24 East Avenue, Suite 244, New Canaan, CT 06840 **Phone:** 203-252-0410, **Email:** [redacted]@sourceittech.com

1.3.1.8 Total Percentages and SDB Subcontractor Commitment Contractual Obligation

RFP	*Requirement*
II-9 B 2	*The total percentages and each SDB subcontractor commitment will become contractual obligations once the contract is fully executed.*

Unisys understands and agrees that the total percentage and each SDB subcontractor commitment as indicated in this submittal will become contractual obligations once the contract is fully executed.

1.3.1.9 Offeror's Project Person for Small Diverse Business information - Contact Information

RFP	*Requirement*
II-9 B 3	*The name and telephone number of the Offeror's project (contact) person for the Small Diverse Business information.*

Offeror's Project Person for SDB Information	Contact Information
Brian Maydick	[redacted]4750 Lindle Road, Harrisburg, PA 17111 **Phone: (O)** 717-526-1214, **(M)** 717-982-3098, **Email:** [redacted]@unisys.com

Request for Proposal

RFP # 6100022698

Commonwealth of Pennsylvania

Office of Administration
Office for Information Technology

Datacenter Computing Services

Schedule I

Offeror Pricing Forms

Description of Exhibit and Instructions

This Schedule I - Offeror Pricing Forms sets forth the following:

Configuration Definitions

- This tab contains the descriptions of the defined configurations which are used on the Volumetrics and Catalog of Services tabs.
- No entry is required on this tab.

1. Volumetrics

- This tab includes the resource unit categories and target quantities that the Offeror's will use to determine their price.
- Offerors should not assume that these are a guaranteed minimum units over the contract period.
- No entry is required on this tab.

2. Total Charges

- Summary of all Services Charges.
- No entry is required on this tab

3. Technical Staff Rate Card

- Offerors should use this tab to provide their staffing rates for the optional support services
- Offeror should only input in highlighted (yellow) cells.
- This rate card will become part of the service catalog at the Effective Date of the contract.

4. Catalog of Services

- Offerors should use this tab to include their Catalog of Services with pricing.
  See "Configuration Definitions" Tab for detail on what is included in each service catalog item.
- Offeror should only input in highlighted (yellow) cells.
- Only provide costs within the highlighted (yellow) cells; no additional services will be accepted here.
- All costs for services must be included in the item cost in the catalog of services. No additional costs should be incurred by the Commonwealth for the services requested by this RFP.

5. Software

- Offerors should use this tab to include their pricing of the required Third Party Software and Hybrid Third Party Software.
- Offeror should only input in highlighted (yellow) cells.
- Only provide costs within the highlighted (yellow) cells; no additional software products will be accepted here.
- Offerors should price software titles listed or equivalent.
- Offerors must provide a catalog of monthly single unit prices as part of its proposal. a single unit could be a single MIP, a single core, a single user, a single server, etc. The configuration will be determined as part of transition planning.
- Offerors are required to provide all of the listed software within this table. The Commonwealth will assume if there is no price indicated for a particular requested software item; that item will be provided at no cost to the Commonwealth.

6. Termination Fees

- This tab identifies the Termination for Convenience Fees.
- No entry is required on this tab.

Additional Notes

a.) All input tabs (3, 4, 5) should be filled out completely.

b.) Total Charges (tab 2): Information is linked with input tabs and will calculate automatically.

c.) Any cost field left blank will indicate the item will be available to the Commonwealth at no cost.

d.) Formulas are imbedded in all tabs. Offeror must verify that all calculations, subtotal costs and grand total costs are accurate.

e.) Please contact the Issuing Officer with any questions or concerns.

f.) Payment for services under this contract are unit-based. The total units (volumetrics) listed are for informational purposes only and will not be binding on the Commonwealth

g.) All Transition costs must be included in the service prices as included in the Catalog of Services tab over years 1 thru 7. Any change to transition plans shall not alter the costs as included in Offeror's completed Schedule I - Offeror Pricing Form. No additional costs will be incurred by the Commonwealth for changes to Offeror's proposed Transition Plan.

h.) All DC architecture costs must be included in the service prices as included in the Catalog of Services tab over years 1 thru 7.

i.) All pricing must not include any assumptions of a minimum commitment for services from the Commonwealth.

j.) Offerors must include in the base unit pricing for all configurations the components and services required to meet the security requirements of the RFP for all compute services, to include but not limited to Schedule F Sections 3.2.4.6 and 3.2.2.5.

Configuration Definitions (**)

The below definitions and configurations are referenced throughout Schedule I - Offeror Pricing Forms.

(1) Fully Managed and (2) Managed Only

Servers and Storage Services (x86, p-Series, i-Series)

Servers and Storage services should include the server, disk and backup devices, as well as hardware supplies; software, including operating and data management systems; the facilities, including raised floor and office space; and facilities management.

Unit Prices should include all services costs associated with providing, managing, operating, and transitioning to each technology unit per the RFP requirements Schedule F COPA Datacenter Statement of Work;

3.1	Establish Datacenter Architecture
3.1.1	Multi Datacenter Environment (2+ Architecture)
3.1.2	Network and Security Architecture
3.1.3	Datacenter Architecture and Technology
3.2	Enable Common Service Portfolio
3.2.1	Program & Service Management
3.2.1.1	PMO & Contract Management
3.2.1.2	Availability/SLA Management
3.2.1.3	Change & Release Management
3.2.1.4	Service Desk
3.2.1.5	Technical Architecture
3.2.1.6	Account Management
3.2.1.7	Configuration Management
3.2.1.8	3rd Party License Management
3.2.2	Technical Services
3.2.2.1	Transition Management (New Customer and/or Services)
3.2.2.2	Infrastructure Architecture
3.2.2.3	Capacity Management
3.2.2.4	DR Planning & Testing
3.2.2.5	Security Management
3.2.2.6	Performance Monitoring & Management
3.2.3	Facilities Management
3.2.3.1	Facilities Architecture / Maintenance
3.2.3.2	Site Operations
3.2.4	Managed Hosting Services
3.2.4.1	Windows Support
3.2.4.2	Storage Management
3.2.4.3	ERP Hosting – SAP / Oracle
3.2.4.4	UNIX Support – AIX / Linux
3.2.4.6	Security & Firewall
3.3	Transition Services
3.3.1	Transition Services – Guiding Principals
3.3.2	Transition Planning/Governance
3.3.2.1	Transition Program Management
3.3.2.2	Security Transition Activities

Fully Managed Infrastructure is fully owned and managed by the Offeror

Managed Only Infrastructure is managed by the Service Provider but owned by the Commonwealth and/or a 3rd Party

(3) Limited Co-Lo

Limited Co-Lo is infrastructure that is located in the Service Provider managed datacenter(s). Either owned or managed by the Commonwealth; or 3rd Party.

Limited Co-Lo Services Unit Prices should include all services costs associated with providing, managing, and transitioning to each technology unit per the RFP requirements Schedule F COPA Datacenter Statement of Work Unit Prices should include all services costs associated with providing, managing, operation, and transitioning to each technology unit per the RFP requirements Schedule F COPA Datacenter Statement of Work;

3.1	Establish Datacenter Architecture
3.1.1	Multi Datacenter Environment (2+ Architecture)
3.1.2	Network and Security Architecture
3.1.3	Datacenter Architecture and Technology
3.2	Enable Common Service Portfolio
3.2.1	Program & Service Management
3.2.1.1	PMO & Contract Management
3.2.1.2	Availability/SLA Management
3.2.1.3	Change & Release Management
3.2.1.4	Service Desk
3.2.1.5	Technical Architecture

Configuration Definitions (**)

3.2.1.6 Account Management
3.2.1.7 Configuration Management
3.2.1.8 3rd Party License Management
3.2.2 Technical Services
3.2.2.1 Transition Management (New Customer and/or Services)
3.2.2.2 Infrastructure Architecture
3.2.2.3 Capacity Management
3.2.2.4 DR Planning & Testing
3.2.2.5 Security Management
3.2.2.6 Performance Monitoring & Management
3.2.3 Facilities Management
3.2.3.1 Facilities Architecture / Maintenance
3.2.3.2 Site Operations
3.2.4 Managed Hosting Services
3.2.4.8 Limited-Use Colocation Services
3.3 Transition Services
3.3.1 Transition Services – Guiding Principals
3.3.2 Transition Planning/Governance
3.3.2.1 Transition Program Management
3.3.2.2 Security Transition Activities

(4) Mainframe Services - Include both IBM and Unisys Mainframe services

Mainframe services should include the hardware for the mainframe processing units; disk and backup devices, as well as hardware supplies; software, including operating and data management systems; the facilities, including raised floor and office space; and facilities management in addition to the services described below.

Mainframe Services Unit Prices should include all services costs associated with providing, managing, operating, and transitioning to each technology unit per the RFP requirements Schedule F COPA Datacenter Statement of Work;

3.1 Establish Datacenter Architecture
3.1.1 Multi Datacenter Environment (2+ Architecture)
3.1.2 Network and Security Architecture
3.1.3 Datacenter Architecture and Technology
3.2 Enable Common Service Portfolio
3.2.1 Program & Service Management
3.2.1.1 PMO & Contract Management
3.2.1.2 Availability/SLA Management
3.2.1.3 Change & Release Management
3.2.1.4 Service Desk
3.2.1.5 Technical Architecture
3.2.1.6 Account Management
3.2.1.7 Configuration Management
3.2.1.8 3rd Party License Management
3.2.2 Technical Services
3.2.2.1 Transition Management (New Customer and/or Services)
3.2.2.2 Infrastructure Architecture
3.2.2.3 Capacity Management
3.2.2.4 DR Planning & Testing
3.2.2.5 Security Management
3.2.2.6 Performance Monitoring & Management
3.2.3 Facilities Management
3.2.3.1 Facilities Architecture / Maintenance
3.2.3.2 Site Operations
3.2.4 Managed Hosting Services
3.2.4.2 Storage Management
3.2.4.5 Mainframe Services
3.2.4.6 Security & Firewall
3.3 Transition Services
3.3.1 Transition Services – Guiding Principals
3.3.2 Transition Planning/Governance
3.3.2.1 Transition Program Management
3.3.2.2 Security Transition Activities

Offerors must also use exhibit B1 DPH Asset List for configuration requirements for mainframe services.

(5) On-Demand (IaaS) Services

On-Demand Unit Prices should include all services costs associated with providing, managing, operating, and transitioning to each technology unit per the RFP requirements Schedule F COPA Datacenter Statement of Work;

3.1 Establish Datacenter Architecture
3.1.1 Multi Datacenter Environment (2+ Architecture)
3.1.2 Network and Security Architecture
3.1.3 Datacenter Architecture and Technology
3.2 Enable Common Service Portfolio

Configuration Definitions (**)

3.2.1	Program & Service Management
3.2.1.1	PMO & Contract Management
3.2.1.2	Availability/SLA Management
3.2.1.3	Change & Release Management
3.2.1.4	Service Desk
3.2.1.5	Technical Architecture
3.2.1.6	Account Management
3.2.1.7	Configuration Management
3.2.1.8	3rd Party License Management
3.2.2	Technical Services
3.2.2.1	Transition Management (New Customer and/or Services)
3.2.2.2	Infrastructure Architecture
3.2.2.3	Capacity Management
3.2.2.4	DR Planning & Testing
3.2.2.5	Security Management
3.2.2.6	Performance Monitoring & Management
3.2.3	Facilities Management
3.2.3.1	Facilities Architecture / Maintenance
3.2.3.2	Site Operations
3.2.5	Capacity on Demand Services
3.2.5.1	Server Capacity on Demand
3.2.5.2	Storage Capacity on Demand
3.2.5.3	DR Infrastructure on Demand
3.2.5.4	Additional Technical Services
3.3	Transition Services
3.3.1	Transition Services – Guiding Principals
3.3.2	Transition Planning/Governance

Configurations (**)

Limited Co-Lo (Data Center Only Charge)

Limited Co-Lo Configurations	Minimum Specifications	Unit
Co-Lo Config - 1	1/4 Rack Configuration includes: 10U Cabinet Space; 5,000 GB Network Bandwidth; 100Mb/s Uplink; 6 IP Addresses; 5 -110V AC Circuits	Monthly Per Config
Co-Lo Config - 2	1/2 Rack Configuration includes: 21U Cabinet Space; 10,000 GB Network Bandwidth; 100Mb/s Uplink; 14 IP Addresses; 10 -110V AC Circuits	Monthly Per Config
Co-Lo Config - 3	Full Rack Configuration includes: 42U Cabinet Space; 20,000 GB Network Bandwidth; 100Mb/s Uplink; 30 IP Addresses; 20 -110V AC Circuits	Monthly Per Config

Server Configurations (Fully Managed)

x86 Server Configurations	Minimum Specifications	Unit
Windows pConfig - 1	2-way Quad-Core 2.0 GHz; 4 GB RAM; Mirrored 146 15K Hard Drives; Windows Server 2008 R2	Physical Server
Windows pConfig - 2	2-way Six-Core 2.4 GHz; 16 GB RAM; Mirrored 146 15K Hard Drives; Windows Server 2008 R2	Physical Server
Windows pConfig - 3	4-way Six-Core 2.0 GHz; 64 GB RAM; 500 GB SAN Attached Storage; Windows Server 2008 R2	Physical Server

Configuration Definitions (**)

Windows pConfig - 4	2-way Six-Core 2.4 GHz; 16 GB RAM; Mirrored 146 15K Hard Drives; Windows Server 2008 R2; Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Physical Server
Windows pConfig - 5	2-way Six-Core 2.4 GHz; 16 GB RAM; Mirrored 146 15K Hard Drives; Windows Server 2008 R2; Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Physical Server
Linux pConfig - 1	2-way Quad-Core 2.0 GHz; 4 GB RAM; Mirrored 146 15K Hard Drives; RedHat or SUSE	Physical Server
Linux pConfig - 2	2-way Six-Core 2.4 GHz; 16 GB RAM; Mirrored 146 15K Hard Drives; RedHat or SUSE	Physical Server
Linux pConfig - 3	4-way Six-Core 2.0 GHz; 64 GB RAM; 500 GB SAN Attached Storage; RedHat or SUSE	Physical Server
Linux pConfig - 4	2-way Six-Core 2.4 GHz; 16 GB RAM; Mirrored 146 15K Hard Drives; RedHat or SUSE; Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Physical Server
Linux pConfig - 5	2-way Six-Core 2.4 GHz; 16 GB RAM; Mirrored 146 15K Hard Drives; RedHat or SUSE; Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Physical Server
Windows vConfig - 1	2vCPU; 4 GB Ram; Windows Server 2008 R2; ~~Firewall/IDS; Site-Site VPN; VPN Client; VLAN~~	Virtual Server Instance
Windows vConfig - 2	4vCPU; 16 GB Ram; Windows Server 2008 R2;~~Firewall/IDS; Site-Site VPN; VPN Client; VLAN~~	Virtual Server Instance
Windows vConfig - 3	8vCPU; 64 GB Ram; Windows Server 2008 R2; ~~Firewall/IDS; Site-Site VPN; VPN Client; VLAN~~	Virtual Server Instance
Windows vConfig - 4	4vCPU; 16 GB Ram; Windows Server 2008 R2; ~~Firewall/IDS; Site-Site VPN; VPN Client; VLAN~~; Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Virtual Server Instance

Configuration Definitions (**)

Windows vConfig - 5	4vCPU; 16 GB Ram; Windows Server 2008 R2; ~~Firewall/IDS; Site-Site VPN; VPN Client; VLAN~~; Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Virtual Server Instance
Linux vConfig - 1	2vCPU; 4 GB Ram; RedHat or SUSE; ~~Firewall/IDS; Site-Site VPN; VPN Client; VLAN~~	Virtual Server Instance
Linux vConfig - 2	4vCPU; 16 GB Ram; RedHat or SUSE; ~~Firewall/IDS; Site-Site VPN; VPN Client; VLAN~~	Virtual Server Instance
Linux vConfig - 3	8vCPU; 64 GB Ram; RedHat or SUSE; ~~Firewall/IDS; Site-Site VPN; VPN Client; VLAN~~	Virtual Server Instance
Linux vConfig - 4	4vCPU; 16 GB Ram; RedHat or SUSE; ~~Firewall/IDS; Site-Site VPN; VPN Client; VLAN;~~ Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Virtual Server Instance
Linux vConfig - 5	4vCPU; 16 GB Ram; RedHat or SUSE; ~~Firewall/IDS; Site-Site VPN; VPN Client; VLAN;~~ Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Virtual Server Instance

P-Series Server Configurations		
AIX Config - 1	3.0GHz POWER7; 0.5 Cores; 6 GB RAM; AIX	LPAR
AIX Config - 2	3.0GHz POWER7; 1.0 Cores; 12 GB RAM; AIX	LPAR
AIX Config - 3	3.0GHz POWER7; 1.5 Cores; 18 GB RAM; AIX	LPAR
AIX Config - 4	3.0GHz POWER7; 1.0 Cores; 12 GB RAM; AIX; Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	LPAR
AIX Config - 5	3.0GHz POWER7; 1.0 Cores; 12 GB RAM; AIX; Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	LPAR

Mainframe Configurations (*)		
IBM Mainframe Configurations	**Minimum Specifications**	**Unit**
IBM Mainframe Config - 1	IBM System zEnterprise Processor z/OS	MIP
IBM Mainframe Config - 2	IBM System zEnterprise Processor Virtual Linux Prod IFL	MIP

Configuration Definitions (**)

IBM Mainframe Config - 3	IBM System zEnterprise Processor Virtual Linux Prod IFL; Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	MIP
IBM AS400 Config 1	IBM i Series / AS400	CPW
IBM AS400 Config 2	IBM i Series / AS400; Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	CPW
Unisys Mainframe Configurations	**Minimum Specifications**	**Unit**
Unisys Mainframe Config - 1	Unisys (Clearpath / Dorado)	MIP
Unisys Mainframe Config - 2	Unisys (Clearpath / Libra)	MIP
Unisys Mainframe Config - 3	Unisys (Clearpath / Dorado); Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	MIP
Unisys Mainframe Config - 4	Unisys (Clearpath / Libra) ; Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	MIP

On-Demand (IaaS) Configurations		
IaaS x86 Server Configurations	**Minimum Specifications**	**Unit (per month)**
IaaS Windows vConfig - 1	2vCPU; 4 GB Ram; Windows Server 2008 R2; ~~Firewall/IDS; Site-Site VPN; VPN Client; VLAN~~	Virtual Server Instance
IaaS Windows vConfig - 2	4vCPU; 16 GB Ram; Windows Server 2008 R2; ~~Firewall/IDS; Site-Site VPN; VPN Client; VLAN~~	Virtual Server Instance
IaaS Windows vConfig - 3	8vCPU; 64 GB Ram; Windows Server 2008 R2; ~~Firewall/IDS; Site-Site VPN; VPN Client; VLAN~~	Virtual Server Instance
IaaS Windows vConfig - 4	4vCPU; 16 GB Ram; Windows Server 2008 R2; ~~Firewall/IDS; Site-Site VPN; VPN Client; VLAN;~~ Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Virtual Server Instance
IaaS Windows vConfig - 5	4vCPU; 16 GB Ram; Windows Server 2008 R2; ~~Firewall/IDS; Site-Site VPN; VPN Client; VLAN;~~ Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Virtual Server Instance
IaaS Linux vConfig - 1	2vCPU; 4 GB Ram; RedHat or SUSE; ~~Firewall/IDS; Site-Site VPN; VPN Client; VLAN~~	Virtual Server Instance

Configuration Definitions (**)

IaaS Linux vConfig - 2	4vCPU; 16 GB Ram; RedHat or SUSE; ~~Firewall/IDS; Site-Site VPN; VPN Client; VLAN~~	Virtual Server Instance
IaaS Linux vConfig - 3	8vCPU; 64 GB Ram; RedHat or SUSE; ~~Firewall/IDS; Site-Site VPN; VPN Client; VLAN~~	Virtual Server Instance
IaaS Linux vConfig - 4	4vCPU; 16 GB Ram; RedHat or SUSE; ~~Firewall/IDS; Site-Site VPN; VPN Client; VLAN;~~ Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Virtual Server Instance
IaaS Linux vConfig - 5	4vCPU; 16 GB Ram; RedHat or SUSE; ~~Firewall/IDS; Site-Site VPN; VPN Client; VLAN;~~ Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Virtual Server Instance
IaaS Storage Configurations		
IaaS Storage Config - 1	SAN attached storage; Raid 5; 10K - 15K RPM discs	Monthly per GB
IaaS Storage Config - 2	SAN attached storage; Raid 10; 10K - 15K RPM discs	Monthly per GB
IaaS Storage Config - 3	Network Attached Storage	Monthly per GB

IaaS Backup Configurations		
IaaS Backup Config - 1	Remote Offsite backup per GB	Monthly per GB

Notes:
(*) Offerors must use exhibit B1 DPH Asset List for configuration requirements for mainframe services.

Baseline Units - Volumetrics

Note: The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all inclusive representation of every service desired by the Commonwealth.

Resource Description	Service Tier / Configuration (6)	Units	Year 1 Qty	Year 2 Qty	Year 3 Qty	Year 4 Qty	Year 5 Qty	Year 6 Qty	Year 7 Qty	Opt - Year 8 Qty	Opt - Year 9 Qty	Opt - Year 10 Qty
Server - Fully Managed (1)												
x86 (Windows, Linux) - Physical Servers												
	Platinum Tier											
	Windows pConfig - 1	Server	27	26	24	23	22	21	20	19	18	17
	Windows pConfig - 2	Server	23	22	21	20	19	18	17	16	15	14
	Windows pConfig - 3	Server	14	13	13	12	11	11	10	10	9	9
	Windows pConfig - 4	Server	2	2	2	2	2	2	1	1	1	1
	Windows pConfig - 5	Server	2	2	2	2	2	2	1	1	1	1
	Linux pConfig - 1	Server	12	11	11	10	10	9	9	8	8	8
	Linux pConfig - 2	Server	8	8	7	7	7	6	6	6	5	5
	Linux pConfig - 3	Server	6	6	5	5	5	5	4	4	4	4
	Linux pConfig - 4	Server	2	2	2	2	2	2	1	1	1	1
	Linux pConfig - 5	Server	2	2	2	2	2	2	1	1	1	1
sub-total x86 (Windows, Linux) - Physical Servers - Plantinum			**98**	**94**	**89**	**85**	**82**	**78**	**70**	**67**	**63**	**61**
	Gold Tier											
	Windows pConfig - 1	Server	245	233	221	210	200	190	180	171	163	154
	Windows pConfig - 2	Server	209	199	189	179	170	162	154	146	139	132
	Windows pConfig - 3	Server	122	116	110	105	99	94	90	85	81	77
	Windows pConfig - 4	Server	18	17	16	15	15	14	13	13	12	11
	Windows pConfig - 5	Server	18	17	16	15	15	14	13	13	12	11
	Linux pConfig - 1	Server	108	103	97	93	88	84	79	75	72	68
	Linux pConfig - 2	Server	72	68	65	62	59	56	53	50	48	45
	Linux pConfig - 3	Server	54	51	49	46	44	42	40	38	36	34
	Linux pConfig - 4	Server	18	17	16	15	15	14	13	13	12	11
	Linux pConfig - 5	Server	18	17	16	15	15	14	13	13	12	11
sub-total x86 (Windows, Linux) - Physical Servers - Gold			**882**	**838**	**795**	**755**	**720**	**684**	**648**	**617**	**587**	**554**
	Silver Tier											
	Windows pConfig - 1	Server	272	258	245	233	222	210	200	190	180	189
	Windows pConfig - 2	Server	236	224	213	202	192	183	173	165	157	164
	Windows pConfig - 3	Server	136	129	123	117	111	105	100	95	90	95
	Windows pConfig - 4	Server	18	17	16	15	15	14	13	13	12	13
	Windows pConfig - 5	Server	18	17	16	15	15	14	13	13	12	13
	Linux pConfig - 1	Server	120	114	108	103	98	93	88	84	80	84
	Linux pConfig - 2	Server	120	114	108	103	98	93	88	84	80	84
	Linux pConfig - 3	Server	24	23	22	21	20	19	18	17	16	17
	Linux pConfig - 4	Server	18	17	16	15	15	14	13	13	12	13
	Linux pConfig - 5	Server	18	17	16	15	15	14	13	13	12	13
sub-total x86 (Windows, Linux) - Physical Servers - Silver			**980**	**930**	**883**	**839**	**801**	**759**	**719**	**687**	**651**	**685**
	Bronze Tier											
	Windows pConfig - 1	Server	120	114	108	103	98	93	88	84	80	76
	Windows pConfig - 2	Server	120	114	108	103	98	93	88	84	80	76
	Windows pConfig - 3	Server	47	45	42	40	38	36	35	33	31	30
	Windows pConfig - 4	Server	8	8	7	7	7	6	6	6	5	5
	Windows pConfig - 5	Server	3	3	3	3	2	2	2	2	2	2
	Linux pConfig - 1	Server	75	71	68	64	61	58	55	52	50	47
	Linux pConfig - 2	Server	75	71	68	64	61	58	55	52	50	47

Baseline Units - Volumetrics

Note: The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all inclusive representation of every service desired by the Commonwealth.

Resource Description	Service Tier / Configuration (6)	Units	Year 1 Qty	Year 2 Qty	Year 3 Qty	Year 4 Qty	Year 5 Qty	Year 6 Qty	Year 7 Qty	Opt - Year 8 Qty	Opt - Year 9 Qty	Opt - Year 10 Qty
	Linux pConfig - 3	Server	20	19	18	17	16	15	15	14	13	13
	Linux pConfig - 4	Server	4	4	4	3	3	3	3	3	3	3
	Linux pConfig - 5	Server	2	2	2	2	2	2	1	1	1	1
sub-total x86 (Windows, Linux) - Physical Servers - Bronze			**474**	**451**	**428**	**406**	**386**	**366**	**348**	**331**	**315**	**300**
	Basic Tier											
	Windows pConfig - 1	Server	240	228	217	206	195	186	176	168	159	151
	Windows pConfig - 2	Server	240	228	217	206	195	186	176	168	159	151
	Windows pConfig - 3	Server	110	105	99	94	90	85	81	77	73	69
	Windows pConfig - 4	Server	17	16	15	15	14	13	12	12	11	11
	Windows pConfig - 5	Server	7	7	6	6	6	5	5	5	5	4
	Linux pConfig - 1	Server	95	90	86	81	77	74	70	66	63	60
	Linux pConfig - 2	Server	95	90	86	81	77	74	70	66	63	60
	Linux pConfig - 3	Server	8	8	7	7	7	6	6	6	5	5
	Linux pConfig - 4	Server	9	9	8	8	7	7	7	6	6	6
	Linux pConfig - 5	Server	5	5	5	4	4	4	4	3	3	3
sub-total x86 (Windows, Linux) - Physical Servers - Basic			**826**	**786**	**746**	**708**	**672**	**640**	**607**	**577**	**547**	**520**
Total - Fully Managed - x86 Physical - All Support Tiers (Window, Linux)			**3,260**	**3,099**	**2,941**	**2,793**	**2,661**	**2,527**	**2,392**	**2,279**	**2,163**	**2,120**
x86 (Windows, Linux) - Virtual Servers												
	Platinum Tier											
	Windows vConfig - 1	Instance	28	29	31	32	34	36	38	39	41	43
	Windows vConfig - 2	Instance	23	24	25	27	28	29	31	32	34	36
	Windows vConfig - 3	Instance	14	15	15	16	17	18	19	20	21	22
	Windows vConfig - 4	Instance	3	3	3	3	4	4	4	4	4	5
	Windows vConfig - 5	Instance	2	2	2	2	2	3	3	3	3	3
	Linux vConfig - 1	Instance	12	13	13	14	15	15	16	17	18	19
	Linux vConfig - 2	Instance	10	11	11	12	12	13	13	14	15	16
	Linux vConfig - 3	Instance	6	6	7	7	7	8	8	8	9	9
	Linux vConfig - 4	Instance	2	2	2	2	2	3	3	3	3	3
	Linux vConfig - 5	Instance	1	1	1	1	1	1	1	1	1	2
sub-total x86 (Windows, Linux) - Virtual Servers - Platinum			**101**	**106**	**110**	**116**	**122**	**130**	**136**	**141**	**149**	**158**
	Gold Tier											
	Windows vConfig - 1	Instance	244	256	269	282	297	311	327	343	360	379
	Windows vConfig - 2	Instance	204	214	225	236	248	260	273	287	301	316
	Windows vConfig - 3	Instance	122	128	135	141	148	156	163	172	180	189
	Windows vConfig - 4	Instance	24	25	26	28	29	31	32	34	35	37
	Windows vConfig - 5	Instance	16	17	18	19	19	20	21	23	24	25
	Linux vConfig - 1	Instance	108	113	119	125	131	138	145	152	160	168
	Linux vConfig - 2	Instance	85	89	94	98	103	108	114	120	126	132
	Linux vConfig - 3	Instance	54	57	60	63	66	69	72	76	80	84
	Linux vConfig - 4	Instance	13	14	14	15	16	17	17	18	19	20
	Linux vConfig - 5	Instance	9	9	10	10	11	11	12	13	13	14
sub-total x86 (Windows, Linux) - Virtual Servers - Gold			**879**	**922**	**970**	**1017**	**1068**	**1121**	**1176**	**1238**	**1298**	**1364**
	Silver Tier											
	Windows vConfig - 1	Instance	272	286	300	315	331	347	365	383	402	422
	Windows vConfig - 2	Instance	232	244	256	269	282	296	311	326	343	360

Baseline Units - Volumetrics

Note: The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all inclusive representation of every service desired by the Commonwealth.

Resource Description	Service Tier / Configuration (6)	Units	Year 1 Qty	Year 2 Qty	Year 3 Qty	Year 4 Qty	Year 5 Qty	Year 6 Qty	Year 7 Qty	Opt - Year 8 Qty	Opt - Year 9 Qty	Opt - Year 10 Qty
	Windows vConfig - 3	Instance	136	143	150	157	165	174	182	191	201	211
	Windows vConfig - 4	Instance	24	25	26	28	29	31	32	34	35	37
	Windows vConfig - 5	Instance	16	17	18	19	19	20	21	23	24	25
	Linux vConfig - 1	Instance	120	126	132	139	146	153	161	169	177	186
	Linux vConfig - 2	Instance	98	103	108	113	119	125	131	138	145	152
	Linux vConfig - 3	Instance	60	63	66	69	73	77	80	84	89	93
	Linux vConfig - 4	Instance	13	14	14	15	16	17	17	18	19	20
	Linux vConfig - 5	Instance	9	9	10	10	11	11	12	13	13	14
sub-total x86 (Windows, Linux) - Virtual Servers - Silver			**980**	**1030**	**1080**	**1134**	**1191**	**1251**	**1312**	**1379**	**1448**	**1520**
	Bronze Tier											
	Windows vConfig - 1	Instance	91	96	100	105	111	116	122	128	134	141
	Windows vConfig - 2	Instance	91	96	100	105	111	116	122	128	134	141
	Windows vConfig - 3	Instance	44	46	49	51	53	56	59	62	65	68
	Windows vConfig - 4	Instance	1	1	1	1	1	1	1	1	1	2
	Windows vConfig - 5	Instance	1	1	1	1	1	1	1	1	1	2
	Linux vConfig - 1	Instance	38	40	42	44	46	48	51	53	56	59
	Linux vConfig - 2	Instance	38	40	42	44	46	48	51	53	56	59
	Linux vConfig - 3	Instance	18	19	20	21	22	23	24	25	27	28
	Linux vConfig - 4	Instance	1	1	1	1	1	1	1	1	1	2
	Linux vConfig - 5	Instance	1	1	1	1	1	1	1	1	1	2
sub-total x86 (Windows, Linux) - Virtual Servers - Bronze			**324**	**341**	**357**	**374**	**393**	**411**	**433**	**453**	**476**	**504**
	Basic Tier											
	Windows vConfig - 1	Instance	181	190	200	210	220	231	243	255	267	281
	Windows vConfig - 2	Instance	181	190	200	210	220	231	243	255	267	281
	Windows vConfig - 3	Instance	90	95	99	104	109	115	121	127	133	140
	Windows vConfig - 4	Instance	1	1	1	1	1	1	1	1	1	2
	Windows vConfig - 5	Instance	1	1	1	1	1	1	1	1	1	2
	Linux vConfig - 1	Instance	80	84	88	93	97	102	107	113	118	124
	Linux vConfig - 2	Instance	80	84	88	93	97	102	107	113	118	124
	Linux vConfig - 3	Instance	40	42	44	46	49	51	54	56	59	62
	Linux vConfig - 4	Instance	1	1	1	1	1	1	1	1	1	2
	Linux vConfig - 5	Instance	1	1	1	1	1	1	1	1	1	2
sub-total x86 (Windows, Linux) - Virtual Servers - Basic			**656**	**689**	**723**	**760**	**796**	**836**	**879**	**923**	**966**	**1020**
Total - Fully Managed - x86 Virtual - All Support Tiers (Window, Linux)			**2,940**	**3,088**	**3,240**	**3,401**	**3,570**	**3,749**	**3,936**	**4,134**	**4,337**	**4,566**
UNIX (IBM P-Series, AIX)												
	Platinum Tier											
	AIX Config - 1	LPAR	36	38	40	42	44	46	48	51	53	56
	AIX Config - 2	LPAR	26	27	29	30	32	33	35	37	38	40
	AIX Config - 3	LPAR	18	19	20	21	22	23	24	25	27	28
	AIX Config - 4	LPAR	5	5	6	6	6	6	7	7	7	8
	AIX Config - 5	LPAR	5	5	6	6	6	6	7	7	7	8
sub-total P-Series (AIX) - Bronze			**90**	**94**	**101**	**105**	**110**	**114**	**121**	**127**	**132**	**140**
	Gold Tier											
	AIX Config - 1	LPAR	36	38	40	42	44	46	48	51	53	56
	AIX Config - 2	LPAR	26	27	29	30	32	33	35	37	38	40

Baseline Units - Volumetrics

Note: The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all inclusive representation of every service desired by the Commonwealth.

Resource Description	Service Tier / Configuration (6)	Units	Year 1 Qty	Year 2 Qty	Year 3 Qty	Year 4 Qty	Year 5 Qty	Year 6 Qty	Year 7 Qty	Opt - Year 8 Qty	Opt - Year 9 Qty	Opt - Year 10 Qty
	AIX Config - 3	LPAR	18	19	20	21	22	23	24	25	27	28
	AIX Config - 4	LPAR	5	5	6	6	6	6	7	7	7	8
	AIX Config - 5	LPAR	5	5	6	6	6	6	7	7	7	8
sub-total P-Series (AIX) - Gold			**90**	**94**	**101**	**105**	**110**	**114**	**121**	**127**	**132**	**140**
	Silver Tier											
	AIX Config - 1	LPAR	72	76	79	83	88	92	96	101	106	112
	AIX Config - 2	LPAR	52	55	57	60	63	66	70	73	77	81
	AIX Config - 3	LPAR	36	38	40	42	44	46	48	51	53	56
	AIX Config - 4	LPAR	10	11	11	12	12	13	13	14	15	16
	AIX Config - 5	LPAR	10	11	11	12	12	13	13	14	15	16
sub-total P-Series (AIX) - Silver			**180**	**191**	**198**	**209**	**219**	**230**	**240**	**253**	**266**	**281**
	Bronze Tier											
	AIX Config - 1	LPAR	24	25	26	28	29	31	32	34	35	37
	AIX Config - 2	LPAR	24	25	26	28	29	31	32	34	35	37
	AIX Config - 3	LPAR	8	8	9	9	10	10	11	11	12	12
	AIX Config - 4	LPAR	2	2	2	2	2	3	3	3	3	3
	AIX Config - 5	LPAR	2	2	2	2	2	3	3	3	3	3
sub-total P-Series (AIX) - Bronze			**60**	**62**	**65**	**69**	**72**	**78**	**81**	**85**	**88**	**92**
	Basic Tier											
	AIX Config - 1	LPAR	64	67	71	74	78	82	86	90	95	99
	AIX Config - 2	LPAR	64	67	71	74	78	82	86	90	95	99
	AIX Config - 3	LPAR	32	34	35	37	39	41	43	45	47	50
	AIX Config - 4	LPAR	10	11	11	12	12	13	13	14	15	16
	AIX Config - 5	LPAR	10	11	11	12	12	13	13	14	15	16
sub-total P-Series (AIX) - Basic			**180**	**190**	**199**	**209**	**219**	**231**	**241**	**253**	**267**	**280**
Total - Fully Managed - P-Series (AIX) - All Support Tiers (Window, Linux)			**600**	**631**	**664**	**697**	**730**	**767**	**804**	**845**	**885**	**933**
Server - Managed Only (2)												
x86 (Windows, Linux)												
	Platinum Tier	Server/Instance	100	60	36	22	50	50	50	50	50	50
	Gold Tier	Server/Instance	900	540	324	194	50	50	50	50	50	50
	Silver Tier	Server/Instance	1000	600	360	216	50	50	50	50	50	50
	Bronze Tier	Server/Instance	750	450	270	162	50	50	50	50	50	50
	Basic Tier	Server/Instance	1050	630	378	227	50	50	50	50	50	50
Total Managed Only- x86 - All Support Tiers (Window, Linux)			**3,800**	**2,280**	**1,368**	**821**	**250**	**250**	**250**	**250**	**250**	**250**
UNIX (IBM P-Series, AIX)												
	Platinum	LPAR	5	3	2	10	10	10	10	10	10	10
	Gold Tier	LPAR	15	9	5	10	10	10	10	10	10	10
	Silver Tier	LPAR	30	18	11	10	10	10	10	10	10	10
	Bronze Tier	LPAR	40	24	14	10	10	10	10	10	10	10
	Basic Tier	LPAR	30	18	11	10	10	10	10	10	10	10
Total Managed Only- P-Series - All Support Tiers (AIX)			**120**	**72**	**43**	**50**	**50**	**50**	**50**	**50**	**50**	**50**
Storage and Backup - Fully Managed (1)												

Baseline Units - Volumetrics

Note: The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all inclusive representation of every service desired by the Commonwealth.

Resource Description	Service Tier / Configuration (6)	Units	Year 1 Qty	Year 2 Qty	Year 3 Qty	Year 4 Qty	Year 5 Qty	Year 6 Qty	Year 7 Qty	Opt - Year 8 Qty	Opt - Year 9 Qty	Opt - Year 10 Qty
Enterprise Storage												
	* Dedicated - Config 1 - SAN Raid 5	GB	2300000	2530000	2783000	3061300	3367430	3704173	4074590	4482049	4930254	5423280
	* Dedicated - Config 2 - SAN Raid 10	GB	400000	440000	484000	532400	585640	644204	708624	779487	857436	943179
	Dedicated - Config 3 - Net Attached	GB	10000	11000	12100	13310	14641	16105	17716	19487	21436	23579
Total Enterprise Storage - Fully Managed			**2,710,000**	**2,981,000**	**3,279,100**	**3,607,010**	**3,967,711**	**4,364,482**	**4,800,930**	**5,281,023**	**5,809,126**	**6,390,038**
Tape and Backup												
	** Server Tape Stored	GB Stored	2700000	2970000	3267000	3593700	3953070	4348377	4783215	5261536	5787690	6366459
	** Offsite Tape Storage	Tapes	5000	5500	6050	6655	7321	8053	8858	9744	10718	11790
Total Tape and Backup - Fully Managed			**2,705,000**	**2,975,500**	**3,273,050**	**3,600,355**	**3,960,391**	**4,356,430**	**4,792,073**	**5,271,280**	**5,798,408**	**6,378,249**

Limited Co-Lo (Data Center Only Charge) (3)												
Server, Storage, Network, Security Equipment												
	Co-Lo Config - 1	Per Config	20	20	20	20	20	20	20	20	20	20
	Co-Lo Config - 2	Per Config	20	20	20	20	20	20	20	20	20	20
	Co-Lo Config - 3	Per Config	80	80	80	80	40	40	40	40	40	40
Total Limited Co-Lo (Data Center Only Charge)			**120**	**120**	**120**	**120**	**80**	**80**	**80**	**80**	**80**	**80**

Mainframe Services (4)												
IBM Services												
	*** IBM Mainframe Allocated DASD	GB	100000	100000	100000	100000	100000	100000	100000	100000	100000	100000
	IBM Tapes in Storage - VTS	GB	100000	100000	100000	100000	100000	100000	100000	100000	100000	100000
	IBM Offsite Tape Storage	Tape/Reel	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000
Total IBM Services			**201,000**	**201,000**	**201,000**	**201,000**	**201,000**	**201,000**	**201,000**	**201,000**	**201,000**	**201,000**
IBM Configurations												
	Platinum Tier											
	IBM Mainframe Config - 1	MIP	1705	1705	1705	1705	1705	1705	1705	1705	1705	1705
	IBM Mainframe Config - 2	MIP	141	141	141	141	141	141	141	141	141	141
	IBM Mainframe Config - 3	MIP	330	330	330	330	330	330	330	330	330	330
	IBM AS400 Config 1	CPW	364	364	364	364	364	364	364	364	364	364
	IBM AS400 Config 2	CPW	1460	1460	1460	1460	1460	1460	1460	1460	1460	1460
sub-total IBM Mainfram Services - Plantinum			**4000**	**4000**	**4000**	**4000**	**4000**	**4000**	**4000**	**4000**	**4000**	**4000**
	Gold Tier											
	IBM Mainframe Config - 1	MIP	213	213	213	213	213	213	213	213	213	213
	IBM Mainframe Config - 2	MIP	18	18	18	18	18	18	18	18	18	18
	IBM Mainframe Config - 3	MIP	41	41	41	41	41	41	41	41	41	41
	IBM AS400 Config 1	CPW	46	46	46	46	46	46	46	46	46	46
	IBM AS400 Config 2	CPW	182	182	182	182	182	182	182	182	182	182
sub-total IBM Mainfram Services - Gold			**500**	**500**	**500**	**500**	**500**	**500**	**500**	**500**	**500**	**500**
	Basic Tier											
	IBM Mainframe Config - 1	MIP	213	213	213	213	213	213	213	213	213	213
	IBM Mainframe Config - 2	MIP	18	18	18	18	18	18	18	18	18	18
	IBM Mainframe Config - 3	MIP	41	41	41	41	41	41	41	41	41	41
	IBM AS400 Config 1	CPW	46	46	46	46	46	46	46	46	46	46
	IBM AS400 Config 2	CPW	182	182	182	182	182	182	182	182	182	182
sub-total IBM Mainfram Services - Basic			**500**	**500**	**500**	**500**	**500**	**500**	**500**	**500**	**500**	**500**

Baseline Units - Volumetrics

Note: The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all inclusive representation of every service desired by the Commonwealth.

Resource Description	Service Tier / Configuration (6)	Units	Year 1 Qty	Year 2 Qty	Year 3 Qty	Year 4 Qty	Year 5 Qty	Year 6 Qty	Year 7 Qty	Opt - Year 8 Qty	Opt - Year 9 Qty	Opt - Year 10 Qty
Total - IBM Mainframe Services - All Support Tiers			**5,000**	**5,000**	**5,000**	**5,000**	**5,000**	**5,000**	**5,000**	**5,000**	**5,000**	**5,000**
Unisys Services												
	*** Unisys DASD	GB	100000	100000	100000	100000	100000	100000	100000	100000	100000	100000
	Unisys Tapes in Storage - VTS	GB	100000	100000	100000	100000	100000	100000	100000	100000	100000	100000
	Unisys Offsite Tape Storage	Tape/Reel	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000
Total Unisys Services			**201,000**	**201,000**	**201,000**	**201,000**	**201,000**	**201,000**	**201,000**	**201,000**	**201,000**	**201,000**
Unisys Configurations												
	Platinum Tier											
	Unisys Mainframe Config - 1	MIP	550	550	550	550	550	550	550	550	550	550
	Unisys Mainframe Config - 2	MIP	220	220	220	220	220	220	220	220	220	220
	Unisys Mainframe Config - 3	MIP	2882	2882	2882	2882	2882	2882	2882	2882	2882	2882
	Unisys Mainframe Config - 4	MIP	875	875	875	875	875	875	875	875	875	875
sub-total Unisys Mainfram Services - Plantinum			**4527**	**4527**	**4527**	**4527**	**4527**	**4527**	**4527**	**4527**	**4527**	**4527**
	Gold Tier											
	Unisys Mainframe Config - 1	MIP	44	44	44	44	44	44	44	44	44	44
	Unisys Mainframe Config - 2	MIP	27	27	27	27	27	27	27	27	27	27
	Unisys Mainframe Config - 3	MIP	176	176	176	176	176	176	176	176	176	176
	Unisys Mainframe Config - 4	MIP	110	110	110	110	110	110	110	110	110	110
sub-total Unisys Mainfram Services - Gold			**357**	**357**	**357**	**357**	**357**	**357**	**357**	**357**	**357**	**357**
	Basic Tier											
	Unisys Mainframe Config - 1	MIP	44	44	44	44	44	44	44	44	44	44
	Unisys Mainframe Config - 2	MIP	27	27	27	27	27	27	27	27	27	27
	Unisys Mainframe Config - 3	MIP	176	176	176	176	176	176	176	176	176	176
	Unisys Mainframe Config - 4	MIP	110	110	110	110	110	110	110	110	110	110
sub-total Unisys Mainfram Services - Basic			**357**	**357**	**357**	**357**	**357**	**357**	**357**	**357**	**357**	**357**
Total - Unisys Mainframe Services - All Support Tiers			**5,241**	**5,241**	**5,241**	**5,241**	**5,241**	**5,241**	**5,241**	**5,241**	**5,241**	**5,241**
On-Demand (IaaS) (5)												
IaaS Servers - x86 (Windows, Linux) - Virtual Servers												
	IaaS Windows vConfig - 1	Instance	40	48	58	69	84	100	120	143	172	188
	IaaS Windows vConfig - 2	Instance	40	48	58	69	84	100	120	143	172	188
	IaaS Windows vConfig - 3	Instance	40	48	58	69	84	100	120	143	172	188
	IaaS Windows vConfig - 4	Instance	15	18	21	25	30	36	44	54	65	72
	IaaS Windows vConfig - 5	Instance	15	18	21	25	30	36	44	54	65	72
	IaaS Linux vConfig - 1	Instance	20	24	29	34	42	50	60	72	86	94
	IaaS Linux vConfig - 2	Instance	20	24	29	34	42	50	60	72	86	94
	IaaS Linux vConfig - 3	Instance	20	24	29	34	42	50	60	72	86	94
	IaaS Linux vConfig - 4	Instance	7	9	11	13	15	18	23	27	32	36
	IaaS Linux vConfig - 5	Instance	7	9	11	13	15	18	23	27	32	36
Total IaaS Servers - x86 (Windows, Linux) - Virtual Servers			**224**	**270**	**325**	**385**	**468**	**558**	**674**	**807**	**968**	**1,062**
IaaS Storage On-Demand												
	IaaS Storage Config - 1	GB	1000	1200	1440	1728	2074	2488	2986	3583	4300	5160
	IaaS Storage Config - 2	GB	500	600	720	864	1037	1244	1493	1792	2150	2580
	IaaS Storage Config - 3	GB	50	50	50	50	50	50	50	50	50	50

Baseline Units - Volumetrics

Note: The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all inclusive representation of every service desired by the Commonwealth.

Resource Description	Service Tier / Configuration (6)	Units	Year 1 Qty	Year 2 Qty	Year 3 Qty	Year 4 Qty	Year 5 Qty	Year 6 Qty	Year 7 Qty	Opt - Year 8 Qty	Opt - Year 9 Qty	Opt - Year 10 Qty
Total IaaS Storage On-Demand			**1,550**	**1,850**	**2,210**	**2,642**	**3,161**	**3,782**	**4,529**	**5,425**	**6,500**	**7,790**
IaaS Backup On-Demand												
	IaaS Backup Config - 1	GB	2,000	2,400	2,880	3,456	4,147	4,977	5,972	7,166	8,600	10320
Total IaaS Backup On-Demand			**2,000**	**2,400**	**2,880**	**3,456**	**4,147**	**4,977**	**5,972**	**7,166**	**8,600**	**10,320**

Reserve Account												
		Mos Balance	1	1	1	1	1	1	1	1	1	1
Reserve Account			**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**

Notes:

For purposes of submitting a proposal, Offerors should assume that tapes are equivalent in capacity to LTO4 tapes.

* For purposes of submitting a proposal, Offerors should assume that the slower Tier1 RAID5 uses 10K drives and the Tier2 RAID10 uses 15K drives.

** The volume is expressed as native.

*** For purposes of evaluation DASD is expressed in Usable (not Raw)

Third Party Software

Third Party Software

Vendor	Product											

Baseline Units - Volumetrics

Note: The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all inclusive representation of every service desired by the Commonwealth.

Resource Description	Service Tier / Configuration (6)	Units	Year 1 Qty	Year 2 Qty	Year 3 Qty	Year 4 Qty	Year 5 Qty	Year 6 Qty	Year 7 Qty	Opt - Year 8 Qty	Opt - Year 9 Qty	Opt - Year 10 Qty

Baseline Units - Volumetrics

Note: The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all inclusive representation of every service desired by the Commonwealth.

Resource Description	Service Tier / Configuration (6)	Units	Year 1 Qty	Year 2 Qty	Year 3 Qty	Year 4 Qty	Year 5 Qty	Year 6 Qty	Year 7 Qty	Opt - Year 8 Qty	Opt - Year 9 Qty	Opt - Year 10 Qty

Baseline Units - Volumetrics

Note: The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all inclusive representation of every service desired by the Commonwealth.

Resource Description	Service Tier / Configuration (6)	Units	Year 1 Qty	Year 2 Qty	Year 3 Qty	Year 4 Qty	Year 5 Qty	Year 6 Qty	Year 7 Qty	Opt - Year 8 Qty	Opt - Year 9 Qty	Opt - Year 10 Qty

Baseline Units - Volumetrics

Note: The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all inclusive representation of every service desired by the Commonwealth.

Resource Description	Service Tier / Configuration (6)	Units	Year 1 Qty	Year 2 Qty	Year 3 Qty	Year 4 Qty	Year 5 Qty	Year 6 Qty	Year 7 Qty	Opt - Year 8 Qty	Opt - Year 9 Qty	Opt - Year 10 Qty

Baseline Units - Volumetrics

Note: The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all inclusive representation of every service desired by the Commonwealth.

Resource Description	Service Tier / Configuration (6)	Units	Year 1 Qty	Year 2 Qty	Year 3 Qty	Year 4 Qty	Year 5 Qty	Year 6 Qty	Year 7 Qty	Opt - Year 8 Qty	Opt - Year 9 Qty	Opt - Year 10 Qty

Baseline Units - Volumetrics

Note: The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all inclusive representation of every service desired by the Commonwealth.

Resource Description	Service Tier / Configuration (6)	Units	Year 1 Qty	Year 2 Qty	Year 3 Qty	Year 4 Qty	Year 5 Qty	Year 6 Qty	Year 7 Qty	Opt - Year 8 Qty	Opt - Year 9 Qty	Opt - Year 10 Qty
Hybrid Third Party Software												
Vendor	**Product**											

Baseline Units - Volumetrics

Note: The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all inclusive representation of every service desired by the Commonwealth.

Resource Description	Service Tier / Configuration (6)	Units	Year 1 Qty	Year 2 Qty	Year 3 Qty	Year 4 Qty	Year 5 Qty	Year 6 Qty	Year 7 Qty	Opt - Year 8 Qty	Opt - Year 9 Qty	Opt - Year 10 Qty

Baseline Units - Volumetrics

Note: The Commonwealth has established mult

Price per unit \ per month

Resource Description	Service Tier / Configuration (6)	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Server - Fully Managed (1)											
x86 (Windows, Linux) - Physical Servers											
	Platinum Tier										
	Windows pConfig - 1	$ 584 49	$ 583 05	$ 581 58	$ 535 05	$ 470 86	$ 400 25	$ 340 19	$ 340 19	$ 340 19	$ 340 19
	Windows pConfig - 2	$ 614 85	$ 613 33	$ 611 79	$ 562 87	$ 495 37	$ 421 12	$ 357 85	$ 357 85	$ 357 85	$ 357 85
	Windows pConfig - 3	$ 665 66	$ 664 20	$ 657 72	$ 605 80	$ 536 06	$ 454 85	$ 383 68	$ 383 68	$ 383 68	$ 383 68
	Windows pConfig - 4	$ 969 12	$ 966 71	$ 964 30	$ 887 18	$ 780 76	$ 663 70	$ 564 04	$ 564 04	$ 564 04	$ 564 04
	Windows pConfig - 5	$ 896 33	$ 894 11	$ 891 88	$ 820 55	$ 722 12	$ 613 86	$ 521 68	$ 521 68	$ 521 68	$ 521 68
	Linux pConfig - 1	$ 618 58	$ 617 05	$ 615 50	$ 566 25	$ 498 32	$ 423 59	$ 360 02	$ 360 02	$ 360 02	$ 360 02
	Linux pConfig - 2	$ 648 94	$ 647 33	$ 645 71	$ 594 07	$ 522 83	$ 444 46	$ 377 68	$ 377 68	$ 377 68	$ 377 68
	Linux pConfig - 3	$ 699 75	$ 698 20	$ 691 64	$ 637 00	$ 563 52	$ 478 19	$ 403 51	$ 403 51	$ 403 51	$ 403 51
	Linux pConfig - 4	$ 1,035 32	$ 1,032 73	$ 1,030 16	$ 947 76	$ 834 08	$ 709 02	$ 602 56	$ 602 56	$ 602 56	$ 602 56
	Linux pConfig - 5	$ 962 53	$ 960 13	$ 957 74	$ 881 13	$ 775 44	$ 659 18	$ 560 19	$ 560 19	$ 560 19	$ 560 19
sub-total x86 (Windows, Linux) - Physical Servers - Plantinum		**$ 7,695.57**	**$ 7,676.84**	**$ 7,648.02**	**$ 7,037.66**	**$ 6,199.36**	**$ 5,268.22**	**$ 4,471.40**	**$ 4,471.40**	**$ 4,471.40**	**$ 4,471.40**
	Gold Tier										
	Windows pConfig - 1	$ 580 54	$ 579 10	$ 577 65	$ 531 43	$ 467 68	$ 397 54	$ 337 88	$ 337 88	$ 337 88	$ 337 88
	Windows pConfig - 2	$ 610 90	$ 609 38	$ 607 86	$ 559 25	$ 492 19	$ 418 41	$ 355 54	$ 355 54	$ 355 54	$ 355 54
	Windows pConfig - 3	$ 661 71	$ 660 25	$ 653 79	$ 602 18	$ 532 88	$ 452 14	$ 381 37	$ 381 37	$ 381 37	$ 381 37
	Windows pConfig - 4	$ 963 07	$ 960 68	$ 958 28	$ 881 63	$ 775 89	$ 659 56	$ 560 51	$ 560 51	$ 560 51	$ 560 51
	Windows pConfig - 5	$ 890 28	$ 888 08	$ 885 86	$ 815 00	$ 717 25	$ 609 72	$ 518 15	$ 518 15	$ 518 15	$ 518 15
	Linux pConfig - 1	$ 605 61	$ 604 11	$ 602 60	$ 554 38	$ 487 87	$ 414 71	$ 352 47	$ 352 47	$ 352 47	$ 352 47
	Linux pConfig - 2	$ 635 97	$ 634 39	$ 632 81	$ 582 20	$ 512 38	$ 435 58	$ 370 13	$ 370 13	$ 370 13	$ 370 13
	Linux pConfig - 3	$ 686 78	$ 685 26	$ 678 74	$ 625 13	$ 553 07	$ 469 31	$ 395 96	$ 395 96	$ 395 96	$ 395 96
	Linux pConfig - 4	$ 1,012 59	$ 1,010 06	$ 1,007 54	$ 926 96	$ 815 77	$ 693 46	$ 589 33	$ 589 33	$ 589 33	$ 589 33
	Linux pConfig - 5	$ 939 80	$ 937 46	$ 935 12	$ 860 33	$ 757 13	$ 643 62	$ 546 96	$ 546 96	$ 546 96	$ 546 96
sub-total x86 (Windows, Linux) - Physical Servers - Gold		**$ 7,587.25**	**$ 7,568.77**	**$ 7,540.25**	**$ 6,938.49**	**$ 6,112.11**	**$ 5,194.05**	**$ 4,408.30**	**$ 4,408.30**	**$ 4,408.30**	**$ 4,408.30**
	Silver Tier										
	Windows pConfig - 1	$ 578 58	$ 577 15	$ 575 70	$ 529 64	$ 466 10	$ 396 20	$ 336 74	$ 336 74	$ 336 74	$ 336 74
	Windows pConfig - 2	$ 608 94	$ 607 43	$ 605 91	$ 557 46	$ 490 61	$ 417 07	$ 354 40	$ 354 40	$ 354 40	$ 354 40
	Windows pConfig - 3	$ 659 75	$ 658 30	$ 651 84	$ 600 39	$ 531 30	$ 450 80	$ 380 23	$ 380 23	$ 380 23	$ 380 23
	Windows pConfig - 4	$ 959 19	$ 956 81	$ 954 42	$ 878 09	$ 772 76	$ 656 90	$ 558 26	$ 558 26	$ 558 26	$ 558 26
	Windows pConfig - 5	$ 886 40	$ 884 21	$ 882 00	$ 811 46	$ 714 12	$ 607 06	$ 515 90	$ 515 90	$ 515 90	$ 515 90
	Linux pConfig - 1	$ 597 95	$ 596 47	$ 594 97	$ 547 37	$ 481 70	$ 409 46	$ 348 01	$ 348 01	$ 348 01	$ 348 01
	Linux pConfig - 2	$ 628 31	$ 626 75	$ 625 18	$ 575 19	$ 506 21	$ 430 33	$ 365 67	$ 365 67	$ 365 67	$ 365 67
	Linux pConfig - 3	$ 679 12	$ 677 62	$ 671 11	$ 618 12	$ 546 90	$ 464 06	$ 391 50	$ 391 50	$ 391 50	$ 391 50
	Linux pConfig - 4	$ 996 90	$ 994 41	$ 991 93	$ 912 60	$ 803 14	$ 682 72	$ 580 20	$ 580 20	$ 580 20	$ 580 20
	Linux pConfig - 5	$ 924 11	$ 921 81	$ 919 51	$ 845 97	$ 744 50	$ 632 88	$ 537 83	$ 537 83	$ 537 83	$ 537 83
sub-total x86 (Windows, Linux) - Physical Servers - Silver		**$ 7,519.25**	**$ 7,500.96**	**$ 7,472.57**	**$ 6,876.29**	**$ 6,057.34**	**$ 5,147.48**	**$ 4,368.74**	**$ 4,368.74**	**$ 4,368.74**	**$ 4,368.74**
	Bronze Tier										
	Windows pConfig - 1	$ 577 84	$ 576 42	$ 574 97	$ 528 97	$ 465 51	$ 395 70	$ 336 32	$ 336 32	$ 336 32	$ 336 32
	Windows pConfig - 2	$ 608 20	$ 606 70	$ 605 18	$ 556 79	$ 490 02	$ 416 57	$ 353 98	$ 353 98	$ 353 98	$ 353 98
	Windows pConfig - 3	$ 659 01	$ 657 57	$ 651 11	$ 599 72	$ 530 71	$ 450 30	$ 379 81	$ 379 81	$ 379 81	$ 379 81
	Windows pConfig - 4	$ 957 56	$ 955 19	$ 952 80	$ 876 60	$ 771 45	$ 655 79	$ 557 31	$ 557 31	$ 557 31	$ 557 31
	Windows pConfig - 5	$ 884 77	$ 882 59	$ 880 38	$ 809 97	$ 712 81	$ 605 95	$ 514 95	$ 514 95	$ 514 95	$ 514 95
	Linux pConfig - 1	$ 594 61	$ 593 13	$ 591 65	$ 544 31	$ 479 01	$ 407 17	$ 346 07	$ 346 07	$ 346 07	$ 346 07
	Linux pConfig - 2	$ 624 97	$ 623 41	$ 621 86	$ 572 13	$ 503 52	$ 428 04	$ 363 73	$ 363 73	$ 363 73	$ 363 73

Note: The Commonwealth has established mult

Baseline Units - Volumetrics

Price per unit \ per month

Resource Description	Service Tier / Configuration (6)	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
	Linux pConfig - 3	$ 675 78	$ 674 28	$ 667 79	$ 615 06	$ 544 21	$ 461 77	$ 389 56	$ 389 56	$ 389 56	$ 389 56
	Linux pConfig - 4	$ 990 06	$ 987 58	$ 985 12	$ 906 33	$ 797 62	$ 678 03	$ 576 21	$ 576 21	$ 576 21	$ 576 21
	Linux pConfig - 5	$ 917 27	$ 914 98	$ 912 70	$ 839 70	$ 738 98	$ 628 19	$ 533 84	$ 533 84	$ 533 84	$ 533 84
sub-total x86 (Windows, Linux) - Physical Servers - Bronze		**$ 7,490.07**	**$ 7,471.85**	**$ 7,443.56**	**$ 6,849.58**	**$ 6,033.84**	**$ 5,127.51**	**$ 4,351.78**	**$ 4,351.78**	**$ 4,351.78**	**$ 4,351.78**
	Basic Tier										
	Windows pConfig - 1	$ 576 56	$ 575 13	$ 573 69	$ 527 79	$ 464 47	$ 394 82	$ 335 57	$ 335 57	$ 335 57	$ 335 57
	Windows pConfig - 2	$ 606 92	$ 605 41	$ 603 90	$ 555 61	$ 488 98	$ 415 69	$ 353 23	$ 353 23	$ 353 23	$ 353 23
	Windows pConfig - 3	$ 657 73	$ 656 28	$ 649 83	$ 598 54	$ 529 67	$ 449 42	$ 379 06	$ 379 06	$ 379 06	$ 379 06
	Windows pConfig - 4	$ 955 42	$ 953 05	$ 950 67	$ 874 63	$ 769 73	$ 654 32	$ 556 06	$ 556 06	$ 556 06	$ 556 06
	Windows pConfig - 5	$ 882 63	$ 880 45	$ 878 25	$ 808 00	$ 711 09	$ 604 48	$ 513 70	$ 513 70	$ 513 70	$ 513 70
	Linux pConfig - 1	$ 591 32	$ 589 85	$ 588 38	$ 541 30	$ 476 36	$ 404 92	$ 344 15	$ 344 15	$ 344 15	$ 344 15
	Linux pConfig - 2	$ 621 68	$ 620 13	$ 618 59	$ 569 12	$ 500 87	$ 425 79	$ 361 81	$ 361 81	$ 361 81	$ 361 81
	Linux pConfig - 3	$ 672 49	$ 671 00	$ 664 52	$ 612 05	$ 541 56	$ 459 52	$ 387 64	$ 387 64	$ 387 64	$ 387 64
	Linux pConfig - 4	$ 983 55	$ 981 09	$ 978 65	$ 900 37	$ 792 38	$ 673 57	$ 572 43	$ 572 43	$ 572 43	$ 572 43
	Linux pConfig - 5	$ 910 76	$ 908 49	$ 906 23	$ 833 74	$ 733 74	$ 623 73	$ 530 06	$ 530 06	$ 530 06	$ 530 06
sub-total x86 (Windows, Linux) - Physical Servers - Basic		**$ 7,459.06**	**$ 7,440.88**	**$ 7,412.71**	**$ 6,821.15**	**$ 6,008.85**	**$ 5,106.26**	**$ 4,333.71**	**$ 4,333.71**	**$ 4,333.71**	**$ 4,333.71**
Total - Fully Managed - x86 Physical - All Support Tiers (Window, Linux)		**$37,751.20**	**$37,659.30**	**$37,517.11**	**$34,523.17**	**$30,411.50**	**$25,843.52**	**$21,933.93**	**$ 21,933.93**	**$ 21,933.93**	**$ 21,933.93**
x86 (Windows, Linux) - Virtual Servers											
	Platinum Tier										
	Windows vConfig - 1	$ 395 65	$ 394 64	$ 393 65	$ 362 16	$ 318 69	$ 270 90	$ 230 26	$ 230 26	$ 230 26	$ 230 26
	Windows vConfig - 2	$ 401 51	$ 400 37	$ 399 39	$ 367 42	$ 323 32	$ 274 88	$ 233 60	$ 233 60	$ 233 60	$ 233 60
	Windows vConfig - 3	$ 422 11	$ 420 49	$ 419 49	$ 385 86	$ 339 53	$ 288 82	$ 245 34	$ 245 34	$ 245 34	$ 245 34
	Windows vConfig - 4	$ 550 79	$ 549 27	$ 547 91	$ 504 06	$ 443 57	$ 377 10	$ 320 47	$ 320 47	$ 320 47	$ 320 47
	Windows vConfig - 5	$ 478 00	$ 476 66	$ 475 49	$ 437 43	$ 384 93	$ 327 26	$ 278 11	$ 278 11	$ 278 11	$ 278 11
	Linux vConfig - 1	$ 450 24	$ 449 08	$ 447 96	$ 412 12	$ 362 66	$ 308 27	$ 262 03	$ 262 03	$ 262 03	$ 262 03
	Linux vConfig - 2	$ 456 10	$ 454 81	$ 453 70	$ 417 38	$ 367 29	$ 312 25	$ 265 37	$ 265 37	$ 265 37	$ 265 37
	Linux vConfig - 3	$ 476 70	$ 474 93	$ 473 80	$ 435 82	$ 383 50	$ 326 19	$ 277 11	$ 277 11	$ 277 11	$ 277 11
	Linux vConfig - 4	$ 701 53	$ 699 63	$ 697 91	$ 642 05	$ 565 00	$ 480 30	$ 408 22	$ 408 22	$ 408 22	$ 408 22
	Linux vConfig - 5	$ 628 75	$ 627 03	$ 625 49	$ 575 42	$ 506 36	$ 430 46	$ 365 86	$ 365 86	$ 365 86	$ 365 86
sub-total x86 (Windows, Linux) - Virtual Servers - Platinum		**$ 4,961.38**	**$ 4,946.91**	**$ 4,934.79**	**$ 4,539.72**	**$ 3,994.85**	**$ 3,396.43**	**$ 2,886.37**	**$ 2,886.37**	**$ 2,886.37**	**$ 2,886.37**
	Gold Tier										
	Windows vConfig - 1	$ 393 55	$ 392 54	$ 391 56	$ 360 23	$ 317 00	$ 269 47	$ 229 04	$ 229 04	$ 229 04	$ 229 04
	Windows vConfig - 2	$ 399 41	$ 398 27	$ 397 30	$ 365 49	$ 321 63	$ 273 45	$ 232 38	$ 232 38	$ 232 38	$ 232 38
	Windows vConfig - 3	$ 420 01	$ 418 39	$ 417 40	$ 383 93	$ 337 84	$ 287 39	$ 244 12	$ 244 12	$ 244 12	$ 244 12
	Windows vConfig - 4	$ 546 59	$ 545 08	$ 543 74	$ 500 21	$ 440 18	$ 374 22	$ 318 03	$ 318 03	$ 318 03	$ 318 03
	Windows vConfig - 5	$ 473 80	$ 472 47	$ 471 32	$ 433 58	$ 381 54	$ 324 38	$ 275 67	$ 275 67	$ 275 67	$ 275 67
	Linux vConfig - 1	$ 440 49	$ 439 35	$ 438 25	$ 403 19	$ 354 80	$ 301 59	$ 256 35	$ 256 35	$ 256 35	$ 256 35
	Linux vConfig - 2	$ 446 35	$ 445 08	$ 443 99	$ 408 45	$ 359 43	$ 305 57	$ 259 69	$ 259 69	$ 259 69	$ 259 69
	Linux vConfig - 3	$ 466 95	$ 465 20	$ 464 09	$ 426 89	$ 375 64	$ 319 51	$ 271 43	$ 271 43	$ 271 43	$ 271 43
	Linux vConfig - 4	$ 682 02	$ 680 17	$ 678 50	$ 624 19	$ 549 28	$ 466 95	$ 396 87	$ 396 87	$ 396 87	$ 396 87
	Linux vConfig - 5	$ 609 24	$ 607 57	$ 606 08	$ 557 56	$ 490 64	$ 417 11	$ 354 51	$ 354 51	$ 354 51	$ 354 51
sub-total x86 (Windows, Linux) - Virtual Servers - Gold		**$ 4,878.41**	**$ 4,864.12**	**$ 4,852.23**	**$ 4,463.72**	**$ 3,927.98**	**$ 3,339.64**	**$ 2,838.09**	**$ 2,838.09**	**$ 2,838.09**	**$ 2,838.09**
	Silver Tier										
	Windows vConfig - 1	$ 391 64	$ 390 64	$ 389 65	$ 358 48	$ 315 45	$ 268 16	$ 227 92	$ 227 92	$ 227 92	$ 227 92
	Windows vConfig - 2	$ 397 50	$ 396 37	$ 395 39	$ 363 74	$ 320 08	$ 272 14	$ 231 26	$ 231 26	$ 231 26	$ 231 26

Baseline Units - Volumetrics

Note: The Commonwealth has established mult

Price per unit \ per month

Resource Description	Service Tier / Configuration (6)	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
	Windows vConfig - 3	$ 418 10	$ 416 49	$ 415 49	$ 382 18	$ 336 29	$ 286 08	$ 243 00	$ 243 00	$ 243 00	$ 243 00
	Windows vConfig - 4	$ 542 76	$ 541 26	$ 539 93	$ 496 71	$ 437 10	$ 371 60	$ 315 80	$ 315 80	$ 315 80	$ 315 80
	Windows vConfig - 5	$ 469 97	$ 468 65	$ 467 51	$ 430 08	$ 378 46	$ 321 76	$ 273 44	$ 273 44	$ 273 44	$ 273 44
	Linux vConfig - 1	$ 432 46	$ 431 34	$ 430 26	$ 395 84	$ 348 33	$ 296 09	$ 251 68	$ 251 68	$ 251 68	$ 251 68
	Linux vConfig - 2	$ 438 32	$ 437 07	$ 436 00	$ 401 10	$ 352 96	$ 300 07	$ 255 02	$ 255 02	$ 255 02	$ 255 02
	Linux vConfig - 3	$ 458 92	$ 457 19	$ 456 10	$ 419 54	$ 369 17	$ 314 01	$ 266 76	$ 266 76	$ 266 76	$ 266 76
	Linux vConfig - 4	$ 665 97	$ 664 16	$ 662 52	$ 609 49	$ 536 35	$ 455 95	$ 387 52	$ 387 52	$ 387 52	$ 387 52
	Linux vConfig - 5	$ 593 19	$ 591 56	$ 590 10	$ 542 86	$ 477 71	$ 406 11	$ 345 16	$ 345 16	$ 345 16	$ 345 16
sub-total x86 (Windows, Linux) - Virtual Servers - Silver		**$ 4,808.83**	**$ 4,794.73**	**$ 4,782.95**	**$ 4,400.02**	**$ 3,871.90**	**$ 3,291.97**	**$ 2,797.56**	**$ 2,797.56**	**$ 2,797.56**	**$ 2,797.56**
	Bronze Tier										
	Windows vConfig - 1	$ 390 74	$ 389 74	$ 388 76	$ 357 66	$ 314 73	$ 267 54	$ 227 40	$ 227 40	$ 227 40	$ 227 40
	Windows vConfig - 2	$ 396 60	$ 395 47	$ 394 50	$ 362 92	$ 319 36	$ 271 52	$ 230 74	$ 230 74	$ 230 74	$ 230 74
	Windows vConfig - 3	$ 417 20	$ 415 59	$ 414 60	$ 381 36	$ 335 57	$ 285 46	$ 242 48	$ 242 48	$ 242 48	$ 242 48
	Windows vConfig - 4	$ 540 97	$ 539 48	$ 538 14	$ 495 07	$ 435 66	$ 370 38	$ 314 76	$ 314 76	$ 314 76	$ 314 76
	Windows vConfig - 5	$ 468 18	$ 466 87	$ 465 72	$ 428 44	$ 377 02	$ 320 54	$ 272 40	$ 272 40	$ 272 40	$ 272 40
	Linux vConfig - 1	$ 428 95	$ 427 85	$ 426 78	$ 392 63	$ 345 51	$ 293 70	$ 249 64	$ 249 64	$ 249 64	$ 249 64
	Linux vConfig - 2	$ 434 81	$ 433 58	$ 432 52	$ 397 89	$ 350 14	$ 297 68	$ 252 98	$ 252 98	$ 252 98	$ 252 98
	Linux vConfig - 3	$ 455 41	$ 453 70	$ 452 62	$ 416 33	$ 366 35	$ 311 62	$ 264 72	$ 264 72	$ 264 72	$ 264 72
	Linux vConfig - 4	$ 658 96	$ 657 17	$ 655 55	$ 603 08	$ 530 70	$ 451 15	$ 383 44	$ 383 44	$ 383 44	$ 383 44
	Linux vConfig - 5	$ 586 18	$ 584 57	$ 583 13	$ 536 45	$ 472 06	$ 401 31	$ 341 08	$ 341 08	$ 341 08	$ 341 08
sub-total x86 (Windows, Linux) - Virtual Servers - Bronze		**$ 4,778.00**	**$ 4,764.02**	**$ 4,752.32**	**$ 4,371.83**	**$ 3,847.10**	**$ 3,270.90**	**$ 2,779.64**	**$ 2,779.64**	**$ 2,779.64**	**$ 2,779.64**
	Basic Tier										
	Windows vConfig - 1	$ 389 89	$ 388 89	$ 387 91	$ 356 88	$ 314 04	$ 266 96	$ 226 90	$ 226 90	$ 226 90	$ 226 90
	Windows vConfig - 2	$ 395 75	$ 394 62	$ 393 65	$ 362 14	$ 318 67	$ 270 94	$ 230 24	$ 230 24	$ 230 24	$ 230 24
	Windows vConfig - 3	$ 416 35	$ 414 74	$ 413 75	$ 380 58	$ 334 88	$ 284 88	$ 241 98	$ 241 98	$ 241 98	$ 241 98
	Windows vConfig - 4	$ 539 25	$ 537 77	$ 536 44	$ 493 50	$ 434 28	$ 369 20	$ 313 76	$ 313 76	$ 313 76	$ 313 76
	Windows vConfig - 5	$ 466 46	$ 465 16	$ 464 02	$ 426 87	$ 375 64	$ 319 36	$ 271 40	$ 271 40	$ 271 40	$ 271 40
	Linux vConfig - 1	$ 425 73	$ 424 64	$ 423 57	$ 389 68	$ 342 91	$ 291 49	$ 247 77	$ 247 77	$ 247 77	$ 247 77
	Linux vConfig - 2	$ 431 59	$ 430 37	$ 429 31	$ 394 94	$ 347 54	$ 295 47	$ 251 11	$ 251 11	$ 251 11	$ 251 11
	Linux vConfig - 3	$ 452 19	$ 450 49	$ 449 41	$ 413 38	$ 363 75	$ 309 41	$ 262 85	$ 262 85	$ 262 85	$ 262 85
	Linux vConfig - 4	$ 652 52	$ 650 74	$ 649 14	$ 597 19	$ 525 52	$ 446 74	$ 379 69	$ 379 69	$ 379 69	$ 379 69
	Linux vConfig - 5	$ 579 74	$ 578 14	$ 576 72	$ 530 56	$ 466 88	$ 396 90	$ 337 33	$ 337 33	$ 337 33	$ 337 33
sub-total x86 (Windows, Linux) - Virtual Servers - Basic		**$ 4,749.47**	**$ 4,735.56**	**$ 4,723.92**	**$ 4,345.72**	**$ 3,824.11**	**$ 3,251.35**	**$ 2,763.03**	**$ 2,763.03**	**$ 2,763.03**	**$ 2,763.03**
Total - Fully Managed - x86 Virtual - All Support Tiers (Window, Linux)		**$24,176.09**	**$24,105.34**	**$24,046.21**	**$22,121.01**	**$19,465.94**	**$16,550.29**	**$14,064.69**	**$ 14,064.69**	**$ 14,064.69**	**$ 14,064.69**
UNIX (IBM P-Series, AIX)											
	Platinum Tier										
	AIX Config - 1	$ 928 73	$ 941 01	$ 952 63	$ 966 12	$ 981 43	$ 946 13	$ 937 13	$ 937 13	$ 937 13	$ 937 13
	AIX Config - 2	$ 977 47	$ 989 58	$ 1,001 04	$ 1,014 39	$ 1,029 60	$ 993 30	$ 983 25	$ 983 25	$ 983 25	$ 983 25
	AIX Config - 3	$ 1,042 97	$ 1,054 11	$ 1,064 59	$ 1,076 94	$ 1,092 06	$ 1,055 59	$ 1,045 33	$ 1,045 33	$ 1,045 33	$ 1,045 33
	AIX Config - 4	$ 1,834 94	$ 1,845 00	$ 1,853 58	$ 1,866 20	$ 1,881 27	$ 1,844 51	$ 1,834 74	$ 1,834 74	$ 1,834 74	$ 1,834 74
	AIX Config - 5	$ 1,680 91	$ 1,685 54	$ 1,688 54	$ 1,694 97	$ 1,703 25	$ 1,660 02	$ 1,643 03	$ 1,643 03	$ 1,643 03	$ 1,643 03
sub-total P-Series (AIX) - Bronze		**$ 6,465.02**	**$ 6,515.24**	**$ 6,560.38**	**$ 6,618.62**	**$ 6,687.61**	**$ 6,499.55**	**$ 6,443.48**	**$ 6,443.48**	**$ 6,443.48**	**$ 6,443.48**
	Gold Tier										
	AIX Config - 1	$ 815 48	$ 829 28	$ 842 51	$ 857 71	$ 874 68	$ 840 23	$ 832 07	$ 832 07	$ 832 07	$ 832 07
	AIX Config - 2	$ 864 17	$ 877 01	$ 889 26	$ 903 46	$ 919 50	$ 884 04	$ 875 67	$ 875 67	$ 875 67	$ 875 67

Note: The Commonwealth has established mult

Baseline Units - Volumetrics

Price per unit \ per month

Resource Description	Service Tier / Configuration (6)	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
	AIX Config - 3	$ 929 76	$ 942 42	$ 954 50	$ 968 53	$ 984 48	$ 948 86	$ 939 44	$ 939 44	$ 939 44	$ 939 44
	AIX Config - 4	$ 1,608 09	$ 1,619 79	$ 1,630 03	$ 1,644 31	$ 1,661 08	$ 1,626 00	$ 1,619 59	$ 1,619 59	$ 1,619 59	$ 1,619 59
	AIX Config - 5	$ 1,454 06	$ 1,460 33	$ 1,464 99	$ 1,473 08	$ 1,483 06	$ 1,441 51	$ 1,427 88	$ 1,427 88	$ 1,427 88	$ 1,427 88
sub-total P-Series (AIX) - Gold		**$ 5,671.56**	**$ 5,728.83**	**$ 5,781.29**	**$ 5,847.09**	**$ 5,922.80**	**$ 5,740.64**	**$ 5,694.65**	**$ 5,694.65**	**$ 5,694.65**	**$ 5,694.65**
	Silver Tier										
	AIX Config - 1	$ 719 11	$ 733 58	$ 747 55	$ 763 57	$ 781 39	$ 747 78	$ 740 46	$ 740 46	$ 740 46	$ 740 46
	AIX Config - 2	$ 767 77	$ 781 29	$ 794 29	$ 809 31	$ 827 04	$ 793 26	$ 785 74	$ 785 74	$ 785 74	$ 785 74
	AIX Config - 3	$ 820 70	$ 834 06	$ 846 91	$ 861 78	$ 878 58	$ 843 79	$ 835 21	$ 835 21	$ 835 21	$ 835 21
	AIX Config - 4	$ 1,414 86	$ 1,428 19	$ 1,440 08	$ 1,456 03	$ 1,476 18	$ 1,444 45	$ 1,439 74	$ 1,439 74	$ 1,439 74	$ 1,439 74
	AIX Config - 5	$ 1,260 83	$ 1,268 73	$ 1,275 04	$ 1,284 80	$ 1,298 16	$ 1,259 96	$ 1,248 03	$ 1,248 03	$ 1,248 03	$ 1,248 03
sub-total P-Series (AIX) - Silver		**$ 4,983.27**	**$ 5,045.85**	**$ 5,103.87**	**$ 5,175.49**	**$ 5,261.35**	**$ 5,089.24**	**$ 5,049.18**	**$ 5,049.18**	**$ 5,049.18**	**$ 5,049.18**
	Bronze Tier										
	AIX Config - 1	$ 622 79	$ 637 88	$ 652 58	$ 669 44	$ 688 10	$ 655 32	$ 648 85	$ 648 85	$ 648 85	$ 648 85
	AIX Config - 2	$ 671 55	$ 686 46	$ 701 00	$ 717 71	$ 736 28	$ 703 34	$ 696 65	$ 696 65	$ 696 65	$ 696 65
	AIX Config - 3	$ 736 95	$ 750 96	$ 764 54	$ 780 26	$ 797 90	$ 763 96	$ 756 20	$ 756 20	$ 756 20	$ 756 20
	AIX Config - 4	$ 1,221 81	$ 1,238 33	$ 1,253 49	$ 1,272 82	$ 1,294 63	$ 1,264 59	$ 1,261 56	$ 1,261 56	$ 1,261 56	$ 1,261 56
	AIX Config - 5	$ 1,067 78	$ 1,078 87	$ 1,088 45	$ 1,101 59	$ 1,116 61	$ 1,080 10	$ 1,069 85	$ 1,069 85	$ 1,069 85	$ 1,069 85
sub-total P-Series (AIX) - Bronze		**$ 4,320.88**	**$ 4,392.50**	**$ 4,460.06**	**$ 4,541.82**	**$ 4,633.52**	**$ 4,467.31**	**$ 4,433.11**	**$ 4,433.11**	**$ 4,433.11**	**$ 4,433.11**
	Basic Tier										
	AIX Config - 1	$ 526 67	$ 542 25	$ 557 61	$ 575 31	$ 594 81	$ 562 88	$ 557 24	$ 557 24	$ 557 24	$ 557 24
	AIX Config - 2	$ 575 39	$ 590 82	$ 606 03	$ 623 58	$ 642 99	$ 610 88	$ 605 03	$ 605 03	$ 605 03	$ 605 03
	AIX Config - 3	$ 640 72	$ 655 29	$ 669 57	$ 686 13	$ 704 61	$ 671 50	$ 664 60	$ 664 60	$ 664 60	$ 664 60
	AIX Config - 4	$ 1,028 89	$ 1,046 83	$ 1,063 55	$ 1,084 56	$ 1,108 05	$ 1,079 69	$ 1,078 32	$ 1,078 32	$ 1,078 32	$ 1,078 32
	AIX Config - 5	$ 874 86	$ 887 37	$ 898 51	$ 913 33	$ 930 03	$ 895 20	$ 886 61	$ 886 61	$ 886 61	$ 886 61
sub-total P-Series (AIX) - Basic		**$ 3,646.53**	**$ 3,722.56**	**$ 3,795.27**	**$ 3,882.91**	**$ 3,980.49**	**$ 3,820.15**	**$ 3,791.80**	**$ 3,791.80**	**$ 3,791.80**	**$ 3,791.80**
Total - Fully Managed - P-Series (AIX) - All Support Tiers (Window, Linux)		**$ 25,087.26**	**$ 25,404.98**	**$ 25,700.87**	**$ 26,065.93**	**$ 26,485.77**	**$ 25,616.89**	**$ 25,412.22**	**$ 25,412.22**	**$ 25,412.22**	**$ 25,412.22**
Server - Managed Only (2)											
x86 (Windows, Linux)											
	Platinum Tier	$ 435 89	$ 434 81	$ 433 72	$ 399 02	$ 351 14	$ 298 47	$ 253 70	$ 253 70	$ 253 70	$ 253 70
	Gold Tier	$ 422 92	$ 421 87	$ 420 82	$ 387 15	$ 340 69	$ 289 59	$ 246 15	$ 246 15	$ 246 15	$ 246 15
	Silver Tier	$ 415 26	$ 414 23	$ 413 19	$ 380 14	$ 334 52	$ 284 34	$ 241 69	$ 241 69	$ 241 69	$ 241 69
	Bronze Tier	$ 411 92	$ 410 89	$ 409 87	$ 377 08	$ 331 83	$ 282 05	$ 239 75	$ 239 75	$ 239 75	$ 239 75
	Basic Tier	$ 408 63	$ 407 61	$ 406 60	$ 374 07	$ 329 18	$ 279 80	$ 237 83	$ 237 83	$ 237 83	$ 237 83
Total Managed Only- x86 - All Support Tiers (Window, Linux)		**$ 2,094.62**	**$ 2,089.41**	**$ 2,084.20**	**$ 1,917.46**	**$ 1,687.36**	**$ 1,434.25**	**$ 1,219.12**	**$ 1,219.12**	**$ 1,219.12**	**$ 1,219.12**
UNIX (IBM P-Series, AIX)											
	Platinum	$ 728 02	$ 743 06	$ 758 40	$ 774 06	$ 791 48	$ 757 50	$ 749 88	$ 749 88	$ 749 88	$ 749 88
	Gold Tier	$ 678 20	$ 694 06	$ 710 29	$ 726 90	$ 745 25	$ 712 21	$ 705 53	$ 705 53	$ 705 53	$ 705 53
	Silver Tier	$ 630 19	$ 645 99	$ 662 18	$ 678 78	$ 697 13	$ 664 10	$ 657 43	$ 657 43	$ 657 43	$ 657 43
	Bronze Tier	$ 572 89	$ 589 46	$ 606 52	$ 624 07	$ 643 36	$ 611 28	$ 605 53	$ 605 53	$ 605 53	$ 605 53
	Basic Tier	$ 462 09	$ 479 27	$ 497 09	$ 515 57	$ 535 81	$ 504 67	$ 499 88	$ 499 88	$ 499 88	$ 499 88
Total Managed Only- P-Series - All Support Tiers (AIX)		**$ 3,071.39**	**$ 3,151.84**	**$ 3,234.48**	**$ 3,319.38**	**$ 3,413.03**	**$ 3,249.76**	**$ 3,218.25**	**$ 3,218.25**	**$ 3,218.25**	**$ 3,218.25**
Storage and Backup - Fully Managed (1)											

Note: The Commonwealth has established mult

Baseline Units - Volumetrics

Price per unit \ per month

Resource Description	Service Tier / Configuration (6)	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Enterprise Storage											
	* Dedicated - Config 1 - SAN Raid 5	$ 0 05	$ 0 05	$ 0 05	$ 0 05	$ 0 04	$ 0 04	$ 0 04	$ 0 04	$ 0 04	$ 0 04
	* Dedicated - Config 2 - SAN Raid 10	$ 0 36	$ 0 34	$ 0 32	$ 0 31	$ 0 29	$ 0 28	$ 0 26	$ 0 26	$ 0 26	$ 0 26
	Dedicated - Config 3 - Net Attached	$ 0 05	$ 0 06	$ 0 06	$ 0 05	$ 0 05	$ 0 05	$ 0 05	$ 0 05	$ 0 05	$ 0 05
Total Enterprise Storage - Fully Managed		**$ 0.46**	**$ 0.45**	**$ 0.43**	**$ 0.41**	**$ 0.38**	**$ 0.37**	**$ 0.35**	**$ 0.35**	**$ 0.35**	**$ 0.35**
Tape and Backup											
	** Server Tape Stored	$ 0 02	$ 0 02	$ 0 02	$ 0 02	$ 0 01	$ 0 01	$ 0 01	$ 0 01	$ 0 01	$ 0 01
	** Offsite Tape Storage	$ 0 38	$ 0 36	$ 0 35	$ 0 34	$ 0 33	$ 0 31	$ 0 31	$ 0 31	$ 0 31	$ 0 31
Total Tape and Backup - Fully Managed		**$ 0.40**	**$ 0.38**	**$ 0.37**	**$ 0.36**	**$ 0.34**	**$ 0.32**	**$ 0.32**	**$ 0.32**	**$ 0.32**	**$ 0.32**
Limited Co-Lo (Data Center Only Charge) (3)											
Server, Storage, Network, Security Equipment											
	Co-Lo Config - 1	$ 130 83	$ 131 18	$ 131 54	$ 134 18	$ 134 18	$ 134 57	$ 134 98	$ 134 98	$ 134 98	$ 134 98
	Co-Lo Config - 2	$ 234 37	$ 235 08	$ 235 78	$ 236 58	$ 239 21	$ 239 98	$ 240 81	$ 240 81	$ 240 81	$ 240 81
	Co-Lo Config - 3	$ 485 18	$ 486 71	$ 488 23	$ 489 93	$ 458 91	$ 460 53	$ 462 27	$ 462 27	$ 462 27	$ 462 27
Total Limited Co-Lo (Data Center Only Charge)		**$ 850.38**	**$ 852.97**	**$ 855.55**	**$ 860.69**	**$ 832.30**	**$ 835.08**	**$ 838.06**	**$ 838.06**	**$ 838.06**	**$ 838.06**
Mainframe Services (4)											
IBM Services											
	*** IBM Mainframe Allocated DASD	$ 1 25	$ 1 19	$ 1 13	$ 1 08	$ 1 02	$ 0 97	$ 0 91	$ 0 91	$ 0 91	$ 0 91
	IBM Tapes in Storage - VTS	$ 0 29	$ 0 29	$ 0 28	$ 0 28	$ 0 27	$ 0 27	$ 0 25	$ 0 25	$ 0 25	$ 0 25
	IBM Offsite Tape Storage	$ 0 38	$ 0 36	$ 0 35	$ 0 34	$ 0 33	$ 0 31	$ 0 31	$ 0 31	$ 0 31	$ 0 31
Total IBM Services		**$ 1.92**	**$ 1.84**	**$ 1.76**	**$ 1.70**	**$ 1.62**	**$ 1.55**	**$ 1.47**	**$ 1.47**	**$ 1.47**	**$ 1.47**
IBM Configurations											
	Platinum Tier										
	IBM Mainframe Config - 1	$ 217 73	$ 307 46	$ 397 18	$ 387 89	$ 379 22	$ 361 87	$ 354 10	$ 354 10	$ 354 10	$ 354 10
	IBM Mainframe Config - 2	$ 191 30	$ 280 42	$ 369 55	$ 361 63	$ 354 26	$ 338 17	$ 331 59	$ 331 59	$ 331 59	$ 331 59
	IBM Mainframe Config - 3	$ 292 45	$ 430 96	$ 569 46	$ 551 55	$ 534 68	$ 509 58	$ 494 43	$ 494 43	$ 494 43	$ 494 43
	IBM AS400 Config 1	$ 23 76	$ 109 11	$ 194 46	$ 195 29	$ 196 24	$ 188 05	$ 188 97	$ 188 97	$ 188 97	$ 188 97
	IBM AS400 Config 2	$ 58 38	$ 150 96	$ 243 52	$ 242 59	$ 241 53	$ 231 64	$ 230 78	$ 230 78	$ 230 78	$ 230 78
sub-total IBM Mainfram Services - Plantinum		**$ 783.62**	**$ 1,278.91**	**$ 1,774.17**	**$ 1,738.95**	**$ 1,705.93**	**$ 1,629.31**	**$ 1,599.87**	**$ 1,599.87**	**$ 1,599.87**	**$ 1,599.87**
	Gold Tier										
	IBM Mainframe Config - 1	$ 203 08	$ 292 48	$ 381 88	$ 373 33	$ 365 38	$ 348 73	$ 341 61	$ 341 61	$ 341 61	$ 341 61
	IBM Mainframe Config - 2	$ 178 45	$ 267 29	$ 356 13	$ 348 87	$ 342 14	$ 326 66	$ 320 64	$ 320 64	$ 320 64	$ 320 64
	IBM Mainframe Config - 3	$ 266 73	$ 404 68	$ 542 62	$ 526 03	$ 510 43	$ 486 54	$ 472 53	$ 472 53	$ 472 53	$ 472 53
	IBM AS400 Config 1	$ 22 16	$ 107 48	$ 192 79	$ 193 71	$ 194 74	$ 186 63	$ 187 60	$ 187 60	$ 187 60	$ 187 60
	IBM AS400 Config 2	$ 55 19	$ 147 69	$ 240 19	$ 239 43	$ 238 52	$ 228 78	$ 228 07	$ 228 07	$ 228 07	$ 228 07
sub-total IBM Mainfram Services - Gold		**$ 725.61**	**$ 1,219.62**	**$ 1,713.61**	**$ 1,681.37**	**$ 1,651.21**	**$ 1,577.34**	**$ 1,550.45**	**$ 1,550.45**	**$ 1,550.45**	**$ 1,550.45**
	Basic Tier										
	IBM Mainframe Config - 1	$ 192 93	$ 282 09	$ 371 26	$ 363 25	$ 355 80	$ 339 64	$ 332 98	$ 332 98	$ 332 98	$ 332 98
	IBM Mainframe Config - 2	$ 169 53	$ 258 16	$ 346 80	$ 340 01	$ 333 73	$ 318 66	$ 313 05	$ 313 05	$ 313 05	$ 313 05
	IBM Mainframe Config - 3	$ 248 90	$ 386 43	$ 523 95	$ 508 32	$ 493 61	$ 470 55	$ 457 35	$ 457 35	$ 457 35	$ 457 35
	IBM AS400 Config 1	$ 21 05	$ 106 35	$ 191 63	$ 192 61	$ 193 69	$ 185 63	$ 186 68	$ 186 68	$ 186 68	$ 186 68
	IBM AS400 Config 2	$ 52 97	$ 145 43	$ 237 87	$ 237 23	$ 236 44	$ 226 80	$ 226 19	$ 226 19	$ 226 19	$ 226 19
sub-total IBM Mainfram Services - Basic		**$ 685.38**	**$ 1,178.46**	**$ 1,671.51**	**$ 1,641.42**	**$ 1,613.27**	**$ 1,541.28**	**$ 1,516.25**	**$ 1,516.25**	**$ 1,516.25**	**$ 1,516.25**

Note: The Commonwealth has established mult

Baseline Units - Volumetrics

Price per unit \ per month

Resource Description	Service Tier / Configuration (6)	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Total - IBM Mainframe Services - All Support Tiers		**$ 2,194.61**	**$ 3,676.99**	**$ 5,159.29**	**$ 5,061.74**	**$ 4,970.41**	**$ 4,747.93**	**$ 4,666.57**	**$ 4,666.57**	**$ 4,666.57**	**$ 4,666.57**
Unisys Services											
	*** Unisys DASD	$ 0 14	$ 0 14	$ 0 14	$ 0 14	$ 0 14	$ 0 12	$ 0 12	$ 0 12	$ 0 12	$ 0 12
	Unisys Tapes in Storage - VTS	$ 0 07	$ 0 07	$ 0 07	$ 0 07	$ 0 07	$ 0 05	$ 0 05	$ 0 05	$ 0 05	$ 0 05
	Unisys Offsite Tape Storage	$ 0 38	$ 0 36	$ 0 35	$ 0 34	$ 0 33	$ 0 31	$ 0 31	$ 0 31	$ 0 31	$ 0 31
Total Unisys Services		**$ 0.59**	**$ 0.57**	**$ 0.56**	**$ 0.55**	**$ 0.54**	**$ 0.48**	**$ 0.48**	**$ 0.48**	**$ 0.48**	**$ 0.48**
Unisys Configurations											
	Platinum Tier										
	Unisys Mainframe Config - 1	$ 302 26	$ 301 47	$ 292 61	$ 293 40	$ 293 87	$ 287 84	$ 288 12	$ 288 12	$ 288 12	$ 288 12
	Unisys Mainframe Config - 2	$ 181 12	$ 183 09	$ 184 77	$ 186 55	$ 186 90	$ 177 59	$ 178 63	$ 178 63	$ 178 63	$ 178 63
	Unisys Mainframe Config - 3	$ 326 21	$ 325 10	$ 317 12	$ 317 29	$ 317 31	$ 310 48	$ 311 48	$ 311 48	$ 311 48	$ 311 48
	Unisys Mainframe Config - 4	$ 258 34	$ 260 06	$ 261 69	$ 263 39	$ 263 99	$ 253 53	$ 252 44	$ 252 44	$ 252 44	$ 252 44
sub-total Unisys Mainfram Services - Plantinum		**$ 1,067.93**	**$ 1,069.72**	**$ 1,056.19**	**$ 1,060.63**	**$ 1,062.07**	**$ 1,029.44**	**$ 1,030.67**	**$ 1,030.67**	**$ 1,030.67**	**$ 1,030.67**
	Gold Tier										
	Unisys Mainframe Config - 1	$ 302 02	$ 301 23	$ 292 39	$ 293 17	$ 293 64	$ 287 62	$ 287 90	$ 287 90	$ 287 90	$ 287 90
	Unisys Mainframe Config - 2	$ 181 12	$ 183 09	$ 184 77	$ 186 55	$ 186 90	$ 177 59	$ 178 63	$ 178 63	$ 178 63	$ 178 63
	Unisys Mainframe Config - 3	$ 326 18	$ 325 07	$ 317 09	$ 317 26	$ 317 28	$ 310 45	$ 311 45	$ 311 45	$ 311 45	$ 311 45
	Unisys Mainframe Config - 4	$ 258 34	$ 260 06	$ 261 69	$ 263 39	$ 263 99	$ 253 53	$ 252 44	$ 252 44	$ 252 44	$ 252 44
sub-total Unisys Mainfram Services - Gold		**$ 1,067.66**	**$ 1,069.45**	**$ 1,055.94**	**$ 1,060.37**	**$ 1,061.81**	**$ 1,029.19**	**$ 1,030.42**	**$ 1,030.42**	**$ 1,030.42**	**$ 1,030.42**
	Basic Tier										
	Unisys Mainframe Config - 1	$ 299 72	$ 298 96	$ 290 24	$ 291 04	$ 291 53	$ 285 51	$ 285 81	$ 285 81	$ 285 81	$ 285 81
	Unisys Mainframe Config - 2	$ 181 12	$ 183 10	$ 184 78	$ 186 49	$ 186 90	$ 177 59	$ 178 63	$ 178 63	$ 178 63	$ 178 63
	Unisys Mainframe Config - 3	$ 325 88	$ 324 77	$ 316 79	$ 316 97	$ 316 99	$ 310 17	$ 311 18	$ 311 18	$ 311 18	$ 311 18
	Unisys Mainframe Config - 4	$ 258 32	$ 260 06	$ 261 69	$ 263 39	$ 263 99	$ 253 53	$ 252 44	$ 252 44	$ 252 44	$ 252 44
sub-total Unisys Mainfram Services - Basic		**$ 1,065.04**	**$ 1,066.89**	**$ 1,053.50**	**$ 1,057.89**	**$ 1,059.41**	**$ 1,026.80**	**$ 1,028.06**	**$ 1,028.06**	**$ 1,028.06**	**$ 1,028.06**
Total - Unisys Mainframe Services - All Support Tiers		**$ 3,200.63**	**$ 3,206.06**	**$ 3,165.63**	**$ 3,178.89**	**$ 3,183.29**	**$ 3,085.43**	**$ 3,089.15**	**$ 3,089.15**	**$ 3,089.15**	**$ 3,089.15**
On-Demand (IaaS) (5)											
IaaS Servers - x86 (Windows, Linux) - Virtual Servers											
	IaaS Windows vConfig - 1	$ 25 81	$ 25 64	$ 25 64	$ 24 19	$ 21 82	$ 19 40	$ 17 30	$ 17 30	$ 17 30	$ 17 30
	IaaS Windows vConfig - 2	$ 31 67	$ 31 37	$ 31 38	$ 29 45	$ 26 45	$ 23 38	$ 20 64	$ 20 64	$ 20 64	$ 20 64
	IaaS Windows vConfig - 3	$ 52 27	$ 51 49	$ 51 48	$ 47 89	$ 42 66	$ 37 32	$ 32 38	$ 32 38	$ 32 38	$ 32 38
	IaaS Windows vConfig - 4	$ 131 40	$ 130 85	$ 130 61	$ 120 74	$ 106 79	$ 91 67	$ 78 68	$ 78 68	$ 78 68	$ 78 68
	IaaS Windows vConfig - 5	$ 58 61	$ 58 24	$ 58 19	$ 54 11	$ 48 15	$ 41 83	$ 36 32	$ 36 32	$ 36 32	$ 36 32
	IaaS Linux vConfig - 1	$ 66 82	$ 66 54	$ 66 44	$ 61 72	$ 54 85	$ 47 47	$ 41 17	$ 41 17	$ 41 17	$ 41 17
	IaaS Linux vConfig - 2	$ 72 68	$ 72 27	$ 72 18	$ 66 98	$ 59 48	$ 51 45	$ 44 51	$ 44 51	$ 44 51	$ 44 51
	IaaS Linux vConfig - 3	$ 93 28	$ 92 39	$ 92 28	$ 85 42	$ 75 69	$ 65 39	$ 56 25	$ 56 25	$ 56 25	$ 56 25
	IaaS Linux vConfig - 4	$ 213 41	$ 212 65	$ 212 21	$ 195 81	$ 172 85	$ 147 81	$ 126 42	$ 126 42	$ 126 42	$ 126 42
	IaaS Linux vConfig - 5	$ 140 63	$ 140 05	$ 139 79	$ 129 18	$ 114 21	$ 97 97	$ 84 06	$ 84 06	$ 84 06	$ 84 06
Total IaaS Servers - x86 (Windows, Linux) - Virtual Servers		**$ 886.53**	**$ 881.49**	**$ 880.20**	**$ 815.49**	**$ 722.95**	**$ 623.69**	**$ 537.73**	**$ 537.73**	**$ 537.73**	**$ 537.73**
IaaS Storage On-Demand											
	IaaS Storage Config - 1	$ 0 30	$ 0 30	$ 0 29	$ 0 27	$ 0 24	$ 0 21	$ 0 18	$ 0 18	$ 0 18	$ 0 18
	IaaS Storage Config - 2	$ 0 61	$ 0 59	$ 0 56	$ 0 53	$ 0 49	$ 0 45	$ 0 40	$ 0 40	$ 0 40	$ 0 40
	IaaS Storage Config - 3	$ 0 05	$ 0 06	$ 0 06	$ 0 05	$ 0 05	$ 0 05	$ 0 05	$ 0 05	$ 0 05	$ 0 05

Baseline Units - Volumetrics

Note: The Commonwealth has established mult

Price per unit \ per month

Resource Description	Service Tier / Configuration (6)	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Total IaaS Storage On-Demand		**$ 0.96**	**$ 0.95**	**$ 0.91**	**$ 0.85**	**$ 0.78**	**$ 0.71**	**$ 0.63**	**$ 0.63**	**$ 0.63**	**$ 0.63**
IaaS Backup On-Demand											
	IaaS Backup Config - 1	$ 0 02	$ 0 02	$ 0 02	$ 0 02	$ 0 01	$ 0 01	$ 0 01	$ 0 01	$ 0 01	$ 0 01
Total IaaS Backup On-Demand		**$ 0.02**	**$ 0.02**	**$ 0.02**	**$ 0.02**	**$ 0.01**	**$ 0.01**	**$ 0.01**	**$ 0.01**	**$ 0.01**	**$ 0.01**
Reserve Account											
		$ 84,000 00	$ 84,000 00	$ 84,000 00	$ 84,000 00	$ 84,000 00	$ 84,000 00	$ 84,000 00	$ 84,000 00	$ 84,000 00	$ 84,000 00
Reserve Account		**$ 84,000.00**	**$ 84,000.00**	**$ 84,000.00**	**$ 84,000.00**	**$ 84,000.00**	**$ 84,000.00**	**$ 84,000.00**	**$ 84,000.00**	**$ 84,000.00**	**$ 84,000.00**

Notes:

For purposes of submitting a proposal, Offerors should assume that tapes are equivalent in ca

* For purposes of submitting a proposal, Offerors should assume that the slower Tier1 RAID!

** The volume is expressed as native.

*** For purposes of evaluation DASD is expressed in Usable (not Raw)

Third Party Software

Third Party Software

Vendor	Product										

Baseline Units - Volumetrics

Note: The Commonwealth has established mult

Price per unit \ per month

Resource Description	Service Tier / Configuration (6)	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10

Baseline Units - Volumetrics

Note: The Commonwealth has established mult

Price per unit \ per month

Resource Description	Service Tier / Configuration (6)	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10

Baseline Units - Volumetrics

Note: The Commonwealth has established mult

Price per unit \ per month

Resource Description	Service Tier / Configuration (6)	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10

Baseline Units - Volumetrics

Note: The Commonwealth has established mult

Price per unit \ per month

Resource Description	Service Tier / Configuration (6)	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10

Baseline Units - Volumetrics

Note: The Commonwealth has established mult

Price per unit \ per month

Resource Description	Service Tier / Configuration (6)	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
A											
A											
	A A A										
	A A										
	A										
	A										
	A										
	A										
	A										
	A										
	A										
	A										
	A										
	A										

Baseline Units - Volumetrics

Note: The Commonwealth has established mult

Price per unit \ per month

Resource Description	Service Tier / Configuration (6)	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Hybrid Third Party Software											
Vendor	**Product**										

Baseline Units - Volumetrics

Note: The Commonwealth has established mult

Price per unit \ per month

Resource Description	Service Tier / Configuration (6)	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10

Baseline Units - Volumetrics

Note: The Commonwealth has established mult

Resource Description	Service Tier / Configuration (6)	Annual Costs Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Server - Fully Managed (1)											
x86 (Windows, Linux) - Physical Servers											
	Platinum Tier										
	Windows pConfig - 1	$ 189,374 76	$ 181,911 60	$ 167,495 04	$ 147,673 80	$ 124,307 04	$ 100,863 00	$ 81,645 60	$ 77,563 32	$ 73,481 04	$ 69,398 76
	Windows pConfig - 2	$ 169,698 60	$ 161,919 12	$ 154,171 08	$ 135,088 80	$ 112,944 36	$ 90,961 92	$ 73,001 40	$ 68,707 20	$ 64,413 00	$ 60,118 80
	Windows pConfig - 3	$ 111,830 88	$ 103,615 20	$ 102,604 32	$ 87,235 20	$ 70,759 92	$ 60,040 20	$ 46,041 60	$ 46,041 60	$ 41,437 44	$ 41,437 44
	Windows pConfig - 4	$ 23,258 88	$ 23,201 04	$ 23,143 20	$ 21,292 32	$ 18,738 24	$ 15,928 80	$ 6,768 48	$ 6,768 48	$ 6,768 48	$ 6,768 48
	Windows pConfig - 5	$ 21,511 92	$ 21,458 64	$ 21,405 12	$ 19,693 20	$ 17,330 88	$ 14,732 64	$ 6,260 16	$ 6,260 16	$ 6,260 16	$ 6,260 16
	Linux pConfig - 1	$ 89,075 52	$ 81,450 60	$ 81,246 00	$ 67,950 00	$ 59,798 40	$ 45,747 72	$ 38,882 16	$ 34,561 92	$ 34,561 92	$ 34,561 92
	Linux pConfig - 2	$ 62,298 24	$ 62,143 68	$ 54,239 64	$ 49,901 88	$ 43,917 72	$ 32,001 12	$ 27,192 96	$ 27,192 96	$ 22,660 80	$ 22,660 80
	Linux pConfig - 3	$ 50,382 00	$ 50,270 40	$ 41,498 40	$ 38,220 00	$ 33,811 20	$ 28,691 40	$ 19,368 48	$ 19,368 48	$ 19,368 48	$ 19,368 48
	Linux pConfig - 4	$ 24,847 68	$ 24,785 52	$ 24,723 84	$ 22,746 24	$ 20,017 92	$ 17,016 48	$ 7,230 72	$ 7,230 72	$ 7,230 72	$ 7,230 72
	Linux pConfig - 5	$ 23,100 72	$ 23,043 12	$ 22,985 76	$ 21,147 12	$ 18,610 56	$ 15,820 32	$ 6,722 28	$ 6,722 28	$ 6,722 28	$ 6,722 28
sub-total x86 (Windows, Linux) - Physical Servers - Plantinum		**$ 765,379.20**	**$ 733,798.92**	**$ 693,512.40**	**$ 610,948.56**	**$ 520,236.24**	**$ 421,803.60**	**$ 313,113.84**	**$ 300,417.12**	**$ 282,904.32**	**$ 274,527.84**
	Gold Tier										
	Windows pConfig - 1	$ 1,706,787 60	$ 1,619,163 60	$ 1,531,927 80	$ 1,339,203 60	$ 1,122,432 00	$ 906,391 20	$ 729,820 80	$ 693,329 76	$ 660,893 28	$ 624,402 24
	Windows pConfig - 2	$ 1,532,137 20	$ 1,455,199 44	$ 1,378,626 48	$ 1,201,269 00	$ 1,004,067 60	$ 813,389 04	$ 657,037 92	$ 622,906 08	$ 593,040 72	$ 563,175 36
	Windows pConfig - 3	$ 968,743 44	$ 919,068 00	$ 863,002 80	$ 758,746 80	$ 633,061 44	$ 510,013 92	$ 411,879 60	$ 388,997 40	$ 370,691 64	$ 352,385 88
	Windows pConfig - 4	$ 208,023 12	$ 195,978 72	$ 183,989 76	$ 158,693 40	$ 139,660 20	$ 110,806 08	$ 87,439 56	$ 87,439 56	$ 80,713 44	$ 73,987 32
	Windows pConfig - 5	$ 192,300 48	$ 181,168 32	$ 170,085 12	$ 146,700 00	$ 129,105 00	$ 102,432 96	$ 80,831 40	$ 80,831 40	$ 74,613 60	$ 68,395 80
	Linux pConfig - 1	$ 784,870 56	$ 746,679 96	$ 701,426 40	$ 618,688 08	$ 515,190 72	$ 418,027 68	$ 334,141 56	$ 317,223 00	$ 304,534 08	$ 287,615 52
	Linux pConfig - 2	$ 549,478 08	$ 517,662 24	$ 493,591 80	$ 433,156 80	$ 362,765 04	$ 292,709 76	$ 235,402 68	$ 222,078 00	$ 213,194 88	$ 199,870 20
	Linux pConfig - 3	$ 445,033 44	$ 419,379 12	$ 399,099 12	$ 345,071 76	$ 292,020 96	$ 236,532 24	$ 190,060 80	$ 180,557 76	$ 171,054 72	$ 161,551 68
	Linux pConfig - 4	$ 218,719 44	$ 206,052 24	$ 193,447 68	$ 166,852 80	$ 146,838 60	$ 116,501 28	$ 91,935 48	$ 91,935 48	$ 84,863 52	$ 77,791 56
	Linux pConfig - 5	$ 202,996 80	$ 191,241 84	$ 179,543 04	$ 154,859 40	$ 136,283 40	$ 108,128 16	$ 85,325 76	$ 85,325 76	$ 78,762 24	$ 72,198 72
sub-total x86 (Windows, Linux) - Physical Servers - Gold		**$ 6,809,090.16**	**$ 6,451,593.48**	**$ 6,094,740.00**	**$ 5,323,241.64**	**$ 4,481,424.96**	**$ 3,614,932.32**	**$ 2,903,875.56**	**$ 2,770,624.20**	**$ 2,632,362.12**	**$ 2,481,374.28**
	Silver Tier										
	Windows pConfig - 1	$ 1,888,485 12	$ 1,786,856 40	$ 1,692,558 00	$ 1,480,873 44	$ 1,241,690 40	$ 998,424 00	$ 808,176 00	$ 767,767 20	$ 727,358 40	$ 763,726 32
	Windows pConfig - 2	$ 1,724,518 08	$ 1,632,771 84	$ 1,548,705 96	$ 1,351,283 04	$ 1,130,365 44	$ 915,885 72	$ 735,734 40	$ 701,712 00	$ 667,689 60	$ 697,459 20
	Windows pConfig - 3	$ 1,076,712 00	$ 1,019,048 40	$ 962,115 84	$ 842,947 56	$ 707,691 60	$ 568,008 00	$ 456,276 00	$ 433,462 20	$ 410,648 40	$ 433,462 20
	Windows pConfig - 4	$ 207,185 04	$ 195,189 24	$ 183,248 64	$ 158,056 20	$ 139,096 80	$ 110,359 20	$ 87,088 56	$ 87,088 56	$ 80,389 44	$ 87,088 56
	Windows pConfig - 5	$ 191,462 40	$ 180,378 84	$ 169,344 00	$ 146,062 80	$ 128,541 60	$ 101,986 08	$ 80,480 40	$ 80,480 40	$ 74,289 60	$ 80,480 40
	Linux pConfig - 1	$ 861,048 00	$ 815,970 96	$ 771,081 12	$ 676,549 32	$ 566,479 20	$ 456,957 36	$ 367,498 56	$ 350,794 08	$ 334,089 60	$ 350,794 08
	Linux pConfig - 2	$ 904,766 40	$ 857,394 00	$ 810,233 28	$ 710,934 84	$ 595,302 96	$ 480,248 28	$ 386,147 52	$ 368,595 36	$ 351,043 20	$ 368,595 36
	Linux pConfig - 3	$ 195,586 56	$ 187,023 12	$ 177,173 04	$ 155,766 24	$ 131,256 00	$ 105,805 68	$ 84,564 00	$ 79,866 00	$ 75,168 00	$ 79,866 00
	Linux pConfig - 4	$ 215,330 40	$ 202,859 64	$ 190,450 56	$ 164,268 00	$ 144,565 20	$ 114,696 96	$ 90,511 20	$ 90,511 20	$ 83,548 80	$ 90,511 20
	Linux pConfig - 5	$ 199,607 76	$ 188,049 24	$ 176,545 92	$ 152,274 60	$ 134,010 00	$ 106,323 84	$ 83,901 48	$ 83,901 48	$ 77,447 52	$ 83,901 48
sub-total x86 (Windows, Linux) - Physical Servers - Silver		**$ 7,464,701.76**	**$ 7,065,541.68**	**$ 6,681,456.36**	**$ 5,839,016.04**	**$ 4,918,999.20**	**$ 3,958,695.12**	**$ 3,180,378.12**	**$ 3,044,178.48**	**$ 2,881,672.56**	**$ 3,035,884.80**
	Bronze Tier										
	Windows pConfig - 1	$ 832,089 60	$ 788,542 56	$ 745,161 12	$ 653,806 92	$ 547,439 76	$ 441,601 20	$ 355,153 92	$ 339,010 56	$ 322,867 20	$ 306,723 84
	Windows pConfig - 2	$ 875,808 00	$ 829,965 60	$ 784,313 28	$ 688,192 44	$ 576,263 52	$ 464,892 12	$ 373,802 88	$ 356,811 84	$ 339,820 80	$ 322,829 76
	Windows pConfig - 3	$ 371,681 64	$ 355,087 80	$ 328,159 44	$ 287,865 60	$ 242,003 76	$ 194,529 60	$ 159,520 20	$ 150,404 76	$ 141,289 32	$ 136,731 60
	Windows pConfig - 4	$ 91,925 76	$ 91,698 24	$ 80,035 20	$ 73,634 40	$ 64,801 80	$ 47,216 88	$ 40,126 32	$ 40,126 32	$ 33,438 60	$ 33,438 60
	Windows pConfig - 5	$ 31,851 72	$ 31,773 24	$ 31,693 68	$ 29,158 92	$ 17,107 44	$ 14,542 80	$ 12,358 80	$ 12,358 80	$ 12,358 80	$ 12,358 80
	Linux pConfig - 1	$ 535,149 00	$ 505,346 76	$ 482,786 40	$ 418,030 08	$ 350,635 32	$ 283,390 32	$ 228,406 20	$ 215,947 68	$ 207,642 00	$ 195,183 48
	Linux pConfig - 2	$ 562,473 00	$ 531,145 32	$ 507,437 76	$ 439,395 84	$ 368,576 64	$ 297,915 84	$ 240,061 80	$ 226,967 52	$ 218,238 00	$ 205,143 72

Note: The Commonwealth has established mult

Baseline Units - Volumetrics

Resource Description	Service Tier / Configuration (6)	Annual Costs Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
	Linux pConfig - 3	$ 162,187 20	$ 153,735 84	$ 144,242 64	$ 125,472 24	$ 104,488 32	$ 83,118 60	$ 70,120 80	$ 65,446 08	$ 60,771 36	$ 60,771 36
	Linux pConfig - 4	$ 47,522 88	$ 47,403 84	$ 47,285 76	$ 32,627 88	$ 28,714 32	$ 24,409 08	$ 20,743 56	$ 20,743 56	$ 20,743 56	$ 20,743 56
	Linux pConfig - 5	$ 22,014 48	$ 21,959 52	$ 21,904 80	$ 20,152 80	$ 17,735 52	$ 15,076 56	$ 6,406 08	$ 6,406 08	$ 6,406 08	$ 6,406 08
sub-total x86 (Windows, Linux) - Physical Servers - Bronze		**$ 3,532,703.28**	**$ 3,356,658.72**	**$ 3,173,020.08**	**$ 2,768,337.12**	**$ 2,317,766.40**	**$ 1,866,693.00**	**$ 1,506,700.56**	**$ 1,434,223.20**	**$ 1,363,575.72**	**$ 1,300,330.80**
	Basic Tier										
	Windows pConfig - 1	$ 1,660,492 80	$ 1,573,555 68	$ 1,493,888 76	$ 1,304,696 88	$ 1,086,859 80	$ 881,238 24	$ 708,723 84	$ 676,509 12	$ 640,267 56	$ 608,052 84
	Windows pConfig - 2	$ 1,747,929 60	$ 1,656,401 76	$ 1,572,555 60	$ 1,373,467 92	$ 1,144,213 20	$ 927,820 08	$ 746,021 76	$ 712,111 68	$ 673,962 84	$ 640,052 76
	Windows pConfig - 3	$ 868,203 60	$ 826,912 80	$ 771,998 04	$ 675,153 12	$ 572,043 60	$ 458,408 40	$ 368,446 32	$ 350,251 44	$ 332,056 56	$ 313,861 68
	Windows pConfig - 4	$ 194,905 68	$ 182,985 60	$ 171,120 60	$ 157,433 40	$ 129,314 64	$ 102,073 92	$ 80,072 64	$ 80,072 64	$ 73,399 92	$ 73,399 92
	Windows pConfig - 5	$ 74,140 92	$ 73,957 80	$ 63,234 00	$ 58,176 00	$ 51,198 48	$ 36,268 80	$ 30,822 00	$ 30,822 00	$ 30,822 00	$ 24,657 60
	Linux pConfig - 1	$ 674,104 80	$ 637,038 00	$ 607,208 16	$ 526,143 60	$ 440,156 64	$ 359,568 96	$ 289,086 00	$ 272,566 80	$ 260,177 40	$ 247,788 00
	Linux pConfig - 2	$ 708,715 20	$ 669,740 40	$ 638,384 88	$ 553,184 64	$ 462,803 88	$ 378,101 52	$ 303,920 40	$ 286,553 52	$ 273,528 36	$ 260,503 20
	Linux pConfig - 3	$ 64,559 04	$ 64,416 00	$ 55,819 68	$ 51,412 20	$ 45,491 04	$ 33,085 44	$ 27,910 08	$ 27,910 08	$ 23,258 40	$ 23,258 40
	Linux pConfig - 4	$ 106,223 40	$ 105,957 72	$ 93,950 40	$ 86,435 52	$ 66,559 92	$ 56,579 88	$ 48,084 12	$ 41,214 96	$ 41,214 96	$ 41,214 96
	Linux pConfig - 5	$ 54,645 60	$ 54,509 40	$ 54,373 80	$ 40,019 52	$ 35,219 52	$ 29,939 04	$ 25,442 88	$ 19,082 16	$ 19,082 16	$ 19,082 16
sub-total x86 (Windows, Linux) - Physical Servers - Basic		**$ 6,153,920.64**	**$ 5,845,475.16**	**$ 5,522,533.92**	**$ 4,826,122.80**	**$ 4,033,860.72**	**$ 3,263,084.28**	**$ 2,628,530.04**	**$ 2,497,094.40**	**$ 2,367,770.16**	**$ 2,251,871.52**
Total - Fully Managed - x86 Physical - All Support Tiers (Window, Linux)		###########	###########	###########	###########	###########	###########	###########	###########	**$ 9,528,284.88**	**$ 9,343,989.24**
x86 (Windows, Linux) - Virtual Servers											
	Platinum Tier										
	Windows vConfig - 1	$ 132,938 40	$ 137,334 72	$ 146,437 80	$ 139,069 44	$ 130,025 52	$ 117,028 80	$ 104,998 56	$ 107,761 68	$ 113,287 92	$ 118,814 16
	Windows vConfig - 2	$ 110,816 76	$ 115,306 56	$ 119,817 00	$ 119,044 08	$ 108,635 52	$ 95,658 24	$ 86,899 20	$ 89,702 40	$ 95,308 80	$ 100,915 20
	Windows vConfig - 3	$ 70,914 48	$ 75,688 20	$ 75,508 20	$ 74,085 12	$ 69,264 12	$ 62,385 12	$ 55,937 52	$ 58,881 60	$ 61,825 68	$ 64,769 76
	Windows vConfig - 4	$ 19,828 44	$ 19,773 72	$ 19,724 76	$ 18,146 16	$ 21,291 36	$ 18,100 80	$ 15,382 56	$ 15,382 56	$ 15,382 56	$ 19,228 20
	Windows vConfig - 5	$ 11,472 00	$ 11,439 84	$ 11,411 76	$ 10,498 32	$ 9,238 32	$ 11,781 36	$ 10,011 96	$ 10,011 96	$ 10,011 96	$ 10,011 96
	Linux vConfig - 1	$ 64,834 56	$ 70,056 48	$ 69,881 76	$ 69,236 16	$ 65,278 80	$ 55,488 60	$ 50,309 76	$ 53,454 12	$ 56,598 48	$ 59,742 84
	Linux vConfig - 2	$ 54,732 00	$ 60,034 92	$ 59,888 40	$ 60,102 72	$ 52,889 76	$ 48,711 00	$ 41,397 72	$ 44,582 16	$ 47,766 60	$ 50,951 04
	Linux vConfig - 3	$ 34,322 40	$ 34,194 96	$ 39,799 20	$ 36,608 88	$ 32,214 00	$ 31,314 24	$ 26,602 56	$ 26,602 56	$ 29,927 88	$ 29,927 88
	Linux vConfig - 4	$ 16,836 72	$ 16,791 12	$ 16,749 84	$ 15,409 20	$ 13,560 00	$ 17,290 80	$ 14,695 92	$ 14,695 92	$ 14,695 92	$ 14,695 92
	Linux vConfig - 5	$ 7,545 00	$ 7,524 36	$ 7,505 88	$ 6,905 04	$ 6,076 32	$ 5,165 52	$ 4,390 32	$ 4,390 32	$ 4,390 32	$ 8,780 64
sub-total x86 (Windows, Linux) - Virtual Servers - Platinum		**$ 524,240.76**	**$ 548,144.88**	**$ 566,724.60**	**$ 549,105.12**	**$ 508,473.72**	**$ 462,924.48**	**$ 410,626.08**	**$ 425,465.28**	**$ 449,196.12**	**$ 477,837.60**
	Gold Tier										
	Windows vConfig - 1	$ 1,152,314 40	$ 1,205,882 88	$ 1,263,955 68	$ 1,219,018 32	$ 1,129,788 00	$ 1,005,662 04	$ 898,752 96	$ 942,728 64	$ 989,452 80	$ 1,041,673 92
	Windows vConfig - 2	$ 977,755 68	$ 1,022,757 36	$ 1,072,710 00	$ 1,035,067 68	$ 957,170 88	$ 853,164 00	$ 761,276 88	$ 800,316 72	$ 839,356 56	$ 881,184 96
	Windows vConfig - 3	$ 614,894 64	$ 642,647 04	$ 676,188 00	$ 649,609 56	$ 600,003 84	$ 537,994 08	$ 477,498 72	$ 503,863 68	$ 527,299 20	$ 553,664 16
	Windows vConfig - 4	$ 157,417 92	$ 163,524 00	$ 169,646 88	$ 168,070 56	$ 153,182 64	$ 139,209 84	$ 122,123 52	$ 129,756 24	$ 133,572 60	$ 141,205 32
	Windows vConfig - 5	$ 90,969 60	$ 96,383 88	$ 101,805 12	$ 98,856 24	$ 86,991 12	$ 77,851 20	$ 69,468 84	$ 76,084 92	$ 79,392 96	$ 82,701 00
	Linux vConfig - 1	$ 570,875 04	$ 595,758 60	$ 625,821 00	$ 604,785 00	$ 557,745 60	$ 499,433 04	$ 446,049 00	$ 467,582 40	$ 492,192 00	$ 516,801 60
	Linux vConfig - 2	$ 455,277 00	$ 475,345 44	$ 500,820 72	$ 480,337 20	$ 444,255 48	$ 396,018 72	$ 355,255 92	$ 373,953 60	$ 392,651 28	$ 411,348 96
	Linux vConfig - 3	$ 302,583 60	$ 318,196 80	$ 334,144 80	$ 322,728 84	$ 297,506 88	$ 264,554 28	$ 234,515 52	$ 247,544 16	$ 260,572 80	$ 273,601 44
	Linux vConfig - 4	$ 106,395 12	$ 114,268 56	$ 113,988 00	$ 112,354 20	$ 105,461 76	$ 95,257 80	$ 80,961 48	$ 85,723 92	$ 90,486 36	$ 95,248 80
	Linux vConfig - 5	$ 65,797 92	$ 65,617 56	$ 72,729 60	$ 66,907 20	$ 64,764 48	$ 55,058 52	$ 51,049 44	$ 55,303 56	$ 55,303 56	$ 59,557 68
sub-total x86 (Windows, Linux) - Virtual Servers - Gold		**$ 4,494,280.92**	**$ 4,700,382.12**	**$ 4,931,809.80**	**$ 4,757,734.80**	**$ 4,396,870.68**	**$ 3,924,203.52**	**$ 3,496,952.28**	**$ 3,682,857.84**	**$ 3,860,280.12**	**$ 4,056,987.84**
	Silver Tier										
	Windows vConfig - 1	$ 1,278,312 96	$ 1,340,676 48	$ 1,402,740 00	$ 1,355,054 40	$ 1,252,967 40	$ 1,116,618 24	$ 998,289 60	$ 1,047,520 32	$ 1,099,486 08	$ 1,154,186 88
	Windows vConfig - 2	$ 1,106,640 00	$ 1,160,571 36	$ 1,214,638 08	$ 1,174,152 72	$ 1,083,150 72	$ 966,641 28	$ 863,062 32	$ 904,689 12	$ 951,866 16	$ 999,043 20

Note: The Commonwealth has established mult

Baseline Units - Volumetrics

Resource Description	Service Tier / Configuration (6)	Annual Costs Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
	Windows vConfig - 3	$ 682,339 20	$ 714,696 84	$ 747,882 00	$ 720,027 12	$ 665,854 20	$ 597,335 04	$ 530,712 00	$ 556,956 00	$ 586,116 00	$ 615,276 00
	Windows vConfig - 4	$ 156,314 88	$ 162,378 00	$ 168,458 16	$ 166,894 56	$ 152,110 80	$ 138,235 20	$ 121,267 20	$ 128,846 40	$ 132,636 00	$ 140,215 20
	Windows vConfig - 5	$ 90,234 24	$ 95,604 60	$ 100,982 16	$ 98,058 24	$ 86,288 88	$ 77,222 40	$ 68,906 88	$ 75,469 44	$ 78,750 72	$ 82,032 00
	Linux vConfig - 1	$ 622,742 40	$ 652,186 08	$ 681,531 84	$ 660,261 12	$ 610,274 16	$ 543,621 24	$ 486,245 76	$ 510,407 04	$ 534,568 32	$ 561,749 76
	Linux vConfig - 2	$ 515,464 32	$ 540,218 52	$ 565,056 00	$ 543,891 60	$ 504,026 88	$ 450,105 00	$ 400,891 44	$ 422,313 12	$ 443,734 80	$ 465,156 48
	Linux vConfig - 3	$ 330,422 40	$ 345,635 64	$ 361,231 20	$ 347,379 12	$ 323,392 92	$ 290,145 24	$ 256,089 60	$ 268,894 08	$ 284,899 68	$ 297,704 16
	Linux vConfig - 4	$ 103,891 32	$ 111,578 88	$ 111,303 36	$ 109,708 20	$ 102,979 20	$ 93,013 80	$ 79,054 08	$ 83,704 32	$ 88,354 56	$ 93,004 80
	Linux vConfig - 5	$ 64,064 52	$ 63,888 48	$ 70,812 00	$ 65,143 20	$ 63,057 72	$ 53,606 52	$ 49,703 04	$ 53,844 96	$ 53,844 96	$ 57,986 88
sub-total x86 (Windows, Linux) - Virtual Servers - Silver		**$ 4,950,426.24**	**$ 5,187,434.88**	**$ 5,424,634.80**	**$ 5,240,570.28**	**$ 4,844,102.88**	**$ 4,326,543.96**	**$ 3,854,221.92**	**$ 4,052,644.80**	**$ 4,254,257.28**	**$ 4,466,355.36**
	Bronze Tier										
	Windows vConfig - 1	$ 426,688 08	$ 448,980 48	$ 466,512 00	$ 450,651 60	$ 419,220 36	$ 372,415 68	$ 332,913 60	$ 349,286 40	$ 365,659 20	$ 384,760 80
	Windows vConfig - 2	$ 433,087 20	$ 455,581 44	$ 473,400 00	$ 457,279 20	$ 425,387 52	$ 377,955 84	$ 337,803 36	$ 354,416 64	$ 371,029 92	$ 390,412 08
	Windows vConfig - 3	$ 220,281 60	$ 229,405 68	$ 243,784 80	$ 233,392 32	$ 213,422 52	$ 191,829 12	$ 171,675 84	$ 180,405 12	$ 189,134 40	$ 197,863 68
	Windows vConfig - 4	$ 6,491 64	$ 6,473 76	$ 6,457 68	$ 5,940 84	$ 5,227 92	$ 4,444 56	$ 3,777 12	$ 3,777 12	$ 3,777 12	$ 7,554 24
	Windows vConfig - 5	$ 5,618 16	$ 5,602 44	$ 5,588 64	$ 5,141 28	$ 4,524 24	$ 3,846 48	$ 3,268 80	$ 3,268 80	$ 3,268 80	$ 6,537 60
	Linux vConfig - 1	$ 195,601 20	$ 205,368 00	$ 215,097 12	$ 207,308 64	$ 190,721 52	$ 169,171 20	$ 152,779 68	$ 158,771 04	$ 167,758 08	$ 176,745 12
	Linux vConfig - 2	$ 198,273 36	$ 208,118 40	$ 217,990 08	$ 210,085 92	$ 193,277 28	$ 171,463 68	$ 154,823 76	$ 160,895 28	$ 170,002 56	$ 179,109 84
	Linux vConfig - 3	$ 98,368 56	$ 103,443 60	$ 108,628 80	$ 104,915 16	$ 96,716 40	$ 86,007 12	$ 76,239 36	$ 79,416 00	$ 85,769 28	$ 88,945 92
	Linux vConfig - 4	$ 7,907 52	$ 7,886 04	$ 7,866 60	$ 7,236 96	$ 6,368 40	$ 5,413 80	$ 4,601 28	$ 4,601 28	$ 4,601 28	$ 9,202 56
	Linux vConfig - 5	$ 7,034 16	$ 7,014 84	$ 6,997 56	$ 6,437 40	$ 5,664 72	$ 4,815 72	$ 4,092 96	$ 4,092 96	$ 4,092 96	$ 8,185 92
sub-total x86 (Windows, Linux) - Virtual Servers - Bronze		**$ 1,599,351.48**	**$ 1,677,874.68**	**$ 1,752,323.28**	**$ 1,688,389.32**	**$ 1,560,530.88**	**$ 1,387,363.20**	**$ 1,241,975.76**	**$ 1,298,930.64**	**$ 1,365,093.60**	**$ 1,449,317.76**
	Basic Tier										
	Windows vConfig - 1	$ 846,841 08	$ 886,669 20	$ 930,984 00	$ 899,337 60	$ 829,065 60	$ 740,013 12	$ 661,640 40	$ 694,314 00	$ 726,987 60	$ 765,106 80
	Windows vConfig - 2	$ 859,569 00	$ 899,733 60	$ 944,760 00	$ 912,592 80	$ 841,288 80	$ 751,045 68	$ 671,379 84	$ 704,534 40	$ 737,688 96	$ 776,369 28
	Windows vConfig - 3	$ 449,658 00	$ 472,803 60	$ 491,535 00	$ 474,963 84	$ 438,023 04	$ 393,134 40	$ 351,354 96	$ 368,777 52	$ 386,200 08	$ 406,526 40
	Windows vConfig - 4	$ 6,471 00	$ 6,453 24	$ 6,437 28	$ 5,922 00	$ 5,211 36	$ 4,430 40	$ 3,765 12	$ 3,765 12	$ 3,765 12	$ 7,530 24
	Windows vConfig - 5	$ 5,597 52	$ 5,581 92	$ 5,568 24	$ 5,122 44	$ 4,507 68	$ 3,832 32	$ 3,256 80	$ 3,256 80	$ 3,256 80	$ 6,513 60
	Linux vConfig - 1	$ 408,700 80	$ 428,037 12	$ 447,289 92	$ 434,882 88	$ 399,147 24	$ 356,783 76	$ 318,136 68	$ 335,976 12	$ 350,842 32	$ 368,681 76
	Linux vConfig - 2	$ 414,326 40	$ 433,812 96	$ 453,351 36	$ 440,753 04	$ 404,536 56	$ 361,655 28	$ 322,425 24	$ 340,505 16	$ 355,571 76	$ 373,651 68
	Linux vConfig - 3	$ 217,051 20	$ 227,046 96	$ 237,288 48	$ 228,185 76	$ 213,885 00	$ 189,358 92	$ 170,326 80	$ 176,635 20	$ 186,097 80	$ 195,560 40
	Linux vConfig - 4	$ 7,830 24	$ 7,808 88	$ 7,789 68	$ 7,166 28	$ 6,306 24	$ 5,360 88	$ 4,556 28	$ 4,556 28	$ 4,556 28	$ 9,112 56
	Linux vConfig - 5	$ 6,956 88	$ 6,937 68	$ 6,920 64	$ 6,366 72	$ 5,602 56	$ 4,762 80	$ 4,047 96	$ 4,047 96	$ 4,047 96	$ 8,095 92
sub-total x86 (Windows, Linux) - Virtual Servers - Basic		**$ 3,223,002.12**	**$ 3,374,885.16**	**$ 3,531,924.60**	**$ 3,415,293.36**	**$ 3,147,574.08**	**$ 2,810,377.56**	**$ 2,510,890.08**	**$ 2,636,368.56**	**$ 2,759,014.68**	**$ 2,917,148.64**
Total - Fully Managed - x86 Virtual - All Support Tiers (Window, Linux)		############	############	############	############	############	############	############	############	############	############
UNIX (IBM P-Series, AIX)											
	Platinum Tier										
	AIX Config - 1	$ 401,211 36	$ 429,100 56	$ 457,262 40	$ 486,924 48	$ 518,195 04	$ 522,263 76	$ 539,786 88	$ 573,523 56	$ 596,014 68	$ 629,751 36
	AIX Config - 2	$ 304,970 64	$ 320,623 92	$ 348,361 92	$ 365,180 40	$ 395,366 40	$ 393,346 80	$ 412,965 00	$ 436,563 00	$ 448,362 00	$ 471,960 00
	AIX Config - 3	$ 225,281 52	$ 240,337 08	$ 255,501 60	$ 271,388 88	$ 288,303 84	$ 291,342 84	$ 301,055 04	$ 313,599 00	$ 338,686 92	$ 351,230 88
	AIX Config - 4	$ 110,096 40	$ 110,700 00	$ 133,457 76	$ 134,366 40	$ 135,451 44	$ 132,804 72	$ 154,118 16	$ 154,118 16	$ 154,118 16	$ 176,135 04
	AIX Config - 5	$ 100,854 60	$ 101,132 40	$ 121,574 88	$ 122,037 84	$ 122,634 00	$ 119,521 44	$ 138,014 52	$ 138,014 52	$ 138,014 52	$ 157,730 88
sub-total P-Series (AIX) - Bronze		**$ 1,142,414.52**	**$ 1,201,893.96**	**$ 1,316,158.56**	**$ 1,379,898.00**	**$ 1,459,950.72**	**$ 1,459,279.56**	**$ 1,545,939.60**	**$ 1,615,818.24**	**$ 1,675,196.28**	**$ 1,786,808.16**
	Gold Tier										
	AIX Config - 1	$ 352,287 36	$ 378,151 68	$ 404,404 80	$ 432,285 84	$ 461,831 04	$ 463,806 96	$ 479,272 32	$ 509,226 84	$ 529,196 52	$ 559,151 04
	AIX Config - 2	$ 269,621 04	$ 284,151 24	$ 309,462 48	$ 325,245 60	$ 353,088 00	$ 350,079 84	$ 367,781 40	$ 388,797 48	$ 399,305 52	$ 420,321 60

Note: The Commonwealth has established mult

Baseline Units - Volumetrics

Resource Description	Service Tier / Configuration (6)	Annual Costs Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
	AIX Config - 3	$ 200,828 16	$ 214,871 76	$ 229,080 00	$ 244,069 56	$ 259,902 72	$ 261,885 36	$ 270,558 72	$ 281,832 00	$ 304,378 56	$ 315,651 84
	AIX Config - 4	$ 96,485 40	$ 97,187 40	$ 117,362 16	$ 118,390 32	$ 119,597 76	$ 117,072 00	$ 136,045 56	$ 136,045 56	$ 136,045 56	$ 155,480 64
	AIX Config - 5	$ 87,243 60	$ 87,619 80	$ 105,479 28	$ 106,061 76	$ 106,780 32	$ 103,788 72	$ 119,941 92	$ 119,941 92	$ 119,941 92	$ 137,076 48
sub-total P-Series (AIX) - Gold		**$ 1,006,465.56**	**$ 1,061,981.88**	**$ 1,165,788.72**	**$ 1,226,053.08**	**$ 1,301,199.84**	**$ 1,296,632.88**	**$ 1,373,599.92**	**$ 1,435,843.80**	**$ 1,488,868.08**	**$ 1,587,681.60**
	Silver Tier										
	AIX Config - 1	$ 621,311 04	$ 669,024 96	$ 708,677 40	$ 760,515 72	$ 825,147 84	$ 825,549 12	$ 853,009 92	$ 897,437 52	$ 941,865 12	$ 995,178 24
	AIX Config - 2	$ 479,088 48	$ 515,651 40	$ 543,294 36	$ 582,703 20	$ 625,242 24	$ 628,261 92	$ 660,021 60	$ 688,308 24	$ 726,023 76	$ 763,739 28
	AIX Config - 3	$ 354,542 40	$ 380,331 36	$ 406,516 80	$ 434,337 12	$ 463,890 24	$ 465,772 08	$ 481,080 96	$ 511,148 52	$ 531,193 56	$ 561,261 12
	AIX Config - 4	$ 169,783 20	$ 188,521 08	$ 190,090 56	$ 209,668 32	$ 212,569 92	$ 225,334 20	$ 224,599 44	$ 241,876 32	$ 259,153 20	$ 276,430 08
	AIX Config - 5	$ 151,299 60	$ 167,472 36	$ 168,305 28	$ 185,011 20	$ 186,935 04	$ 196,553 76	$ 194,692 68	$ 209,669 04	$ 224,645 40	$ 239,621 76
sub-total P-Series (AIX) - Silver		**$ 1,776,024.72**	**$ 1,921,001.16**	**$ 2,016,884.40**	**$ 2,172,235.56**	**$ 2,313,785.28**	**$ 2,341,471.08**	**$ 2,413,404.60**	**$ 2,548,439.64**	**$ 2,682,881.04**	**$ 2,836,230.48**
	Bronze Tier										
	AIX Config - 1	$ 179,363 52	$ 191,364 00	$ 203,604 96	$ 224,931 84	$ 239,458 80	$ 243,779 04	$ 249,158 40	$ 264,730 80	$ 272,517 00	$ 288,089 40
	AIX Config - 2	$ 193,406 40	$ 205,938 00	$ 218,712 00	$ 241,150 56	$ 256,225 44	$ 261,642 48	$ 267,513 60	$ 284,233 20	$ 292,593 00	$ 309,312 60
	AIX Config - 3	$ 70,747 20	$ 72,092 16	$ 82,570 32	$ 84,268 08	$ 95,748 00	$ 91,675 20	$ 99,818 40	$ 99,818 40	$ 108,892 80	$ 108,892 80
	AIX Config - 4	$ 29,323 44	$ 29,719 92	$ 30,083 76	$ 30,547 68	$ 31,071 12	$ 45,525 24	$ 45,416 16	$ 45,416 16	$ 45,416 16	$ 45,416 16
	AIX Config - 5	$ 25,626 72	$ 25,892 88	$ 26,122 80	$ 26,438 16	$ 26,798 64	$ 38,883 60	$ 38,514 60	$ 38,514 60	$ 38,514 60	$ 38,514 60
sub-total P-Series (AIX) - Bronze		**$ 498,467.28**	**$ 525,006.96**	**$ 561,093.84**	**$ 607,336.32**	**$ 649,302.00**	**$ 681,505.56**	**$ 700,421.16**	**$ 732,713.16**	**$ 757,933.56**	**$ 790,225.56**
	Basic Tier										
	AIX Config - 1	$ 404,482 56	$ 435,969 00	$ 475,083 72	$ 510,875 28	$ 556,742 16	$ 553,873 92	$ 575,071 68	$ 601,819 20	$ 635,253 60	$ 662,001 12
	AIX Config - 2	$ 441,899 52	$ 475,019 28	$ 516,337 56	$ 553,739 04	$ 601,838 64	$ 601,105 92	$ 624,390 96	$ 653,432 40	$ 689,734 20	$ 718,775 64
	AIX Config - 3	$ 246,036 48	$ 267,358 32	$ 281,219 40	$ 304,641 72	$ 329,757 48	$ 330,378 00	$ 342,933 60	$ 358,884 00	$ 374,834 40	$ 398,760 00
	AIX Config - 4	$ 123,466 80	$ 138,181 56	$ 140,388 60	$ 156,176 64	$ 159,559 20	$ 168,431 64	$ 168,217 92	$ 181,157 76	$ 194,097 60	$ 207,037 44
	AIX Config - 5	$ 104,983 20	$ 117,132 84	$ 118,603 32	$ 131,519 52	$ 133,924 32	$ 139,651 20	$ 138,311 16	$ 148,950 48	$ 159,589 80	$ 170,229 12
sub-total P-Series (AIX) - Basic		**$ 1,320,868.56**	**$ 1,433,661.00**	**$ 1,531,632.60**	**$ 1,656,952.20**	**$ 1,781,821.80**	**$ 1,793,440.68**	**$ 1,848,925.32**	**$ 1,944,243.84**	**$ 2,053,509.60**	**$ 2,156,803.32**
Total - Fully Managed - P-Series (AIX) - All Support Tiers (Window, Linux)		**$ 5,744,240.64**	**$ 6,143,544.96**	**$ 6,591,558.12**	**$ 7,042,475.16**	**$ 7,506,059.64**	**$ 7,572,329.76**	**$ 7,882,290.60**	**$ 8,277,058.68**	**$ 8,658,388.56**	**$ 9,157,749.12**
Server - Managed Only (2)											
x86 (Windows, Linux)											
	Platinum Tier	$ 523,068 00	$ 313,063 20	$ 187,367 04	$ 105,341 28	$ 210,684 00	$ 179,082 00	$ 152,220 00	$ 152,220 00	$ 152,220 00	$ 152,220 00
	Gold Tier	$ 4,567,536 00	$ 2,733,717 60	$ 1,636,148 16	$ 901,285 20	$ 204,414 00	$ 173,754 00	$ 147,690 00	$ 147,690 00	$ 147,690 00	$ 147,690 00
	Silver Tier	$ 4,983,120 00	$ 2,982,456 00	$ 1,784,980 80	$ 985,322 88	$ 200,712 00	$ 170,604 00	$ 145,014 00	$ 145,014 00	$ 145,014 00	$ 145,014 00
	Bronze Tier	$ 3,707,280 00	$ 2,218,806 00	$ 1,327,978 80	$ 733,043 52	$ 199,098 00	$ 169,230 00	$ 143,850 00	$ 143,850 00	$ 143,850 00	$ 143,850 00
	Basic Tier	$ 5,148,738 00	$ 3,081,531 60	$ 1,844,337 60	$ 1,018,966 68	$ 197,508 00	$ 167,880 00	$ 142,698 00	$ 142,698 00	$ 142,698 00	$ 142,698 00
Total Managed Only- x86 - All Support Tiers (Window, Linux)		**$ 18,929,742.00**	**$ 11,329,574.40**	**$ 6,780,812.40**	**$ 3,743,959.56**	**$ 1,012,416.00**	**$ 860,550.00**	**$ 731,472.00**	**$ 731,472.00**	**$ 731,472.00**	**$ 731,472.00**
UNIX (IBM P-Series, AIX)											
	Platinum	$ 43,681 44	$ 26,750 05	$ 18,201 60	$ 92,887 20	$ 94,977 60	$ 90,900 00	$ 89,985 60	$ 89,985 60	$ 89,985 60	$ 89,985 60
	Gold Tier	$ 122,075 99	$ 74,958 43	$ 42,617 40	$ 87,228 00	$ 89,430 00	$ 85,465 20	$ 84,663 60	$ 84,663 60	$ 84,663 60	$ 84,663 60
	Silver Tier	$ 226,867 67	$ 139,532 97	$ 87,407 76	$ 81,453 60	$ 83,655 60	$ 79,692 00	$ 78,891 60	$ 78,891 60	$ 78,891 60	$ 78,891 60
	Bronze Tier	$ 274,985 63	$ 169,765 50	$ 101,895 36	$ 74,888 40	$ 77,203 20	$ 73,353 60	$ 72,663 60	$ 72,663 60	$ 72,663 60	$ 72,663 60
	Basic Tier	$ 166,353 64	$ 103,522 84	$ 65,615 88	$ 61,868 40	$ 64,297 20	$ 60,560 40	$ 59,985 60	$ 59,985 60	$ 59,985 60	$ 59,985 60
Total Managed Only- P-Series - All Support Tiers (AIX)		**$ 833,964.37**	**$ 514,529.78**	**$ 315,738.00**	**$ 398,325.60**	**$ 409,563.60**	**$ 389,971.20**	**$ 386,190.00**	**$ 386,190.00**	**$ 386,190.00**	**$ 386,190.00**
Storage and Backup - Fully Managed (1)											

Note: The Commonwealth has established mult

Baseline Units - Volumetrics

Resource Description	Service Tier / Configuration (6)	Annual Costs Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Enterprise Storage											
	* Dedicated - Config 1 - SAN Raid 5	$ 1,380,000 00	$ 1,518,000 00	$ 1,669,800 00	$ 1,836,780 00	$ 1,616,366 40	$ 1,778,003 04	$ 1,955,803 20	$ 2,151,383 52	$ 2,366,521 92	$ 2,603,174 40
	* Dedicated - Config 2 - SAN Raid 10	$ 1,722,947 37	$ 1,795,200 00	$ 1,858,560 00	$ 1,980,528 00	$ 2,038,027 20	$ 2,164,525 44	$ 2,210,906 88	$ 2,431,999 44	$ 2,675,200 32	$ 2,942,718 48
	Dedicated - Config 3 - Net Attached	$ 6,000 00	$ 7,920 00	$ 8,712 00	$ 7,986 00	$ 8,784 60	$ 9,663 00	$ 10,629 60	$ 11,692 20	$ 12,861 60	$ 14,147 40
Total Enterprise Storage - Fully Managed		**$ 3,108,947.37**	**$ 3,321,120.00**	**$ 3,537,072.00**	**$ 3,825,294.00**	**$ 3,663,178.20**	**$ 3,952,191.48**	**$ 4,177,339.68**	**$ 4,595,075.16**	**$ 5,054,583.84**	**$ 5,560,040.28**
Tape and Backup											
	** Server Tape Stored	$ 648,000 00	$ 712,800 00	$ 784,080 00	$ 862,488 00	$ 474,368 40	$ 521,805 24	$ 573,985 80	$ 631,384 32	$ 694,522 80	$ 763,975 08
	** Offsite Tape Storage	$ 22,800 00	$ 23,760 00	$ 25,410 00	$ 27,152 40	$ 28,991 16	$ 29,957 16	$ 32,951 76	$ 36,247 68	$ 39,870 96	$ 43,858 80
Total Tape and Backup - Fully Managed		**$ 670,800.00**	**$ 736,560.00**	**$ 809,490.00**	**$ 889,640.40**	**$ 503,359.56**	**$ 551,762.40**	**$ 606,937.56**	**$ 667,632.00**	**$ 734,393.76**	**$ 807,833.88**
Limited Co-Lo (Data Center Only Charge) (3)											
Server, Storage, Network, Security Equipment											
	Co-Lo Config - 1	$ 31,399 20	$ 31,483 20	$ 31,569 60	$ 32,203 20	$ 32,203 20	$ 32,296 80	$ 32,395 20	$ 32,395 20	$ 32,395 20	$ 32,395 20
	Co-Lo Config - 2	$ 56,248 80	$ 56,419 20	$ 56,587 20	$ 56,779 20	$ 57,410 40	$ 57,595 20	$ 57,794 40	$ 57,794 40	$ 57,794 40	$ 57,794 40
	Co-Lo Config - 3	$ 465,772 80	$ 467,241 60	$ 468,700 80	$ 470,332 80	$ 220,276 80	$ 221,054 40	$ 221,889 60	$ 221,889 60	$ 221,889 60	$ 221,889 60
Total Limited Co-Lo (Data Center Only Charge)		**$ 553,420.80**	**$ 555,144.00**	**$ 556,857.60**	**$ 559,315.20**	**$ 309,890.40**	**$ 310,946.40**	**$ 312,079.20**	**$ 312,079.20**	**$ 312,079.20**	**$ 312,079.20**
Mainframe Services (4)											
IBM Services											
	*** IBM Mainframe Allocated DASD	$ 1,500,000 00	$ 1,428,000 00	$ 1,356,000 00	$ 1,296,000 00	$ 1,224,000 00	$ 1,164,000 00	$ 1,092,000 00	$ 1,092,000 00	$ 1,092,000 00	$ 1,092,000 00
	IBM Tapes in Storage - VTS	$ 348,000 00	$ 348,000 00	$ 336,000 00	$ 336,000 00	$ 324,000 00	$ 324,000 00	$ 300,000 00	$ 300,000 00	$ 300,000 00	$ 300,000 00
	IBM Offsite Tape Storage	$ 4,560 00	$ 4,320 00	$ 4,200 00	$ 4,080 00	$ 3,960 00	$ 3,720 00	$ 3,720 00	$ 3,720 00	$ 3,720 00	$ 3,720 00
Total IBM Services		**$ 1,852,560.00**	**$ 1,780,320.00**	**$ 1,696,200.00**	**$ 1,636,080.00**	**$ 1,551,960.00**	**$ 1,491,720.00**	**$ 1,395,720.00**	**$ 1,395,720.00**	**$ 1,395,720.00**	**$ 1,395,720.00**
IBM Configurations											
	Platinum Tier										
	IBM Mainframe Config - 1	$ 4,454,755 80	$ 6,290,631 60	$ 8,126,302 80	$ 7,936,229 40	$ 7,758,841 20	$ 7,403,860 20	$ 7,244,886 00	$ 7,244,886 00	$ 7,244,886 00	$ 7,244,886 00
	IBM Mainframe Config - 2	$ 323,679 60	$ 474,470 64	$ 625,278 60	$ 611,877 96	$ 599,407 92	$ 572,183 64	$ 561,050 28	$ 561,050 28	$ 561,050 28	$ 561,050 28
	IBM Mainframe Config - 3	$ 1,158,102 00	$ 1,706,601 60	$ 2,255,061 60	$ 2,184,138 00	$ 2,117,332 80	$ 2,017,936 80	$ 1,957,942 80	$ 1,957,942 80	$ 1,957,942 80	$ 1,957,942 80
	IBM AS400 Config 1	$ 103,783 68	$ 476,592 48	$ 849,401 28	$ 853,026 72	$ 857,176 32	$ 821,402 40	$ 825,420 96	$ 825,420 96	$ 825,420 96	$ 825,420 96
	IBM AS400 Config 2	$ 1,022,817 60	$ 2,644,819 20	$ 4,266,470 40	$ 4,250,176 80	$ 4,231,605 60	$ 4,058,332 80	$ 4,043,265 60	$ 4,043,265 60	$ 4,043,265 60	$ 4,043,265 60
sub-total IBM Mainfram Services - Plantinum		**$ 7,063,138.68**	**$ 11,593,115.52**	**$ 16,122,514.68**	**$ 15,835,448.88**	**$ 15,564,363.84**	**$ 14,873,715.84**	**$ 14,632,565.64**	**$ 14,632,565.64**	**$ 14,632,565.64**	**$ 14,632,565.64**
	Gold Tier										
	IBM Mainframe Config - 1	$ 519,072 48	$ 747,578 88	$ 976,085 28	$ 954,231 48	$ 933,911 28	$ 891,353 88	$ 873,155 16	$ 873,155 16	$ 873,155 16	$ 873,155 16
	IBM Mainframe Config - 2	$ 38,545 20	$ 57,734 64	$ 76,924 08	$ 75,355 92	$ 73,902 24	$ 70,558 56	$ 69,258 24	$ 69,258 24	$ 69,258 24	$ 69,258 24
	IBM Mainframe Config - 3	$ 131,231 16	$ 199,102 56	$ 266,969 04	$ 258,806 76	$ 251,131 56	$ 239,377 68	$ 232,484 76	$ 232,484 76	$ 232,484 76	$ 232,484 76
	IBM AS400 Config 1	$ 12,232 32	$ 59,328 96	$ 106,420 08	$ 106,927 92	$ 107,496 48	$ 103,019 76	$ 103,555 20	$ 103,555 20	$ 103,555 20	$ 103,555 20
	IBM AS400 Config 2	$ 120,534 96	$ 322,554 96	$ 524,574 96	$ 522,915 12	$ 520,927 68	$ 499,655 52	$ 498,104 88	$ 498,104 88	$ 498,104 88	$ 498,104 88
sub-total IBM Mainfram Services - Gold		**$ 821,616.12**	**$ 1,386,300.00**	**$ 1,950,973.44**	**$ 1,918,237.20**	**$ 1,887,369.24**	**$ 1,803,965.40**	**$ 1,776,558.24**	**$ 1,776,558.24**	**$ 1,776,558.24**	**$ 1,776,558.24**
	Basic Tier										
	IBM Mainframe Config - 1	$ 493,129 08	$ 721,022 04	$ 948,940 56	$ 928,467 00	$ 909,424 80	$ 868,119 84	$ 851,096 88	$ 851,096 88	$ 851,096 88	$ 851,096 88
	IBM Mainframe Config - 2	$ 36,618 48	$ 55,762 56	$ 74,908 80	$ 73,442 16	$ 72,085 68	$ 68,830 56	$ 67,618 80	$ 67,618 80	$ 67,618 80	$ 67,618 80
	IBM Mainframe Config - 3	$ 122,458 80	$ 190,123 56	$ 257,783 40	$ 250,093 44	$ 242,856 12	$ 231,510 60	$ 225,016 20	$ 225,016 20	$ 225,016 20	$ 225,016 20
	IBM AS400 Config 1	$ 11,619 60	$ 58,705 20	$ 105,779 76	$ 106,320 72	$ 106,916 88	$ 102,467 76	$ 103,047 36	$ 103,047 36	$ 103,047 36	$ 103,047 36
	IBM AS400 Config 2	$ 115,686 48	$ 317,619 12	$ 519,508 08	$ 518,110 32	$ 516,384 96	$ 495,331 20	$ 493,998 96	$ 493,998 96	$ 493,998 96	$ 493,998 96
sub-total IBM Mainfram Services - Basic		**$ 779,512.44**	**$ 1,343,232.48**	**$ 1,906,920.60**	**$ 1,876,433.64**	**$ 1,847,668.44**	**$ 1,766,259.96**	**$ 1,740,778.20**	**$ 1,740,778.20**	**$ 1,740,778.20**	**$ 1,740,778.20**

Note: The Commonwealth has established mult

Baseline Units - Volumetrics

Resource Description	Service Tier / Configuration (6)	Annual Costs Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Total - IBM Mainframe Services - All Support Tiers		**$ 8,664,267.24**	###########	###########	###########	###########	###########	###########	###########	###########	###########
Unisys Services											
	*** Unisys DASD	$ 168,000 00	$ 168,000 00	$ 168,000 00	$ 168,000 00	$ 168,000 00	$ 144,000 00	$ 144,000 00	$ 144,000 00	$ 144,000 00	$ 144,000 00
	Unisys Tapes in Storage - VTS	$ 84,000 00	$ 84,000 00	$ 84,000 00	$ 84,000 00	$ 84,000 00	$ 60,000 00	$ 60,000 00	$ 60,000 00	$ 60,000 00	$ 60,000 00
	Unisys Offsite Tape Storage	$ 4,560 00	$ 4,320 00	$ 4,200 00	$ 4,080 00	$ 3,960 00	$ 3,720 00	$ 3,720 00	$ 3,720 00	$ 3,720 00	$ 3,720 00
Total Unisys Services		**$ 256,560.00**	**$ 256,320.00**	**$ 256,200.00**	**$ 256,080.00**	**$ 255,960.00**	**$ 207,720.00**	**$ 207,720.00**	**$ 207,720.00**	**$ 207,720.00**	**$ 207,720.00**
Unisys Configurations											
	Platinum Tier										
	Unisys Mainframe Config - 1	$ 1,994,916 00	$ 1,989,702 00	$ 1,931,226 00	$ 1,936,440 00	$ 1,939,542 00	$ 1,899,744 00	$ 1,901,592 00	$ 1,901,592 00	$ 1,901,592 00	$ 1,901,592 00
	Unisys Mainframe Config - 2	$ 478,156 80	$ 483,357 60	$ 487,792 80	$ 492,492 00	$ 493,416 00	$ 468,837 60	$ 471,583 20	$ 471,583 20	$ 471,583 20	$ 471,583 20
	Unisys Mainframe Config - 3	$ 11,281,646 64	$ 11,243,258 40	$ 10,967,278 08	$ 10,973,157 36	$ 10,973,849 04	$ 10,737,640 32	$ 10,772,224 32	$ 10,772,224 32	$ 10,772,224 32	$ 10,772,224 32
	Unisys Mainframe Config - 4	$ 2,712,570 00	$ 2,730,630 00	$ 2,747,745 00	$ 2,765,595 00	$ 2,771,895 00	$ 2,662,065 00	$ 2,650,620 00	$ 2,650,620 00	$ 2,650,620 00	$ 2,650,620 00
sub-total Unisys Mainfram Services - Plantinum		**$ 16,467,289.44**	**$ 16,446,948.00**	**$ 16,134,041.88**	**$ 16,167,684.36**	**$ 16,178,702.04**	**$ 15,768,286.92**	**$ 15,796,019.52**	**$ 15,796,019.52**	**$ 15,796,019.52**	**$ 15,796,019.52**
	Gold Tier										
	Unisys Mainframe Config - 1	$ 159,466 56	$ 159,049 44	$ 154,381 92	$ 154,793 76	$ 155,041 92	$ 151,863 36	$ 152,011 20	$ 152,011 20	$ 152,011 20	$ 152,011 20
	Unisys Mainframe Config - 2	$ 58,682 88	$ 59,321 16	$ 59,865 48	$ 60,442 20	$ 60,555 60	$ 57,539 16	$ 57,876 12	$ 57,876 12	$ 57,876 12	$ 57,876 12
	Unisys Mainframe Config - 3	$ 688,892 16	$ 686,547 84	$ 669,694 08	$ 670,053 12	$ 670,095 36	$ 655,670 40	$ 657,782 40	$ 657,782 40	$ 657,782 40	$ 657,782 40
	Unisys Mainframe Config - 4	$ 341,008 80	$ 343,279 20	$ 345,430 80	$ 347,674 80	$ 348,466 80	$ 334,659 60	$ 333,220 80	$ 333,220 80	$ 333,220 80	$ 333,220 80
sub-total Unisys Mainfram Services - Gold		**$ 1,248,050.40**	**$ 1,248,197.64**	**$ 1,229,372.28**	**$ 1,232,963.88**	**$ 1,234,159.68**	**$ 1,199,732.52**	**$ 1,200,890.52**	**$ 1,200,890.52**	**$ 1,200,890.52**	**$ 1,200,890.52**
	Basic Tier										
	Unisys Mainframe Config - 1	$ 158,252 16	$ 157,850 88	$ 153,246 72	$ 153,669 12	$ 153,927 84	$ 150,749 28	$ 150,907 68	$ 150,907 68	$ 150,907 68	$ 150,907 68
	Unisys Mainframe Config - 2	$ 58,682 88	$ 59,324 40	$ 59,868 72	$ 60,422 76	$ 60,555 60	$ 57,539 16	$ 57,876 12	$ 57,876 12	$ 57,876 12	$ 57,876 12
	Unisys Mainframe Config - 3	$ 688,258 56	$ 685,914 24	$ 669,060 48	$ 669,440 64	$ 669,482 88	$ 655,079 04	$ 657,212 16	$ 657,212 16	$ 657,212 16	$ 657,212 16
	Unisys Mainframe Config - 4	$ 340,982 40	$ 343,279 20	$ 345,430 80	$ 347,674 80	$ 348,466 80	$ 334,659 60	$ 333,220 80	$ 333,220 80	$ 333,220 80	$ 333,220 80
sub-total Unisys Mainfram Services - Basic		**$ 1,246,176.00**	**$ 1,246,368.72**	**$ 1,227,606.72**	**$ 1,231,207.32**	**$ 1,232,433.12**	**$ 1,198,027.08**	**$ 1,199,216.76**	**$ 1,199,216.76**	**$ 1,199,216.76**	**$ 1,199,216.76**
Total - Unisys Mainframe Services - All Support Tiers		###########	###########	###########	###########	###########	###########	###########	###########	###########	###########
On-Demand (IaaS) (5)											
IaaS Servers - x86 (Windows, Linux) - Virtual Servers											
	IaaS Windows vConfig - 1	$ 12,386 43	$ 14,768 64	$ 17,845 44	$ 20,029 32	$ 21,994 56	$ 23,280 00	$ 24,912 00	$ 29,686 80	$ 35,707 20	$ 39,028 80
	IaaS Windows vConfig - 2	$ 15,199 23	$ 18,069 12	$ 21,840 48	$ 24,384 60	$ 26,661 60	$ 28,056 00	$ 29,721 60	$ 35,418 24	$ 42,600 96	$ 46,563 84
	IaaS Windows vConfig - 3	$ 25,087 23	$ 29,658 24	$ 35,830 08	$ 39,652 92	$ 43,001 28	$ 44,784 00	$ 46,627 20	$ 55,564 08	$ 66,832 32	$ 73,049 28
	IaaS Windows vConfig - 4	$ 23,651 11	$ 28,263 60	$ 32,913 72	$ 36,222 00	$ 38,444 40	$ 39,601 44	$ 41,543 04	$ 50,984 64	$ 61,370 40	$ 67,979 52
	IaaS Windows vConfig - 5	$ 10,548 91	$ 12,579 84	$ 14,663 88	$ 16,233 00	$ 17,334 00	$ 18,070 56	$ 19,176 96	$ 23,535 36	$ 28,329 60	$ 31,380 48
	IaaS Linux vConfig - 1	$ 16,035 61	$ 19,163 52	$ 23,121 12	$ 25,181 76	$ 27,644 40	$ 28,482 00	$ 29,642 40	$ 35,570 88	$ 42,487 44	$ 46,439 76
	IaaS Linux vConfig - 2	$ 17,442 01	$ 20,813 76	$ 25,118 64	$ 27,327 84	$ 29,977 92	$ 30,870 00	$ 32,047 20	$ 38,456 64	$ 45,934 32	$ 50,207 28
	IaaS Linux vConfig - 3	$ 22,386 01	$ 26,608 32	$ 32,113 44	$ 34,851 36	$ 38,147 76	$ 39,234 00	$ 40,500 00	$ 48,600 00	$ 58,050 00	$ 63,450 00
	IaaS Linux vConfig - 4	$ 17,926 02	$ 22,966 20	$ 28,011 72	$ 30,546 36	$ 31,113 00	$ 31,926 96	$ 34,891 92	$ 40,960 08	$ 48,545 28	$ 54,613 44
	IaaS Linux vConfig - 5	$ 11,812 50	$ 15,125 40	$ 18,452 28	$ 20,152 08	$ 20,557 80	$ 21,161 52	$ 23,200 56	$ 27,235 44	$ 32,279 04	$ 36,313 92
Total IaaS Servers - x86 (Windows, Linux) - Virtual Servers		**$ 172,475.07**	**$ 208,016.64**	**$ 249,910.80**	**$ 274,581.24**	**$ 294,876.72**	**$ 305,466.48**	**$ 322,262.88**	**$ 386,012.16**	**$ 462,136.56**	**$ 509,026.32**
IaaS Storage On-Demand											
	IaaS Storage Config - 1	$ 3,602 47	$ 4,320 00	$ 5,011 20	$ 5,598 72	$ 5,973 12	$ 6,269 76	$ 6,449 76	$ 7,739 28	$ 9,288 00	$ 11,145 60
	IaaS Storage Config - 2	$ 3,654 92	$ 4,248 00	$ 4,838 40	$ 5,495 04	$ 6,097 56	$ 6,717 60	$ 7,166 40	$ 8,601 60	$ 10,320 00	$ 12,384 00
	IaaS Storage Config - 3	$ 30 00	$ 36 00	$ 36 00	$ 30 00	$ 30 00	$ 30 00	$ 30 00	$ 30 00	$ 30 00	$ 30 00

Note: The Commonwealth has established mult

Baseline Units - Volumetrics

Resource Description	Service Tier / Configuration (6)	Annual Costs Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Total IaaS Storage On-Demand		**$ 7,287.38**	**$ 8,604.00**	**$ 9,885.60**	**$ 11,123.76**	**$ 12,100.68**	**$ 13,017.36**	**$ 13,646.16**	**$ 16,370.88**	**$ 19,638.00**	**$ 23,559.60**
IaaS Backup On-Demand											
	IaaS Backup Config - 1	$ 480 00	$ 576 00	$ 691 20	$ 829 44	$ 497 64	$ 597 24	$ 716 64	$ 859 92	$ 1,032 00	$ 1,238 40
Total IaaS Backup On-Demand		**$ 480.00**	**$ 576.00**	**$ 691.20**	**$ 829.44**	**$ 497.64**	**$ 597.24**	**$ 716.64**	**$ 859.92**	**$ 1,032.00**	**$ 1,238.40**
Reserve Account											
		$ 1,008,000 00	$ 1,008,000 00	$ 1,008,000 00	$ 1,008,000 00	$ 1,008,000 00	$ 1,008,000 00	$ 1,008,000 00	$ 1,008,000 00	$ 1,008,000 00	$ 1,008,000 00
Reserve Account		**$ 1,008,000.00**	**$ 1,008,000.00**	**$ 1,008,000.00**	**$ 1,008,000.00**	**$ 1,008,000.00**	**$ 1,008,000.00**	**$ 1,008,000.00**	**$ 1,008,000.00**	**$ 1,008,000.00**	**$ 1,008,000.00**

Notes:

For purposes of submitting a proposal, Offerors should assume that tapes are equivalent in ca

* For purposes of submitting a proposal, Offerors should assume that the slower Tier1 RAID

** The volume is expressed as native.

*** For purposes of evaluation DASD is expressed in Usable (not Raw)

Third Party Software

Third Party Software

Vendor	Product										
□□□	□□□□

Baseline Units - Volumetrics

Note: The Commonwealth has established mult

Resource Description	Service Tier / Configuration (6)	Annual Costs									
		Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
		$ 5 64	$ 5 76	$ 5 76	$ 5 88	$ 6 00	$ 6 00	$ 6 12	$ 6 24	$ 6 24	$ 6 48
		$ 119,736 00	$ 122,556 00	$ 125,412 00	$ 128,364 00	$ 131,400 00	$ 129,456 00	$ 132,720 00	$ 136,044 00	$ 139,464 00	$ 142,980 00
		$ 192,000 00	$ 198,000 00	$ 204,000 00	$ 210,000 00	$ 216,000 00	$ 210,000 00	$ 216,000 00	$ 222,000 00	$ 228,000 00	$ 234,000 00
		$ 302,491 56	$ 308,828 52	$ 315,271 32	$ 321,907 32	$ 328,742 40	$ 324,366 72	$ 331,713 00	$ 339,181 92	$ 346,874 88	$ 354,798 72
		$ 17,595 12	$ 18,000 72	$ 18,413 04	$ 18,837 60	$ 19,275 12	$ 18,995 04	$ 19,465 20	$ 19,943 28	$ 20,435 52	$ 20,942 64
		$ 5,842 08	$ 5,994 72	$ 6,148 80	$ 6,308 64	$ 6,471 36	$ 6,367 68	$ 6,543 36	$ 6,721 92	$ 6,907 68	$ 7,097 76
		$ 24,236 76	$ 24,963 84	$ 25,712 76	$ 26,484 12	$ 27,278 64	$ 28,096 92	$ 28,939 92	$ 29,808 12	$ 30,702 36	$ 31,623 48
		$ 14,737 20	$ 15,179 28	$ 15,634 68	$ 16,103 76	$ 16,586 88	$ 17,084 52	$ 17,597 04	$ 18,124 92	$ 18,668 64	$ 19,228 80
		$ 18,067 08	$ 18,609 12	$ 19,167 48	$ 19,742 40	$ 20,334 72	$ 20,944 80	$ 21,573 12	$ 22,220 40	$ 22,886 88	$ 23,573 52
		$ 2,858 52	$ 2,938 20	$ 3,027 84	$ 3,107 52	$ 3,197 16	$ 3,147 36	$ 3,237 00	$ 3,336 60	$ 3,436 20	$ 3,535 80
		$ 8,678 88	$ 8,920 80	$ 9,192 96	$ 9,434 88	$ 9,707 04	$ 9,555 84	$ 9,828 00	$ 10,130 40	$ 10,432 80	$ 10,735 20
		$ 2,274 12	$ 2,339 64	$ 2,406 36	$ 2,475 00	$ 2,545 68	$ 2,500 44	$ 2,576 52	$ 2,653 80	$ 2,733 36	$ 2,815 32
		$ 21,098 88	$ 21,706 56	$ 22,325 76	$ 22,962 24	$ 23,618 88	$ 23,198 40	$ 23,904 00	$ 24,621 12	$ 25,361 28	$ 26,121 60
		$ 149,988 00	$ 153,931 20	$ 157,939 92	$ 162,068 88	$ 166,321 92	$ 163,599 36	$ 168,170 40	$ 172,817 52	$ 177,604 32	$ 182,534 64
		$ 33,772 32	$ 34,670 16	$ 35,582 76	$ 36,523 08	$ 37,491 48	$ 36,871 56	$ 37,912 32	$ 38,970 36	$ 40,060 08	$ 41,182 56
		$ 7,121 16	$ 7,326 36	$ 7,535 16	$ 7,750 08	$ 7,971 48	$ 7,829 64	$ 8,067 96	$ 8,309 88	$ 8,559 00	$ 8,815 68
		$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
		$ 52,471 80	$ 54,045 72	$ 55,667 16	$ 57,337 20	$ 59,057 28	$ 60,829 20	$ 62,654 04	$ 64,533 60	$ 66,469 68	$ 68,463 72
		$ 39,563 16	$ 40,703 76	$ 41,863 56	$ 43,058 04	$ 44,288 52	$ 43,500 84	$ 44,823 24	$ 46,167 72	$ 47,552 52	$ 48,978 84
		$ 64,103 88	$ 65,952 24	$ 67,831 32	$ 69,766 80	$ 71,760 36	$ 70,484 16	$ 72,626 88	$ 74,805 24	$ 77,049 00	$ 79,360 08
		$ 5,607 36	$ 5,769 36	$ 5,933 52	$ 6,102 72	$ 6,277 68	$ 6,166 08	$ 6,353 28	$ 6,544 08	$ 6,739 92	$ 6,942 24
		$ 11,821 68	$ 12,160 32	$ 12,504 00	$ 12,858 00	$ 13,222 56	$ 17,093 52	$ 17,486 16	$ 17,884 56	$ 18,294 72	$ 18,717 36
		$ 55,630 80	$ 57,299 76	$ 59,018 76	$ 60,789 24	$ 62,613 00	$ 64,491 24	$ 66,426 12	$ 68,418 84	$ 70,471 44	$ 72,585 60
		$ 39,146 16	$ 40,320 48	$ 41,530 08	$ 42,776 04	$ 44,059 32	$ 45,381 12	$ 46,742 52	$ 48,144 84	$ 49,589 16	$ 51,076 80
		$ 19,806 60	$ 20,400 72	$ 21,012 72	$ 21,643 08	$ 22,292 40	$ 22,961 16	$ 23,650 08	$ 24,359 52	$ 25,090 32	$ 25,842 96
		$ 61,290 00	$ 63,128 76	$ 65,022 60	$ 66,973 32	$ 68,982 48	$ 71,052 00	$ 73,183 56	$ 75,378 96	$ 77,640 36	$ 79,969 56
		$ 443 04	$ 456 36	$ 469 92	$ 484 08	$ 498 60	$ 513 60	$ 528 96	$ 544 80	$ 561 24	$ 578 04
		$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
		$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
		$ 105,529 20	$ 108,562 20	$ 111,645 60	$ 114,821 40	$ 118,092 60	$ 115,998 60	$ 119,514 60	$ 123,089 40	$ 126,771 00	$ 130,563 60
		$ 19,333 44	$ 19,889 76	$ 20,455 20	$ 21,037 92	$ 21,637 44	$ 21,253 44	$ 21,898 56	$ 22,553 76	$ 23,229 12	$ 23,924 64
		$ 17,054 40	$ 17,545 20	$ 18,045 60	$ 18,560 40	$ 19,090 80	$ 18,751 20	$ 19,321 20	$ 19,900 80	$ 20,497 20	$ 21,112 80
		$ 65,769 60	$ 67,656 00	$ 69,572 40	$ 71,547 60	$ 73,581 60	$ 72,279 60	$ 74,464 80	$ 76,687 20	$ 78,976 80	$ 81,334 80
		$ 72,003 36	$ 74,077 08	$ 76,186 44	$ 78,357 84	$ 80,595 24	$ 79,163 04	$ 81,568 08	$ 84,012 72	$ 86,531 28	$ 89,125 08
		$ 3,430 08	$ 3,528 48	$ 3,628 32	$ 3,731 28	$ 3,837 36	$ 3,769 44	$ 3,883 44	$ 3,999 36	$ 4,118 88	$ 4,241 76
		$ 13,681 92	$ 14,074 56	$ 14,474 88	$ 14,886 72	$ 15,311 04	$ 15,039 36	$ 15,495 36	$ 15,959 04	$ 16,437 12	$ 16,928 64
		$ 13,681 44	$ 14,075 04	$ 14,474 88	$ 14,886 72	$ 15,311 04	$ 15,039 36	$ 15,495 36	$ 15,959 04	$ 16,436 64	$ 16,928 64
		$ 190 80	$ 195 96	$ 201 12	$ 206 52	$ 212 16	$ 208 56	$ 214 56	$ 220 56	$ 226 80	$ 233 28
		$ 1,316 88	$ 1,352 16	$ 1,388 88	$ 1,425 60	$ 1,464 48	$ 1,439 28	$ 1,481 04	$ 1,522 80	$ 1,566 00	$ 1,610 64
		$ 2,366 40	$ 2,434 56	$ 2,504 64	$ 2,575 68	$ 2,648 64	$ 2,601 60	$ 2,681 28	$ 2,760 96	$ 2,844 48	$ 2,928 96

Baseline Units - Volumetrics

Note: The Commonwealth has established mult

Resource Description	Service Tier / Configuration (6)	Annual Costs									
		Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
		$ 262,381 92	$ 269,947 68	$ 277,615 68	$ 285,556 32	$ 293,701 44	$ 288,487 20	$ 297,245 76	$ 306,174 72	$ 315,342 24	$ 324,816 48
		$ 210,032 64	$ 216,100 08	$ 222,243 84	$ 228,616 56	$ 235,141 92	$ 230,944 32	$ 237,965 76	$ 245,101 68	$ 252,466 56	$ 260,022 24
		$ 38,507 04	$ 39,620 88	$ 40,734 72	$ 41,901 60	$ 43,095 00	$ 42,325 92	$ 43,625 40	$ 44,924 88	$ 46,277 40	$ 47,656 44
		$ 4,908 00	$ 5,052 00	$ 5,196 00	$ 5,340 00	$ 5,496 00	$ 5,400 00	$ 5,556 00	$ 5,724 00	$ 5,904 00	$ 6,072 00
		$ 2,822 40	$ 2,872 80	$ 2,973 60	$ 3,074 40	$ 3,124 80	$ 3,074 40	$ 3,175 20	$ 3,276 00	$ 3,376 80	$ 3,477 60
		$ 1,188 00	$ 1,221 12	$ 1,257 12	$ 1,291 68	$ 1,329 12	$ 1,306 08	$ 1,344 96	$ 1,385 28	$ 1,427 04	$ 1,470 24
		$ 7,805 16	$ 8,029 56	$ 8,259 24	$ 8,494 20	$ 8,737 08	$ 8,581 32	$ 8,842 68	$ 9,108 00	$ 9,381 24	$ 9,662 40
		$ 105,024 24	$ 108,174 96	$ 111,420 24	$ 114,762 72	$ 118,205 64	$ 121,751 76	$ 125,404 44	$ 129,166 44	$ 133,041 48	$ 137,032 80
		$ 18,952 80	$ 19,418 40	$ 19,890 00	$ 20,377 20	$ 20,878 80	$ 20,557 20	$ 21,096 00	$ 21,644 40	$ 22,208 40	$ 22,789 20
		$ 35,298 36	$ 36,357 12	$ 37,447 92	$ 38,571 12	$ 39,728 52	$ 40,920 12	$ 42,147 72	$ 43,412 04	$ 44,714 52	$ 46,055 88
		$ 132,516 00	$ 135,827 28	$ 139,192 56	$ 142,661 52	$ 146,232 00	$ 143,946 72	$ 147,785 04	$ 151,686 00	$ 155,705 76	$ 159,846 48
		$ 13,862 16	$ 14,192 88	$ 14,531 40	$ 14,879 28	$ 15,236 52	$ 15,152 28	$ 15,537 60	$ 15,927 60	$ 16,331 64	$ 16,746 60
		$ 5,124 60	$ 5,272 56	$ 5,422 68	$ 5,577 48	$ 5,736 60	$ 5,634 72	$ 5,806 08	$ 5,980 32	$ 6,159 60	$ 6,344 28
		$ 155,071 68	$ 158,411 64	$ 161,807 40	$ 165,304 92	$ 168,907 44	$ 166,601 16	$ 170,473 08	$ 174,409 68	$ 178,464 36	$ 182,640 60
		$ 13,878 72	$ 14,234 88	$ 14,596 80	$ 14,970 24	$ 15,354 24	$ 15,108 48	$ 15,521 28	$ 15,941 76	$ 16,373 76	$ 16,819 20
		$ 15,348 84	$ 15,760 68	$ 16,181 88	$ 16,617 12	$ 17,063 28	$ 17,069 52	$ 17,548 44	$ 18,036 72	$ 18,540 60	$ 19,058 52
		$ 14,892 96	$ 15,249 60	$ 15,611 52	$ 15,984 96	$ 16,368 96	$ 16,123 20	$ 16,536 00	$ 16,956 00	$ 17,388 48	$ 17,833 92
		$ 9,401 76	$ 9,672 96	$ 9,948 48	$ 10,232 64	$ 10,524 96	$ 10,337 76	$ 10,652 16	$ 10,971 36	$ 11,300 64	$ 11,639 52
		$ 90,899 88	$ 93,626 88	$ 96,435 60	$ 99,328 68	$ 102,308 52	$ 105,377 88	$ 108,539 16	$ 111,795 24	$ 115,149 24	$ 118,603 68
		$ 8,791 44	$ 9,044 88	$ 9,302 64	$ 9,568 08	$ 9,841 44	$ 9,666 36	$ 9,960 24	$ 10,259 04	$ 10,566 72	$ 10,883 64
		$ 4,029 36	$ 4,145 52	$ 4,263 72	$ 4,385 40	$ 4,510 68	$ 4,430 40	$ 4,565 16	$ 4,702 08	$ 4,843 08	$ 4,988 40
		$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
		$ 1,248 72	$ 1,279 20	$ 1,310 16	$ 1,342 32	$ 1,375 20	$ 1,354 08	$ 1,389 36	$ 1,425 36	$ 1,462 32	$ 1,500 48
		$ 5,292 00	$ 5,444 40	$ 5,599 20	$ 5,758 80	$ 5,923 20	$ 5,817 60	$ 5,994 00	$ 6,174 00	$ 6,360 00	$ 6,549 60
		$ 4,689 60	$ 4,811 52	$ 4,935 36	$ 5,063 04	$ 5,194 56	$ 5,110 08	$ 5,252 16	$ 5,396 16	$ 5,544 00	$ 5,696 64
		$ 11,859 12	$ 12,176 64	$ 12,504 24	$ 12,841 92	$ 13,184 64	$ 12,962 88	$ 13,335 84	$ 13,713 84	$ 14,101 92	$ 14,500 08
		$ 13,191 96	$ 13,547 28	$ 13,913 88	$ 14,286 12	$ 14,675 28	$ 14,427 12	$ 14,844 48	$ 15,267 48	$ 15,701 76	$ 16,147 32
		$ 624 48	$ 639 60	$ 655 20	$ 671 04	$ 687 60	$ 677 04	$ 694 80	$ 712 56	$ 731 28	$ 750 24
		$ 212 40	$ 217 80	$ 223 20	$ 230 40	$ 237 60	$ 232 20	$ 239 40	$ 246 60	$ 253 80	$ 261 00
		$ 11,504 16	$ 11,835 72	$ 12,173 04	$ 12,520 44	$ 12,877 92	$ 12,648 96	$ 13,033 44	$ 13,424 40	$ 13,827 24	$ 14,241 96
		$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
		$ 8,820 12	$ 9,084 72	$ 9,357 36	$ 9,638 04	$ 9,927 24	$ 10,224 96	$ 10,531 80	$ 10,847 76	$ 11,173 08	$ 11,508 36
		$ 704 40	$ 724 20	$ 744 00	$ 764 52	$ 785 64	$ 1,820 76	$ 1,843 68	$ 1,866 84	$ 1,890 60	$ 1,915 08
		$ 865 56	$ 889 92	$ 914 64	$ 939 96	$ 966 12	$ 1,998 00	$ 2,026 32	$ 2,054 88	$ 2,084 28	$ 2,114 52
		$ 1,031 64	$ 1,060 80	$ 1,090 32	$ 1,120 68	$ 1,152 00	$ 2,180 64	$ 2,214 48	$ 2,248 68	$ 2,283 84	$ 2,320 20
		$ 1,192 80	$ 1,226 64	$ 1,260 84	$ 1,296 12	$ 1,332 48	$ 2,357 76	$ 2,397 00	$ 2,436 72	$ 2,477 64	$ 2,519 64
		$ 1,647 00	$ 1,693 92	$ 1,741 44	$ 1,790 52	$ 1,840 92	$ 2,857 20	$ 2,911 68	$ 2,966 76	$ 3,023 52	$ 3,081 96

Baseline Units - Volumetrics

Note: The Commonwealth has established mult

Resource Description	Service Tier / Configuration (6)	Annual Costs									
		Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
		$ 704 40	$ 724 20	$ 744 00	$ 764 52	$ 785 64	$ 1,820 76	$ 1,843 68	$ 1,866 84	$ 1,890 60	$ 1,915 08
		$ 865 56	$ 889 92	$ 914 64	$ 939 96	$ 966 12	$ 1,998 00	$ 2,026 32	$ 2,054 88	$ 2,084 28	$ 2,114 52
		$ 1,031 64	$ 1,060 80	$ 1,090 32	$ 1,120 68	$ 1,152 00	$ 2,180 64	$ 2,214 48	$ 2,248 68	$ 2,283 84	$ 2,320 20
		$ 1,192 80	$ 1,226 64	$ 1,260 84	$ 1,296 12	$ 1,332 48	$ 2,357 76	$ 2,397 00	$ 2,436 72	$ 2,477 64	$ 2,519 64
		$ 1,647 00	$ 1,693 92	$ 1,741 44	$ 1,790 52	$ 1,840 92	$ 2,857 20	$ 2,911 68	$ 2,966 76	$ 3,023 52	$ 3,081 96
		$ 1,891 20	$ 1,945 20	$ 1,999 92	$ 2,056 20	$ 2,114 28	$ 3,125 76	$ 3,188 28	$ 3,251 76	$ 3,317 04	$ 3,384 36
		$ 704 40	$ 724 20	$ 744 00	$ 764 52	$ 785 64	$ 1,820 76	$ 1,843 68	$ 1,866 84	$ 1,890 60	$ 1,915 08
		$ 865 56	$ 889 92	$ 914 64	$ 939 96	$ 966 12	$ 1,998 00	$ 2,026 32	$ 2,054 88	$ 2,084 28	$ 2,114 52
		$ 1,031 64	$ 1,060 80	$ 1,090 32	$ 1,120 68	$ 1,152 00	$ 2,180 64	$ 2,214 48	$ 2,248 68	$ 2,283 84	$ 2,320 20
		$ 1,192 80	$ 1,226 64	$ 1,260 84	$ 1,296 12	$ 1,332 48	$ 2,357 76	$ 2,397 00	$ 2,436 72	$ 2,477 64	$ 2,519 64
		$ 1,647 00	$ 1,693 92	$ 1,741 44	$ 1,790 52	$ 1,840 92	$ 2,857 20	$ 2,911 68	$ 2,966 76	$ 3,023 52	$ 3,081 96
		$ 716 64	$ 736 68	$ 756 96	$ 777 84	$ 799 32	$ 1,834 20	$ 1,857 48	$ 1,881 00	$ 1,905 24	$ 1,930 20
		$ 865 56	$ 889 92	$ 914 64	$ 939 96	$ 966 12	$ 1,998 00	$ 2,026 32	$ 2,054 88	$ 2,084 28	$ 2,114 52
		$ 1,031 64	$ 1,060 80	$ 1,090 32	$ 1,120 68	$ 1,152 00	$ 2,180 64	$ 2,214 48	$ 2,248 68	$ 2,283 84	$ 2,320 20
		$ 1,192 80	$ 1,226 64	$ 1,260 84	$ 1,296 12	$ 1,332 48	$ 2,357 76	$ 2,397 00	$ 2,436 72	$ 2,477 64	$ 2,519 64
		$ 1,647 00	$ 1,693 92	$ 1,741 44	$ 1,790 52	$ 1,840 92	$ 2,857 20	$ 2,911 68	$ 2,966 76	$ 3,023 52	$ 3,081 96
		$ 1,891 20	$ 1,945 20	$ 1,999 92	$ 2,056 20	$ 2,114 28	$ 3,125 76	$ 3,188 28	$ 3,251 76	$ 3,317 04	$ 3,384 36
		$ 704 40	$ 724 20	$ 744 00	$ 764 52	$ 785 64	$ 1,820 76	$ 1,843 68	$ 1,866 84	$ 1,890 60	$ 1,915 08
		$ 865 56	$ 889 92	$ 914 64	$ 939 96	$ 966 12	$ 1,998 00	$ 2,026 32	$ 2,054 88	$ 2,084 28	$ 2,114 52
		$ 1,031 64	$ 1,060 80	$ 1,090 32	$ 1,120 68	$ 1,152 00	$ 2,180 64	$ 2,214 48	$ 2,248 68	$ 2,283 84	$ 2,320 20
		$ 1,192 80	$ 1,226 64	$ 1,260 84	$ 1,296 12	$ 1,332 48	$ 2,357 76	$ 2,397 00	$ 2,436 72	$ 2,477 64	$ 2,519 64
		$ 1,647 00	$ 1,693 92	$ 1,741 44	$ 1,790 52	$ 1,840 92	$ 2,857 20	$ 2,911 68	$ 2,966 76	$ 3,023 52	$ 3,081 96
		$ 1,891 20	$ 1,945 20	$ 1,999 92	$ 2,056 20	$ 2,114 28	$ 3,125 76	$ 3,188 28	$ 3,251 76	$ 3,317 04	$ 3,384 36
		$ 704 40	$ 724 20	$ 744 00	$ 764 52	$ 785 64	$ 1,820 76	$ 1,843 68	$ 1,866 84	$ 1,890 60	$ 1,915 08
		$ 865 56	$ 889 92	$ 914 64	$ 939 96	$ 966 12	$ 1,998 00	$ 2,026 32	$ 2,054 88	$ 2,084 28	$ 2,114 52
		$ 1,031 64	$ 1,060 80	$ 1,090 32	$ 1,120 68	$ 1,152 00	$ 2,180 64	$ 2,214 48	$ 2,248 68	$ 2,283 84	$ 2,320 20
		$ 1,192 80	$ 1,226 64	$ 1,260 84	$ 1,296 12	$ 1,332 48	$ 2,357 76	$ 2,397 00	$ 2,436 72	$ 2,477 64	$ 2,519 64

Baseline Units - Volumetrics

Note: The Commonwealth has established mult

Resource Description	Service Tier / Configuration (6)	Annual Costs									
		Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
		$ 1,647 00	$ 1,693 92	$ 1,741 44	$ 1,790 52	$ 1,840 92	$ 2,857 20	$ 2,911 68	$ 2,966 76	$ 3,023 52	$ 3,081 96
		$ 1,891 20	$ 1,945 20	$ 1,999 92	$ 2,056 20	$ 2,114 28	$ 3,125 76	$ 3,188 28	$ 3,251 76	$ 3,317 04	$ 3,384 36
		$ 1,383 24	$ 1,422 60	$ 1,462 44	$ 1,503 48	$ 1,545 60	$ 2,567 28	$ 2,612 88	$ 2,658 96	$ 2,706 48	$ 2,755 44
		$ 1,705 68	$ 1,754 28	$ 1,803 48	$ 1,854 24	$ 1,906 56	$ 2,921 64	$ 2,978 04	$ 3,035 16	$ 3,093 96	$ 3,154 56
		$ 2,037 72	$ 2,095 92	$ 2,154 96	$ 2,215 68	$ 2,278 32	$ 3,286 92	$ 3,354 36	$ 3,422 76	$ 3,493 20	$ 3,565 68
		$ 2,360 04	$ 2,427 60	$ 2,496 00	$ 2,566 56	$ 2,639 16	$ 3,641 28	$ 3,719 52	$ 3,798 84	$ 3,880 56	$ 3,964 80
		$ 3,268 56	$ 3,362 28	$ 3,457 32	$ 3,555 24	$ 3,656 04	$ 4,640 16	$ 4,748 76	$ 4,859 04	$ 4,972 56	$ 5,089 44
		$ 3,756 96	$ 3,864 72	$ 3,974 16	$ 4,086 84	$ 4,202 88	$ 5,177 16	$ 5,302 08	$ 5,428 92	$ 5,559 60	$ 5,694 12
		$ 6,912 12	$ 7,110 84	$ 7,312 68	$ 7,520 64	$ 7,734 84	$ 8,646 36	$ 8,876 76	$ 9,110 76	$ 9,351 84	$ 9,600 12
		$ 7,923 12	$ 8,151 00	$ 8,382 48	$ 8,620 92	$ 8,866 56	$ 9,758 04	$ 10,022 16	$ 10,290 60	$ 10,566 96	$ 10,851 72
		$ 12,533 64	$ 12,894 48	$ 13,261 20	$ 13,638 84	$ 14,027 88	$ 14,827 44	$ 15,245 76	$ 15,670 80	$ 16,108 68	$ 16,559 64
		$ 14,379 84	$ 14,793 96	$ 15,214 68	$ 15,648 12	$ 16,094 52	$ 16,857 36	$ 17,337 48	$ 17,825 28	$ 18,327 72	$ 18,845 16
		$ 2,897 40	$ 2,980 32	$ 3,064 56	$ 3,151 20	$ 3,240 60	$ 4,232 04	$ 4,328 28	$ 4,425 84	$ 4,526 40	$ 4,629 96
		$ 3,512 76	$ 3,613 44	$ 3,715 68	$ 3,821 04	$ 3,929 52	$ 4,908 72	$ 5,025 48	$ 5,143 92	$ 5,266 08	$ 5,391 72
		$ 5,818 08	$ 5,985 24	$ 6,155 04	$ 6,330 00	$ 6,510 12	$ 7,443 36	$ 7,637 28	$ 7,834 08	$ 8,036 88	$ 8,245 68
		$ 2,897 40	$ 2,980 32	$ 3,064 56	$ 3,151 20	$ 3,240 60	$ 4,232 04	$ 4,328 28	$ 4,425 84	$ 4,526 40	$ 4,629 96
		$ 3,512 76	$ 3,613 44	$ 3,715 68	$ 3,821 04	$ 3,929 52	$ 4,908 72	$ 5,025 48	$ 5,143 92	$ 5,266 08	$ 5,391 72
		$ 5,818 08	$ 5,985 24	$ 6,155 04	$ 6,330 00	$ 6,510 12	$ 7,443 36	$ 7,637 28	$ 7,834 08	$ 8,036 88	$ 8,245 68
		$ 6,741 12	$ 6,934 92	$ 7,131 84	$ 7,334 64	$ 7,543 44	$ 8,458 44	$ 8,683 08	$ 8,911 32	$ 9,146 40	$ 9,388 44
		$ 2,897 40	$ 2,980 32	$ 3,064 56	$ 3,151 20	$ 3,240 60	$ 4,232 04	$ 4,328 28	$ 4,425 84	$ 4,526 40	$ 4,629 96
		$ 3,512 76	$ 3,613 44	$ 3,715 68	$ 3,821 04	$ 3,929 52	$ 4,908 72	$ 5,025 48	$ 5,143 92	$ 5,266 08	$ 5,391 72
		$ 5,818 08	$ 5,985 24	$ 6,155 04	$ 6,330 00	$ 6,510 12	$ 7,443 36	$ 7,637 28	$ 7,834 08	$ 8,036 88	$ 8,245 68
		$ 2,076 48	$ 2,136 12	$ 2,196 60	$ 2,257 92	$ 2,321 76	$ 3,329 76	$ 3,398 64	$ 3,468 36	$ 3,539 76	$ 3,613 68
		$ 4,127 76	$ 4,247 04	$ 4,367 16	$ 4,490 64	$ 4,618 32	$ 5,585 16	$ 5,722 92	$ 5,862 36	$ 6,006 00	$ 6,153 84
		$ 3,932 64	$ 4,045 44	$ 4,160 16	$ 4,278 24	$ 4,399 68	$ 5,370 72	$ 5,501 28	$ 5,634 24	$ 5,771 04	$ 5,911 68
		$ 9,695 88	$ 9,974 88	$ 10,258 56	$ 10,550 52	$ 10,851 12	$ 11,707 20	$ 12,030 84	$ 12,359 52	$ 12,697 92	$ 13,046 76
A		$ 4,258 44	$ 4,360 32	$ 4,463 76	$ 4,570 20	$ 4,679 88	$ 4,559 64	$ 4,677 72	$ 4,797 60	$ 4,921 08	$ 5,048 16
A		$ 25,919 64	$ 26,541 36	$ 27,172 56	$ 27,822 72	$ 28,492 32	$ 24,357 36	$ 25,078 08	$ 25,809 84	$ 26,563 56	$ 27,339 84
A		$ 2,375 88	$ 1,238 52	$ 1,273 20	$ 1,308 84	$ 1,345 68	$ 1,982 28	$ 2,022 00	$ 2,062 20	$ 2,103 60	$ 2,146 20
A		$ 12,967 32	$ 13,278 12	$ 13,593 72	$ 13,918 80	$ 14,253 60	$ 12,519 24	$ 12,879 72	$ 13,245 48	$ 13,622 40	$ 14,010 48
A		$ 4,542 00	$ 4,650 96	$ 4,761 60	$ 4,875 60	$ 4,993 08	$ 4,151 28	$ 4,277 52	$ 4,405 92	$ 4,538 04	$ 4,674 12

Note: The Commonwealth has established mult

Baseline Units - Volumetrics

Resource Description	Service Tier / Configuration (6)	Annual Costs									
		Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
□□A	□ □□ □□□□□□□□ □□□□□□□□	$ 7,781 64	$ 7,968 36	$ 8,157 96	$ 8,353 32	$ 8,554 44	$ 7,112 16	$ 7,328 64	$ 7,548 48	$ 7,774 92	$ 8,008 08
□□A	□ □□ □□□□□□□□ □□□□□□□□	$ 2,019 60	$ 1,046 52	$ 1,077 12	$ 1,107 72	$ 1,138 32	$ 1,113 84	$ 1,146 48	$ 1,181 16	$ 1,217 88	$ 1,252 56
□□□□□	□A□ □□□□□□□ □□□□□A□□□□□□□□A□□□□	$ 3,581 04	$ 3,684 24	$ 3,789 36	$ 3,897 36	$ 4,008 72	$ 3,937 44	$ 4,057 20	$ 4,178 88	$ 4,304 16	$ 4,433 28
□□□□□	□A□ □□□□□□□ □□□□□A□□□□□□□□□□	$ 896 64	$ 922 32	$ 948 72	$ 975 84	$ 1,003 68	$ 985 68	$ 1,015 68	$ 1,046 16	$ 1,077 60	$ 1,110 00
□□□ □□□□□	□□□□□□□□ □□□□□ □□□□□ □□ □□□□□□□□□ □□□□□	$ 966 12	$ 996 00	$ 1,025 88	$ 1,045 80	$ 1,075 68	$ 1,065 72	$ 1,095 60	$ 1,125 48	$ 1,155 36	$ 1,195 20
□□□ □□□□□	□□□□ □□□□□ □□□□□□□□	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
□□□ □□□□□	□ □□□□□ □□□□□□□□ □□□□	$ 198 00	$ 204 00	$ 207 00	$ 213 00	$ 219 00	$ 216 00	$ 222 00	$ 231 00	$ 237 00	$ 243 00
□□□ □□□□□	□ □□□ □□□□□□□ □□□□□A□□□□ □□□□□□□ □□□□□□□ □□□□□□□ □□ □□□□□	$ 21 60	$ 22 32	$ 22 68	$ 23 40	$ 24 12	$ 23 76	$ 24 48	$ 25 20	$ 25 92	$ 26 64
□□□ □□□□□	□ □□□ □□□□□□□ □□□□□A□□□□ □□□□□□□ □□□□□□□ □□□□□□□ □□ □□□□□	$ 4,199 28	$ 4,320 48	$ 4,443 60	$ 4,570 32	$ 4,700 88	$ 4,617 36	$ 4,757 76	$ 4,900 32	$ 5,047 44	$ 5,198 88
□□□ □□□□□	□ □□□ □□□□□□□ □□□□□A□□□□ □□□□□□□ □□□□□□□ □□□□□□□ □□ □□□□□	$ 2,265 48	$ 2,331 00	$ 2,397 36	$ 2,466 24	$ 2,536 80	$ 2,491 44	$ 2,567 04	$ 2,644 32	$ 2,723 28	$ 2,804 76
□□□ □□□□□	□ □□□ □□□□□□□ □□□□□A□□□□ □□□□□□□ □□□□□□□ □□□□□□□ □□ □□□□□	$ 8,383 20	$ 8,625 60	$ 8,870 40	$ 9,124 80	$ 9,384 00	$ 9,218 40	$ 9,499 20	$ 9,782 40	$ 10,077 60	$ 10,377 60
□□□ □□□□□	□ □□□ □□□□□□□ □□□□□A□□□□ □□□□□□□ □□□□□□□ □□□□□□□ □□ □□□□□	$ 629 28	$ 647 40	$ 665 88	$ 684 84	$ 704 40	$ 691 92	$ 712 92	$ 734 28	$ 756 36	$ 779 04
□□□ □□□□□	□ □□□ □□□□□□□ □□□□□□□□ □□□□□□ □□□□□□□ □□ □□□□□	$ 2,596 20	$ 2,671 08	$ 2,747 16	$ 2,825 52	$ 2,906 28	$ 2,854 56	$ 2,941 44	$ 3,029 64	$ 3,120 48	$ 3,214 08
□□□ □□□□□	□ □□□ □□□□□□□ □□□□□□□□ □□□□□□ □□□□□□□ □□ □□□□□	$ 1,486 80	$ 1,529 64	$ 1,573 20	$ 1,618 20	$ 1,664 28	$ 1,634 76	$ 1,684 44	$ 1,734 84	$ 1,787 04	$ 1,840 68
□□□ □□□□□	□ □□□ □□□□□□□ □□□□□□□□ □□□□□□ □□□□□□□ □□ □□□□□	$ 5,910 00	$ 6,080 40	$ 6,254 40	$ 6,433 20	$ 6,616 80	$ 6,499 20	$ 6,696 00	$ 6,897 60	$ 7,104 00	$ 7,317 60
□□□ □□□□□	□ □□□ □□□□□□□ □□□□□□□□ □□□□□□ □□□□□□□ □□ □□□□□	$ 14,076 72	$ 14,482 80	$ 14,895 36	$ 15,318 72	$ 15,757 20	$ 15,476 40	$ 15,947 28	$ 16,426 80	$ 16,919 28	$ 17,426 88
□□□ □□□□□	□ □□□ □□□□□□□ □□□□□□□□ □□□□□□ □□□□□□□ □□ □□□□□	$ 3,151 08	$ 3,241 80	$ 3,334 32	$ 3,429 36	$ 3,527 28	$ 3,464 64	$ 3,569 76	$ 3,677 04	$ 3,787 20	$ 3,900 96
□□□ □□□□□	□ □□□ □□□□□□□ □□□□□□□□ □□□□□□ □□□□□□□ □□ □□□□□	$ 24,443 52	$ 25,148 16	$ 25,866 24	$ 26,603 52	$ 27,363 84	$ 26,876 16	$ 27,694 08	$ 28,525 44	$ 29,379 84	$ 30,261 12
□□□ □□□□□	□ □□□ □□□□□□□□□□□

Baseline Units - Volumetrics

Note: The Commonwealth has established mult

Resource Description	Service Tier / Configuration (6)	Annual Costs Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
[illegible]	[illegible]	$ 14,065 92	$ 14,471 04	$ 14,883 84	$ 15,308 16	$ 15,745 92	$ 15,465 60	$ 15,936 00	$ 16,414 08	$ 16,907 52	$ 17,414 40
[illegible]	[illegible]	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
[illegible]	[illegible]	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
[illegible]	[illegible]	$ 184 08	$ 184 08	$ 191 16	$ 198 24	$ 205 32	$ 198 24	$ 205 32	$ 212 40	$ 219 48	$ 226 56
[illegible]	[illegible]	$ 16,483 92	$ 16,959 12	$ 17,442 36	$ 17,940 00	$ 18,452 64	$ 18,124 44	$ 18,675 48	$ 19,235 64	$ 19,812 60	$ 20,406 84
[illegible]	[illegible]	$ 11,966 04	$ 12,311 04	$ 12,661 80	$ 13,023 12	$ 13,395 24	$ 13,157 04	$ 13,557 00	$ 13,963 68	$ 14,382 48	$ 14,813 88
[illegible]	[illegible]	$ 935 28	$ 184 20	$ 189 36	$ 194 64	$ 200 16	$ 192 84	$ 198 84	$ 204 72	$ 210 84	$ 217 20
[illegible]	[illegible]	$ 21,817 92	$ 22,446 96	$ 23,086 56	$ 23,745 36	$ 24,423 84	$ 23,989 44	$ 24,718 80	$ 25,460 16	$ 26,223 84	$ 27,010 32
[illegible]	[illegible]	$ 160 56	$ 31 56	$ 32 52	$ 33 36	$ 34 32	$ 33 12	$ 34 08	$ 35 16	$ 36 24	$ 37 32
[illegible]	[illegible]	$ 781 44	$ 794 64	$ 808 08	$ 821 88	$ 836 16	$ 503 52	$ 518 88	$ 534 48	$ 550 44	$ 567 00
Hybrid Third Party Software											
Vendor	**Product**										
[illegible]	[illegible]	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
[illegible]	[illegible]	$ 287,020 92	$ 295,631 64	$ 304,500 48	$ 313,635 60	$ 323,044 56	$ 332,736 00	$ 342,717 96	$ 352,999 56	$ 363,589 56	$ 374,497 20
[illegible]	[illegible]	$ 140,625 84	$ 144,844 56	$ 149,189 88	$ 153,665 64	$ 158,275 68	$ 163,023 84	$ 167,914 56	$ 172,951 92	$ 178,140 48	$ 183,484 68
[illegible]	[illegible]	$ 72,735 24	$ 74,917 20	$ 77,164 68	$ 79,479 72	$ 81,864 00	$ 84,320 04	$ 86,849 64	$ 89,455 20	$ 92,138 76	$ 94,902 96
[illegible]	[illegible]	$ 44,014 68	$ 45,335 04	$ 46,695 12	$ 48,095 88	$ 49,538 76	$ 51,024 96	$ 52,555 68	$ 54,132 36	$ 55,756 44	$ 57,429 00
[illegible]	[illegible]	$ 22,764 72	$ 23,447 76	$ 24,151 08	$ 24,875 76	$ 25,622 04	$ 26,390 64	$ 27,182 28	$ 27,997 80	$ 28,837 68	$ 29,702 88
[illegible]	[illegible]	$ 66,280 44	$ 68,268 84	$ 70,316 76	$ 72,426 36	$ 74,599 20	$ 76,837 20	$ 79,142 16	$ 81,516 48	$ 83,961 96	$ 86,480 88
[illegible]	[illegible]	$ 34,281 48	$ 35,309 88	$ 36,369 24	$ 37,460 40	$ 38,584 20	$ 39,741 60	$ 40,933 92	$ 42,161 88	$ 43,426 80	$ 44,729 52
[illegible]	[illegible]	$ 16,819 08	$ 17,323 56	$ 17,843 40	$ 18,378 60	$ 18,929 88	$ 19,497 84	$ 20,082 72	$ 20,685 24	$ 21,305 76	$ 21,944 88
[illegible]	[illegible]	$ 5,418 36	$ 5,580 96	$ 5,748 36	$ 5,920 80	$ 6,098 40	$ 6,281 40	$ 6,469 80	$ 6,663 96	$ 6,863 88	$ 7,069 80
[illegible]	[illegible]	$ 51,302 16	$ 52,841 16	$ 54,426 36	$ 56,059 32	$ 57,741 00	$ 59,473 20	$ 61,257 48	$ 63,095 16	$ 64,988 04	$ 66,937 56
[illegible]	[illegible]	$ 27,658 08	$ 28,487 88	$ 29,342 52	$ 30,222 72	$ 31,129 32	$ 32,063 16	$ 33,025 20	$ 34,016 04	$ 35,036 40	$ 36,087 60
[illegible]	[illegible]	$ 217,737 72	$ 224,269 92	$ 230,998 08	$ 237,927 96	$ 245,065 80	$ 252,417 72	$ 259,990 20	$ 267,790 08	$ 275,823 72	$ 284,098 44
[illegible]	[illegible]	$ 127,404 12	$ 131,226 24	$ 135,162 96	$ 139,217 88	$ 143,394 48	$ 147,696 36	$ 152,127 24	$ 156,690 96	$ 161,391 72	$ 166,233 48
[illegible]	[illegible]	$ 100,231 32	$ 103,238 28	$ 106,335 48	$ 109,525 56	$ 112,811 40	$ 116,195 52	$ 119,681 52	$ 123,272 04	$ 126,970 08	$ 130,779 24
[illegible]	[illegible]	$ 60,143 52	$ 61,947 72	$ 63,806 16	$ 65,720 40	$ 67,692 00	$ 69,722 64	$ 71,814 36	$ 73,968 96	$ 76,187 88	$ 78,473 64
[illegible]	[illegible]	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
[illegible]	[illegible]	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
[illegible]	[illegible]	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
[illegible]	[illegible]	$ 7,121 16	$ 7,326 36	$ 7,535 16	$ 7,750 08	$ 7,971 48	$ 7,829 64	$ 8,067 96	$ 8,309 88	$ 8,559 00	$ 8,815 68
[illegible]	[illegible]	$ 39,563 16	$ 40,703 76	$ 41,863 56	$ 43,058 04	$ 44,288 52	$ 43,500 84	$ 44,823 24	$ 46,167 72	$ 47,552 52	$ 48,978 84
[illegible]	[illegible]	$ 5,231 16	$ 5,388 24	$ 5,549 76	$ 5,716 32	$ 5,887 80	$ 6,064 56	$ 6,246 48	$ 6,433 80	$ 6,626 76	$ 6,825 60
[illegible]	[illegible]	$ 1,054 08	$ 1,085 64	$ 1,118 16	$ 1,151 76	$ 1,186 32	$ 1,221 84	$ 1,258 56	$ 1,296 36	$ 1,335 24	$ 1,375 32
[illegible]	[illegible]	$ 138,165 84	$ 142,310 88	$ 146,580 12	$ 150,977 52	$ 155,506 80	$ 160,172 16	$ 164,977 32	$ 169,926 48	$ 175,024 32	$ 180,275 04
[illegible]	[illegible]	$ 12,201 24	$ 12,567 36	$ 12,944 40	$ 13,332 72	$ 13,732 68	$ 14,144 64	$ 14,568 96	$ 15,006 12	$ 15,456 24	$ 15,920 04
[illegible]	[illegible]	$ 13,098 84	$ 13,491 84	$ 13,896 60	$ 14,313 48	$ 14,742 96	$ 15,185 16	$ 15,640 80	$ 16,109 88	$ 16,593 24	$ 17,091 00
[illegible]	[illegible]	$ 16,383 84	$ 16,875 24	$ 17,381 52	$ 17,903 04	$ 18,440 16	$ 18,993 24	$ 19,563 12	$ 20,149 92	$ 20,754 48	$ 21,377 16
[illegible]	[illegible]	$ 7,218 12	$ 7,434 60	$ 7,657 68	$ 7,887 48	$ 8,124 00	$ 8,367 72	$ 8,618 76	$ 8,877 36	$ 9,143 64	$ 9,417 96
[illegible]	[illegible]	$ 3,609 12	$ 3,717 48	$ 3,828 84	$ 3,943 80	$ 4,062 12	$ 4,183 92	$ 4,309 44	$ 4,438 80	$ 4,571 88	$ 4,709 04
[illegible]	[illegible]	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
[illegible]	[illegible]	$ 64,103 88	$ 65,952 24	$ 67,831 32	$ 69,766 80	$ 71,760 36	$ 70,484 16	$ 72,626 88	$ 74,805 24	$ 77,049 00	$ 79,360 08
[illegible]	[illegible]	$ 29,304 60	$ 30,149 40	$ 31,008 60	$ 31,893 60	$ 32,805 00	$ 32,221 20	$ 33,201 00	$ 34,196 40	$ 35,222 40	$ 36,279 00

Note: The Commonwealth has established mult

Baseline Units - Volumetrics

		Annual Costs									
Resource Description	**Service Tier / Configuration (6)**	**Year 1**	**Year 2**	**Year 3**	**Year 4**	**Year 5**	**Year 6**	**Year 7**	**Opt - Year 8**	**Opt - Year 9**	**Opt - Year 10**
		$ 4,151 52	$ 4,271 16	$ 4,392 84	$ 4,518 24	$ 4,647 36	$ 4,564 68	$ 4,703 40	$ 4,844 52	$ 4,989 84	$ 5,139 48
		$ 4,158 00	$ 4,284 00	$ 4,410 00	$ 4,536 00	$ 4,662 00	$ 4,578 00	$ 4,704 00	$ 4,872 00	$ 4,998 00	$ 5,166 00
		$ 1,030 20	$ 1,059 96	$ 1,090 20	$ 1,121 28	$ 1,153 32	$ 1,132 80	$ 1,167 24	$ 1,202 28	$ 1,238 28	$ 1,275 48
		$ 915 72	$ 942 12	$ 969 00	$ 996 72	$ 1,025 16	$ 1,006 92	$ 1,037 52	$ 1,068 60	$ 1,100 76	$ 1,133 76
		$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
		$ 2,536 32	$ 2,609 52	$ 2,683 68	$ 2,760 48	$ 2,839 20	$ 2,788 80	$ 2,873 52	$ 2,959 68	$ 3,048 48	$ 3,139 92
		$ 154,071 24	$ 158,693 40	$ 163,454 16	$ 168,357 84	$ 173,408 52	$ 178,610 88	$ 183,969 12	$ 189,488 28	$ 195,172 80	$ 201,028 08
		$ 97,528 80	$ 100,454 76	$ 103,468 44	$ 106,572 48	$ 109,769 64	$ 113,062 68	$ 116,454 60	$ 119,948 28	$ 123,546 72	$ 127,253 04
		$ 97,528 80	$ 100,454 76	$ 103,468 44	$ 106,572 48	$ 109,769 64	$ 113,062 68	$ 116,454 60	$ 119,948 28	$ 123,546 72	$ 127,253 04
		$ 97,528 80	$ 100,454 76	$ 103,468 44	$ 106,572 48	$ 109,769 64	$ 113,062 68	$ 116,454 60	$ 119,948 28	$ 123,546 72	$ 127,253 04
		$ 97,528 80	$ 100,454 76	$ 103,468 44	$ 106,572 48	$ 109,769 64	$ 113,062 68	$ 116,454 60	$ 119,948 28	$ 123,546 72	$ 127,253 04
		$ 133,628 88	$ 137,637 60	$ 141,766 80	$ 146,019 84	$ 150,400 44	$ 154,912 44	$ 159,559 80	$ 164,346 48	$ 169,276 92	$ 174,355 32
		$ 97,528 80	$ 100,454 76	$ 103,468 44	$ 106,572 48	$ 109,769 64	$ 113,062 68	$ 116,454 60	$ 119,948 28	$ 123,546 72	$ 127,253 04
		$ 105,158 04	$ 108,312 72	$ 111,562 08	$ 114,908 88	$ 118,356 24	$ 121,906 92	$ 125,564 04	$ 129,331 08	$ 133,210 92	$ 137,207 28
		$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
		$ 3,555 00	$ 3,657 48	$ 3,761 64	$ 3,869 04	$ 3,979 56	$ 3,908 76	$ 4,027 56	$ 4,148 40	$ 4,272 84	$ 4,401 00
		$ 12,918 60	$ 13,291 08	$ 13,669 68	$ 14,059 80	$ 14,461 56	$ 14,204 28	$ 14,636 16	$ 15,075 12	$ 15,527 28	$ 15,993 12
		$ 33,368 76	$ 34,330 92	$ 35,309 04	$ 36,316 56	$ 37,354 32	$ 36,690 00	$ 37,805 28	$ 38,939 28	$ 40,107 24	$ 41,310 24
		$ 5,406 00	$ 5,562 00	$ 5,720 40	$ 5,883 60	$ 6,051 60	$ 5,944 20	$ 6,124 80	$ 6,308 40	$ 6,497 40	$ 6,692 40
		$ 892 80	$ 919 80	$ 945 00	$ 972 00	$ 1,000 80	$ 982 80	$ 1,011 60	$ 1,042 20	$ 1,074 60	$ 1,105 20
		$ 3,581 04	$ 3,684 24	$ 3,789 36	$ 3,897 36	$ 4,008 72	$ 3,937 44	$ 4,057 20	$ 4,178 88	$ 4,304 16	$ 4,433 28
		$ 896 64	$ 922 32	$ 948 72	$ 975 84	$ 1,003 68	$ 985 68	$ 1,015 68	$ 1,046 16	$ 1,077 60	$ 1,110 00
		$ 412,106 16	$ 68,684 76	$ 68,684 76	$ 68,684 76	$ 68,684 76	$ 68,684 76	$ 68,684 76	$ 68,684 76	$ 68,684 76	$ 68,684 76
		$ 21,421 68	$ 22,039 44	$ 22,667 28	$ 23,314 08	$ 23,980 32	$ 23,553 84	$ 24,269 76	$ 24,997 68	$ 25,747 68	$ 26,520 00
		$ 3,999 96	$ 4,115 52	$ 4,232 52	$ 4,353 48	$ 4,477 68	$ 4,398 12	$ 4,532 04	$ 4,667 76	$ 4,807 80	$ 4,952 16
		$ 10,710 84	$ 11,019 72	$ 11,333 64	$ 11,657 04	$ 11,990 16	$ 11,776 92	$ 12,134 88	$ 12,498 84	$ 12,873 84	$ 13,260 00
		$ 2,000 16	$ 2,057 76	$ 2,116 44	$ 2,176 56	$ 2,238 84	$ 2,199 24	$ 2,265 84	$ 2,333 88	$ 2,404 08	$ 2,476 08
		$ 1,333 32	$ 1,371 84	$ 1,410 84	$ 1,451 16	$ 1,492 56	$ 1,466 04	$ 1,510 68	$ 1,555 92	$ 1,602 60	$ 1,650 72
		$ 3,999 96	$ 4,115 52	$ 4,232 52	$ 4,353 48	$ 4,477 68	$ 4,398 12	$ 4,532 04	$ 4,667 76	$ 4,807 80	$ 4,952 16
		$ 2,212 08	$ 2,340 48	$ 2,407 20	$ 2,475 84	$ 2,546 64	$ 2,501 76	$ 2,577 60	$ 2,655 12	$ 2,734 56	$ 2,816 64
		$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
		$ 15 84	$ 16 08	$ 16 56	$ 17 04	$ 17 52	$ 17 28	$ 17 76	$ 18 24	$ 18 96	$ 19 44
Total Third Party Software		**$ 7,074,607.68**	**$ 6,905,919.00**	**$ 7,088,633.64**	**$ 7,276,653.48**	**$ 7,470,086.76**	**$ 7,541,689.44**	**$ 7,747,877.64**	**$ 7,958,784.12**	**$ 8,175,742.44**	**$ 8,399,046.12**

Total Charges

Description	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Total Base Term	Opt - Year 8	Opt - Year 9	Opt - Year 10	Total Renewal Years	Total Base Term + Renewal Years
Total Charges Summary													
Server - Fully Managed													
Total - Fully Managed - x86 Physical - All Support Tiers (Window, Linux)	$24,725,795 04	$23,453,067 96	$22,165,262 76	$19,367,666 16	$16,272,287 52	$13,125,208 32	$10,532,598 12	$129,641,885 88	$10,046,537 40	$9,528,284 88	$9,343,989 24	$28,918,811 52	$158,560,697 40
Total - Fully Managed - x86 Virtual - All Support Tiers (Window, Linux)	$14,791,301 52	$15,488,721 72	$16,207,417 08	$15,651,092 88	$14,457,552 24	$12,911,412 72	$11,514,666 12	$101,022,164 28	$12,096,267 12	$12,687,841 80	$13,367,647 20	$38,151,756 12	$139,173,920 40
Total - Fully Managed - P-Series (AIX) - All Support Tiers (Window, Linux)	$5,744,240 64	$6,143,544 96	$6,591,558 12	$7,042,475 16	$7,506,059 64	$7,572,329 76	$7,882,290 60	$48,482,498 88	$8,277,058 68	$8,658,388 56	$9,157,749 12	$26,093,196 36	$74,575,695 24
Server - Managed Only													
Total Managed Only- x86 - All Support Tiers (Window, Linux)	$18,929,742 00	$11,329,574 40	$6,780,812 40	$3,743,959 56	$1,012,416 00	$860,550 00	$731,472 00	$43,388,526 36	$731,472 00	$731,472 00	$731,472 00	$2,194,416 00	$45,582,942 36
Total Managed Only- P-Series - All Support Tiers (AIX)	$833,964 37	$514,529 78	$315,738 00	$398,325 60	$409,563 60	$389,971 20	$386,190 00	$3,248,282 55	$386,190 00	$386,190 00	$386,190 00	$1,158,570 00	$4,406,852 55
Storage and Backup - Fully Managed													
Total Enterprise Storage - Fully Managed	$3,108,947 37	$3,321,120 00	$3,537,072 00	$3,825,294 00	$3,663,178 20	$3,952,191 48	$4,177,339 68	$25,585,142 73	$4,595,075 16	$5,054,583 84	$5,560,040 28	$15,209,699 28	$40,794,842 01
Total Tape and Backup - Fully Managed	$670,800 00	$736,560 00	$809,490 00	$889,640 40	$503,359 56	$551,762 40	$606,937 56	$4,768,549 92	$667,632 00	$734,393 76	$807,833 88	$2,209,859 64	$6,978,409 56
Limited Co-Lo (Data Center Only Charge)													
Total Limited Co-Lo (Data Center Only Charge)	$553,420 80	$555,144 00	$556,857 60	$559,315 20	$309,890 40	$310,946 40	$312,079 20	$3,157,653 60	$312,079 20	$312,079 20	$312,079 20	$936,237 60	$4,093,891 20
Mainframe Services													
Total IBM Services	$1,852,560 00	$1,780,320 00	$1,696,200 00	$1,636,080 00	$1,551,960 00	$1,491,720 00	$1,395,720 00	$11,404,560 00	$1,395,720 00	$1,395,720 00	$1,395,720 00	$4,187,160 00	$15,591,720 00
Total - IBM Mainframe Services - All Support Tiers	$8,664,267 24	$14,322,648 00	$19,980,408 72	$19,630,119 72	$19,299,401 52	$18,443,941 20	$18,149,902 08	$118,490,688 48	$18,149,902 08	$18,149,902 08	$18,149,902 08	$54,449,706 24	$172,940,394 72
Total Unisys Services	$256,560 00	$256,320 00	$256,200 00	$256,080 00	$255,960 00	$207,720 00	$207,720 00	$1,696,560 00	$207,720 00	$207,720 00	$207,720 00	$623,160 00	$2,319,720 00
Total - Unisys Mainframe Services - All Support Tiers	$18,961,515 84	$18,941,514 36	$18,591,020 88	$18,631,855 56	$18,645,294 84	$18,166,046 52	$18,196,126 80	$130,133,374 80	$18,196,126 80	$18,196,126 80	$18,196,126 80	$54,588,380 40	$184,721,755 20
On-Demand (IaaS)													
Total IaaS Servers - x86 (Windows, Linux) - Virtual Servers	$172,475 07	$208,016 64	$249,910 80	$274,581 24	$294,876 72	$305,466 48	$322,262 88	$1,827,589 83	$386,012 16	$462,136 56	$509,026 32	$1,357,175 04	$3,184,764 87
Total IaaS Storage On-Demand	$7,287 38	$8,604 00	$9,885 60	$11,123 76	$12,100 68	$13,017 36	$13,646 16	$75,664 94	$16,370 88	$19,638 00	$23,559 60	$59,568 48	$135,233 42
Total IaaS Backup On-Demand	$480 00	$576 00	$691 20	$829 44	$497 64	$597 24	$716 64	$4,388 16	$859 92	$1,032 00	$1,238 40	$3,130 32	$7,518 48
Reserve Account													
Reserve Account	$1,008,000 00	$1,008,000 00	$1,008,000 00	$1,008,000 00	$1,008,000 00	$1,008,000 00	$1,008,000 00	$7,056,000 00	$1,008,000 00	$1,008,000 00	$1,008,000 00	$3,024,000 00	$10,080,000 00
Third Party Software													
Total Third Party Software	$7,074,607 68	$6,905,919 00	$7,088,633 64	$7,276,653 48	$7,470,086 76	$7,541,689 44	$7,747,877 64	$51,105,467 64	$7,958,784 12	$8,175,742 44	$8,399,046 12	$24,533,572 68	$75,639,040 32
Yearly Total	**$107,355,964.95**	**$104,974,180.82**	**$105,845,158.80**	**$100,203,092.16**	**$92,672,485.32**	**$86,852,570.52**	**$83,185,545.48**	**$681,088,998.06**	**$84,431,807.52**	**$85,709,251.92**	**$87,557,340.24**	**$257,698,399.68**	**$938,787,397.74**

Services (Base Term)	**$681,088,998.06**
Grand Total Base Term	**$681,088,998.06**
Services (Renewal Years)	**$257,698,399.68**
Grand Total w/ Renewal Years	**$938,787,397.74**

Technical Staff Rate Card

Staff Hourly Rate (*)										
Resource Description	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Infrastructure (mainframe, mid-range and x86) Architects/Engineers	$130.00	$132.00	$135.00	$137.00	$140.00	$142.00	$145.00	$148.00	$150.00	$153.00
Microsoft Product Specialists (e.g. Exchange, SharePoint)	$130.00	$132.00	$135.00	$137.00	$140.00	$142.00	$145.00	$148.00	$150.00	$153.00
Basis and SAP Oracle support	$190.00	$194.00	$199.00	$203.00	$207.00	$212.00	$217.00	$221.00	$226.00	$231.00
Performance Specialists	$130.00	$132.00	$135.00	$137.00	$140.00	$142.00	$145.00	$148.00	$150.00	$153.00
Mainframe Systems Programmers	$104.00	$106.00	$108.00	$110.00	$112.00	$114.00	$116.00	$118.00	$120.00	$123.00
Batch Administrators	$93.00	$95.00	$96.00	$98.00	$100.00	$102.00	$104.00	$106.00	$108.00	$110.00
3rd Party Software Product Specialists	$130.00	$132.00	$135.00	$137.00	$140.00	$142.00	$145.00	$148.00	$150.00	$153.00
System Administrator (Windows, AIX, Linux)	$130.00	$132.00	$135.00	$137.00	$140.00	$142.00	$145.00	$148.00	$150.00	$153.00
System Administrator (Middleware support)	$104.00	$106.00	$108.00	$110.00	$112.00	$114.00	$116.00	$118.00	$120.00	$123.00
Storage Administrator	$104.00	$106.00	$108.00	$110.00	$112.00	$114.00	$116.00	$118.00	$120.00	$123.00
Data Backup Administrator	$93.00	$95.00	$96.00	$98.00	$100.00	$102.00	$104.00	$106.00	$108.00	$110.00
Database Administrator	$210.00	$215.00	$220.00	$225.00	$230.00	$235.00	$240.00	$245.00	$250.00	$256.00
Database Architects	$172.00	$175.00	$179.00	$182.00	$185.00	$189.00	$192.00	$196.00	$200.00	$204.00
Database Analysts	$100.00	$102.00	$104.00	$106.00	$108.00	$110.00	$112.00	$114.00	$116.00	$118.00
Project Management Support	$148.00	$151.00	$154.00	$157.00	$159.00	$162.00	$166.00	$169.00	$172.00	$175.00
Network Administrator	$130.00	$132.00	$135.00	$137.00	$140.00	$142.00	$145.00	$148.00	$150.00	$153.00
Facilities Administrator	$72.00	$74.00	$75.00	$77.00	$78.00	$79.00	$81.00	$82.00	$84.00	$86.00
Security Administrator	$130.00	$132.00	$135.00	$137.00	$140.00	$142.00	$145.00	$148.00	$150.00	$153.00
Security Architects	$172.00	$175.00	$179.00	$182.00	$185.00	$189.00	$192.00	$196.00	$200.00	$204.00
Security Analysts	$100.00	$102.00	$104.00	$106.00	$108.00	$110.00	$112.00	$114.00	$116.00	$118.00
Asset Management Administrator	$67.00	$68.00	$69.00	$71.00	$72.00	$73.00	$75.00	$76.00	$78.00	$79.00
Quality Assurance Support	$85.00	$87.00	$89.00	$90.00	$92.00	$94.00	$95.00	$97.00	$99.00	$101.00
Remedy Support Specialist	$157.00	$160.00	$163.00	$166.00	$169.00	$173.00	$176.00	$179.00	$183.00	$186.00
IT Service Continuity Specialist	$130.00	$132.00	$135.00	$137.00	$140.00	$142.00	$145.00	$148.00	$150.00	$153.00

(*) Rates are "Not to Exceed Rates" and can be negotiated per order.

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	Product Name	Unit	Qty per config	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
* Note: This data is sample data provided as an example. The data contained do not contain actual prices or product information.																			
* Sample Data ==>	Mainframe_Dorado_MIPS	Per MIP		ABC51323698	45687	1245	rv 5.0.1	FDCFG12599	XYZ123	$0.001	$0.001	$0.001	$0.001	$0.001	$0.001	$0.001	$0.001	$0.001	$0.001
* Sample Data ==>	VirtualServer_Windows2008_vCPU	Per VCPU		ABC51323699	45688	1246	rv 5.0.2	FDCFG12600	XYZ124	$0.002	$0.002	$0.002	$0.002	$0.002	$0.002	$0.002	$0.002	$0.002	$0.002
* Sample Data ==>	VirtualServer_Windows2008_vRAM	Per Gig		ABC51323700	45689	1247	rv 5.0.3	FDCFG12601	XYZ125	$0.003	$0.003	$0.003	$0.003	$0.003	$0.003	$0.003	$0.003	$0.003	$0.003
* Sample Data ==>	VirtualServer_Windows2008_Gig_Diskspace_Tier1	Per Gig		ABC51323701	45690	1248	rv 5.0.4	FDCFG12602	XYZ126	$0.004	$0.004	$0.004	$0.004	$0.004	$0.004	$0.004	$0.004	$0.004	$0.004
* Sample Data ==>	VirtualServer_Windows2008_Gig_Diskspace_Tier2	Per Gig		ABC51323702	45691	1249	rv 5.0.5	FDCFG12603	XYZ127	$0.005	$0.005	$0.005	$0.005	$0.005	$0.005	$0.005	$0.005	$0.005	$0.005
* Sample Data ==>	VirtualServer_Windows2008_IIS_Feature	Per Instance		ABC51323703	45692	1250	rv 5.0.6	FDCFG12604	XYZ128	$0.006	$0.006	$0.006	$0.006	$0.006	$0.006	$0.006	$0.006	$0.006	$0.006
* Sample Data ==>	VirtualServer_Windows2008_WebServer_Feature	Per Instance		ABC51323704	45693	1251	rv 5.0.7	FDCFG12605	XYZ129	$0.007	$0.007	$0.007	$0.007	$0.007	$0.007	$0.007	$0.007	$0.007	$0.007
* Sample Data ==>	Backup_Service_Disk	Per Server		ABC51323705	45694	1252	rv 5.0.8	FDCFG12606	XYZ130	$0.008	$0.008	$0.008	$0.008	$0.008	$0.008	$0.008	$0.008	$0.008	$0.008
* Sample Data ==>	SSL_Certificate	Per Cert		ABC51323706	45695	1253	rv 5.0.9	FDCFG12607	XYZ131	$0.009	$0.009	$0.009	$0.009	$0.009	$0.009	$0.009	$0.009	$0.009	$0.009
Server - Fully Managed (1)																			
x86 Server Configurations (Windows)																			
Windows pConfig - 1	2-way Quad-Core 2.0 GHz	Per Server		CCSU13310001-A						$ 28.41	$ 28.34	$ 28.27	$ 26.00	$ 22.88	$ 19.45	$ 16.53	$ 16.53	$ 16.53	$ 16.53
Windows pConfig - 2 4 5	2-way Six-Core 2.4 GHz	Per Server		CCSU13310002-A						$ 58.53	$ 58.38	$ 58.24	$ 53.58	$ 47.15	$ 40.08	$ 34.07	$ 34.07	$ 34.07	$ 34.07
Windows pConfig - 3	4-way Six-Core 2.0 GHz	Per Server		CCSU13310003-A						$ 48.01	$ 47.89	$ 47.77	$ 43.94	$ 38.67	$ 32.87	$ 27.94	$ 27.94	$ 27.94	$ 27.94
Windows pConfig - 1 2 3 4 5	GB RAM	Per GB		CCSU13310004-A						$ 0.02	$ 0.02	$ 0.02	$ 0.02	$ 0.02	$ 0.02	$ 0.01	$ 0.01	$ 0.01	$ 0.01
Windows pConfig - 1, 2, 4, 5	Mirrored 146 15K Hard Drives	Per Primary + Mirror drive		CCSU13310005-A						$ 14.63	$ 14.60	$ 14.56	$ 13.39	$ 11.79	$ 10.02	$ 8.52	$ 8.52	$ 8.52	$ 8.52
Windows pConfig - 3	SAN Attached Storage	Per GB		CCSU13310006-A						$ 0.15	$ 0.15	$ 0.14	$ 0.13	$ 0.12	$ 0.10	$ 0.08	$ 0.08	$ 0.08	$ 0.08
Windows pConfig - 1, 2, 3, 4, 5	Windows Server 2008 R2	Per License		CCSU13310007-A						$ 162.58	$ 162.18	$ 161.77	$ 148.83	$ 130.97	$ 111.33	$ 94.63	$ 94.63	$ 94.63	$ 94.63
Windows pConfig - 4	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization Site s Local SAN Storage from hourly data synchronization	Per Service		CCSU13310008-A						$ 308.91	$ 308.14	$ 307.37	$ 282.78	$ 248.85	$ 211.52	$ 179.79	$ 179.79	$ 179.79	$ 179.79
Windows pConfig - 5	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Service		CCSU13310009-A						$ 236.12	$ 235.54	$ 234.95	$ 216.15	$ 190.21	$ 161.68	$ 137.43	$ 137.43	$ 137.43	$ 137.43
Windows pConfig - 1	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310010-A						$ 378.79	$ 377.85	$ 376.90	$ 346.75	$ 305.14	$ 259.37	$ 220.47	$ 220.47	$ 220.47	$ 220.47
Windows pConfig - 1	Fully Managed (1) - Gold Tier	Per Config		CCSU13310011-A						$ 374.84	$ 373.90	$ 372.97	$ 343.13	$ 301.96	$ 256.66	$ 218.16	$ 218.16	$ 218.16	$ 218.16
Windows pConfig - 1	Fully Managed (1) - Silver Tier	Per Config		CCSU13310012-A						$ 372.88	$ 371.95	$ 371.02	$ 341.34	$ 300.38	$ 255.32	$ 217.02	$ 217.02	$ 217.02	$ 217.02
Windows pConfig - 1	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310013-A						$ 372.14	$ 371.22	$ 370.29	$ 340.67	$ 299.79	$ 254.82	$ 216.60	$ 216.60	$ 216.60	$ 216.60
Windows pConfig - 1	Fully Managed (1) - Basic Tier	Per Config		CCSU13310014-A						$ 370.86	$ 369.93	$ 369.01	$ 339.49	$ 298.75	$ 253.94	$ 215.85	$ 215.85	$ 215.85	$ 215.85
Windows pConfig - 2	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310015-A						$ 378.79	$ 377.85	$ 376.90	$ 346.75	$ 305.14	$ 259.37	$ 220.47	$ 220.47	$ 220.47	$ 220.47
Windows pConfig - 2	Fully Managed (1) - Gold Tier	Per Config		CCSU13310016-A						$ 374.84	$ 373.90	$ 372.97	$ 343.13	$ 301.96	$ 256.66	$ 218.16	$ 218.16	$ 218.16	$ 218.16
Windows pConfig - 2	Fully Managed (1) - Silver Tier	Per Config		CCSU13310017-A						$ 372.88	$ 371.95	$ 371.02	$ 341.34	$ 300.38	$ 255.32	$ 217.02	$ 217.02	$ 217.02	$ 217.02
Windows pConfig - 2	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310018-A						$ 372.14	$ 371.22	$ 370.29	$ 340.67	$ 299.79	$ 254.82	$ 216.60	$ 216.60	$ 216.60	$ 216.60
Windows pConfig - 2	Fully Managed (1) - Basic Tier	Per Config		CCSU13310019-A						$ 370.86	$ 369.93	$ 369.01	$ 339.49	$ 298.75	$ 253.94	$ 215.85	$ 215.85	$ 215.85	$ 215.85
Windows pConfig - 3	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310020-A						$ 378.79	$ 377.85	$ 376.90	$ 346.75	$ 305.14	$ 259.37	$ 220.47	$ 220.47	$ 220.47	$ 220.47
Windows pConfig - 3	Fully Managed (1) - Gold Tier	Per Config		CCSU13310021-A						$ 374.84	$ 373.90	$ 372.97	$ 343.13	$ 301.96	$ 256.66	$ 218.16	$ 218.16	$ 218.16	$ 218.16
Windows pConfig - 3	Fully Managed (1) - Silver Tier	Per Config		CCSU13310022-A						$ 372.88	$ 371.95	$ 371.02	$ 341.34	$ 300.38	$ 255.32	$ 217.02	$ 217.02	$ 217.02	$ 217.02
Windows pConfig - 3	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310023-A						$ 372.14	$ 371.22	$ 370.29	$ 340.67	$ 299.79	$ 254.82	$ 216.60	$ 216.60	$ 216.60	$ 216.60
Windows pConfig - 3	Fully Managed (1) - Basic Tier	Per Config		CCSU13310024-A						$ 370.86	$ 369.93	$ 369.01	$ 339.49	$ 298.75	$ 253.94	$ 215.85	$ 215.85	$ 215.85	$ 215.85
Windows pConfig - 4	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310025-A						$ 424.15	$ 423.09	$ 422.04	$ 388.28	$ 341.68	$ 290.43	$ 246.87	$ 246.87	$ 246.87	$ 246.87
Windows pConfig - 4	Fully Managed (1) - Gold Tier	Per Config		CCSU13310026-A						$ 418.10	$ 417.06	$ 416.02	$ 382.73	$ 336.81	$ 286.29	$ 243.34	$ 243.34	$ 243.34	$ 243.34
Windows pConfig - 4	Fully Managed (1) - Silver Tier	Per Config		CCSU13310027-A						$ 414.22	$ 413.19	$ 412.16	$ 379.19	$ 333.68	$ 283.63	$ 241.09	$ 241.09	$ 241.09	$ 241.09
Windows pConfig - 4	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310028-A						$ 412.59	$ 411.57	$ 410.54	$ 377.70	$ 332.37	$ 282.52	$ 240.14	$ 240.14	$ 240.14	$ 240.14
Windows pConfig - 4	Fully Managed (1) - Basic Tier	Per Config		CCSU13310029-A						$ 410.45	$ 409.43	$ 408.41	$ 375.73	$ 330.65	$ 281.05	$ 238.89	$ 238.89	$ 238.89	$ 238.89
Windows pConfig - 5	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310030-A						$ 424.15	$ 423.09	$ 422.04	$ 388.28	$ 341.68	$ 290.43	$ 246.87	$ 246.87	$ 246.87	$ 246.87
Windows pConfig - 5	Fully Managed (1) - Gold Tier	Per Config		CCSU13310031-A						$ 418.10	$ 417.06	$ 416.02	$ 382.73	$ 336.81	$ 286.29	$ 243.34	$ 243.34	$ 243.34	$ 243.34
Windows pConfig - 5	Fully Managed (1) - Silver Tier	Per Config		CCSU13310032-A						$ 414.22	$ 413.19	$ 412.16	$ 379.19	$ 333.68	$ 283.63	$ 241.09	$ 241.09	$ 241.09	$ 241.09
Windows pConfig - 5	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310033-A						$ 412.59	$ 411.57	$ 410.54	$ 377.70	$ 332.37	$ 282.52	$ 240.14	$ 240.14	$ 240.14	$ 240.14
Windows pConfig - 5	Fully Managed (1) - Basic Tier	Per Config		CCSU13310034-A						$ 410.45	$ 409.43	$ 408.41	$ 375.73	$ 330.65	$ 281.05	$ 238.89	$ 238.89	$ 238.89	$ 238.89
Windows pConfig - 1	2-way Quad-Core 2.0 GHz		1							$ 28.41	$ 28.34	$ 28.27	$ 26.00	$ 22.88	$ 19.45	$ 16.53	$ 16.53	$ 16.53	$ 16.53
	GB RAM		4							$ 0.08	$ 0.08	$ 0.08	$ 0.08	$ 0.08	$ 0.08	$ 0.04	$ 0.04	$ 0.04	$ 0.04
	Mirrored 146 15K Hard Drives		1							$ 14.63	$ 14.60	$ 14.56	$ 13.39	$ 11.79	$ 10.02	$ 8.52	$ 8.52	$ 8.52	$ 8.52
	Windows Server 2008 R2		1							$ 162.58	$ 162.18	$ 161.77	$ 148.83	$ 130.97	$ 111.33	$ 94.63	$ 94.63	$ 94.63	$ 94.63

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	Product Name	Unit	Qty per config	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
	Sub-Total									**$ 205.70**	**$ 205.20**	**$ 204.68**	**$ 188.30**	**$ 165.72**	**$ 140.88**	**$ 119.72**	**$ 119.72**	**$ 119.72**	**$ 119.72**
Windows pConfig - 1	Fully Managed (1) - Platinum Tier		1							$ 584.49	$ 583.05	$ 581.58	$ 535.05	$ 470.86	$ 400.25	$ 340.19	$ 340.19	$ 340.19	$ 340.19
Windows pConfig - 1	Fully Managed (1) - Gold Tier		1							$ 580.54	$ 579.10	$ 577.65	$ 531.43	$ 467.68	$ 397.54	$ 337.88	$ 337.88	$ 337.88	$ 337.88
Windows pConfig - 1	Fully Managed (1) - Silver Tier		1							$ 578.58	$ 577.15	$ 575.70	$ 529.64	$ 466.10	$ 396.20	$ 336.74	$ 336.74	$ 336.74	$ 336.74
Windows pConfig - 1	Fully Managed (1) - Bronze Tier		1							$ 577.84	$ 576.42	$ 574.97	$ 528.97	$ 465.51	$ 395.70	$ 336.32	$ 336.32	$ 336.32	$ 336.32
Windows pConfig - 1	Fully Managed (1) - Basic Tier		1							$ 576.56	$ 575.13	$ 573.69	$ 527.79	$ 464.47	$ 394.82	$ 335.57	$ 335.57	$ 335.57	$ 335.57
Windows pConfig - 2	2-way Six-Core 2.4 GHz		1							$ 58.53	$ 58.38	$ 58.24	$ 53.58	$ 47.15	$ 40.08	$ 34.07	$ 34.07	$ 34.07	$ 34.07
	GB RAM		16							$ 0.32	$ 0.32	$ 0.32	$ 0.32	$ 0.32	$ 0.32	$ 0.16	$ 0.16	$ 0.16	$ 0.16
	Mirrored 146 15K Hard Drives		1							$ 14.63	$ 14.60	$ 14.56	$ 13.39	$ 11.79	$ 10.02	$ 8.52	$ 8.52	$ 8.52	$ 8.52
	Windows Server 2008 R2		1							$ 162.58	$ 162.18	$ 161.77	$ 148.83	$ 130.97	$ 111.33	$ 94.63	$ 94.63	$ 94.63	$ 94.63
	Sub-Total									**$ 236.06**	**$ 235.48**	**$ 234.89**	**$ 216.12**	**$ 190.23**	**$ 161.75**	**$ 137.38**	**$ 137.38**	**$ 137.38**	**$ 137.38**
Windows pConfig - 2	Fully Managed (1) - Platinum Tier		1							$ 614.85	$ 613.33	$ 611.79	$ 562.87	$ 495.37	$ 421.12	$ 357.85	$ 357.85	$ 357.85	$ 357.85
Windows pConfig - 2	Fully Managed (1) - Gold Tier		1							$ 610.90	$ 609.38	$ 607.86	$ 559.25	$ 492.19	$ 418.41	$ 355.54	$ 355.54	$ 355.54	$ 355.54
Windows pConfig - 2	Fully Managed (1) - Silver Tier		1							$ 608.94	$ 607.43	$ 605.91	$ 557.46	$ 490.61	$ 417.07	$ 354.40	$ 354.40	$ 354.40	$ 354.40
Windows pConfig - 2	Fully Managed (1) - Bronze Tier		1							$ 608.20	$ 606.70	$ 605.18	$ 556.79	$ 490.02	$ 416.57	$ 353.98	$ 353.98	$ 353.98	$ 353.98
Windows pConfig - 2	Fully Managed (1) - Basic Tier		1							$ 606.92	$ 605.41	$ 603.90	$ 555.61	$ 488.98	$ 415.69	$ 353.23	$ 353.23	$ 353.23	$ 353.23
Windows pConfig - 3	4-way Six-Core 2.0 GHz		1							$ 48.01	$ 47.89	$ 47.77	$ 43.94	$ 38.67	$ 32.87	$ 27.94	$ 27.94	$ 27.94	$ 27.94
	GB RAM		64							$ 1.28	$ 1.28	$ 1.28	$ 1.28	$ 1.28	$ 1.28	$ 0.64	$ 0.64	$ 0.64	$ 0.64
	SAN Attached Storage		500							$ 75.00	$ 75.00	$ 70.00	$ 65.00	$ 60.00	$ 50.00	$ 40.00	$ 40.00	$ 40.00	$ 40.00
	Windows Server 2008 R2		1							$ 162.58	$ 162.18	$ 161.77	$ 148.83	$ 130.97	$ 111.33	$ 94.63	$ 94.63	$ 94.63	$ 94.63
	Sub-Total									**$ 286.87**	**$ 286.35**	**$ 280.82**	**$ 259.05**	**$ 230.92**	**$ 195.48**	**$ 163.21**	**$ 163.21**	**$ 163.21**	**$ 163.21**
Windows pConfig - 3	Fully Managed (1) - Platinum Tier		1							$ 665.66	$ 664.20	$ 657.72	$ 605.80	$ 536.06	$ 454.85	$ 383.68	$ 383.68	$ 383.68	$ 383.68
Windows pConfig - 3	Fully Managed (1) - Gold Tier		1							$ 661.71	$ 660.25	$ 653.79	$ 602.18	$ 532.88	$ 452.14	$ 381.37	$ 381.37	$ 381.37	$ 381.37
Windows pConfig - 3	Fully Managed (1) - Silver Tier		1							$ 659.75	$ 658.30	$ 651.84	$ 600.39	$ 531.30	$ 450.80	$ 380.23	$ 380.23	$ 380.23	$ 380.23
Windows pConfig - 3	Fully Managed (1) - Bronze Tier		1							$ 659.01	$ 657.57	$ 651.11	$ 599.72	$ 530.71	$ 450.30	$ 379.81	$ 379.81	$ 379.81	$ 379.81
Windows pConfig - 3	Fully Managed (1) - Basic Tier		1							$ 657.73	$ 656.28	$ 649.83	$ 598.54	$ 529.67	$ 449.42	$ 379.06	$ 379.06	$ 379.06	$ 379.06
Windows pConfig - 4	2-way Six-Core 2.4 GHz		1							$ 58.53	$ 58.38	$ 58.24	$ 53.58	$ 47.15	$ 40.08	$ 34.07	$ 34.07	$ 34.07	$ 34.07
	GB RAM		16							$ 0.32	$ 0.32	$ 0.32	$ 0.32	$ 0.32	$ 0.32	$ 0.16	$ 0.16	$ 0.16	$ 0.16
	Mirrored 146 15K Hard Drives		1							$ 14.63	$ 14.60	$ 14.56	$ 13.39	$ 11.79	$ 10.02	$ 8.52	$ 8.52	$ 8.52	$ 8.52
	Windows Server 2008 R2		1							$ 162.58	$ 162.18	$ 161.77	$ 148.83	$ 130.97	$ 111.33	$ 94.63	$ 94.63	$ 94.63	$ 94.63
	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization Site s Local SAN Storage from hourly data synchronization		1							$ 308.91	$ 308.14	$ 307.37	$ 282.78	$ 248.85	$ 211.52	$ 179.79	$ 179.79	$ 179.79	$ 179.79
	Sub-Total									**$ 544.97**	**$ 543.62**	**$ 542.26**	**$ 498.90**	**$ 439.08**	**$ 373.27**	**$ 317.17**	**$ 317.17**	**$ 317.17**	**$ 317.17**
Windows pConfig - 4	Fully Managed (1) - Platinum Tier		1							$ 969.12	$ 966.71	$ 964.30	$ 887.18	$ 780.76	$ 663.70	$ 564.04	$ 564.04	$ 564.04	$ 564.04
Windows pConfig - 4	Fully Managed (1) - Gold Tier		1							$ 963.07	$ 960.68	$ 958.28	$ 881.63	$ 775.89	$ 659.56	$ 560.51	$ 560.51	$ 560.51	$ 560.51
Windows pConfig - 4	Fully Managed (1) - Silver Tier		1							$ 959.19	$ 956.81	$ 954.42	$ 878.09	$ 772.76	$ 656.90	$ 558.26	$ 558.26	$ 558.26	$ 558.26
Windows pConfig - 4	Fully Managed (1) - Bronze Tier		1							$ 957.56	$ 955.19	$ 952.80	$ 876.60	$ 771.45	$ 655.79	$ 557.31	$ 557.31	$ 557.31	$ 557.31
Windows pConfig - 4	Fully Managed (1) - Basic Tier		1							$ 955.42	$ 953.05	$ 950.67	$ 874.63	$ 769.73	$ 654.32	$ 556.06	$ 556.06	$ 556.06	$ 556.06
Windows pConfig - 5	2-way Six-Core 2.4 GHz		1							$ 58.53	$ 58.38	$ 58.24	$ 53.58	$ 47.15	$ 40.08	$ 34.07	$ 34.07	$ 34.07	$ 34.07
	GB RAM		16							$ 0.32	$ 0.32	$ 0.32	$ 0.32	$ 0.32	$ 0.32	$ 0.16	$ 0.16	$ 0.16	$ 0.16
	Mirrored 146 15K Hard Drives		1							$ 14.63	$ 14.60	$ 14.56	$ 13.39	$ 11.79	$ 10.02	$ 8.52	$ 8.52	$ 8.52	$ 8.52
	Windows Server 2008 R2		1							$ 162.58	$ 162.18	$ 161.77	$ 148.83	$ 130.97	$ 111.33	$ 94.63	$ 94.63	$ 94.63	$ 94.63
	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from Backup off-site tape Backups		1							$ 236.12	$ 235.54	$ 234.95	$ 216.15	$ 190.21	$ 161.68	$ 137.43	$ 137.43	$ 137.43	$ 137.43
	Sub-Total									**$ 472.18**	**$ 471.02**	**$ 469.84**	**$ 432.27**	**$ 380.44**	**$ 323.43**	**$ 274.81**	**$ 274.81**	**$ 274.81**	**$ 274.81**
Windows pConfig - 5	Fully Managed (1) - Platinum Tier		1							$ 896.33	$ 894.11	$ 891.88	$ 820.55	$ 722.12	$ 613.86	$ 521.68	$ 521.68	$ 521.68	$ 521.68
Windows pConfig - 5	Fully Managed (1) - Gold Tier		1							$ 890.28	$ 888.08	$ 885.86	$ 815.00	$ 717.25	$ 609.72	$ 518.15	$ 518.15	$ 518.15	$ 518.15
Windows pConfig - 5	Fully Managed (1) - Silver Tier		1							$ 886.40	$ 884.21	$ 882.00	$ 811.46	$ 714.12	$ 607.06	$ 515.90	$ 515.90	$ 515.90	$ 515.90
Windows pConfig - 5	Fully Managed (1) - Bronze Tier		1							$ 884.77	$ 882.59	$ 880.38	$ 809.97	$ 712.81	$ 605.95	$ 514.95	$ 514.95	$ 514.95	$ 514.95
Windows pConfig - 5	Fully Managed (1) - Basic Tier		1							$ 882.63	$ 880.45	$ 878.25	$ 808.00	$ 711.09	$ 604.48	$ 513.70	$ 513.70	$ 513.70	$ 513.70
x86 Server Configurations (Linux)																			
Linux pConfig - 1	2-way Quad-Core 2.0 GHz	Per Server		CCSU13310035-A						$ 28.41	$ 28.34	$ 28.27	$ 26.00	$ 22.88	$ 19.45	$ 16.53	$ 16.53	$ 16.53	$ 16.53
Linux pConfig - 2, 4, 5	2-way Six-Core 2.4 GHz	Per Server		CCSU13310036-A						$ 58.53	$ 58.38	$ 58.24	$ 53.58	$ 47.15	$ 40.08	$ 34.07	$ 34.07	$ 34.07	$ 34.07
Linux pConfig - 3	4-way Six-Core 2.0 GHz	Per Server		CCSU13310037-A						$ 48.01	$ 47.89	$ 47.77	$ 43.94	$ 38.67	$ 32.87	$ 27.94	$ 27.94	$ 27.94	$ 27.94
Linux pConfig - 1	GB RAM	Per GB		CCSU13310038-A						$ 0.02	$ 0.02	$ 0.02	$ 0.02	$ 0.02	$ 0.02	$ 0.01	$ 0.01	$ 0.01	$ 0.01
Linux pConfig - 1, 2, 4, 5	Mirrored 146 15K Hard Drives	Per Primary + Mirror drive		CCSU13310039-A						$ 14.63	$ 14.60	$ 14.56	$ 13.39	$ 11.79	$ 10.02	$ 8.52	$ 8.52	$ 8.52	$ 8.52
Linux pConfig - 3	SAN Attached Storage	Per GB		CCSU13310040-A						$ 0.15	$ 0.15	$ 0.14	$ 0.13	$ 0.12	$ 0.10	$ 0.08	$ 0.08	$ 0.08	$ 0.08
Linux pConfig - 1, 2, 3, 4 , 5	RedHat or SUSE	Per License		CCSU13310041-A						$ 139.57	$ 139.22	$ 138.87	$ 127.76	$ 112.43	$ 95.57	$ 81.23	$ 81.23	$ 81.23	$ 81.23

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	Product Name	Unit	Qty per config	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Linux pConfig - 4	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Service		CCSU13310042-A						$ 285.90	$ 285.18	$ 284.47	$ 261.71	$ 230.31	$ 195.76	$ 166.40	$ 166.40	$ 166.40	$ 166.40
Linux pConfig - 5	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Service		CCSU13310043-A						$ 213.11	$ 212.58	$ 212.05	$ 195.08	$ 171.67	$ 145.92	$ 124.03	$ 124.03	$ 124.03	$ 124.03
Linux pConfig - 1	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310044-A						$ 435.89	$ 434.81	$ 433.72	$ 399.02	$ 351.14	$ 298.47	$ 253.70	$ 253.70	$ 253.70	$ 253.70
Linux pConfig - 1	Fully Managed (1) - Gold Tier	Per Config		CCSU13310045-A						$ 422.92	$ 421.87	$ 420.82	$ 387.15	$ 340.69	$ 289.59	$ 246.15	$ 246.15	$ 246.15	$ 246.15
Linux pConfig - 1	Fully Managed (1) - Silver Tier	Per Config		CCSU13310046-A						$ 415.26	$ 414.23	$ 413.19	$ 380.14	$ 334.52	$ 284.34	$ 241.69	$ 241.69	$ 241.69	$ 241.69
Linux pConfig - 1	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310047-A						$ 411.92	$ 410.89	$ 409.87	$ 377.08	$ 331.83	$ 282.05	$ 239.75	$ 239.75	$ 239.75	$ 239.75
Linux pConfig - 1	Fully Managed (1) - Basic Tier	Per Config		CCSU13310048-A						$ 408.63	$ 407.61	$ 406.60	$ 374.07	$ 329.18	$ 279.80	$ 237.83	$ 237.83	$ 237.83	$ 237.83
Linux pConfig - 2	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310049-A						$ 435.89	$ 434.81	$ 433.72	$ 399.02	$ 351.14	$ 298.47	$ 253.70	$ 253.70	$ 253.70	$ 253.70
Linux pConfig - 2	Fully Managed (1) - Gold Tier	Per Config		CCSU13310050-A						$ 422.92	$ 421.87	$ 420.82	$ 387.15	$ 340.69	$ 289.59	$ 246.15	$ 246.15	$ 246.15	$ 246.15
Linux pConfig - 2	Fully Managed (1) - Silver Tier	Per Config		CCSU13310051-A						$ 415.26	$ 414.23	$ 413.19	$ 380.14	$ 334.52	$ 284.34	$ 241.69	$ 241.69	$ 241.69	$ 241.69
Linux pConfig - 2	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310052-A						$ 411.92	$ 410.89	$ 409.87	$ 377.08	$ 331.83	$ 282.05	$ 239.75	$ 239.75	$ 239.75	$ 239.75
Linux pConfig - 2	Fully Managed (1) - Basic Tier	Per Config		CCSU13310053-A						$ 408.63	$ 407.61	$ 406.60	$ 374.07	$ 329.18	$ 279.80	$ 237.83	$ 237.83	$ 237.83	$ 237.83
Linux pConfig - 3	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310054-A						$ 435.89	$ 434.81	$ 433.72	$ 399.02	$ 351.14	$ 298.47	$ 253.70	$ 253.70	$ 253.70	$ 253.70
Linux pConfig - 3	Fully Managed (1) - Gold Tier	Per Config		CCSU13310055-A						$ 422.92	$ 421.87	$ 420.82	$ 387.15	$ 340.69	$ 289.59	$ 246.15	$ 246.15	$ 246.15	$ 246.15
Linux pConfig - 3	Fully Managed (1) - Silver Tier	Per Config		CCSU13310056-A						$ 415.26	$ 414.23	$ 413.19	$ 380.14	$ 334.52	$ 284.34	$ 241.69	$ 241.69	$ 241.69	$ 241.69
Linux pConfig - 3	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310057-A						$ 411.92	$ 410.89	$ 409.87	$ 377.08	$ 331.83	$ 282.05	$ 239.75	$ 239.75	$ 239.75	$ 239.75
Linux pConfig - 3	Fully Managed (1) - Basic Tier	Per Config		CCSU13310058-A						$ 408.63	$ 407.61	$ 406.60	$ 374.07	$ 329.18	$ 279.80	$ 237.83	$ 237.83	$ 237.83	$ 237.83
Linux pConfig - 4	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310059-A						$ 536.37	$ 535.03	$ 533.70	$ 491.00	$ 432.08	$ 367.27	$ 312.18	$ 312.18	$ 312.18	$ 312.18
Linux pConfig - 4	Fully Managed (1) - Gold Tier	Per Config		CCSU13310060-A						$ 513.64	$ 512.36	$ 511.08	$ 470.20	$ 413.77	$ 351.71	$ 298.95	$ 298.95	$ 298.95	$ 298.95
Linux pConfig - 4	Fully Managed (1) - Silver Tier	Per Config		CCSU13310061-A						$ 497.95	$ 496.71	$ 495.47	$ 455.84	$ 401.14	$ 340.97	$ 289.82	$ 289.82	$ 289.82	$ 289.82
Linux pConfig - 4	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310062-A						$ 491.11	$ 489.88	$ 488.66	$ 449.57	$ 395.62	$ 336.28	$ 285.83	$ 285.83	$ 285.83	$ 285.83
Linux pConfig - 4	Fully Managed (1) - Basic Tier	Per Config		CCSU13310063-A						$ 484.60	$ 483.39	$ 482.19	$ 443.61	$ 390.38	$ 331.82	$ 282.05	$ 282.05	$ 282.05	$ 282.05
Linux pConfig - 5	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310064-A						$ 536.37	$ 535.03	$ 533.70	$ 491.00	$ 432.08	$ 367.27	$ 312.18	$ 312.18	$ 312.18	$ 312.18
Linux pConfig - 5	Fully Managed (1) - Gold Tier	Per Config		CCSU13310065-A						$ 513.64	$ 512.36	$ 511.08	$ 470.20	$ 413.77	$ 351.71	$ 298.95	$ 298.95	$ 298.95	$ 298.95
Linux pConfig - 5	Fully Managed (1) - Silver Tier	Per Config		CCSU13310066-A						$ 497.95	$ 496.71	$ 495.47	$ 455.84	$ 401.14	$ 340.97	$ 289.82	$ 289.82	$ 289.82	$ 289.82
Linux pConfig - 5	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310067-A						$ 491.11	$ 489.88	$ 488.66	$ 449.57	$ 395.62	$ 336.28	$ 285.83	$ 285.83	$ 285.83	$ 285.83
Linux pConfig - 5	Fully Managed (1) - Basic Tier	Per Config		CCSU13310068-A						$ 484.60	$ 483.39	$ 482.19	$ 443.61	$ 390.38	$ 331.82	$ 282.05	$ 282.05	$ 282.05	$ 282.05
Linux pConfig - 1	2-way Quad-Core 2.0 GHz		1							$ 28.41	$ 28.34	$ 28.27	$ 26.00	$ 22.88	$ 19.45	$ 16.53	$ 16.53	$ 16.53	$ 16.53
	4 GB RAM		4							$ 0.08	$ 0.08	$ 0.08	$ 0.08	$ 0.08	$ 0.08	$ 0.04	$ 0.04	$ 0.04	$ 0.04
	Mirrored 146 15K Hard Drives		1							$ 14.63	$ 14.60	$ 14.56	$ 13.39	$ 11.79	$ 10.02	$ 8.52	$ 8.52	$ 8.52	$ 8.52
	RedHat or SUSE		1							$ 139.57	$ 139.22	$ 138.87	$ 127.76	$ 112.43	$ 95.57	$ 81.23	$ 81.23	$ 81.23	$ 81.23
	Sub-Total									**$ 182.69**	**$ 182.24**	**$ 181.78**	**$ 167.23**	**$ 147.18**	**$ 125.12**	**$ 106.32**	**$ 106.32**	**$ 106.32**	**$ 106.32**
Linux pConfig - 1	Fully Managed (1) - Platinum Tier		1							$ 618.58	$ 617.05	$ 615.50	$ 566.25	$ 498.32	$ 423.59	$ 360.02	$ 360.02	$ 360.02	$ 360.02
Linux pConfig - 1	Fully Managed (1) - Gold Tier		1							$ 605.61	$ 604.11	$ 602.60	$ 554.38	$ 487.87	$ 414.71	$ 352.47	$ 352.47	$ 352.47	$ 352.47
Linux pConfig - 1	Fully Managed (1) - Silver Tier		1							$ 597.95	$ 596.47	$ 594.97	$ 547.37	$ 481.70	$ 409.46	$ 348.01	$ 348.01	$ 348.01	$ 348.01
Linux pConfig - 1	Fully Managed (1) - Bronze Tier		1							$ 594.61	$ 593.13	$ 591.65	$ 544.31	$ 479.01	$ 407.17	$ 346.07	$ 346.07	$ 346.07	$ 346.07
Linux pConfig - 1	Fully Managed (1) - Basic Tier		1							$ 591.32	$ 589.85	$ 588.38	$ 541.30	$ 476.36	$ 404.92	$ 344.15	$ 344.15	$ 344.15	$ 344.15
Linux pConfig - 2	2-way Six-Core 2.4 GHz		1							$ 58.53	$ 58.38	$ 58.24	$ 53.58	$ 47.15	$ 40.08	$ 34.07	$ 34.07	$ 34.07	$ 34.07
	16 GB RAM		16							$ 0.32	$ 0.32	$ 0.32	$ 0.32	$ 0.32	$ 0.32	$ 0.16	$ 0.16	$ 0.16	$ 0.16
	Mirrored 146 15K Hard Drives		1							$ 14.63	$ 14.60	$ 14.56	$ 13.39	$ 11.79	$ 10.02	$ 8.52	$ 8.52	$ 8.52	$ 8.52
	RedHat or SUSE		1							$ 139.57	$ 139.22	$ 138.87	$ 127.76	$ 112.43	$ 95.57	$ 81.23	$ 81.23	$ 81.23	$ 81.23
	Sub-Total									**$ 213.05**	**$ 212.52**	**$ 211.99**	**$ 195.05**	**$ 171.69**	**$ 145.99**	**$ 123.98**	**$ 123.98**	**$ 123.98**	**$ 123.98**
Linux pConfig - 2	Fully Managed (1) - Platinum Tier		1							$ 648.94	$ 647.33	$ 645.71	$ 594.07	$ 522.83	$ 444.46	$ 377.68	$ 377.68	$ 377.68	$ 377.68
Linux pConfig - 2	Fully Managed (1) - Gold Tier		1							$ 635.97	$ 634.39	$ 632.81	$ 582.20	$ 512.38	$ 435.58	$ 370.13	$ 370.13	$ 370.13	$ 370.13
Linux pConfig - 2	Fully Managed (1) - Silver Tier		1							$ 628.31	$ 626.75	$ 625.18	$ 575.19	$ 506.21	$ 430.33	$ 365.67	$ 365.67	$ 365.67	$ 365.67
Linux pConfig - 2	Fully Managed (1) - Bronze Tier		1							$ 624.97	$ 623.41	$ 621.86	$ 572.13	$ 503.52	$ 428.04	$ 363.73	$ 363.73	$ 363.73	$ 363.73
Linux pConfig - 2	Fully Managed (1) - Basic Tier		1							$ 621.68	$ 620.13	$ 618.59	$ 569.12	$ 500.87	$ 425.79	$ 361.81	$ 361.81	$ 361.81	$ 361.81
Linux pConfig - 3	4-way Six-Core 2.0 GHz		1							$ 48.01	$ 47.89	$ 47.77	$ 43.94	$ 38.67	$ 32.87	$ 27.94	$ 27.94	$ 27.94	$ 27.94
	64 GB RAM		64							$ 1.28	$ 1.28	$ 1.28	$ 1.28	$ 1.28	$ 1.28	$ 0.64	$ 0.64	$ 0.64	$ 0.64
	SAN Attached Storage		500							$ 75.00	$ 75.00	$ 70.00	$ 65.00	$ 60.00	$ 50.00	$ 40.00	$ 40.00	$ 40.00	$ 40.00
	RedHat or SUSE		1							$ 139.57	$ 139.22	$ 138.87	$ 127.76	$ 112.43	$ 95.57	$ 81.23	$ 81.23	$ 81.23	$ 81.23
	Sub-Total									**$ 263.86**	**$ 263.39**	**$ 257.92**	**$ 237.98**	**$ 212.38**	**$ 179.72**	**$ 149.81**	**$ 149.81**	**$ 149.81**	**$ 149.81**
Linux pConfig - 3	Fully Managed (1) - Platinum Tier		1							$ 699.75	$ 698.20	$ 691.64	$ 637.00	$ 563.52	$ 478.19	$ 403.51	$ 403.51	$ 403.51	$ 403.51
Linux pConfig - 3	Fully Managed (1) - Gold Tier		1							$ 686.78	$ 685.26	$ 678.74	$ 625.13	$ 553.07	$ 469.31	$ 395.96	$ 395.96	$ 395.96	$ 395.96
Linux pConfig - 3	Fully Managed (1) - Silver Tier		1							$ 679.12	$ 677.62	$ 671.11	$ 618.12	$ 546.90	$ 464.06	$ 391.50	$ 391.50	$ 391.50	$ 391.50
Linux pConfig - 3	Fully Managed (1) - Bronze Tier		1							$ 675.78	$ 674.28	$ 667.79	$ 615.06	$ 544.21	$ 461.77	$ 389.56	$ 389.56	$ 389.56	$ 389.56
Linux pConfig - 3	Fully Managed (1) - Basic Tier		1							$ 672.49	$ 671.00	$ 664.52	$ 612.05	$ 541.56	$ 459.52	$ 387.64	$ 387.64	$ 387.64	$ 387.64
Linux pConfig - 4	2-way Six-Core 2.4 GHz		1							$ 58.53	$ 58.38	$ 58.24	$ 53.58	$ 47.15	$ 40.08	$ 34.07	$ 34.07	$ 34.07	$ 34.07

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	Product Name	Unit	Qty per config	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
	16 GB RAM		16							$ 0.32	$ 0.32	$ 0.32	$ 0.32	$ 0.32	$ 0.32	$ 0.16	$ 0.16	$ 0.16	$ 0.16
	Mirrored 146 15K Hard Drives		1							$ 14.63	$ 14.60	$ 14.56	$ 13.39	$ 11.79	$ 10.02	$ 8.52	$ 8.52	$ 8.52	$ 8.52
	RedHat or SUSE		1							$ 139.57	$ 139.22	$ 138.87	$ 127.76	$ 112.43	$ 95.57	$ 81.23	$ 81.23	$ 81.23	$ 81.23
	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization		1							$ 285.90	$ 285.18	$ 284.47	$ 261.71	$ 230.31	$ 195.76	$ 166.40	$ 166.40	$ 166.40	$ 166.40
	Sub-Total									**$ 498.95**	**$ 497.70**	**$ 496.46**	**$ 456.76**	**$ 402.00**	**$ 341.75**	**$ 290.38**	**$ 290.38**	**$ 290.38**	**$ 290.38**
Linux pConfig - 4	Fully Managed (1) - Platinum Tier		1							$ 1,035.32	$ 1,032.73	$ 1,030.16	$ 947.76	$ 834.08	$ 709.02	$ 602.56	$ 602.56	$ 602.56	$ 602.56
Linux pConfig - 4	Fully Managed (1) - Gold Tier		1							$ 1 012.59	$ 1 010.06	$ 1 007.54	$ 926.96	$ 815.77	$ 693.46	$ 589.33	$ 589.33	$ 589.33	$ 589.33
Linux pConfig - 4	Fully Managed (1) - Silver Tier		1							$ 996.90	$ 994.41	$ 991.93	$ 912.60	$ 803.14	$ 682.72	$ 580.20	$ 580.20	$ 580.20	$ 580.20
Linux pConfig - 4	Fully Managed (1) - Bronze Tier		1							$ 990.06	$ 987.58	$ 985.12	$ 906.33	$ 797.62	$ 678.03	$ 576.21	$ 576.21	$ 576.21	$ 576.21
Linux pConfig - 4	Fully Managed (1) - Basic Tier		1							$ 983.55	$ 981.09	$ 978.65	$ 900.37	$ 792.38	$ 673.57	$ 572.43	$ 572.43	$ 572.43	$ 572.43
Linux pConfig - 5	2-way Six-Core 2.4 GHz		1							$ 58.53	$ 58.38	$ 58.24	$ 53.58	$ 47.15	$ 40.08	$ 34.07	$ 34.07	$ 34.07	$ 34.07
	16 GB RAM		16							$ 0.32	$ 0.32	$ 0.32	$ 0.32	$ 0.32	$ 0.32	$ 0.16	$ 0.16	$ 0.16	$ 0.16
	Mirrored 146 15K Hard Drives		1							$ 14.63	$ 14.60	$ 14.56	$ 13.39	$ 11.79	$ 10.02	$ 8.52	$ 8.52	$ 8.52	$ 8.52
	RedHat or SUSE		1							$ 139.57	$ 139.22	$ 138.87	$ 127.76	$ 112.43	$ 95.57	$ 81.23	$ 81.23	$ 81.23	$ 81.23
	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups		1							$ 213.11	$ 212.58	$ 212.05	$ 195.08	$ 171.67	$ 145.92	$ 124.03	$ 124.03	$ 124.03	$ 124.03
	Sub-Total									**$ 426.16**	**$ 425.10**	**$ 424.04**	**$ 390.13**	**$ 343.36**	**$ 291.91**	**$ 248.01**	**$ 248.01**	**$ 248.01**	**$ 248.01**
Linux pConfig - 5	Fully Managed (1) - Platinum Tier		1							$ 962.53	$ 960.13	$ 957.74	$ 881.13	$ 775.44	$ 659.18	$ 560.19	$ 560.19	$ 560.19	$ 560.19
Linux pConfig - 5	Fully Managed (1) - Gold Tier		1							$ 939.80	$ 937.46	$ 935.12	$ 860.33	$ 757.13	$ 643.62	$ 546.96	$ 546.96	$ 546.96	$ 546.96
Linux pConfig - 5	Fully Managed (1) - Silver Tier		1							$ 924.11	$ 921.81	$ 919.51	$ 845.97	$ 744.50	$ 632.88	$ 537.83	$ 537.83	$ 537.83	$ 537.83
Linux pConfig - 5	Fully Managed (1) - Bronze Tier		1							$ 917.27	$ 914.98	$ 912.70	$ 839.70	$ 738.98	$ 628.19	$ 533.84	$ 533.84	$ 533.84	$ 533.84
Linux pConfig - 5	Fully Managed (1) - Basic Tier		1							$ 910.76	$ 908.49	$ 906.23	$ 833.74	$ 733.74	$ 623.73	$ 530.06	$ 530.06	$ 530.06	$ 530.06
x86 (Windows) - Virtual Servers																			
Windows vConfig - 1	2vCPU	Per Instance		CCSU13310069-A						$ 1.42	$ 1.42	$ 1.41	$ 1.30	$ 1.14	$ 0.97	$ 0.83	$ 0.83	$ 0.83	$ 0.83
Windows vConfig - 2, 4, 5	4vCPU	Per Instance		CCSU13310070-A						$ 2.84	$ 2.83	$ 2.83	$ 2.60	$ 2.29	$ 1.95	$ 1.65	$ 1.65	$ 1.65	$ 1.65
Windows vConfig - 3	8vCPU	Per Instance		CCSU13310071-A						$ 5.68	$ 5.67	$ 5.65	$ 5.20	$ 4.58	$ 3.89	$ 3.31	$ 3.31	$ 3.31	$ 3.31
Windows vConfig - 1 2 3 4 5	GB Ram	Per GB		CCSU13310072-A						$ 0.37	$ 0.36	$ 0.36	$ 0.33	$ 0.29	$ 0.25	$ 0.21	$ 0.21	$ 0.21	$ 0.21
Windows vConfig - 1, 2, 3, 4, 5	Windows Server 2008 R2	Per License		CCSU13310073-A						$ 18.25	$ 18.21	$ 18.16	$ 16.71	$ 14.70	$ 12.50	$ 10.62	$ 10.62	$ 10.62	$ 10.62
~~Windows vConfig - 1, 2, 3, 4, 5~~	~~Firewall/IDS~~	~~Per Config~~																	
~~Windows vConfig - 1 2 3 4 5~~	~~Site-Site VPN~~	~~Per Config~~																	
~~W d C f g , 2, 3, 4, 5~~	~~VPN Cl t~~	~~P C f g~~																	
~~Windows vConfig - 1, 2, 3, 4, 5~~	~~VLAN~~	~~Per Config~~																	
Windows vConfig - 4	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Config		CCSU13310078-A						$ 99.73	$ 99.48	$ 99.23	$ 91.29	$ 80.34	$ 68.29	$ 58.04	$ 58.04	$ 58.04	$ 58.04
Windows vConfig - 5	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Config		CCSU13310079-A						$ 26.94	$ 26.87	$ 26.81	$ 24.66	$ 21.70	$ 18.45	$ 15.68	$ 15.68	$ 15.68	$ 15.68
Windows vConfig - 1	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310080-A						$ 374.50	$ 373.57	$ 372.64	$ 342.83	$ 301.69	$ 256.43	$ 217.97	$ 217.97	$ 217.97	$ 217.97
Windows vConfig - 1	Fully Managed (1) - Gold Tier	Per Config		CCSU13310081-A						$ 372.40	$ 371.47	$ 370.55	$ 340.90	$ 300.00	$ 255.00	$ 216.75	$ 216.75	$ 216.75	$ 216.75
Windows vConfig - 1	Fully Managed (1) - Silver Tier	Per Config		CCSU13310082-A						$ 370.49	$ 369.57	$ 368.64	$ 339.15	$ 298.45	$ 253.69	$ 215.63	$ 215.63	$ 215.63	$ 215.63
Windows vConfig - 1	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310083-A						$ 369.59	$ 368.67	$ 367.75	$ 338.33	$ 297.73	$ 253.07	$ 215.11	$ 215.11	$ 215.11	$ 215.11
Windows vConfig - 1	Fully Managed (1) - Basic Tier	Per Config		CCSU13310084-A						$ 368.74	$ 367.82	$ 366.90	$ 337.55	$ 297.04	$ 252.49	$ 214.61	$ 214.61	$ 214.61	$ 214.61
Windows vConfig - 2	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310085-A						$ 374.50	$ 373.57	$ 372.64	$ 342.83	$ 301.69	$ 256.43	$ 217.97	$ 217.97	$ 217.97	$ 217.97
Windows vConfig - 2	Fully Managed (1) - Gold Tier	Per Config		CCSU13310086-A						$ 372.40	$ 371.47	$ 370.55	$ 340.90	$ 300.00	$ 255.00	$ 216.75	$ 216.75	$ 216.75	$ 216.75
Windows vConfig - 2	Fully Managed (1) - Silver Tier	Per Config		CCSU13310087-A						$ 370.49	$ 369.57	$ 368.64	$ 339.15	$ 298.45	$ 253.69	$ 215.63	$ 215.63	$ 215.63	$ 215.63
Windows vConfig - 2	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310088-A						$ 369.59	$ 368.67	$ 367.75	$ 338.33	$ 297.73	$ 253.07	$ 215.11	$ 215.11	$ 215.11	$ 215.11
Windows vConfig - 2	Fully Managed (1) - Basic Tier	Per Config		CCSU13310089-A						$ 368.74	$ 367.82	$ 366.90	$ 337.55	$ 297.04	$ 252.49	$ 214.61	$ 214.61	$ 214.61	$ 214.61
Windows vConfig - 3	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310090-A						$ 374.50	$ 373.57	$ 372.64	$ 342.83	$ 301.69	$ 256.43	$ 217.97	$ 217.97	$ 217.97	$ 217.97
Windows vConfig - 3	Fully Managed (1) - Gold Tier	Per Config		CCSU13310091-A						$ 372.40	$ 371.47	$ 370.55	$ 340.90	$ 300.00	$ 255.00	$ 216.75	$ 216.75	$ 216.75	$ 216.75
Windows vConfig - 3	Fully Managed (1) - Silver Tier	Per Config		CCSU13310092-A						$ 370.49	$ 369.57	$ 368.64	$ 339.15	$ 298.45	$ 253.69	$ 215.63	$ 215.63	$ 215.63	$ 215.63
Windows vConfig - 3	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310093-A						$ 369.59	$ 368.67	$ 367.75	$ 338.33	$ 297.73	$ 253.07	$ 215.11	$ 215.11	$ 215.11	$ 215.11
Windows vConfig - 3	Fully Managed (1) - Basic Tier	Per Config		CCSU13310094-A						$ 368.74	$ 367.82	$ 366.90	$ 337.55	$ 297.04	$ 252.49	$ 214.61	$ 214.61	$ 214.61	$ 214.61
Windows vConfig - 4	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310095-A						$ 424.05	$ 422.99	$ 421.93	$ 388.18	$ 341.60	$ 290.36	$ 246.80	$ 246.80	$ 246.80	$ 246.80
Windows vConfig - 4	Fully Managed (1) - Gold Tier	Per Config		CCSU13310096-A						$ 419.85	$ 418.80	$ 417.76	$ 384.33	$ 338.21	$ 287.48	$ 244.36	$ 244.36	$ 244.36	$ 244.36
Windows vConfig - 4	Fully Managed (1) - Silver Tier	Per Config		CCSU13310097-A						$ 416.02	$ 414.98	$ 413.95	$ 380.83	$ 335.13	$ 284.86	$ 242.13	$ 242.13	$ 242.13	$ 242.13
Windows vConfig - 4	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310098-A						$ 414.23	$ 413.20	$ 412.16	$ 379.19	$ 333.69	$ 283.64	$ 241.09	$ 241.09	$ 241.09	$ 241.09
Windows vConfig - 4	Fully Managed (1) - Basic Tier	Per Config		CCSU13310099-A						$ 412.51	$ 411.49	$ 410.46	$ 377.62	$ 332.31	$ 282.46	$ 240.09	$ 240.09	$ 240.09	$ 240.09
Windows vConfig - 5	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310100-A						$ 424.05	$ 422.99	$ 421.93	$ 388.18	$ 341.60	$ 290.36	$ 246.80	$ 246.80	$ 246.80	$ 246.80

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	**Product Name**	**Unit**	**Qty per config**	**Provider Part Number**	**Version Major**	**Version Minor**	**Version Build**	**Manufacturer ID**	**Equipment Code**	**Price per unit \ Per Month**									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Windows vConfig - 5	Fully Managed (1) - Gold Tier	Per Config		CCSU13310101-A						$ 419.85	$ 418.80	$ 417.76	$ 384.33	$ 338.21	$ 287.48	$ 244.36	$ 244.36	$ 244.36	$ 244.36
Windows vConfig - 5	Fully Managed (1) - Silver Tier	Per Config		CCSU13310102-A						$ 416.02	$ 414.98	$ 413.95	$ 380.83	$ 335.13	$ 284.86	$ 242.13	$ 242.13	$ 242.13	$ 242.13
Windows vConfig - 5	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310103-A						$ 414.23	$ 413.20	$ 412.16	$ 379.19	$ 333.69	$ 283.64	$ 241.09	$ 241.09	$ 241.09	$ 241.09
Windows vConfig - 5	Fully Managed (1) - Basic Tier	Per Config		CCSU13310104-A						$ 412.51	$ 411.49	$ 410.46	$ 377.62	$ 332.31	$ 282.46	$ 240.09	$ 240.09	$ 240.09	$ 240.09
Windows vConfig - 1	2vCPU		1							$ 1.42	$ 1.42	$ 1.41	$ 1.30	$ 1.14	$ 0.97	$ 0.83	$ 0.83	$ 0.83	$ 0.83
	GB Ram		4							$ 1.48	$ 1.44	$ 1.44	$ 1.32	$ 1.16	$ 1.00	$ 0.84	$ 0.84	$ 0.84	$ 0.84
	Windows Server 2008 R2		1							$ 18.25	$ 18.21	$ 18.16	$ 16.71	$ 14.70	$ 12.50	$ 10.62	$ 10.62	$ 10.62	$ 10.62
	~~F ll IDS~~		0																
	~~Site-Site VPN~~		0																
	~~VPN Client~~		0																
	~~VLAN~~		0																
	Sub-Total									**$ 21.15**	**$ 21.07**	**$ 21.01**	**$ 19.33**	**$ 17.00**	**$ 14.47**	**$ 12.29**	**$ 12.29**	**$ 12.29**	**$ 12.29**
Windows vConfig - 1	Fully Managed (1) - Platinum Tier		1							$ 395.65	$ 394.64	$ 393.65	$ 362.16	$ 318.69	$ 270.90	$ 230.26	$ 230.26	$ 230.26	$ 230.26
Windows vConfig - 1	Fully Managed (1) - Gold Tier		1							$ 393.55	$ 392.54	$ 391.56	$ 360.23	$ 317.00	$ 269.47	$ 229.04	$ 229.04	$ 229.04	$ 229.04
Windows vConfig - 1	Fully Managed (1) - Silver Tier		1							$ 391.64	$ 390.64	$ 389.65	$ 358.48	$ 315.45	$ 268.16	$ 227.92	$ 227.92	$ 227.92	$ 227.92
Windows vConfig - 1	Fully Managed (1) - Bronze Tier		1							$ 390.74	$ 389.74	$ 388.76	$ 357.66	$ 314.73	$ 267.54	$ 227.40	$ 227.40	$ 227.40	$ 227.40
Windows vConfig - 1	Fully Managed (1) - Basic Tier		1							$ 389.89	$ 388.89	$ 387.91	$ 356.88	$ 314.04	$ 266.96	$ 226.90	$ 226.90	$ 226.90	$ 226.90
Windows vConfig - 2	4vCPU		1							$ 2.84	$ 2.83	$ 2.83	$ 2.60	$ 2.29	$ 1.95	$ 1.65	$ 1.65	$ 1.65	$ 1.65
	GB Ram		16							$ 5.92	$ 5.76	$ 5.76	$ 5.28	$ 4.64	$ 4.00	$ 3.36	$ 3.36	$ 3.36	$ 3.36
	Windows Server 2008 R2		1							$ 18.25	$ 18.21	$ 18.16	$ 16.71	$ 14.70	$ 12.50	$ 10.62	$ 10.62	$ 10.62	$ 10.62
	~~Firewall/IDS~~		0																
	~~Site-Site VPN~~		0																
	~~VPN Cl t~~		0																
	~~VLAN~~		0																
	Sub-Total									**$ 27.01**	**$ 26.80**	**$ 26.75**	**$ 24.59**	**$ 21.63**	**$ 18.45**	**$ 15.63**	**$ 15.63**	**$ 15.63**	**$ 15.63**
Windows vConfig - 2	Fully Managed (1) - Platinum Tier		1							$ 401.51	$ 400.37	$ 399.39	$ 367.42	$ 323.32	$ 274.88	$ 233.60	$ 233.60	$ 233.60	$ 233.60
Windows vConfig - 2	Fully Managed (1) - Gold Tier		1							$ 399.41	$ 398.27	$ 397.30	$ 365.49	$ 321.63	$ 273.45	$ 232.38	$ 232.38	$ 232.38	$ 232.38
Windows vConfig - 2	Fully Managed (1) - Silver Tier		1							$ 397.50	$ 396.37	$ 395.39	$ 363.74	$ 320.08	$ 272.14	$ 231.26	$ 231.26	$ 231.26	$ 231.26
Windows vConfig - 2	Fully Managed (1) - Bronze Tier		1							$ 396.60	$ 395.47	$ 394.50	$ 362.92	$ 319.36	$ 271.52	$ 230.74	$ 230.74	$ 230.74	$ 230.74
Windows vConfig - 2	Fully Managed (1) - Basic Tier		1							$ 395.75	$ 394.62	$ 393.65	$ 362.14	$ 318.67	$ 270.94	$ 230.24	$ 230.24	$ 230.24	$ 230.24
Windows vConfig - 3	8vCPU		1							$ 5.68	$ 5.67	$ 5.65	$ 5.20	$ 4.58	$ 3.89	$ 3.31	$ 3.31	$ 3.31	$ 3.31
	GB Ram		64							$ 23.68	$ 23.04	$ 23.04	$ 21.12	$ 18.56	$ 16.00	$ 13.44	$ 13.44	$ 13.44	$ 13.44
	Windows Server 2008 R2		1							$ 18.25	$ 18.21	$ 18.16	$ 16.71	$ 14.70	$ 12.50	$ 10.62	$ 10.62	$ 10.62	$ 10.62
	~~Firewall IDS~~		0																
	~~Site-Site VPN~~		0																
	~~VPN Client~~		0																
	~~VLAN~~		0																
	Sub-Total									**$ 47.61**	**$ 46.92**	**$ 46.85**	**$ 43.03**	**$ 37.84**	**$ 32.39**	**$ 27.37**	**$ 27.37**	**$ 27.37**	**$ 27.37**
Windows vConfig - 3	Fully Managed (1) - Platinum Tier		1							$ 422.11	$ 420.49	$ 419.49	$ 385.86	$ 339.53	$ 288.82	$ 245.34	$ 245.34	$ 245.34	$ 245.34
Windows vConfig - 3	Fully Managed (1) - Gold Tier		1							$ 420.01	$ 418.39	$ 417.40	$ 383.93	$ 337.84	$ 287.39	$ 244.12	$ 244.12	$ 244.12	$ 244.12
Windows vConfig - 3	Fully Managed (1) - Silver Tier		1							$ 418.10	$ 416.49	$ 415.49	$ 382.18	$ 336.29	$ 286.08	$ 243.00	$ 243.00	$ 243.00	$ 243.00
Windows vConfig - 3	Fully Managed (1) - Bronze Tier		1							$ 417.20	$ 415.59	$ 414.60	$ 381.36	$ 335.57	$ 285.46	$ 242.48	$ 242.48	$ 242.48	$ 242.48
Windows vConfig - 3	Fully Managed (1) - Basic Tier		1							$ 416.35	$ 414.74	$ 413.75	$ 380.58	$ 334.88	$ 284.88	$ 241.98	$ 241.98	$ 241.98	$ 241.98
Windows vConfig - 4	4vCPU		1							$ 2.84	$ 2.83	$ 2.83	$ 2.60	$ 2.29	$ 1.95	$ 1.65	$ 1.65	$ 1.65	$ 1.65
	GB Ram		16							$ 5.92	$ 5.76	$ 5.76	$ 5.28	$ 4.64	$ 4.00	$ 3.36	$ 3.36	$ 3.36	$ 3.36
	Windows Server 2008 R2		1							$ 18.25	$ 18.21	$ 18.16	$ 16.71	$ 14.70	$ 12.50	$ 10.62	$ 10.62	$ 10.62	$ 10.62
	~~Firewall/IDS~~		0																
	~~Site-Site VPN~~		0																
	~~VPN Cl t~~		0																
	~~VLAN~~		0																
	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization		1							$ 99.73	$ 99.48	$ 99.23	$ 91.29	$ 80.34	$ 68.29	$ 58.04	$ 58.04	$ 58.04	$ 58.04
	Sub-Total									**$ 126.74**	**$ 126.28**	**$ 125.98**	**$ 115.88**	**$ 101.97**	**$ 86.74**	**$ 73.67**	**$ 73.67**	**$ 73.67**	**$ 73.67**
Windows vConfig - 4	Fully Managed (1) - Platinum Tier		1							$ 550.79	$ 549.27	$ 547.91	$ 504.06	$ 443.57	$ 377.10	$ 320.47	$ 320.47	$ 320.47	$ 320.47
Windows vConfig - 4	Fully Managed (1) - Gold Tier		1							$ 546.59	$ 545.08	$ 543.74	$ 500.21	$ 440.18	$ 374.22	$ 318.03	$ 318.03	$ 318.03	$ 318.03
Windows vConfig - 4	Fully Managed (1) - Silver Tier		1							$ 542.76	$ 541.26	$ 539.93	$ 496.71	$ 437.10	$ 371.60	$ 315.80	$ 315.80	$ 315.80	$ 315.80
Windows vConfig - 4	Fully Managed (1) - Bronze Tier		1							$ 540.97	$ 539.48	$ 538.14	$ 495.07	$ 435.66	$ 370.38	$ 314.76	$ 314.76	$ 314.76	$ 314.76
Windows vConfig - 4	Fully Managed (1) - Basic Tier		1							$ 539.25	$ 537.77	$ 536.44	$ 493.50	$ 434.28	$ 369.20	$ 313.76	$ 313.76	$ 313.76	$ 313.76
Windows vConfig - 5	4vCPU		1							$ 2.84	$ 2.83	$ 2.83	$ 2.60	$ 2.29	$ 1.95	$ 1.65	$ 1.65	$ 1.65	$ 1.65
	GB Ram		16							$ 5.92	$ 5.76	$ 5.76	$ 5.28	$ 4.64	$ 4.00	$ 3.36	$ 3.36	$ 3.36	$ 3.36
	Windows Server 2008 R2		1							$ 18.25	$ 18.21	$ 18.16	$ 16.71	$ 14.70	$ 12.50	$ 10.62	$ 10.62	$ 10.62	$ 10.62

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	Product Name	Unit	Qty per config	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
	~~Firewall IDS~~		0																
	~~S t - S t - VPN~~		0																
	~~VPN Client~~		0																
	~~VLAN~~		0																
	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups		1							$ 26.94	$ 26.87	$ 26.81	$ 24.66	$ 21.70	$ 18.45	$ 15.68	$ 15.68	$ 15.68	$ 15.68
	Sub-Total									**$ 53.95**	**$ 53.67**	**$ 53.56**	**$ 49.25**	**$ 43.33**	**$ 36.90**	**$ 31.31**	**$ 31.31**	**$ 31.31**	**$ 31.31**
Windows vConfig - 5	Fully Managed (1) - Platinum Tier		1							$ 478.00	$ 476.66	$ 475.49	$ 437.43	$ 384.93	$ 327.26	$ 278.11	$ 278.11	$ 278.11	$ 278.11
Windows vConfig - 5	Fully Managed (1) - Gold Tier		1							$ 473.80	$ 472.47	$ 471.32	$ 433.58	$ 381.54	$ 324.38	$ 275.67	$ 275.67	$ 275.67	$ 275.67
Windows vConfig - 5	Fully Managed (1) - Silver Tier		1							$ 469.97	$ 468.65	$ 467.51	$ 430.08	$ 378.46	$ 321.76	$ 273.44	$ 273.44	$ 273.44	$ 273.44
Windows vConfig - 5	Fully Managed (1) - Bronze Tier		1							$ 468.18	$ 466.87	$ 465.72	$ 428.44	$ 377.02	$ 320.54	$ 272.40	$ 272.40	$ 272.40	$ 272.40
Windows vConfig - 5	Fully Managed (1) - Basic Tier		1							$ 466.46	$ 465.16	$ 464.02	$ 426.87	$ 375.64	$ 319.36	$ 271.40	$ 271.40	$ 271.40	$ 271.40
x86 (Linux) - Virtual Servers																			
Linux vConfig - 1	2vCPU	Per Instance		CCSU13310105-A						$ 1.42	$ 1.42	$ 1.41	$ 1.30	$ 1.14	$ 0.97	$ 0.83	$ 0.83	$ 0.83	$ 0.83
Linux vConfig - 2, 4, 5	4vCPU	Per Instance		CCSU13310106-A						$ 2.84	$ 2.83	$ 2.83	$ 2.60	$ 2.29	$ 1.95	$ 1.65	$ 1.65	$ 1.65	$ 1.65
Linux vConfig - 3	8vCPU	Per Instance		CCSU13310107-A						$ 5.68	$ 5.67	$ 5.65	$ 5.20	$ 4.58	$ 3.89	$ 3.31	$ 3.31	$ 3.31	$ 3.31
Linux vConfig - 1, 2, 3, 4, 5	GB Ram	Per GB		CCSU13310108-A						$ 0.37	$ 0.36	$ 0.36	$ 0.33	$ 0.29	$ 0.25	$ 0.21	$ 0.21	$ 0.21	$ 0.21
Linux vConfig - 1, 2, 3, 4, 5	RedHat or SUSE	Per License		CCSU13310109-A						$ 59.26	$ 59.11	$ 58.96	$ 54.24	$ 47.73	$ 40.57	$ 34.49	$ 34.49	$ 34.49	$ 34.49
Linux vConfig - 1 2 3 4 5	~~Firewall IDS~~	~~Per Config~~																	
Linux vConfig - 1, 2, 3, 4, 5	~~S t - S t - VPN~~	~~P C f g~~																	
Linux vConfig - 1 2 3 4 5	~~VPN Client~~	~~Per Config~~																	
Linux vConfig - 1 2 3 4 5	~~VLAN~~	~~Per Config~~																	
Linux vConfig - 4	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Config		CCSU13310114-A						$ 140.73	$ 140.38	$ 140.03	$ 128.83	$ 113.37	$ 96.36	$ 81.91	$ 81.91	$ 81.91	$ 81.91
Linux vConfig - 5	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Config		CCSU13310115-A						$ 67.95	$ 67.78	$ 67.61	$ 62.20	$ 54.73	$ 46.52	$ 39.55	$ 39.55	$ 39.55	$ 39.55
Linux vConfig - 1	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310116-A						$ 388.08	$ 387.11	$ 386.15	$ 355.26	$ 312.63	$ 265.73	$ 225.87	$ 225.87	$ 225.87	$ 225.87
Linux vConfig - 1	Fully Managed (1) - Gold Tier	Per Config		CCSU13310117-A						$ 378.33	$ 377.38	$ 376.44	$ 346.33	$ 304.77	$ 259.05	$ 220.19	$ 220.19	$ 220.19	$ 220.19
Linux vConfig - 1	Fully Managed (1) - Silver Tier	Per Config		CCSU13310118-A						$ 370.30	$ 369.37	$ 368.45	$ 338.98	$ 298.30	$ 253.55	$ 215.52	$ 215.52	$ 215.52	$ 215.52
Linux vConfig - 1	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310119-A						$ 366.79	$ 365.88	$ 364.97	$ 335.77	$ 295.48	$ 251.16	$ 213.48	$ 213.48	$ 213.48	$ 213.48
Linux vConfig - 1	Fully Managed (1) - Basic Tier	Per Config		CCSU13310120-A						$ 363.57	$ 362.67	$ 361.76	$ 332.82	$ 292.88	$ 248.95	$ 211.61	$ 211.61	$ 211.61	$ 211.61
Linux vConfig - 2	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310121-A						$ 388.08	$ 387.11	$ 386.15	$ 355.26	$ 312.63	$ 265.73	$ 225.87	$ 225.87	$ 225.87	$ 225.87
Linux vConfig - 2	Fully Managed (1) - Gold Tier	Per Config		CCSU13310122-A						$ 378.33	$ 377.38	$ 376.44	$ 346.33	$ 304.77	$ 259.05	$ 220.19	$ 220.19	$ 220.19	$ 220.19
Linux vConfig - 2	Fully Managed (1) - Silver Tier	Per Config		CCSU13310123-A						$ 370.30	$ 369.37	$ 368.45	$ 338.98	$ 298.30	$ 253.55	$ 215.52	$ 215.52	$ 215.52	$ 215.52
Linux vConfig - 2	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310124-A						$ 366.79	$ 365.88	$ 364.97	$ 335.77	$ 295.48	$ 251.16	$ 213.48	$ 213.48	$ 213.48	$ 213.48
Linux vConfig - 2	Fully Managed (1) - Basic Tier	Per Config		CCSU13310125-A						$ 363.57	$ 362.67	$ 361.76	$ 332.82	$ 292.88	$ 248.95	$ 211.61	$ 211.61	$ 211.61	$ 211.61
Linux vConfig - 3	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310126-A						$ 388.08	$ 387.11	$ 386.15	$ 355.26	$ 312.63	$ 265.73	$ 225.87	$ 225.87	$ 225.87	$ 225.87
Linux vConfig - 3	Fully Managed (1) - Gold Tier	Per Config		CCSU13310127-A						$ 378.33	$ 377.38	$ 376.44	$ 346.33	$ 304.77	$ 259.05	$ 220.19	$ 220.19	$ 220.19	$ 220.19
Linux vConfig - 3	Fully Managed (1) - Silver Tier	Per Config		CCSU13310128-A						$ 370.30	$ 369.37	$ 368.45	$ 338.98	$ 298.30	$ 253.55	$ 215.52	$ 215.52	$ 215.52	$ 215.52
Linux vConfig - 3	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310129-A						$ 366.79	$ 365.88	$ 364.97	$ 335.77	$ 295.48	$ 251.16	$ 213.48	$ 213.48	$ 213.48	$ 213.48
Linux vConfig - 3	Fully Managed (1) - Basic Tier	Per Config		CCSU13310130-A						$ 363.57	$ 362.67	$ 361.76	$ 332.82	$ 292.88	$ 248.95	$ 211.61	$ 211.61	$ 211.61	$ 211.61
Linux vConfig - 4	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310131-A						$ 492.78	$ 491.55	$ 490.33	$ 451.10	$ 396.97	$ 337.42	$ 286.81	$ 286.81	$ 286.81	$ 286.81
Linux vConfig - 4	Fully Managed (1) - Gold Tier	Per Config		CCSU13310132-A						$ 473.27	$ 472.09	$ 470.92	$ 433.24	$ 381.25	$ 324.07	$ 275.46	$ 275.46	$ 275.46	$ 275.46
Linux vConfig - 4	Fully Managed (1) - Silver Tier	Per Config		CCSU13310133-A						$ 457.22	$ 456.08	$ 454.94	$ 418.54	$ 368.32	$ 313.07	$ 266.11	$ 266.11	$ 266.11	$ 266.11
Linux vConfig - 4	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310134-A						$ 450.21	$ 449.09	$ 447.97	$ 412.13	$ 362.67	$ 308.27	$ 262.03	$ 262.03	$ 262.03	$ 262.03
Linux vConfig - 4	Fully Managed (1) - Basic Tier	Per Config		CCSU13310135-A						$ 443.77	$ 442.66	$ 441.56	$ 406.24	$ 357.49	$ 303.86	$ 258.28	$ 258.28	$ 258.28	$ 258.28
Linux vConfig - 5	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310136-A						$ 492.78	$ 491.55	$ 490.33	$ 451.10	$ 396.97	$ 337.42	$ 286.81	$ 286.81	$ 286.81	$ 286.81
Linux vConfig - 5	Fully Managed (1) - Gold Tier	Per Config		CCSU13310137-A						$ 473.27	$ 472.09	$ 470.92	$ 433.24	$ 381.25	$ 324.07	$ 275.46	$ 275.46	$ 275.46	$ 275.46
Linux vConfig - 5	Fully Managed (1) - Silver Tier	Per Config		CCSU13310138-A						$ 457.22	$ 456.08	$ 454.94	$ 418.54	$ 368.32	$ 313.07	$ 266.11	$ 266.11	$ 266.11	$ 266.11
Linux vConfig - 5	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310139-A						$ 450.21	$ 449.09	$ 447.97	$ 412.13	$ 362.67	$ 308.27	$ 262.03	$ 262.03	$ 262.03	$ 262.03
Linux vConfig - 5	Fully Managed (1) - Basic Tier	Per Config		CCSU13310140-A						$ 443.77	$ 442.66	$ 441.56	$ 406.24	$ 357.49	$ 303.86	$ 258.28	$ 258.28	$ 258.28	$ 258.28
Linux vConfig - 1	2vCPU		1							$ 1.42	$ 1.42	$ 1.41	$ 1.30	$ 1.14	$ 0.97	$ 0.83	$ 0.83	$ 0.83	$ 0.83
	GB Ram		4							$ 1.48	$ 1.44	$ 1.44	$ 1.32	$ 1.16	$ 1.00	$ 0.84	$ 0.84	$ 0.84	$ 0.84
	RedHat or SUSE		1							$ 59.26	$ 59.11	$ 58.96	$ 54.24	$ 47.73	$ 40.57	$ 34.49	$ 34.49	$ 34.49	$ 34.49
	~~Firewall IDS~~		0																
	~~S t - S t - VPN~~		0																
	~~VPN Client~~		0																
	~~VLAN~~		0																
	Sub-Total									**$ 62.16**	**$ 61.97**	**$ 61.81**	**$ 56.86**	**$ 50.03**	**$ 42.54**	**$ 36.16**	**$ 36.16**	**$ 36.16**	**$ 36.16**

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	Product Name	Unit	Qty per config	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Linux vConfig - 1	Fully Managed (1) - Platinum Tier		1							$ 450.24	$ 449.08	$ 447.96	$ 412.12	$ 362.66	$ 308.27	$ 262.03	$ 262.03	$ 262.03	$ 262.03
Linux vConfig - 1	Fully Managed (1) - Gold Tier		1							$ 440.49	$ 439.35	$ 438.25	$ 403.19	$ 354.80	$ 301.59	$ 256.35	$ 256.35	$ 256.35	$ 256.35
Linux vConfig - 1	Fully Managed (1) - Silver Tier		1							$ 432.46	$ 431.34	$ 430.26	$ 395.84	$ 348.33	$ 296.09	$ 251.68	$ 251.68	$ 251.68	$ 251.68
Linux vConfig - 1	Fully Managed (1) - Bronze Tier		1							$ 428.95	$ 427.85	$ 426.78	$ 392.63	$ 345.51	$ 293.70	$ 249.64	$ 249.64	$ 249.64	$ 249.64
Linux vConfig - 1	Fully Managed (1) - Basic Tier		1							$ 425.73	$ 424.64	$ 423.57	$ 389.68	$ 342.91	$ 291.49	$ 247.77	$ 247.77	$ 247.77	$ 247.77
Linux vConfig - 2	4vCPU		1							$ 2.84	$ 2.83	$ 2.83	$ 2.60	$ 2.29	$ 1.95	$ 1.65	$ 1.65	$ 1.65	$ 1.65
	GB Ram		16							$ 5.92	$ 5.76	$ 5.76	$ 5.28	$ 4.64	$ 4.00	$ 3.36	$ 3.36	$ 3.36	$ 3.36
	RedHat or SUSE		1							$ 59.26	$ 59.11	$ 58.96	$ 54.24	$ 47.73	$ 40.57	$ 34.49	$ 34.49	$ 34.49	$ 34.49
	~~Firewall IDS~~		0																
	~~S-t - S-t - VPN~~		0																
	~~VPN Client~~		0																
	~~VLAN~~		0																
	Sub-Total									**$ 68.02**	**$ 67.70**	**$ 67.55**	**$ 62.12**	**$ 54.66**	**$ 46.52**	**$ 39.50**	**$ 39.50**	**$ 39.50**	**$ 39.50**
Linux vConfig - 2	Fully Managed (1) - Platinum Tier		1							$ 456.10	$ 454.81	$ 453.70	$ 417.38	$ 367.29	$ 312.25	$ 265.37	$ 265.37	$ 265.37	$ 265.37
Linux vConfig - 2	Fully Managed (1) - Gold Tier		1							$ 446.35	$ 445.08	$ 443.99	$ 408.45	$ 359.43	$ 305.57	$ 259.69	$ 259.69	$ 259.69	$ 259.69
Linux vConfig - 2	Fully Managed (1) - Silver Tier		1							$ 438.32	$ 437.07	$ 436.00	$ 401.10	$ 352.96	$ 300.07	$ 255.02	$ 255.02	$ 255.02	$ 255.02
Linux vConfig - 2	Fully Managed (1) - Bronze Tier		1							$ 434.81	$ 433.58	$ 432.52	$ 397.89	$ 350.14	$ 297.68	$ 252.98	$ 252.98	$ 252.98	$ 252.98
Linux vConfig - 2	Fully Managed (1) - Basic Tier		1							$ 431.59	$ 430.37	$ 429.31	$ 394.94	$ 347.54	$ 295.47	$ 251.11	$ 251.11	$ 251.11	$ 251.11
Linux vConfig - 3	8vCPU		1							$ 5.68	$ 5.67	$ 5.65	$ 5.20	$ 4.58	$ 3.89	$ 3.31	$ 3.31	$ 3.31	$ 3.31
	GB Ram		64							$ 23.68	$ 23.04	$ 23.04	$ 21.12	$ 18.56	$ 16.00	$ 13.44	$ 13.44	$ 13.44	$ 13.44
	RedHat or SUSE		1							$ 59.26	$ 59.11	$ 58.96	$ 54.24	$ 47.73	$ 40.57	$ 34.49	$ 34.49	$ 34.49	$ 34.49
	~~F l IDS~~		0																
	~~Site-Site VPN~~		0																
	~~VPN Client~~		0																
	~~VLAN~~		0																
	Sub-Total									**$ 88.62**	**$ 87.82**	**$ 87.65**	**$ 80.56**	**$ 70.87**	**$ 60.46**	**$ 51.24**	**$ 51.24**	**$ 51.24**	**$ 51.24**
Linux vConfig - 3	Fully Managed (1) - Platinum Tier		1							$ 476.70	$ 474.93	$ 473.80	$ 435.82	$ 383.50	$ 326.19	$ 277.11	$ 277.11	$ 277.11	$ 277.11
Linux vConfig - 3	Fully Managed (1) - Gold Tier		1							$ 466.95	$ 465.20	$ 464.09	$ 426.89	$ 375.64	$ 319.51	$ 271.43	$ 271.43	$ 271.43	$ 271.43
Linux vConfig - 3	Fully Managed (1) - Silver Tier		1							$ 458.92	$ 457.19	$ 456.10	$ 419.54	$ 369.17	$ 314.01	$ 266.76	$ 266.76	$ 266.76	$ 266.76
Linux vConfig - 3	Fully Managed (1) - Bronze Tier		1							$ 455.41	$ 453.70	$ 452.62	$ 416.33	$ 366.35	$ 311.62	$ 264.72	$ 264.72	$ 264.72	$ 264.72
Linux vConfig - 3	Fully Managed (1) - Basic Tier		1							$ 452.19	$ 450.49	$ 449.41	$ 413.38	$ 363.75	$ 309.41	$ 262.85	$ 262.85	$ 262.85	$ 262.85
Linux vConfig - 4	4vCPU		1							$ 2.84	$ 2.83	$ 2.83	$ 2.60	$ 2.29	$ 1.95	$ 1.65	$ 1.65	$ 1.65	$ 1.65
	GB Ram		16							$ 5.92	$ 5.76	$ 5.76	$ 5.28	$ 4.64	$ 4.00	$ 3.36	$ 3.36	$ 3.36	$ 3.36
	RedHat or SUSE		1							$ 59.26	$ 59.11	$ 58.96	$ 54.24	$ 47.73	$ 40.57	$ 34.49	$ 34.49	$ 34.49	$ 34.49
	~~Firewall/IDS~~		0																
	~~Site-Site VPN~~		0																
	~~VPN Client~~		0																
	~~VLAN~~		0																
	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization		1							$ 140.73	$ 140.38	$ 140.03	$ 128.83	$ 113.37	$ 96.36	$ 81.91	$ 81.91	$ 81.91	$ 81.91
	Sub-Total									**$ 208.75**	**$ 208.08**	**$ 207.58**	**$ 190.95**	**$ 168.03**	**$ 142.88**	**$ 121.41**	**$ 121.41**	**$ 121.41**	**$ 121.41**
Linux vConfig - 4	Fully Managed (1) - Platinum Tier		1							$ 701.53	$ 699.63	$ 697.91	$ 642.05	$ 565.00	$ 480.30	$ 408.22	$ 408.22	$ 408.22	$ 408.22
Linux vConfig - 4	Fully Managed (1) - Gold Tier		1							$ 682.02	$ 680.17	$ 678.50	$ 624.19	$ 549.28	$ 466.95	$ 396.87	$ 396.87	$ 396.87	$ 396.87
Linux vConfig - 4	Fully Managed (1) - Silver Tier		1							$ 665.97	$ 664.16	$ 662.52	$ 609.49	$ 536.35	$ 455.95	$ 387.52	$ 387.52	$ 387.52	$ 387.52
Linux vConfig - 4	Fully Managed (1) - Bronze Tier		1							$ 658.96	$ 657.17	$ 655.55	$ 603.08	$ 530.70	$ 451.15	$ 383.44	$ 383.44	$ 383.44	$ 383.44
Linux vConfig - 4	Fully Managed (1) - Basic Tier		1							$ 652.52	$ 650.74	$ 649.14	$ 597.19	$ 525.52	$ 446.74	$ 379.69	$ 379.69	$ 379.69	$ 379.69
Linux vConfig - 5	4vCPU		1							$ 2.84	$ 2.83	$ 2.83	$ 2.60	$ 2.29	$ 1.95	$ 1.65	$ 1.65	$ 1.65	$ 1.65
	GB Ram		16							$ 5.92	$ 5.76	$ 5.76	$ 5.28	$ 4.64	$ 4.00	$ 3.36	$ 3.36	$ 3.36	$ 3.36
	RedHat or SUSE		1							$ 59.26	$ 59.11	$ 58.96	$ 54.24	$ 47.73	$ 40.57	$ 34.49	$ 34.49	$ 34.49	$ 34.49
	~~Firewall/IDS~~		0																
	~~Site-Site VPN~~		0																
	~~VPN Client~~		0																
	~~VLAN~~		0																
	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups		1							$ 67.95	$ 67.78	$ 67.61	$ 62.20	$ 54.73	$ 46.52	$ 39.55	$ 39.55	$ 39.55	$ 39.55
	Sub-Total									**$ 135.97**	**$ 135.48**	**$ 135.16**	**$ 124.32**	**$ 109.39**	**$ 93.04**	**$ 79.05**	**$ 79.05**	**$ 79.05**	**$ 79.05**
Linux vConfig - 5	Fully Managed (1) - Platinum Tier		1							$ 628.75	$ 627.03	$ 625.49	$ 575.42	$ 506.36	$ 430.46	$ 365.86	$ 365.86	$ 365.86	$ 365.86
Linux vConfig - 5	Fully Managed (1) - Gold Tier		1							$ 609.24	$ 607.57	$ 606.08	$ 557.56	$ 490.64	$ 417.11	$ 354.51	$ 354.51	$ 354.51	$ 354.51
Linux vConfig - 5	Fully Managed (1) - Silver Tier		1							$ 593.19	$ 591.56	$ 590.10	$ 542.86	$ 477.71	$ 406.11	$ 345.16	$ 345.16	$ 345.16	$ 345.16
Linux vConfig - 5	Fully Managed (1) - Bronze Tier		1							$ 586.18	$ 584.57	$ 583.13	$ 536.45	$ 472.06	$ 401.31	$ 341.08	$ 341.08	$ 341.08	$ 341.08
Linux vConfig - 5	Fully Managed (1) - Basic Tier		1							$ 579.74	$ 578.14	$ 576.72	$ 530.56	$ 466.88	$ 396.90	$ 337.33	$ 337.33	$ 337.33	$ 337.33

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	Product Name	Unit	Qty per config	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
P-Series Server Configurations																			
AIX Config - 1, 2, 3, 4, 5	3.0GHz POWER7	Per Server		CCSI13310141-A						$ 97.49	$ 96.52	$ 95.55	$ 94.59	$ 93.64	$ 92.71	$ 91.79	$ 91.79	$ 91.79	$ 91.79
AIX Config - 1 2 3 4 5	Cores	Per .5 Core		CCSI13310142-A						$ 30.26	$ 29.95	$ 29.65	$ 29.36	$ 29.07	$ 28.77	$ 28.48	$ 28.48	$ 28.48	$ 28.48
AIX Config - 1, 2, 3, 4, 5	GB RAM	Per GB		CCSI13310143-A						$ 1.26	$ 1.25	$ 1.24	$ 1.23	$ 1.23	$ 1.22	$ 1.20	$ 1.20	$ 1.20	$ 1.20
AIX Config - 1 2 3 4 5	AIX	Per License		CCSI13310144-A						$ 47.07	$ 49.59	$ 51.27	$ 54.64	$ 57.15	$ 59.67	$ 63.04	$ 63.04	$ 63.04	$ 63.04
AIX Config - 4	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Config		CCSI13310145-A						$ 360.37	$ 366.72	$ 372.41	$ 380.40	$ 388.18	$ 395.64	$ 404.70	$ 404.70	$ 404.70	$ 404.70
AIX Config - 5	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Config		CCSI13310146-A						$ 206.34	$ 207.26	$ 207.37	$ 209.17	$ 210.16	$ 211.15	$ 212.99	$ 212.99	$ 212.99	$ 212.99
AIX Config - 1	Fully Managed (1) - Platinum Tier	Per Config		CCSI13310147-A						$ 746.35	$ 757.45	$ 768.72	$ 780.15	$ 794.19	$ 757.66	$ 746.62	$ 746.62	$ 746.62	$ 746.62
AIX Config - 1	Fully Managed (1) - Gold Tier	Per Config		CCSI13310148-A						$ 633.10	$ 645.72	$ 658.60	$ 671.74	$ 687.44	$ 651.76	$ 641.56	$ 641.56	$ 641.56	$ 641.56
AIX Config - 1	Fully Managed (1) - Silver Tier	Per Config		CCSI13310149-A						$ 536.73	$ 550.02	$ 563.64	$ 577.60	$ 594.15	$ 559.31	$ 549.95	$ 549.95	$ 549.95	$ 549.95
AIX Config - 1	Fully Managed (1) - Bronze Tier	Per Config		CCSI13310150-A						$ 440.41	$ 454.32	$ 468.67	$ 483.47	$ 500.86	$ 466.85	$ 458.34	$ 458.34	$ 458.34	$ 458.34
AIX Config - 1	Fully Managed (1) - Basic Tier	Per Config		CCSI13310151-A						$ 344.29	$ 358.69	$ 373.70	$ 389.34	$ 407.57	$ 374.41	$ 366.73	$ 366.73	$ 366.73	$ 366.73
AIX Config - 2	Fully Managed (1) - Platinum Tier	Per Config		CCSI13310152-A						$ 757.27	$ 768.57	$ 780.04	$ 791.68	$ 805.91	$ 768.74	$ 757.06	$ 757.06	$ 757.06	$ 757.06
AIX Config - 2	Fully Managed (1) - Gold Tier	Per Config		CCSI13310153-A						$ 643.97	$ 656.00	$ 668.26	$ 680.75	$ 695.81	$ 659.48	$ 649.48	$ 649.48	$ 649.48	$ 649.48
AIX Config - 2	Fully Managed (1) - Silver Tier	Per Config		CCSI13310154-A						$ 547.57	$ 560.28	$ 573.29	$ 586.60	$ 603.35	$ 568.70	$ 559.55	$ 559.55	$ 559.55	$ 559.55
AIX Config - 2	Fully Managed (1) - Bronze Tier	Per Config		CCSI13310155-A						$ 451.35	$ 465.45	$ 480.00	$ 495.00	$ 512.59	$ 478.78	$ 470.46	$ 470.46	$ 470.46	$ 470.46
AIX Config - 2	Fully Managed (1) - Basic Tier	Per Config		CCSI13310156-A						$ 355.19	$ 369.81	$ 385.03	$ 400.87	$ 419.30	$ 386.32	$ 378.84	$ 378.84	$ 378.84	$ 378.84
AIX Config - 3	Fully Managed (1) - Platinum Tier	Per Config		CCSI13310157-A						$ 784.95	$ 795.65	$ 806.50	$ 817.49	$ 831.92	$ 794.94	$ 783.46	$ 783.46	$ 783.46	$ 783.46
AIX Config - 3	Fully Managed (1) - Gold Tier	Per Config		CCSI13310158-A						$ 671.74	$ 683.96	$ 696.41	$ 709.08	$ 724.34	$ 688.21	$ 677.57	$ 677.57	$ 677.57	$ 677.57
AIX Config - 3	Fully Managed (1) - Silver Tier	Per Config		CCSI13310159-A						$ 562.68	$ 575.60	$ 588.82	$ 602.33	$ 618.44	$ 583.14	$ 573.34	$ 573.34	$ 573.34	$ 573.34
AIX Config - 3	Fully Managed (1) - Bronze Tier	Per Config		CCSI13310160-A						$ 478.93	$ 492.50	$ 506.45	$ 520.81	$ 537.76	$ 503.31	$ 494.33	$ 494.33	$ 494.33	$ 494.33
AIX Config - 3	Fully Managed (1) - Basic Tier	Per Config		CCSI13310161-A						$ 382.70	$ 396.83	$ 411.48	$ 426.68	$ 444.47	$ 410.85	$ 402.73	$ 402.73	$ 402.73	$ 402.73
AIX Config - 4	Fully Managed (1) - Platinum Tier	Per Config		CCSI13310162-A						$ 1,254.37	$ 1,257.27	$ 1,260.17	$ 1,263.09	$ 1,269.40	$ 1,224.31	$ 1,203.85	$ 1,203.85	$ 1,203.85	$ 1,203.85
AIX Config - 4	Fully Managed (1) - Gold Tier	Per Config		CCSI13310163-A						$ 1,027.52	$ 1,032.06	$ 1,036.62	$ 1,041.20	$ 1,049.21	$ 1,005.80	$ 988.70	$ 988.70	$ 988.70	$ 988.70
AIX Config - 4	Fully Managed (1) - Silver Tier	Per Config		CCSI13310164-A						$ 834.29	$ 840.46	$ 846.67	$ 852.92	$ 864.31	$ 824.25	$ 808.85	$ 808.85	$ 808.85	$ 808.85
AIX Config - 4	Fully Managed (1) - Bronze Tier	Per Config		CCSI13310165-A						$ 641.24	$ 650.60	$ 660.08	$ 669.71	$ 682.76	$ 644.39	$ 630.67	$ 630.67	$ 630.67	$ 630.67
AIX Config - 4	Fully Managed (1) - Basic Tier	Per Config		CCSI13310166-A						$ 448.32	$ 459.10	$ 470.14	$ 481.45	$ 496.18	$ 459.49	$ 447.43	$ 447.43	$ 447.43	$ 447.43
AIX Config - 5	Fully Managed (1) - Platinum Tier	Per Config		CCSI13310167-A						$ 1 254.37	$ 1 257.27	$ 1 260.17	$ 1 263.09	$ 1 269.40	$ 1 224.31	$ 1 203.85	$ 1 203.85	$ 1 203.85	$ 1 203.85
AIX Config - 5	Fully Managed (1) - Gold Tier	Per Config		CCSI13310168-A						$ 1,027.52	$ 1,032.06	$ 1,036.62	$ 1,041.20	$ 1,049.21	$ 1,005.80	$ 988.70	$ 988.70	$ 988.70	$ 988.70
AIX Config - 5	Fully Managed (1) - Silver Tier	Per Config		CCSI13310169-A						$ 834.29	$ 840.46	$ 846.67	$ 852.92	$ 864.31	$ 824.25	$ 808.85	$ 808.85	$ 808.85	$ 808.85
AIX Config - 5	Fully Managed (1) - Bronze Tier	Per Config		CCSI13310170-A						$ 641.24	$ 650.60	$ 660.08	$ 669.71	$ 682.76	$ 644.39	$ 630.67	$ 630.67	$ 630.67	$ 630.67
AIX Config - 5	Fully Managed (1) - Basic Tier	Per Config		CCSI13310171-A						$ 448.32	$ 459.10	$ 470.14	$ 481.45	$ 496.18	$ 459.49	$ 447.43	$ 447.43	$ 447.43	$ 447.43
AIX Config - 1	3.0GHz POWER7		1							$ 97.49	$ 96.52	$ 95.55	$ 94.59	$ 93.64	$ 92.71	$ 91.79	$ 91.79	$ 91.79	$ 91.79
	0.5 Cores (1 X 0.5 Cores)		1							$ 30.26	$ 29.95	$ 29.65	$ 29.36	$ 29.07	$ 28.77	$ 28.48	$ 28.48	$ 28.48	$ 28.48
	6 GB RAM		6							$ 7.56	$ 7.50	$ 7.44	$ 7.38	$ 7.38	$ 7.32	$ 7.20	$ 7.20	$ 7.20	$ 7.20
	AIX		1							$ 47.07	$ 49.59	$ 51.27	$ 54.64	$ 57.15	$ 59.67	$ 63.04	$ 63.04	$ 63.04	$ 63.04
	Sub-Total									**$ 182.38**	**$ 183.56**	**$ 183.91**	**$ 185.97**	**$ 187.24**	**$ 188.47**	**$ 190.51**	**$ 190.51**	**$ 190.51**	**$ 190.51**
AIX Config - 1	Fully Managed (1) - Platinum Tier		1							$ 928.73	$ 941.01	$ 952.63	$ 966.12	$ 981.43	$ 946.13	$ 937.13	$ 937.13	$ 937.13	$ 937.13
AIX Config - 1	Fully Managed (1) - Gold Tier		1							$ 815.48	$ 829.28	$ 842.51	$ 857.71	$ 874.68	$ 840.23	$ 832.07	$ 832.07	$ 832.07	$ 832.07
AIX Config - 1	Fully Managed (1) - Silver Tier		1							$ 719.11	$ 733.58	$ 747.55	$ 763.57	$ 781.39	$ 747.78	$ 740.46	$ 740.46	$ 740.46	$ 740.46
AIX Config - 1	Fully Managed (1) - Bronze Tier		1							$ 622.79	$ 637.88	$ 652.58	$ 669.44	$ 688.10	$ 655.32	$ 648.85	$ 648.85	$ 648.85	$ 648.85
AIX Config - 1	Fully Managed (1) - Basic Tier		1							$ 526.67	$ 542.25	$ 557.61	$ 575.31	$ 594.81	$ 562.88	$ 557.24	$ 557.24	$ 557.24	$ 557.24
AIX Config - 2	3.0GHz POWER7		1							$ 97.49	$ 96.52	$ 95.55	$ 94.59	$ 93.64	$ 92.71	$ 91.79	$ 91.79	$ 91.79	$ 91.79
	1.0 Cores (2 X 0.5 Cores)		2							$ 60.52	$ 59.90	$ 59.30	$ 58.72	$ 58.14	$ 57.54	$ 56.96	$ 56.96	$ 56.96	$ 56.96
	12 GB RAM		12							$ 15.12	$ 15.00	$ 14.88	$ 14.76	$ 14.76	$ 14.64	$ 14.40	$ 14.40	$ 14.40	$ 14.40
	AIX		1							$ 47.07	$ 49.59	$ 51.27	$ 54.64	$ 57.15	$ 59.67	$ 63.04	$ 63.04	$ 63.04	$ 63.04
	Sub-Total									**$ 220.20**	**$ 221.01**	**$ 221.00**	**$ 222.71**	**$ 223.69**	**$ 224.56**	**$ 226.19**	**$ 226.19**	**$ 226.19**	**$ 226.19**
AIX Config - 2	Fully Managed (1) - Platinum Tier		1							$ 977.47	$ 989.58	$ 1,001.04	$ 1,014.39	$ 1,029.60	$ 993.30	$ 983.25	$ 983.25	$ 983.25	$ 983.25
AIX Config - 2	Fully Managed (1) - Gold Tier		1							$ 864.17	$ 877.01	$ 889.26	$ 903.46	$ 919.50	$ 884.04	$ 875.67	$ 875.67	$ 875.67	$ 875.67
AIX Config - 2	Fully Managed (1) - Silver Tier		1							$ 767.77	$ 781.29	$ 794.29	$ 809.31	$ 827.04	$ 793.26	$ 785.74	$ 785.74	$ 785.74	$ 785.74
AIX Config - 2	Fully Managed (1) - Bronze Tier		1							$ 671.55	$ 686.46	$ 701.00	$ 717.71	$ 736.28	$ 703.34	$ 696.65	$ 696.65	$ 696.65	$ 696.65
AIX Config - 2	Fully Managed (1) - Basic Tier		1							$ 575.39	$ 590.82	$ 606.03	$ 623.58	$ 642.99	$ 610.88	$ 605.03	$ 605.03	$ 605.03	$ 605.03
AIX Config - 3	3.0GHz POWER7		1							$ 97.49	$ 96.52	$ 95.55	$ 94.59	$ 93.64	$ 92.71	$ 91.79	$ 91.79	$ 91.79	$ 91.79
	1.5 Cores (3 X 0.5 Cores)		3							$ 90.78	$ 89.85	$ 88.95	$ 88.08	$ 87.21	$ 86.31	$ 85.44	$ 85.44	$ 85.44	$ 85.44
	18 GB RAM		18							$ 22.68	$ 22.50	$ 22.32	$ 22.14	$ 22.14	$ 21.96	$ 21.60	$ 21.60	$ 21.60	$ 21.60
	AIX		1							$ 47.07	$ 49.59	$ 51.27	$ 54.64	$ 57.15	$ 59.67	$ 63.04	$ 63.04	$ 63.04	$ 63.04
	Sub-Total									**$ 258.02**	**$ 258.46**	**$ 258.09**	**$ 259.45**	**$ 260.14**	**$ 260.65**	**$ 261.87**	**$ 261.87**	**$ 261.87**	**$ 261.87**
AIX Config - 3	Fully Managed (1) - Platinum Tier		1							$ 1 042.97	$ 1 054.11	$ 1 064.59	$ 1 076.94	$ 1 092.06	$ 1 055.59	$ 1 045.33	$ 1 045.33	$ 1 045.33	$ 1 045.33

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	Product Name	Unit	Qty per config	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
AIX Config - 3	Fully Managed (1) - Gold Tier		1							$ 929.76	$ 942.42	$ 954.50	$ 968.53	$ 984.48	$ 948.86	$ 939.44	$ 939.44	$ 939.44	$ 939.44
AIX Config - 3	Fully Managed (1) - Silver Tier		1							$ 820.70	$ 834.06	$ 846.91	$ 861.78	$ 878.58	$ 843.79	$ 835.21	$ 835.21	$ 835.21	$ 835.21
AIX Config - 3	Fully Managed (1) - Bronze Tier		1							$ 736.95	$ 750.96	$ 764.54	$ 780.26	$ 797.90	$ 763.96	$ 756.20	$ 756.20	$ 756.20	$ 756.20
AIX Config - 3	Fully Managed (1) - Basic Tier		1							$ 640.72	$ 655.29	$ 669.57	$ 686.13	$ 704.61	$ 671.50	$ 664.60	$ 664.60	$ 664.60	$ 664.60
AIX Config - 4	3.0GHz POWER7		1							$ 97.49	$ 96.52	$ 95.55	$ 94.59	$ 93.64	$ 92.71	$ 91.79	$ 91.79	$ 91.79	$ 91.79
	1.0 Cores (2 X 0.5 Cores)		2							$ 60.52	$ 59.90	$ 59.30	$ 58.72	$ 58.14	$ 57.54	$ 56.96	$ 56.96	$ 56.96	$ 56.96
	12 GB RAM		12							$ 15.12	$ 15.00	$ 14.88	$ 14.76	$ 14.76	$ 14.64	$ 14.40	$ 14.40	$ 14.40	$ 14.40
	AIX		1							$ 47.07	$ 49.59	$ 51.27	$ 54.64	$ 57.15	$ 59.67	$ 63.04	$ 63.04	$ 63.04	$ 63.04
	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization		1							$ 360.37	$ 366.72	$ 372.41	$ 380.40	$ 388.18	$ 395.64	$ 404.70	$ 404.70	$ 404.70	$ 404.70
	Sub-Total									**$ 580.57**	**$ 587.73**	**$ 593.41**	**$ 603.11**	**$ 611.87**	**$ 620.20**	**$ 630.89**	**$ 630.89**	**$ 630.89**	**$ 630.89**
AIX Config - 4	Fully Managed (1) - Platinum Tier		1							$ 1,834.94	$ 1,845.00	$ 1,853.58	$ 1,866.20	$ 1,881.27	$ 1,844.51	$ 1,834.74	$ 1,834.74	$ 1,834.74	$ 1,834.74
AIX Config - 4	Fully Managed (1) - Gold Tier		1							$ 1 608.09	$ 1 619.79	$ 1 630.03	$ 1 644.31	$ 1 661.08	$ 1 626.00	$ 1 619.59	$ 1 619.59	$ 1 619.59	$ 1 619.59
AIX Config - 4	Fully Managed (1) - Silver Tier		1							$ 1,414.86	$ 1,428.19	$ 1,440.08	$ 1,456.03	$ 1,476.18	$ 1,444.45	$ 1,439.74	$ 1,439.74	$ 1,439.74	$ 1,439.74
AIX Config - 4	Fully Managed (1) - Bronze Tier		1							$ 1,221.81	$ 1,238.33	$ 1,253.49	$ 1,272.82	$ 1,294.63	$ 1,264.59	$ 1,261.56	$ 1,261.56	$ 1,261.56	$ 1,261.56
AIX Config - 4	Fully Managed (1) - Basic Tier		1							$ 1 028.89	$ 1 046.83	$ 1 063.55	$ 1 084.56	$ 1 108.05	$ 1 079.69	$ 1 078.32	$ 1 078.32	$ 1 078.32	$ 1 078.32
AIX Config - 5	3.0GHz POWER7		1							$ 97.49	$ 96.52	$ 95.55	$ 94.59	$ 93.64	$ 92.71	$ 91.79	$ 91.79	$ 91.79	$ 91.79
	1.0 Cores (2 X 0.5 Cores)		2							$ 60.52	$ 59.90	$ 59.30	$ 58.72	$ 58.14	$ 57.54	$ 56.96	$ 56.96	$ 56.96	$ 56.96
	12 GB RAM		12							$ 15.12	$ 15.00	$ 14.88	$ 14.76	$ 14.76	$ 14.64	$ 14.40	$ 14.40	$ 14.40	$ 14.40
	AIX		1							$ 47.07	$ 49.59	$ 51.27	$ 54.64	$ 57.15	$ 59.67	$ 63.04	$ 63.04	$ 63.04	$ 63.04
	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups		1							$ 206.34	$ 207.26	$ 207.37	$ 209.17	$ 210.16	$ 211.15	$ 212.99	$ 212.99	$ 212.99	$ 212.99
	Sub-Total									**$ 426.54**	**$ 428.27**	**$ 428.37**	**$ 431.88**	**$ 433.85**	**$ 435.71**	**$ 439.18**	**$ 439.18**	**$ 439.18**	**$ 439.18**
AIX Config - 5	Fully Managed (1) - Platinum Tier		1							$ 1 680.91	$ 1 685.54	$ 1 688.54	$ 1 694.97	$ 1 703.25	$ 1 660.02	$ 1 643.03	$ 1 643.03	$ 1 643.03	$ 1 643.03
AIX Config - 5	Fully Managed (1) - Gold Tier		1							$ 1,454.06	$ 1,460.33	$ 1,464.99	$ 1,473.08	$ 1,483.06	$ 1,441.51	$ 1,427.88	$ 1,427.88	$ 1,427.88	$ 1,427.88
AIX Config - 5	Fully Managed (1) - Silver Tier		1							$ 1 260.83	$ 1 268.73	$ 1 275.04	$ 1 284.80	$ 1 298.16	$ 1 259.96	$ 1 248.03	$ 1 248.03	$ 1 248.03	$ 1 248.03
AIX Config - 5	Fully Managed (1) - Bronze Tier		1							$ 1,067.78	$ 1,078.87	$ 1,088.45	$ 1,101.59	$ 1,116.61	$ 1,080.10	$ 1,069.85	$ 1,069.85	$ 1,069.85	$ 1,069.85
AIX Config - 5	Fully Managed (1) - Basic Tier		1							$ 874.86	$ 887.37	$ 898.51	$ 913.33	$ 930.03	$ 895.20	$ 886.61	$ 886.61	$ 886.61	$ 886.61
AIX Config - 5	**Total**									**$ 7,191.52**	**$ 7,237.38**	**$ 7,272.27**	**$ 7,331.53**	**$ 7,398.81**	**$ 7,208.21**	**$ 7,153.76**	**$ 7,153.76**	**$ 7,153.76**	**$ 7,153.76**
Server - Managed Only (2)																			
Server - Managed Only x86 (Windows, Linux)																			
	Platinum Tier	Server/Instance		CCSU13320001-A						$ 435.89	$ 434.81	$ 433.72	$ 399.02	$ 351.14	$ 298.47	$ 253.70	$ 253.70	$ 253.70	$ 253.70
	Gold Tier	Server/Instance		CCSU13320002-A						$ 422.92	$ 421.87	$ 420.82	$ 387.15	$ 340.69	$ 289.59	$ 246.15	$ 246.15	$ 246.15	$ 246.15
	Silver Tier	Server/Instance		CCSU13320003-A						$ 415.26	$ 414.23	$ 413.19	$ 380.14	$ 334.52	$ 284.34	$ 241.69	$ 241.69	$ 241.69	$ 241.69
	Bronze Tier	Server/Instance		CCSU13320004-A						$ 411.92	$ 410.89	$ 409.87	$ 377.08	$ 331.83	$ 282.05	$ 239.75	$ 239.75	$ 239.75	$ 239.75
	Basic Tier	Server/Instance		CCSU13320005-A						$ 408.63	$ 407.61	$ 406.60	$ 374.07	$ 329.18	$ 279.80	$ 237.83	$ 237.83	$ 237.83	$ 237.83
Server - Managed Only UNIX (IBM P-Series, AIX)																			
	Platinum	LPAR		CCSI13320006-A						$ 728.02	$ 743.06	$ 758.40	$ 774.06	$ 791.48	$ 757.50	$ 749.88	$ 749.88	$ 749.88	$ 749.88
	Gold Tier	LPAR		CCSI13320007-A						$ 678.20	$ 694.06	$ 710.29	$ 726.90	$ 745.25	$ 712.21	$ 705.53	$ 705.53	$ 705.53	$ 705.53
	Silver Tier	LPAR		CCSI13320008-A						$ 630.19	$ 645.99	$ 662.18	$ 678.78	$ 697.13	$ 664.10	$ 657.43	$ 657.43	$ 657.43	$ 657.43
	Bronze Tier	LPAR		CCSI13320009-A						$ 572.89	$ 589.46	$ 606.52	$ 624.07	$ 643.36	$ 611.28	$ 605.53	$ 605.53	$ 605.53	$ 605.53
	Basic Tier	LPAR		CCSI13320010-A						$ 462.09	$ 479.27	$ 497.09	$ 515.57	$ 535.81	$ 504.67	$ 499.88	$ 499.88	$ 499.88	$ 499.88
Storage and Backup - Fully Managed (1)																			
Enterprise Storage																			
	* Dedicated - Config 1 - SAN Raid 5	GB		CCSZ13310172-A						$ 0.05	$ 0.05	$ 0.05	$ 0.05	$ 0.04	$ 0.04	$ 0.04	$ 0.04	$ 0.04	$ 0.04
	* Dedicated - Config 2 - SAN Raid 10	GB		CCSZ13310173-A						$ 0.36	$ 0.34	$ 0.32	$ 0.31	$ 0.29	$ 0.28	$ 0.26	$ 0.26	$ 0.26	$ 0.26
	Dedicated - Config 3 - Net Attached	GB		CCSZ13310174-A						$ 0.05	$ 0.06	$ 0.06	$ 0.05	$ 0.05	$ 0.05	$ 0.05	$ 0.05	$ 0.05	$ 0.05
Tape and Backup																			
	** Server Tape Stored	GB Stored		CCSU13310175-A						$ 0.02	$ 0.02	$ 0.02	$ 0.02	$ 0.01	$ 0.01	$ 0.01	$ 0.01	$ 0.01	$ 0.01
	** Offsite Tape Storage	Tapes		CCSU13310176-A						$ 0.38	$ 0.36	$ 0.35	$ 0.34	$ 0.33	$ 0.31	$ 0.31	$ 0.31	$ 0.31	$ 0.31
Limited Co-Lo (Data Center Only Charge) (3)																			
Limited Co-Lo Configurations																			
Co-Lo Config - 1	1/4 Rack Configuration includes 10U Cabinet	Per Config		CCSU13330001-A						$ 50.08	$ 48.14	$ 46.16	$ 46.35	$ 43.85	$ 41.67	$ 39.42	$ 39.42	$ 39.42	$ 39.42
Co-Lo Config - 2	1/2 Rack Configuration includes 21U Cabinet	Per Config		CCSU13330002-A						$ 77.62	$ 73.94	$ 70.15	$ 66.25	$ 64.08	$ 59.93	$ 55.65	$ 55.65	$ 55.65	$ 55.65
Co-Lo Config - 3	Full Rack Configuration includes 42U Cabinet	Per Config		CCSU13330003-A						$ 176.43	$ 169.37	$ 162.10	$ 154.60	$ 114.18	$ 106.18	$ 97.91	$ 97.91	$ 97.91	$ 97.91
Co-Lo Config - 1 2 3	Network Bandwidth	Per GB		CCSU13330004-A						$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Co-Lo Config - 1, 2, 3	100Mb/s Uplink	Each		CCSU13330005-A						$ 6.25	$ 6.44	$ 6.63	$ 6.83	$ 7.03	$ 7.25	$ 7.46	$ 7.46	$ 7.46	$ 7.46
Co-Lo Config - 1, 2, 3	IP Addresses	Each		CCSU13330006-A						$ 0.75	$ 0.75	$ 0.75	$ 0.75	$ 0.75	$ 0.75	$ 0.75	$ 0.75	$ 0.75	$ 0.75
Co-Lo Config - 1	110V AC Circuits	Per Circuit		CCSU13330007-A						$ 14.00	$ 14.42	$ 14.85	$ 15.30	$ 15.76	$ 16.23	$ 16.72	$ 16.72	$ 16.72	$ 16.72

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	**Product Name**	**Unit**	**Qty per config**	**Provider Part Number**	**Version Major**	**Version Minor**	**Version Build**	**Manufacturer ID**	**Equipment Code**	**Price per unit \ Per Month**									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Co-Lo Config - 1	1/4 Rack Configuration includes 10U Cabinet		1							$ 50.08	$ 48.14	$ 46.16	$ 46.35	$ 43.85	$ 41.67	$ 39.42	$ 39.42	$ 39.42	$ 39.42
	GB Network Bandwidth		5000							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	100Mb/s Uplink		1							$ 6.25	$ 6.44	$ 6.63	$ 6.83	$ 7.03	$ 7.25	$ 7.46	$ 7.46	$ 7.46	$ 7.46
	IP Addresses		6							$ 4.50	$ 4.50	$ 4.50	$ 4.50	$ 4.50	$ 4.50	$ 4.50	$ 4.50	$ 4.50	$ 4.50
	110V AC Circuits		5							$ 70.00	$ 72.10	$ 74.25	$ 76.50	$ 78.80	$ 81.15	$ 83.60	$ 83.60	$ 83.60	$ 83.60
Co-Lo Config - 1	**Total**									**$ 130.83**	**$ 131.18**	**$ 131.54**	**$ 134.18**	**$ 134.18**	**$ 134.57**	**$ 134.98**	**$ 134.98**	**$ 134.98**	**$ 134.98**
Co-Lo Config - 2	1/2 Rack Configuration includes 21U Cabinet Space		1							$ 77.62	$ 73.94	$ 70.15	$ 66.25	$ 64.08	$ 59.93	$ 55.65	$ 55.65	$ 55.65	$ 55.65
	10,000 GB Network Bandwidth		10000							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	100Mb/s Uplink		1							$ 6.25	$ 6.44	$ 6.63	$ 6.83	$ 7.03	$ 7.25	$ 7.46	$ 7.46	$ 7.46	$ 7.46
	IP Addresses		14							$ 10.50	$ 10.50	$ 10.50	$ 10.50	$ 10.50	$ 10.50	$ 10.50	$ 10.50	$ 10.50	$ 10.50
	110V AC Circuits		10							$ 140.00	$ 144.20	$ 148.50	$ 153.00	$ 157.60	$ 162.30	$ 167.20	$ 167.20	$ 167.20	$ 167.20
Co-Lo Config - 2	**Total**									**$ 234.37**	**$ 235.08**	**$ 235.78**	**$ 236.58**	**$ 239.21**	**$ 239.98**	**$ 240.81**	**$ 240.81**	**$ 240.81**	**$ 240.81**
Co-Lo Config - 3	Full Rack Configuration includes 42U Cabinet		1							$ 176.43	$ 169.37	$ 162.10	$ 154.60	$ 114.18	$ 106.18	$ 97.91	$ 97.91	$ 97.91	$ 97.91
	GB Network Bandwidth		20000							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	100Mb/s Uplink		1							$ 6.25	$ 6.44	$ 6.63	$ 6.83	$ 7.03	$ 7.25	$ 7.46	$ 7.46	$ 7.46	$ 7.46
	IP Addresses		30							$ 22.50	$ 22.50	$ 22.50	$ 22.50	$ 22.50	$ 22.50	$ 22.50	$ 22.50	$ 22.50	$ 22.50
	110V AC Circuits		20							$ 280.00	$ 288.40	$ 297.00	$ 306.00	$ 315.20	$ 324.60	$ 334.40	$ 334.40	$ 334.40	$ 334.40
Co-Lo Config - 3	**Total**									**$ 485.18**	**$ 486.71**	**$ 488.23**	**$ 489.93**	**$ 458.91**	**$ 460.53**	**$ 462.27**	**$ 462.27**	**$ 462.27**	**$ 462.27**
Mainframe Services (4)																			
IBM Mainframe																			
	*** IBM Mainframe Allocated DASD	GB		CCSI13310177-A						$ 1.25	$ 1.19	$ 1.13	$ 1.08	$ 1.02	$ 0.97	$ 0.91	$ 0.91	$ 0.91	$ 0.91
	IBM Tapes in Storage - VTS	GB		CCSI13310178-A						$ 0.29	$ 0.29	$ 0.28	$ 0.28	$ 0.27	$ 0.27	$ 0.25	$ 0.25	$ 0.25	$ 0.25
	IBM Offsite Tape Storage	Tape/Reel		CCSI13310179-A						$ 0.38	$ 0.36	$ 0.35	$ 0.34	$ 0.33	$ 0.31	$ 0.31	$ 0.31	$ 0.31	$ 0.31
IBM Mainframe Configurations																			
IBM Mainframe Config - 1	IBM System zEnterprise Processor z/OS	Per MIP		CCSI13310180-A						$ 102.61	$ 104.92	$ 107.23	$ 101.87	$ 96.78	$ 91.94	$ 87.34	$ 87.34	$ 87.34	$ 87.34
IBM Mainframe Config - 2	IBM System zEnterprise Processor Virtual Linux Prod IFL	Per MIP		CCSI13310181-A						$ 90.16	$ 92.19	$ 94.22	$ 89.51	$ 85.04	$ 80.79	$ 76.75	$ 76.75	$ 76.75	$ 76.75
IBM Mainframe Config - 3	IBM System zEnterprise Processor Virtual Linux Prod IFLw/ Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per MIP		CCSI13310182-A						$ 104.67	$ 107.56	$ 110.44	$ 105.58	$ 100.57	$ 96.12	$ 91.71	$ 91.71	$ 91.71	$ 91.71
IBM AS400 Config 1	IBM i Series / AS400	Per CPW		CCSI13310183-A						$ 11.20	$ 11.45	$ 11.69	$ 11.12	$ 10.56	$ 10.03	$ 9.53	$ 9.53	$ 9.53	$ 9.53
IBM AS400 Config 2	IBM i Series / AS400 w/ Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per CPW		CCSI13310184-A						$ 28.17	$ 29.38	$ 30.58	$ 29.73	$ 28.57	$ 27.71	$ 26.71	$ 26.71	$ 26.71	$ 26.71
IBM Mainframe Config - 1	Mainframe Services (4) - Platinum Tier	Per Config		CCSI13310185-A						$ 115.12	$ 202.54	$ 289.95	$ 286.02	$ 282.44	$ 269.93	$ 266.76	$ 266.76	$ 266.76	$ 266.76
IBM Mainframe Config - 1	Mainframe Services (4) - Gold Tier	Per Config		CCSI13310186-A						$ 100.47	$ 187.56	$ 274.65	$ 271.46	$ 268.60	$ 256.79	$ 254.27	$ 254.27	$ 254.27	$ 254.27
IBM Mainframe Config - 1	Mainframe Services (4) - Basic Tier	Per Config		CCSI13310187-A						$ 90.32	$ 177.17	$ 264.03	$ 261.38	$ 259.02	$ 247.70	$ 245.64	$ 245.64	$ 245.64	$ 245.64
IBM Mainframe Config - 2	Mainframe Services (4) - Platinum Tier	Per Config		CCSI13310188-A						$ 101.14	$ 188.23	$ 275.33	$ 272.12	$ 269.22	$ 257.38	$ 254.84	$ 254.84	$ 254.84	$ 254.84
IBM Mainframe Config - 2	Mainframe Services (4) - Gold Tier	Per Config		CCSI13310189-A						$ 88.29	$ 175.10	$ 261.91	$ 259.36	$ 257.10	$ 245.87	$ 243.89	$ 243.89	$ 243.89	$ 243.89
IBM Mainframe Config - 2	Mainframe Services (4) - Basic Tier	Per Config		CCSI13310190-A						$ 79.37	$ 165.97	$ 252.58	$ 250.50	$ 248.69	$ 237.87	$ 236.30	$ 236.30	$ 236.30	$ 236.30
IBM Mainframe Config - 3	Mainframe Services (4) - Platinum Tier	Per Config		CCSI13310191-A						$ 187.78	$ 323.40	$ 459.02	$ 445.97	$ 434.11	$ 413.46	$ 402.72	$ 402.72	$ 402.72	$ 402.72
IBM Mainframe Config - 3	Mainframe Services (4) - Gold Tier	Per Config		CCSI13310192-A						$ 162.06	$ 297.12	$ 432.18	$ 420.45	$ 409.86	$ 390.42	$ 380.82	$ 380.82	$ 380.82	$ 380.82
IBM Mainframe Config - 3	Mainframe Services (4) - Basic Tier	Per Config		CCSI13310193-A						$ 144.23	$ 278.87	$ 413.51	$ 402.74	$ 393.04	$ 374.43	$ 365.64	$ 365.64	$ 365.64	$ 365.64
IBM AS400 Config 1	Mainframe Services (4) - Platinum Tier	Per Config		CCSI13310194-A						$ 12.56	$ 97.66	$ 182.77	$ 184.17	$ 185.68	$ 178.02	$ 179.44	$ 179.44	$ 179.44	$ 179.44
IBM AS400 Config 1	Mainframe Services (4) - Gold Tier	Per Config		CCSI13310195-A						$ 10.96	$ 96.03	$ 181.10	$ 182.59	$ 184.18	$ 176.60	$ 178.07	$ 178.07	$ 178.07	$ 178.07
IBM AS400 Config 1	Mainframe Services (4) - Basic Tier	Per Config		CCSI13310196-A						$ 9.85	$ 94.90	$ 179.94	$ 181.49	$ 183.13	$ 175.60	$ 177.15	$ 177.15	$ 177.15	$ 177.15
IBM AS400 Config 2	Mainframe Services (4) - Platinum Tier	Per Config		CCSI13310197-A						$ 30.21	$ 121.58	$ 212.94	$ 212.86	$ 212.96	$ 203.93	$ 204.07	$ 204.07	$ 204.07	$ 204.07
IBM AS400 Config 2	Mainframe Services (4) - Gold Tier	Per Config		CCSI13310198-A						$ 27.02	$ 118.31	$ 209.61	$ 209.70	$ 209.95	$ 201.07	$ 201.36	$ 201.36	$ 201.36	$ 201.36
IBM AS400 Config 2	Mainframe Services (4) - Basic Tier	Per Config		CCSI13310199-A						$ 24.80	$ 116.05	$ 207.29	$ 207.50	$ 207.87	$ 199.09	$ 199.48	$ 199.48	$ 199.48	$ 199.48
IBM Mainframe Config - 1	IBM System zEnterprise Processor z/OS		1							$ 102.61	$ 104.92	$ 107.23	$ 101.87	$ 96.78	$ 91.94	$ 87.34	$ 87.34	$ 87.34	$ 87.34
	Sub-Total									**$ 102.61**	**$ 104.92**	**$ 107.23**	**$ 101.87**	**$ 96.78**	**$ 91.94**	**$ 87.34**	**$ 87.34**	**$ 87.34**	**$ 87.34**
IBM Mainframe Config - 1	Mainframe Services (4) - Platinum Tier		1							$ 217.73	$ 307.46	$ 397.18	$ 387.89	$ 379.22	$ 361.87	$ 354.10	$ 354.10	$ 354.10	$ 354.10
IBM Mainframe Config - 1	Mainframe Services (4) - Gold Tier		1							$ 203.08	$ 292.48	$ 381.88	$ 373.33	$ 365.38	$ 348.73	$ 341.61	$ 341.61	$ 341.61	$ 341.61
IBM Mainframe Config - 1	Mainframe Services (4) - Basic Tier		1							$ 192.93	$ 282.09	$ 371.26	$ 363.25	$ 355.80	$ 339.64	$ 332.98	$ 332.98	$ 332.98	$ 332.98
IBM Mainframe Config - 2	IBM System zEnterprise Processor Virtual Linux Prod IFL		1							$ 90.16	$ 92.19	$ 94.22	$ 89.51	$ 85.04	$ 80.79	$ 76.75	$ 76.75	$ 76.75	$ 76.75

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	Product Name	Unit	Qty per config	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
	Sub-Total									**$ 90.16**	**$ 92.19**	**$ 94.22**	**$ 89.51**	**$ 85.04**	**$ 80.79**	**$ 76.75**	**$ 76.75**	**$ 76.75**	**$ 76.75**
IBM Mainframe Config - 2	Mainframe Services (4) - Platinum Tier		1							$ 191.30	$ 280.42	$ 369.55	$ 361.63	$ 354.26	$ 338.17	$ 331.59	$ 331.59	$ 331.59	$ 331.59
IBM Mainframe Config - 2	Mainframe Services (4) - Gold Tier		1							$ 178.45	$ 267.29	$ 356.13	$ 348.87	$ 342.14	$ 326.66	$ 320.64	$ 320.64	$ 320.64	$ 320.64
IBM Mainframe Config - 2	Mainframe Services (4) - Basic Tier		1							$ 169.53	$ 258.16	$ 346.80	$ 340.01	$ 333.73	$ 318.66	$ 313.05	$ 313.05	$ 313.05	$ 313.05
IBM Mainframe Config - 3	IBM System zEnterprise Processor Virtual Linux Prod IFL w/ Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization		1							$ 104.67	$ 107.56	$ 110.44	$ 105.58	$ 100.57	$ 96.12	$ 91.71	$ 91.71	$ 91.71	$ 91.71
	Sub-Total									**$ 104.67**	**$ 107.56**	**$ 110.44**	**$ 105.58**	**$ 100.57**	**$ 96.12**	**$ 91.71**	**$ 91.71**	**$ 91.71**	**$ 91.71**
IBM Mainframe Config - 3	Mainframe Services (4) - Platinum Tier		1							$ 292.45	$ 430.96	$ 569.46	$ 551.55	$ 534.68	$ 509.58	$ 494.43	$ 494.43	$ 494.43	$ 494.43
IBM Mainframe Config - 3	Mainframe Services (4) - Gold Tier		1							$ 266.73	$ 404.68	$ 542.62	$ 526.03	$ 510.43	$ 486.54	$ 472.53	$ 472.53	$ 472.53	$ 472.53
IBM Mainframe Config - 3	Mainframe Services (4) - Basic Tier		1							$ 248.90	$ 386.43	$ 523.95	$ 508.32	$ 493.61	$ 470.55	$ 457.35	$ 457.35	$ 457.35	$ 457.35
IBM AS400 Config 1	IBM i Series / AS400		1							$ 11.20	$ 11.45	$ 11.69	$ 11.12	$ 10.56	$ 10.03	$ 9.53	$ 9.53	$ 9.53	$ 9.53
	Sub-Total									**$ 11.20**	**$ 11.45**	**$ 11.69**	**$ 11.12**	**$ 10.56**	**$ 10.03**	**$ 9.53**	**$ 9.53**	**$ 9.53**	**$ 9.53**
IBM AS400 Config 1	Mainframe Services (4) - Platinum Tier		1							$ 23.76	$ 109.11	$ 194.46	$ 195.29	$ 196.24	$ 188.05	$ 188.97	$ 188.97	$ 188.97	$ 188.97
IBM AS400 Config 1	Mainframe Services (4) - Gold Tier		1							$ 22.16	$ 107.48	$ 192.79	$ 193.71	$ 194.74	$ 186.63	$ 187.60	$ 187.60	$ 187.60	$ 187.60
IBM AS400 Config 1	Mainframe Services (4) - Basic Tier		1							$ 21.05	$ 106.35	$ 191.63	$ 192.61	$ 193.69	$ 185.63	$ 186.68	$ 186.68	$ 186.68	$ 186.68
IBM AS400 Config 2	IBM i Series / AS400 w/ Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization		1							$ 28.17	$ 29.38	$ 30.58	$ 29.73	$ 28.57	$ 27.71	$ 26.71	$ 26.71	$ 26.71	$ 26.71
	Sub-Total									**$ 28.17**	**$ 29.38**	**$ 30.58**	**$ 29.73**	**$ 28.57**	**$ 27.71**	**$ 26.71**	**$ 26.71**	**$ 26.71**	**$ 26.71**
IBM AS400 Config 2	Mainframe Services (4) - Platinum Tier		1							$ 58.38	$ 150.96	$ 243.52	$ 242.59	$ 241.53	$ 231.64	$ 230.78	$ 230.78	$ 230.78	$ 230.78
IBM AS400 Config 2	Mainframe Services (4) - Gold Tier		1							$ 55.19	$ 147.69	$ 240.19	$ 239.43	$ 238.52	$ 228.78	$ 228.07	$ 228.07	$ 228.07	$ 228.07
IBM AS400 Config 2	Mainframe Services (4) - Basic Tier		1							$ 52.97	$ 145.43	$ 237.87	$ 237.23	$ 236.44	$ 226.80	$ 226.19	$ 226.19	$ 226.19	$ 226.19
Unisys Mainframe																			
	*** Unisys DASD	GB		CCSU13310200-A						$ 0.14	$ 0.14	$ 0.14	$ 0.14	$ 0.14	$ 0.12	$ 0.12	$ 0.12	$ 0.12	$ 0.12
	Unisys Tapes in Storage - VTS	GB		CCSU13310201-A						$ 0.07	$ 0.07	$ 0.07	$ 0.07	$ 0.07	$ 0.05	$ 0.05	$ 0.05	$ 0.05	$ 0.05
	Unisys Offsite Tape Storage	Tape/Reel		CCSU13310202-A						$ 0.38	$ 0.36	$ 0.35	$ 0.34	$ 0.33	$ 0.31	$ 0.31	$ 0.31	$ 0.31	$ 0.31
Unisys Mainframe Configurations																			
Unisys Mainframe Config - 1	Unisys (Clearpath / Dorado)	Per MIP		CCSU13310203-A						$ 190.93	$ 188.45	$ 177.92	$ 176.87	$ 175.47	$ 174.53	$ 173.13	$ 173.13	$ 173.13	$ 173.13
Unisys Mainframe Config - 2	Unisys (Clearpath / Libra)	Per MIP		CCSU13310204-A						$ 79.83	$ 79.77	$ 79.77	$ 79.76	$ 78.42	$ 74.51	$ 73.23	$ 73.23	$ 73.23	$ 73.23
Unisys Mainframe Config - 3	Unisys (Clearpath / Dorado) w/ Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per MIP		CCSU13310205-A						$ 215.77	$ 212.93	$ 202.35	$ 200.91	$ 199.26	$ 197.93	$ 196.16	$ 196.16	$ 196.16	$ 196.16
Unisys Mainframe Config - 4	Unisys (Clearpath / Libra) w/ Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per MIP		CCSU13310206-A						$ 152.12	$ 152.05	$ 152.04	$ 152.07	$ 149.96	$ 144.93	$ 141.63	$ 141.63	$ 141.63	$ 141.63
Unisys Mainframe Config - 1	Mainframe Services (4) - Platinum Tier	Per Config		CCSU13310207-A						$ 111.33	$ 113.02	$ 114.69	$ 116.53	$ 118.40	$ 113.31	$ 114.99	$ 114.99	$ 114.99	$ 114.99
Unisys Mainframe Config - 1	Mainframe Services (4) - Gold Tier	Per Config		CCSU13310208-A						$ 111.09	$ 112.78	$ 114.47	$ 116.30	$ 118.17	$ 113.09	$ 114.77	$ 114.77	$ 114.77	$ 114.77
Unisys Mainframe Config - 1	Mainframe Services (4) - Basic Tier	Per Config		CCSU13310209-A						$ 108.79	$ 110.51	$ 112.32	$ 114.17	$ 116.06	$ 110.98	$ 112.68	$ 112.68	$ 112.68	$ 112.68
Unisys Mainframe Config - 2	Mainframe Services (4) - Platinum Tier	Per Config		CCSU13310210-A						$ 101.29	$ 103.32	$ 105.00	$ 106.79	$ 108.48	$ 103.08	$ 105.40	$ 105.40	$ 105.40	$ 105.40
Unisys Mainframe Config - 2	Mainframe Services (4) - Gold Tier	Per Config		CCSU13310211-A						$ 101.29	$ 103.32	$ 105.00	$ 106.79	$ 108.48	$ 103.08	$ 105.40	$ 105.40	$ 105.40	$ 105.40
Unisys Mainframe Config - 2	Mainframe Services (4) - Basic Tier	Per Config		CCSU13310212-A						$ 101.29	$ 103.33	$ 105.01	$ 106.73	$ 108.48	$ 103.08	$ 105.40	$ 105.40	$ 105.40	$ 105.40
Unisys Mainframe Config - 3	Mainframe Services (4) - Platinum Tier	Per Config		CCSU13310213-A						$ 110.44	$ 112.17	$ 114.77	$ 116.38	$ 118.05	$ 112.55	$ 115.32	$ 115.32	$ 115.32	$ 115.32
Unisys Mainframe Config - 3	Mainframe Services (4) - Gold Tier	Per Config		CCSU13310214-A						$ 110.41	$ 112.14	$ 114.74	$ 116.35	$ 118.02	$ 112.52	$ 115.29	$ 115.29	$ 115.29	$ 115.29
Unisys Mainframe Config - 3	Mainframe Services (4) - Basic Tier	Per Config		CCSU13310215-A						$ 110.11	$ 111.84	$ 114.44	$ 116.06	$ 117.73	$ 112.24	$ 115.02	$ 115.02	$ 115.02	$ 115.02
Unisys Mainframe Config - 4	Mainframe Services (4) - Platinum Tier	Per Config		CCSU13310216-A						$ 106.22	$ 108.01	$ 109.65	$ 111.32	$ 114.03	$ 108.60	$ 110.81	$ 110.81	$ 110.81	$ 110.81
Unisys Mainframe Config - 4	Mainframe Services (4) - Gold Tier	Per Config		CCSU13310217-A						$ 106.22	$ 108.01	$ 109.65	$ 111.32	$ 114.03	$ 108.60	$ 110.81	$ 110.81	$ 110.81	$ 110.81
Unisys Mainframe Config - 4	Mainframe Services (4) - Basic Tier	Per Config		CCSU13310218-A						$ 106.20	$ 108.01	$ 109.65	$ 111.32	$ 114.03	$ 108.60	$ 110.81	$ 110.81	$ 110.81	$ 110.81
Unisys Mainframe Config - 1	Unisys (Clearpath / Dorado)		1							$ 190.93	$ 188.45	$ 177.92	$ 176.87	$ 175.47	$ 174.53	$ 173.13	$ 173.13	$ 173.13	$ 173.13
	Sub-Total									**$ 190.93**	**$ 188.45**	**$ 177.92**	**$ 176.87**	**$ 175.47**	**$ 174.53**	**$ 173.13**	**$ 173.13**	**$ 173.13**	**$ 173.13**
Unisys Mainframe Config - 1	Mainframe Services (4) - Platinum Tier		1							$ 302.26	$ 301.47	$ 292.61	$ 293.40	$ 293.87	$ 287.84	$ 288.12	$ 288.12	$ 288.12	$ 288.12
Unisys Mainframe Config - 1	Mainframe Services (4) - Gold Tier		1							$ 302.02	$ 301.23	$ 292.39	$ 293.17	$ 293.64	$ 287.62	$ 287.90	$ 287.90	$ 287.90	$ 287.90
Unisys Mainframe Config - 1	Mainframe Services (4) - Basic Tier		1							$ 299.72	$ 298.96	$ 290.24	$ 291.04	$ 291.53	$ 285.51	$ 285.81	$ 285.81	$ 285.81	$ 285.81
Unisys Mainframe Config - 2	Unisys (Clearpath / Libra)		1							$ 79.83	$ 79.77	$ 79.77	$ 79.76	$ 78.42	$ 74.51	$ 73.23	$ 73.23	$ 73.23	$ 73.23

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	Product Name	Unit	Qty per config	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
	Sub-Total									**$ 79.83**	**$ 79.77**	**$ 79.77**	**$ 79.76**	**$ 78.42**	**$ 74.51**	**$ 73.23**	**$ 73.23**	**$ 73.23**	**$ 73.23**
Unisys Mainframe Config - 2	Mainframe Services (4) - Platinum Tier		1							$ 181.12	$ 183.09	$ 184.77	$ 186.55	$ 186.90	$ 177.59	$ 178.63	$ 178.63	$ 178.63	$ 178.63
Unisys Mainframe Config - 2	Mainframe Services (4) - Gold Tier		1							$ 181.12	$ 183.09	$ 184.77	$ 186.55	$ 186.90	$ 177.59	$ 178.63	$ 178.63	$ 178.63	$ 178.63
Unisys Mainframe Config - 2	Mainframe Services (4) - Basic Tier		1							$ 181.12	$ 183.10	$ 184.78	$ 186.49	$ 186.90	$ 177.59	$ 178.63	$ 178.63	$ 178.63	$ 178.63
Unisys Mainframe Config - 3	Unisys (Clearpath / Dorado) w/ Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization		1							$ 215.77	$ 212.93	$ 202.35	$ 200.91	$ 199.26	$ 197.93	$ 196.16	$ 196.16	$ 196.16	$ 196.16
	Sub-Total									**$ 215.77**	**$ 212.93**	**$ 202.35**	**$ 200.91**	**$ 199.26**	**$ 197.93**	**$ 196.16**	**$ 196.16**	**$ 196.16**	**$ 196.16**
Unisys Mainframe Config - 3	Mainframe Services (4) - Platinum Tier		1							$ 326.21	$ 325.10	$ 317.12	$ 317.29	$ 317.31	$ 310.48	$ 311.48	$ 311.48	$ 311.48	$ 311.48
Unisys Mainframe Config - 3	Mainframe Services (4) - Gold Tier		1							$ 326.18	$ 325.07	$ 317.09	$ 317.26	$ 317.28	$ 310.45	$ 311.45	$ 311.45	$ 311.45	$ 311.45
Unisys Mainframe Config - 3	Mainframe Services (4) - Basic Tier		1							$ 325.88	$ 324.77	$ 316.79	$ 316.97	$ 316.99	$ 310.17	$ 311.18	$ 311.18	$ 311.18	$ 311.18
Unisys Mainframe Config - 4	Unisys (Clearpath / Libra) w/ Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization		1							$ 152.12	$ 152.05	$ 152.04	$ 152.07	$ 149.96	$ 144.93	$ 141.63	$ 141.63	$ 141.63	$ 141.63
	Sub-Total									**$ 152.12**	**$ 152.05**	**$ 152.04**	**$ 152.07**	**$ 149.96**	**$ 144.93**	**$ 141.63**	**$ 141.63**	**$ 141.63**	**$ 141.63**
Unisys Mainframe Config - 4	Mainframe Services (4) - Platinum Tier		1							$ 258.34	$ 260.06	$ 261.69	$ 263.39	$ 263.99	$ 253.53	$ 252.44	$ 252.44	$ 252.44	$ 252.44
Unisys Mainframe Config - 4	Mainframe Services (4) - Gold Tier		1							$ 258.34	$ 260.06	$ 261.69	$ 263.39	$ 263.99	$ 253.53	$ 252.44	$ 252.44	$ 252.44	$ 252.44
Unisys Mainframe Config - 4	Mainframe Services (4) - Basic Tier		1							$ 258.32	$ 260.06	$ 261.69	$ 263.39	$ 263.99	$ 253.53	$ 252.44	$ 252.44	$ 252.44	$ 252.44
IaaS x86 Server Configurations (Windows)																			
IaaS Windows vConfig - 1	2vCPU	Per Server		CCSU13340001-A						$ 1.42	$ 1.42	$ 1.41	$ 1.30	$ 1.14	$ 0.97	$ 0.83	$ 0.83	$ 0.83	$ 0.83
IaaS Windows vConfig - 2, 4, 5	4vCPU	Per Server		CCSU13340002-A						$ 2.84	$ 2.83	$ 2.83	$ 2.60	$ 2.29	$ 1.95	$ 1.65	$ 1.65	$ 1.65	$ 1.65
IaaS Windows vConfig - 3	8vCPU	Per Server		CCSU13340003-A						$ 5.68	$ 5.67	$ 5.65	$ 5.20	$ 4.58	$ 3.89	$ 3.31	$ 3.31	$ 3.31	$ 3.31
IaaS Windows vConfig - 1, 2, 3, 4, 5	GB Ram	Per GB		CCSU13340004-A						$ 0.37	$ 0.36	$ 0.36	$ 0.33	$ 0.29	$ 0.25	$ 0.21	$ 0.21	$ 0.21	$ 0.21
IaaS Windows vConfig - 1, 2, 3, 4, 5	Windows Server 2008 R2	Per License		CCSU13340005-A						$ 22.91	$ 22.78	$ 22.79	$ 21.57	$ 19.52	$ 17.43	$ 15.63	$ 15.63	$ 15.63	$ 15.63
IaaS Windows vConfig - 1 2 3 4 5	~~Firewall IDS~~	~~Per Config~~																	
IaaS Windows vConfig - 1, 2, 3, 4, 5	~~S t - S t - VPN~~	~~P - C - f g~~																	
IaaS Windows vConfig - 1, 2, 3, 4, 5	~~VPN Client~~	~~Per Config~~																	
IaaS Windows vConfig - 1 2 3 4 5	~~VLAN~~	~~Per Config~~																	
IaaS Windows vConfig - 4	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Config		CCSU13340010-A						$ 99.73	$ 99.48	$ 99.23	$ 91.29	$ 80.34	$ 68.29	$ 58.04	$ 58.04	$ 58.04	$ 58.04
IaaS Windows vConfig - 5	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Config		CCSU13340011-A						$ 26.94	$ 26.87	$ 26.81	$ 24.66	$ 21.70	$ 18.45	$ 15.68	$ 15.68	$ 15.68	$ 15.68
IaaS Windows vConfig - 1	2vCPU		1							$ 1.42	$ 1.42	$ 1.41	$ 1.30	$ 1.14	$ 0.97	$ 0.83	$ 0.83	$ 0.83	$ 0.83
	GB Ram		4							$ 1.48	$ 1.44	$ 1.44	$ 1.32	$ 1.16	$ 1.00	$ 0.84	$ 0.84	$ 0.84	$ 0.84
	Windows Server 2008 R2		1							$ 22.91	$ 22.78	$ 22.79	$ 21.57	$ 19.52	$ 17.43	$ 15.63	$ 15.63	$ 15.63	$ 15.63
	~~Firewall IDS~~		0																
	~~S t - S t - VPN~~		0																
	~~VPN Client~~		0																
	~~VLAN~~		0																
IaaS Windows vConfig - 1	Total									$ 25.81	$ 25.64	$ 25.64	$ 24.19	$ 21.82	$ 19.40	$ 17.30	$ 17.30	$ 17.30	$ 17.30
IaaS Windows vConfig - 2	4vCPU		1							$ 2.84	$ 2.83	$ 2.83	$ 2.60	$ 2.29	$ 1.95	$ 1.65	$ 1.65	$ 1.65	$ 1.65
	GB Ram		16							$ 5.92	$ 5.76	$ 5.76	$ 5.28	$ 4.64	$ 4.00	$ 3.36	$ 3.36	$ 3.36	$ 3.36
	Windows Server 2008 R2		1							$ 22.91	$ 22.78	$ 22.79	$ 21.57	$ 19.52	$ 17.43	$ 15.63	$ 15.63	$ 15.63	$ 15.63
	~~Firewall IDS~~		0																
	~~Site-Site VPN~~		0																
	~~VPN Client~~		0																
	~~VLAN~~		0																
IaaS Windows vConfig - 2	Total									$ 31.67	$ 31.37	$ 31.38	$ 29.45	$ 26.45	$ 23.38	$ 20.64	$ 20.64	$ 20.64	$ 20.64
IaaS Windows vConfig - 3	8vCPU		1							$ 5.68	$ 5.67	$ 5.65	$ 5.20	$ 4.58	$ 3.89	$ 3.31	$ 3.31	$ 3.31	$ 3.31
	GB Ram		64							$ 23.68	$ 23.04	$ 23.04	$ 21.12	$ 18.56	$ 16.00	$ 13.44	$ 13.44	$ 13.44	$ 13.44
	Windows Server 2008 R2		1							$ 22.91	$ 22.78	$ 22.79	$ 21.57	$ 19.52	$ 17.43	$ 15.63	$ 15.63	$ 15.63	$ 15.63
	~~Firewall/IDS~~		0																
	~~Site-Site VPN~~		0																
	~~VPN Cl t~~		0																
	~~VLAN~~		0																
IaaS Windows vConfig - 3	Total									$ 52.27	$ 51.49	$ 51.48	$ 47.89	$ 42.66	$ 37.32	$ 32.38	$ 32.38	$ 32.38	$ 32.38

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	Product Name	Unit	Qty per config	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
IaaS Windows vConfig - 4	4vCPU		1							$ 2.84	$ 2.83	$ 2.83	$ 2.60	$ 2.29	$ 1.95	$ 1.65	$ 1.65	$ 1.65	$ 1.65
	GB Ram		16							$ 5.92	$ 5.76	$ 5.76	$ 5.28	$ 4.64	$ 4.00	$ 3.36	$ 3.36	$ 3.36	$ 3.36
	Windows Server 2008 R2		1							$ 22.91	$ 22.78	$ 22.79	$ 21.57	$ 19.52	$ 17.43	$ 15.63	$ 15.63	$ 15.63	$ 15.63
	~~Firewall IDS~~		0																
	~~S t- S t- VPN~~		0																
	~~VPN Client~~		0																
	~~VLAN~~		0																
	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization		1							$ 99.73	$ 99.48	$ 99.23	$ 91.29	$ 80.34	$ 68.29	$ 58.04	$ 58.04	$ 58.04	$ 58.04
IaaS Windows vConfig - 4	Total									$ 131.40	$ 130.85	$ 130.61	$ 120.74	$ 106.79	$ 91.67	$ 78.68	$ 78.68	$ 78.68	$ 78.68
IaaS Windows vConfig - 5	4vCPU		1							$ 2.84	$ 2.83	$ 2.83	$ 2.60	$ 2.29	$ 1.95	$ 1.65	$ 1.65	$ 1.65	$ 1.65
	GB Ram		16							$ 5.92	$ 5.76	$ 5.76	$ 5.28	$ 4.64	$ 4.00	$ 3.36	$ 3.36	$ 3.36	$ 3.36
	Windows Server 2008 R2		1							$ 22.91	$ 22.78	$ 22.79	$ 21.57	$ 19.52	$ 17.43	$ 15.63	$ 15.63	$ 15.63	$ 15.63
	~~Firewall IDS~~		0																
	~~Site-Site VPN~~		0																
	~~VPN Cl t~~		0																
	~~VLAN~~		0																
	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups		1							$ 26.94	$ 26.87	$ 26.81	$ 24.66	$ 21.70	$ 18.45	$ 15.68	$ 15.68	$ 15.68	$ 15.68
IaaS Windows vConfig - 5	Total									$ 58.61	$ 58.24	$ 58.19	$ 54.11	$ 48.15	$ 41.83	$ 36.32	$ 36.32	$ 36.32	$ 36.32
IaaS x86 Server Configurations (Linux)																			
IaaS Linux vConfig - 1	2vCPU	Per Server		CCSU13340012-A						$ 1.42	$ 1.42	$ 1.41	$ 1.30	$ 1.14	$ 0.97	$ 0.83	$ 0.83	$ 0.83	$ 0.83
IaaS Linux vConfig - 2, 4, 5	4vCPU	Per Server		CCSU13340013-A						$ 2.84	$ 2.83	$ 2.83	$ 2.60	$ 2.29	$ 1.95	$ 1.65	$ 1.65	$ 1.65	$ 1.65
IaaS Linux vConfig - 3	8vCPU	Per Server		CCSU13340014-A						$ 5.68	$ 5.67	$ 5.65	$ 5.20	$ 4.58	$ 3.89	$ 3.31	$ 3.31	$ 3.31	$ 3.31
IaaS Linux vConfig - 1, 2, 3, 4, 5	GB Ram	Per GB		CCSU13340015-A						$ 0.37	$ 0.36	$ 0.36	$ 0.33	$ 0.29	$ 0.25	$ 0.21	$ 0.21	$ 0.21	$ 0.21
IaaS Linux vConfig - 1, 2, 3, 4, 5	RedHat or SUSE	Per License		CCSU13340016-A						$ 63.92	$ 63.68	$ 63.59	$ 59.10	$ 52.55	$ 45.50	$ 39.50	$ 39.50	$ 39.50	$ 39.50
IaaS Linux vConfig - 1 2 3 4 5	~~Firewall IDS~~	~~Per Config~~																	
IaaS Linux vConfig - 1, 2, 3, 4, 5	~~S t- S t- VPN~~	~~P C f g~~																	
IaaS Linux vConfig - 1, 2, 3, 4, 5	~~VPN Client~~	~~Per Config~~																	
IaaS Linux vConfig - 1 2 3 4 5	~~VLAN~~	~~Per Config~~																	
IaaS Linux vConfig - 4	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Config		CCSU13340021-A						$ 140.73	$ 140.38	$ 140.03	$ 128.83	$ 113.37	$ 96.36	$ 81.91	$ 81.91	$ 81.91	$ 81.91
IaaS Linux vConfig - 5	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Config		CCSU13340022-A						$ 67.95	$ 67.78	$ 67.61	$ 62.20	$ 54.73	$ 46.52	$ 39.55	$ 39.55	$ 39.55	$ 39.55
IaaS Linux vConfig - 1	2vCPU		1							$ 1.42	$ 1.42	$ 1.41	$ 1.30	$ 1.14	$ 0.97	$ 0.83	$ 0.83	$ 0.83	$ 0.83
	4 GB Ram		4							$ 1.48	$ 1.44	$ 1.44	$ 1.32	$ 1.16	$ 1.00	$ 0.84	$ 0.84	$ 0.84	$ 0.84
	RedHat or SUSE		1							$ 63.92	$ 63.68	$ 63.59	$ 59.10	$ 52.55	$ 45.50	$ 39.50	$ 39.50	$ 39.50	$ 39.50
	~~Firewall IDS~~		0																
	~~S t- S t- VPN~~		0																
	~~VPN Client~~		0																
	~~VLAN~~		0																
IaaS Linux vConfig - 1	Total									$ 66.82	$ 66.54	$ 66.44	$ 61.72	$ 54.85	$ 47.47	$ 41.17	$ 41.17	$ 41.17	$ 41.17
IaaS Linux vConfig - 2	4vCPU		1							$ 2.84	$ 2.83	$ 2.83	$ 2.60	$ 2.29	$ 1.95	$ 1.65	$ 1.65	$ 1.65	$ 1.65
	16 GB Ram		16							$ 5.92	$ 5.76	$ 5.76	$ 5.28	$ 4.64	$ 4.00	$ 3.36	$ 3.36	$ 3.36	$ 3.36
	RedHat or SUSE		1							$ 63.92	$ 63.68	$ 63.59	$ 59.10	$ 52.55	$ 45.50	$ 39.50	$ 39.50	$ 39.50	$ 39.50
	~~Firewall IDS~~		0																
	~~S t- S t- VPN~~		0																
	~~VPN Client~~		0																
	~~VLAN~~		0																
IaaS Linux vConfig - 2	Total									$ 72.68	$ 72.27	$ 72.18	$ 66.98	$ 59.48	$ 51.45	$ 44.51	$ 44.51	$ 44.51	$ 44.51
IaaS Linux vConfig - 3	8vCPU		1							$ 5.68	$ 5.67	$ 5.65	$ 5.20	$ 4.58	$ 3.89	$ 3.31	$ 3.31	$ 3.31	$ 3.31
	64 GB Ram		64							$ 23.68	$ 23.04	$ 23.04	$ 21.12	$ 18.56	$ 16.00	$ 13.44	$ 13.44	$ 13.44	$ 13.44
	RedHat or SUSE		1							$ 63.92	$ 63.68	$ 63.59	$ 59.10	$ 52.55	$ 45.50	$ 39.50	$ 39.50	$ 39.50	$ 39.50
	~~Firewall IDS~~		0																
	~~Site-Site VPN~~		0																
	~~VPN Client~~		0																
	~~VLAN~~		0																

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	Product Name	Unit	Qty per config	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
IaaS Linux vConfig - 3	Total									$ 93.28	$ 92.39	$ 92.28	$ 85.42	$ 75.69	$ 65.39	$ 56.25	$ 56.25	$ 56.25	$ 56.25
IaaS Linux vConfig - 4	4vCPU		1							$ 2.84	$ 2.83	$ 2.83	$ 2.60	$ 2.29	$ 1.95	$ 1.65	$ 1.65	$ 1.65	$ 1.65
	16 GB Ram		16							$ 5.92	$ 5.76	$ 5.76	$ 5.28	$ 4.64	$ 4.00	$ 3.36	$ 3.36	$ 3.36	$ 3.36
	RedHat or SUSE		1							$ 63.92	$ 63.68	$ 63.59	$ 59.10	$ 52.55	$ 45.50	$ 39.50	$ 39.50	$ 39.50	$ 39.50
	~~F l IDS~~		0																
	~~Site Site VPN~~		0																
	~~VPN Client~~		0																
	~~VLAN~~		0																
	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization		1							$ 140.73	$ 140.38	$ 140.03	$ 128.83	$ 113.37	$ 96.36	$ 81.91	$ 81.91	$ 81.91	$ 81.91
IaaS Linux vConfig - 4	Total									$ 213.41	$ 212.65	$ 212.21	$ 195.81	$ 172.85	$ 147.81	$ 126.42	$ 126.42	$ 126.42	$ 126.42
IaaS Linux vConfig - 5	4vCPU		1							$ 2.84	$ 2.83	$ 2.83	$ 2.60	$ 2.29	$ 1.95	$ 1.65	$ 1.65	$ 1.65	$ 1.65
	16 GB Ram		16							$ 5.92	$ 5.76	$ 5.76	$ 5.28	$ 4.64	$ 4.00	$ 3.36	$ 3.36	$ 3.36	$ 3.36
	RedHat or SUSE		1							$ 63.92	$ 63.68	$ 63.59	$ 59.10	$ 52.55	$ 45.50	$ 39.50	$ 39.50	$ 39.50	$ 39.50
	~~Firewall IDS~~		0																
	~~S t S t VPN~~		0																
	~~VPN Client~~		0																
	~~VLAN~~		0																
	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups		1							$ 67.95	$ 67.78	$ 67.61	$ 62.20	$ 54.73	$ 46.52	$ 39.55	$ 39.55	$ 39.55	$ 39.55
IaaS Linux vConfig - 5	Total									$ 140.63	$ 140.05	$ 139.79	$ 129.18	$ 114.21	$ 97.97	$ 84.06	$ 84.06	$ 84.06	$ 84.06
IaaS Storage Configurations																			
IaaS Storage Config - 1, 2	SAN attached storage	Per GB		CCSU13340023-A						$ 0.15	$ 0.15	$ 0.14	$ 0.13	$ 0.12	$ 0.10	$ 0.08	$ 0.08	$ 0.08	$ 0.08
IaaS Storage Config - 3	Network Attached Storage	Per GB		CCSU13340024-A						$ 0.05	$ 0.06	$ 0.06	$ 0.05	$ 0.05	$ 0.05	$ 0.05	$ 0.05	$ 0.05	$ 0.05
IaaS Storage Config - 1	Raid 5	Per GB		CCSU13340025-A						$ 0.05	$ 0.05	$ 0.05	$ 0.05	$ 0.04	$ 0.04	$ 0.04	$ 0.04	$ 0.04	$ 0.04
IaaS Storage Config - 2	Raid 10	Per GB		CCSU13340026-A						$ 0.36	$ 0.34	$ 0.32	$ 0.31	$ 0.29	$ 0.28	$ 0.26	$ 0.26	$ 0.26	$ 0.26
IaaS Storage Config - 1 2	10K - 15K RPM discs	Per GB		CCSU13340027-A						$ 0.10	$ 0.10	$ 0.10	$ 0.09	$ 0.08	$ 0.07	$ 0.06	$ 0.06	$ 0.06	$ 0.06
IaaS Storage Config - 1	SAN attached storage		1							$ 0.15	$ 0.15	$ 0.14	$ 0.13	$ 0.12	$ 0.10	$ 0.08	$ 0.08	$ 0.08	$ 0.08
	Raid 5		1							$ 0.05	$ 0.05	$ 0.05	$ 0.05	$ 0.04	$ 0.04	$ 0.04	$ 0.04	$ 0.04	$ 0.04
	10K - 15K RPM discs		1							$ 0.10	$ 0.10	$ 0.10	$ 0.09	$ 0.08	$ 0.07	$ 0.06	$ 0.06	$ 0.06	$ 0.06
IaaS Storage Config - 1	Total									$ 0.30	$ 0.30	$ 0.29	$ 0.27	$ 0.24	$ 0.21	$ 0.18	$ 0.18	$ 0.18	$ 0.18
IaaS Storage Config - 2	SAN attached storage		1							$ 0.15	$ 0.15	$ 0.14	$ 0.13	$ 0.12	$ 0.10	$ 0.08	$ 0.08	$ 0.08	$ 0.08
	Raid 10		1							$ 0.36	$ 0.34	$ 0.32	$ 0.31	$ 0.29	$ 0.28	$ 0.26	$ 0.26	$ 0.26	$ 0.26
	10K - 15K RPM discs		1							$ 0.10	$ 0.10	$ 0.10	$ 0.09	$ 0.08	$ 0.07	$ 0.06	$ 0.06	$ 0.06	$ 0.06
IaaS Storage Config - 2	Total									$ 0.61	$ 0.59	$ 0.56	$ 0.53	$ 0.49	$ 0.45	$ 0.40	$ 0.40	$ 0.40	$ 0.40
IaaS Storage Config - 3	Network Attached Storage		1							$ 0.05	$ 0.06	$ 0.06	$ 0.05	$ 0.05	$ 0.05	$ 0.05	$ 0.05	$ 0.05	$ 0.05
IaaS Storage Config - 3	Total									$ 0.05	$ 0.06	$ 0.06	$ 0.05	$ 0.05	$ 0.05	$ 0.05	$ 0.05	$ 0.05	$ 0.05
IaaS Backup Configurations																			
IaaS Backup Config - 1	Remote Offsite backup per GB	Per GB		CCSU13340028-A						$ 0.02	$ 0.02	$ 0.02	$ 0.02	$ 0.01	$ 0.01	$ 0.01	$ 0.01	$ 0.01	$ 0.01
Reserve Account																			
	Reserve Account - Enterprise Datacenter									$84,000.00	$84,000.00	$84,000.00	$84,000.00	$84,000.00	$84,000.00	$84,000.00	$84,000.00	$84,000.00	$84,000.00

Software

Field Name ==>	Product Name		Unit	Price per unit \ Per Month									
Description / Use ==>	*Unique Identifier*		*Unit*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Vendor	**Product**	**Title if equivalency is priced**											
Third Party Software													
□□□□	□□□□

				$ 1,650.55	$ 1,700.06	$ 1,751.06	$ 1,803.59	$ 1,857.70	$ 1,913.43	$ 1,970.84	$ 2,029.96	$ 2,090.86	$ 2,153.58
				$ 5 107.50	$ 5 260.73	$ 5 418.55	$ 5 581.11	$ 5 748.54	$ 5 921.00	$ 6 098.63	$ 6 281.58	$ 6 470.03	$ 6 664.13
				$ 36.92	$ 38.03	$ 39.16	$ 40.34	$ 41.55	$ 42.80	$ 44.08	$ 45.40	$ 46.77	$ 48.17
				$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
				$ 1 758.82	$ 1 809.37	$ 1 860.76	$ 1 913.69	$ 1 968.21	$ 1 933.31	$ 1 991.91	$ 2 051.49	$ 2 112.85	$ 2 176.06
				$ 402.78	$ 414.37	$ 426.15	$ 438.29	$ 450.78	$ 442.78	$ 456.22	$ 469.87	$ 483.94	$ 498.43
				$ 142.12	$ 146.21	$ 150.38	$ 154.67	$ 159.09	$ 156.26	$ 161.01	$ 165.84	$ 170.81	$ 175.94
				$ 548.08	$ 563.80	$ 579.77	$ 596.23	$ 613.18	$ 602.33	$ 620.54	$ 639.06	$ 658.14	$ 677.79
				$ 545.48	$ 561.19	$ 577.17	$ 593.62	$ 610.57	$ 599.72	$ 617.94	$ 636.46	$ 655.54	$ 675.19
				$ 142.92	$ 147.02	$ 151.18	$ 155.47	$ 159.89	$ 157.06	$ 161.81	$ 166.64	$ 171.62	$ 176.74
				$ 142.52	$ 146.61	$ 150.78	$ 155.07	$ 159.49	$ 156.66	$ 161.41	$ 166.24	$ 171.22	$ 176.34
				$ 285.03	$ 293.23	$ 301.56	$ 310.14	$ 318.98	$ 313.32	$ 322.82	$ 332.48	$ 342.43	$ 352.68
				$ 15.90	$ 16.33	$ 16.76	$ 17.21	$ 17.68	$ 17.38	$ 17.88	$ 18.38	$ 18.90	$ 19.44
				$ 18.29	$ 18.78	$ 19.29	$ 19.80	$ 20.34	$ 19.99	$ 20.57	$ 21.15	$ 21.75	$ 22.37
				$ 24.65	$ 25.36	$ 26.09	$ 26.83	$ 27.59	$ 27.10	$ 27.93	$ 28.76	$ 29.63	$ 30.51
				$ 76.99	$ 79.21	$ 81.46	$ 83.79	$ 86.18	$ 84.65	$ 87.22	$ 89.84	$ 92.53	$ 95.31
				$ 55.04	$ 56.63	$ 58.24	$ 59.91	$ 61.62	$ 60.52	$ 62.36	$ 64.23	$ 66.16	$ 68.14
				$ 14.52	$ 14.94	$ 15.36	$ 15.80	$ 16.25	$ 15.96	$ 16.45	$ 16.94	$ 17.45	$ 17.97
				$ 4.09	$ 4.21	$ 4.33	$ 4.45	$ 4.58	$ 4.50	$ 4.63	$ 4.77	$ 4.92	$ 5.06
				$ 0.56	$ 0.57	$ 0.59	$ 0.61	$ 0.62	$ 0.61	$ 0.63	$ 0.65	$ 0.67	$ 0.69
				$ 8.25	$ 8.48	$ 8.73	$ 8.97	$ 9.23	$ 9.07	$ 9.34	$ 9.62	$ 9.91	$ 10.21
				$ 59.13	$ 60.83	$ 62.57	$ 64.35	$ 66.19	$ 65.01	$ 66.99	$ 69.00	$ 71.07	$ 73.20
				$ 8,752.02	$ 9,014.58	$ 9,285.02	$ 9,563.56	$ 9,850.47	$ 10,145.98	$ 10,450.37	$ 10,763.87	$ 11,086.79	$ 11,419.40
				$ 157.94	$ 161.82	$ 165.75	$ 169.81	$ 173.99	$ 171.31	$ 175.80	$ 180.37	$ 185.07	$ 189.91
				$ 980.51	$ 1 009.92	$ 1 040.22	$ 1 071.42	$ 1 103.57	$ 1 136.67	$ 1 170.77	$ 1 205.89	$ 1 242.07	$ 1 279.33
				$ 613.50	$ 628.83	$ 644.41	$ 660.47	$ 677.00	$ 666.42	$ 684.19	$ 702.25	$ 720.86	$ 740.03
				$ 88.86	$ 90.98	$ 93.15	$ 95.38	$ 97.67	$ 97.13	$ 99.60	$ 102.10	$ 104.69	$ 107.35
				$ 142.35	$ 146.46	$ 150.63	$ 154.93	$ 159.35	$ 156.52	$ 161.28	$ 166.12	$ 171.10	$ 176.23
				$ 12,922.64	$ 13,200.97	$ 13,483.95	$ 13,775.41	$ 14,075.62	$ 13,883.43	$ 14,206.09	$ 14,534.14	$ 14,872.03	$ 15,220.05
				$ 144.57	$ 148.28	$ 152.05	$ 155.94	$ 159.94	$ 157.38	$ 161.68	$ 166.06	$ 170.56	$ 175.20
				$ 98.39	$ 101.03	$ 103.73	$ 106.52	$ 109.38	$ 109.42	$ 112.49	$ 115.62	$ 118.85	$ 122.17
				$ 310.27	$ 317.70	$ 325.24	$ 333.02	$ 341.02	$ 335.90	$ 344.50	$ 353.25	$ 362.26	$ 371.54
				$ 195.87	$ 201.52	$ 207.26	$ 213.18	$ 219.27	$ 215.37	$ 221.92	$ 228.57	$ 235.43	$ 242.49
				$ 7,574.99	$ 7,802.24	$ 8,036.30	$ 8,277.39	$ 8,525.71	$ 8,781.49	$ 9,044.93	$ 9,316.27	$ 9,595.77	$ 9,883.64
				$ 732.62	$ 753.74	$ 775.22	$ 797.34	$ 820.12	$ 805.53	$ 830.02	$ 854.92	$ 880.56	$ 906.97
				$ 335.78	$ 345.46	$ 355.31	$ 365.45	$ 375.89	$ 369.20	$ 380.43	$ 391.84	$ 403.59	$ 415.70
				$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
				$ 52.03	$ 53.30	$ 54.59	$ 55.93	$ 57.30	$ 56.42	$ 57.89	$ 59.39	$ 60.93	$ 62.52
				$ 44.10	$ 45.37	$ 46.66	$ 47.99	$ 49.36	$ 48.48	$ 49.95	$ 51.45	$ 53.00	$ 54.58
				$ 48.85	$ 50.12	$ 51.41	$ 52.74	$ 54.11	$ 53.23	$ 54.71	$ 56.21	$ 57.75	$ 59.34
				$ 23.53	$ 24.16	$ 24.81	$ 25.48	$ 26.16	$ 25.72	$ 26.46	$ 27.21	$ 27.98	$ 28.77
				$ 23.39	$ 24.02	$ 24.67	$ 25.33	$ 26.02	$ 25.58	$ 26.32	$ 27.07	$ 27.84	$ 28.63
				$ 26.02	$ 26.65	$ 27.30	$ 27.96	$ 28.65	$ 28.21	$ 28.95	$ 29.69	$ 30.47	$ 31.26
				$ 1.18	$ 1.21	$ 1.24	$ 1.28	$ 1.32	$ 1.29	$ 1.33	$ 1.37	$ 1.41	$ 1.45
				$ 319.56	$ 328.77	$ 338.14	$ 347.79	$ 357.72	$ 351.36	$ 362.04	$ 372.90	$ 384.09	$ 395.61
				$ 735.01	$ 757.06	$ 779.78	$ 803.17	$ 827.27	$ 852.08	$ 877.65	$ 903.98	$ 931.09	$ 959.03
				$ 58.70	$ 60.35	$ 62.00	$ 63.71	$ 65.47	$ 151.73	$ 153.64	$ 155.57	$ 157.55	$ 159.59
				$ 72.13	$ 74.16	$ 76.22	$ 78.33	$ 80.51	$ 166.50	$ 168.86	$ 171.24	$ 173.69	$ 176.21
				$ 85.97	$ 88.40	$ 90.86	$ 93.39	$ 96.00	$ 181.72	$ 184.54	$ 187.39	$ 190.32	$ 193.35
				$ 99.40	$ 102.22	$ 105.07	$ 108.01	$ 111.04	$ 196.48	$ 199.75	$ 203.06	$ 206.47	$ 209.97
				$ 137.25	$ 141.16	$ 145.12	$ 149.21	$ 153.41	$ 238.10	$ 242.64	$ 247.23	$ 251.96	$ 256.83
				$ 58.70	$ 60.35	$ 62.00	$ 63.71	$ 65.47	$ 151.73	$ 153.64	$ 155.57	$ 157.55	$ 159.59
				$ 72.13	$ 74.16	$ 76.22	$ 78.33	$ 80.51	$ 166.50	$ 168.86	$ 171.24	$ 173.69	$ 176.21
				$ 85.97	$ 88.40	$ 90.86	$ 93.39	$ 96.00	$ 181.72	$ 184.54	$ 187.39	$ 190.32	$ 193.35
				$ 99.40	$ 102.22	$ 105.07	$ 108.01	$ 111.04	$ 196.48	$ 199.75	$ 203.06	$ 206.47	$ 209.97
				$ 137.25	$ 141.16	$ 145.12	$ 149.21	$ 153.41	$ 238.10	$ 242.64	$ 247.23	$ 251.96	$ 256.83

				$ 157.60	$ 162.10	$ 166.66	$ 171.35	$ 176.19	$ 260.48	$ 265.69	$ 270.98	$ 276.42	$ 282.03
				$ 58.70	$ 60.35	$ 62.00	$ 63.71	$ 65.47	$ 151.73	$ 153.64	$ 155.57	$ 157.55	$ 159.59
				$ 72.13	$ 74.16	$ 76.22	$ 78.33	$ 80.51	$ 166.50	$ 168.86	$ 171.24	$ 173.69	$ 176.21
				$ 85.97	$ 88.40	$ 90.86	$ 93.39	$ 96.00	$ 181.72	$ 184.54	$ 187.39	$ 190.32	$ 193.35
				$ 99.40	$ 102.22	$ 105.07	$ 108.01	$ 111.04	$ 196.48	$ 199.75	$ 203.06	$ 206.47	$ 209.97
				$ 137.25	$ 141.16	$ 145.12	$ 149.21	$ 153.41	$ 238.10	$ 242.64	$ 247.23	$ 251.96	$ 256.83
				$ 59.72	$ 61.39	$ 63.08	$ 64.82	$ 66.61	$ 152.85	$ 154.79	$ 156.75	$ 158.77	$ 160.85
				$ 72.13	$ 74.16	$ 76.22	$ 78.33	$ 80.51	$ 166.50	$ 168.86	$ 171.24	$ 173.69	$ 176.21
				$ 85.97	$ 88.40	$ 90.86	$ 93.39	$ 96.00	$ 181.72	$ 184.54	$ 187.39	$ 190.32	$ 193.35
				$ 99.40	$ 102.22	$ 105.07	$ 108.01	$ 111.04	$ 196.48	$ 199.75	$ 203.06	$ 206.47	$ 209.97
				$ 137.25	$ 141.16	$ 145.12	$ 149.21	$ 153.41	$ 238.10	$ 242.64	$ 247.23	$ 251.96	$ 256.83
				$ 157.60	$ 162.10	$ 166.66	$ 171.35	$ 176.19	$ 260.48	$ 265.69	$ 270.98	$ 276.42	$ 282.03
				$ 58.70	$ 60.35	$ 62.00	$ 63.71	$ 65.47	$ 151.73	$ 153.64	$ 155.57	$ 157.55	$ 159.59
				$ 72.13	$ 74.16	$ 76.22	$ 78.33	$ 80.51	$ 166.50	$ 168.86	$ 171.24	$ 173.69	$ 176.21
				$ 85.97	$ 88.40	$ 90.86	$ 93.39	$ 96.00	$ 181.72	$ 184.54	$ 187.39	$ 190.32	$ 193.35
				$ 99.40	$ 102.22	$ 105.07	$ 108.01	$ 111.04	$ 196.48	$ 199.75	$ 203.06	$ 206.47	$ 209.97
				$ 137.25	$ 141.16	$ 145.12	$ 149.21	$ 153.41	$ 238.10	$ 242.64	$ 247.23	$ 251.96	$ 256.83
				$ 157.60	$ 162.10	$ 166.66	$ 171.35	$ 176.19	$ 260.48	$ 265.69	$ 270.98	$ 276.42	$ 282.03
				$ 58.70	$ 60.35	$ 62.00	$ 63.71	$ 65.47	$ 151.73	$ 153.64	$ 155.57	$ 157.55	$ 159.59
				$ 72.13	$ 74.16	$ 76.22	$ 78.33	$ 80.51	$ 166.50	$ 168.86	$ 171.24	$ 173.69	$ 176.21
				$ 85.97	$ 88.40	$ 90.86	$ 93.39	$ 96.00	$ 181.72	$ 184.54	$ 187.39	$ 190.32	$ 193.35
				$ 99.40	$ 102.22	$ 105.07	$ 108.01	$ 111.04	$ 196.48	$ 199.75	$ 203.06	$ 206.47	$ 209.97
				$ 137.25	$ 141.16	$ 145.12	$ 149.21	$ 153.41	$ 238.10	$ 242.64	$ 247.23	$ 251.96	$ 256.83
				$ 157.60	$ 162.10	$ 166.66	$ 171.35	$ 176.19	$ 260.48	$ 265.69	$ 270.98	$ 276.42	$ 282.03
				$ 115.27	$ 118.55	$ 121.87	$ 125.29	$ 128.80	$ 213.94	$ 217.74	$ 221.58	$ 225.54	$ 229.62
				$ 142.14	$ 146.19	$ 150.29	$ 154.52	$ 158.88	$ 243.47	$ 248.17	$ 252.93	$ 257.83	$ 262.88
				$ 169.81	$ 174.66	$ 179.58	$ 184.64	$ 189.86	$ 273.91	$ 279.53	$ 285.23	$ 291.10	$ 297.14
				$ 196.67	$ 202.30	$ 208.00	$ 213.88	$ 219.93	$ 303.44	$ 309.96	$ 316.57	$ 323.38	$ 330.40
				$ 272.38	$ 280.19	$ 288.11	$ 296.27	$ 304.67	$ 386.68	$ 395.73	$ 404.92	$ 414.38	$ 424.12
				$ 313.08	$ 322.06	$ 331.18	$ 340.57	$ 350.24	$ 431.43	$ 441.84	$ 452.41	$ 463.30	$ 474.51
				$ 576.01	$ 592.57	$ 609.39	$ 626.72	$ 644.57	$ 720.53	$ 739.73	$ 759.23	$ 779.32	$ 800.01
				$ 660.26	$ 679.25	$ 698.54	$ 718.41	$ 738.88	$ 813.17	$ 835.18	$ 857.55	$ 880.58	$ 904.31
				$ 1,044.47	$ 1,074.54	$ 1,105.10	$ 1,136.57	$ 1,168.99	$ 1,235.62	$ 1,270.48	$ 1,305.90	$ 1,342.39	$ 1,379.97
				$ 1,198.32	$ 1,232.83	$ 1,267.89	$ 1,304.01	$ 1,341.21	$ 1,404.78	$ 1,444.79	$ 1,485.44	$ 1,527.31	$ 1,570.43
				$ 241.45	$ 248.36	$ 255.38	$ 262.60	$ 270.05	$ 352.67	$ 360.69	$ 368.82	$ 377.20	$ 385.83
				$ 292.73	$ 301.12	$ 309.64	$ 318.42	$ 327.46	$ 409.06	$ 418.79	$ 428.66	$ 438.84	$ 449.31
				$ 484.84	$ 498.77	$ 512.92	$ 527.50	$ 542.51	$ 620.28	$ 636.44	$ 652.84	$ 669.74	$ 687.14
				$ 241.45	$ 248.36	$ 255.38	$ 262.60	$ 270.05	$ 352.67	$ 360.69	$ 368.82	$ 377.20	$ 385.83
				$ 292.73	$ 301.12	$ 309.64	$ 318.42	$ 327.46	$ 409.06	$ 418.79	$ 428.66	$ 438.84	$ 449.31
				$ 484.84	$ 498.77	$ 512.92	$ 527.50	$ 542.51	$ 620.28	$ 636.44	$ 652.84	$ 669.74	$ 687.14
				$ 561.76	$ 577.91	$ 594.32	$ 611.22	$ 628.62	$ 704.87	$ 723.59	$ 742.61	$ 762.20	$ 782.37
				$ 241.45	$ 248.36	$ 255.38	$ 262.60	$ 270.05	$ 352.67	$ 360.69	$ 368.82	$ 377.20	$ 385.83
				$ 292.73	$ 301.12	$ 309.64	$ 318.42	$ 327.46	$ 409.06	$ 418.79	$ 428.66	$ 438.84	$ 449.31
				$ 484.84	$ 498.77	$ 512.92	$ 527.50	$ 542.51	$ 620.28	$ 636.44	$ 652.84	$ 669.74	$ 687.14
				$ 24.72	$ 25.43	$ 26.15	$ 26.88	$ 27.64	$ 39.64	$ 40.46	$ 41.29	$ 42.14	$ 43.02
				$ 49.14	$ 50.56	$ 51.99	$ 53.46	$ 54.98	$ 66.49	$ 68.13	$ 69.79	$ 71.50	$ 73.26
				$ 81.93	$ 84.28	$ 86.67	$ 89.13	$ 91.66	$ 111.89	$ 114.61	$ 117.38	$ 120.23	$ 123.16
				$ 269.33	$ 277.08	$ 284.96	$ 293.07	$ 301.42	$ 325.20	$ 334.19	$ 343.32	$ 352.72	$ 362.41
A				$ 354.87	$ 363.36	$ 371.98	$ 380.85	$ 389.99	$ 379.97	$ 389.81	$ 399.80	$ 410.09	$ 420.68

				$ 2,159.97	$ 2,211.78	$ 2,264.38	$ 2,318.56	$ 2,374.36	$ 2,029.78	$ 2,089.84	$ 2,150.82	$ 2,213.63	$ 2,278.32
				$ 197.99	$ 103.21	$ 106.10	$ 109.07	$ 112.14	$ 165.19	$ 168.50	$ 171.85	$ 175.30	$ 178.85
				$ 1,080.61	$ 1,106.51	$ 1,132.81	$ 1,159.90	$ 1,187.80	$ 1,043.27	$ 1,073.31	$ 1,103.79	$ 1,135.20	$ 1,167.54
				$ 378.50	$ 387.58	$ 396.80	$ 406.30	$ 416.09	$ 345.94	$ 356.46	$ 367.16	$ 378.17	$ 389.51
				$ 648.47	$ 664.03	$ 679.83	$ 696.11	$ 712.87	$ 592.68	$ 610.72	$ 629.04	$ 647.91	$ 667.34
				$ 9.90	$ 5.13	$ 5.28	$ 5.43	$ 5.58	$ 5.46	$ 5.62	$ 5.79	$ 5.97	$ 6.14
				$ 149.21	$ 153.51	$ 157.89	$ 162.39	$ 167.03	$ 164.06	$ 169.05	$ 174.12	$ 179.34	$ 184.72
				$ 37.36	$ 38.43	$ 39.53	$ 40.66	$ 41.82	$ 41.07	$ 42.32	$ 43.59	$ 44.90	$ 46.25
				$ 0.97	$ 1.00	$ 1.03	$ 1.05	$ 1.08	$ 1.07	$ 1.10	$ 1.13	$ 1.16	$ 1.20
				$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
				$ 0.66	$ 0.68	$ 0.69	$ 0.71	$ 0.73	$ 0.72	$ 0.74	$ 0.77	$ 0.79	$ 0.81
				$ 0.60	$ 0.62	$ 0.63	$ 0.65	$ 0.67	$ 0.66	$ 0.68	$ 0.70	$ 0.72	$ 0.74
				$ 174.97	$ 180.02	$ 185.15	$ 190.43	$ 195.87	$ 192.39	$ 198.24	$ 204.18	$ 210.31	$ 216.62
				$ 26.97	$ 27.75	$ 28.54	$ 29.36	$ 30.20	$ 29.66	$ 30.56	$ 31.48	$ 32.42	$ 33.39
				$ 34.93	$ 35.94	$ 36.96	$ 38.02	$ 39.10	$ 38.41	$ 39.58	$ 40.76	$ 41.99	$ 43.24
				$ 52.44	$ 53.95	$ 55.49	$ 57.07	$ 58.70	$ 57.66	$ 59.41	$ 61.19	$ 63.03	$ 64.92
				$ 216.35	$ 222.59	$ 228.93	$ 235.46	$ 242.19	$ 237.88	$ 245.12	$ 252.47	$ 260.04	$ 267.84
				$ 41.30	$ 42.49	$ 43.70	$ 44.95	$ 46.23	$ 45.41	$ 46.79	$ 48.19	$ 49.64	$ 51.13
				$ 49.25	$ 50.67	$ 52.12	$ 53.61	$ 55.14	$ 54.16	$ 55.80	$ 57.48	$ 59.20	$ 60.98
				$ 65.17	$ 67.05	$ 68.96	$ 70.92	$ 72.95	$ 71.65	$ 73.83	$ 76.05	$ 78.33	$ 80.68
				$ 87.53	$ 90.05	$ 92.62	$ 95.26	$ 97.98	$ 96.24	$ 99.16	$ 102.14	$ 105.20	$ 108.36
				$ 127.31	$ 130.98	$ 134.72	$ 138.56	$ 142.52	$ 139.98	$ 144.24	$ 148.57	$ 153.02	$ 157.61
				$ 47.74	$ 49.12	$ 50.52	$ 51.96	$ 53.44	$ 52.49	$ 54.09	$ 55.71	$ 57.38	$ 59.10
				$ 87.53	$ 90.05	$ 92.62	$ 95.26	$ 97.98	$ 96.24	$ 99.16	$ 102.14	$ 105.20	$ 108.36
				$ 198.93	$ 204.66	$ 210.49	$ 216.50	$ 222.69	$ 218.72	$ 225.37	$ 232.13	$ 239.10	$ 246.27
				$ 31.83	$ 32.75	$ 33.68	$ 34.64	$ 35.63	$ 35.00	$ 36.06	$ 37.14	$ 38.26	$ 39.40
				$ 9.47	$ 9.74	$ 10.02	$ 10.31	$ 10.60	$ 10.41	$ 10.73	$ 11.05	$ 11.38	$ 11.72
				$ 31.83	$ 32.75	$ 33.68	$ 34.64	$ 35.63	$ 35.00	$ 36.06	$ 37.14	$ 38.26	$ 39.40
				$ 159.14	$ 163.73	$ 168.39	$ 173.20	$ 178.15	$ 174.98	$ 180.30	$ 185.71	$ 191.28	$ 197.01
				$ 127.31	$ 130.98	$ 134.72	$ 138.56	$ 142.52	$ 139.98	$ 144.24	$ 148.57	$ 153.02	$ 157.61
				$ 52.44	$ 53.95	$ 55.49	$ 57.07	$ 58.70	$ 57.66	$ 59.41	$ 61.19	$ 63.03	$ 64.92
				$ 1 469.71	$ 1 512.08	$ 1 555.17	$ 1 599.54	$ 1 645.25	$ 1 615.99	$ 1 665.11	$ 1 715.06	$ 1 766.50	$ 1 819.49
				$ 55.56	$ 57.16	$ 58.79	$ 60.46	$ 62.19	$ 61.09	$ 62.94	$ 64.83	$ 66.78	$ 68.78
				$ 892.57	$ 918.31	$ 944.47	$ 971.42	$ 999.18	$ 981.41	$ 1,011.24	$ 1,041.57	$ 1,072.82	$ 1,105.00
				$ 62.37	$ 64.17	$ 66.00	$ 67.88	$ 69.82	$ 68.58	$ 70.67	$ 72.79	$ 74.97	$ 77.22
				$ 111.11	$ 114.32	$ 117.57	$ 120.93	$ 124.38	$ 122.17	$ 125.89	$ 129.66	$ 133.55	$ 137.56
				$ 111.11	$ 114.32	$ 117.57	$ 120.93	$ 124.38	$ 122.17	$ 125.89	$ 129.66	$ 133.55	$ 137.56
				$ 89.03	$ 91.60	$ 94.21	$ 96.90	$ 99.67	$ 97.89	$ 100.87	$ 103.90	$ 107.01	$ 110.22
				$ 9.75	$ 10.03	$ 10.31	$ 10.61	$ 10.91	$ 10.72	$ 11.04	$ 11.38	$ 11.72	$ 12.07
				$ 12.88	$ 13.25	$ 13.63	$ 14.02	$ 14.42	$ 14.16	$ 14.59	$ 15.03	$ 15.48	$ 15.95
				$ 12.88	$ 13.25	$ 13.63	$ 14.02	$ 14.42	$ 14.16	$ 14.59	$ 15.03	$ 15.48	$ 15.95
				$ 73.26	$ 75.37	$ 77.52	$ 79.73	$ 82.01	$ 80.55	$ 83.00	$ 85.49	$ 88.06	$ 90.70
				$ 73.26	$ 75.37	$ 77.52	$ 79.73	$ 82.01	$ 80.55	$ 83.00	$ 85.49	$ 88.06	$ 90.70
				$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
				$ 0.26	$ 0.26	$ 0.27	$ 0.28	$ 0.29	$ 0.28	$ 0.29	$ 0.30	$ 0.31	$ 0.32
				$ 1 373.66	$ 1 413.26	$ 1 453.53	$ 1 495.00	$ 1 537.72	$ 1 510.37	$ 1 556.29	$ 1 602.97	$ 1 651.05	$ 1 700.57
				$ 997.17	$ 1 025.92	$ 1 055.15	$ 1 085.26	$ 1 116.27	$ 1 096.42	$ 1 129.75	$ 1 163.64	$ 1 198.54	$ 1 234.49
				$ 77.94	$ 15.35	$ 15.78	$ 16.22	$ 16.68	$ 16.07	$ 16.57	$ 17.06	$ 17.57	$ 18.10
				$ 909.08	$ 935.29	$ 961.94	$ 989.39	$ 1,017.66	$ 999.56	$ 1,029.95	$ 1,060.84	$ 1,092.66	$ 1,125.43
				$ 13.38	$ 2.63	$ 2.71	$ 2.78	$ 2.86	$ 2.76	$ 2.84	$ 2.93	$ 3.02	$ 3.11
				$ 65.12	$ 66.22	$ 67.34	$ 68.49	$ 69.68	$ 41.96	$ 43.24	$ 44.54	$ 45.87	$ 47.25
Hybrid Third Party Software													
Vendor	**Product**												
				$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
				$ 23 918.41	$ 24 635.97	$ 25 375.04	$ 26 136.30	$ 26 920.38	$ 27 728.00	$ 28 559.83	$ 29 416.63	$ 30 299.13	$ 31 208.10
				$ 11,718.82	$ 12,070.38	$ 12,432.49	$ 12,805.47	$ 13,189.64	$ 13,585.32	$ 13,992.88	$ 14,412.66	$ 14,845.04	$ 15,290.39
				$ 6,061.27	$ 6,243.10	$ 6,430.39	$ 6,623.31	$ 6,822.00	$ 7,026.67	$ 7,237.47	$ 7,454.60	$ 7,678.23	$ 7,908.58
				$ 3,667.89	$ 3,777.92	$ 3,891.26	$ 4,007.99	$ 4,128.23	$ 4,252.08	$ 4,379.64	$ 4,511.03	$ 4,646.37	$ 4,785.75
				$ 1,897.06	$ 1,953.98	$ 2,012.59	$ 2,072.98	$ 2,135.17	$ 2,199.22	$ 2,265.19	$ 2,333.15	$ 2,403.14	$ 2,475.24
				$ 5,523.37	$ 5,689.07	$ 5,859.73	$ 6,035.53	$ 6,216.60	$ 6,403.10	$ 6,595.18	$ 6,793.04	$ 6,996.83	$ 7,206.74
				$ 2 856.79	$ 2 942.49	$ 3 030.77	$ 3 121.70	$ 3 215.35	$ 3 311.80	$ 3 411.16	$ 3 513.49	$ 3 618.90	$ 3 727.46

				$ 1,401.59	$ 1,443.63	$ 1,486.95	$ 1,531.55	$ 1,577.49	$ 1,624.82	$ 1,673.56	$ 1,723.77	$ 1,775.48	$ 1,828.74
				$ 451.53	$ 465.08	$ 479.03	$ 493.40	$ 508.20	$ 523.45	$ 539.15	$ 555.33	$ 571.99	$ 589.15
				$ 4,275.18	$ 4,403.43	$ 4,535.53	$ 4,671.61	$ 4,811.75	$ 4,956.10	$ 5,104.79	$ 5,257.93	$ 5,415.67	$ 5,578.13
				$ 2,304.84	$ 2,373.99	$ 2,445.21	$ 2,518.56	$ 2,594.11	$ 2,671.93	$ 2,752.10	$ 2,834.67	$ 2,919.70	$ 3,007.30
				$ 18,144.81	$ 18,689.16	$ 19,249.84	$ 19,827.33	$ 20,422.15	$ 21,034.81	$ 21,665.85	$ 22,315.84	$ 22,985.31	$ 23,674.87
				$ 10 617.01	$ 10 935.52	$ 11 263.58	$ 11 601.49	$ 11 949.54	$ 12 308.03	$ 12 677.27	$ 13 057.58	$ 13 449.31	$ 13 852.79
				$ 8 352.61	$ 8 603.19	$ 8 861.29	$ 9 127.13	$ 9 400.95	$ 9 682.96	$ 9 973.46	$ 10 272.67	$ 10 580.84	$ 10 898.27
				$ 5,011.96	$ 5,162.31	$ 5,317.18	$ 5,476.70	$ 5,641.00	$ 5,810.22	$ 5,984.53	$ 6,164.08	$ 6,348.99	$ 6,539.47
				$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
				$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
				$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
				$ 197.81	$ 203.51	$ 209.31	$ 215.28	$ 221.43	$ 217.49	$ 224.11	$ 230.83	$ 237.75	$ 244.88
				$ 3 296.93	$ 3 391.98	$ 3 488.63	$ 3 588.17	$ 3 690.71	$ 3 625.07	$ 3 735.27	$ 3 847.31	$ 3 962.71	$ 4 081.57
				$ 435.93	$ 449.02	$ 462.48	$ 476.36	$ 490.65	$ 505.38	$ 520.54	$ 536.15	$ 552.23	$ 568.80
				$ 87.84	$ 90.47	$ 93.18	$ 95.98	$ 98.86	$ 101.82	$ 104.88	$ 108.03	$ 111.27	$ 114.61
				$ 11,513.82	$ 11,859.24	$ 12,215.01	$ 12,581.46	$ 12,958.90	$ 13,347.68	$ 13,748.11	$ 14,160.54	$ 14,585.36	$ 15,022.92
				$ 1,016.77	$ 1,047.28	$ 1,078.70	$ 1,111.06	$ 1,144.39	$ 1,178.72	$ 1,214.08	$ 1,250.51	$ 1,288.02	$ 1,326.67
				$ 1,091.57	$ 1,124.32	$ 1,158.05	$ 1,192.79	$ 1,228.58	$ 1,265.43	$ 1,303.40	$ 1,342.49	$ 1,382.77	$ 1,424.25
				$ 1 365.32	$ 1 406.27	$ 1 448.46	$ 1 491.92	$ 1 536.68	$ 1 582.77	$ 1 630.26	$ 1 679.16	$ 1 729.54	$ 1 781.43
				$ 601.51	$ 619.55	$ 638.14	$ 657.29	$ 677.00	$ 697.31	$ 718.23	$ 739.78	$ 761.97	$ 784.83
				$ 300.76	$ 309.79	$ 319.07	$ 328.65	$ 338.51	$ 348.66	$ 359.12	$ 369.90	$ 380.99	$ 392.42
				$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
				$ 5 341.99	$ 5 496.02	$ 5 652.61	$ 5 813.90	$ 5 980.03	$ 5 873.68	$ 6 052.24	$ 6 233.77	$ 6 420.75	$ 6 613.34
				$ 488.41	$ 502.49	$ 516.81	$ 531.56	$ 546.75	$ 537.02	$ 553.35	$ 569.94	$ 587.04	$ 604.65
				$ 345.96	$ 355.93	$ 366.07	$ 376.52	$ 387.28	$ 380.39	$ 391.95	$ 403.71	$ 415.82	$ 428.29
				$ 0.99	$ 1.02	$ 1.05	$ 1.08	$ 1.11	$ 1.09	$ 1.12	$ 1.16	$ 1.19	$ 1.23
				$ 85.85	$ 88.33	$ 90.85	$ 93.44	$ 96.11	$ 94.40	$ 97.27	$ 100.19	$ 103.19	$ 106.29
				$ 76.31	$ 78.51	$ 80.75	$ 83.06	$ 85.43	$ 83.91	$ 86.46	$ 89.05	$ 91.73	$ 94.48
				$ 105.68	$ 108.73	$ 111.82	$ 115.02	$ 118.30	$ 116.20	$ 119.73	$ 123.32	$ 127.02	$ 130.83
				$ 12,839.27	$ 13,224.45	$ 13,621.18	$ 14,029.82	$ 14,450.71	$ 14,884.24	$ 15,330.76	$ 15,790.69	$ 16,264.40	$ 16,752.34
				$ 8,127.40	$ 8,371.23	$ 8,622.37	$ 8,881.04	$ 9,147.47	$ 9,421.89	$ 9,704.55	$ 9,995.69	$ 10,295.56	$ 10,604.42
				$ 8 127.40	$ 8 371.23	$ 8 622.37	$ 8 881.04	$ 9 147.47	$ 9 421.89	$ 9 704.55	$ 9 995.69	$ 10 295.56	$ 10 604.42
				$ 8 127.40	$ 8 371.23	$ 8 622.37	$ 8 881.04	$ 9 147.47	$ 9 421.89	$ 9 704.55	$ 9 995.69	$ 10 295.56	$ 10 604.42
				$ 8,127.40	$ 8,371.23	$ 8,622.37	$ 8,881.04	$ 9,147.47	$ 9,421.89	$ 9,704.55	$ 9,995.69	$ 10,295.56	$ 10,604.42
				$ 11,135.74	$ 11,469.80	$ 11,813.90	$ 12,168.32	$ 12,533.37	$ 12,909.37	$ 13,296.65	$ 13,695.54	$ 14,106.41	$ 14,529.61
				$ 8,127.40	$ 8,371.23	$ 8,622.37	$ 8,881.04	$ 9,147.47	$ 9,421.89	$ 9,704.55	$ 9,995.69	$ 10,295.56	$ 10,604.42
				$ 8,763.17	$ 9,026.06	$ 9,296.84	$ 9,575.74	$ 9,863.02	$ 10,158.91	$ 10,463.67	$ 10,777.59	$ 11,100.91	$ 11,433.94
				$ 296.25	$ 304.79	$ 313.47	$ 322.42	$ 331.63	$ 325.73	$ 335.63	$ 345.70	$ 356.07	$ 366.75
				$ 1,076.55	$ 1,107.59	$ 1,139.14	$ 1,171.65	$ 1,205.13	$ 1,183.69	$ 1,219.68	$ 1,256.26	$ 1,293.94	$ 1,332.76
				$ 2,780.73	$ 2,860.91	$ 2,942.42	$ 3,026.38	$ 3,112.86	$ 3,057.50	$ 3,150.44	$ 3,244.94	$ 3,342.27	$ 3,442.52
				$ 90.10	$ 92.70	$ 95.34	$ 98.06	$ 100.86	$ 99.07	$ 102.08	$ 105.14	$ 108.29	$ 111.54
				$ 4.96	$ 5.11	$ 5.25	$ 5.40	$ 5.56	$ 5.46	$ 5.62	$ 5.79	$ 5.97	$ 6.14
				$ 149.21	$ 153.51	$ 157.89	$ 162.39	$ 167.03	$ 164.06	$ 169.05	$ 174.12	$ 179.34	$ 184.72
				$ 37.36	$ 38.43	$ 39.53	$ 40.66	$ 41.82	$ 41.07	$ 42.32	$ 43.59	$ 44.90	$ 46.25
				$ 34 342.18	$ 5 723.73	$ 5 723.73	$ 5 723.73	$ 5 723.73	$ 5 723.73	$ 5 723.73	$ 5 723.73	$ 5 723.73	$ 5 723.73
				$ 892.57	$ 918.31	$ 944.47	$ 971.42	$ 999.18	$ 981.41	$ 1,011.24	$ 1,041.57	$ 1,072.82	$ 1,105.00
				$ 111.11	$ 114.32	$ 117.57	$ 120.93	$ 124.38	$ 122.17	$ 125.89	$ 129.66	$ 133.55	$ 137.56
				$ 892.57	$ 918.31	$ 944.47	$ 971.42	$ 999.18	$ 981.41	$ 1,011.24	$ 1,041.57	$ 1,072.82	$ 1,105.00
				$ 55.56	$ 57.16	$ 58.79	$ 60.46	$ 62.19	$ 61.09	$ 62.94	$ 64.83	$ 66.78	$ 68.78
				$ 111.11	$ 114.32	$ 117.57	$ 120.93	$ 124.38	$ 122.17	$ 125.89	$ 129.66	$ 133.55	$ 137.56
				$ 111.11	$ 114.32	$ 117.57	$ 120.93	$ 124.38	$ 122.17	$ 125.89	$ 129.66	$ 133.55	$ 137.56
				$ 92.17	$ 97.52	$ 100.30	$ 103.16	$ 106.11	$ 104.24	$ 107.40	$ 110.63	$ 113.94	$ 117.36
				$ 0.66	$ 0.67	$ 0.69	$ 0.71	$ 0.73	$ 0.72	$ 0.74	$ 0.76	$ 0.79	$ 0.81

Termination for Convenience Fees

	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
(A) Termination Fee Base	$30,000,000 00	$75,000,000 00	$30,000,000 00							
(B) Value of Services Performed*	(Services Performed)	(Services Performed)	(Services Performed)							
(C) Actual Termination for Convenience Fees	C =A-B	C =A-B	C =A-B							

No Termination for Convenience Fees are available after Year 3.

Termination for Conveinence Fees are not cumulative.

(*) The value of all Services performed by the Contractor consistent with the terms of the Contract prior to the effective date of termination

List Of Items For Offeror

Clarification	*Text*
1	*Section 3.2.2.5 (Security Management) of the RFP states "The Offeror must comply with Commonwealth IT policies and directives as well as federal and Commonwealth laws, regulations and policies, including but not limited to the Criminal History Record Information Act (CHRIA), Health Insurance Portability and Accountability Act (HIPPA), Criminal Justice Information Services (CJIS) regulations, The United States Social Security Administration (SSA) regulations, Internal Revenue Services (IRS) Publications, Commonwealth Information Technology Bulletins (ITBs) and the Payment Card Industry (PCI) standards."* *Please provide a detailed explanation on how Unisys Corporation ("Unisys") will satisfy each of the security requirements listed below in its base solution. Each requirement in the list must be addressed separately:* • *Criminal History Record Information Act (CHRIA)* • *Health Insurance Portability and Accountability Act (HIPPA)* • *Criminal Justice Information Services (CJIS) regulations* • *The United States Social Security Administration (SSA) regulations* • *Internal Revenue Services (IRS) Publications* • *Commonwealth Information Technology Bulletins (ITBs)* • *Payment Card Industry (PCI) standards*

Unisys Response:

The Unisys Team understands the importance of information security and regulations, standards, and policies mandated through the Commonwealth Information Technology Bulletins (ITBs) and Commonwealth and Federal agencies. The Unisys Team has envisioned a six-step approach to establish a risk aware data center that addresses several regulatory requirements including:

- Commonwealth Information Technology Bulletins (ITBs)
- Health Insurance Portability and Accountability Act (HIPAA)
- Criminal Justice Information Services (CJIS) regulations
- Criminal History Record Information Act (CHRIA)
- The United States Social Security Administration (SSA) regulations
- Internal Revenue Services (IRS) Publication 1075
- Payment Card Industry (PCI) Data Security Standards (DSS)

As part of our solution, the table below identifies the detailed technical controls that will be implemented, their applicability to each regulation and how the Unisys Team's proposed solution meets each control.

CONTROL	PA ITB	HIPPA-HITECH	IRS 1075 (FTI)	SSA	CJIS	PCI	CHRIA
Common Controls							
Classify as a Business Associate		X					
Add IRS 1075 Exhibit 7 to Contract			X				
Add CJIS Security Addendum to Contract					X		
CHRIA Authorization to Administer Exception letter							X
Notification of Data Loss	X	X	X	X	X	X	X
Provide Background Checks based up ITB-SEC009	X	X	X	X	X	X	X
Use US only Support Personnel	X	X	X	X	X	X	X
Risk Management							
Establish Data Center Security Management Plan	X	X	X	X	X	X	X
Perform periodic review and update of Security Management Plan	X	X	X	X	X	X	X
Perform annual risk assessment of data center operations	X	X	X	X	X	X	X
Awareness and Training							
Provide Security Awareness Training meeting Regulatory requirements	X	X	X	X	X	X	X
Support Security Control Reviews	X	X	X	X	X	X	X
Separation of Data							
Facilitate separation of FTI data from non-FTI data			X				
Facilitate separation of CJIS data from non-CJIS data					X		
Label Physical Media containing Regulated Data	X	X	X	X	X	X	X
Provide Multiple Security Zones (e.g. Web / Application / Database /Test /Dev)	X	X	X	X	X	X	X

CONTROL	PA ITB	HIPPA-HITECH	IRS 1075 (FTI)	SSA	CJIS	PCI	CHRIA
Facility							
Slab to Slab Secure Room	X	X	X	X	X	X	X
Locked Secure Room (Physical or Electronic Locks)	X	X	X	X	X	X	X
Cages Available upon request for addition separation	X	X	X	X	X	X	X
Security Cabinet available upon request for addition separation	X	X	X	X	X	X	X
Multi-factor access to building	X	X	X	X	X	X	X
Multi-factor access to Computer Room	X	X	X	X	X	X	X
Multiple Access Control Points to access Computer Room	X	X	X	X	X	X	X
Log and Monitoring of physical	X	X	X	X	X	X	X
Visitor Access Logs	X	X	X	X	X	X	X
On-Site Security Guards	X	X	X	X	X	X	X
CCTV Monitoring	X	X	X	X	X	X	X
Fire Suppression	X	X	X	X	X	X	X
Water Detection	X	X	X	X	X	X	X
Fire Alarms	X	X	X	X	X	X	X
Backup Power	X	X	X	X	X	X	X
Technology							
System and Communication Protection							
Network Infrastructure Firewall	X	X	X	X	X	X	X
Data Loss Prevention Monitoring	X	X	X	X	X	X	X
Web Application Firewall	X	X	X	X	X	X	X
Database Firewall	X	X	X	X	X	X	X
Data Discovery Solution	X	X	X	X	X	X	X
Intrusion Prevention Systems	X	X	X	X	X	X	X
File Integrity Monitoring Systems	X	X	X	X	X	X	X
Support Time Synchronization	X	X	X	X	X	X	X
Cryptographic Services							
Encryption uses FIPS 140-2 Validated modules	X	X	X	X	X	X	X

CONTROL	PA ITB	HIPPA-HITECH	IRS 1075 (FTI)	SSA	CJIS	PCI	CHRIA
Use AES Encryption	X	X	X	X	X	X	X
Encryption - Data at Rest	X	X	X	X	X	X	X
Encryption - Data In Motion (Network Site to Site)	X	X	X	X	X	X	X
Encryption - Data In Motion (Server to Server)	X	X	X	X	X	X	X
Encryption - Remote Access VPN	X	X	X	X	X	X	X
Facilitate PKI Cryptography Key Management	X	X	X	X	X	X	X
Malicious Code Protection							
Implement Antivirus Solution	X	X	X	X	X	X	X
Implement Malware Prevention	X	X	X	X	X	X	X
Provide Cyber Threat Intelligence Diagnostics	X	X	X	X	X	X	X
Perform External Quarterly Vulnerability Scans	X	X	X	X	X	X	X
Perform Internal Quarterly Vulnerability Scans	X	X	X	X	X	X	X
Perform Penetration Tests	X	X	X	X	X	X	X
Implement Patch Management Automation	X	X	X	X	X	X	X
Audit Log Management							
Automatically Log auditable events	X	X	X	X	X	X	X
Protect and Retain Audit Logs	X	X	X	X	X	X	X
Security Information and Event Management (SIEM)	X	X	X	X	X	X	X
Perform Periodic Review of Audit Logs	X	X	X	X	X	X	X
Integrate Audit Log event notification with ITSM	X	X	X	X	X	X	X
User Access Control Technologies	X	X	X	X	X	X	X
Privileged User Management	X	X	X	X	X	X	X
Role Based Access Control	X	X	X	X	X	X	X
Automated Password Updates through Privileged User Management	X	X	X	X	X	X	X

CONTROL	PA ITB	HIPPA-HITECH	IRS 1075 (FTI)	SSA	CJIS	PCI	CHRIA
User ID and Password Complexity	X	X	X	X	X	X	X
Annual User Authorization Validation	X	X	X	X	X	X	X
User Privilege Recertification	X	X	X	X	X	X	X
User Provisioning and Deprovisioning	X	X	X	X	X	X	X
Provide Session Lock Out Configurations	X	X	X	X	X	X	X
Support Multi-Factor Authentication	X	X	X	X	X	X	X
Support Multi- Factor Authentication for Remote Access	X	X	X	X	X	X	X
Provide System Use Notification Message	X	X	X	X	X	X	X
Provide notification of authorized user changes	X	X	X	X	X	X	X
Configuration Management							
Establish Change Management Board to review all changes	X	X	X	X	X	X	X
Automate notification of changes through ITSM	X	X	X	X	X	X	X
Implement Configuration Management Database	X	X	X	X	X	X	X
Track config changes through ITSM and CMDB	X	X	X	X	X	X	X
Automate configuration changes with Run-books	X	X	X	X	X	X	X
Change Activity Authorization is logged within ITSM	X	X	X	X	X	X	X
CMDB is updated with all configuration changes	X	X	X	X	X	X	X
Maintain and document baseline configurations	X	X	X	X	X	X	X
Implement Baseline configuration deployment automation	X	X	X	X	X	X	X
Implement Patch Management Automation	X	X	X	X	X	X	X
Implement monthly health checks automation for baseline configuration validation	X	X	X	X	X	X	X
Maintain list of authorized maintenance personnel	X	X	X	X	X	X	X

CONTROL	PA ITB	HIPPA-HITECH	IRS 1075 (FTI)	SSA	CJIS	PCI	CHRIA
Contingency Plan							
Provide Disaster Recovery Plan for applicable IT Systems	X	X	X	X	X	X	X
Continuity of Operations Plan for Service Management	X	X	X	X	X	X	X
Provide Disk Based Backup Services	X	X	X	X	X	X	X
Provide Tape Based Backup Services	X	X	X	X	X	X	X
Provide Tape Encryption	X	X	X	X	X	X	X
Label Physical Media containing Regulated Data	X	X	X	X	X	X	X
Provide Secondary Operations Center	X	X	X	X	X	X	X
Provide Tests for Disaster Recovery Plans	X	X	X	X	X	X	X
Provide Tests for Continuity of Operations Plans	X	X	X	X	X	X	X
Provide alternate processing site	X	X	X	X	X	X	X
Provide tests for Backup and Recovery plans	X	X	X	X	X	X	X
Incident Response							
Provide process to support Incident response	X	X	X	X	X	X	X
Use ITIL V3 based and ISO20000 certified processes	X	X	X	X	X	X	X
Use Integrated Service Management and ITSM to manage incidents	X	X	X	X	X	X	X
Provide notification to Commonwealth for Incidents	X	X	X	X	X	X	X

We have illustrated our six-step approach to establish a regulatory compliant data center in the figure below. Our approach, developed by our teaming partner Deloitte through their extensive experience in helping organizations achieve regulatory compliance, enables the use of regulations as a driving factor to proactively assess, identify and mitigate gaps. Throughout this process, the Unisys Team will collaborate with the Commonwealth stakeholders to review gaps identified, help prioritize mitigation steps, and monitor remediation steps. Note that while collaboration with Commonwealth agencies is essential throughout the data center transition process, it is particularly required here as some of the gaps with the documented regulatory requirements may be with applications not in Unisys control.

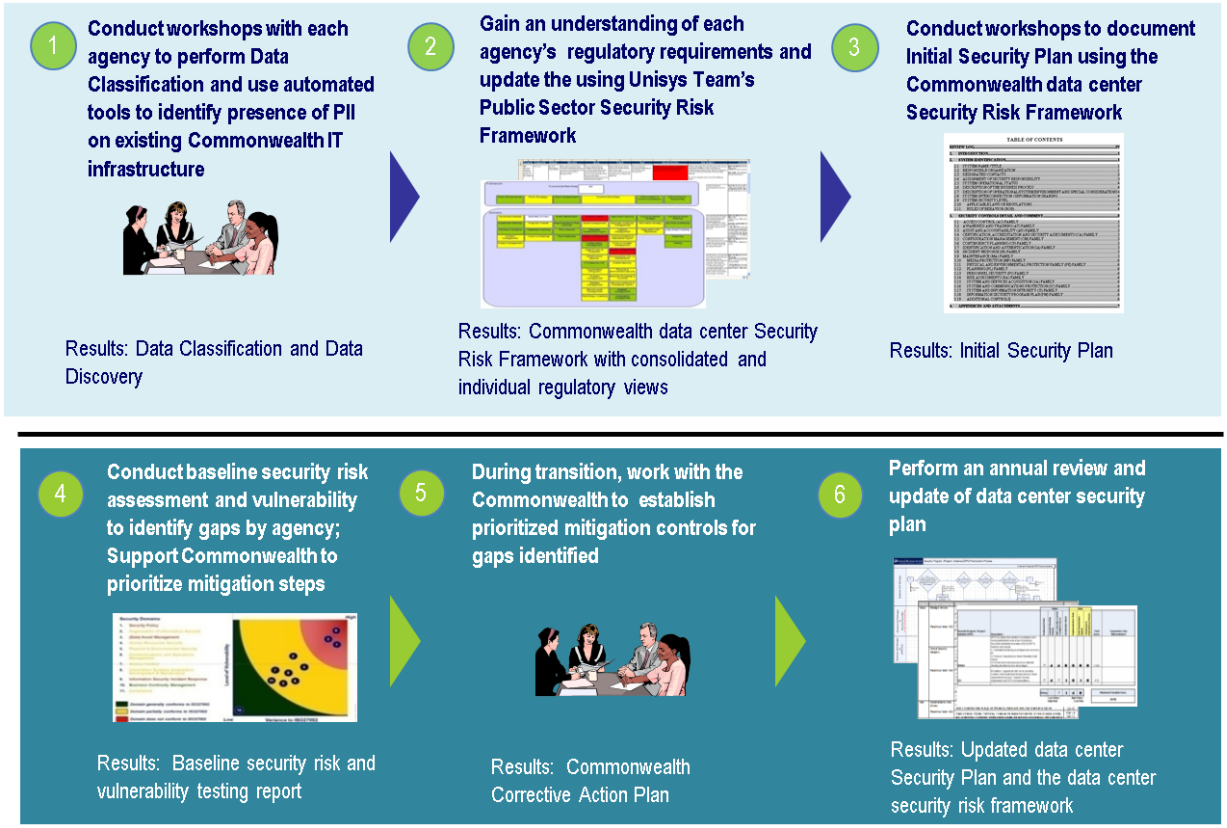


Figure 1 – The Unisys Team collaborates with the Commonwealth, using our six-step approach, to establish a risk aware data center.

Deloitte's public sector security risk framework – The Unisys Team uses its teaming partner, Deloitte's demonstrated public sector security risk framework to identify, assess and document the appropriate data protection controls to secure Commonwealth data. Our approach to use an integrated security risk framework is an innovative method to "assess once, comply and report many regulations".

Our teaming partner, Deloitte's public sector security risk framework contains over 4,000 individual regulatory requirements mapped to over 290 unique integrated requirements initially driven by NIST SP800-53 rev 3 (moderate level). This detailed Microsoft Excel-based framework contains the regulatory requirements and their integrated controls. This technology agnostic approach to manage risks is still a pioneer in state governments.

Our related experience – Our teaming partner, Deloitte has established the security risk framework at over 10 states to help the states integrate and assess security regulatory requirements as part of systems development efforts and conduct integrated enterprise level security assessments. Selected experience includes:

- Commonwealth of Pennsylvania – Department of Public Welfare (DPW)
- State of Indiana
- State of Delaware
- State of Washington
-

For example, the Commonwealth of Pennsylvania DPW's security risk framework rationalizes more than 4,000 individual regulatory requirements into 350 unique integrated requirements, including:

- Commonwealth security ITBs
- DPW security policies and standards
- IRS 1075
- SSA
- HIPAA
- Family Educational Rights Protection Act (FEPRA)
- NIST SP800-53 (Note that the existing framework leverages rev 3, but is in the process of being updated for rev 4 which was recently released. That update will be completed for use with the new Commonwealth data centers, so the rest of this answer refers to rev 4)
- ISO 27001:2005

Unique and *Distinguishing* Factors

Benefits from the Unisys Teaming partner, Deloitte's public sector security risk framework:

- Contains authoritative sources from more than 30 regulations & standards
- Provides a core set of risk & compliance management solutions
- Allows for consistent comparison, prioritization & aggregation of risk and compliance across the Commonwealth's agencies
- Allows the team to "hit the ground running"
- Provides pre-configured reports for key individual regulations.

Additionally, Deloitte's efforts at the state of Delaware included integration of CJIS and PCI DSS v2. Our teaming partner Deloitte has also established security risk frameworks at several of our commercial clients including very large Banking & Securities, Life Sciences & Health Care, Retail and Oil & Gas firms. Although the current version of the framework does not include the Pennsylvania-specific CHRIA requirements, Deloitte will include them as part of the initial security plan activities.

Reporting for regulatory requirements – The data center's current security posture will be documented as part of the initial security plan and within the data center's security risk framework. When a Commonwealth agency requires a report on the data center's current measures to meet the agency's corresponding regulatory requirements, the data center security manager will uses the pre-existing reporting capability of the security framework to extract reports specific to individual regulations such as IRS 1075, SSA, CJIS and PCI DSS.

We use our risk framework driven approach to address the Commonwealth selected key regulations identified in the questions, through our six-step process. The table below illustrates the key components of our approach to establish a Commonwealth data center that meets the Commonwealth identified security regulations and policies/standards.

Regulation/ Policy/Standard	Step1: Used to classify Commonwealth data	Step 2: Integrated with the data center risk framework	Step 3: Considered in data center initial security plan	Step 4: Used to perform baseline risk & vulnerability assessment	Step 5:Used to develop and monitor corrective action plan	Step 6: Used to perform an annual security risk assessment & security plan update	Provides ability to generate individual regulatory reports
Commonwealth ITBs	✓	✓	✓	✓	✓	✓	✓
IRS 1075	✓	✓	✓	✓	✓	✓	✓
CJIS	✓	✓	✓	✓	✓	✓	✓
PA CHRIA	✓	✓	✓	✓	✓	✓	✓
SSA	✓	✓	✓	✓	✓	✓	✓
HIPAA	✓	✓	✓	✓	✓	✓	✓
PCI DSS	✓	✓	✓	✓	✓	✓	✓

Step 1: Data identification process and sensitivity classification

As part of the initial security plan, the Unisys Team will work with the Commonwealth stakeholders to establish a data classification standard data sensitivity levels and establish a data classification based on applicable regulations and leading practices such as NIST SP800-122 (Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)).

Perform Commonwealth data classification – The Unisys Team will conduct workshops with the Commonwealth stakeholders to define a data classification standard for the Commonwealth Personally Identifiable Information (PII) based on data sensitivity levels. For example, some of the categories include:

- Special handling PII (that contains SSN, driver license number, FEIN, and Medicare ID)
- Protected Health Information
- Federal Taxpayer Information (FTI)
- US Social Security Administration (SSA)
- Criminal Justice Information (CJI), including Pennsylvania's Criminal History Records Information Act (CHRIA)
- Sensitive PII (such as racial/ethnic origin, religious/philosophical beliefs, Trade-union membership and criminal convictions)

From our experience of working with the Commonwealth and several public sector clients, the Unisys Team understands the Commonwealth's regulatory landscape. In the table below, we illustrate our understanding of a sample of Federal and Commonwealth regulations that impact the data used by the Commonwealth data center IT infrastructure.

Type of Data	Regulatory impact
Personal Health Information (PHI) **Electronic Health Records (EHR)**	• Health information portability and accountability act (HIPAA) • Federal HHS CMS regulations and information security – Minimum Acceptable Risk Safeguards (MARS) • 45 CFR • Health Information Technology for Economic and Clinical Health Act (HITECH)
Child welfare data	• Federal HHS and PA Adoption and Foster Care Analysis and Reporting System (AFCARS) • Family Educational Rights and Privacy Act (FERPA) • Child Abuse Prevention and Treatment Act (CAPTA) • Child Abuse Prevention and Enforcement Act of 2000 • Social Security Act • Adam Walsh Child Protection and Safety Act of 2006 • Fair Access Foster Care Act of 2005 • Keeping Children and Families Safe Act of 2003 • Children's Health Act of 2000
HHS and Health data	• Family Educational Rights and Privacy Act (FERPA) • Children Online Privacy Protection Act (COPPA) • PA Early Intervention Services Systems Act (Act 212) • Individuals with Disabilities Education Act (IDEA) • Licensure or Approval of Facilities and Agencies (55 Pa. code chapter 20) • Mental Health and Mental Retardation Act of 1966 • PA special education services and programs (Chapter 14 of 20 Pa.B. 3339)
Educational records	• Family Educational Rights and Privacy Act (FERPA)
Criminal History Records	• PA Criminal History Records Information Act (CHRIA) • Criminal Justice Information Services (CJIS)
Federal	• Internal Revenue Service (IRS) publication 1075

Type of Data	Regulatory impact
Taxpayer Information	
Social Security Administration	• United States Social Security Administration (SSA)
Financial and Credit Card Information	• Payment Card Information (PCI) Data Security Standards (DSS) • Payment Application (PA) Data Security Standards (DSS)
Special handling data such as SSNs, driver's license and FEIN	• Commonwealth Information Technology Bulletins (ITBs) • Federal Privacy Act of 1974 • Federal Driver's Privacy Protection Act • Pennsylvania Breach of Personal Information Notification Act - SB 712 • Pennsylvania SSN Obfuscation Law – SB 601 • Pennsylvania House Resolution 351 (2005) • Americans with Disability Act (ADA)

Identify presence of PII within the Commonwealth IT infrastructure – In addition to the above illustrated data classification, the Unisys Team will conduct a one-time data discovery assessment. During development of the initial security plan, we perform a data discovery using the Symantec Data Loss Prevention (DLP) solution's data discovery tool. This assessment supports the Unisys Team to identify the presence of PII at rest within the current Commonwealth data center IT infrastructure.

The data collected will be documented as part of the IT asset inventory. This information will be used during the data center transition to establish appropriate data protection controls based on the data sensitivity and regulatory requirements (using the Commonwealth data center security risk framework).

DID YOU KNOW

Pennsylvania's DPW team was recognized with the Computerworld Honors Laureate in 2013 in the "Safety and Security" category.

DPW was recognized for developing the Information Security Risk Management System which is a big advancement in protecting citizen private information by proactively identifying security risks to reduce identity theft exposure. Our teaming partner, Deloitte was part of the project and assisted DPW in the implementation of the EMC Archer based security risk framework.

THE COMPUTERWORLD HONORS PROGRAM

Step 2: Gain an understanding of Commonwealth agency's individual regulatory requirements and define the data center security risk framework

From our experience of working with the Commonwealth and several public sector clients, the Unisys Team understands Commonwealth's regulatory landscape. We will conduct workshops with the Commonwealth agencies as part of the transition planning to identify the applicable regulations, standards and industry leading practices for the data managed by the data center. We will use this information to integrate each agency's individual regulatory requirements as part of the Commonwealth data center security risk framework and to develop the initial security plan (discussed in step 4). The figure below

illustrates a sample of the regulations, standards and industry practices that the Unisys Team uses to define the Commonwealth data center security framework.

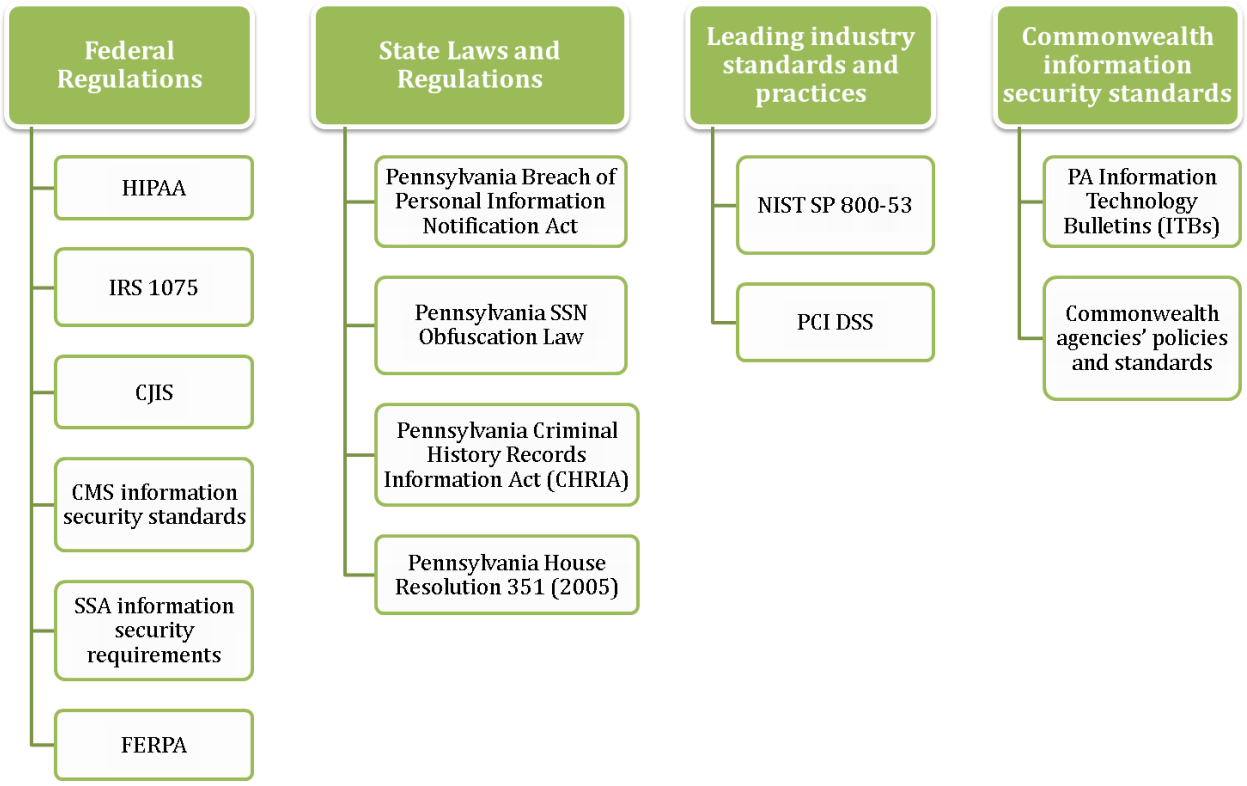


Figure 2 – Sample List of Regulations, Industry Standards and Leading Industry Practices Applicable to the Commonwealth

Establish the Commonwealth data center security risk framework

The Unisys Team establishes the Commonwealth data center security risk framework. This framework is a broad library of the applicable security and privacy requirements. These requirements are integrated from the relevant Commonwealth ITBs, industry standards, State and Federal regulations. As part of transition and during the ongoing operations, the Unisys Team uses the security risk framework to help document data protection controls that meets the relevant regulations and business requirements.

We bring a pre-configured security risk framework to "hit the ground running" – We use our teaming partner Deloitte's pre-configured and highly customizable public sector security risk framework to "hit the ground running" and reduce costs. This framework was developed based on more than 12 years of security and privacy experience within the Commonwealth and the public sector marketplace.

The public sector security risk framework contains over 4,000 individual regulatory requirements mapped to over 290 unique integrated requirements primarily driven by NIST SP800-53 rev 4 (moderate level). This detailed Microsoft Excel-based framework contains the regulatory requirements and their integrated controls. This technology agnostic approach to manage risks is still a pioneer in state governments. The existing Unisys Team's public sector security risk framework provides an integration of regulatory requirements from the following:

- Internal Revenue Services (IRS) publication 1075
- United States Social Security Administration (SSA)
- Health Information Portability and Accountability Act (HIPAA)
- Criminal Justice Information Services (CJIS)
- Payment Card Industry (PCI) Data Security Standard (DSS) v2.0
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 rev 4

The screenshot below illustrates the Unisys Team's public sector security risk framework showcasing a sample integration of the above described regulatory requirements.

Figure 3 – Sample Integration of Regulatory Requirements available in our pre-configured Public Sector Security Risk Framework.

As described in step 2, we will conduct workshops with the Commonwealth agencies to identify each agency's regulatory requirements such as Commonwealth ITBs, Commonwealth agency policy/standards and PA Criminal History Records Information Act (CHRIA). The Unisys Team will extend the Unisys Team's public sector security risk framework to integrate additional regulations to establish the Commonwealth data center security risk framework.

Once developed, Unisys Team estimates that the data center's security risk framework will contain over 4,000 individual regulatory requirements mapped to over 300 integrated/baseline controls, primarily driven by NIST SP800-53 rev 4 as the primary baseline control. As necessary, we will extend the baseline controls with additional leading industry standards to accommodate selected regulatory requirements that may not integrate with NIST SP800-53. The figure below illustrates our demonstrated approach to extend our public sector security risk framework with additional Commonwealth data center regulatory and policy requirements.

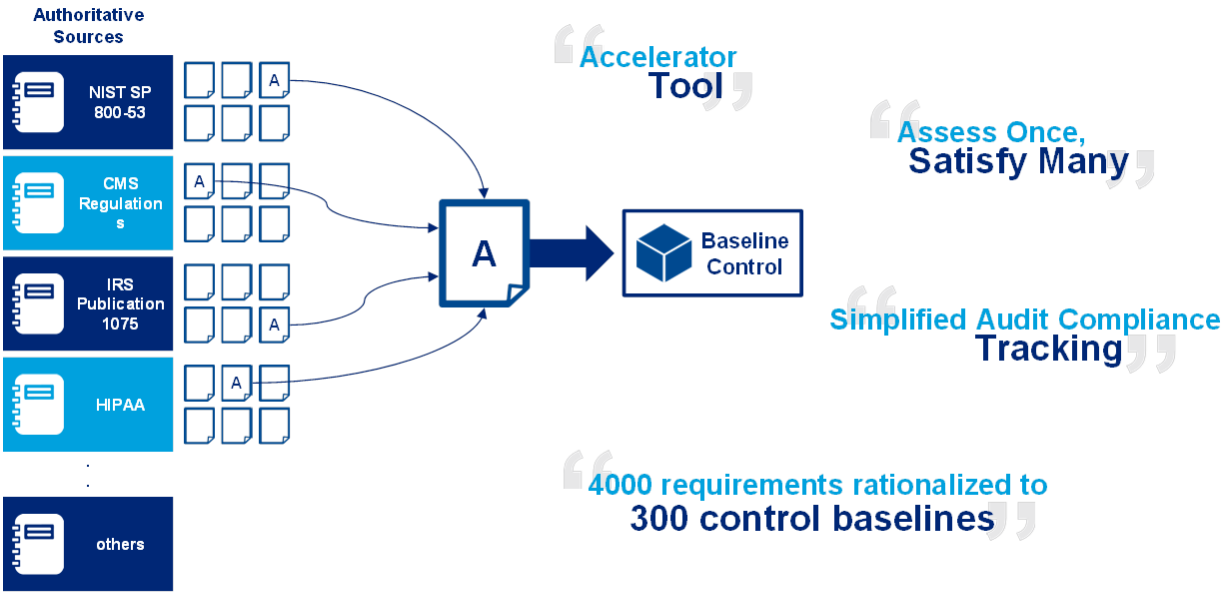


Figure 4 – The Unisys Team's approach to integrate data protection requirements using the Commonwealth data center security risk framework.

The Unisys Team uses this security risk framework to identify current state and document the initial security plan (described in Step 3). In addition, we use the security risk framework to perform the baseline security risk assessment (described in Step 4).

As part of ongoing data center transition and maintenance, we use the established security risk framework to identify relevant data protection requirements to help implement appropriate controls to protect Commonwealth data.

Step 3: Document Initial Security Plan (security management plan) and support Commonwealth's need to develop reports based on regulations

We will establish the Commonwealth data center security plan using guidelines provided by leading industry standards: NIST SP800-18 (RFP requirement specified by Q50 of round 1 part 2) and control guidelines established by NIST SP800-53 rev 4. To develop this plan, the Unisys Team uses

the Centers for Medicare and Medicaid Services (CMS) Systems Security Plan (SSP) template to define and maintain the appropriate security controls. The figure below illustrates the planned Table of Contents of the Commonwealth data center Initial Security Plan.

TABLE OF CONTENTS

REVIEW LOG ..... **IV**
1. INTRODUCTION **1**
2. SYSTEM IDENTIFICATION **1**
2.1 SYSTEM NAME / TITLE 1
2.2 RESPONSIBLE ORGANIZATION 1
2.3 DESIGNATED CONTACTS 2
2.4 ASSIGNMENT OF SECURITY RESPONSIBILITY 3
2.5 SYSTEM OPERATIONAL STATUS 4
2.6 DESCRIPTION OF THE BUSINESS PROCESS 4
2.7 DESCRIPTION OF OPERATIONAL/SYSTEM ENVIRONMENT AND SPECIAL CONSIDERATIONS 4
2.8 SYSTEM INTERCONNECTION / INFORMATION SHARING 4
2.9 SYSTEM SECURITY LEVEL 4
2.10 APPLICABLE LAWS OR REGULATIONS 4
2.11 RULES OF BEHAVIOR (ROB) 4
3. SECURITY CONTROLS DETAIL AND COMMENT **5**
3.1 ACCESS CONTROL (AC) FAMILY 5
3.2 AWARENESS AND TRAINING (AT) FAMILY 5
3.3 AUDIT AND ACCOUNTABILITY (AU) FAMILY 5
3.4 CERTIFICATION, ACCREDITATION AND SECURITY ASSESSMENTS (CA) FAMILY 5
3.5 CONFIGURATION MANAGEMENT (CM) FAMILY 5
3.6 CONTINGENCY PLANNING (CP) FAMILY 5
3.7 IDENTIFICATION AND AUTHENTICATION (IA) FAMILY 5
3.8 INCIDENT RESPONSE (IR) FAMILY 5
3.9 MAINTENANCE (MA) FAMILY 5
3.10 MEDIA PROTECTION (MP) FAMILY 6
3.11 PHYSICAL AND ENVIRONMENTAL PROTECTION FAMILY (PE) FAMILY 6
3.12 PLANNING (PL) FAMILY 6
3.13 PERSONNEL SECURITY (PS) FAMILY 6
3.14 RISK ASSESSMENTS (RA) FAMILY 6
3.15 SYSTEM AND SERVICES ACQUISITION (SA) FAMILY 6
3.16 SYSTEM AND COMMUNICATIONS PROTECTION (SC) FAMILY 6
3.17 SYSTEM AND INFORMATION INTEGRITY (SI) FAMILY 6
3.18 INFORMATION SECUIRTY PROGRAM PLAN (PM) FAMILY 6
3.19 ADDITIONAL CONTROLS 6
4. APPENDICES AND ATTACHMENTS **7**

Figure 5 – Sample Commonwealth data center Initial Security Plan – Proposed Table of Contents.

Step 4: Conduct baseline security risk and vulnerability assessment

The Unisys Team performs the baseline security risk and vulnerability assessment to identify gaps within the current Commonwealth data center infrastructure. The Unisys Team will work with the Commonwealth to establish a corrective action plan and prioritize mitigation efforts. We have illustrated our steps to perform the baseline security risk and vulnerability assessment in the table below.

Steps	Activities
Scope and Plan	• Document project requirements, scope and objectives • Identify Commonwealth's point of Contact ("Commonwealth Trusted Agent"). • Identify and document the time frame for conducting baseline security risk and vulnerability assessment.
Conduct Vulnerability Assessment	• Identify the Commonwealth's target IT and application infrastructure using passive scanning (from public resources such as Search Engines) • Work with the Commonwealth's stakeholders to understand the architecture, business logic/functionality, external dependencies, user roles and privileges within the target IT infrastructure and application • Identify, using passive scanning techniques, the technology and infrastructure dependencies • Perform active reconnaissance and identify network protocols present on the target infrastructure and web applications using network discovery (SolarWinds, Ping and Xprobe2) • Identify well-known open TCP ports and services present on the target infrastructure using port scanning tools (Nmap and SuperScan) • Perform infrastructure vulnerability tests using automated vulnerability scanning tools (Tenable Nessus and Qualys) • Perform database vulnerability testing, using automated database vulnerability scanners (AppDetective Pro) on a total of 50 standard database instances of Oracle, Microsoft SQL Server, MySQL and IBM DB2 • Conduct manual assimilation of the vulnerability scan results to identify false positives and manually verify the vulnerabilities identified by the vulnerability scanning tools.
Perform Risk Assessment and Security Architecture Review	Conduct a security risk assessment and IT architecture review of the existing seven datacenter IT infrastructure using NIST SP800-53 rev 4. The IT security architecture review includes specific components such as, • Trust Zone Architecture. • User Role Design. • Authentication and Authorization. • Data Protection. • Security Audit Logs and SIEM. • Data Privacy.
Perform Security Configuration Risk Review	Perform security configuration risk review using the IRS 1075 based Safeguard Computer Security Evaluation Matrix (SCSEM) on Commonwealth selected infrastructure handling Federal Taxpayer Information (FTI)
Reporting	• Develop and submit the baseline security risk and vulnerability assessment report along with an executive dashboard • Notify the Unisys Security Manager and "Commonwealth Trusted Agent" immediately upon identification/verification of a high severity security vulnerability.

Step 5: Establish Corrective Action Plan

The Unisys Team will work with the Commonwealth stakeholders to review the gaps identified by the baseline security risk and vulnerability assessment for establishing the corrective action plan, determining milestones and prioritizing remediation measures. The Unisys Team will work with the Commonwealth to update the corrective action plan based on milestones, results from the annual risk assessment and the quarterly vulnerability assessments. The figure below illustrates a sample corrective action plan process, based on CMS guidelines:

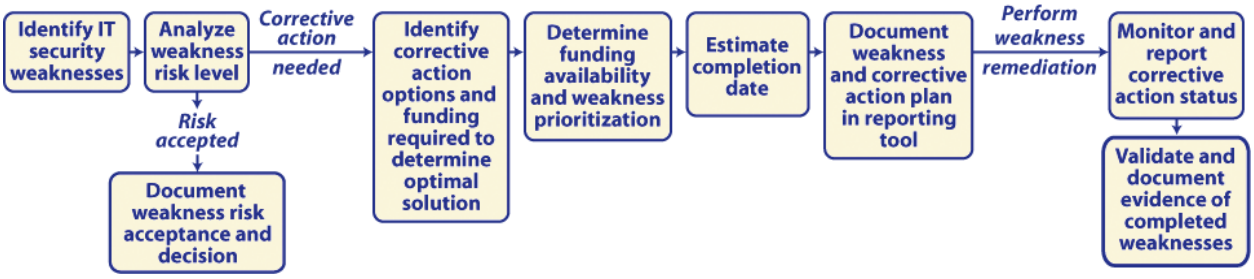


Figure 6 – The Unisys Team works with the Commonwealth Stakeholders to Establish a Corrective Action Plan.

The figure below illustrates a sample Corrective Action Plan template based on CMS guidelines.

Weakness Identifier	Security Control No.	Weakness Description	POC	Resources Required (One-time)	Scheduled Completion Date	Milestones With Completion Dates
State Defined-x	(i.e. AC-2(2))	[Selected Risk Description from final SAR]	[Name, Office/Org]	[man-hours or costs, indicate resource requirement (i.e. new, reallocated or current)]	[field cannot be changed once negotiated and agreed upon]	[include expected completion date with each milestone]
[System Acronym]-1 (ex.)	CP-3 (2)	BCP training has not been conducted.	John Doe - OCISO	(48 Total Man-hours) 40 man-hours - current	6/30/2013 (This should ONLY contain a date - no additional information)	(CP-3 (2)) Employ automated mechanisms to provide a more thorough and realistic training environment. (06/15/2013) (Ensure you put the completion date just as shown above for EACH milestone.)

Changes to Milestones Date	Completion Date	Weakness Status	Risk Level	Weakness Severity	Exception or Waiver	Comments
[When a corrective action is not completed as originally scheduled indicate new date.]	[MM/DD/YY (Completed means weakness has been fully resolved and tested)]	[Completed/Closed, Delayed or Ongoing/Open]	[High, Medium, Low]	[Significant Deficiency, Reportable Condition, Weakness]	[Provide reason, date and signatory for exception or waiver]	[Add additional detail for any previous entries]
N/A	6/29/2013	Completed/Closed	Medium	Weakness	N/A	

Figure 7 – The Unisys Team uses the CMS provided Plan of Action & Milestones (POA&M) template to create the Commonwealth data center Corrective Action Plan.

Step 6: Perform an annual review and update of the data center security management plan and security risk framework

The Unisys Team will perform an annual review and update of data center security plan and the security risk framework. The Unisys Team performs the following steps to update and submit the security management plan.

Steps	Activities
Scope and Plan	• Document scope and objectives • Identify Commonwealth's point of contact ("Trusted Agent"). • Identify and document the time frame to update the security plan. • Understand the business initiatives and additional security objectives that will be required for the year.

Update IT asset inventory	• Update datacenter asset inventory with new/updated/retired:
	  • Software
	  • Hardware and
	  • Information systems.
	• Review and update data classification standard
	• Perform one-time data discovery on datacenter's database instances and servers

Update Security Risk Framework	• Review and update the datacenter security risk framework with additional or updated regulations, policies and standards • Review and update integrated security requirements

Perform Security Risk Assessment	• Use the datacenter security risk framework to conduct a high level security risk assessment of the datacenter operational controls, that includes,
	  • Trust Zone Architecture.
	  • User Role Design, Authentication and Authorization.
	  • Data Protection.
	  • Security Audit Logs and SIEM.
	  • Data Privacy.
	• Work with the Commonwealth stakeholders to define and establish a corrective action plan for identified gaps.

Update and Submit the Security Management Plan	• Identify and document potential mitigation steps • Work with the Commonwealth to categorize gaps into initiatives/security roadmap

Our approach to maintain and address individual regulatory requirements specified by the Commonwealth

The Unisys Team uses the risk framework driven approach to address individual requirements specified by the following regulations:

- Internal Revenue Services (IRS) Publication 1075
- Payment Card Industry (PCI) Data Security Standards(DSS)

- The United States Social Security Administration (SSA) regulations
- Health Insurance Portability and Accountability Act (HIPAA)
- Criminal Justice Information Services (CJIS) regulations
- Criminal History Record Information Act (CHRIA)
- Commonwealth Information Technology Bulletins (ITBs)

Risk framework provides an integrated view of the regulatory requirements – The data center's security risk framework provides an integrated view of the regulatory requirements and provides a unified approach to document the data center's security plan. Each regulatory requirement within the data center risk framework is integrated with a baseline control that integrates similar requirements. This baseline control is based on NIST SP800-53 rev 4. Note that NIST SP800-53 is used as the base of several federal regulations such as CJIS and IRS 1075.

The data center risk framework provides pre-existing reports to generate individual regulatory compliance reports – The Unisys Team understands that the Commonwealth agencies have individual regulatory requirements and require reports corresponding to those regulatory requirements. The Unisys Team risk framework provides pre-configured reports for the following regulatory requirements:

- Internal Revenue Services (IRS) publication 1075
- Payment Card Industry (PCI) Data Security Standards (DSS)
- Health Information Portability and Accountability Act (HIPAA)
- Criminal Justice Information Services (CJIS)
- United States Social Security Administration (SSA)

In addition to the above pre-configured reports, the Unisys Team will configure the risk framework to generate reports for PA CHRIA and the Commonwealth ITBs.

Process employed to generate individual reports from the integrated risk framework – Within the security risk framework, each regulatory requirement is reviewed and mapped to a baseline/integrated control (based on NIST SP800-53). Each of the baseline controls are associated a framework control number. The data center's current security posture will be documented as part of the initial security management plan (Initial Security Plan) and within the data center's security risk framework. When a Commonwealth agency requires a report that describes the data center's current measures to meet the agency's corresponding regulatory requirements, the Unisys Team will use the pre-existing reporting capability of the framework to extract reports specific to those regulations.

As part of the initial security plan, we will extend the Unisys Team's public sector security risk framework to include additional regulatory requirements such as PA CHRIA and Commonwealth ITBs.

For example, if a Commonwealth agency requires a report that describes the data center's security controls to meet IRS 1075, the security manger generates a report that provides the following information

- Security Framework Identifier (ID)
- NIST SP800-53 Security (control) Domain
- Regulation
- Regulatory reference
- Regulatory Requirement Description
- Established control
- Last assessment date
- Weakness identified
- Mitigation status
- Plan of Action
- Milestone.

These readily available reports will help the Commonwealth agencies to analyze the regulatory posture and submit as part of periodic reports submitted to regulatory agencies.

Sample risk framework reports: The figures below illustrate samples of the risk framework's pre-configured reports. The first illustrates the report that will be used to describe the data center's security posture for IRS1075 regulation. The second illustrates the report that will be used to describe the data center's security posture for PCI DSS industry regulation.

Security Framework ID	Security Domain	Regulation	Regulatory Reference	Regulatory Requirement Description	Established Control	Last Assessment Date	Weakness identified	Mitigation Status	Plan of Action	Milestone
DPP6	Data Privacy & Protection	IRS 1075 Reporting Improper Inspections or Disclosures	10.1 General	Upon discovering a possible improper inspection or disclosure of FTI, including breaches and security incidents, by a federal employee, a state employee, or any other person, the individual making the observation or receiving information should contact the office of the appropriate Special Agent-in-Charge, Treasury Inspector General for Tax Administration (TIGTA) and the IRS (section 10.2).						
DPP6	Data Privacy & Protection	IRS 1075 Reporting Improper Inspections or	10.2 Office of Safeguards Notification	Simultaneously to notifying TIGTA, the agency must notify the IRS Office of Safeguards. The TIGTA contact information is shown in section 10.1.						
DPP6	Data Privacy & Protection	IRS 1075 Reporting Improper Inspections or Disclosures	10.3 Incident Response Procedures	Incident response policies and procedures required in section 9.9 should be used when responding to an identified unauthorized disclosure or data breach incident. Once the incident has been addressed, the agency will conduct a post-incident review to ensure the incident response policies and procedures provided adequate guidance. Any identified deficiencies in the incident response policies and procedures should be resolved immediately. Additional training on any changes to the incident response policies and procedures should be provided to all employees, including contractors and consolidated data center employees, immediately.						
DPP6	Data Privacy & Protection	IRS 1075 Reporting Improper Inspections or	10.4 Incident Response Timeframes	The agency will contact TIGTA and the IRS immediately, but no later than 24-hours after identification of a possible issue involving FTI. The						
DPP6	Data Privacy & Protection	IRS 1075 Reporting Improper Inspections or	10.5 Incident Response Cooperation	The agency will cooperate with TIGTA and Office of Safeguards investigators, providing data and access as needed to determine the facts and						

Figure 8 – The Unisys Team's security risk framework provides a regulatory report customized to Commonwealth agency requirements (example of IRS 1075).

Security Framework ID	Security Domain	Regulation	Regulatory Reference	Regulatory Requirement Description	Established Control	Last Assessment Date	Weakness identified	Mitigation Status	Plan of Action	Milestone
AC11	Access Control	PCI DSS v2.0	1.1.1	1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations: 1.1.1 Verify that there is a formal process for testing and approval of all network connections and changes to firewall and router configurations.						
ISA39	IS Acquisition Dev. & Maintenance	PCI DSS v2.0	1.1.2	1.1.2 Current network diagram with all connections to cardholder data, including any wireless networks. 1.1.2.a Verify that a current network diagram (for example, onethat shows cardholder data flows over the network) exists and that it documents all connections to cardholder data, including any wireless networks. 1.1.2.b Verify that the diagram is kept current.						
IS6	Infrastructure Security	PCI DSS v2.0	1.1.3	1.1.3 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone. 1.1.3.a Verify that firewall configuration standards include requirements for a firewall at each Internet connection and between any DMZ and the internal network zone. 1.1.3.b Verify that the current network diagram is consistent with the firewall configuration standards.						
ISA38	IS Acquisition Dev. & Maintenance	PCI DSS v2.0	1.1.4	1.1.4 Description of groups, roles, and responsibilities for logical management of network components. 1.1.4 Verify that firewall and router configuration standards includea description of groups, roles, and responsibilities for logical management of network components.						
AC3	Access Control	PCI DSS v2.0	1.1.5	1.1.5 Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be						

Figure 9 – The Unisys Team's security risk framework provides a regulatory report customized to Commonwealth agency requirements (example of PCI DSS).

Through the data center consolidation effort, the Commonwealth is embarking on a journey of integration within and beyond the enterprise. We understand this evolution requires a comprehensive security and privacy strategy and approach that are critical to its operation. The Unisys Team brings to the Commonwealth a strong mix of industry leading regulatory risk management practices, experienced team members, and related Commonwealth and public sector experiences that add value to establish and maintain a regulatory compliant data center. We believe that these qualifications, combined with our technology strategy and implementation capabilities, uniquely position us to collaborate with the Commonwealth to help effectively evolve and mature the data center's security regulatory posture.

Clarification	*Text*
2.	*Please clarify whether the PSP security requirements described in Section 3.2.2.5 (Security Management) and the referenced exhibits will be met by utilizing a dedicated set of firewalls, hardware, and software for PSP; and if the separations are logical or physical.*

Unisys Response:

The PSP security requirements described in Schedule F Section 3.2.2.5 (Security Management) and the referenced exhibits are met by a dedicated set of server hardware and software in a dedicated cabinet, and are separated by dedicated virtual firewall instances.

In addition, as part of the Enterprise Services Catalog, PSP can select any or all of the following options:

- Dedicated physical firewall(s)
- Secure (locked) cabinet(s)
- Separate secure (locked) cage(s)

Clarification	*Text*
3.	*Please describe in detail how Unisys will provide for justice agency only management of data considering Unisys is not a CHRIA named justice entity.*

Unisys Response:

Unisys understands the Commonwealth's requirement that only CHRIA named justice entities can have access to and manage CHRIA data. We address the requirement of restricting access to and management of data through the combination of the following measures:

1. The Unisys Team will work with the Commonwealth to obtain a Management Control Agreement (waiver) for this contract that allows us to manage CHRIA data as directed by the appropriate CHRIA named Commonwealth justice entity (or entities). In order to obtain the Management Control Agreement, we will show evidence that all Unisys Team personnel who access CHRIA data have passed a security background check per an approved Commonwealth process and have completed security training as to how to appropriately handle CHRIA data based on the regulations in the CHRIA Handbook.

2. If Unisys is not able to obtain a Management Control Agreement from the Commonwealth for this contract, we restrict access to CHRIA data in much the same way as we currently restrict access by the Unisys DPH Support Team. For the Pennsylvania State Police, we currently manage only the hardware not the CHRIA data. Our administrators do not have access to PSP databases to view any data. We enforce segregation of duties between the

Commonwealth and Unisys Team personnel, such as requiring that database administrators be from CHRIA named justice entities only. During the transition phase of the new contract, we will collaborate with the Commonwealth to define a process for obtaining approval from the appropriate CHRIA named Commonwealth justice entity or entities for any requests for DBA services under the contract to work on databases that we suspect may contain data covered by CHRIA.

3. In either case, whether the Unisys Team works under a Management Control Agreement allowing us to manage CHRIA data (#1 above) or whether we are restricted from doing so (#2 above), the following applies:

    a. Through our Data Loss Prevention (DLP) implementation process during the transition phase, we work collaboratively with each Commonwealth agency to discover classified data within that agency, inventory the data, and define appropriate protection measures for the various classifications of data. CHRIA data, per governing regulations, is encrypted while stored and when in transit. These encryption measures offer the first level of protection of CHRIA data while being managed by the Unisys Team. Unisys does not have direct access to the CHRIA data as the ability to decrypt the CHRIA data resides with those who are authorized to access CHRIA data. We only manage the encrypted data.

    b. The Data Loss Prevention (DLP) and Database Firewall (DBFW) tools appropriately identify, monitor and protect sensitive data, including CHRIA data as described in Section 2.3.4, “Data Management”, in Schedule F of our proposal response. These tools allow us to track CHRIA data and through auditing measures, and identify and stop any data breaches at data storage locations and data center egress points.

    c. The proposed implementation also includes the use of the Cyber-Ark privileged account management tool, to manage and log the access to protected data by privileged users including Unisys Team administrators. If the Commonwealth desires, Unisys can also add to the Enterprise Services Catalog the Cyber-Ark module that enables the Commonwealth and the Unisys Team to monitor, log, and audit every action taken by a privileged user.

    d. All Unisys employees and subcontractors providing data center services are subjected to background checks and form signatures and completion of annual security training.

Clarification	*Text*
4.	*Please describe how Unisys will support agency specific Disaster Recovery tests twice a year.*

Unisys Response:

The IT Risk Manager in the Unisys Program Management Office reviews and guides the selection of needed services as part of the Transition activities. Following this review process Unisys builds out the Disaster Recovery infrastructure selected by each agency and works with the agency to schedule the twice-annual testing cycles.

The IT Risk Manager manages the reporting and review for all Disaster Recovery testing with agency directors. Unisys has always used the testing event as a means not only for testing to success but also as an opportunity to identify means to improve services. Unisys expects that the Disaster Recovery testing also results in changes to the agency's plans maintained in the online disaster recovery-planning tool included in the Unisys solution.

The Unisys solution for Disaster Recovery testing takes into account the practices, processes and improvements that the Unisys team has brought to the annual Disaster Recovery testing over the past decade. We have used this experience to model the team of experts that Unisys expects to deploy for a Disaster Recovery test and predict the labor effort needed based on the count of servers involved in the test and the mix of servers that rely upon disk replication for recovery (e.g. Config-4 servers) versus those that use tape-based recovery for recovery.

The Unisys Enterprise Services Catalog provides Agencies with the tools to select the appropriate services to provide Disaster Recovery services that match the criticality of the agency applications that rely upon Unisys IT services.

Clarification	*Text*
5.	*Please describe how Unisys will establish a quiesce point for recovery for tightly integrated environments of mainframe, midrange and x86.*

Unisys Response:

The establishment of a quiesce point for recovery for tightly integrated environments of mainframe, midrange and x86 is highly dependent on application design. Many applications, which have multi-tier environments, have an established process to ensure all transactions are committed before a transaction is complete. For these applications, there is the ability to establish a quiesce point in which the application can be placed in a state to allow a synchronized backup across all tiers to occur. These backups are then used in the recovery process.

Determining quiesce points will be an outcome of populating the Configuration Management Database (CMDB) through auto discovery during transition, which will store the relationships associated to a given application and infrastructure components. The CMDB will store the downstream relationship of components associated to an application; therefore, to determine what needs to be quiesed, the CMDB is used to determine the interdependent components when then indicates the process of creating a quiese point and the automation required to do so.

Interdependency mapping is also an activity Unisys takes up with Agency application owners using the discovered connections. Application architectures are applied to the captured information to provide a view of the applications that permits identification of quiesce points in each of the application's infrastructure tiers and the needed sequence and timing for application sub-system stops and the sequence of tier restarts.

Ultimately, establishing a quiesce point is a function of application design. The Unisys team will be collaborating and working with the Agencies' application owners to identify and establish quiesce points and then build DR plans and build run-books for the applications in its care.

Clarification	*Text*
6.	*Please provide a detailed explanation (i.e. steps required) of how Unisys proposes to transition tightly coupled/integrated applications that reside on multiple and differing technologies (mainframe/midrange/x86) in differing Commonwealth datacenter environments.*

Unisys Response:

Unisys has designed the solution architecture to provide a range of options to meet the risks of transitioning tightly coupled/integrated applications. From the selection of data center locations and their inter-datacenter networks, to the range of tools provided, Unisys has anticipated the issues surrounding application migration. To start, Unisys will create an application taxonomy, which is composed of Agency applications, and their associated components that helps determine tightly coupled/integrated application infrastructure components. The completion of the application taxonomy is then used to determine the application move groups. Unisys will accomplish the creation of the application taxonomy through a Data Gathering phase in the transition that is to be performed in the following manner:

1. Unisys plans to deploy a self-discovery tool that discovers infrastructure and application components. The discovery tool is capable of discovering applications and mapping the conversations between them. Once these application components are discovered they are loaded in the CMDB along with the associated relationships that were identified during discovery. The same holds true for infrastructure components where network IP conversations between devices are captured to create relationships between infrastructure components, which are then captured and loaded in the CMDB. At the end of this auto discovery phase Unisys' goal is to have captured up to 85% of the tightly integrated

application and infrastructure components and their associated upstream and down relationships that can be used to determine move groups.

2. For custom applications or devices not discoverable on the network, Unisys will conduct an application interview and provide questionnaires that will assist the agencies to identify these components. In addition, Unisys will contribute its own knowledge of the Commonwealth's applications during this process. The data collected during this effort is manually entered in the CMDB with the associated relationships.

3. Working in collaboration with the agencies, an audit of the CMDB for accuracy starting from an application name and tracing the relationships down through all related components is completed. Once the audit is complete, we then work in collaboration with the agencies using the CMDB to determine move groups based on the application taxonomy that been derived from the CMDB.

4. With the base application move groups determined, other potential impacts such as, network latency issues, application interface dependencies between other agency applications, and seasonal business restrictions are then factored in to determine the final migration plan of the move groups.

Once the above is completed, we then move into the migration project, which may entail several different migration techniques including

- Over-the-Wire – where data will be copied from the source to the target environment,
- Lift-and-Shift when allowed –where the current infrastructure is turned off, packed and moved to the target data center and
- Greenfield – where application workloads will be reinstalled on new hardware that contains a basic build.

The Unisys Team reviews and recommends one of these strategies for each application but the final decision is made jointly between the Commonwealth and Unisys.

Each phase of the Migration Program provides a solid foundation to prepare for subsequent phases. The early phases of the program collect required data and create the overall migration plan. The middle activities combine to create a high-level approach to the migrations and create the micro design for the migration units. Lastly, detailed plans are created for the migration events. Once the workloads are migrated, we will notify the Commonwealth when physical assets in their environment are ready to be decommissioned.

Move package analysis and design uses information collected in the Data Gathering activities to validate the agencies' current server environments taking into account consideration of outage windows, application release cycles, and anything that could impact the schedule. This data, which cannot be gathered programmatically, is gathered manually through an application interview process. Then this information is analyzed and used to create the initial design which specifies the high-level migration types and the sequenced migration move groups.

Migration analysis and planning activities focus on developing the detailed design and migration plan. The technical solution document takes into consideration environmental readiness including: network, system and storage availability. Any security requirements are identified such as encryption, network zoning and firewall requirements. The micro design takes into consideration any application specific information that could impact the performance of the application in the proposed target environment. This data is manually collected data through the application interview process with the application SMEs. The output from the phases is a refined migration plan and schedule.

Application Migration – The migration phase is executed in the source data center, or over the network. Migration over the network allows server images to be migrated directly to the target environment. The migration approach(s) leverages host-based migration tools allowing for the migration data at a volume/block level, locally or over a distance, between multi-vendor storage subsystems. Once the initial data is migrated, the tools have the ability to refresh the data up to the final cutover. When a source server can be decommissioned, the Commonwealth is notified so they may initiate that process.

As seen in the application migration process described above, the Unisys application migration teams work with the Commonwealth on multiple levels to identify potential challenges including tightly coupled/integrated applications. This is a common situation that has several potential solutions. Each situation is reviewed with the Commonwealth application owners on a case-by-case basis in order to identify the best solution. It is important to understand that just because two applications are tightly coupled does not mean they will experience problems due to being located in separate locations. The three components that determine if remediation needs to take place are

1. Additional latency created by added distance in the network (approximately 1 milli-second per 100 miles),
2. The number of round trips the inter-server communications must make, and
3. The sensitivity of the application and/or user to additional delays.

With this in mind, the four most common solutions to mitigate this risk are:

4. Relocate both applications to the same target data center in the same move package
5. Tune the application to reduce the number of round-trip communications required in the applications
6. Implement WAN acceleration tools
7. Nothing – The additional delay is acceptable

At a high level, the Unisys migration schedule has been designed to begin to mitigate this risk. Often, but not always, closely related applications currently reside in the same data center. As Unisys begins to migrate applications, we will be focused by data centers. In addition, Unisys specifically chose the [redacted] facility due to its proximity to Harrisburg (approximately 90 miles) which adds less than 1 milli-second of latency.

Clarification	*Text*
7.	*Please provide details on each proposed datacenter and what services will/can be provided from each. Address each proposed datacenter individually. Include references to all environments, including but not limited to, production, test, development and DR.*

Unisys Response:

The Unisys 2+ multi-data center architecture permits the placement of any service at any location having sufficient space, power and availability with only one exception – the placement of active mainframes must be at one of the two Unisys locations. Unisys determines the placement of applications, systems and services upon consultation with the Agencies and their application owners.

System Designation	Unisys [redacted]	Unisys [redacted]	Commonwealth Enterprise Data Center
Production	Any equipment type	Any equipment type	No mainframe service
Test	Any equipment type	Any equipment type	No mainframe service
Development	Any equipment type	Any equipment type	No mainframe service
DR	Any equipment type	Any equipment type	No mainframe service
Other	Any equipment type	Any equipment type	No mainframe service

In all other cases, whether considered production, test, development or DR, or considered Fully-Managed, Managed-Only, Limited Co-Location, Mainframe Services or On-Demand (Infrastructure-As-A-Service), or, any site having sufficient space, power and availability can host the service.

Service Type	Unisys [redacted]	Unisys [redacted]	Commonwealth Enterprise Data Center
Fully-Managed	Any service type	Any service type	Any service type
Managed-Only	Any service type	Any service type	Any service type
Limited-CoLocation	Any service type	Any service type	Any service type
Mainframe Services	Any service type	Any service type	No mainframe service
On-Demand (IaaS)	Any service type	Any service type	Any service type

Initially, Unisys anticipates the placement of the [redacted] (Data Powerhouse) systems in Unisys [redacted] with placement of the DR services currently residing at SunGard [redacted] into Unisys [redacted]

IBM Sterling Forest may be used if the Commonwealth elects to continue with its IBM mainframe DR services, as they currently exist via the IBM DR subscription services. No other use for IBM Sterling Forest is intended. The site has been included in Schedule E, "Datacenter Locations", for completeness.

Unisys [redacted]

Unisys [redacted] is hosted within the [redacted] Data Center at [redacted] in [redacted] The site is about 90 direct miles or 104 road miles from Harrisburg and is in the [redacted]. The location is in the same seismic zone as Harrisburg – Seismic Zone 1 – where there is less than a 1% chance of a major earthquake of 5.0 magnitude or greater in the next five years and within 50 km of the [redacted] area.

The facility is at the center of one of the most fiber rich areas of the country and at the center of the key mid-Atlantic networking location in Northern [redacted] Consequently, it provides one of the most flexible and scalable locations to meet the networking requirements that address any possible latency issues encountered during migration.

Unisys [redacted] – Services

Unisys [redacted] may be utilized for Fully-Managed, Managed-Only, Limited-CoLocation, Mainframe Services or On-Demand (IaaS). The facility can be considered for any type of environment including production, test, development or DR.

Unisys [redacted] – Building Design

The facility opened for service in April 2012 and consists of 150,000 square feet of space, of which, approximately 70,000 square feet are usable data center floor space. This data center space is configured as five pods or vaults constructed within a single protective structure as shown on the drawing that follows.

The structure's design and construction includes

- Concrete slab foundation
- 6" reinforced concrete exterior tilt-up outer shell, IBC Type IIB construction
- Interior roof height at 27 feet – 24 feet clearance above 3 foot raised floors
- Roof sprayed, highly reflective polyurethane foam that acts as a moisture barrier as well as an additional protective layer.
- Lateral design supports wind speed of at least 75 miles per hour.
- Implementation of a building-within-a-building design for the vaults providing a 6 to 10 foot air wall between the vaults or the facility's outer wall. Among several benefits of this design, there is no direct path from a vault to the building's exterior and all mechanical and electrical service areas are to the outside of the vaults rendering all raised floor usable to IT equipment and services. In addition, all vaults are access controlled to only those requiring access to the systems inside.

- A signal reference grid (grounding grid) in 20'x20' squares internal to the facility (2/0 AWG), a 4/0 AWG ring around the facility exterior, and a 5/0 AWG ring around the outside of each data center vault. Floor stanchions, conduits, chilled water piping, cabinets, etc., tie into the signal reference grid.
- Offices, meeting rooms and common spaces including showers and a lounge/kitchen area for breaks.
- Curved-steel fencing with security gate post surrounding the mechanical-electrical plant infrastructure.
- Three mantraps with fixed cameras control access to the major security zones within the facility.

Unisys [redacted] – Certifications

The facility meets or exceeds the requirements for

- SSAE-16 Type 2 SOC 1 Compliance (zero exceptions)
- PCI DSS 2.0 Certification
- Safe Harbor Certification (100% compliant)
- FISMA Moderate Compliance
- TIA-942 Data Center Standard (89% of the Tier 3 and Tier 4 requirements; 75% of the Tier 4 requirements)
- Up Time Institute - While not officially rated, mechanical systems meet the requirements for Tier 3; electrical systems meet the requirements for Tier 4.

The facility's SSAE 16 Type 2 SOC 1 and PCI DSS 2.0 audits completed with zero exceptions. The SSAE-16 report is included with Schedule E, "Location of Datacenters". The PCI attestation report is available upon request. Together these audits cover the spectrum of data center operations, focusing on financial integrity, data center physical and personnel security, and financial reporting. In addition, the facility has met all but the time-based requirements for

- Energy Star Rating as Energy Efficient
- LEED Certification

These certifications waiting periods will be complete before the Commonwealth's IT environment resides in the facility.

Unisys [redacted] – Electrical Systems

All components of the building electrical, mechanical, branch circuit monitoring, and environmental monitoring systems are managed by [redacted]'s [redacted]™, a suite of data center infrastructure management systems. There are no single points of failure in the facility's electrical system. [redacted]™ provides

- Monitoring and optimizing of power delivery
- Management of the facility cooling mode and configuration automatically

- Monitoring of the security and environmental systems
- Maximization of performance and uptime
- Meeting SLAs with no maintenance windows
- 2N+2 redundancy at the rack level
- Patented maintenance bypass and isolation technology meeting a "fix-one, break-one with a utility outage" design criteria
- Patented distributed redundant UPS design with live load switching for scalability
- Metered power

Supply - Unisys [redacted] has a [redacted] delivering 21 megawatts at a 14.4 megawatts critical power load. The feed runs 3,300 feet underground in concrete-encased, weather-hardened ductwork from the substation. Because of [redacted] high-priority location in [redacted], [redacted] has increased the redundancy of the substation. Improvements include five 230kV transmission lines that feed the substation (only one is required to support the current substation load) in a geo-diverse fashion (3 from the east, 2 from the west).

The substation electrical distribution is a networked 230kV system with a doubly fault tolerant breaker-and-a-half networked bus configuration. The substation transformers (230kV to 34.5kV) are also in at least an N+1 configuration and [redacted] has assigned a high priority to the [redacted] in terms of contingency analysis for load restoration priority in the case of a systemic utility power outage.

Uninterruptible Power Supply – Electrical circuits (120V, 208V, single or three phase, from 20 to 80 amps) are supplied from Power Distribution Units (PDUs) on the data center raised floor. Each PDU is fed from two separate 1,000kVA Uninterruptible Power Supplies (UPS). Dual-corded equipment in racks or cabinets on the data center raised floor are then supplied circuits from two different UPS's. As a result, dual-corded equipment is protected from loss of power from any single source. In the UPS, the AC signal is rectified to provide auctioneered DC power that is inverted back to supply AC power to the Remote Distribution Units (RDUs) and PDUs on the data floor.

Electrical circuits (120V, 208V, single or three phase, from 20 to 80 amps) are supplied from Power Distribution Units (PDUs) on the data center raised floor. UPS Switch Points (USPs) allow any facility UPS to power any PDU in the facility

Each MSB is backed up by one 2MW diesel generator that will automatically pick up on loss of power. In addition, there is a series of N+2 generators that can pick up any MSB upon failure of its associated diesel generator.

The overall facility UPS topology is a distributed redundant configuration, with a patented maintenance bypass isolation feature. This feature enables the facility to exceed Uptime Tier 4 standards for data centers to be concurrently maintainable or fault tolerant. Because of this technology, the facility is concurrently maintainable and fault tolerant, with a simultaneous utility outage. This innovative level of critical infrastructure redundancy has been termed 2N+2: two completely separate power paths from the power utility to the customer rack (2N) AND all of the

critical components in those two independent power paths have (at least) two extras for backup (N+2).

Our ability to scale power across the facility, from any UPS to any RDU is also a patented technology that differentiates this Unisys facility from our competitors. This technology is especially beneficial to the Commonwealth as it desire to scale over time, as it allows the critical infrastructure to scale seamless as the Commonwealth experiences growth. We can implement and commission new phases of the electrical plant, including UPS load balancing, seamlessly without any interruption to equipment power (or decrease in reliability).

In the Unisys [redacted] data center, Schneider-Electric 1000 kVA dual-module UPS systems with internal bypass and a dedicated System Control Cabinet (SCC) each (and patented external maintenance bypass) are utilized in a distributed redundant configuration. Each PDU (power distribution unit) is fed from two separate 1,000kVA lines from the UPS systems. The facility uses a 2N+2 electrical topology controlled and monitored by [redacted]s patented N-Matrix™ technology.

At 100% capacity, each UPS system may operate on battery for 14 minutes. In the event of a utility outage, the time on battery is not only engineered for the normal 15-second transfer to the dedicated generator but time was allotted in the event of a re-alignment to the redundant generator.

The maintenance performed on these double conversion static UPS systems is in line with the industry standard of a semi-annual UPS inspection followed by an Annual. Readings are taken daily on each system and reviewed by senior staff for any anomalies.

Unisys [redacted] utilizes flooded lead acid batteries in the data center UPS systems. Each 1.8-megawatt UPS system contains two 900-kilowatt modules. Each UPS module has its own dedicated battery string. Each battery is monitored 24x7 by a monitoring system that will visually and remotely indicate a battery that requires preventative maintenance (e.g. impedance, AC ripple and temperature). These batteries will carry a 3-year full warranty and 17 years pro-rated product warranty.

The flooded batteries are maintained monthly by the critical facilities team and annually by an independent specialized battery maintenance vendor. BigFoot is used for CMMS scheduling, tracking and updating. Intellibat, the battery monitoring system, provides an endless amount of analytics showing how the batteries currently sit in their projected life cycle. In the event of a UPS maintenance event, the Unisys [redacted] contracted UPS vendor is required to be onsite within 4 hours of initial call out. However, the backup plan lies within the site's topography of 2N+2 meaning that the site can continue to provide a 2N level of redundancy in the event of the loss of one UPS system through the fix-one-break-one patented technology.

Generation – Unisys [redacted] currently has five 2-megawatt Cummins diesel generators outside the building in a secure fenced-in area. At full operation, the facility anticipates a total of 14 generators. The generators are housed in outdoor container enclosures with belly tanks at one unit per container. The generators burn approximately 120 gallons per hour at full load and can run 24

hours at full load. The facility maintains refueling contracts with multiple suppliers to guarantee delivery within 24 hours from initial contact and to provide continuous top-offs until utility power has been restored.

The generators are exercised monthly at greater than 30% load for at least 30 minutes. The data center facility is transitioned to generator power on a quarterly basis for at least 30 minutes. Any abnormal operating conditions are recorded in material history. Daily logs are taken across the facility's infrastructure, including the electrical systems, HVAC systems, BMS, security operations and general conditions. These logs are maintained by critical facilities operations staff and reviewed by critical facilities management on a regular basis for trending and analysis.

Power Density – The facility power plan delivers high scalable power via diverse paths to each vault. Power densities available are from 150 watts per square foot to 250+ watts per square foot. Even with these high power densities, the facility maintains one of the best PUE (Power Usage Efficiency) in the industry at 1.45. This power density enables Unisys to meet the Commonwealth's IT data center needs in far less space than typically used in facilities like Willow Oak. Combined with the new technology equipment configured to meet the Commonwealth's requirements much less floor space can be employed to provide much more IT resource. This feature of the facility is among the keys to the Unisys solution's unique scalability and flexibility.

Unisys [redacted] – Mechanical Systems

[redacted] has installed centralized 1800-ton air-cooled chillers with waterside economization and with water-cooled chillers installed and scaled as the facility load increases. Facility CRAH (computer room air handler) units are custom-built Energy Labs 100-ton units which stretch from floor to ceiling with the capability to perform airside economization; Unisys [redacted] CRAHs operate on free outside air about 60% of the year.

In airside economization mode, air is pulled from the outside via roof plenums at the top of the CRAH units, passes through the CRAH unit (no chilled water flow through piping), and is pushed under the raised floor to maintain the static pressure used to push cold air into the cold aisles of the facility. The cooling system maintains cold aisle temperature at the outlet of the cold aisle perforated tile at 72 degrees F +/- 5 degrees.

In partial airside economization mode, the process is the same, but chilled water flows through the CRAH unit chilled piping at the same time. During the high-temperature months, the chiller plant cools the facility with CRAH units operating to pull hot air from the data center ceiling over chilled water piping to transfer heat from the data floor to the chilled water return, where that heat is rejected to the air (at the air cooled chillers). The air-cooled chillers also have economizer coils for "dry cooler" mode of operation.

All chillers, pumps, cooling towers and associated HVAC components are N+1 or greater redundancy. The data center air handlers are installed at an N+2 redundancy. Facility HVAC and mechanical systems monitoring is accomplished via Schneider Citect and SynapSense.

A leak detection rope system comprised of multiple zones is used throughout the facility and is routed beneath all CRAH's and chilled water piping throughout the facility. The system is testing quarterly with all results reported into the CMMS. Security roving patrols walk the entirety of the facility on an hourly basis and inspect for any water intrusion at the drip pans. The drip pans have drain valves for drain lines to be attached to in the event draining is needed.

Installation of a well is completing at the [redacted] data center. In addition to utility potable water, reclaimed water is also used by the cooling towers. In all, there are three water sources onsite to support the cooling plant water makeup requirements. Overall, the Unisys [redacted] facility's design incorporates a cooling system with zero single points of failure. In the event of any mechanical system or component failure, the redundant architecture plans for a failure. Included is loss of chiller, chilled water pump, piping rupture, etc. The cooling system meets UTI Tier 3 requirements.

Unisys [redacted] – Fire Systems

Unisys [redacted] utilizes a multi-zone, dual-interlock, pre-action, dry pipe fire suppression system with intelligent smoke and thermal detectors which require both sensors in the same zone to detect an alarm condition in order to admit water into the pipes inside a critical area. Sprinkler heads are also fitted with a high-temperature fusible head in order to preclude admitting water into a computer room area where no fire is present. The fire suppression and alarm system is integrated into the site's Network Operations Center and security office monitoring systems. In the event of a fire, all fire rated doors automatically close but still allow for egress. In addition, the Unisys ITSM system receives the facility alerts and alarms to alert the Unisys Team in Harrisburg to the event.

Non-critical environments are protected by wet sprinkler systems with protection/notification as required by local ordinances/codes.

Unisys [redacted] – Security

[redacted] security team is 24x7.The security lobby is staffed 24x7 by an in-house security team that is comprised of military veterans and career police officers. Each client's equipment within the data center is housed in a vault, cage enclosure or cabinet that is exclusively dedicated to that client. Access is restricted to authorized personnel only, who must pass through multiple security zones delineated by mantraps with card readers and keypads for personal identification numbers, as well as biometric iris scanners. The facility's security features include

- Multiple security zones
- 3600 digital camera coverage
- 3-factor ID for data floor access
- Building within a building design
- Curved-steel fencing with security gate post around the mechanical-electrical plant

Physical Security – At the core of the security operation is the hardened security lobby surrounded by bullet and blast-resistant glass. 175 concrete and steel bollards surround building itself. Excepting the main lobby entrance and shipping and receiving, the only external doors from the

facility are for emergency exit only and do not open from the computer room floors; they open from the corridor that surrounds the data center vaults. These emergency exit doors are protected by intrusion detection alarms that sound in the security office (located in main lobby) and at the door itself.

Entry into the exterior lobby of the facility requires use of a unique RF proximity badge or a call to the Security department with a valid reason for entering the exterior lobby of the facility. Then, all personnel must authenticate via biometric iris scan to enter the interior of the facility. Personnel must be biometrically enrolled using iris scans (and authorized access to the data floor) in order to gain entry onto the data center raised floor areas. Passage through the mantrap then requires entry of a PIN code. Entry of an improper PIN code generates alarms that display on the centralized electronic access control system, which is monitored 24x7x365 by on-site security personnel.

Physical facility security includes a building-within-a-building design, ensuring there is no direct access to the data floor from the external walls of the facility. CCTV that monitors the facilities parking lots, roof and entrances is monitored in the security office. Over 150 steel and concrete bollards surround the facility in front of parking and the main entrance. All other back-of-house MEP infrastructure and the shipping & receiving area is surrounded by steel fencing and secured with entrance gates and a guardhouse.

All visitors to the data center that are not current customers or customer vendors (who are badged and granted access to the facility via customer account custodians) are escorted by [redacted] personnel at all times. Visitor access times are electronically tracked and recorded as they enter and leave secured areas (they are also monitored via CCTV).

The facility's centralized electronic access system is in operation 24x7 – it will alarm if an unoccupied secure space is accessed without proper authentication or even if it is attempted to be accessed without a proper pin code, RF proximity card or biometric iris scan. Generator enclosures are kept physically locked at all times unless they are being maintained by critical facilities staff who are present at all times while the enclosures are open.

The loading dock area is secured by high-security steel fencing, a gate and guard post monitored 24x7 by CCTV. The gate may only be operated by the 24x7-security team physically present at the gate. No vehicles are authorized inside the gated and fenced-in mechanical-electrical plant and loading dock area, besides authorized shipments and shipping trucks. The gated and fenced access to the loading dock area is manned only when a truck has checked in to the front security lobby and cleared security. With advance notice, shipments and items stored in shipping and receiving may be retrieved after normal working hours.

Vehicle access to the site is via a public road entrance. All parking areas are monitored by CCTV with all facility and parking access available 24x7.

Access Control – Unisys [redacted] has a centralized, electronic access control system that provides alarm monitoring points on all personnel and equipment doors, as well as intrusion detection throughout the facility. Photo ID badges with unique personal identification numbers, as well as

biometric iris scanners, provide multiple levels of electronic access control and provide individual accountability throughout the facility. The site's security systems control physical and electronic access to the building, the data center floor, and each vault or caged area.

Access to the facility is restricted to authorized personnel only. All personnel (site employees, clients, vendors, contractors, and any other visitors) must be badged before entrance and badges must be displayed at all times. Each badge is programmed to grant access only to areas the personnel has been authorized to enter. All temporary badges must be returned to security control and logged out daily.

Client access to the facility is strictly regulated by adherence to specific badge authorization procedures. Unisys maintains a minimum of two account custodians from the Unisys Security Team for the Commonwealth vault. The account custodians are deemed authoritative and are exclusively responsible for approving access to the facility and to the vault's equipment cage or cabinet. Authorization is verified by means of a password unique to the Unisys account custodian. After approval has been received at the site for an individual to gain access to the data center and client equipment, a Badge Authorization Form is initiated.

This form verifies the name of the individual, the access time, and what access level they should be granted. The Badge Authorization Form is then sent to the site's Security department, where it is reviewed by the Security Manager and either approved or returned for clarification. Once approved, an access badge is made and an individual PIN code is assigned to that badge. Identification is verified by use of a government picture ID. In the event of a short notice (or nights or weekends) authorization request, the account custodian can telephone the site's Operations Control Center (OCC) and request authorization for access verbally. Passwords will be verified and the OCC will then generate the Badge Authorization Form for Security. Access controls include

- Government-issued ID required
- No public access
- Biometric iris scanning technology to access data floor: multi-point iris recognition and normal pupil dilation required for approved access
- Three-factor authentication to access data center, including Commonwealth-only areas
- Security-only access to shipping and receiving
- MDF/Telco Room protected and access-controlled like a SCIF

Monitoring – Active security monitoring includes

- Multiple security zones
- Multiple access levels for customers and employees
- 43 pan-tilt-zoom digital cameras monitor facility – coverage retained for at least 90 days
- Intrusion detection system on all fire exits
- Multiple fire suppression zones
- Redundant access control and monitoring systems – one in Security and one in NOC

Unisys [redacted] – Building Management

The systems used for building management include:

- GE iFIX is used for monitoring of the overall electrical plant.
- Schneider Citect is used for monitoring of the mechanical plant.
- Trendpoint is used for branch circuit breaker monitoring.
- Intellibat is used for battery monitoring.
- SynapSense is used for data center environmental monitoring.
- Bigfoot's computer maintenance and management system is used for facility equipment maintenance management.

The monitoring systems oversee

- Multiple security zones
- Multiple access levels for customers and employees
- 43 pan-tilt-zoom digital cameras monitor facility – coverage retained for at least 90 days
- Intrusion detection system on all fire exits
- Multiple fire suppression zones
- Redundant access control and monitoring systems – one in site Security and one in the local facility NOC

Data from the BMS and power management systems is tracked and data is collected and analyzed by the critical facilities group. Automated alarming schemes are integrated into the power circuit monitoring system, which emails alerts to both staff and customers that own the affected circuits (low, warning high, high). The systems are backed up daily with software stored onsite. Senior staff continually provides training, and staff is sent to offsite training as available. The training is been pre-approved for verification purposes. In addition, the facility's training matrix helps to determine needs as well as skill assessments. [redacted]'s facilities operations staff is highly trained and skilled, the majority of which are ex-Navy nuclear operators and technicians.

Unisys[redacted] – Operations

Operations within the facility include:

- Above raised floor cleaning in general areas weekly, within the computer rooms annually and sub-floor cleaning every third year.
- Electrical and HVAC system testing monthly, quarterly, semi-annually and annually depending upon the system.
- Service tickets are required for all work to be performed and these tickets require three levels of internal facility approval.

Unisys[redacted] – Networking

Unisys[redacted] has three diverse fiber entrances, [redacted]. The following providers are built into the facility: XO, Zayo Group, Level 3, Fiberlight, Fibergate, Yellowfiber Networks, Datatility, BroadAspect, Cogent, SummitIG.

The Unisys [redacted] facility is carrier neutral and has fiber tethering capability to all of the surrounding data centers in the [redacted] fiber area. Cross-connects from demarc to intermediate demarc are run in multiple secure overhead steel conduits with plenty of growth space. From intermediate demarc to vault racks and cages cross connects are run in overhead ladder racking.

The Unisys [redacted] demark is the MDF (main distribution frame) [redacted] and distributes cross-connects to IDFs (intermediate distribution frame) in the subsequent vaults. The Commonwealth equipment will then connect to the dedicated data center core network as described in Schedule F.

Unisys [redacted] – Computer Room

The vault dedicated to the Commonwealth meets the following specifications:

- Designed to ASHRAE TC 9.9 that is 20-80% humidity and 80.6F at the top of the rack.
- 36" raised floor plenum utilizing 2'x2' Tate Concore raised flooring system.
- Power cutouts are a 4" hole with a 3" steel chase.
- Tate Concore 1250 tiles are rated at 312.5 pounds per square foot.
- A vault isolated by security doors and welded-mesh caging in any plenum spaces (under floor at vault wall and at ceiling at the vault wall).
- Separation from adjacent vaults by mechanical chaises containing CRAH units (facility employee-only security zone).
- 12-foot tall cage mesh standard is used in building optional security cages.

Electrical circuits (120V, 208V, single or three phase, from 20 to 80 amps) are supplied from Power Distribution Units (PDUs) on the data center raised floor. Each PDU is fed from two separate 1,000kVA Uninterruptible Power Supplies (UPS). Dual-corded equipment in racks or cabinets on the data center raised floor are then supplied circuits from two different UPS's. As a result, dual-corded equipment is protected from loss of power from any single source. In the UPS, the AC signal is rectified to provide auctioneered DC power that is inverted back to supply AC power to the Remote Distribution Units (RDUs) and PDUs on the data floor. Power may be monitored down to the circuit.

Unisys [redacted]

Unisys' flagship outsourcing data center is the [redacted] Service Center (ESC) at [redacted] in [redacted] [redacted] is in the [redacted] in a southwest suburb of [redacted] The area is a part of the United States' seismic zone 0 rated with the areas having the lowest seismic risk in North America. The site is approximately 6 miles from [redacted] International Airport.

Built explicitly to host multiple outsourcing data center clients, this advanced service center embodies Unisys' commitment to providing our clients with the best services possible—those that incorporate best-of-class technology and are embedded in industry-accepted standards and forward-thinking, proven methodologies.

The Unisys ESC is a 312,000-square-foot facility that is home to two distinct data centers: The main data center is a 100,000-square-foot raised floor facility. This data center is home to about 3,500 mainframe, UNIX, and Wintel platforms composed of technologies from every major manufacturer, including IBM, Sun/Oracle, Unisys, Dell, HP/Compaq, Microsoft, EMC, and StorageTek. Unisys operations staff provides support to these systems, whose combined processing power equals more than 100,000 MIPS and whose peripheral capability includes more than three petabytes of disk storage and more than 1 million library volumes. Unisys built the second data center to accommodate increasing requirements and is now reserved for the Commonwealth of Pennsylvania. This data center consists of 17,000 square feet of Tier 3 equivalent raised floor.

The Unisys ESC is safe, secure, and protected from disruption or intrusion. All critical procedures, equipment, and software systems have a backup, an acceptable alternative, or a proven workaround solution for use in component or system failure. The ESC also complies fully with industry guidelines for safety, fire protection, uninterruptible power supply, and security requirements. Each year, the ESC is required to pass a SSAE-16 audit for its overall operations.

Multiple SSAE-16 audits that are tailored for specific clients are also performed. Unisys' ESC along with other has Unisys datacenters and Managed Services Centers around the globe hold ISO 27001 certification.

Security at the Unisys ESC includes 24-hour guard protection, a complete badge control system, and interior and exterior video surveillance consisting of cameras and recorders, some with motion detection sensors. Access to restricted or sensitive areas at the ESC is controlled by the badge control system and limited to individuals who need to have it.

With more than 400 professionals on site, the Unisys ESC has the business and technical IT resources with the specialized experience, education, and training needed to support our clients' IT environment. Unisys can closely align our technical IT professionals with the Commonwealth clients' day-to-day system requirements.

Unisys [redacted] – Services

Unisys [redacted] may be utilized for Fully-Managed, Managed-Only, Limited-CoLocation, Mainframe Services or On-Demand (IaaS). The facility can be considered for any type of environment including production, test, development or DR.

Unisys [redacted] – Building Design

The facility sits on a 35-acre campus above the surround area. The structure's design and construction includes:

- 312,000 square feet of space, of which, approximately 100,000 square feet in 1 data center area and 16,700 in a second data center are raised-floor areas.
- Concurrently maintainable facility electrical and cooling services
- Electrical-mechanical support space occupying 30,000 square feet.
- A steel frame structure with a pre-cast concrete panel exterior.
- Walls in the structure provide a 2-hour fire rating.
- Floors are poured concrete over steel pans.
- The roof is a rubber membrane over insulation with rock ballast.
- A truck height loading dock.
- 900 square foot secure staging area.
- Available office and conference facilities.
- Mantraps with fixed cameras control access to the major security zones within the facility.

Mechanical and electrical systems are concurrently maintainable and control the temperature and humidity required in equipment spaces. The facility includes water detection and complete drainage facilities. Grounding is provided by driven ground systems connected to the raised-floor grid system. Emergency lighting exists in all areas of the building.

Environmentally friendly design – [redacted] was upgraded and expanded in 2007 to avoid the problems of many data centers – the rabid consumption of electric power. The Unisys data center in

[redacted] is an environmentally advanced green outsourcing center that reduces its carbon footprint and benefits clients and the community.

For the [redacted] data center, Unisys created a comprehensive solution focused on generating more computing power with fewer physical devices. With this virtualization technology, Unisys can reduce carbon emissions by 67 percent when the number of physical devices diminishes.

Virtualization was just one step. Unisys used integrated and sustainable design elements such as a 30-inch raised floor that maintains superior airflow around servers to maximize cooling efficiency. We also installed a glycol air conditioning system that is more than 40 percent more efficient than those typically found at data centers. This system also uses "free cooling" when the outside temperature is below 50 degrees Fahrenheit, saving 8 percent of power consumption and cost. Other energy-saving equipment includes computer designed fluorescent lighting, central humidification systems, better cable management, and lower emitting emergency generators.

Matching air conditioning with power usage saved $7,000 a month in electric costs in [redacted] This green operational procedure has served as a model for other Unisys data centers to implement.

Unisys saw the surrounding community as an extension of the upgrade and expansion project. During construction, we recycled more than 166,000 pounds of building material—including carpeting, ceiling tiles, conduit, and electrical wire—and achieved a waste recovery rate of 62 percent. Working with the City of [redacted] we also launched land-based initiatives outside our facility, including a 4.5-acre oak savanna restoration that involved the removal of buckthorn, an invasive, non-native plant species that overwhelms native plants. To enhance security for our facility, this project improved views and reduced the risk of brush fire.

Expanding our [redacted] facility was just the first step for Unisys in the IT community. We have already leveraged best practices from [redacted] throughout our existing data centers in North America and around the globe and will continue to do so. This effort has already begun to replicate efforts with clients, including the City of Minneapolis. Unisys is also working closely with power companies to establish baseline metrics for energy efficiency and power utilization.

In December 2007, InfoWorld said, "Now we can add Unisys to the list of companies pushing the green envelope a bit further." Added Victoria Bond, Director, Infrastructure and Operations at Unisys: "This is just the start for [redacted] and Unisys as a whole."

Unisys design criteria for [redacted] as a green data center incorporates green sources of power and works with local utilities that have green sources of power: hydroelectric, wind, solar, and others.

Unisys reevaluated systems, applications, and databases to determine which are essential for our business and eliminated systems that are not required. We consolidated departments, databases, and applications for those that are required. We simplified and modernized our applications and infrastructure. We chose strategies that get us closer to business processes and the inner relationships of our data.

Unisys drove up our own system utilization rates and implemented server virtualization. We internally use shared infrastructure and drive up utilization rates of all our own servers to reduce the total number of servers required and reduce power consumption. The virtualization of servers can reduce carbon emissions up to 67 percent.

Unisys proliferates culture and awareness throughout our organization and the community to welcome suggestions for efficiency, recycling and energy alternatives. Unisys designed a data center that incorporates best practices and is most efficient at power consumption and cooling provision, including optimal airflow. We use computer modeling simulations for optimal airflow and rack and cooling placement on the floor.

Unisys [redacted] saves on cooling by:

- Stepping down computer room air conditioners (CRACS).
- Use of glycol to improve circulation of outside cold air by 8 percent.
- Balance of cooling with load to achieve efficiencies up to 44 percent.
- Utilizing free cooling whenever weather permits.
- Optimal placement of CRACS and racks.

Unisys [redacted] saves on power by

- Using variable speed pumps and fans.
- Turning unneeded equipment off and rotating it.
- Monitoring.
- Computer controlled fluorescent lighting.
- Central humidification.

Unisys established baseline metrics so that we can track improvements as they are implemented, and we use these metrics as we define goals for energy use and savings.

Unisys [redacted] – Certifications

The facility meets or exceeds the requirements for

- SSAE-16 Type 2 SOC 1 Compliance
- ISO 9000, 20001 and 27001 Certification
- ISO/IEC Standard 17799

Unisys [redacted] – Electrical Systems

Supply – Unisys [redacted] maintains two separate supply designs for the two data centers with the facility. The Area F data center, designated for the Commonwealth, receives its supply via a single Xcel Energy Cedarvale Substation Interruptible Service utility feed into two redundant, concurrently maintainable indoor substations that are connected to utility paralleling soft loading switchgear. A dual power distribution system then completes the connections to UPS and generators.

Uninterruptible Power Supply – Area F receives 1400-kilowatt UPS power supplied from an N+1 four-module system.

Generation – Area F has four 1000-kilowatt generators in an N+1 four-module system matched to the UPS. Generators activate 13 to 15 seconds after transfer to the UPS systems. Unisys maintains a 60-hour fuel capacity for the generators at full load.

Power Density – Computer room power is provided to the floor via 12 Liebert 300 kVA PDUs with 400A static switches. Average power and cooling density to the Area F computer room is 80 watts per square foot.

Unisys [redacted] – Mechanical Systems

Unisys [redacted] cooling systems consist of redundant chillers, pumps, cooling towers, controls, and 19-ton glycol/DX CRAC units. A 100,000 gallon chilled water storage tank provides a 1-hour backup operation. In addition, multiple chilled water piping loops run through the facility to provide redundancy. In the event of a municipal water failure, Unisys [redacted] has a backup water well. Dual power sources exist to all mechanical equipment.

[redacted]

Unisys [redacted] – Fire Systems

The Unisys [redacted] fire and smoke detection systems consist of:

- Fenwal and Vesda high sensitivity smoke detection systems
- Fully zoned wet pipe sprinkler system
- A fire suppression system meeting NFPA standards
- A multiple zone water detection system

Unisys [redacted] – Security

Physical Security – Unisys [redacted] maintains on-site guard coverage 24x7x365. Guard coverage is joined with surveillance cameras with video recording. The facility has silent alarm alerting along with

- Badge readers with multiple level access control
- Silent alarm alerting
- Compliant with ISO/IEC Standard 17799
- Lenel 2 factor prox card Secure entrances
- CCTV and DVR monitoring of entrances and exits
- 7x24x365 security officer services

Access Control – The facility maintains a multi-level access control system utilizing role-based access control, badge readers, and mantraps at key security zone boundaries.

Monitoring – All security alarms go to the security desk for response.

Unisys [redacted] – Building Management

Siemens automated building management system with redundant components manages the facility. A facility support team for mechanical/electrical is on-site 24x7x365 with the environment maintaining automated monitoring 24x7x365. A Site Scan Web Based Monitoring System monitors all critical equipment.

Unisys [redacted] – Operations

Unisys [redacted] services personnel include more than 300 professions including Data Center Services, Help Desk and Media Services coverage 24x7x365. Technical support and computer engineering support along with on-site smart hands coverage is available 24x7.

Unisys [redacted] – Networking

Like Unisys [redacted] Unisys [redacted] is a carrier-neutral network location. Six different internet service providers exist in the facility via redundant entrances and points of presence.

Unisys [redacted] – Computer Room

The Area F computer room designated for the Commonwealth provides 16,700 square feet of raised floor space. An illustration of the room as it can be configured shows the floor space available.

Clarification	*Text*
8.	*Please describe in detail how Unisys' data security solution and policies/controls will secure the Commonwealth's data (including any storage or compute device used by Unisys to support the Commonwealth) and meet the requirements of the Commonwealth ITBs, including specifically ITB-SEC020 – Encryption Standards for Data at Rest, and ITB-SEC031 – Encryption Standards for Data in Transit.*

Unisys Response:

The Unisys Team's data security solution and policies/controls will secure the Commonwealth's data and meet the requirements of the Commonwealth ITBs, including specifically ITB-SEC020 – Encryption Standards for Data at Rest, and ITB-SEC031 – Encryption Standards for Data in Transit. The solution starts with our conduct of a baseline security risk and vulnerability assessment, to help the agencies classify their data to determine which data need to be encrypted. Our process for

conducting the baseline security risk and vulnerability assessment, more fully described in Section 3.3.2.2 in Schedule F of our proposal.

- Step 1: **Scope and Plan** where we document project requirements, scope and objectives. See the figure below for a sample of the security assessment and planning data

- Step 2: **Conduct vulnerability assessment** where we use passive and active scanning techniques, and perform infrastructure and database vulnerability testing to identify vulnerabilities.

- Step 3: **Perform penetration testing** where we exploit the vulnerabilities found in Step 2 to fully determine risk to Commonwealth assets

- Step 4: **Perform security risk assessment and architecture review** where we use our public sector security risk framework to develop the data center security risk framework. This framework is customized to the data center, helps integrate several relevant regulatory requirements and perform a risk assessment to identify the data center security posture with regard to relevant regulations and Commonwealth policies. An IT architecture review of the existing data center IT infrastructures is also conducted.

- Step 5: **Perform security configuration risk review** where we assess compliance with applicable regulations (for example, using the IRS 1075 based Safeguard Computer Security Evaluation Matrix on Commonwealth selected IT infrastructure handling Federal Taxpayer Information).

At the conclusion of the baseline security risk and vulnerability assessment, Unisys will have a comprehensive view of the security posture of the Commonwealth. This view will be documented in the baseline security vulnerability assessment report and a remediation plan will be developed. The execution of the remediation plan is the first step in protecting Commonwealth data and assets.

Our solution also leverages both Data Loss Prevention (DLP) and Database Firewall (DBFW) tools to help identify, monitor and protect sensitive and confidential data in transit and at rest at the data storage server locations and data center egress points. As part of this implementation of DLP and DBFW, we will collaborate with each agency to classify their data and determine the appropriate levels of protection (e.g., encryption) needed for each type of data. Our DLP and DBFW implementation approaches are more fully described in Section 2.3.4, Data Protection.

Using our Data Loss Prevention (DLP) and Database Firewall (DBFW) tools assists us to appropriately identify, monitor and protect sensitive and confidential data in transit and data at rest for the Commonwealth. The more specific protection mechanisms that must be employed are defined by governing policies and regulations including CJIS, CHRIA, HIPAA, SSA, IRS, PCI and the Commonwealth ITBs. As discussed earlier, an output of the baseline security risk and vulnerability assessment, which in part assesses the Commonwealth's compliance with these governing regulations, is the remediation plan, where gaps are identified between existing and necessary

measures to protect Commonwealth data. Through the execution of the remediation plan, protection measures will be taken to protect Commonwealth data.

As noted, ITB-SEC020 calls for the protection of stored sensitive, protected or exempt data at rest through the use of encryption in accordance with the Advanced Encryption Standard (AES) for symmetric encryption and following ITB-SEC013 and ITB-SEC014 for asymmetric encryption.

To protect the data that is classified as needing ITB-SEC020-level protection through our data classification activities described above, we will be encrypting all physical tape drives using IBM Tivoli Key License Manager (TKLM). TKLM is platform independent and enables the centralized management and generation of encryption keys that are used by storage platforms such as the IBM TS3500 and Oracle SL8500 Tape Libraries. These keys combined with FIPS 140-2 validated cryptographic modules on the tape drives support encrypting the data stored on the tapes using AES. TKLM will be deployed at both [redacted] and [redacted] to support disaster recovery functionality, but only one instance can own the key generation at a time. TKLM can be configured to support Agency specific master keys and supports role based control to limit access to authorized Commonwealth personnel.

In addition, we offer full disk encryption using the McAfee Full Disk Encryption product. This software is available as a part of the Windows or Linux Server Configuration. We also offer McAfee Endpoint Encryption software that provides advanced data encryption and file encryption for desktops, laptops and removable storage devices. These additional encryption tools meet the current Commonwealth product standard STD-SEC020A, and will be used to encrypt disks or data as determined by the data classification activities described above.

In addition to data at rest, ITB-SEC031 provides encryption standards for data in transit, calling for AES data encryption with 256-bit keys through the use of encryption products that are certified through the NIST Cryptographic Module Validation Program. Data encryption is required based on guidelines found in ITB-SEC019 and whenever required by law. The Juniper firewall and VPN appliances proposed in our solution are FIPS 140-2 compliant that includes NIST validation in accordance with http://csrc.nist.gov/groups/STM/cmvp/validation.html. The NIST certification for the specific Juniper equipment FIPS 140-2 compliance can be viewed as follows (note that though the link indicates 140-1, the certificates are for 140-2):

- Juniper SRX 5800: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140crt/FIPS140ConsolidatedCertList0009.pdf.
- Juniper SRX 650: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140crt/FIPS140ConsolidatedCertList0016.pdf
- Juniper SRX 3600: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140crt/FIPS140ConsolidatedCertList0010.pdf
- The Juniper Pulse MAG4610 AES encryption to be used with VPN has been validated by NIST at http://csrc.nist.gov/groups/STM/cavp/documents/aes/aesval.html number 2553.

The Unisys team will work with agencies to determine the need and the method of encryption on a case-by-case basis within the guidelines of ITB-SEC019 and ITB-SEC031. Unisys will provide data center termination of AES encrypted tunnels using Juniper FIPS-2 NIST certified equipment in accordance with

the guidelines provided by ITB-SEC031 when necessary to meet requirements. Other means of end-to-end encryption such as HTTPS and the Unisys Stealth Solution™ product may mitigate the need for tunnel termination on Juniper equipment and will be used based on a collaborative assessment of the individual application requirements. Note that the Unisys Stealth Solution is an optional product in the Enterprise Services Catalog.

Note also that compliance with the encryption specified in ITB-SEC020 and ITB-SEC031 for an application is dependent on the capability of the application to create and/or use encrypted data. The Unisys Team will provide solutions to address infrastructure compliance with these ITBs, and will work with the agencies as they make application level changes for application compliance.

In summary, data protection starts with our baseline security risk and vulnerability assessment and remediation plan. We will implement DLP and DBFW solutions to identify, monitor and protect identified sensitive and confidential data in transit and data at rest. Based on the classification of the data and applicable governing policies and regulations, such as the Commonwealth ITBs ITB-SEC019, ITB-SEC020, and ITB-SEC031, specific appropriate measures will be taken to protect Commonwealth data including encryption as required to protect data at rest and in transit.

Clarification	*Text*
9.	*Please provide complete details on the Unisys Stealth SolutionTM, its capabilities, and proposed use in the Commonwealth.*

Unisys Response:

The Unisys Stealth Solution™ ("Stealth") is a certified software encryption solution that is designed to secure data-in-motion while at the same time organizing that data into virtualized, cloaked Communities of Interest (COIs) that can co-exist on a single network infrastructure without risk that one COI can see or access another COI. A COI is a group of users and devices (e.g., servers) that must share information. Using Stealth, Agencies and organizations can share a common infrastructure while their data is kept securely isolated from one another; selectively allowing users from other COIs access as needed. Management of COIs is easy with Stealth, as access is defined by user identity (or server device) rather than physical topology.

Stealth is a Multi-Domain hardware/software data protection product that allows data of multiple access levels to be processed without the need for discrete networks and redundant hardware, while maintaining logical separation of the data through the network. By using the Stealth product, separate external networks may be securely consolidated using cryptographic techniques over a single infrastructure deployment.

Stealth provides security by encrypting data using a FIPS 140-2 certified module that employs AES-256 encryption. Stealth is NSA Common Criteria certified at EAL4+ as a multi-domain solution.

Stealth cryptographically separates COIs within a common physical network. Data is protected in such a way that the isolation and containment of data for different COIs is enforced cryptographically. Stealth also optionally allows the Commonwealth or an agency to define "Clear Text COIs" – filters that allow given endpoints to use split tunneling to access both Stealth endpoints via encrypted tunnels as well as predefined unencrypted sites.

Stealth features endpoint software that is installed on client machines and servers to establish secure tunnels through the internal network or across external networks such as the Internet. Stealth Gateway appliances are also available to integrate separate external networks or devices that do not support the endpoint software (printers, third party appliances, etc.) into the internal encrypted network. One Gateway function, called the "Home Gateway" is used to integrate servers supporting the internal network processes such as DNS, Active Directory Domain Controller (DC) and the like. Each endpoint module (and Gateway appliance) utilizes the FIPS certified cryptographic software module to parse and encrypt traffic passed through the secure tunnels.

[redacted]

Stealth endpoint software can be currently installed on many IP based devices, such as Windows® and Linux PCs, servers, laptops, and Windows mobile tablets. Stealth endpoint software for other mobile OS devices is planned for future release. Each endpoint is assigned to a unique virtual COI. The end point encrypts all data leaving the device intended for transmission through a network to another Stealth endpoint in the same COI, where it is unencrypted.

The drawing below shows a representative overview of a number of endpoints and network elements with a set of COIs.

Authentication and Authorization

The Stealth client workstations use Windows based Active Directory or other LDAP-compatible directory services mechanisms (for Windows and Linux) to identify and authenticate users (using credentials as specified by the Commonwealth) prior to performing any functions. For the Commonwealth we assume we would use the existing CWOPA Active Directory, though that is not required.

The administrator's workstation performs identification and authentication using Windows domain or could use local Windows OS mechanisms if the Commonwealth prefers. It requires each user to be identified and authenticated prior to performing any functions, maintaining a local database of accounts or domain accounts including their identities, authentication information, group associations and privilege and logon rights associations for Stealth Administration.

Authorization Server

The Authorization Server ("Auth Server") software provides an interface between the Commonwealth's authentication service and the client endpoints, to automate the user COI assignment process during user logon.

The Auth Server presents a web interface and listens on Commonwealth-specified ports using either http or https protocols; this address is part of the client endpoint installation package. The Auth Server is called once user logon credentials have been verified and the user permitted to log on. The client Stealth endpoint then issues a web call to the Auth Server (via an encrypted tunnel created using the service key included as part of the client endpoint installation package) to search for user assigned certificates in the Windows Security Groups assigned to the user to see if the currently logging in user has any Stealth workgroup membership to be assigned. If this is successful, the new user keys are passed back to the client Stealth endpoint which toggles to the new workgroup keys for each COI the user is a member of.

Several instances of the Authorization Server can be configured and distributed throughout the enterprise to service user logon COI assignment. Once these are identified, the installation provisioning files populate the order and addresses of these servers for each endpoint to get user COI keys during logon processing.

Teaming

The Stealth appliances are designed to be used as teams presenting one virtual IP address for the teams. A team of one is allowed, but is only recommended for small pilots, not production. There can be as many as 255 appliances in a team and can support thousands of users and COI possibilities. The team is normally configured in an N+1 configuration, where N is the number of appliances needed to cover the desired concurrent license count or throughput, plus a hot spare (the +1). The hot spare will take over if any of the N appliances should fail in the team. Replacing the broken appliance requires loading the applicable configuration to the new appliance and adding it back into the team.

Stealth Secure Virtual Terminal (SSVT)

The Stealth Secure Virtual Terminal (SSVT) is a tamper-proof, partitioned USB form-factor Smartcard device with optional storage capability (the "SSVT stick") that will boot essentially any x86 PC using a hardened operating system, a locked-down browser, and a Stealth-secured undetectable tunnel. SSVT bypasses the operating system on the hard drive of the host system and does not interact with it in any way. Any malware on that system that might log keystrokes or connection details or might otherwise snoop on the data being exchanged cannot execute.

SSVT can be used for secure remote access to COPANET or the Datacenters for internal users, as well as securing high-risk transactions from external users. Once a user boots from the SSVT device, a secure AES-256 encrypted tunnel is established to COPANET or the Datacenters. Based on individual user credentials and the implemented configuration, the user would be allowed to access:

a. Web enabled applications (typically the only option for external users)

b. An existing desktop within the agency via a Remote Desktop Protocol (RDP) session (the user's own desktop or a shared remote access kiosk)

c. A virtual desktop through VDI (such as VMware View or Citrix XenDesktop)

For both internal and external users, SSVT communications can lock the communications channel to pre-defined, targeted endpoints (normally a defined set of web sites). Access is only permitted to the targeted endpoints (normally via web browsing).

Other distinguishing features of the SSVT stick include:

- Requires password at boot to provide two-factor authentication (password plus the SSVT device)
- The SSVT image stored on the tamper-proof partition of the USB device cannot be corrupted
- For additional protection, the SSVT image is verified at every boot
- Both Linux and Windows-based SSVT devices are available
- SSVT sticks can be manufactured to be fully read-only, or can include both the read-only bootable partition and a writable partition for saving documents downloaded from the allowed sites
- SSVT sticks are tamper evident, tied to individual users, and serial-numbered for loss/theft management, PIN recovery and rapid turn off.

Technology

The Stealth technology is implemented as an NDIS 5 Intermediate Filter driver or an NDIS 6 Lightweight Filter driver. This allows the Unisys Stealth Solution driver to process all network packets as they traverse the network stack. This gives Stealth the ability to apply the rules, filters and cryptology that have been defined for that endpoint based on the Identity that has been assigned to that endpoint. In addition, the Stealth drivers drop all packets that are not expected (i.e., either Stealth packets or packets from IP addresses matching CLEAR-Text filters on this endpoint). Thus, the device will be obscured from those attempting to discover it via scanning.

Reporting

The Unisys Stealth Solution reports audit events for the health and welfare of each endpoint and the gateway appliances. In addition to their gateway functions, the gateway appliances act as licensing authorities for the installed enclave and record endpoint activity such as successful COI tunnel creation between two endpoints or failed attempts to join a COI that could be an endpoint under attack.

Common Use Cases

Unisys has identified a number of common use cases where Stealth provides value. Of particular importance to the Commonwealth are the following:

- Unisys Stealth Solution for Data Center Segmentation – allows the Commonwealth or an agency to flatten out the physical network infrastructure and use COIs to provide secure separation between application suites as well as between zones. Also enables restricting access to applications via client-side COIs.

- Unisys Stealth Solution for Secure Remote Access – provides the Commonwealth or an agency with secure access for external users, extending the benefits of COI separation to external users.

- Unisys Stealth Solution for Secure Virtual Terminal (SSVT) – as a special case of Secure Remote Access, SSVT provides high confidence that a user's desktop is free from malware when executing high-value/high-risk transactions.

- Unisys Stealth Solution for Regional Isolation – provides highly secure site-to-site connections.

- Stealth technology is currently being used by several organizations to protect their sensitive communications, including secure government agencies like the Coast Guard and private sector companies like Hertz (NZ). The table below includes some of the areas identified in the Response as optional uses of Stealth technology, as well as some other possibilities:

Section	Item	How Met
3.1.2 Network and Security Architecture	6.A Secure Network Connectivity between Datacenters	Juniper VPN with Unisys Stealth Solution for Regional Isolation as an option
3.1.2 Network and Security Architecture	6.B Secure Network Connectivity from the Internet	Juniper VPN with Unisys Stealth Solution for Secure Remote Access as an option
3.1.3 Datacenter Architecture and Technology	2.B.4 Security Zones	Juniper Firewall with Unisys Stealth Solution for Data Center Segmentation as an option
–	–	PSP external users optionally use Stealth Secure Remote Access to access Agency applications via the Internet

To meet the requirements of this RFP, Unisys proposed Juniper firewall and VPN using the Juniper FIPS 140-2 certified encryption module. The Unisys Stealth Solution is not required to meet any of the security requirements of the RFP. It is included in the Enterprise Services Catalog as an option for the Commonwealth to use when the Commonwealth determines it is appropriate; some possibilities are suggested in the table above.

Clarification	*Text*
10.	*If the Commonwealth does not accept the use of Stealth, how will Unisys meet the security requirements of the RFP?*

Unisys Response:

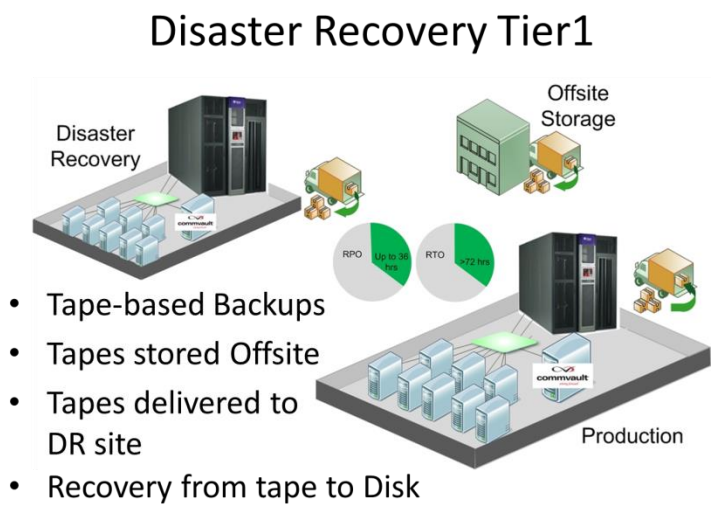
The Unisys Stealth Solution is not required to meet any of the security requirements of the RFP. It is included in the Enterprise Services Catalog as an option for the Commonwealth to use when the Commonwealth determines it is appropriate; some possibilities are suggested in the table at the end of the answer to Question 9 above. .

We will meet the requirements of the RFP by employing the Juniper Firewall and VPN using the Juniper FIPS 140-2 certified encryption module, which is included in the proposed data center configuration.

Clarification	*Text*
11.	*Please provide clarification on the Disaster Recovery tiers listed in Schedule F (pages 63-64) of the proposal, including detailed information on how Unisys will provide Disaster Recovery for application or component level disasters.*

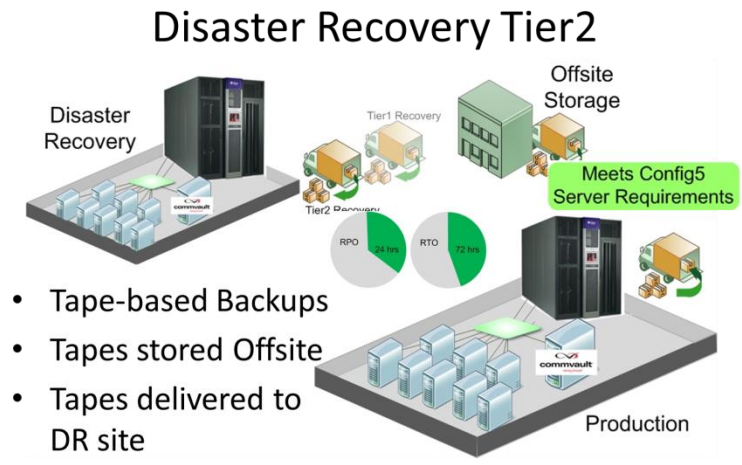
Unisys Response:

All of the Disaster Recovery tiers provided in the Unisys solution offer the Commonwealth and its agencies the means to achieve business continuity following a disaster of sufficient magnitude to render a data center incapable of providing required services. The tools that provide these disaster recovery services can also be implemented to provide recovery from application or component level disasters.



Tier 1

Tier 1 Disaster Recovery services provide tape-based disaster recovery that is initiated after all services protected with Tier 2 tape-based Disaster Recovery services have been restored. This level of service provides a means for agencies to protect and restore non-critical applications following a disaster declaration for a data center. The recovery point objective (RPO) is based on the nightly cycle of writing data to tapes. The recovery time objective (RTO) may exceed 72 hours given that the Tier1 recoveries do not begin until Tier2 recoveries were completed.



Tier 2

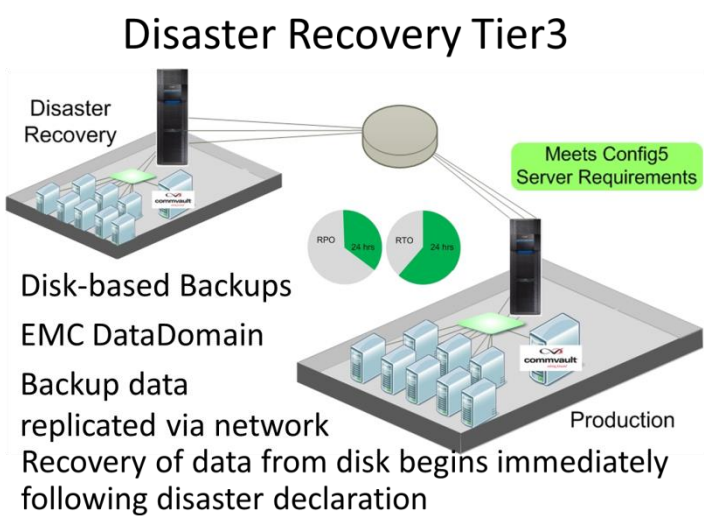
Tier 2 Disaster Recovery services provide tape-based disaster recovery that is initiated upon declaration of data center disaster. This level of service provides a means for agencies to protect and restore applications which support business processes that could reasonably withstand an outage of no more than 72 hours, the stated RTO for this level

of service. The recovery point objective (RPO) is based on the nightly cycle of writing data to tapes. On balance, the Unisys solution provides a greater number of tape drives in DR than in production for data protected by Tier 2 DR services in order to meet the 72-hour RTO. This is because the full backup of Tier 2-protected data can be spread over a week's time with incremental backups during Production cycles but the restore must be completed within no more than 3 days.

The Backup technology provided for tape-based backups in the production environment will be used for restores whenever a limited application or component level disaster occurs that does not necessitate invocation of a full data center disaster recovery declaration. These more limited restore activities can be prioritized above normal backup operations.

Tier 3

Tier3 Disaster Recovery services rely upon backups to EMC's disk-based technologies such as DataDomain to provide an RPO based on the nightly cycle of writing backup data to disks and an accelerated RTO of no more than 24 hours. The backup data is replicated to the Disaster Recovery site as it is written to the DataDomain storage in the production site. Upon declaration of a disaster, the restore process begins immediately at the Disaster Recovery site. These restores are initiated remotely by the Unisys DR team and complete within 24 hours.

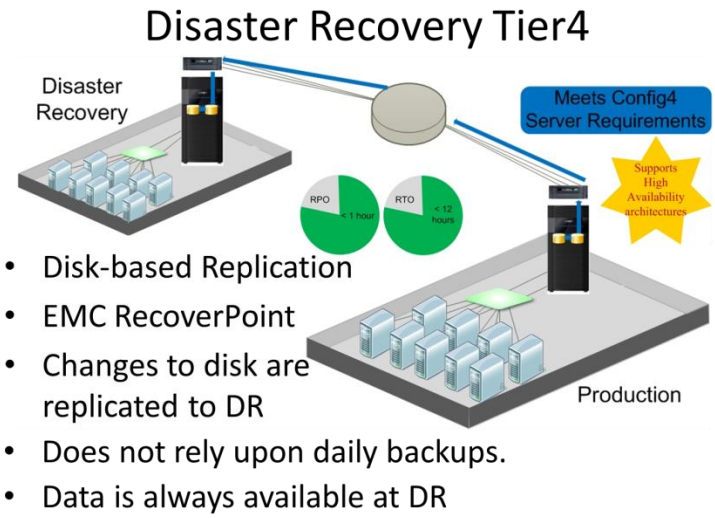


As with Tier 1 and Tier 2 services which also rely upon backup services, the production-based backup-to-disk DataDomain infrastructure is available for restores whenever a limited application or component level disaster occurs that does not necessitate invocation of a full data center disaster recovery declaration. However, the disk-based restores in production are also initiated much more quickly than tape-based restores because the backed-up data remains at the production data center and does not require the recall of data from offsite storage locations.

Tier 4

Tier 4 Disaster Recovery services meet the minimum requirements specified for Config-4 servers. The Tier 4 services rely upon asynchronous disk-to-disk replication of data between the production and Disaster Recovery sites. The RPO for this service is, at most, 1 hour. Unisys manages the network capacity to provide replication of all data in a cost-effective manner to insure that at maximum data change peaks that replication does not exceed 1 hour. The storage replication tools include caching mechanisms so that, when required, replication achieves the highest network

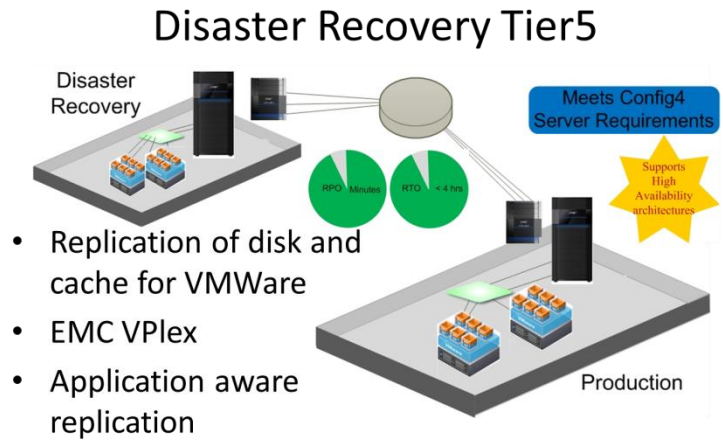
utilization possible. The RTO for this service is no more than 12 hours. As the Unisys DR team has demonstrated in the past, Unisys expects to improve upon the initial RTO by implementing automation steps following successive tests of the DR processes.



As described in Question 5 above, the EMC RecoverPoint replication tool that forms the basis of x86 and Unisys mainframe storage replication can be integrated with Commonwealth application development to include application determined quiesce points so that the recovery provides a data set that is consistent at the application level. The EMC RecoverPoint can also be configured to provide local recovery to the production data center site in order to recover from limited application or component level disasters. The EMC RecoverPoint tool can also be selected from the Enterprise Services Catalog to provide full local copies of SAN-based storage in alternate frames to provide, where needed, an RPO of within seconds.

<u>Tier 5</u>

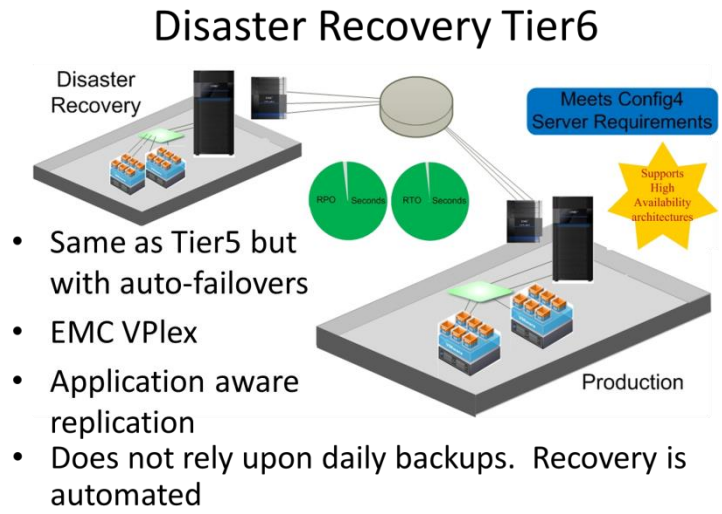
Tier 5 Disaster Recovery services are available for the VMWare-based virtual servers. This is an elevated tier of service. The EMC VNX storage solution that underpins the Unisys storage service for VMWare can be combined with EMC's VPlex technology to provide the foundation VMWare High Availability, VMotion Distributed Resource Scheduler (DRS) and VMWare Fault Tolerance (FT) over distance. The RPO is determined by transfers between the production site and the Disaster Recovery site. The RTO is no more than 4 hours and is largely governed by a re-configuration of the network properties at the Disaster Recovery site which Unisys would expect to automate over time.



This high availability Disaster Recovery/Business Continuity service provides the service resiliency that the Commonwealth may require for emergency services and other highly critical services. The premise of this

service is to provide clustering capability across distances for the Commonwealth.

As with the EMC RecoverPoint tool, EMC's VPlex infrastructure can also be configured to provide high availability services within the production data center. Thus, the Commonwealth can configure clustering within a production data center that delivers an RPO with no lost transactions and an RTO in the range of microseconds. Configured in this manner the Commonwealth may receive full business continuity for the most highly critical applications regardless of local component failures.



Tier 6

Tier 6 Disaster Recovery services are based on the tools and infrastructure detailed in Tier 5 Disaster Recovery services. The primary difference is that the IT Risk Manager and the agency directors determine a degree of automation to insert into the infrastructure so that Disaster Recovery services can be invoked automatically under pre-determined conditions.

As described for Tier 5 above, automation is already included when the Tier 5 or Tier 6 Disaster Recovery service is configured to provide disaster recovery services and clustering capabilities within the production data center.

Clarification	*Text*
12.	*Please provide details on the Security Operations Center(s) described in Schedule F of the proposal, including but not limited to, where the Security Operations Center(s) will be located.*

Unisys Response:

The Unisys Team Operations Centers – Network, Console, and Security – will maintain primary locations within [redacted]. To provide redundancy, the [redacted] will provide the off-hours and emergency alternate location, when required. In addition, each data center facility also maintains facility security and facility network operations centers that can support the primary Security Operations team in the [redacted], as required.

Clarification	*Text*
13.	*Page 641 of the proposal states "We will perform the rogue device discovery will be performed on the data center network that supports up to 2,000 data center servers." Please confirm the above statement should read "We will perform rogue device discovery on the data center network that supports up to 2,000 data center servers." Please provide the reason for the limitation of up to 2,000 data center servers.*

Unisys Response:

The Unisys Team will perform the rogue device discovery on up to 50 Class C IP address ranges within the Commonwealth data center network supporting a total of 2,000 servers.

Description of This Service

As part of this service, the Unisys team performs an analysis on the data center IT infrastructure to identify if the devices exhibit rogue or stealth-like characteristics. This process includes analysis of the Network Dynamic Host Configuration Protocol (DHCP) and Address Resolution Protocol (ARP)/Content Addressable Memory (CAM) data from the data center's core network switches supporting critical datacenter servers.

Frequency of This Service

The Unisys team performs this service quarterly and documents the results as part of the Deliverable #D-07.03 (Security Management Plan).

Scope of This Service

As part of the recurring quarterly assessment, the Unisys team will work with the Commonwealth to identify a representative sample of the data center network segments on a rotational basis. As part of the selection process, the Unisys team helps identify 50 Class C segments supporting up to a total of 2,000 servers that establishes a representative sample of the breadth in Commonwealth IT infrastructure. The selection criteria include:

- Business criticality of data managed
- Regulatory impact
- Additional factors such as public, business partner or private facing network segments, De-Militarized Zone (DMZ) and network segments interfacing with federal systems.

Clarification	*Text*
14.	*How does Unisys propose to secure remote admin access to Commonwealth systems and does Unisys' proposed solution provide multi-factor authentication?*

Unisys Response:

Unisys has proposed Citrix Xenapp Platinum Edition to support secure remote administrator access for Unisys system administrators including partners, and to control access to Commonwealth systems. This solution has multi-factor authentication and complete logging of all activity in order to provide the Commonwealth with a secure solution for remote administration.

The two-factor authentication supports XenApp's VPN and authentication service. Two-factor authentication uses Active Directory including role-based definitions for the first factor and SecureAuth's certificate and pin based technology for the second factor.

Clarification	*Text*
15.	*Please confirm that Unisys' solution addresses the Commonwealth's requirement that Service Request, Incident Management, Problem Management, Change Management incident\requests are initiated in the Commonwealth ITSM system. Unisys' solution must also interface with the Commonwealth ITSM system and exchange data. Unisys' solution must be able to initiate and pass data to the Commonwealth ITSM system in event a request is initiated on Unisys' solution. Please clarify when these processes will be automated and online for Commonwealth use.*

Unisys Response:

To confirm the requirement that Service Request, Incident Management, Problem Management, Change Management incident\requests are initiated in the Commonwealth ITSM system Unisys has proposed synchronizing the Unisys and Commonwealth ITSM systems bi-directionally on a frequency basis that is to be determined in transition. Unisys plans to utilize the BMC Remedy Distributed Server Option (DSO) to synchronize the two Remedy Systems for all major transactions and data including:

- Service Requests
- Incident Tickets/Data
- Problem Tickets/Data
- Change Tickets/Data
- Configuration Information (CMDB)

Transactions for the above can originate from either ITSM platform as our solution supports bi-directional synchronization of transactions. Bi-directional replication of data is to be scheduled on a frequent basis and the intervals are to be determined during Transition.

To synchronize data bi-directionally and successfully, the solution may be dependent upon the Commonwealth making some changes to its ITSM System to accommodate the synchronization approach.

If the Commonwealth decides to move to ServiceNow Unisys will use a different replication technology that we current use for other ServiceNow implementations. The net effect is the same as it will still be a bi-directional synchronization of the data between the two systems.

Unisys is committed to complete the synchronization of the Unisys and Commonwealth ITSM Systems for Commonwealth and Unisys use within the first six months of the contract effective date.

Delivering the Future of IT

Services that Empower Government. Innovation that Serves Citizens.

UNISYS RESPONSE TO
COMMONWEALTH OF PENNSYLVANIA

Oral Presentation
July 29, 2013

UNISYS

Delivering the Future of IT

Services that Empower Government. Innovation that Serves Citizens.

Opening Remarks

[redacted] – Unisys Chief Executive Officer

UNISYS

Delivering the Future of IT

Services that Empower Government. Innovation that Serves Citizens.

Company and Program Overview

[redacted] – Engagement Executive

Recognize and respect differences among individual agencies

We must recognize that agencies will have their autonomy to execute their business goals while assisting the Office of Administration with achieving its enterprise objectives.

UNISYS

Oral Presentation Agenda

Agenda Item	Speaker	Time
Opening Remarks	[redacted]	5
Company and Program Overview	[redacted]	15
Compute Architecture Overview	[redacted]	25
Security Overview	[redacted]	25
Network Connectivity Overview	[redacted]	5
Disaster Recovery	[redacted]	7
Transition Methodology	[redacted]	20
Service Delivery Overview	[redacted]	7
Support, Incident and SLA Overview	[redacted]	10
Closing Remarks	[redacted]	1
Questions and Answers		30

UNISYS

© 2013 Unisys Corporation. All rights reserved.

Meet the Unisys Team

© 2013 Unisys Corporation. All rights reserved.

Meet the Unisys Team

IBM

- A valued partner on the DPH contract and long-term partner to many Commonwealth agencies
- IBM provides over 90% of technology in use in agency data centers

Deloitte

- Largest provider of Application Integration and Support as well as Security services to the Commonwealth
- National State Security practice is based in Harrisburg, PA

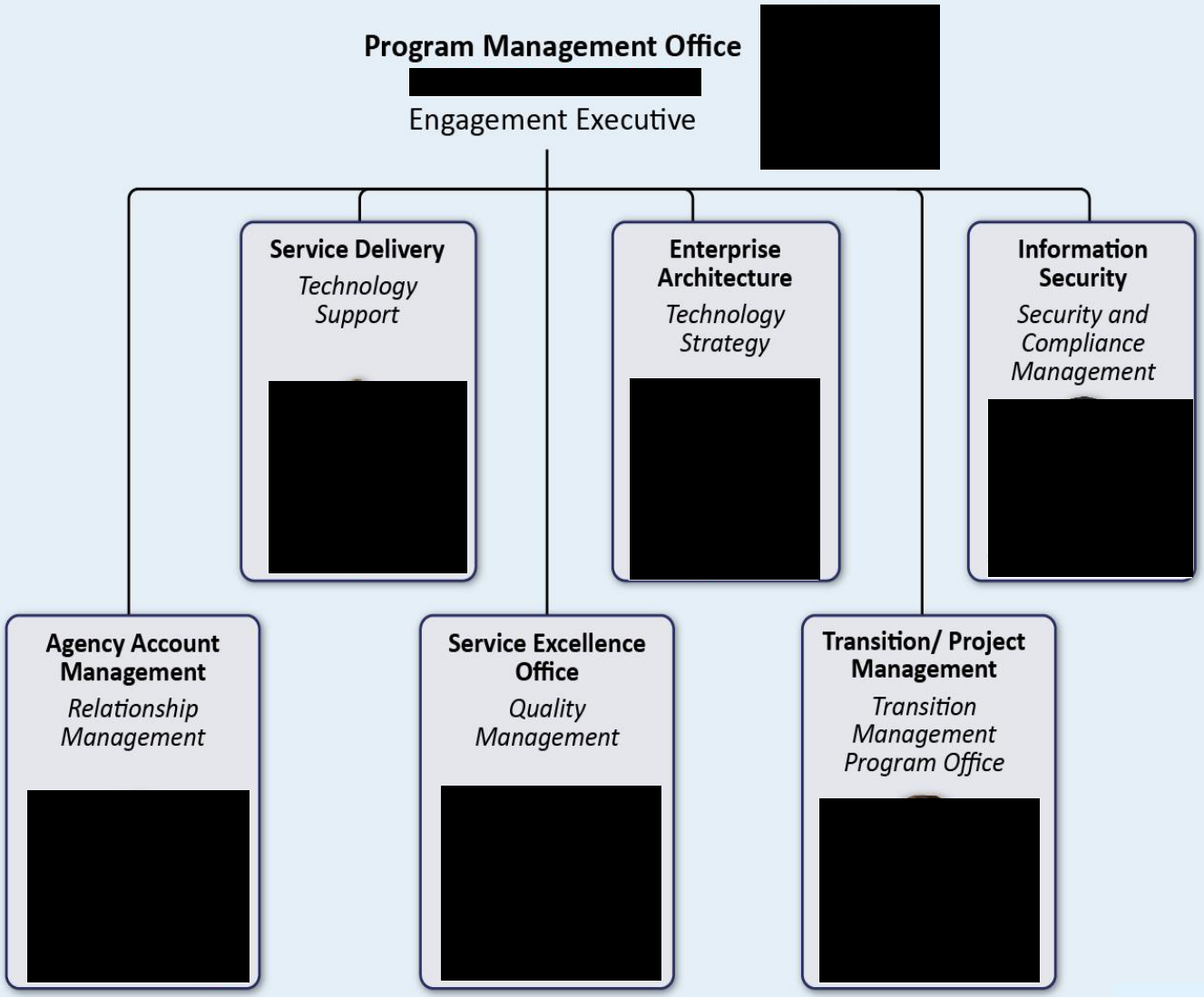
Small Diverse Businesses

- 11 partners providing various services in their areas of expertise
- Commonwealth experience

UNISYS

© 2013 Unisys Corporation. All rights reserved.

Data Center Compute Services Key Personnel



- 28 Key Personnel
- Harrisburg based
- 23 assigned to Commonwealth projects today
- 100% Dedicated
- Experienced leaders
- Growing PA jobs

UNISYS

© 2013 Unisys Corporation. All rights reserved.

Key Personnel Details

Key Personnel Booklet

- Name
- Position in the Organization
- Proposed Role on Project
- Experience in the Proposed Role
- Qualifications for the Proposed Role
- Percentage of time Dedicated to the Project

Name	Proposed Account Role	Position in Organization	Experience in Proposed Role
Role on last 3 projects		**Qualifications for Proposed Role**	
[redacted]	Engagement Executive	Engagement Executive	15 years
• Unisys, DPH Engagement Executive (2 years) DPH Service Delivery Director (2 years) DPH Chief Technologist (1 year) • Cegedigm-Dendrite, Vice President, Technical Services (10 years) • Electronic Data Systems, Operations Manager (11 years)		• 15 years managing high-quality, large-scale outsourcing programs with extremely high SLA achievement and customer satisfaction • ITIL V3 Foundation Certified • Established Commonwealth leader with 5 years of experience managing the DPH contract, including the 2008 Transformation • 26 years managing programs with complex Data Center Services transitions, including data center facility design, consolidations, and physical and logical data center migrations • Laser focused on driving organizations to continually improve service level performance and customer satisfaction	
100% Dedicated to the Commonwealth Data Center Computing Services Project			

UNISYS

© 2013 Unisys Corporation. All rights reserved.

Unisys Team Foundational Tenets

Unisys and the Commonwealth… Driving Technology for over 50 Years

- Commonwealth applications are **critical** to citizens
- **Innovation** is a must
- Recognize and **respect differences** among individual agencies
- **Align compute services** with the business
- **Managing change** is key to success
- **Security** is paramount
- Focus on **moving applications** rather than moving hardware
- **Flexibility** and **transparency**
- Achieve success **together**
- Do **no harm** – no unplanned service interruptions

© 2013 Unisys Corporation. All rights reserved.

Why choose the Unisys Team?

- **Our team's collective knowledge of the Commonwealth**
- We have a proven record of success over many years of service delivery to Commonwealth agencies
- We have brought innovation to the Commonwealth
- We offer the lowest risk and minimal ramp-up

© 2013 Unisys Corporation. All rights reserved.

Delivering the Future of Computing Architecture

New Models that Drive Efficiency. Experience that Empowers Success.

Compute Architecture Overview

[redacted] – Senior Enterprise Infrastructure Architect

Align compute services with the business

Our proposed solution must provide a transparent and flexible compute services environment aligned with the business needs of the agencies.

UNISYS

An Innovative Architecture

- Flexible
- Secure
- Stable
- Integrated
- Proactive

UNISYS

© 2013 Unisys Corporation. All rights reserved.

Data Center Architecture

Provides the Commonwealth No Single Point of Failure

- Exhaustive search to find a leading data center facility close to Harrisburg versus simply moving all your workloads to existing facilities outside a 100 mile radius.
- Designed to mitigate potential application latency issues
- Provide geo-separation for DR needs
- Each facility supports Production, Test, Dev, DR, Capacity on Demand, Colocation
- Single virtual command center with the primary function being in Harrisburg

UNISYS

© 2013 Unisys Corporation. All rights reserved.

Unisys [redacted] Facility

Located Close to Harrisburg to Minimize Risk

- Location relative to Harrisburg mitigates potential application latency issues
- All workloads from the DPH will move here to minimize application connectivity and interface issues, and efficiently migrate tightly coupled applications

[redacted]

[redacted]

UNISYS

© 2013 Unisys Corporation. All rights reserved.

Unisys [redacted] Facility

Chosen to Provide Geographical Workload Distribution

- Home of many mission critical applications and Public Sector clients
- SSAE-16, ISO 27000, and 9001 certified
- Dedicated computer room with separate secured access
- Two factor physical access
- Multiple carrier access
- LEED certified and award winner

UNISYS

© 2013 Unisys Corporation. All rights reserved.

Commonwealth EDC Facility

Take over in place to provide stability

- Maintain as-is to minimize disruption of existing workloads and network connections
  - COPANET
  - PennDOT
  - Web Services
- Introduce Capacity-on-Demand capabilities to support scalability
- Transition within six months to take over operations support
- Provide a gap analysis and action plan for the facility

UNISYS

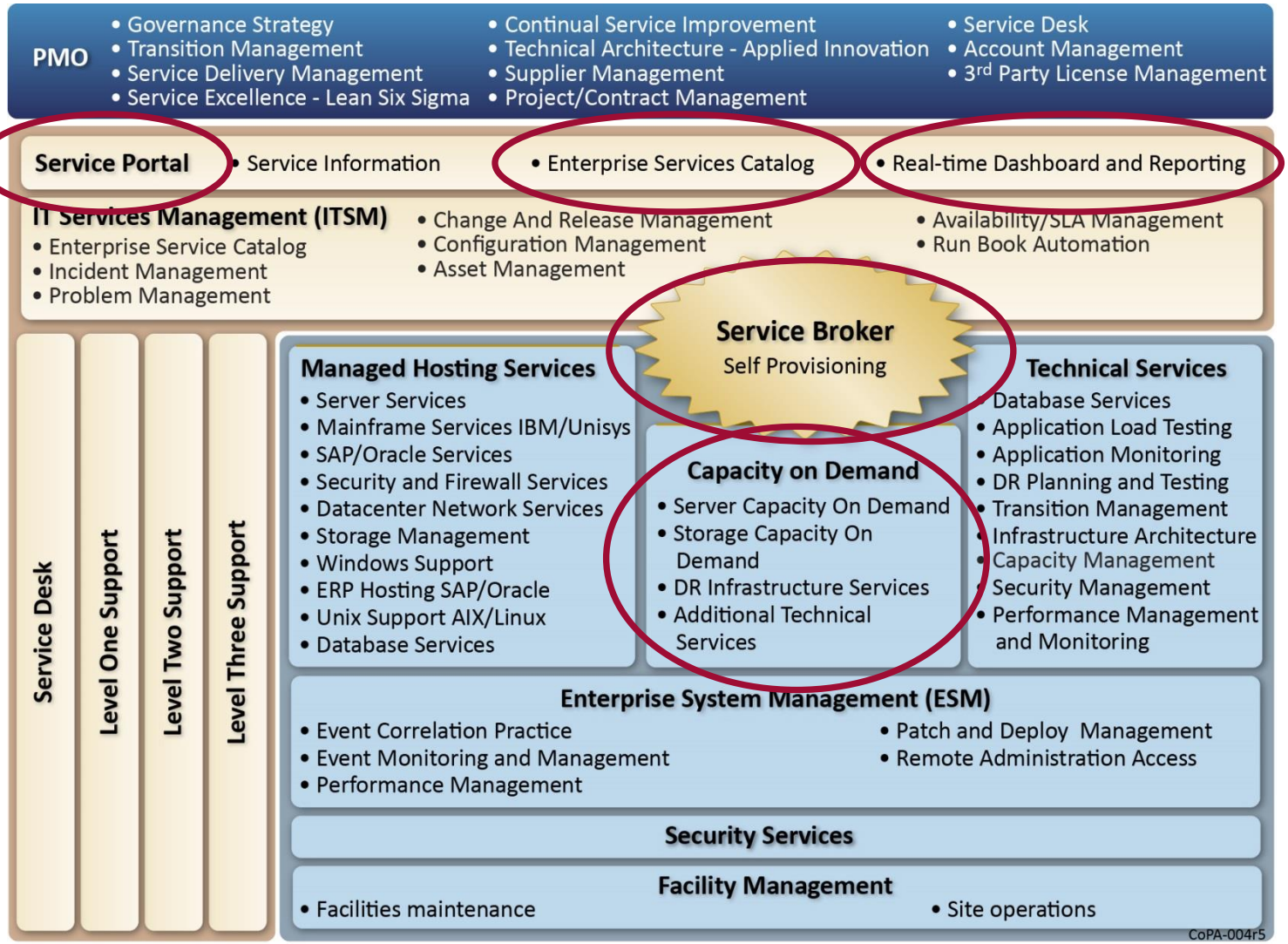
© 2013 Unisys Corporation. All rights reserved.

[redacted]

UNISYS

Integrated Component Architecture

Providing the Model to Support the Commonwealth's Vision



© 2013 Unisys Corporation. All rights reserved.

Services Portal

Providing the Commonwealth a central interface for service engagement

- Central Point for all interaction and information
- Separate instance per agency to provide autonomy and role-based access
- Submit a Request for Service using the Enterprise Service Catalog
- Submit an incident and receive up-to-date status
- View predictive performance indicators
- Search knowledgebase

© 2013 Unisys Corporation. All rights reserved.

Enterprise Services Catalog

Simplifying and Speeding the Service Request Process

- Configurable by agency and role
- Automated Request for Service process
- Configurations included in Schedule I will be in the catalog upon release
- On-line shopping method
- Automated approval process
- Approved orders are submitted to Change Management for approval to provision into service
- Billing on a monthly interval by agency and resource type

© 2013 Unisys Corporation. All rights reserved.

Dashboards and Reporting

Provides Commonwealth a Comprehensive View

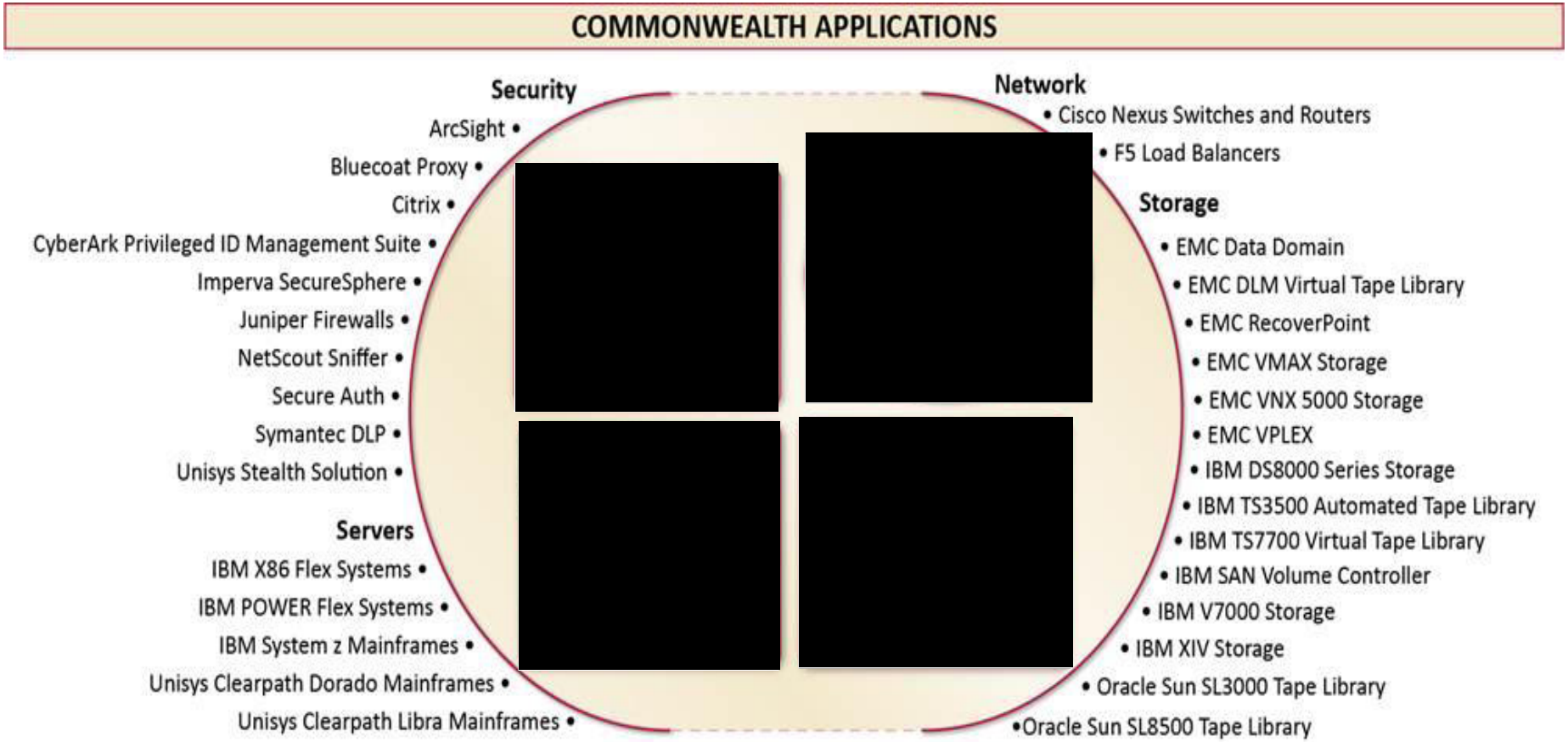
- Configurable by agency and by role
- Proactive metrics to establish a green, yellow, red performance methodology
- Provides near real-time status
- Viewable on mobile devices
- Provides ability to track many types of metrics as long as a data source of metrics can be established

UNISYS

© 2013 Unisys Corporation. All rights reserved.

Managed Hosting Services

Technology Supporting Commonwealth Applications



Maintaining majority of existing technology to eliminate application compatibility issues

UNISYS

© 2013 Unisys Corporation. All rights reserved.

Managed Hosting Services

Common Blade Architecture to Support all Operating Systems

- Move to IBM Flex Systems common blade architecture that supports all distributed operating systems in scope
- Optimizes capacity utilization
- Simplifies self-provisioning
- Provides a central point of management for the physical infrastructure
- Integrates storage seamlessly
- Optimizes space utilization in the data center

UNISYS

© 2013 Unisys Corporation. All rights reserved.

Service Broker

Providing Automated Provisioning of Resources

- Automated runbooks are executed from an approved change to provision and de-provision services automatically
- After provisioning is complete, CMDB is automatically updated
- Agencies can develop their own runbooks to automatically provision application workloads
- Can provision DR workloads in a sequenced manner

UNISYS

© 2013 Unisys Corporation. All rights reserved.

Capacity on Demand

Providing business value by providing resources when needed

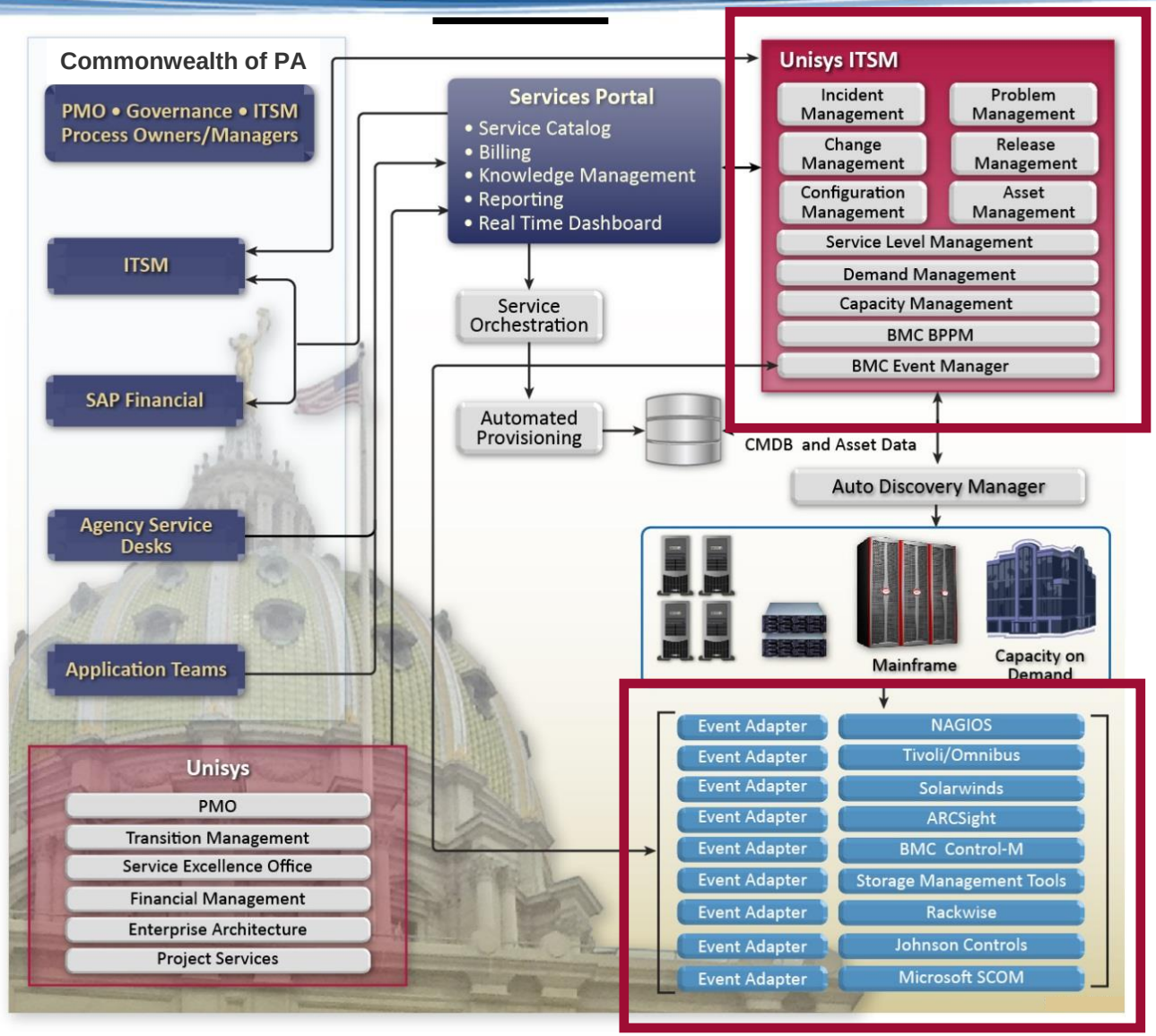
- Available in all three data centers
- Can be provisioned for scale up during disasters, testing, application trouble shooting, and more
- Transparent pricing

UNISYS

© 2013 Unisys Corporation. All rights reserved.

Integrated Service Management

Provides a consistent delivery of services



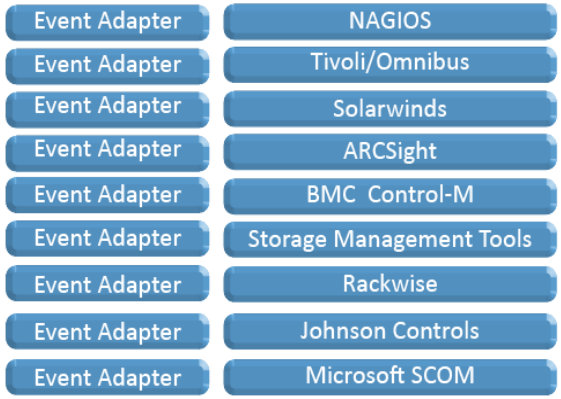
UNISYS

© 2013 Unisys Corporation. All rights reserved.

Integrated Service Management

Provides a consistent delivery of services

- Central engagement point for Commonwealth IT professionals and Unisys Service Delivery staff
- Separate instance for each agency to provide autonomy
- Integrated with the Services Portal and Dashboards to provide an easy to use interface to use the platform
- All single event managers tree up to an event correlation engine to isolate the root event
- Root event will auto create an incident that will be auto-routed to the right skill and support level
- Within the incident ticket, the CMDB relationship tree is visible to determine service impact



UNISYS

© 2013 Unisys Corporation. All rights reserved.

Creating a Comprehensive CMDB

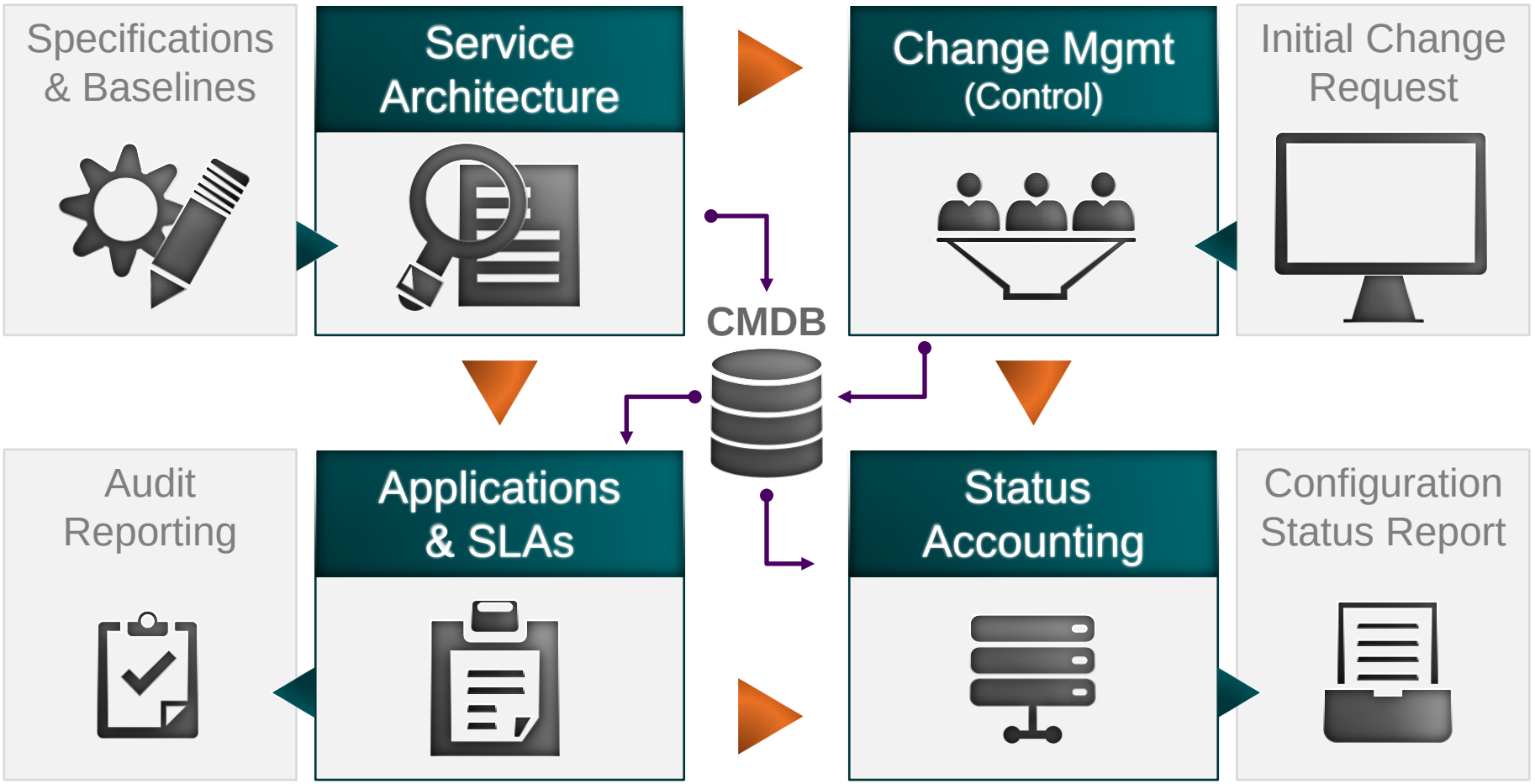
Knowing the interdependencies between application and infrastructure items

- Auto-discovery of application and infrastructure items and their associated relationships
- Once relationships are built from the service tier to the infrastructure component level:
  - Proactive Service Impact can be obtained
  - Change Impact can be performed to determine effect on tightly integrated applications to minimize failed changes
- Provides basis to perform effective event correlation to suppress false events and incident tickets
- Can include relationships to users and locations
- Includes asset information

UNISYS

© 2013 Unisys Corporation. All rights reserved.

Day in the Life of a CMDB



© 2013 Unisys Corporation. All rights reserved.

Key Elements

- Multi data center design
- Proven technologies
- On Demand Services
- Integrated Services Management

© 2013 Unisys Corporation. All rights reserved.

Delivering the Future of Security

Proactive Frameworks to Safeguard Your Assets, People and Citizens

Security Overview

[redacted] CISSP – Security Manager

Security is paramount

We must encapsulate everything we do with a strong security framework that protects all Commonwealth data and IT resources.

UNISYS

Guiding Design Principles

- Integrated Security Risk Framework
  - Reduce risk
  - Unified across Agencies and Data Centers
  - Improve security consistency
- Meet Diverse Regulatory Requirements
  - CJIS, CHRIA for criminal justice
  - HIPAA for health-related
  - IRS 1075, SSA, PCI-DSS for financial
  - Commonwealth ITBs across the board
- Collaboration

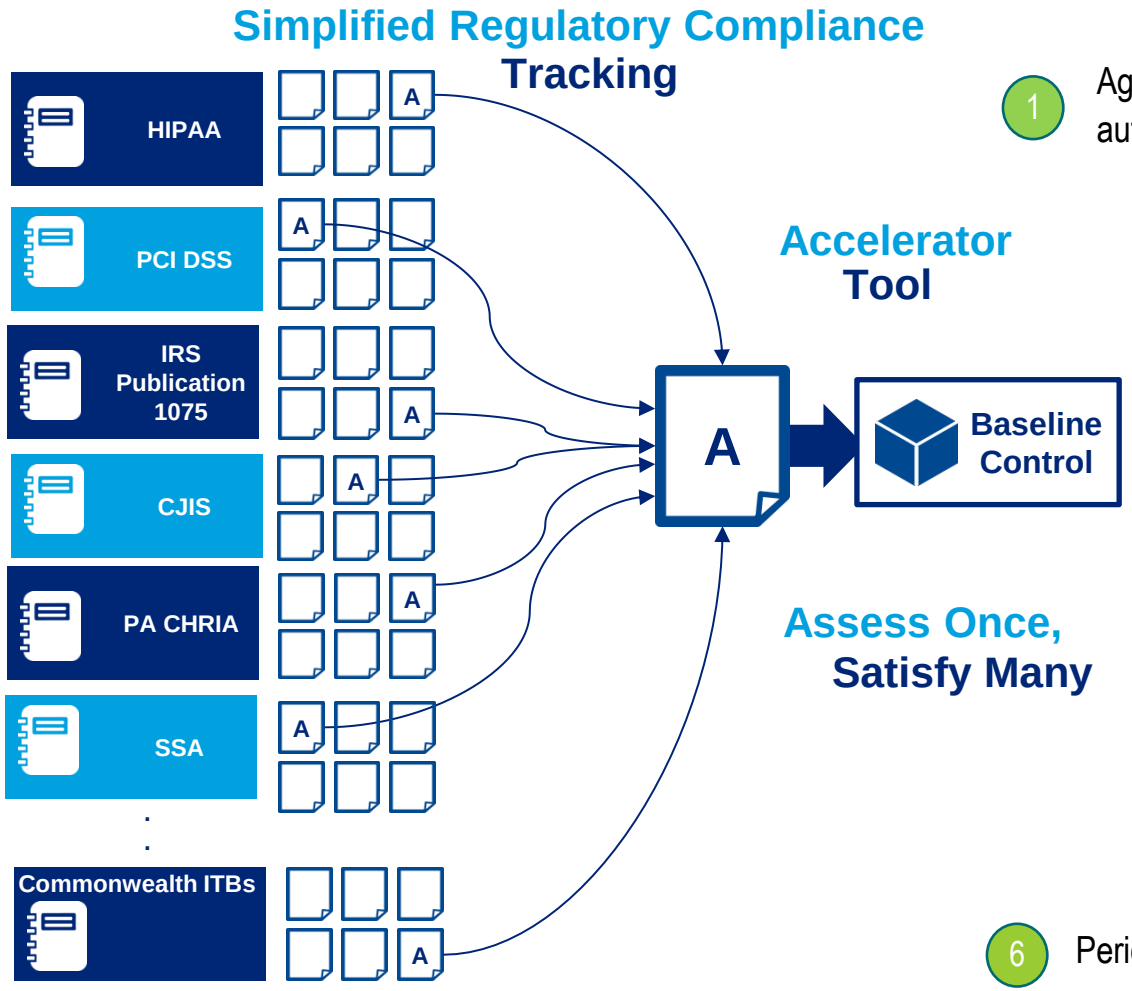
© 2013 Unisys Corporation. All rights reserved.

Security Solution

- One Unified Data Center Security Plan
  - Details vary by Agency, but the plan is common
  - Details vary by data center, but the plan is common
  - Provide both logical and physical security
- Transition Services
  - Establish the Framework
    - Initial security plan
    - Baseline assessment
- Ongoing Operations

© 2013 Unisys Corporation. All rights reserved.

Establishing a Regulatory Compliant Data Center

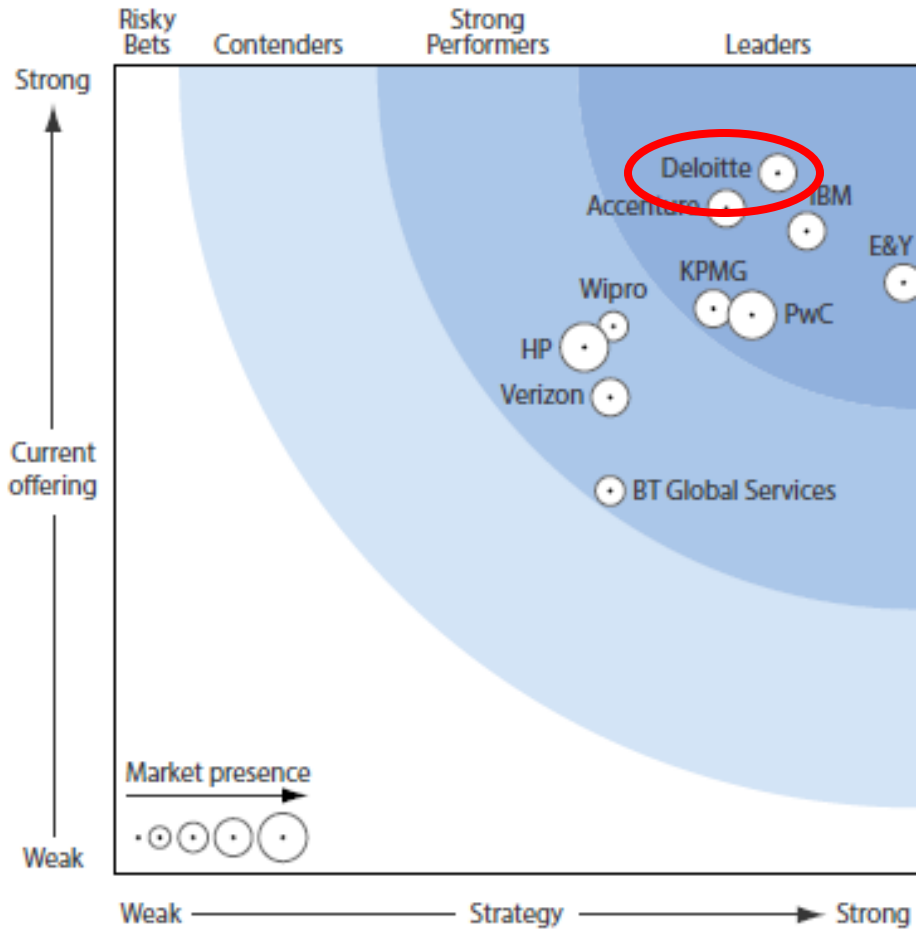


1. Agency workshops to perform Data Classification; automated tools identify existing PII
2. Understand each agency's regulatory requirements and document the Security Risk Framework
3. Document Initial Security Plan
4. Baseline security risk and vulnerability assessments; identify gaps by agency; prioritize mitigation steps
5. Establish prioritized mitigation controls for gaps identified
6. Periodic review and update of data center security plan

UNISYS

© 2013 Unisys Corporation. All rights reserved.

Deloitte is a Leader in Information Security Consulting



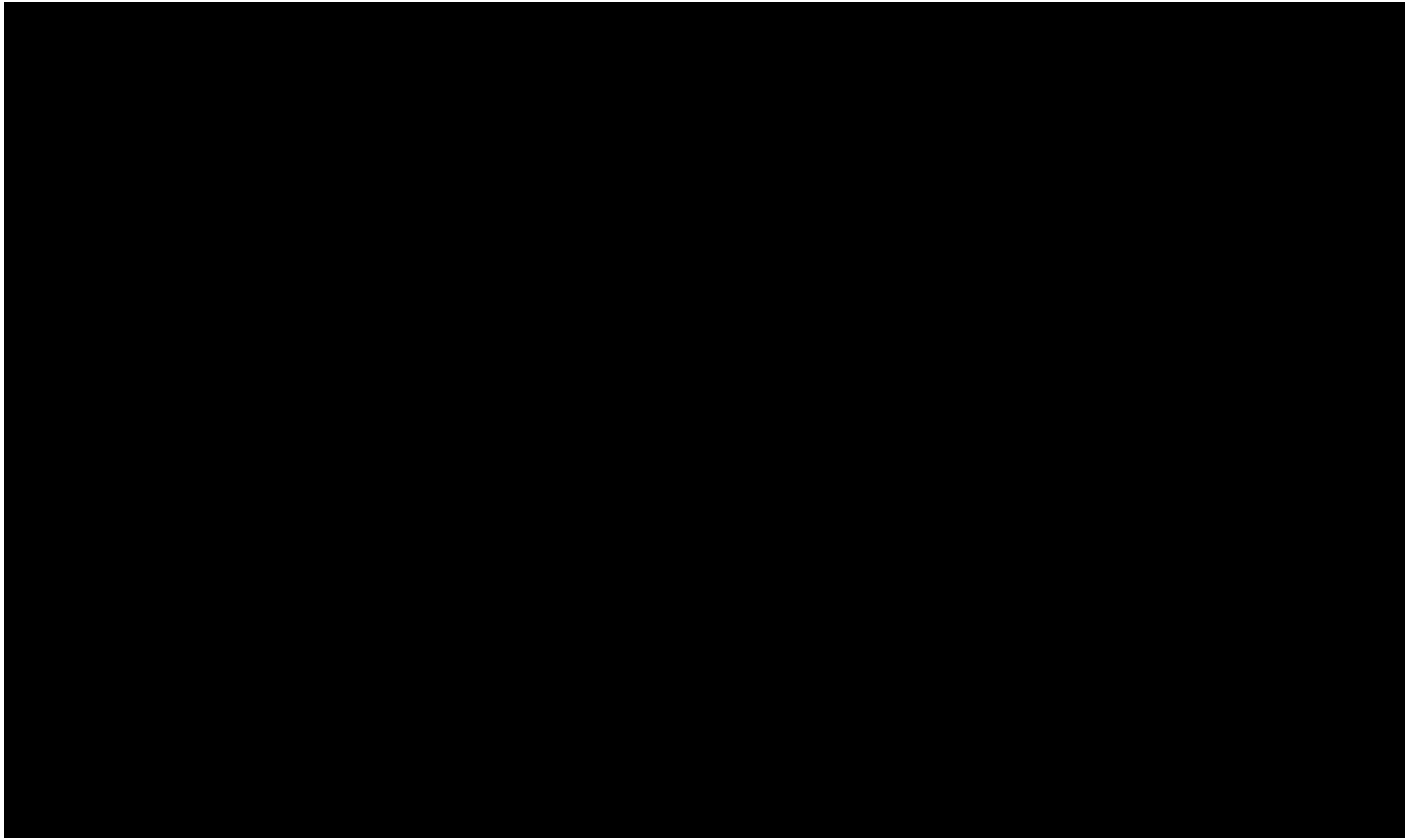
Forrester Research, Forrester Wave™: Information Security Consulting Services Q1 2013", Ed Ferrara and Andrew Rose, February 1, 2013

"One reason Deloitte succeeds against the four other top firms is that its global delivery network is the largest and **most mature** compared with those firms." – Gartner, Security Consulting 2012

- **Srini Subramanian:**
  - **Leads Deloitte National State Security Practice**
  - **Part of NGA's State Cyber Security Policy Council**
  - **Based in Harrisburg**

© 2013 Unisys Corporation. All rights reserved.

Approach to Security Regulatory Compliance



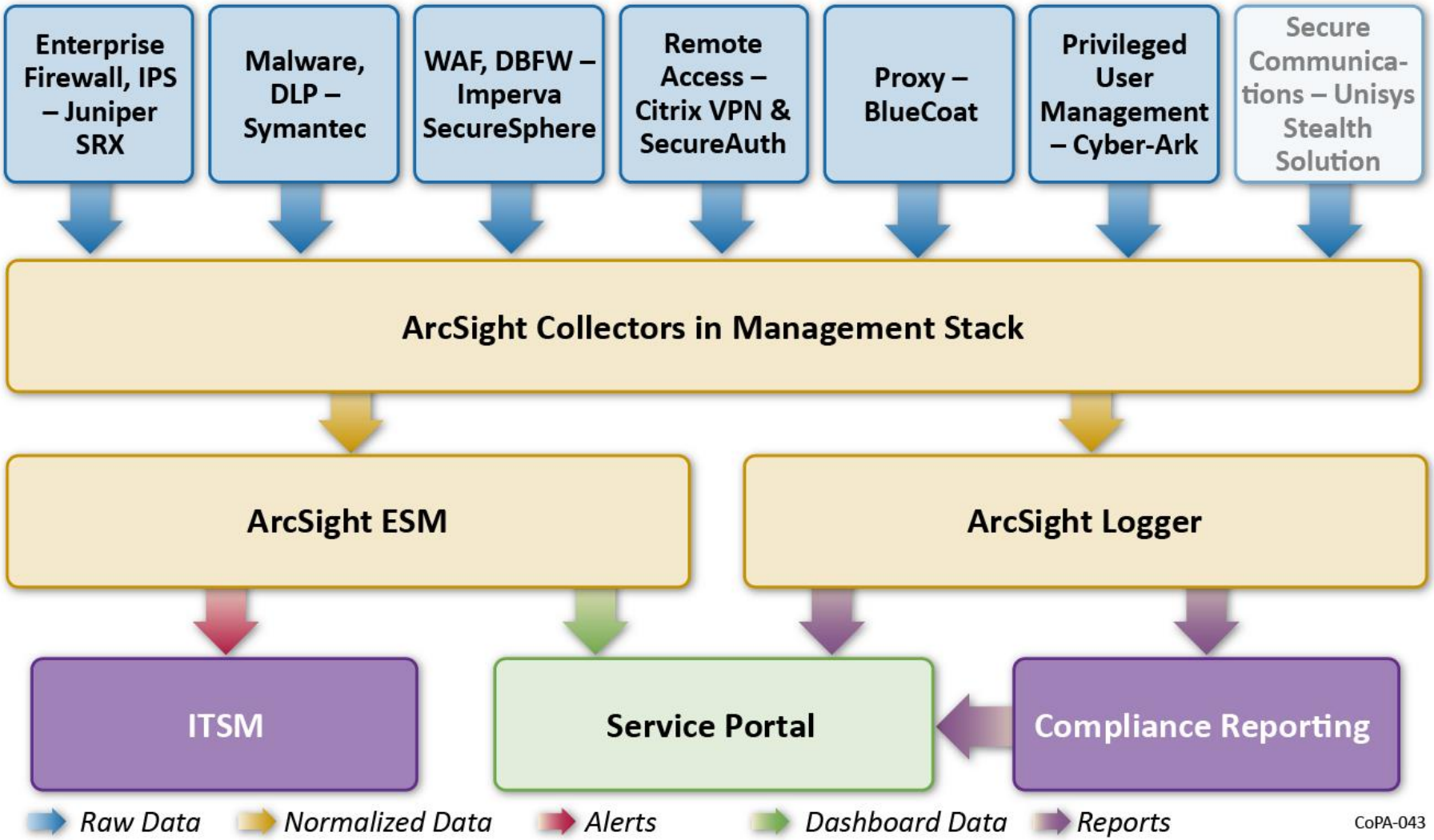
© 2013 Unisys Corporation. All rights reserved.

Security Solution

- One unified Data Center security plan
  - Details vary by Agency, but the plan is common
  - Details vary by Data Center, but the plan is common
  - Provide both logical and physical security
- Transition Services
  - Establish the framework
    - Initial security plan
    - Baseline assessment
  - Implement policies, processes, technologies, and tools
- Ongoing Operations
  - Manage the services and technologies
  - Update the security plan
  - Periodically re-assess

© 2013 Unisys Corporation. All rights reserved.

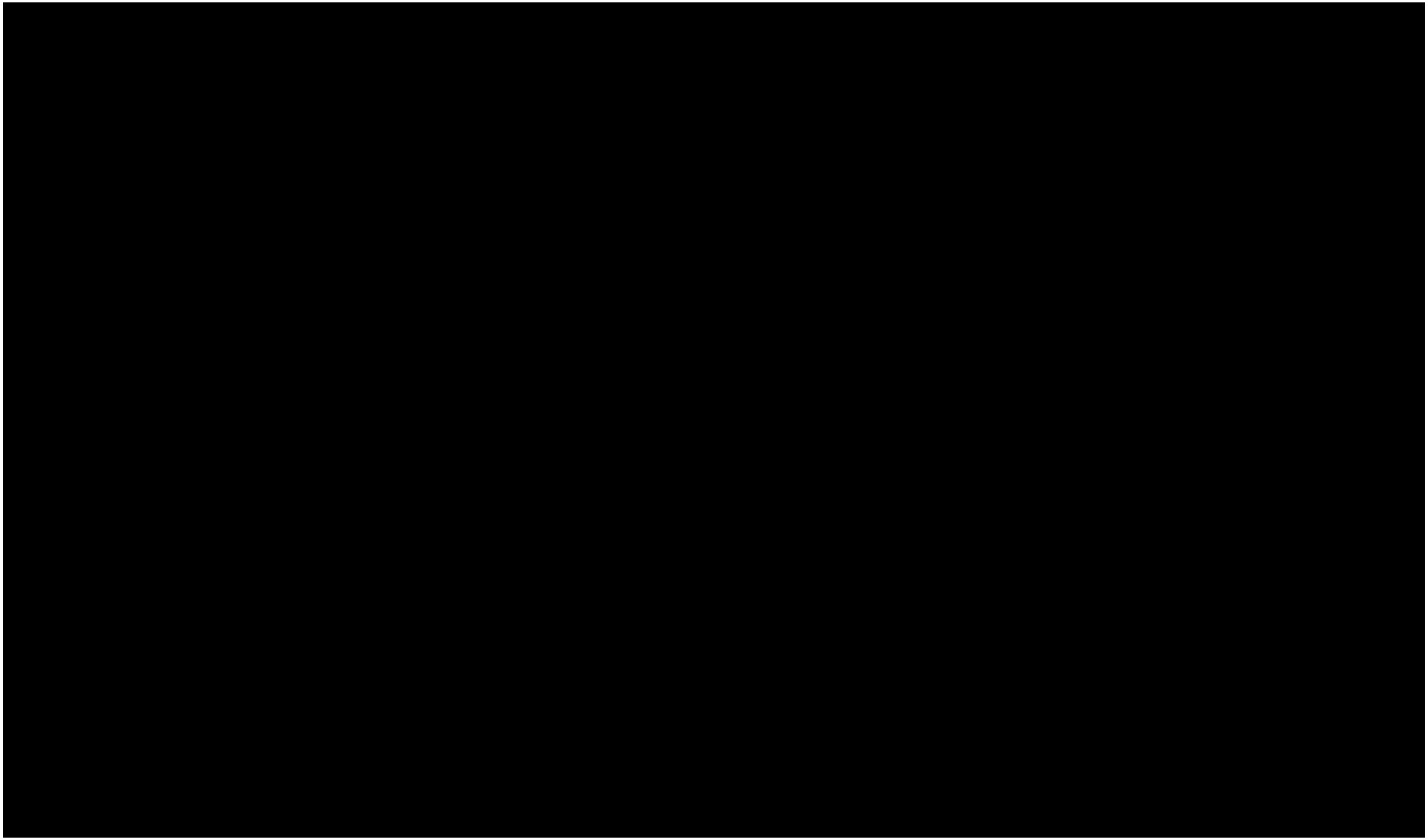
Technology and Tools



UNISYS

© 2013 Unisys Corporation. All rights reserved.

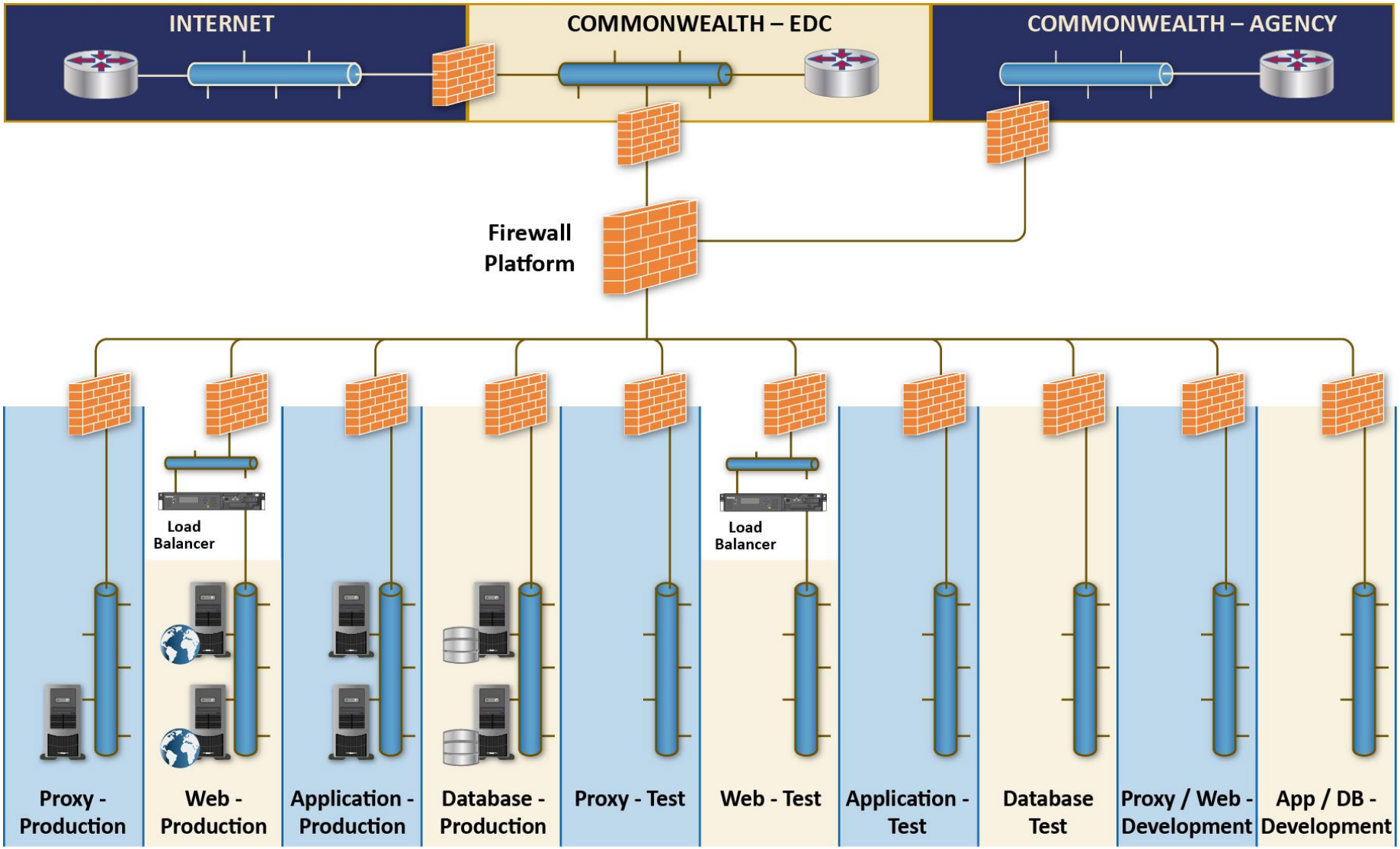
Secure Remote Admin Access



UNISYS

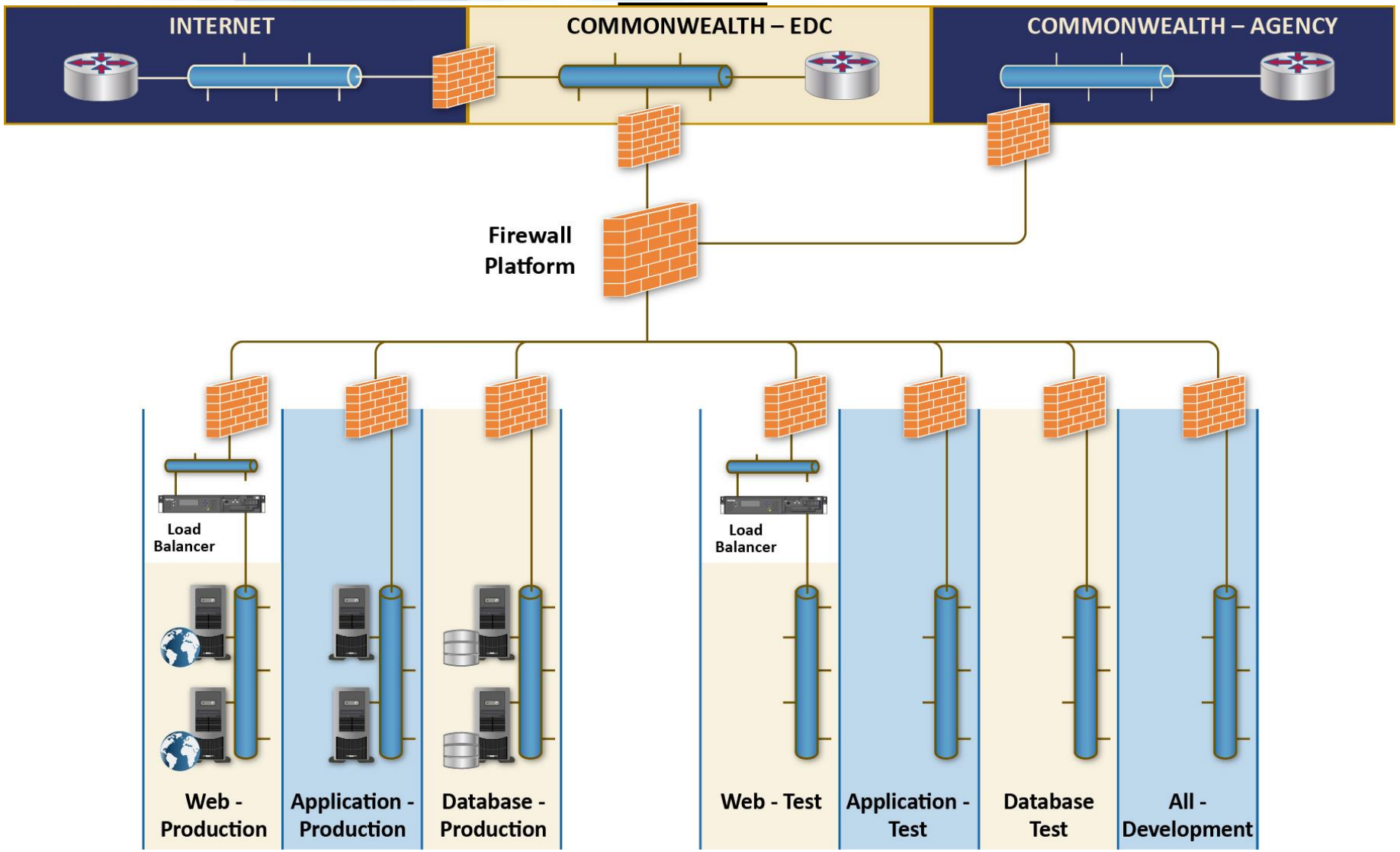
© 2013 Unisys Corporation. All rights reserved.

Security Zones



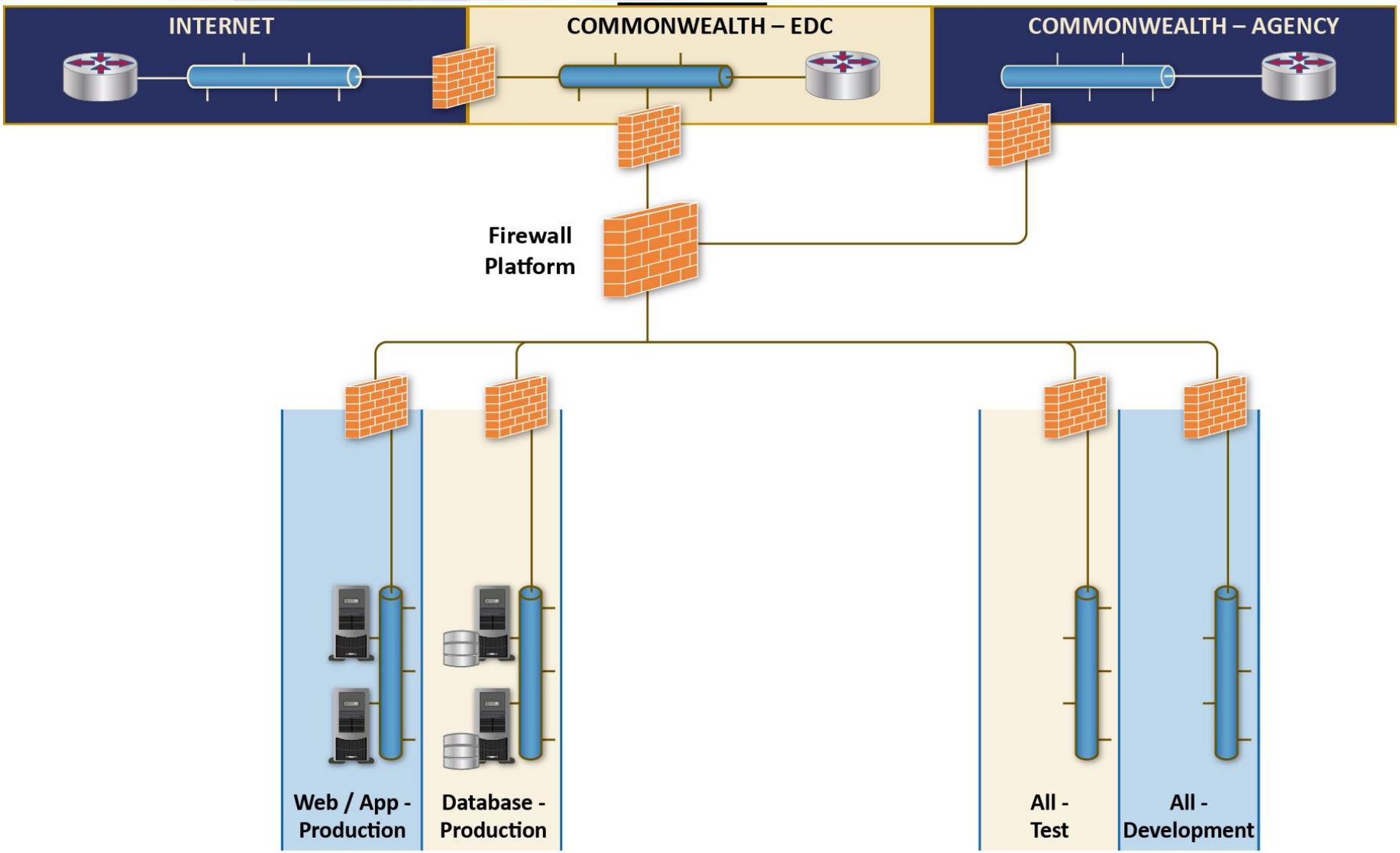
© 2013 Unisys Corporation. All rights reserved.

Security Zones – Sample Agency Application



© 2013 Unisys Corporation. All rights reserved.

Security Zones – Simple Application



© 2013 Unisys Corporation. All rights reserved.

Key Elements

- Meet diverse regulatory requirements
- Unified security framework
  - Security plan
- Flexible for each Agency

© 2013 Unisys Corporation. All rights reserved.

Delivering the Future of Network Connectivity

Consistently Reliable. Locally Flexible. Enabled Productivity.

Network Connectivity Overview

[redacted] – Senior Enterprise Infrastructure Architect

UNISYS

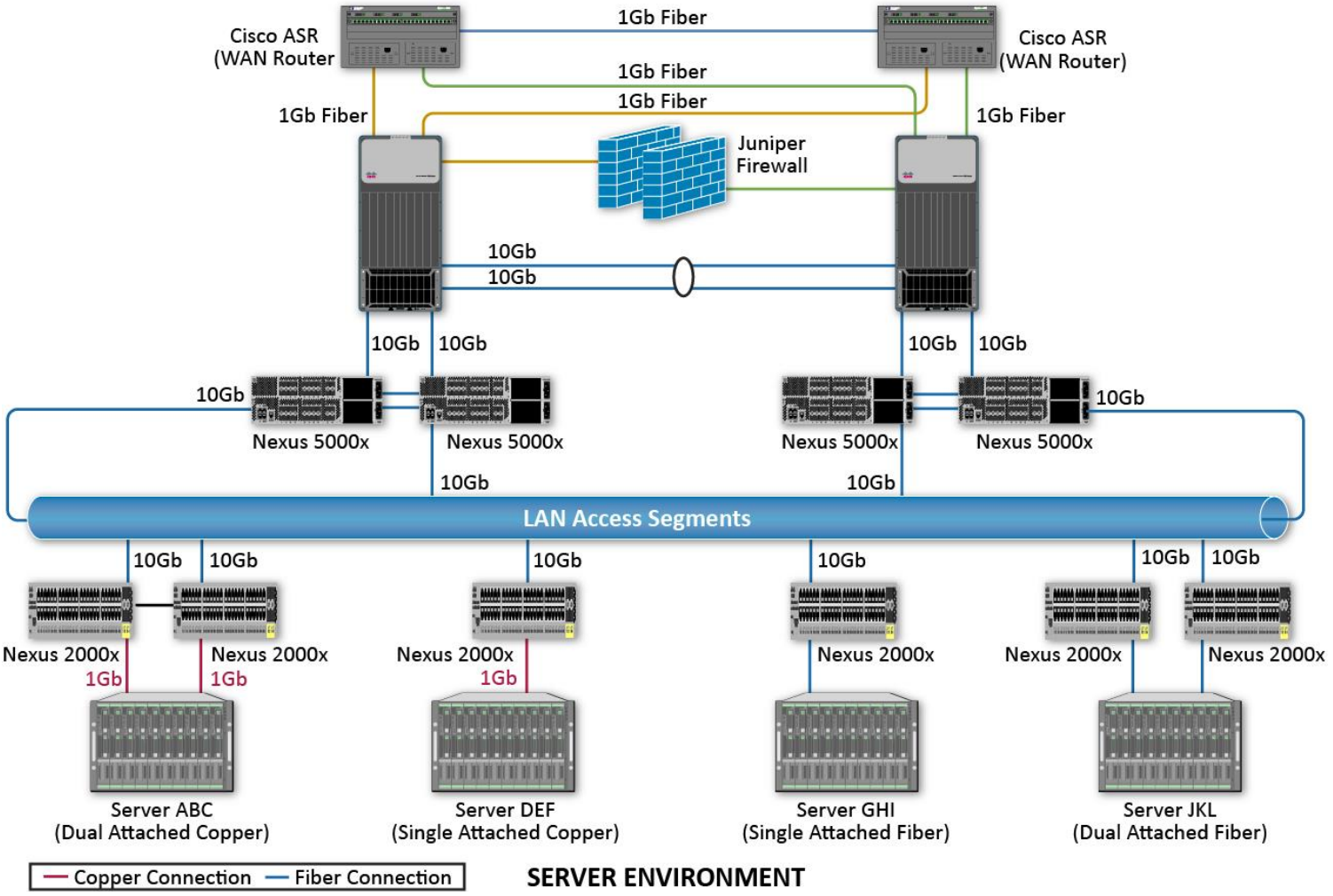
Network Architecture

- Maintaining a core Cisco Nexus architecture to aid in self-provisioning activities
- Three-layer network architecture
- Introducing Juniper virtual firewalls to simplify firewall scaling and policy management
- Introducing F5 application delivery controllers
- Expanding the use of Imperva Application and database firewalls
- Dual network links between data centers with no single point of failure

UNISYS

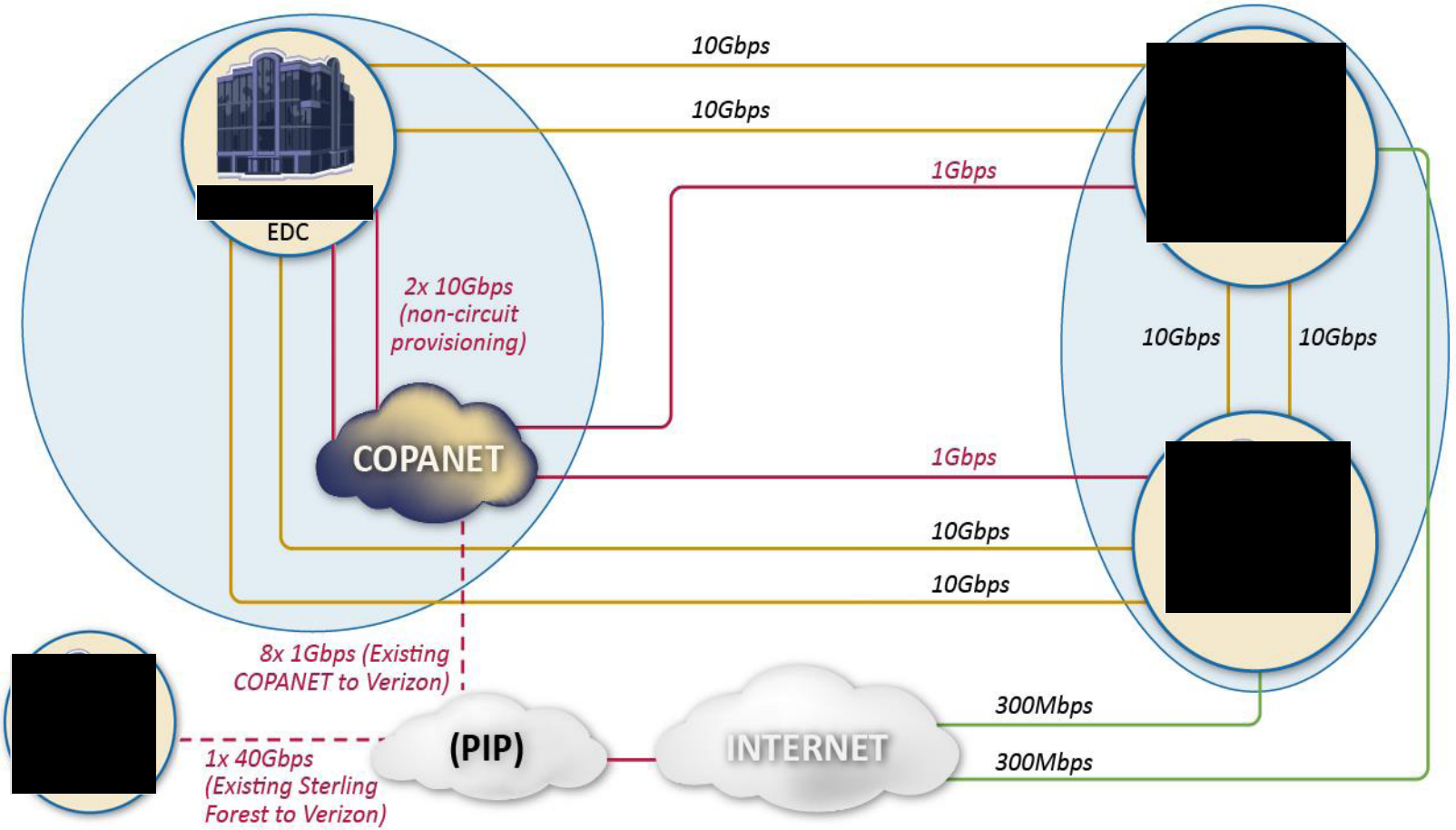
© 2013 Unisys Corporation. All rights reserved.

Data Center Local Area Network Design



© 2013 Unisys Corporation. All rights reserved.

Data Center WAN and Internet Connections



© 2013 Unisys Corporation. All rights reserved.

Business Partner Connectivity

- Business Partners connections available in each site
- Colocation space will be used for Business Partner hardware
- Secure connections via VPN or dedicated circuits

UNISYS

© 2013 Unisys Corporation. All rights reserved.

Delivering the Future of Disaster Recovery

Robust Capabilities. Proven Expertise. Maintained Operations.

Disaster Recovery Overview

[redacted] – Senior Enterprise Infrastructure Architect

UNISYS

Addressing the Commonwealth's Critical DR Requirements

Flexible and Scalable DR options make DR readily available for use

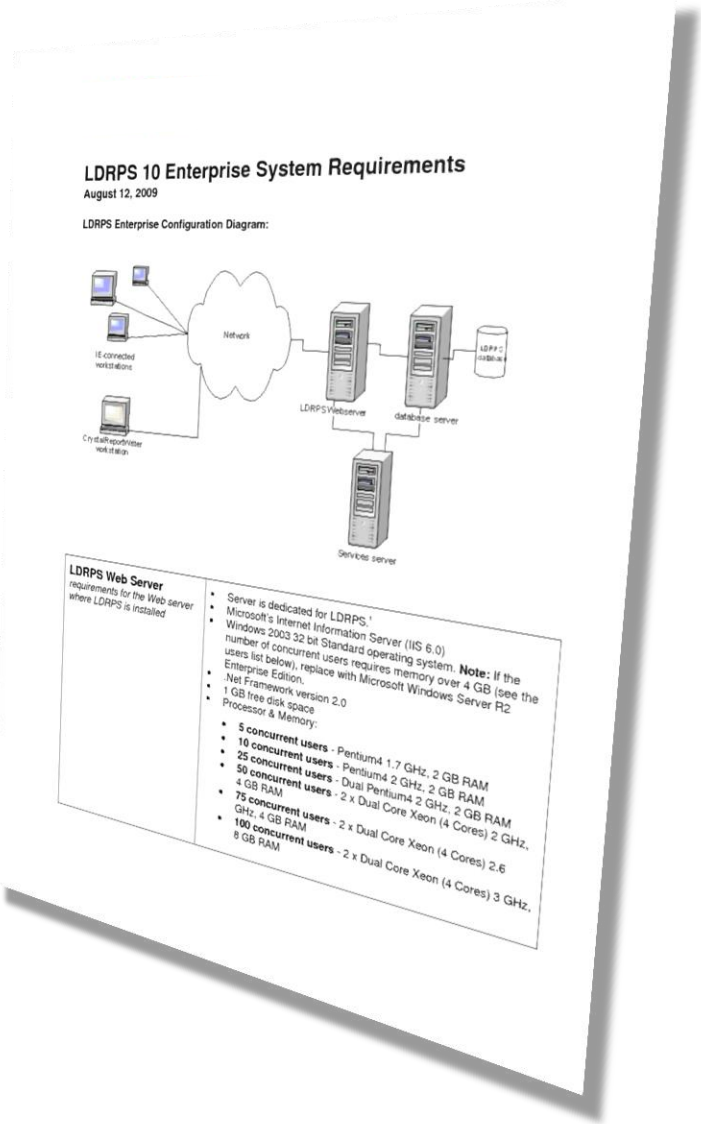
- Current DR being provided by SunGard will be moved to [redacted] after DPH is transitioned to Unisys [redacted]
- IBM Mainframes will continue to use IBM [redacted] site for recovery
- Living Disaster Recovery Planning System (LDRPS) will be used for DR planning
- A dedicated DR coordinator will support the agencies
- The data center architecture and network design enables new DR options
- A rich menu of DR services is available via the Enterprise Services Catalog including six tiers of DR services
- DR services can be selected by the agency in support of their specific business applications

© 2013 Unisys Corporation. All rights reserved.

Coordination enables DR Testing

Executing two DR Tests a year takes Effective Coordination

- DR Planning to document
  - Stored in the DR planning tool
  - Led by the DR coordinator
- Testing
  - Scheduled and coordinated with Agencies
  - ITSM updated to communicate DR tests
- CMDB is central to providing data to identify application components
- After the tests
  - Analysis of results
  - Action plans developed
  - DR plans updated



LDRPS 10 Enterprise System Requirements

August 12, 2009

LDRPS Enterprise Configuration Diagram:

LDRPS Web Server

requirements for the Web server where LDRPS is installed

- Server is dedicated for LDRPS.'
- Microsoft's Internet Information Server (IIS 6.0)
- Windows 2003 32 bit Standard operating system. **Note:** If the number of concurrent users requires memory over 4 GB (see the users list below), replace with Microsoft Windows Server R2 Enterprise Edition.
- .Net Framework version 2.0
- 1 GB free disk space
- Processor & Memory:
  - **5 concurrent users** - Pentium4 1.7 GHz, 2 GB RAM
  - **10 concurrent users** - Pentium4 2 GHz, 2 GB RAM
  - **25 concurrent users** - Dual Pentium4 2 GHz, 2 GB RAM
  - **50 concurrent users** - 2 x Dual Core Xeon (4 Cores) 2 GHz, 4 GB RAM
  - **75 concurrent users** - 2 x Dual Core Xeon (4 Cores) 2.6 GHz, 4 GB RAM
  - **100 concurrent users** - 2 x Dual Core Xeon (4 Cores) 3 GHz, 8 GB RAM

© 2013 Unisys Corporation. All rights reserved.

Six Tiers of DR Services for Windows, Linux, and AIX Servers are Available for Agency Selection

	Tier 1	Tier 2	Tier 3	Tier 4	Tier 5	Tier 6
RPO	< 36 Hours	24 Hours	24 Hour	1 Hour	Minutes	Seconds
RTO	> 72 Hours	72 Hours	24 Hours	24 Hours	< 4 Hours	Seconds
Approach	Tape Recovery	Tape Recovery	Disk-based Backup with Replication	Disk-based Replication	Disk-based Replication	Disk-based Replication, Auto Failover for Virtual Servers Only
Support High Availability	No	No	No	Yes	Yes	Yes

UNISYS

© 2013 Unisys Corporation. All rights reserved.

Multiple DR Options for IBM and Unisys Mainframes

	Current DPH solution for Mainframe and iSeries	IBM MF Config 3	IBM iSeries Config 2	Unisys Mainframe Config 3	Unisys Mainframe Config 4
RPO	24 hours	1 hour	1 hour	1 Hour	1 Hour
RTO	72 hours	24 hours	24 hours	24 hours	24 hours
Approach	Tape Recovery to IBM Recovery Center (Cold Site)	Disk-based Replication and Geographically Dispersed Parallel Sysplex	Disk-based Replication	Disk-based Replication	Disk-based Replication
DR Site	[redacted]				
Support High Availability	No	Yes	No	No	No

UNISYS

© 2013 Unisys Corporation. All rights reserved.

Key Elements

- Resilient network design to support normal operations and disaster recovery functionality
- Maintaining current DR functionality from DPH and other data centers
- Providing new DR options to support Commonwealth business needs

© 2013 Unisys Corporation. All rights reserved.

Delivering the Future of Transition Methodology

Leveraging a History of Success along with Low-Risk Processes.

Transition Methodology Overview

[redacted] – Transition Director

Focus on moving software applications rather than moving hardware

This is about moving software applications that support the most important functions of Pennsylvania state government.

UNISYS

Guiding Principles

FOCUS – BALANCE – LEARN

Do THE RIGHT THING

in THE RIGHT WAY

at THE RIGHT TIME

EVERYTIME

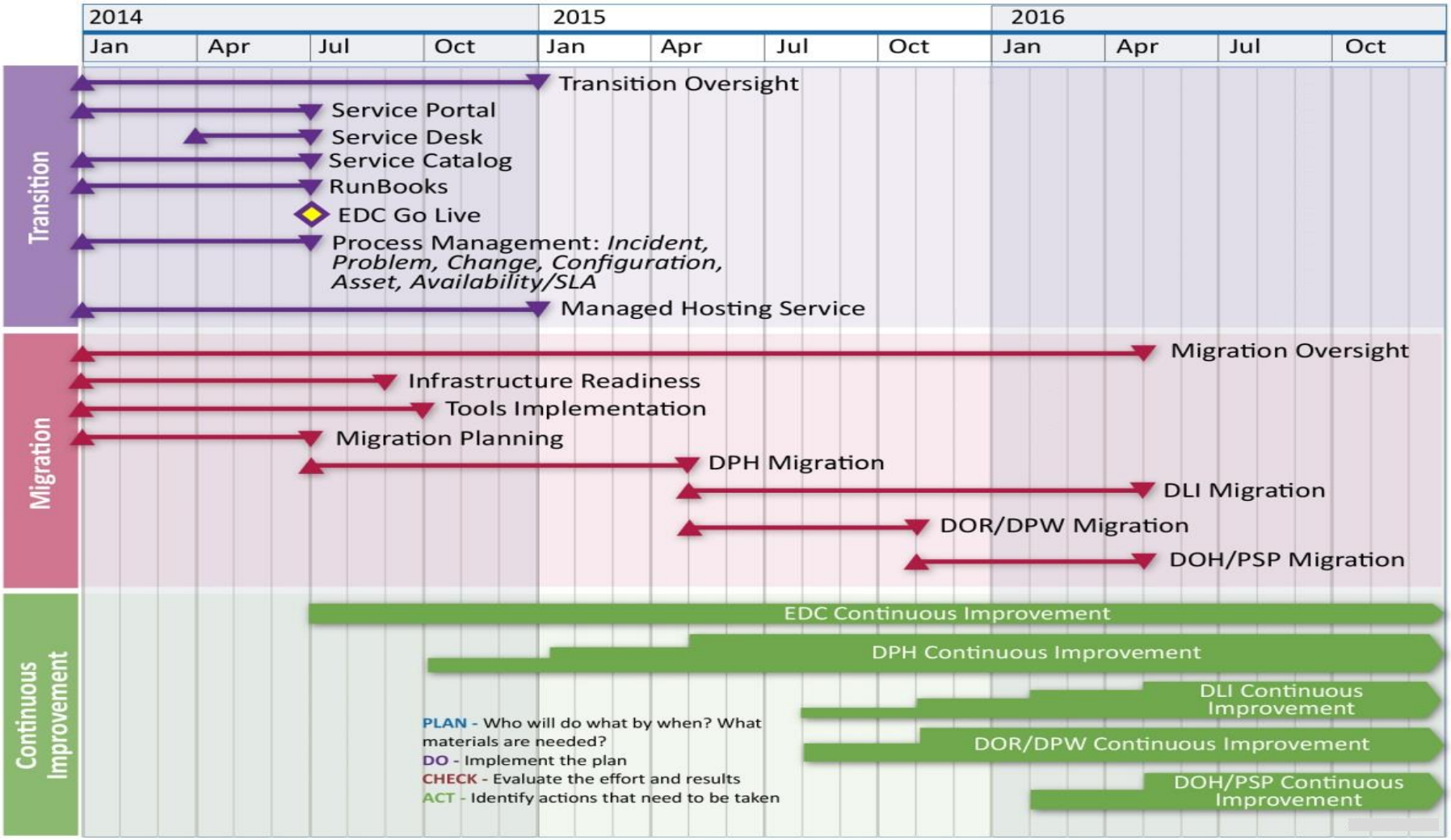
- Maintain **focus** on Commonwealth Agencies and Applications
- Maintain an appropriate **balance** between Cost, Risk and Benefit to achieve our goals
- Be a **learning** organization

ALWAYS do what is RIGHT

UNISYS

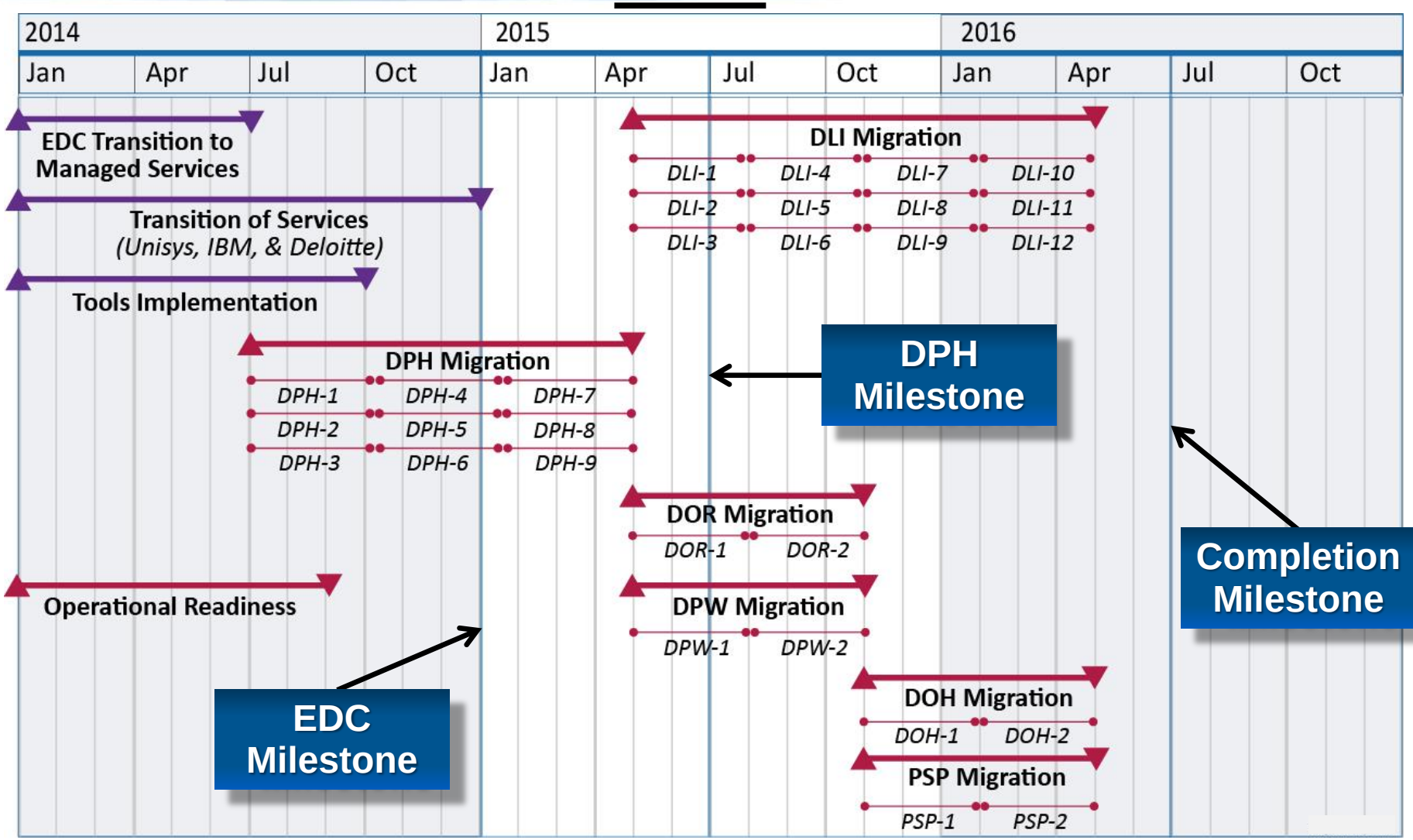
© 2013 Unisys Corporation. All rights reserved.

Proposed Work Breakdown and Schedule



© 2013 Unisys Corporation. All rights reserved.

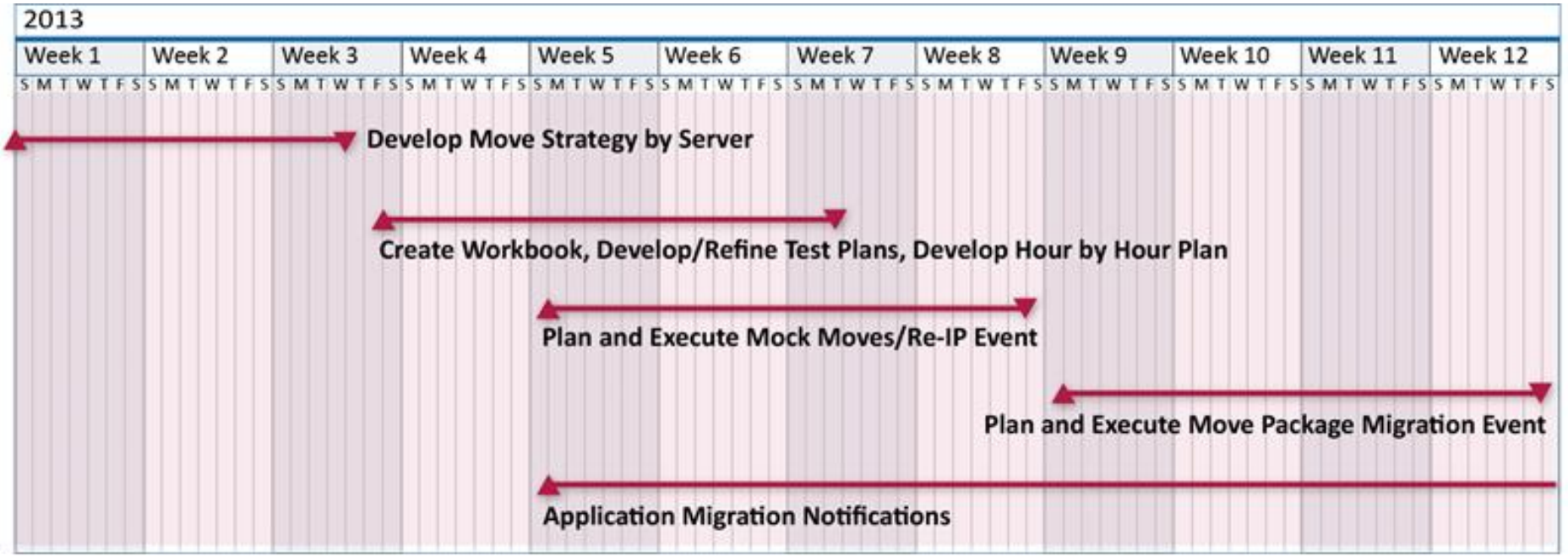
Proposed Work Breakdown and Schedule



UNISYS

© 2013 Unisys Corporation. All rights reserved.

Application Migration Project Breakdown

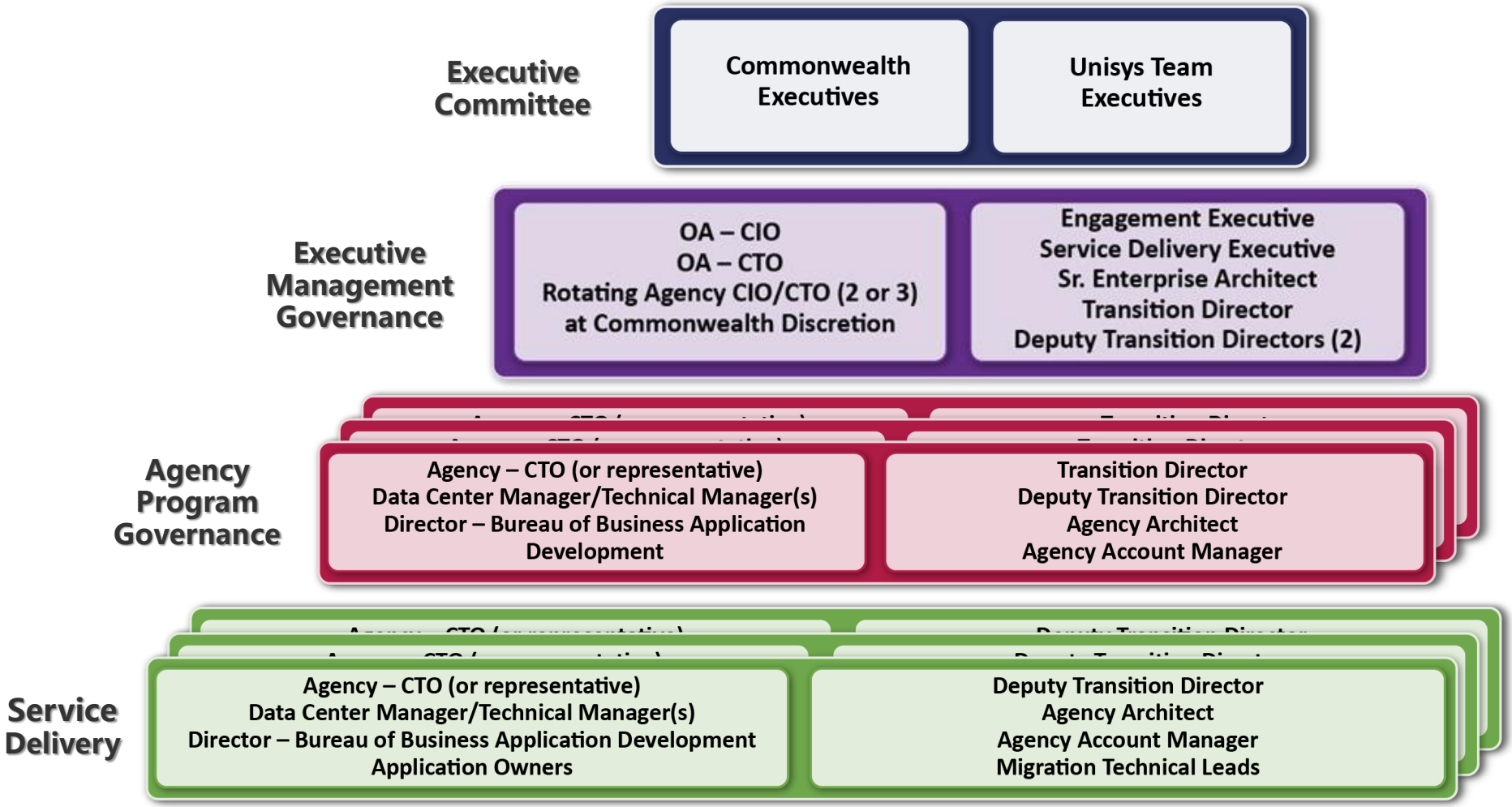


- **Month 1 – Move Package Planning**
- **Month 2 – Test Move Planning & Execution**
- **Month 3 – Migration Planning & Execution**
- **Throughout - Communications**

UNISYS

© 2013 Unisys Corporation. All rights reserved.

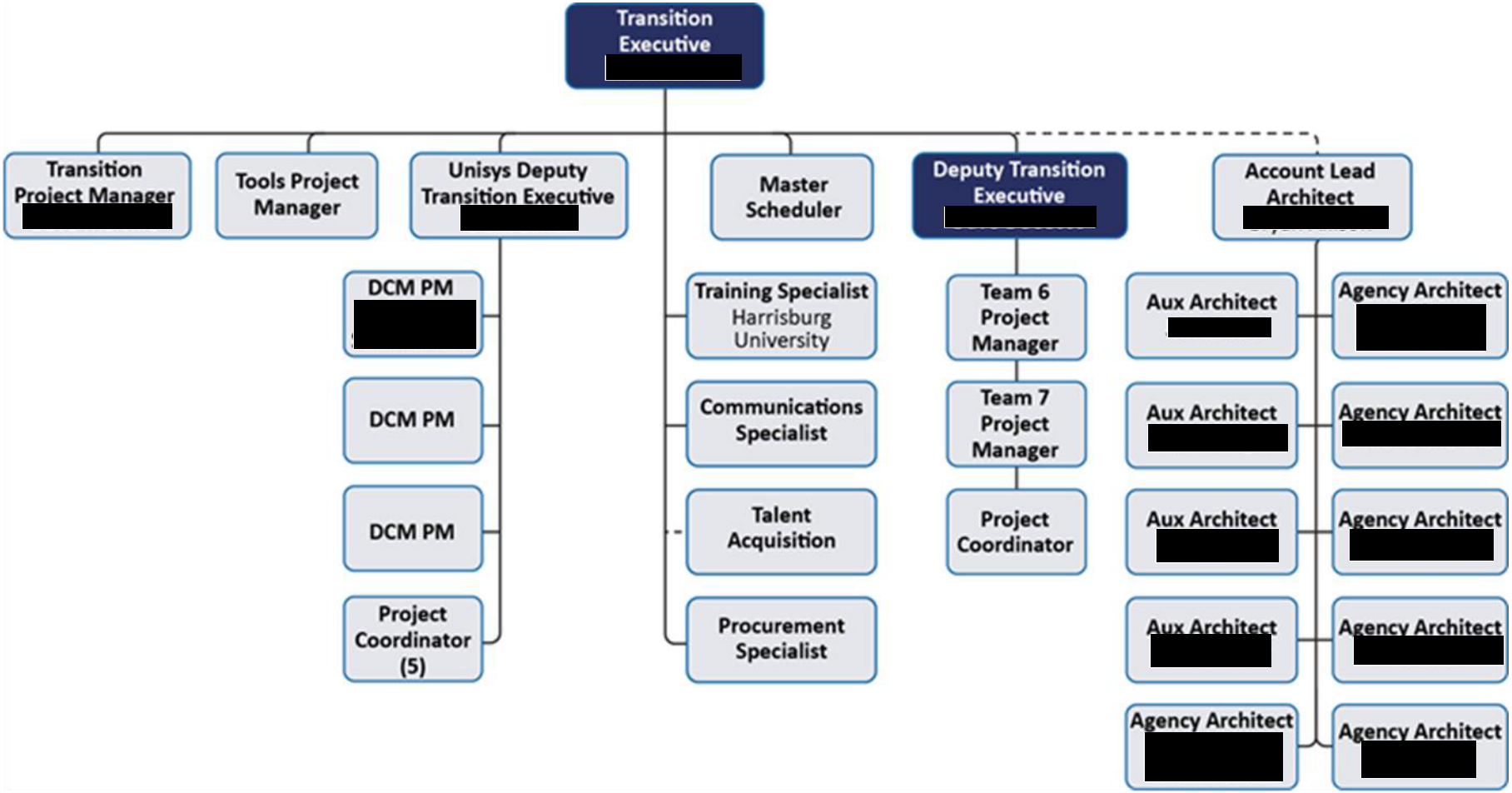
Proposed Multi-Tier Governance



UNISYS

© 2013 Unisys Corporation. All rights reserved.

Transition [redacted] Support Team



© 2013 Unisys Corporation. All rights reserved.

Keys to Success

- Minimize Risk
- Minimize Agency Workload
- Exceeding Commonwealth Milestone expectations
- Strong Governance
- Effective Communications
- Continue Strong Partnership

© 2013 Unisys Corporation. All rights reserved.

Delivering the Future of Service Delivery

Innovative Service Management Enabling Efficiency, Flexibility, Agility.

Service Delivery Overview

[redacted] – Agency Account Manager

Achieve success together

Work closely with Commonwealth staff, understand and address their individual issues, and provide needed training to facilitate knowledge transfer and adoption of best practices.

UNISYS

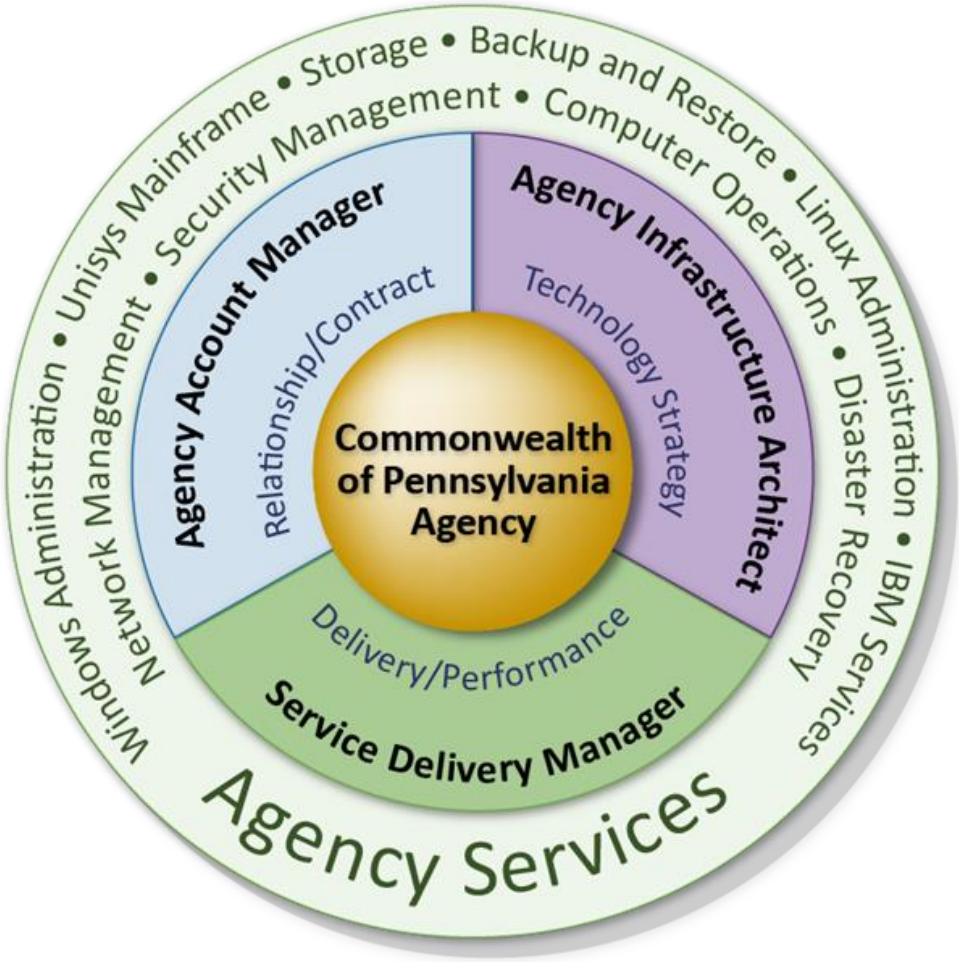
Agency Account Management Model

New model

- Drives service delivery and customer satisfaction
- Agency focus
- Six teams
- Leadership

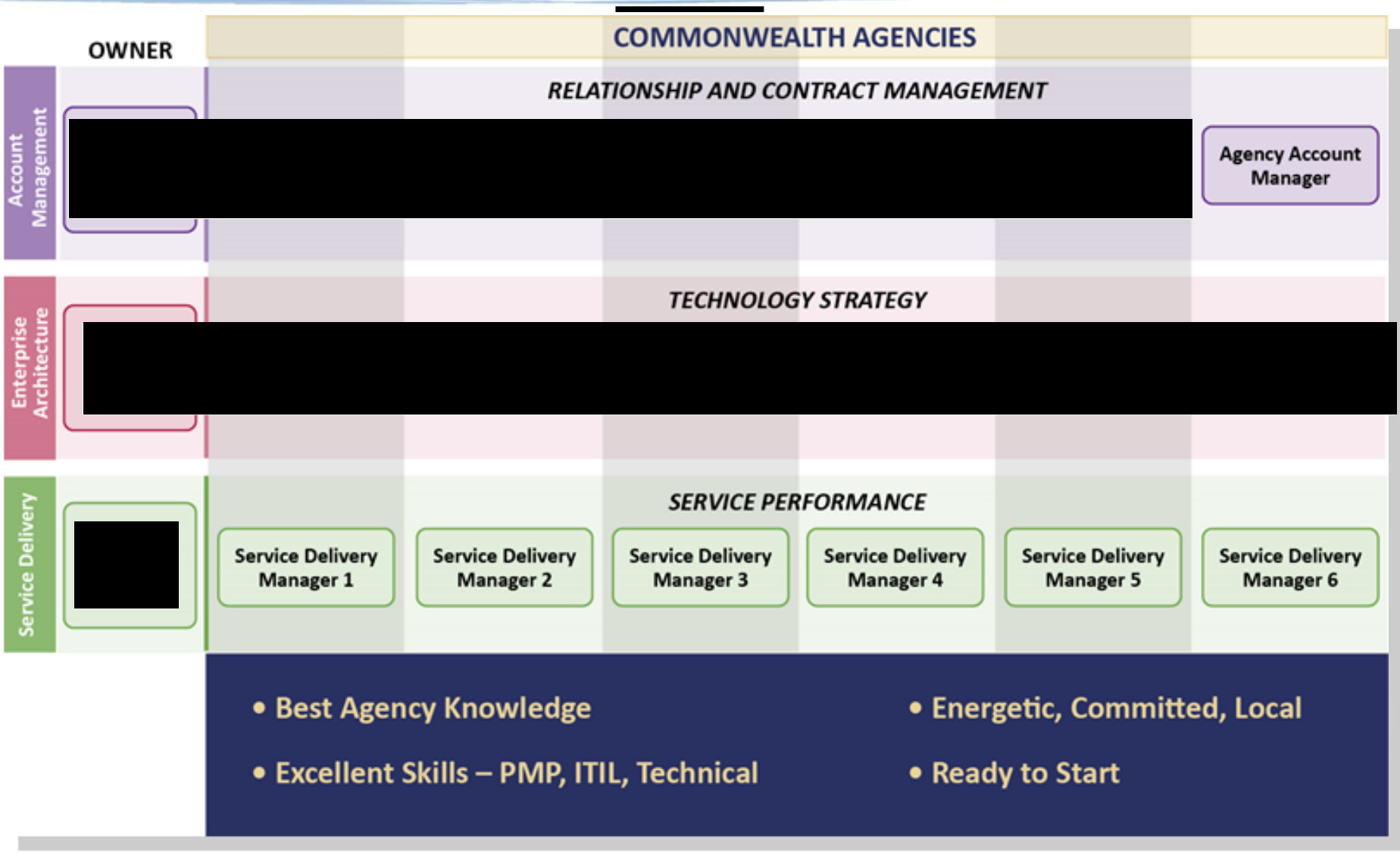
Value

- Personal approach
- Accountability at Agency level
- Recognition of unique needs
- Compute services aligned to your specific needs
- Consistent services across all Agencies
- **Achieve success together**



© 2013 Unisys Corporation. All rights reserved.

Account Management Structure



UNISYS

© 2013 Unisys Corporation. All rights reserved.

Delivering the Future of Service Delivery

Innovative Service Management Enabling Efficiency, Flexibility, Agility.

Service Delivery Overview

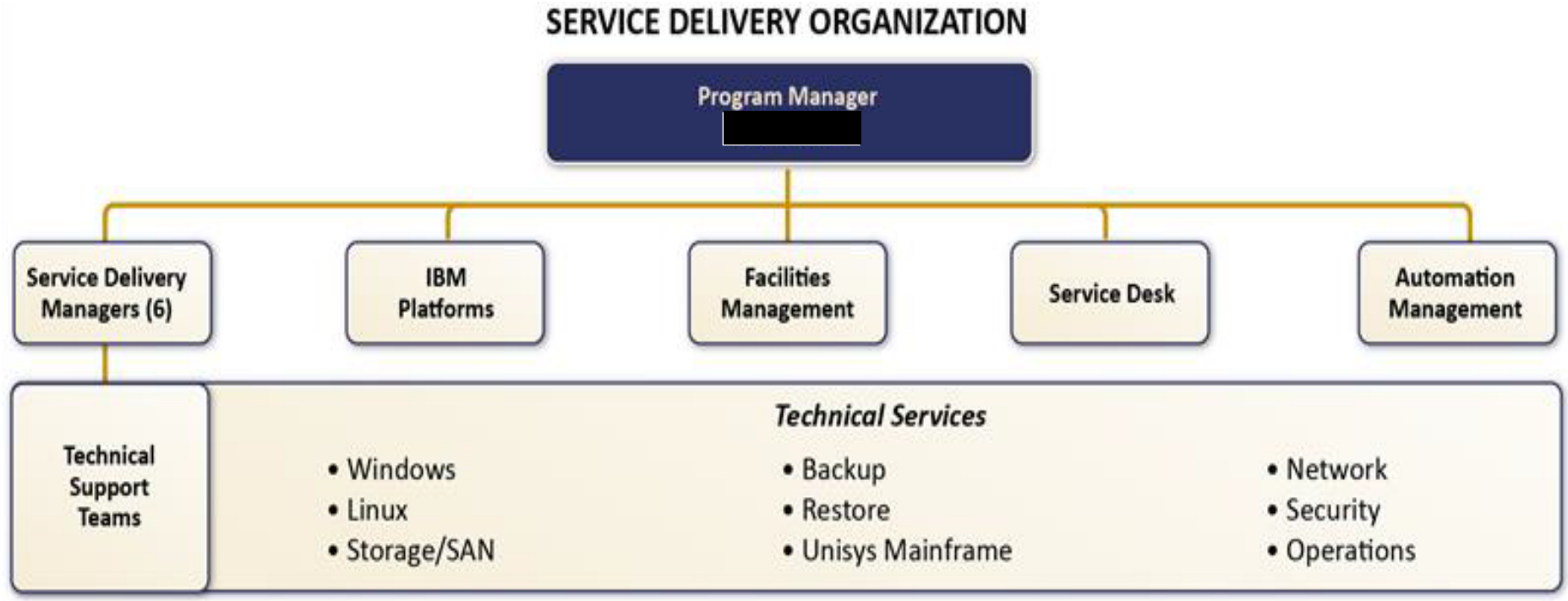
[redacted] – Service Delivery Executive

Achieve success together

Work closely with Commonwealth staff, understand and address their individual issues, and provide needed training to facilitate knowledge transfer and adoption of best practices.

UNISYS

Service Delivery



IBM Mainframes
System i
AIX Platforms
zLinux

"Lights out" Operations

Incidents
Service Requests

Configuring

© 2013 Unisys Corporation. All rights reserved.

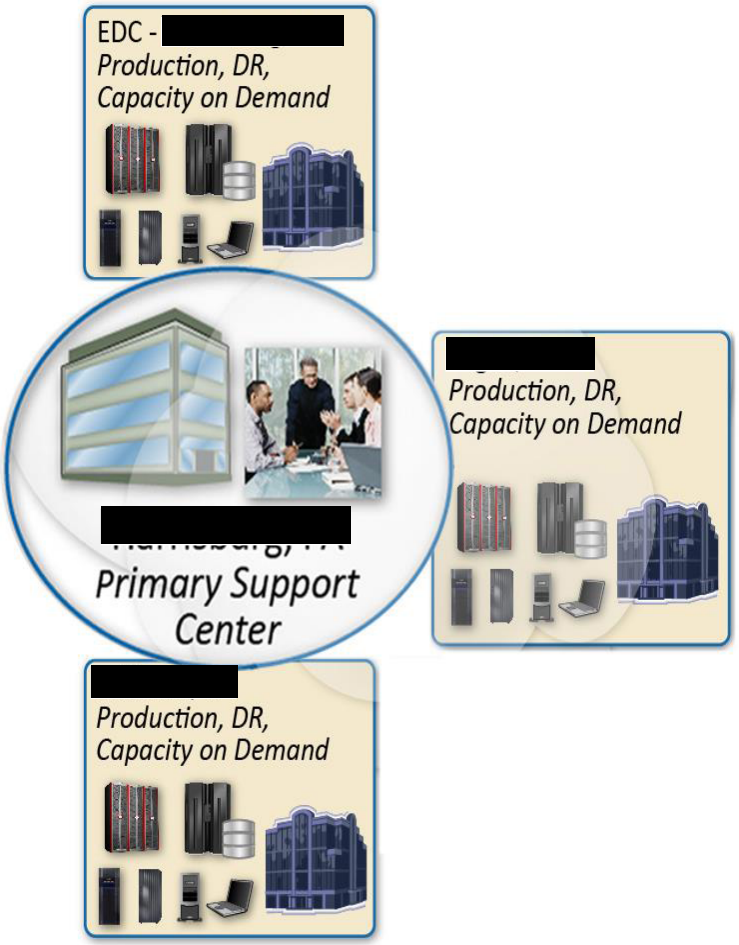
Harrisburg
Central Point of Interaction

[redacted] will be the Primary Support Center for:

- Program Management Office
- Local Service Desk and operations teams
- Security operations
- Platform support teams
- Access to additional US-based resources

[redacted] will be the Secondary Support Center

- Provides off hours support for the Service Desk
- Provides additional support during peak periods



UNISYS

© 2013 Unisys Corporation. All rights reserved.

Delivering the Future of Support

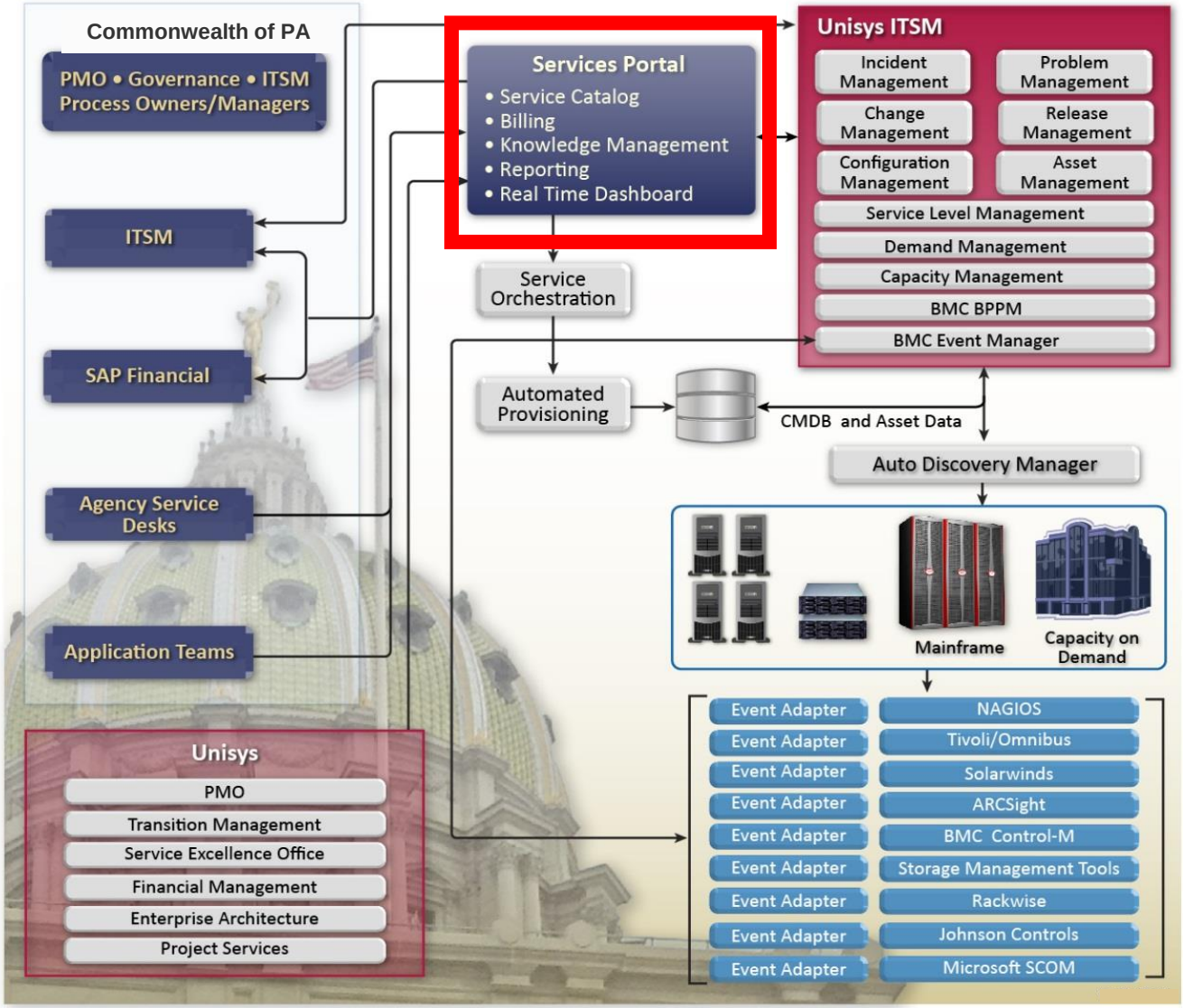
Driving Continuous Improvement and Innovation.

Support, Incident, and SLA Overview

[redacted] – Service Delivery Executive

UNISYS

IT Service Management Model



UNISYS

© 2013 Unisys Corporation. All rights reserved.

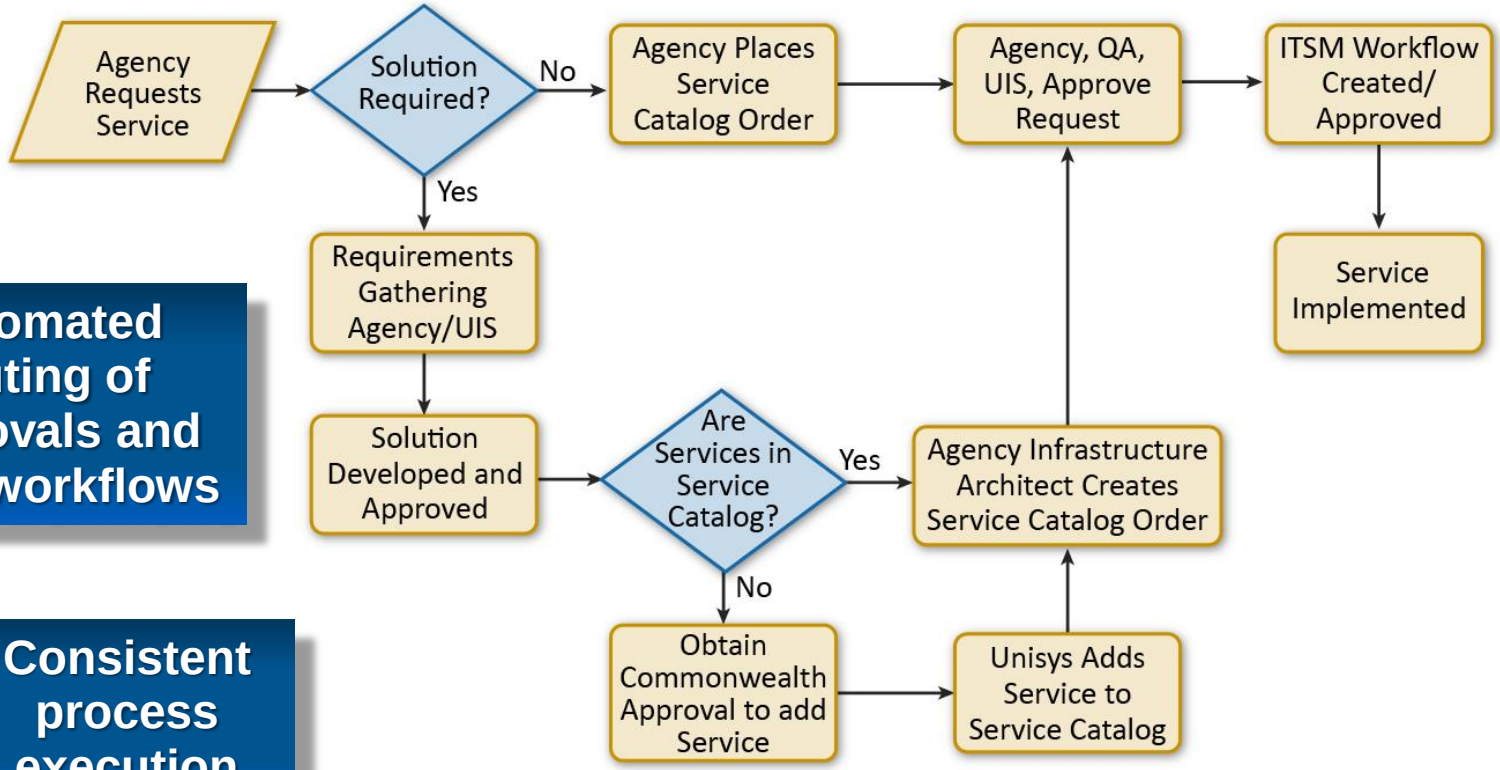
IT Service Management Model

Services Portal

- Service Catalog
- Billing
- Knowledge Management
- Reporting
- Real Time Dashboard

© 2013 Unisys Corporation. All rights reserved.

Request for Service Management Process



Automated routing of approvals and ITSM workflows

Consistent process execution

Transparent pricing details

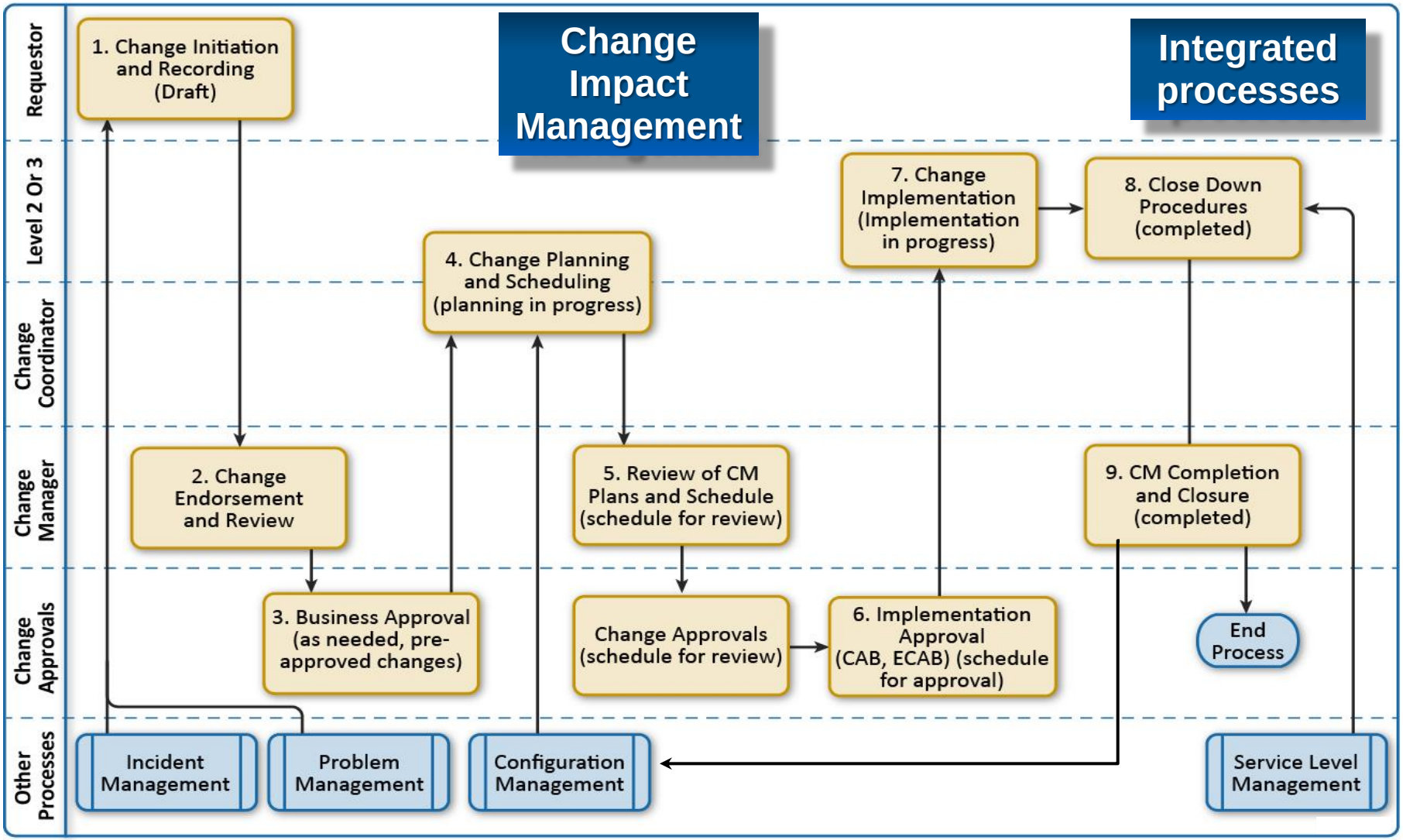
Charging to desired funding stream

Linked to invoicing

UNISYS

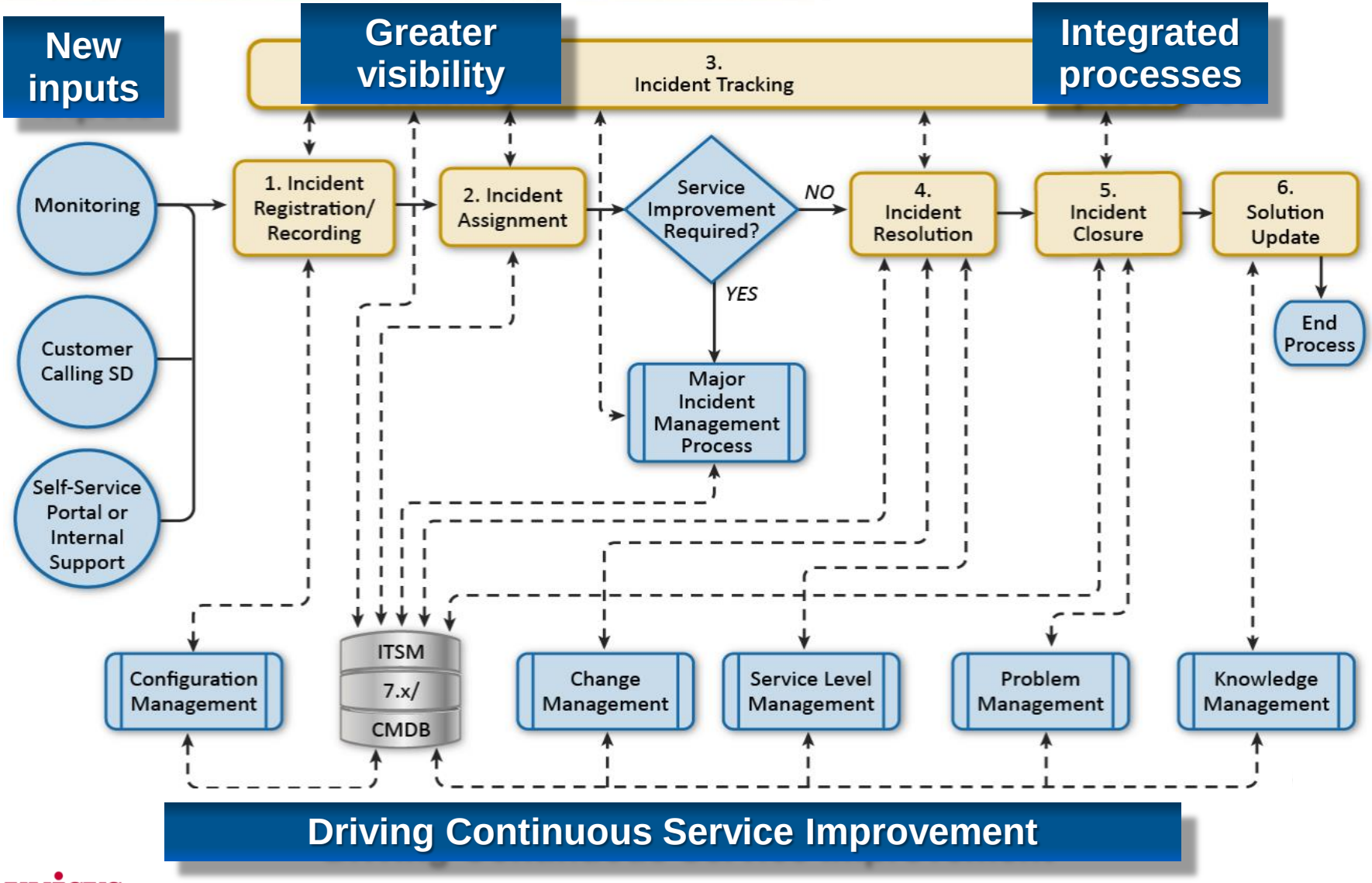
© 2013 Unisys Corporation. All rights reserved.

Service Delivery: Flow of Change Management



© 2013 Unisys Corporation. All rights reserved.

Service Delivery: Flow of Incident Management



© 2013 Unisys Corporation. All rights reserved.

Delivering the Future of Support

Driving Continuous Service Improvement and Innovation.

Support, Incident, and SLA Overview

[redacted] – Service Excellence Officer

Managing change is key to success

We must implement strong change management practices, a solid training plan, and effective communications when transforming the Commonwealth to its future model.

UNISYS

Delivering the Future of Support

Driving Continuous Service Improvement and Innovation

UNISYS

© 2013 Unisys Corporation. All rights reserved.

Delivering the Future of Support

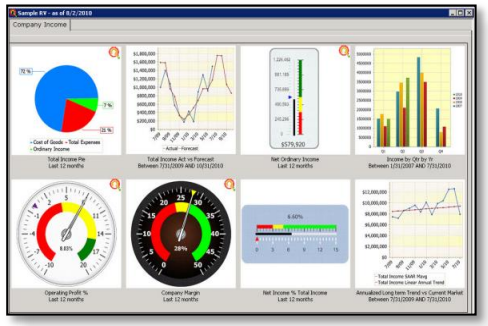
SLA Management & Driving Transparency

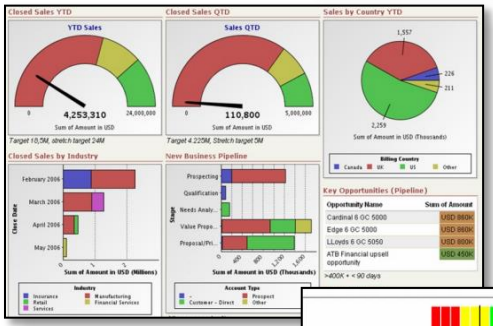
SLA Management

- Aggregate system availability 99.99% since 2008
- Service Level Management module
- Proactive SLA Management
- Selectable SLA by application
- Maintaining excellence

Dashboards

- Agency centric
- Robust reporting
- Proactive metrics Green/Yellow/Red
- Readily available





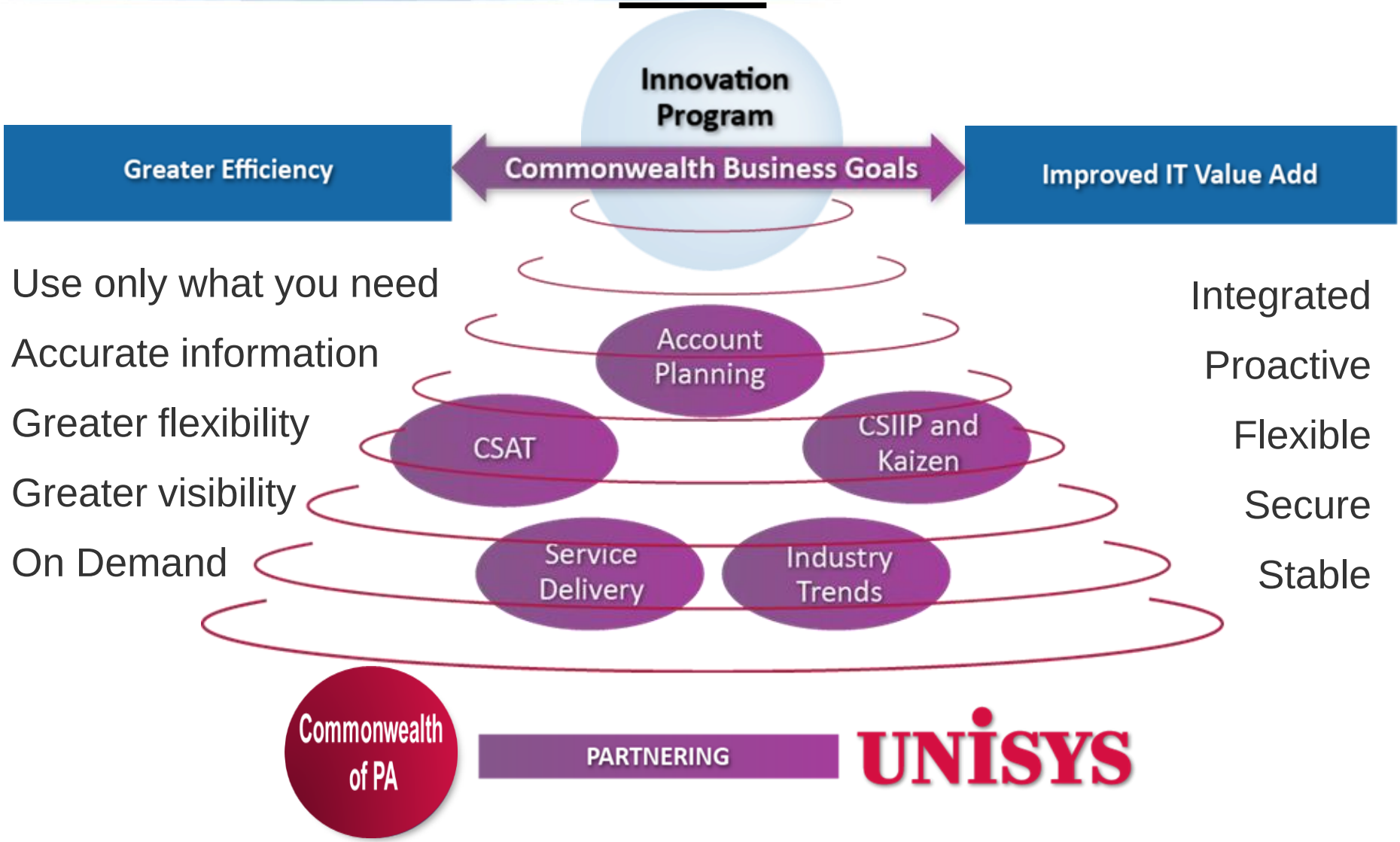
Agency Dashboards delivering Robust Transparent SLA Reporting

UNISYS

© 2013 Unisys Corporation. All rights reserved.

Delivering the Future of Support

Partnering with the Commonwealth to Drive Innovation



© 2013 Unisys Corporation. All rights reserved.

Thank You

UNISYS

Questions and Answers

UNISYS

Unisys Response to

Commonwealth of Pennsylvania
Office of Administration
Office for Information Technology

Data Center Computing Services

Request for Proposal (RFP)
RFP 6100022698

Unisys Key Personnel Details

July 29, 2013

UNISYS

July 29, 2013

Bureau of IT Procurement
c/o Commonwealth Mail Processing Center
2 Technology Park (rear)
Attn: IT Procurement 506 Finance
Harrisburg, PA 17110
Attn: Janis Brown

RE: **Request for Proposal (RFP Number 6100022698) for the Commonwealth of Pennsylvania Data Center Computing Services**

Dear Ms. Brown:

Unisys Corporation is pleased to submit this Key Personnel Details document to provide requested information for the Company and Program Overview section of the Offeror Orals Presentation.

We have included a description of all Unisys Team proposed key personnel for the project including:

- Name
- Position in organization
- Proposed role on project
- Experience in the proposed role
- Qualifications for the proposed role
- Percentage of time the person will be dedicated to the project

We appreciate this opportunity to provide IT Infrastructure support services to support your mission.

Sincerely,

[redacted]

[redacted]
Senior Account Executive
Unisys Global Managed Services

Table of Contents

KEY PERSONNEL OVERVIEW 4

ENGAGEMENT EXECUTIVE: [redacted] 6

PMO TRANSITION MANAGER: [redacted] 8

SERVICE DELIVERY EXECUTIVE (PROGRAM MANAGER): [redacted] 9

SERVICE EXCELLENCE OFFICER: [redacted] 10

SENIOR ENTERPRISE INFRASTRUCTURE ARCHITECT: [redacted] 11

INCIDENT MANAGEMENT MANAGER: [redacted] 12

CHANGE MANAGER: [redacted] 13

CHANGE ANALYST: BETH VILLARREAL 14

SERVICE LEVEL MANAGEMENT ANALYST: [redacted] 15

FINANCE MANAGER: [redacted] 16

FINANCE ANALYST: [redacted] 17

AGENCY ACCOUNT MANAGER: [redacted] 18

AGENCY ACCOUNT MANAGER: [redacted] 19

AGENCY ACCOUNT MANAGER: [redacted] 20

AGENCY ACCOUNT MANAGER: [redacted] 21

AGENCY INFRASTRUCTURE ARCHITECT: [redacted] 22

AGENCY INFRASTRUCTURE ARCHITECT: [redacted] 23

AGENCY INFRASTRUCTURE ARCHITECT: [redacted] 24

SECURITY MANAGER: [redacted] 25

PMO TRANSITION MANAGER 2: [redacted] 26

AVAILABILITY MANAGER: [redacted] 27

AGENCY ACCOUNT MANAGER: [redacted] 28

AGENCY INFRASTRUCTURE ARCHITECT: [redacted] 29

AGENCY INFRASTRUCTURE ARCHITECT: [redacted] 30

AGENCY INFRASTRUCTURE ARCHITECT: [redacted] 31

IBM PROJECT EXECUTIVE: [redacted] 32

IBM DELIVERY PROJECT EXECUTIVE: [redacted] 33

EXECUTIVE LEADERSHIP COMMITTEE 34

Key Personnel Overview

The core of this successful program is comprised of 28 key personnel. They are motivated, seasoned, ITIL V3 Foundations certified and well-educated professionals guided by an executive leader experienced with managing complex IT organizations and projects. The **key personnel** selected by Unisys provide targeted executive focus in key program areas, including program management, service delivery, service excellence and quality, enterprise architecture, transition and steady state project management, information security, and account management.

This organization's key personnel were selected not only for their experience with supporting large, complex customer environments and getting the job done with high success, but also for the collaborative style of their approach. This team of leaders can see the future of the Commonwealth Data Center Computing Services model with all of its nuances and will create a vision with a roadmap guiding the delivery. They work proactively to prioritize and enable desired outcomes to be achieved to your satisfaction. The key personnel listed in the table below have entrusted their faith to Unisys by providing us the exclusive right to represent them in our proposal to the Commonwealth.

All Unisys Team members identified to fill key personnel roles will provide services from the Harrisburg area office and will be 100% dedicated to performing that role on the account, as required in the RFP, with two exceptions which will benefit the Commonwealth. The individual who serves as IBM Mainframe Agency Infrastructure Architect will be assigned on a 50 percent dedicated basis due to minimal changes required to the mainframe architecture. Another architect possessing extensive experience with IBM AIX and Windows platforms be assigned on a 50 percent dedicated basis. This staffing approach will provide the equivalent of a full time employee using two individuals with a better blend of skills to support the project's requirements. In addition, the second PMO Transition Manager specified in Schedule G will work on the project through the transition's duration and will no longer be needed when transition is complete.

The key personnel are briefly introduced to you in the table below, which is followed by a short summary of each of their responsibilities. The individuals who will perform these functions are the project's linchpins. Their performance in the assigned roles will be a determining factor in the program's success.

Key Personnel Table

Role/Position	Name	Reports to
Engagement Executive	[redacted]	Regional Vice President
Program Manager/Service Delivery	[redacted]	Engagement Executive
PMO Transition Manager 1	[redacted]	Engagement Executive
PMO Transition Manager 2	[redacted]	PMO Transition Manager 1
Security Manager	[redacted]	Engagement Executive
Service Excellence Officer	[redacted]	Engagement Executive
Sr. Enterprise Infrastructure Architect	[redacted]	Engagement Executive
Incident Management Manager	[redacted]	Service Excellence Officer
Availability Manager	[redacted]	Service Excellence Officer
Service Level Management Analyst	[redacted]	Service Excellence Officer
Change Manager	[redacted]	Service Excellence Officer
Change Analyst	[redacted]	Service Excellence Officer
Agency Account Manager 1	[redacted]	Engagement Executive
Agency Account Manager 2	[redacted]	Agency Account Manager 1
Agency Account Manager 3	[redacted]	Agency Account Manager 1
Agency Account Manager 4	[redacted]	Agency Account Manager 1
Agency Account Manager 5	[redacted]	Agency Account Manager 1
Agency Account Manager 6	Unnamed	Agency Account Manager 1
Agency Infrastructure Architect 1	[redacted]	Sr. Enterprise Architect
Agency Infrastructure Architect 2	[redacted]	Sr. Enterprise Architect
Agency Infrastructure Architect 3	[redacted]	Sr. Enterprise Architect
Agency Infrastructure Architect 4	[redacted]	Sr. Enterprise Architect
Agency Infrastructure Architect 5	[redacted]	Sr. Enterprise Architect
Agency Infrastructure Architect 6	[redacted]	Sr. Enterprise Architect
Finance Analyst	[redacted]	Finance Manager
Finance Manager	[redacted]	Engagement Executive
IBM Project Executive	[redacted]	Engagement Executive
IBM Service Delivery Executive	[redacted]	Program Manager

Engagement Executive: [redacted]

The Program Management Office will confirm that the Unisys Team meets all of your requirements for the new contract under the leadership of [redacted] **(based in Harrisburg)**, who has worked closely with Commonwealth executives to manage many aspects of the current DPH Program during the past 5 years. On joining Unisys, Ann oversaw the contract, managing commitments and expectations for the major transformation and infrastructure consolidation initiative with the contract's extension in 2008.

During her tenure with Unisys, Ann spearheaded a number of innovative technology solutions that reduced cost for the Commonwealth, including server virtualization and the implementation of a shared infrastructure strategy. She also fostered the evolution of the DPH architecture to new technology concepts, including disk-based backup solutions and flexible service offerings. Ann has also demonstrated vigilance in customer satisfaction by implementing a number of in-depth survey processes designed to take the customer's pulse at many different levels on all aspects of service. She has held the team accountable to document issues and follow-up actions in collaboration with the agencies. These activities significantly improved customer satisfaction across the board.

Ann has 26 years of experience with managing large-scale outsourcing contracts, leading teams of more than 500 staff members to achieve service excellence. She thoroughly **understands the Commonwealth's goals for the Data Center Computing Services engagement and has achieved success with managing similar consolidation and Data Center migration initiatives** as the Vice President, Technical Services at Cegedigm-Dendrite. During her 10 years at the company, Ann implemented global data center standards, attained the highest customer satisfaction ratings ever achieved, and grew the operation's scope by more than 900 percent.

Under Ann's direction, her team had many successes, including designing and building a world-class data center from the ground up, then migrating dozens of customers to the center without disruption. **She provided a vision that led to the adoption of new technologies designed to reduce operational costs and provide customers with increased flexibility.** She established a winning culture and a team that always stepped up to the plate regardless of time pressures or the complexity of projects undertaken. Under her leadership, the reputation of the company's support services was dramatically enhanced.

Name	Proposed Account Role	Position in Organization	Experience in Proposed Role (Years)
Role on last 3 projects		**Qualifications for Proposed Role**	
[redacted]	Engagement Executive	Engagement Executive	15 years
• Unisys, DPH Engagement Executive (2 years) DPH Service Delivery Director (2 years) DPH Chief Technologist (1 year) • Cegedigm-Dendrite, Vice President, Technical Services (10 years) • Electronic Data Systems, Operations Manager (11 years)		• 15 years managing high-quality, large-scale outsourcing programs with extremely high SLA achievement and customer satisfaction • ITIL V3 Foundation Certified • Established Commonwealth leader with 5 years of experience managing the DPH contract, including the 2008 Transformation • 26 years managing programs with complex Data Center Services transitions, including data center facility design, consolidations, and physical and logical data center migrations • Laser focused on driving organizations to continually improve service level performance and customer satisfaction	
100% Dedicated to the Commonwealth Data Center Computing Services Project			

PMO Transition Manager: [redacted]

[redacted] **(based in Harrisburg)** will serve the Commonwealth as PMO Transition Manager 1 under the new contract. He brings 27 years of IT delivery experience working for large IT outsourcing firms before joining Unisys at the beginning of this year. As a Transition Management Consultant working for Dell Services/Perot Systems, Scott led four large-scale data center transitions, migrations, and system upgrades during his 5-year tenure.

Scott has achieved ITIL Foundations V3 and Project Management Professional certifications and applies the strengths of these methodologies in his approach to transition management. He has a long track record of success with building and leading technology teams on new business development initiatives and transformational programs for existing clients. Scott is a well-organized, communicative business professional who is proficient at establishing fruitful relationships with clients and Unisys technical teams to create synergistic transition support units.

Name	Proposed Account Role	Position in Organization	Experience in Proposed Role (Years)
Role on last 3 projects		**Qualifications for Proposed Role**	
[redacted]	PMO Transition Manager 1	Transition Director	5 years
• Unisys, Transition Director (1 year) • Dell Services, Transition Management (1 year of responsibility for *all* healthcare transitions and 4 years as a consultant) • Electronic Data Systems, Client Delivery Executive (8 years)		• Provided stellar leadership managing four large-scale data center transitions, migrations, and system upgrades for Dell Services • Exceptional experience with managing accounts, project requirements, and building and leading technical teams • Certifications: ITIL V3 Foundation, Project Management Professional	
100% Dedicated to the Commonwealth Data Center Computing Services Project			

Service Delivery Executive (Program Manager): [redacted]

[redacted] **(based in Harrisburg, PA)** will be serving the Commonwealth as the Service Delivery Executive (Program Manager) under the data center compute services contract. He joined the Unisys Team on July 1, 2013 as Service Delivery Director on the Data PowerHouse project. He brings 14 years of experience leading several large Service Delivery organizations supporting outsourced engagements for Computer Sciences Corporation (CSC). Ricky will leverage his experience leading a number of large-scale data center delivery teams, including the Textron account where he directed the consolidation of 10 sites with multiple mainframes and over 800 open systems servers, and then managed an ongoing Service Delivery team of 500 employees.

Ricky is a charismatic, service-driven leader who builds strong performing teams and a winning culture. He has specific management experience with all technologies in use by the Commonwealth. Ricky has attained ITIL V3 Foundations certification and has a demonstrated track record of success with establishing process discipline and sound metrics that have facilitated performance improvements. For example, his attention to process discipline resulted in improving a 60%-70% SLA achievement to consistently realizing 99.5% or better in two separate major CSC clients in less than a year.

Name	Proposed Account Role	Position in Organization	Experience in Proposed Role (Years)
[redacted]	Program Manager (Service Delivery Executive)	Program Manager (Service Delivery Executive) as of July 1, 2013	14 Years
Role on last 3 projects		**Qualifications for Proposed Role**	
• Unisys, DPH Service Delivery Director, effective July 1, 2013 • CSC, Service Delivery Executive (14 years) • Powercom-2000, Global IT Manager (4 years)		• 28 years of experience in senior IT leadership roles, with specialization in large outsourcing engagements • Energetic leader adept at motivating large teams to accomplish goals in fast paced environments • Managed Service Delivery organizations of more than 400 employees through extensive data center consolidation and migration initiatives • Solid track record of process re-engineering to achieve exceptional SLA performance and customer satisfaction • Great communicator with strong emphasis on customer executive relationships	
100% Dedicated to the Commonwealth Data Center Computing Services Project			

Service Excellence Officer: [redacted]

[redacted] will serve the Commonwealth as the Service Excellence Officer under the new contract. He is a 32-year Unisys employee who has held a variety of Operations and Quality Management leadership roles supporting numerous Unisys and customer organizations. Michael achieved Six Sigma Lean Black Belt Certification and is well versed in Six Sigma and Lean quality principles. He is ITIL V3 2011 Foundation certified. Leveraging this background, Michael has facilitated numerous client business planning and continual service improvement workshops for Unisys key accounts. Through his leadership, many Unisys teams reengineered operational processes streamlining operations by 30 percent

Michael has conducted multiple Kaizen Process Optimization workshops with the Unisys Team supporting the Commonwealth of Pennsylvania. One of these workshops laid the groundwork to transition the DPH contract from an antiquated Remedy system to the current ITSM 7.6 Remedy system. Michael led the team in the identification of process gaps that needed to be addressed to align local processes with ITIL-aligned industry best practices. He will be leveraging an optimized approach refined from numerous past successes with continuous improvement and process management and confirm that metrics and controls are established, analyzed, improved, and maintained to drive Service Excellence and Continuous Improvement.

Name	Proposed Account Role	Position in Organization	Experience in Proposed Role (Years)
Role on last 3 projects		**Qualifications for Proposed Role**	
[redacted]	Service Excellence Officer	Director of Operations, North America	2 years
• Unisys, Operations Management for North America Global Managed Services organization (2 years) • Unisys, Account Process Optimization for DPH and the Commonwealth (2012) • Unisys, ITSM7 Transition Kaizen Workshop for DPH and the Commonwealth (2009)		• More than 30 years of experience in service delivery, with focus on operations, quality, service improvement, and finance • Demonstrated leadership in service excellence, with extensive training and experience in Six Sigma Lean (Black Belt), ITIL, Kaizen facilitation, project and program management • In-depth knowledge of the DPH project, account process, and ITSM7 • Certifications: Six Sigma Lean Black Belt, ITIL V3 Foundation (with ITIL Intermediate Practitioner Service Transition/Change Management certification in progress)	
100% Dedicated to the Commonwealth Data Center Computing Services Project			

Senior Enterprise Infrastructure Architect: [redacted]

[redacted] **(based in Harrisburg)** will serve the Commonwealth as the Senior Enterprise Architect under the new contract. He has 16 years of IT industry experience working for IBM in a number of architect roles before joining Unisys in 2011 as the Lead Client Architect managing the North American Client Architect team, which included overseeing the Client Architects supporting the Commonwealth. While working for IBM, Bryan served as Transformation Integration Architect leading a large team of architects to develop technical components to build a multi-tenant data center to support the State of Georgia's strategic consolidation plans.

Bryan has served in roles providing strategic technical advice to account directors and state agency CIOs and CISOs, developing consumption-based managed hosting service models, and developing business continuity system architectures to support recovery of critical business applications. Having supported numerous agencies for the State of Georgia, he is well versed on the importance of regulatory compliance and has led architecture teams to integrate federal regulatory guidelines and requirements into technology solutions. Bryan is an accomplished technologist and excellent communicator who keeps stakeholders informed through a rigorous architecture review process and periodic technology briefings.

<table>
<tr><th>Name</th><th>Proposed Account Role</th><th>Position in Organization</th><th>Experience in Proposed Role (Years)</th></tr>
<tr><th colspan="2">Role on last 3 projects</th><th colspan="2">Qualifications for Proposed Role</th></tr>
<tr><td>[redacted]</td><td>Senior Enterprise Infrastructure Architect</td><td>North American Lead Architect</td><td>7 years</td></tr>
<tr><td colspan="2">Unisys, Lead Architect (2 years)
IBM, Transformation Integration Architect for the State of Georgia (2 years)
IBM, Transformation Integration Architect for Virgin Mobile (20 months)</td><td colspan="2">Demonstrated experience and success in leading a large team of architects to develop technical components (server, storage, network, security) to build a multitenant data center to support the State of Georgia’s strategic and consolidation plans
Domain expertise in managed hosting services, capacity on demand, data center architecture, system architecture, servers, virtualization, security, and networking
Certifications: IBM IT architect (infrastructure), Open Group Master IT Architect, and ITIL V3 Foundation</td></tr>
<tr><td colspan="4">100% Dedicated to the Commonwealth Data Center Computing Services Project</td></tr>
</table>

Incident Management Manager: [redacted]

[redacted] **(based in Harrisburg)** will serve the Commonwealth as the Incident Management Manager under the new contract. He is an 8-year Unisys employee who has contributed to a number of Unisys outsourcing engagements across multiple service lines, including data center services, managed service desks, and field services. Tom is a versatile, results-driven service delivery professional with a proven ability to develop strong client relationships, build teams, and deliver on commitments with a solid emphasis on quality and continuous improvement.

Tom has held a number of leadership and process management roles, including oversight of problem, incident, and change management processes for many Unisys clients supported in our multi-client service center in Salt Lake City, Utah. He also monitored and managed services as well as maintained consistent delivery to contracted service level agreements. Tom is well-versed in Six Sigma Lean Green Belt and ITIL V3 Foundation methodologies that he consistently applies in the performance of his duties. He will move to Harrisburg at the beginning of the Data Center Computing Services contract.

Name	Proposed Account Role	Position in Organization	Experience in Proposed Role (Years)
[redacted]	Incident Management Manager	Account Relationship and Service Delivery Manager	6 years
Role on last 3 projects		**Qualifications for Proposed Role**	
• Unisys, Account Relationship Manager for a Microsoft Retail store environment (not permitted to name) (1 year) • Unisys, Account Relationship Manager for NEC/7-11 (2 years) • Unisys, Service Delivery Manager, General Growth Properties (2 years)		• More than 6 years of proven ability to direct and deliver new client implementations and steady state operations • Skills: Incident, change and problem management; SLA/KPI management; quality improvement program implementation and management; continuous improvement; and new process development and implementation • Training: ITIL V3, Six Sigma Lean Green Belt	
100% Dedicated to the Commonwealth Data Center Computing Services Project			

Change Manager: [redacted]

[redacted] **(based in Harrisburg)** will serve the Commonwealth as the Change Manager under the new contract. He is a thorough and results-oriented information technology professional with more than 30 years of experience in delivering advanced technical support to government agencies. Stephen is a 9-year Unisys employee who has worked for the Commonwealth of Pennsylvania as a Service Delivery Manager on the DPH contract. In this role, he has worked with numerous Commonwealth agencies, enabling data center needs and services to be met, including managing large-scale technology refresh projects, the capacity planning process, and all details of agency change and incident management processes.

Stephen is well-known for his ability to achieve results and effectively manage projects as well as his process management diligence. His orientation to detail has effectively confirmed that Commonwealth changes are scheduled and executed by the most qualified resources wherever possible without incident. Stephen has extensive experience with managing organizations through significant periods of change, including leading the DPH ERP implementations for the Integrated Enterprise System (IES) and the Department of Revenue (DOR).

Name	Proposed Account Role	Position in Organization	Experience in Proposed Role (Years)
[redacted]	Change Manager	Service Delivery Manager	9 years

Role on last 3 projects	Qualifications for Proposed Role
• Unisys, IT Service Delivery Manager at the DPH project (7.6 years) • Unisys, IT Resource and Asst. Technical Support Manager at the DPH project (1.6 years) • Endress+Hauser, Advanced Systems Group Manager and LAN Manager (2 years) • U.S. Air Force (22 years); encompassed several Change Management positions	• More than 30 years of IT experience • More than 9 years of experience on the DPH project, largely as a service delivery manager with deep knowledge of all service delivery processes, particularly change management • Proven change management expertise, having led process creation for 13 Commonwealth agencies, focusing on providing change management resource allocation performance reporting, capacity planning, contractual requirements, and incident reporting for data centers. • Demonstrated expertise in delivering advanced technical support to government agencies and meeting their technology needs by monitoring security, updating systems, and troubleshooting. • Certifications: ITIL V3 Foundation (with ITIL Intermediate Practitioner Service Transition/Change Management certifications in progress)

100% Dedicated to the Commonwealth Data Center Computing Services Project

Change Analyst: Beth Villarreal

Beth Villarreal (based in Harrisburg) will serve the Commonwealth as a Change Analyst under the new contract. She is a 30-year Unisys employee who has worked to support the Commonwealth for the past 16 years in operational leadership positions, including Change Manager, Help Desk Manager, and Agency Liaison to Data Center Operations.

In her current role as Change Manager, Beth works with DPH technical teams to process more than 300 data center infrastructure changes per month on average, confirming that all change requests include required information such as detailed tasks and back out plans. As a true leader, a collaborative approach comes naturally to her when working with the DPH team, and she is diligent in equipping team with process and ITSM product training to successfully execute the change management process.

Name	Proposed Account Role	Position in Organization	Experience in Proposed Role (Years)
Role on last 3 projects		**Qualifications for Proposed Role**	
[redacted]	Change Analyst	Change Analyst	10 years
• Unisys, Data Center Analyst for the DPH project (10 years) • Unisys, Computer Operations Supervisor for the DPH project (4 years) • Lockheed Martin, Operations Manager (3 years)		• 27 years of experience providing data center analysis, change analysis, and support • Extensive experience with Remedy IT Services Management, with certifications in change management and resource tracking software • Certification: ITIL V3 Foundation	
100% Dedicated to the Commonwealth Data Center Computing Services Project			

Service Level Management Analyst: [redacted]

[redacted] **(based in Harrisburg, PA)** will be serving the Commonwealth as a Service Level Management Analyst under the new contract. She has worked in the IT industry and specifically in large data centers for over 11 years, and will be joining Unisys in July 2013. Suzanne utilizes strong interpersonal skills and a keen attention to detail in order to successfully deliver high-quality, detailed analysis and reporting, which drive cost-effective, quality IT solutions and continuous service improvement to her clients.

Suzanne has detailed knowledge of IT Service Management and in managing ITIL IT processes: service level management, change management, capacity management, and business continuity management. While working in the IT Industry, Suzanne's responsibilities have included: building a comprehensive model for capacity metrics and consolidation reporting; implementing executive reporting summarizing daily processing metrics and current problem status to provide complete transparency; defining and negotiating service-level agreements with customers and service partners to improve customer satisfaction; and managing facility availability activities to 99.99% availability. Suzanne's extensive experience, knowledge, and communication skills will confirm that SLAs are effectively managed, analyzed, and communicated to the Commonwealth.

Name	Proposed Account Role	Position in Organization	Experience in Proposed Role (Years)
Role on last 3 projects		**Qualifications for Proposed Role**	
[redacted]	Service Level Management Analyst	Service Level Management Analyst (as of July 2013)	11 years
• Unisys, Service Level Management Analyst, (as of July 2013) • Comcast, Data Center Services Manager and Data Center Management Tools Program Manager (6 years) • Yellow Book USA, Senior Data Center Operations Manager (11 years)		• 20 years of IT industry experience with primary focus on data center services, tools and reporting • Built a comprehensive model for capacity metrics and consolidation reporting • Implemented executive reporting summarizing daily processing metrics and current problem status to provide complete transparency; • Defined and negotiated service-level agreements with customers and service partners to improve customer satisfaction	
100% Dedicated to the Commonwealth Data Center Computing Services Project			

Finance Manager: [redacted]

[redacted] will be serving the Commonwealth as the Finance Manager on the Data Center Computing Services contract. He is a tenured Unisys employee who has held various financial management positions for more than 25 years, most recently the past 13 years as the Finance Manager on the Commonwealth of Pennsylvania DPH contract. Gary delivers financial management and billing oversight for several Unisys internal organizations and subcontractors.

Because of his experience with the Commonwealth, Gary has a clear understanding of the Commonwealth's financial processes and requirements for invoicing at the agency level and the tracking of federal funds against grants by project. He has supported restructuring of billing reports into a single Commonwealth invoice with agency-level detail. He is a motivated, conscientious, and diligent professional who takes a meticulous approach to the management of all aspects of finance, including development of financial plans, invoicing and billing activities, change order pricing and processing, and Service Level Agreement tracking.

Name	Proposed Account Role	Position in Organization	Experience in Proposed Role (Years)
[redacted]	Finance Manager	Financial Analysis Manager	25 years
Role on last 3 projects		**Qualifications for Proposed Role**	
• Unisys, Manager, Financial Analysis for the DPH project (14 years) • Unisys, Manager, Business Operations Data Center (7 years) • Unisys, Financial & Asset Control Government Systems (6 years)		• 14 years as a finance manager supporting the DPH project in Harrisburg • In-depth understanding of the DPH billing processes • Designed and implemented many process improvements for the DPH project • Recipient of Unisys Excellence Award • Certification: ITIL V3 Foundation	
100% Dedicated to the Commonwealth Data Center Computing Services Project			

Finance Analyst: [redacted]

[redacted] **(based in Harrisburg)** will be serving the Commonwealth as a Financial Analyst on the Data Center Computing Services contract. He has worked in a variety of financial and accounting roles over the past 30 years, with the past 13 years working for Unisys on the Commonwealth of Pennsylvania DPH contract as the Financial Analyst and Project Controller. In his current role, David provides financial reporting and analysis for Unisys management, internal auditors, and external auditors and oversees a wide range of activities, including journal entries, internal billing, external billing, revenue recognition, cash collection, receivables, and asset database entries.

David has extensive experience with preparing amendments to Commonwealth agency fee schedules together with contract change orders. He developed internal processes to confirm the change order impacts agree with timing used in Commonwealth invoicing programs. David continually has an eye on process improvement and was recognized with Unisys Excellence and Silver Recognition Awards for his unwavering customer commitment.

Name	Proposed Account Role	Position in Organization	Experience in Proposed Role (Years)
Role on last 3 projects		**Qualifications for Proposed Role**	
[redacted]	Finance Analyst	Senior Project Controller and Financial Analyst	36 years
• Unisys, Project Controller and Financial Analyst for the DPH project (14 years) • AMP, Financial Analyst (2 years) • AMP, Pricing Accountant (14 years)		• 14 years as project controller and financial analyst supporting the DPH project in Harrisburg • Extensive experience with billing and accounts receivables • Supported the creation and improvement of consolidated billing process • Recipient of the Unisys Excellence Award and Silver Recognition Award for Unwavering Customer Commitment • Certification: ITIL V3 Foundation	
100% Dedicated to the Commonwealth Data Center Computing Services Project			

Agency Account Manager: [redacted]

Peter Cavanaugh (based in Harrisburg) will serve the Commonwealth as an Agency Account Manager under the new contract. He is a 23-year Unisys employee who has worked for the Commonwealth of Pennsylvania since 2002 in a variety of project management and client services management roles supporting numerous Commonwealth organizations. Since 2005, he has worked on site at the Enterprise Data Center in very close collaboration with the CTO, CISO, Client Management, EDC, Enterprise Networking and Security, Enterprise Services, GIS, PMO, and many agencies.

Peter developed and introduced a customer satisfaction program for the EDC that continues today under the Bureau of Enterprise Services as an important component of OIT's process for continuous improvement and building strategic relationships. Under this program, he facilitated regular communications and acted as a liaison for OIT with the CIOs for half of the agencies, describing the center's managed services programs, facility services, and benefits.

Communications, customer service and satisfaction, facilitation, infrastructure, project and program management, and strategic relationship building are common threads of Peter's experience of more than a decade working with the Commonwealth and more than 20 years working at Unisys.

<table>
<tr><th>Name</th><th>Proposed Account Role</th><th>Position in Organization</th><th>Experience in Proposed Role (Years)</th></tr>
<tr><td colspan="2">Role on last 3 projects</td><td colspan="2">Qualifications for Proposed Role</td></tr>
<tr><td>[redacted]</td><td>Lead Agency Account Manager</td><td>Project Manager and Client Service Manager</td><td>5 years</td></tr>
<tr><td colspan="2">• Unisys, Project Manager and Client Service Manager, Pennsylvania Commonwealth Technology Center (5 years)
• Unisys, Project Manager and Resource Manager (6 years)
• Unisys, Portfolio Sales Executive (5 years)</td><td colspan="2">• More than 10 years of experience working in project management and client service roles in the Commonwealth Technology Center
• Proven project management and communications skills and a reputation for bringing commitment and energy to each assignment
• A unique blend of project management and sales experience and knowledge of the Commonwealth and its many leaders
• Certifications: ITIL V3 Foundation, Project Management Professional</td></tr>
<tr><td colspan="4">100% Dedicated to the Commonwealth Data Center Computing Services Project</td></tr>
</table>

Agency Account Manager: [redacted]

[redacted] **(based in Harrisburg)** will serve the Commonwealth as an Agency Account Manager under the new contract. He has more than 15 years of experience working in the IT industry and has supported the Commonwealth of Pennsylvania since 1999, holding positions of progressive responsibility, including his current role as the Service Delivery Manager at the Commonwealth's EDC. In this role, Kannan actively collaborates with many Commonwealth agency IT managers to form technology solutions to address business needs with long-term operational strategies that enable real value to be delivered to the Commonwealth. He is well versed with the Commonwealth standards and ITBs and has personally contributed to developing a few of the ITBs.

Kannan understands the importance of agency participation in major consolidation and migration projects because he played a large role in architecting the e-Government server farm for the Commonwealth to host Web applications for various agencies. On this project, Kannan leveraged excellent leadership and communication skills to direct a team of technical consultants and to collaborate with more than 40 agencies in their successful application deployment and operation, functioning as a liaison, and moving ideas between the development community and the customer community to confirm the needs of the Commonwealth were represented in the server farm's design and delivery.

Name	Proposed Account Role	Position in Organization	Experience in Proposed Role (Years)
[redacted]	Agency Account Manager	Service Delivery Manager	6 years
Role on last 3 projects		**Qualifications for Proposed Role**	
• Unisys, Service Delivery Manager and Operations Architect, Pennsylvania Commonwealth Technology Center (6 years) • Unisys, Operations Architect, Pennsylvania Commonwealth Technology Center (6 years) • Unisys, Team Leader, Pennsylvania Commonwealth Technology Center (2 years)		• More than 14 years at the Commonwealth's EDC ascending from a technical role in 1999 to the current position as Service Delivery Manager, a role that spans responsibilities for customer relations and satisfaction, technology consulting, operations, and account management. • An original member of the EDC and the center's Operations Architect for more than a decade; offers a very deep understanding of all aspects of the EDC and application hosting. • A very distinctive blend of technology, customer service, operations, and communications knowledge, skills, and experience. • Certifications: PMP, ITIL V3 and V2 Foundation, MCSA 2003, MCSE 2000	
100% Dedicated to the Commonwealth Data Center Computing Services Project			

Agency Account Manager: [redacted]

[redacted] **(based in Harrisburg)** will serve the Commonwealth as an Agency Account Manager under the new contract. He is a 7-year Unisys employee who has worked for the Commonwealth of Pennsylvania for more than 15 years, providing technology solutions, consulting, and complex project management services. For the past 7 years, Brian has served the Commonwealth on the Unisys DPH contract in various Service Delivery and Business Management roles acting as a liaison to the Office of Administration and agencies receiving service.

Brian provided exceptional leadership to the DPH team through the alignment with ITIL best practices and the migration to the new ITSM Remedy system. With a service-centric approach, he directed the service delivery organization to support complex solution/design implementation, managed services functions, quality improvement, and cost management activities. He is skilled at contract management and managing vendors and subcontractors to ensure shared accountability for outcomes.

Name	Proposed Account Role	Position in Organization	Experience in Proposed Role (Years)
[redacted]	Agency Account Manager	Account Business Management and Service Delivery Manager	7 years

Role on last 3 projects	Qualifications for Proposed Role
• Unisys, DPH Account and Service Delivery Management (7 years) • Computer Aid, Senior Consultant (4 years) • IBM, Principal Consultant (5 years)	• IT Services professional with 34 years of experience helping customers achieve their IT objectives • 7 years in account and service delivery management supporting the DPH project • Extensive knowledge of the DPH IT infrastructure, processes, deliverables, and personnel • Diverse IT background with proven expertise in consulting, technology, and business development • Education: M.S., Information Systems, Penn State; MBA, Rutgers University; BA, Computer Science SUNY Potsdam • Certifications: PMP and ITIL V3 Foundation

100% Dedicated to the Commonwealth Data Center Computing Services Project

Agency Account Manager: [redacted]

[redacted] **(based in Harrisburg)** will serve the Commonwealth as an Agency Account Manager under the new contract. She has worked in the IT industry for 14 years and is a 5-year Unisys employee supporting the Commonwealth of Pennsylvania as a Service Delivery Manager on the DPH contract. Lydia has worked with numerous Commonwealth agencies to develop strong partnerships with agency leadership while aligning Unisys service delivery teams with executing policies and procedures as outlined in the contract with a focus on agency priorities and outstanding customer service.

Lydia adroitly oversees subcontractors to maintain top-notch service delivery across environments deployed at the DPH. She has managed numerous successful initiatives, including implementations of new systems for the Pennsylvania Liquor Control Board and the Department of Health, along with hardware upgrades for the Department of State. Lydia is a superb communicator who keeps agency management informed of the status of initiatives and she received numerous accolades from Commonwealth management for her unwavering professionalism and skilled leadership.

Name	Proposed Account Role	Position in Organization	Experience in Proposed Role (Years)
[redacted]	Agency Account Manager	Service Delivery Project Manager	14 years

Role on last 3 projects	Qualifications for Proposed Role
• Unisys, Service Delivery Manager (5 years) • Affiliated Computer Sciences, Account Manager, (9 years) • Foundation Health, Program Director (2 years)	• 5 years in account and service delivery management supporting the DPH project • In-depth knowledge of business and service needs for many agencies, including State Police, Department of Environmental Protection, Department of State, and Department of Health • Excellent interpersonal, customer service and general communication skills • Extensive project and program management experience • Certification: ITIL V3 Foundation
100% Dedicated to the Commonwealth Data Center Computing Services Project	

Agency Infrastructure Architect: [redacted]

[redacted] **(based in Harrisburg)** will serve the Commonwealth as one of our Agency Infrastructure Architects under the new contract. He has more than 18 years of experience in the IT industry working in data center technical management and architecture roles; for the past 4 years, he has worked as a Client Architect supporting the Commonwealth on the DPH contract. In his role at the DPH, Mike designed detailed technical data center solutions for 17 Commonwealth agencies across all technology platforms supported at the DPH.

Mike routinely provides guidance and recommendations to Commonwealth agencies on emerging technologies to increase performance, gain functionality, and reduce cost. He has a solid track record of developing highly accurate solutions that are subsequently implemented successfully because of his attention to detail. With a strong background in data center technical management, Mike understands the importance of having technical team members participate in the solution development and takes a collaborative approach to fostering accountability on the team, promoting a successful implementation.

Name	Proposed Account Role	Position in Organization	Experience in Proposed Role (Years)
[redacted]	Agency Infrastructure Architect	Client Architect	4 years
Role on last 3 projects		**Qualifications for Proposed Role**	
• Unisys, Client Architect at the DPH (4 years) • Cegedigm Dendrite, Technical Account Manager and Project Manager (3 years) • Dendrite International, Director of Hardware Services (2 years)		• More than 18 years in technical management and architect roles for government and commercial enterprises • In-depth knowledge of the DPH; worked as key member of the data center transformation project team to transition to a shared enterprise infrastructure model • Proven technical expertise, designing detailed technical data center solutions to support 17 Commonwealth agencies covering mainframe, server, storage, networking, software, and facility components • Strong record of success with data center architecture, management, and relocations • Certification: ITIL V3 Foundation	
100% Dedicated to the Commonwealth Data Center Computing Services Project			

Agency Infrastructure Architect: [redacted]

[redacted] **(based in Harrisburg)** will serve the Commonwealth as one of our Agency Infrastructure Architects under the new contract. She has worked in various roles supporting the Commonwealth over the past 12 years, starting as a long-term consultant to the Department of Public Welfare providing network security expertise for the installation, configuration, and maintenance of the department's extranet. In her current role, Shobha provides architecture services and manages the implementation teams supporting the secure integration of agency applications into the EDC.

Shobha has worked with numerous agencies establishing positive customer relationships and confirming that solutions developed fulfill agency business needs. She has demonstrated superior knowledge across various data center technologies, including Windows server, virtualization, and network. She also attained CISSP certification acknowledging her expertise in security. Shobha is a strong leader who has skillfully led her team through the implementation of several solutions over the 9 years she has worked in the EDC. This experience enables her to implement solutions that are well thought with successful implementation in mind.

<table>
<tr><th>Name</th><th>Proposed Account Role</th><th>Position in Organization</th><th>Experience in Proposed Role (Years)</th></tr>
<tr><th colspan="2">Role on last 3 projects</th><th colspan="2">Qualifications for Proposed Role</th></tr>
<tr><td>[redacted]</td><td>Agency Infrastructure Architect</td><td>IT Manager</td><td>9 years</td></tr>
<tr><td colspan="2">Unisys, Manager, OA EDC (3 years)
Unisys, Deployment Consultant, OA EDC (6 years)
Citibank, Consultant (3 months)
Unisys, Consultant, Pennsylvania Department of Public Welfare (2 years)</td><td colspan="2">More than 14 years of IT experience
9 years of service and technical excellence at the OA EDC
Proven expertise with TCP/IP Networking, DNS and Name Services; joining Active Directory domains; COM+ applications; IIS Web server and its configuration, administration, and troubleshooting; Access Control; Public Key Infrastructure; CA SiteMinder; Virtual Directory (RadiantOne); VPN; and Portal Technologies
Broad experience implementing high availability solutions using CSS (Cisco Content Switches), Microsoft Windows Clustering, NLB, and Application Center; hands-on experience with designing and implementing Web publishing solutions using Microsoft ISA Server.
Certifications: CISSP, ITIL V3 Foundation, Windows MCSE</td></tr>
<tr><td colspan="4">100% Dedicated to the Commonwealth Data Center Computing Services Project</td></tr>
</table>

Agency Infrastructure Architect: [redacted]

[redacted] **(based in Harrisburg)** will serve the Commonwealth as one of our Agency Infrastructure Architects under the new contract. He has worked for Unisys supporting many Commonwealth agencies in the DPH over the past 5 years. While at the DPH, Brett spearheaded several initiatives that advanced our architecture and support capabilities in Windows and backup technologies, including consolidation of the DPH NetBackup infrastructure that significantly reduced compute and media resources consumed by the backup process.

Brett has worked closely with many DPH agencies and took the lead in developing and executing the migration of the Integrated Enterprise Systems Windows platform to the DPH. Brett also determined a strategy for using the virtual infrastructure to replicate backup master servers to the disaster recovery site, expediting this component's recovery time from 2.5 hours to 30 minutes. He has consistently applied ingenuity and creativity to developing solutions that solve agency and DPH technology challenges.

Name	Proposed Account Role	Position in Organization	Experience in Proposed Role (Years)
[redacted]	Agency Infrastructure Architect	Systems Analyst and Project Leader	9 years
Role on last 3 projects		**Qualifications for Proposed Role**	
• Unisys, Systems Analyst and Project Leader, at the DPH (5 years) • Business Information Group, Network Engineering Consultant (1 year) • Rite Aid Corporation, Systems Administrator and Development (3 years)		• 5 years of experience as a systems analyst at the DPH managing regular upgrades, security enhancements, virtualization deployments, data center consolidations and migrations, and DR design • Through his ingenuity, has implemented a number of Windows and backup technology innovations to gain process efficiencies at the DPH • Expansive knowledge in the following areas: VMware vSphere ESX/ESXi 3.x, 4.x, & 5.x; Windows 2003, 2008, & 2012; Powershell & VB Script; Active Directory; Security Policies; IIS; DHCP; DNS; FTP; IBM Blade Center Servers; Dell and IBM x86 systems; Enterprise Backup/Replication & Disaster Recovery technologies, including Symantec NetBackup, EMC Data Domain, EMC Avamar, Microsoft Failover Clustering, Network Load Balancing, and Microsoft DFS & DFS-R • Certifications: VMware VCP4, VMware VCP5, Microsoft Windows 2008 MCITP: SA, Microsoft Windows 2008 MCA: Virtualization, MCSA: Windows 2012, and ITIL V3 Foundation	
100% Dedicated to the Commonwealth Data Center Computing Services Project			

Security Manager: [redacted]

[redacted] will serve the Commonwealth as the Security Manager under the new contract. He brings more than 38 years of senior technical and management experience, including 6 years with the Commonwealth covering security design, consulting, project management, technology assessment, automation, and distributed network architecture. Mike has specialized security expertise throughout a broad range of product sets, including identity management, identification and credentialing, access control, and confirming compliance with security standards.

Mike has worked with several federal and state agencies, including the Pennsylvania State Police, where he managed security for the new Commonwealth Law Enforcement Assistance Network (CLEAN) upgrade encompassing security policy; access control by CA SiteMinder; and integration with PSP's RSA Adaptive Authentication using a RadiantOne Virtual Directory Server (VDS) as the user repository. He also collaborated with JNET to most efficiently provide access to CLEAN by JNET users without requiring additional authentication and assisted Commonwealth leadership creating Security ITBs. Mike's efforts enabled deployment of the new Megan's Law application to its full user base much faster than would have been achievable otherwise, enabling PSP to meet its legislatively mandated deadline.

Name	Proposed Account Role	Position in Organization	Experience in Proposed Role (Years)
[redacted]	Chief Information Security Officer	Senior Security Architect	4 years
Role on last 3 projects		**Qualifications for Proposed Role**	
• Unisys, Security Architect and effective Unisys CISO at the Pennsylvania State Police (4 years) • Unisys, Security Architect at the Michigan Department of Human Services (2 years) • Unisys, Security Architect at the U.S. Department of Justice (1 year)		• 38 years of technical, business, and management experience in the IT and manufacturing automation industries • 6 years supporting the Commonwealth of Pennsylvania, including 4 acting as the Unisys CISO for PSP's CLEAN Services Project • Experienced with security policy and design, consulting, technology assessment, project management, automation, and distributed network architecture • Broad experience with overseeing large, complex projects to verify compliance with both security requirements and security policies and standards • Excellent technical, leadership, and communication skills • Certifications: CISSP (ISC2), GSEC (SANS/GIAC)	
100% Dedicated to the Commonwealth Data Center Computing Services Project			

PMO Transition Manager 2: [redacted]

[redacted] **(based in Harrisburg)** will serve the Commonwealth as PMO Transition Manager 2 under the new contract. He has spent more than 14 years on the IBM Commonwealth delivery team, gaining extensive experience in transition leadership, project management, IT infrastructure implementations, and IT operations and services management. Dave has held various leadership roles supporting the DPH, supporting the Integrated Enterprise System ERP contract, and as a project leader with the Department of Labor & Industry.

In October 2005, Dave led the transition of the Commonwealth's ERP systems from legacy providers to upgraded systems and network infrastructure on schedule and with no interruption to customer operations or applications. He has been successful on several similar large-scale transitions and projects by designing consistent transition plans with clear team member roles, responsibilities, and deliverables to enable every team member to understand his or her part of the transition. He understands that success relies on working together with the Commonwealth agencies to reach firm agreements on milestones and schedule.

Name	Proposed Account Role	Position in Organization	Experience in Proposed Role (Years)
Role on last 3 projects		**Qualifications for Proposed Role**	
[redacted]	PMO Transition Manager 2	Senior Project Manager	3 years
• IBM, DPH Service Delivery Manager (3 years) • IBM, IES Service Delivery Manager (5 years) • IBM, Network Support Project Leader at the Pennsylvania Department of Labor & Industry (7 years)		• Extensive experience in transition leadership, project management, IT infrastructure implementations and IT operations, and services management • Demonstrated performance in leading transition teams comprised of clients, subcontractors, and vendors for implementing data center operations services for mainframe and distributed technologies • More than 14 years of Commonwealth experience • Certifications: Cisco Certified Network Associate, ITIL V3 Foundation, Project Management Professional	
100% Dedicated to the Commonwealth Data Center Computing Services Project			

Availability Manager: [redacted]

[redacted] **(based in Harrisburg)** will serve the Commonwealth as the Availability Manager under the new contract. He is a 13-year IBM employee who has worked in operational leadership roles, including Availability and Change Manager and Data Center Operations Team Lead. Over the past 10 years, Mic has served as an IBM Availability and Change Manager for the Commonwealth of Pennsylvania Data PowerHouse project, and for 7 years he managed Data Center Operations for the Commonwealth's Integrated Enterprise System.

Mic brings expertise in overseeing processes, including availability management, trend analysis, change control, project planning, implementation, and reporting. He is adept at evaluating processes and applying process improvements, as evidenced by his contributions during our recent implementation of ITIL process standards and the new Remedy ITSM tool. He is well regarded by the Commonwealth and the DPH team for his expertise in the process management area.

Name	Proposed Account Role	Position in Organization	Experience in Proposed Role (Years)
Role on last 3 projects		**Qualifications for Proposed Role**	
[redacted]	Availability Manager	Availability Manager	10 years
• IBM, Availability Manager for DPH (3 years) • IBM, Availability and Change Manager for IES (7 years) • IBM, Microsoft Exchange Administrator for Lucent Technologies (1 year)		• 10 years of experience supporting the Commonwealth availability and change process management roles • ITIL V3 Foundations Certification • Adept at process improvement, streamlining, and process control metrics • Team leader for the Remedy ITSM7 and ITIL process implementation	
100% Dedicated to the Commonwealth Data Center Computing Services Project			

Agency Account Manager: [redacted]

[redacted] **(based in Harrisburg)** will serve the Commonwealth as an Agency Account Manager under the new contract. He has held a variety of IT leadership positions since joining IBM in 1976 and has worked with many Commonwealth agencies in the role of Service Delivery Manager for the past 12 years. He has a strong background and proven expertise in many IBM technologies, including zSeries and iSeries technical management, support of the Disaster Recovery process, and relationship management. Barry possesses strong working knowledge of many Commonwealth agencies' business priorities, aligning cost-effective Data Center solutions to meet agency needs.

Barry has extensive experience with managing Commonwealth agencies through planning and smooth execution of system migrations and upgrades to new hardware and software product upgrades. He possesses superior knowledge of disaster recovery and business continuity planning demonstrated by creation of the disaster recovery plans supporting all IBM mainframe customers of the DPH and coordination of all disaster recovery tests. Barry is highly regarded as an expert in the field and for his knowledge of the Commonwealth, as evidenced by commendable ratings in customer satisfaction surveys during his tenure.

Name	Proposed Account Role	Position in Organization	Experience in Proposed Role (Years)
Role on last 3 projects		**Qualifications for Proposed Role**	
[redacted]	Agency Account Manager	Service Delivery Manager	11 years
• IBM, Service Delivery Manager for DPH (11 years) • IBM, Disaster Recovery Coordinator Manager for DPH (3 years) • IBM, AS/400 Marketing Specialist (7 years)		• 14 years of service excellence on the DPH project • In-depth knowledge of business and service needs for many agencies, including the Department of Transportation, Department of Labor & Industry, and Department of Corrections • Proven communications skills and ability to build and manage teams • Demonstrated knowledge of IBM platforms and disaster recovery • Extensive experience in managing IT projects	
100% Dedicated to the Commonwealth Data Center Computing Services Project			

Agency Infrastructure Architect: [redacted]

[redacted] **(based in Harrisburg)** from our partner IBM will serve the Commonwealth as one of our Agency Infrastructure Architects under the new contract. Mary has more than 34 years of information technology experience and has been assigned to the IBM Commonwealth of Pennsylvania team since 1996, when she led the design and implementation of multiple complex IBM infrastructure solutions, including the SAP and Unemployment Compensation infrastructure environments.

Mary has supported Commonwealth agencies for the past 17 years, designing and implementing highly available IT systems and subsystems. Using a consultative approach, she works closely with agency IT technical and operations stakeholders to gather their requirements to develop systems management solutions that address needs of the business. Through her solutioning efforts, Mary has been instrumental in assisting the Commonwealth with the realization of goals to reduce the number of data centers and servers and to significantly increase server virtualization at the Commonwealth.

Name	Proposed Account Role	Position in Organization	Experience in Proposed Role (Years)
[redacted]	Agency Infrastructure Architect	Senior Certified IT Architect	17 years
Role on last 3 projects		**Qualifications for Proposed Role**	
• IBM, IT Architect for Unemployment Compensation Management System and Data Center for Pennsylvania Department of Labor & Industry • IBM, IT Architect for EDC at Commonwealth of Pennsylvania • IBM, IT Architect for Integrated Enterprise System (SAP) for Commonwealth of Pennsylvania		• More than 17 years of IT experience with the Commonwealth of Pennsylvania • More than 34 years of IT experience overall • Proven expertise with the design and implementation of complex infrastructure solutions, including the SAP and Unemployment Compensation infrastructure environments • Certifications: IBM Senior Certified Architect – Infrastructure; ITIL V3 Foundation	
50% Dedicated to the Commonwealth Data Center Computing Services Project			

Agency Infrastructure Architect: [redacted]

[redacted] **(based in Harrisburg)** will serve the Commonwealth as one of our Agency Infrastructure Architects under the new contract. He has more than 39 years of experience in the information technology field supporting the Commonwealth in various positions demonstrating superb skills in IBM mainframe technologies. Joe has supported the Commonwealth for 27 years, the past 14 years as an IT Architect on the DPH contract, and before that spending several years in various systems support roles at the Pennsylvania Department of Transportation.

Throughout his tenure on the DPH contract, Joe has continuously developed innovative solutions that improved the IBM mainframe platform performance and resiliency for agencies supported at the DPH. With the DPH transformation in 2008, he consolidated several disparate mainframe platforms onto a single z10 frame that exploited group capacity and sub-capacity software to allow the Commonwealth workloads to gain access to available MIPS beyond their allocated capacity and at the same time not exceeding software licensing limits. This innovation saved the Commonwealth millions of dollars by providing additional capacity to agencies experiencing extraordinary processing requirements for short periods.

Name	Proposed Account Role	Position in Organization	Experience in Proposed Role (Years)
[redacted]	Agency Infrastructure Architect 2	Senior IT Architect	14 years
Role on last 3 projects		**Qualifications for Proposed Role**	
• IBM, IT Architect, DPH (14 years) • IBM, Systems Engineer (13 years) • IBM, Operating System Programmer (2 years)		• 39 years of IT experience supporting the Commonwealth of Pennsylvania • More than 14 years with the DPH, designing, implementing, and maintaining highly available data center systems and subsystems • Proven expertise in designing and implementing technology infrastructure for complex information systems, including large enterprise systems and mid-range systems	
50% Dedicated to the Commonwealth Data Center Computing Services Project			

Agency Infrastructure Architect: [redacted]

[redacted] **(based in Harrisburg)** from PCN will serve the Commonwealth as one of our Agency Infrastructure Architects under the new contract. Charlie has worked on a variety of assignments crossing diverse technologies and industries, including government agencies and military contracts. He has performed as a Data Center Infrastructure Architect for large organizations for which he has focused on introducing emerging technologies and solutions to the company's vision and leveraging them to enhance capabilities and reduce cost.

Throughout his career, Charlie has consolidated more than 25 data centers to centralized mega-data centers, built three new data centers, designed six SANs across six data centers, and developed multiple Disaster Recovery solutions including the use of SunGard as well as in house Disaster Recovery solutions using internal infrastructure and data centers. He is skilled in a broad spectrum of data center infrastructure technologies we will be using for the Commonwealth solution.

<table>
<tr><th>Name</th><th>Proposed Account Role</th><th>Position in Organization</th><th>Experience in Proposed Role (Years)</th></tr>
<tr><th colspan="2">Role on last 3 projects</th><th colspan="2">Qualifications for Proposed Role</th></tr>
<tr><td>[redacted]</td><td>Agency Infrastructure Architect</td><td>Infrastructure Data Center Technical Architect</td><td>15 years</td></tr>
<tr><td colspan="2">• PCN, Solution Architect (5 years)
• Business owner and software developer (2 years)
• DHL Logistics, Manager IT Architecture (10 years)</td><td colspan="2">• Senior architect with more than 15 years of experience in designing, building, consolidating, and managing data centers and infrastructure
• Experience includes consolidating 25 data centers to centralized mega-data centers, building three new data centers, designing six SANs in six data centers, and developing multiple DR solutions
• Demonstrated ability to work in a team environment, solid negotiator, quickly learn new data center technologies and embrace change; driven and dedicated person with a passion for information technologies and solutions
• Certifications: ITIL, MCP, CheckPoint administration, project management</td></tr>
<tr><td colspan="4">100% Dedicated to the Commonwealth Data Center Computing Services Project</td></tr>
</table>

IBM Project Executive: [redacted]

[redacted] **(based in Harrisburg)** will serve the Commonwealth as the IBM Project Executive (PE) responsible for the leadership of the IBM team. In her current position as the IBM PE, she is responsible for the IBM scope of services to the Unisys Data Power House contract. Her background also includes a previous role supporting the DPH from 2000 to 2005 as the Deputy PE. Kathy's long standing commitment to excellence in support of the Commonwealth of PA agencies positions her well to lead the IBM team. She supported the agency transitions in 2000 during the contract start up and was part of the team who successfully brought the support to steady state.

Kathy has over thirty years of experience in leadership positions providing project management, customer satisfaction, and new business growth at IBM. For over fifteen years, Kathy's career focus has been in Strategic Outsourcing (SO) delivery and project management supporting multiple tower commercial outsourcing contracts with content including: Help Desk, Desktop support, Mid-range server management, Data Center operations, Application Management Services, Network Services and Mainframe print. Her experience includes managing multi-million dollar outsourcing contracts for customers in the Public Sector/State and Local Government, Healthcare, Insurance, and Telecommunications sectors. She holds several certifications including PMI Project Management Professional (PMP), IBM Project Management, IBM Project Executive, and ITILv3 Foundation. Kathy is well positioned to lead the IBM team to support the Data Center Computing Services project with strong, consistent delivery and with innovation to continue bringing value to the Commonwealth of PA.

<table>
<tr><th>Name</th><th>Proposed Account Role</th><th>Position in Organization</th><th>Experience in Proposed Role (Years)</th></tr>
<tr><th colspan="2">Role on last 3 projects</th><th colspan="2">Qualifications for Proposed Role</th></tr>
<tr><td>[redacted]</td><td>IBM Project Executive</td><td>IBM Project Executive</td><td>15 years</td></tr>
<tr><td colspan="2">IBM Project Executive, Unisys DPH contract, Commonwealth of Pennsylvania (6 months)
IBM Deputy Project Executive, Unisys DPH contract, Commonwealth of Pennsylvania (5 years)
IBM Project Executive supporting multiple public sector clients to address governance and contract stabilization (18 months)
IBM Project Executive supporting the MTA New York City Transit Data Center Services contract (5 years)</td><td colspan="2">More than 30 years of experience in leadership positions at IBM, with the last 15 years focused mainly on providing data center services to multiple large computing service contracts in state and local government, healthcare, insurance, and telecommunications industries
Proven project executive skills and experience with a strong track record for delivery, innovation, and value
Certification: Project Management Professional</td></tr>
<tr><td colspan="4">100% Dedicated to the Commonwealth Data Center Computing Services Project</td></tr>
</table>

IBM Delivery Project Executive: [redacted]

[redacted] **(based in Harrisburg)** will serve as the dedicated IBM Delivery Project Executive as he has for the past 10 years on the Data PowerHouse Project. In this capacity, Bob has led the IBM support for the Unisys Team in providing not only outstanding steady-state support for the Commonwealth systems and applications, but also supported the introduction of new technologies such as Linux on System z. Bob has demonstrated his ability to harness the broad resources of IBM for implementation of technical changes, provide additional hardware and software capabilities, and manage technical issues by including the IBM Product Engineering and Software Labs to meet Commonwealth needs.

Going forward, Bob will support the Unisys Team by leveraging the breadth of IBM support in the implementation of new technologies and transitions to new datacenter facilities. His ITIL and PMI certifications and experience with the Commonwealth agencies will guide his leadership of the services management and technical staff to provide the best possible operating environment for the Commonwealth applications.

Name	Proposed Account Role	Position in Organization	Experience in Proposed Role (Years)
Role on last 3 projects		**Qualifications for Proposed Role**	
[redacted]	IBM Delivery Project Executive	IBM Delivery Project Executive	10 years
• IBM Delivery Project Executive, Unisys DPH contract, Commonwealth of Pennsylvania (10 years) • IBM Sr. Delivery Manager/Delivery Project Executive responsible for high-quality delivery of Wintel, UNIX desktop support, UNIX and NT server services, and hardware maintenance for 700 servers and 5,000 end users for a large telecommunications customer (3 years) • IBM Service Delivery Manager managing services to multiple locations for a large telecommunications customer (3 years)		• More than 30 years of experience with IBM demonstrating leadership across a range of positions in quality control, engineering, and management delivering high-quality service and solutions to large IBM accounts • 10+ years of experience and expertise in leading teams to achieve consistent delivery results, providing leadership, experience, and innovation in working through solutions for the Commonwealth • Certification: ITIL V3 Foundation, Project Management Professional	
100% Dedicated to the Commonwealth Data Center Computing Services Project			

Executive Leadership Committee

Because of the importance of this engagement and our commitment to the Commonwealth of Pennsylvania, Ed Coleman, Unisys Chairman and CEO, has chosen to serve as Executive Sponsor and will personally ensure our company's complete commitment to its success in the implementation of a new compute services model for the Commonwealth.

In addition to Ed Coleman's role as Executive Sponsor, Unisys established an Executive Leadership Committee shown in the figure below to support the efforts of our Harrisburg-based leadership team. We created this committee to provide direct visibility into senior leadership at Unisys to confirm that we meet our commitments to the Commonwealth, during both transition and steady state operations, and to break down the inevitable barriers that arise during engagements of this magnitude.

Unisys Executive Leadership Committee

Our **Executive Committee** consists of**:**

- [redacted], Unisys President of Global Service Delivery
- [redacted], Unisys Vice President of Global Service Delivery
- [redacted], IBM Vice President of Global Technology Services
- [redacted], Unisys Vice President of North America Service Delivery
- [redacted], Unisys Vice President and General Manager of North America Service Delivery
- [redacted], Unisys Chief Technology Officer, Technology and Innovation
- [redacted], Unisys Vice President, Commonwealth of Pennsylvania Region
- [redacted], Deloitte Principal, Security and Privacy Services

Trade Secret/Confidential Proprietary Information Notice

Instructions:

The Commonwealth may not assert on behalf of a third party an exception to the public release of materials that contain trade secrets or confidential proprietary information unless the materials are accompanied, at the time they are submitted, by this form or a document containing similar information.

It is the responsibility of the party submitting this form to ensure that all statements and assertions made below are legally defensible and accurate. The Commonwealth will not provide a submitting party any advice with regard to trade secret law.

Name of submitting party:

Contact information for submitting party:

[redacted]

[redacted]

Please provide a brief overview of the materials that you are submitting (e.g. bid proposal, grant application, technical schematics):

Oral Presentation
Response to Follow-up Questions

Please provide a brief explanation of why the materials are being submitted to the Commonwealth (e.g. response to bid #12345, application for grant XYZ being offered by the Department of Health, documents required to be submitted under law ABC)

Response to Request for Proposal 36100022698

Please provide a list detailing which portions of the material being submitted you believe constitute a trade secret or confidential proprietary information, and please provide an explanation of why you think those materials constitute a trade secret or confidential proprietary information. Also, please mark the submitted material in such a way to allow a reviewer to easily distinguish between the parts referenced below. (You may attach additional pages if needed)

Note: The following information will not be considered a trade secret or confidential proprietary information:

- Any information submitted as part of a vendor's cost proposal
- Information submitted as part of a vendor's technical response that does not pertain to specific business practices or product specification
- Information submitted as part of a vendor's technical or disadvantaged business response that is otherwise publicly available or otherwise easily obtained
- Information detailing the name, quantity, and price paid for any product or service being purchased by the Commonwealth

Page Number	Description	Explanation
Slide 14	Oral Presentation	Information and picture of Data Center that will host Mission Critical Commonwealth servers.
Slide 17	Oral Presentation	Proprietary Video of in-scope Data Centers
Slide 36	Oral Presentation	Proprietary Security Regulatory Approach
Slide 39	Oral Presentation	Commonwealth Secure Remote Access architecture
Page 13	Unisys Data Center Clarification Response	Public Sector Security Risk Framework
Multiple	Unisys Data Center Clarification Response	Any reference (address, name, photo, power & network entry points, floor plans, etc.) to the Mission Critical Data Center located in [redacted] that could constitute a security threat
Multiple	Unisys Data Center Clarification Response	Any reference to the power substations and fiber locations that could constitute a security threat.
Multiple	Unisys Data Center Clarification Response	Any graphics of floor plans showing the Commonwealth's location for the Eagan, MN Data Center that could constitute a security threat.
Multiple	Unisys Data Center Clarification Response	Any proprietary information on the Unisys Stealth Security tool.

Acknowledgment

The undersigned party hereby agrees that it has read and completed this form, and has marked the material being submitted in accordance with the instructions above. The undersigned party acknowledges that the Commonwealth is not liable for the use or disclosure of trade secret data or confidential proprietary information that has not been clearly marked as such, and which was not accompanied by a specific explanation included with this form.

The undersigned agrees to defend any action seeking release of the materials it believes to be trade secret or confidential, and indemnify and hold harmless the Commonwealth, its agents and employees, from any judgments awarded against the Commonwealth in favor of the party requesting the materials, and any and all costs connected with that defense. This indemnification survives so long as the Commonwealth has possession of the submitted material, and will apply to all costs unless and until the undersigned provides a written statement or similar notice to the Commonwealth stating that it no longer wishes to exempt the submitted material from public disclosure.

The undersigned acknowledges that the Commonwealth is required to keep all records for at least as long as specified in its published records retention schedule.

The undersigned acknowledges that the Commonwealth reserves the right to reject the undersigned's claim of trade secret/confidential proprietary information if the Commonwealth determines that the undersigned has not met the burden of establishing that the information constitutes a trade secret or is confidential. The undersigned also acknowledges that if only a certain part of the submitted material is found to constitute a trade secret or is confidential, the remainder of the submitted material will become public; only the protected information will be removed and remain nonpublic.

If being submitted electronically, the undersigned agrees that the mark below is a valid electronic signature.

Signature	Title	Date

APPENDIX B - PROPOSAL COVER SHEET
COMMONWEALTH OF PENNSYLVANIA
OFFICE OF ADMINISTRATION – OFFICE FOR INFORMATION TECHNOLOGY
RFP# 6100022698

Enclosed in three separately sealed submittals is the proposal of the Offeror identified below for the above-referenced RFP:

Offeror Information:	
Offeror Name	UNISYS Corporation
Offeror Mailing Address	4750 Lindle Road, Harrisburg, PA 17111
Offeror Website	WWW. UNISYS. com
Offeror Contact Person	Dean R. Shaner
Contact Person's Phone Number	(717) 526- 1267
Contact Person's Facsimile Number	(717) 526 - 1175
Contact Person's E-Mail Address	dean.shaner@UNISYS, com
Offeror Federal ID Number	[redacted]
Offeror SAP/SRM Vendor Number	163299

Submittals Enclosed and Separately Sealed:	
☐	Technical Submittal
☐	Disadvantaged Business Submittal
☒	Cost Submittal

[redacted] *Signature*	
Signature of an official authorized to bind the Offeror to the provisions contained in the Offeror's proposal: Printed Name John Edward Coleman	
Title Chairman & CEO	

FAILURE TO COMPLETE, SIGN AND RETURN THIS FORM WITH THE OFFEROR'S PROPOSAL MAY RESULT IN THE REJECTION OF THE OFFEROR'S PROPOSAL

Request for Proposal

RFP # 6100022698

Commonwealth of Pennsylvania

Office of Administration
Office for Information Technology

Datacenter Computing Services

Schedule I

Offeror Pricing Forms

Description of Exhibit and Instructions

This Schedule I - Offeror Pricing Forms sets forth the following:

Configuration Definitions

- This sheet contains the descriptions of the defined configurations which are used on the Volumetrics and Catalog of Services tabs.

1. Volumetrics

- This sheet includes the resource unit categories and target quantities that the Offeror's will use to determine their price.
- Offerors should not assume that these are a guaranteed minimum units over the contract period.
-No entry is required on this sheet.

2. DC Architecture Charges

- Offerors should use this sheet to indicate their charges associated with the startup of their Datacenter Architecture.
- Offeror should only input in highlighted (yellow) cells.

3. Transition Charges

- Offerors should use this sheet to indicate their charges associated with transition as described in Schedule D. All transition costs should be included in these costs.
- Offeror should only input in highlighted (yellow) cells.

4. Total Charges

- Summary of Datacenter Architecture Charges, Transition Charges, and Services Charges.
-No entry is required on this sheet.

5. Technical Staff Rate Card

- Offerors should use this sheet to provide their staffing rates for the optional support services
- Offeror should only input in highlighted (yellow) cells.

6. Catalog of Services

- Offerors should use this sheet to include their Catalog of Services with pricing.
- Offeror should only input in highlighted (yellow) cells.

Additional Notes

a.) All input sheets (2, 3, 5, 6) must be filled out completely

b.) Total Charges (sheet 4): Information is linked with input sheets and will calculate automatically.

c.) Formulas are imbedded in all sheets. Offeror must verify that all calculations, subtotal costs and grand total costs are accurate.

d.) Please contact the Issuing Officer with any questions or concerns.

e.) Payment for services under this contract are unit-based. The total units (volumetrics) listed are for informational purposes only and will not be binding on the Commonwealth

Configuration Definitions

The below definitions and configurations are referenced throughout Schedule I - Offeror Pricing Forms.

Definitions

(1) Fully Managed - Infrastructure that is fully owned and managed by the Service Provider

(2) Managed Only - Infrastructure that is managed by the Service Provider but owned by the Commonwealth and/or a 3rd Party; each of these units typically would also include a Limited Co-Lo charge for datacenter related services.

(3) Limited Co-Lo - Infrastructure that is located in the Service Provider managed datacenter(s). Either owned and managed by the Commonwealth or 3rd Party.

(4) Mainframe Services - Include both IBM mainframe and Unisys mainframe services

(5) On-Demand (IaaS) Services - Provide pricing for Offeror's IaaS offerings using the target configurations listed within.

(6) Configurations - Offerors will use the sample configurations below to support their pricing presentation.

Limited Co-Lo (Data Center Only Charge)		
Limited Co-Lo Configurations	**Minimum Specifications**	**Unit**
Co-Lo Config - 1	1/4 Rack Configuration includes 10U Cabinet Space; 5,000 GB Network Bandwidth; 100Mb/s Uplink; 6 IP Addresses; 5 -110V AC Circuits	Monthly Per Config
Co-Lo Config - 2	1/2 Rack Configuration includes 21U Cabinet Space; 10,000 GB Network Bandwidth; 100Mb/s Uplink; 14 IP Addresses; 10 -110V AC Circuits	Monthly Per Config
Co-Lo Config - 3	Full Rack Configuration includes 42U Cabinet Space; 20,000 GB Network Bandwidth; 100Mb/s Uplink; 30 IP Addresses; 20 -110V AC Circuits	Monthly Per Config

Server Configurations (Fully Managed)		
x86 Server Configurations	**Minimum Specifications**	**Unit**
Windows pConfig - 1	2-way Quad-Core 2.0 GHz; 4 GB RAM; Mirrored 146 15K Hard Drives; Windows Server 2008 R2	Physical Server
Windows pConfig - 2	2-way Six-Core 2.4 GHz; 16 GB RAM; Mirrored 146 15K Hard Drives; Windows Server 2008 R2	Physical Server
Windows pConfig - 3	4-way Six-Core 2.0 GHz; 64 GB RAM; 500 GB SAN Attached Storage; Windows Server 2008 R2	Physical Server
Windows pConfig - 4	2-way Six-Core 2.4 GHz; 16 GB RAM; Mirrored 146 15K Hard Drives; Windows Server 2008 R2; Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site s Local SAN Storage from hourly data synchronization	Physical Server
Windows pConfig - 5	2-way Six-Core 2.4 GHz; 16 GB RAM; Mirrored 146 15K Hard Drives; Windows Server 2008 R2; Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Physical Server
Linux pConfig - 1	2-way Quad-Core 2.0 GHz; 4 GB RAM; Mirrored 146 15K Hard Drives; RedHat or SUSE	Physical Server
Linux pConfig - 2	2-way Six-Core 2.4 GHz; 16 GB RAM; Mirrored 146 15K Hard Drives; RedHat or SUSE	Physical Server
Linux pConfig - 3	4-way Six-Core 2.0 GHz; 64 GB RAM; 500 GB SAN Attached Storage; RedHat or SUSE	Physical Server
Linux pConfig - 4	2-way Six-Core 2.4 GHz; 16 GB RAM; Mirrored 146 15K Hard Drives; RedHat or SUSE; Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Physical Server
Linux pConfig - 5	2-way Six-Core 2.4 GHz; 16 GB RAM; Mirrored 146 15K Hard Drives; RedHat or SUSE; Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Physical Server
Windows vConfig - 1	2vCPU; 4 GB Ram; Windows Server 2008 R2; Firewall/IDS; Site-Site VPN; VPN Client; VLAN	Virtual Server Instance
Windows vConfig - 2	4vCPU; 16 GB Ram; Windows Server 2008 R2; Firewall/IDS; Site-Site VPN; VPN Client; VLAN	Virtual Server Instance
Windows vConfig - 3	8vCPU; 64 GB Ram; Windows Server 2008 R2; Firewall/IDS; Site-Site VPN; VPN Client; VLAN	Virtual Server Instance
Windows vConfig - 4	4vCPU; 16 GB Ram; Windows Server 2008 R2; Firewall/IDS; Site-Site VPN; VPN Client; VLAN; Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site s Local SAN Storage from hourly data synchronization	Virtual Server Instance
Windows vConfig - 5	4vCPU; 16 GB Ram; Windows Server 2008 R2; Firewall/IDS; Site-Site VPN; VPN Client; VLAN; Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Virtual Server Instance
Linux vConfig - 1	2vCPU; 4 GB Ram; RedHat or SUSE; Firewall/IDS; Site-Site VPN; VPN Client; VLAN	Virtual Server Instance
Linux vConfig - 2	4vCPU; 16 GB Ram; RedHat or SUSE; Firewall/IDS; Site-Site VPN; VPN Client VLAN	Virtual Server Instance
Linux vConfig - 3	8vCPU; 64 GB Ram; RedHat or SUSE; Firewall/IDS; Site-Site VPN; VPN Client; VLAN	Virtual Server Instance

Configuration Definitions

Linux vConfig - 4	4vCPU; 16 GB Ram; RedHat or SUSE; Firewall/IDS; Site-Site VPN; VPN Client; VLAN; Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site s Local SAN Storage from hourly data synchronization	Virtual Server Instance
Linux vConfig - 5	4vCPU; 16 GB Ram; RedHat or SUSE; Firewall/IDS; Site-Site VPN; VPN Client; VLAN; Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Virtual Server Instance

P-Series Server Configurations		
AIX Config - 1	3.0GHz POWER7; 0.5 Cores; 6 GB RAM AIX	LPAR
AIX Config - 2	3.0GHz POWER7; 1.0 Cores; 12 GB RAM AIX	LPAR
AIX Config - 3	3.0GHz POWER7; 1.5 Cores; 18 GB RAM; AIX	LPAR
AIX Config - 4	3.0GHz POWER7; 1.0 Cores; 12 GB RAM; AIX; Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site s Local SAN Storage from hourly data synchronization	LPAR
AIX Config - 5	3.0GHz POWER7; 1.0 Cores; 12 GB RAM; AIX; Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	LPAR

Mainframe Configurations		
IBM Mainframe Configurations	**Minimum Specifications**	**Unit**
IBM Mainframe Config - 1	IBM System zEnterprise Processor z/OS	MIP
IBM Mainframe Config - 2	IBM System zEnterprise Processor Virtual Linux Prod IFL	MIP
IBM Mainframe Config - 3	IBM System zEnterprise Processor Virtual Linux Prod IFL; Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site s Local SAN Storage from hourly data synchronization	MIP
IBM AS400 Config 1	IBM i Series / AS400	CPW
IBM AS400 Config 2	IBM i Series / AS400; Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site s Local SAN Storage from hourly data synchronization	CPW
Unisys Mainframe Configurations	**Minimum Specifications**	**Unit**
Unisys Mainframe Config - 1	Unisys (Clearpath / Dorado)	MIP
Unisys Mainframe Config - 2	Unisys (Clearpath / Libra)	MIP
Unisys Mainframe Config - 3	Unisys (Clearpath / Dorado); Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site s Local SAN Storage from hourly data synchronization	MIP
Unisys Mainframe Config - 4	Unisys (Clearpath / Libra) ; Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site s Local SAN Storage from hourly data synchronization	MIP

On-Demand (IaaS) Configurations		
IaaS x86 Server Configurations	**Minimum Specifications**	**Unit (per month)**
IaaS Windows vConfig - 1	2vCPU; 4 GB Ram; Windows Server 2008 R2; Firewall/IDS; Site-Site VPN; VPN Client VLAN	Virtual Server Instance
IaaS Windows vConfig - 2	4vCPU; 16 GB Ram; Windows Server 2008 R2; Firewall/IDS; Site-Site VPN; VPN Client VLAN	Virtual Server Instance
IaaS Windows vConfig - 3	8vCPU; 64 GB Ram; Windows Server 2008 R2; Firewall/IDS; Site-Site VPN; VPN Client; VLAN	Virtual Server Instance
IaaS Windows vConfig - 4	4vCPU; 16 GB Ram; Windows Server 2008 R2; Firewall/IDS; Site-Site VPN; VPN Client; VLAN; Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site s Local SAN Storage from hourly data synchronization	Virtual Server Instance
IaaS Windows vConfig - 5	4vCPU; 16 GB Ram; Windows Server 2008 R2; Firewall/IDS; Site-Site VPN; VPN Client; VLAN; Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Virtual Server Instance
IaaS Linux vConfig - 1	2vCPU; 4 GB Ram; RedHat or SUSE; Firewall/IDS; Site-Site VPN; VPN Client; VLAN	Virtual Server Instance
IaaS Linux vConfig - 2	4vCPU; 16 GB Ram; RedHat or SUSE; Firewall/IDS; Site-Site VPN; VPN Client; VLAN	Virtual Server Instance
IaaS Linux vConfig - 3	8vCPU; 64 GB Ram; RedHat or SUSE; Firewall/IDS; Site-Site VPN; VPN Client VLAN	Virtual Server Instance
IaaS Linux vConfig - 4	4vCPU; 16 GB Ram; RedHat or SUSE; Firewall/IDS; Site-Site VPN; VPN Client; VLAN; Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site s Local SAN Storage from hourly data synchronization	Virtual Server Instance
IaaS Linux vConfig - 5	4vCPU; 16 GB Ram; RedHat or SUSE; Firewall/IDS; Site-Site VPN; VPN Client; VLAN; Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Virtual Server Instance
IaaS Storage Configurations		
IaaS Storage Config - 1	SAN attached storage; Raid 5; 10K - 15K RPM discs	Monthly per GB

Configuration Definitions

IaaS Storage Config - 2	SAN attached storage; Raid 10; 10K - 15K RPM discs	Monthly per GB
IaaS Storage Config - 3	Network Attached Storage	Monthly per GB

IaaS Backup Configurations		
IaaS Backup Config - 1	Remote Offsite backup per GB	Monthly per GB

Baseline Units - Volumetrics

Note: The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all inclusive representation of every service desired by the Commonwealth.

Resource Description	Service Tier / Configuration (6)	Units	Year 1 Qty	Year 2 Qty	Year 3 Qty	Year 4 Qty	Year 5 Qty	Year 6 Qty	Year 7 Qty	Opt - Year 8 Qty	Opt - Year 9 Qty	Opt - Year 10 Qty
Server - Fully Managed (1)												
x86 (Windows, Linux) - Physical Servers												
	Platinum Tier											
	Windows pConfig - 1	Server	27	26	24	23	22	21	20	19	18	17
	Windows pConfig - 2	Server	23	22	21	20	19	18	17	16	15	14
	Windows pConfig - 3	Server	14	13	13	12	11	11	10	10	9	9
	Windows pConfig - 4	Server	2	2	2	2	2	2	1	1	1	1
	Windows pConfig - 5	Server	2	2	2	2	2	2	1	1	1	1
	Linux pConfig - 1	Server	12	11	11	10	10	9	9	8	8	8
	Linux pConfig - 2	Server	8	8	7	7	7	6	6	6	5	5
	Linux pConfig - 3	Server	6	6	5	5	5	5	4	4	4	4
	Linux pConfig - 4	Server	2	2	2	2	2	2	1	1	1	1
	Linux pConfig - 5	Server	2	2	2	2	2	2	1	1	1	1
sub-total x86 (Windows, Linux) - Physical Servers - Plantinum			**98**	**94**	**89**	**85**	**82**	**78**	**70**	**67**	**63**	**61**
	Gold Tier											
	Windows pConfig - 1	Server	245	233	221	210	200	190	180	171	163	154
	Windows pConfig - 2	Server	209	199	189	179	170	162	154	146	139	132
	Windows pConfig - 3	Server	122	116	110	105	99	94	90	85	81	77
	Windows pConfig - 4	Server	18	17	16	15	15	14	13	13	12	11
	Windows pConfig - 5	Server	18	17	16	15	15	14	13	13	12	11
	Linux pConfig - 1	Server	108	103	97	93	88	84	79	75	72	68
	Linux pConfig - 2	Server	72	68	65	62	59	56	53	50	48	45
	Linux pConfig - 3	Server	54	51	49	46	44	42	40	38	36	34
	Linux pConfig - 4	Server	18	17	16	15	15	14	13	13	12	11
	Linux pConfig - 5	Server	18	17	16	15	15	14	13	13	12	11
sub-total x86 (Windows, Linux) - Physical Servers - Gold			**882**	**838**	**795**	**755**	**720**	**684**	**648**	**617**	**587**	**554**
	Silver Tier											
	Windows pConfig - 1	Server	272	258	245	233	222	210	200	190	180	189
	Windows pConfig - 2	Server	236	224	213	202	192	183	173	165	157	164
	Windows pConfig - 3	Server	136	129	123	117	111	105	100	95	90	95
	Windows pConfig - 4	Server	18	17	16	15	15	14	13	13	12	13
	Windows pConfig - 5	Server	18	17	16	15	15	14	13	13	12	13
	Linux pConfig - 1	Server	120	114	108	103	98	93	88	84	80	84
	Linux pConfig - 2	Server	120	114	108	103	98	93	88	84	80	84
	Linux pConfig - 3	Server	24	23	22	21	20	19	18	17	16	17
	Linux pConfig - 4	Server	18	17	16	15	15	14	13	13	12	13
	Linux pConfig - 5	Server	18	17	16	15	15	14	13	13	12	13
sub-total x86 (Windows, Linux) - Physical Servers - Silver			**980**	**930**	**883**	**839**	**801**	**759**	**719**	**687**	**651**	**685**
	Bronze Tier											
	Windows pConfig - 1	Server	120	114	108	103	98	93	88	84	80	76
	Windows pConfig - 2	Server	120	114	108	103	98	93	88	84	80	76
	Windows pConfig - 3	Server	47	45	42	40	38	36	35	33	31	30
	Windows pConfig - 4	Server	8	8	7	7	7	6	6	6	5	5
	Windows pConfig - 5	Server	3	3	3	3	2	2	2	2	2	2
	Linux pConfig - 1	Server	75	71	68	64	61	58	55	52	50	47
	Linux pConfig - 2	Server	75	71	68	64	61	58	55	52	50	47

Baseline Units - Volumetrics

Note: The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all inclusive representation of every service desired by the Commonwealth.

Resource Description	Service Tier / Configuration (6)	Units	Year 1 Qty	Year 2 Qty	Year 3 Qty	Year 4 Qty	Year 5 Qty	Year 6 Qty	Year 7 Qty	Opt - Year 8 Qty	Opt - Year 9 Qty	Opt - Year 10 Qty
	Linux pConfig - 3	Server	20	19	18	17	16	15	15	14	13	13
	Linux pConfig - 4	Server	4	4	4	3	3	3	3	3	3	3
	Linux pConfig - 5	Server	2	2	2	2	2	2	1	1	1	1
sub-total x86 (Windows, Linux) - Physical Servers - Bronze			**474**	**451**	**428**	**406**	**386**	**366**	**348**	**331**	**315**	**300**
	Basic Tier											
	Windows pConfig - 1	Server	240	228	217	206	195	186	176	168	159	151
	Windows pConfig - 2	Server	240	228	217	206	195	186	176	168	159	151
	Windows pConfig - 3	Server	110	105	99	94	90	85	81	77	73	69
	Windows pConfig - 4	Server	17	16	15	15	14	13	12	12	11	11
	Windows pConfig - 5	Server	7	7	6	6	6	5	5	5	5	4
	Linux pConfig - 1	Server	95	90	86	81	77	74	70	66	63	60
	Linux pConfig - 2	Server	95	90	86	81	77	74	70	66	63	60
	Linux pConfig - 3	Server	8	8	7	7	7	6	6	6	5	5
	Linux pConfig - 4	Server	9	9	8	8	7	7	7	6	6	6
	Linux pConfig - 5	Server	5	5	5	4	4	4	4	3	3	3
sub-total x86 (Windows, Linux) - Physical Servers - Basic			**826**	**786**	**746**	**708**	**672**	**640**	**607**	**577**	**547**	**520**
Total - Fully Managed - x86 Physical - All Support Tiers (Window, Linux)			**3,260**	**3,099**	**2,941**	**2,793**	**2,661**	**2,527**	**2,392**	**2,279**	**2,163**	**2,120**
x86 (Windows, Linux) - Virtual Servers												
	Platinum Tier											
	Windows vConfig - 1	Instance	28	29	31	32	34	36	38	39	41	43
	Windows vConfig - 2	Instance	23	24	25	27	28	29	31	32	34	36
	Windows vConfig - 3	Instance	14	15	15	16	17	18	19	20	21	22
	Windows vConfig - 4	Instance	3	3	3	3	4	4	4	4	4	5
	Windows vConfig - 5	Instance	2	2	2	2	2	3	3	3	3	3
	Linux vConfig - 1	Instance	12	13	13	14	15	15	16	17	18	19
	Linux vConfig - 2	Instance	10	11	11	12	12	13	13	14	15	16
	Linux vConfig - 3	Instance	6	6	7	7	7	8	8	8	9	9
	Linux vConfig - 4	Instance	2	2	2	2	2	3	3	3	3	3
	Linux vConfig - 5	Instance	1	1	1	1	1	1	1	1	1	2
sub-total x86 (Windows, Linux) - Virtual Servers - Platinum			**101**	**106**	**110**	**116**	**122**	**130**	**136**	**141**	**149**	**158**
	Gold Tier											
	Windows vConfig - 1	Instance	244	256	269	282	297	311	327	343	360	379
	Windows vConfig - 2	Instance	204	214	225	236	248	260	273	287	301	316
	Windows vConfig - 3	Instance	122	128	135	141	148	156	163	172	180	189
	Windows vConfig - 4	Instance	24	25	26	28	29	31	32	34	35	37
	Windows vConfig - 5	Instance	16	17	18	19	19	20	21	23	24	25
	Linux vConfig - 1	Instance	108	113	119	125	131	138	145	152	160	168
	Linux vConfig - 2	Instance	85	89	94	98	103	108	114	120	126	132
	Linux vConfig - 3	Instance	54	57	60	63	66	69	72	76	80	84
	Linux vConfig - 4	Instance	13	14	14	15	16	17	17	18	19	20
	Linux vConfig - 5	Instance	9	9	10	10	11	11	12	13	13	14
sub-total x86 (Windows, Linux) - Virtual Servers - Gold			**879**	**922**	**970**	**1017**	**1068**	**1121**	**1176**	**1238**	**1298**	**1364**
	Silver Tier											
	Windows vConfig - 1	Instance	272	286	300	315	331	347	365	383	402	422
	Windows vConfig - 2	Instance	232	244	256	269	282	296	311	326	343	360

Baseline Units - Volumetrics

Note: The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all inclusive representation of every service desired by the Commonwealth.

Resource Description	Service Tier / Configuration (6)	Units	Year 1 Qty	Year 2 Qty	Year 3 Qty	Year 4 Qty	Year 5 Qty	Year 6 Qty	Year 7 Qty	Opt - Year 8 Qty	Opt - Year 9 Qty	Opt - Year 10 Qty
	Windows vConfig - 3	Instance	136	143	150	157	165	174	182	191	201	211
	Windows vConfig - 4	Instance	24	25	26	28	29	31	32	34	35	37
	Windows vConfig - 5	Instance	16	17	18	19	19	20	21	23	24	25
	Linux vConfig - 1	Instance	120	126	132	139	146	153	161	169	177	186
	Linux vConfig - 2	Instance	98	103	108	113	119	125	131	138	145	152
	Linux vConfig - 3	Instance	60	63	66	69	73	77	80	84	89	93
	Linux vConfig - 4	Instance	13	14	14	15	16	17	17	18	19	20
	Linux vConfig - 5	Instance	9	9	10	10	11	11	12	13	13	14
sub-total x86 (Windows, Linux) - Virtual Servers - Silver			**980**	**1030**	**1080**	**1134**	**1191**	**1251**	**1312**	**1379**	**1448**	**1520**
	Bronze Tier											
	Windows vConfig - 1	Instance	91	96	100	105	111	116	122	128	134	141
	Windows vConfig - 2	Instance	91	96	100	105	111	116	122	128	134	141
	Windows vConfig - 3	Instance	44	46	49	51	53	56	59	62	65	68
	Windows vConfig - 4	Instance	1	1	1	1	1	1	1	1	1	2
	Windows vConfig - 5	Instance	1	1	1	1	1	1	1	1	1	2
	Linux vConfig - 1	Instance	38	40	42	44	46	48	51	53	56	59
	Linux vConfig - 2	Instance	38	40	42	44	46	48	51	53	56	59
	Linux vConfig - 3	Instance	18	19	20	21	22	23	24	25	27	28
	Linux vConfig - 4	Instance	1	1	1	1	1	1	1	1	1	2
	Linux vConfig - 5	Instance	1	1	1	1	1	1	1	1	1	2
sub-total x86 (Windows, Linux) - Virtual Servers - Bronze			**324**	**341**	**357**	**374**	**393**	**411**	**433**	**453**	**476**	**504**
	Basic Tier											
	Windows vConfig - 1	Instance	181	190	200	210	220	231	243	255	267	281
	Windows vConfig - 2	Instance	181	190	200	210	220	231	243	255	267	281
	Windows vConfig - 3	Instance	90	95	99	104	109	115	121	127	133	140
	Windows vConfig - 4	Instance	1	1	1	1	1	1	1	1	1	2
	Windows vConfig - 5	Instance	1	1	1	1	1	1	1	1	1	2
	Linux vConfig - 1	Instance	80	84	88	93	97	102	107	113	118	124
	Linux vConfig - 2	Instance	80	84	88	93	97	102	107	113	118	124
	Linux vConfig - 3	Instance	40	42	44	46	49	51	54	56	59	62
	Linux vConfig - 4	Instance	1	1	1	1	1	1	1	1	1	2
	Linux vConfig - 5	Instance	1	1	1	1	1	1	1	1	1	2
sub-total x86 (Windows, Linux) - Virtual Servers - Basic			**656**	**689**	**723**	**760**	**796**	**836**	**879**	**923**	**966**	**1020**
Total - Fully Managed - x86 Virtual - All Support Tiers (Window, Linux)			**2,940**	**3,088**	**3,240**	**3,401**	**3,570**	**3,749**	**3,936**	**4,134**	**4,337**	**4,566**
UNIX (IBM P-Series, AIX)												
	Platinum Tier											
	AIX Config - 1	LPAR	36	38	40	42	44	46	48	51	53	56
	AIX Config - 2	LPAR	26	27	29	30	32	33	35	37	38	40
	AIX Config - 3	LPAR	18	19	20	21	22	23	24	25	27	28
	AIX Config - 4	LPAR	5	5	6	6	6	6	7	7	7	8
	AIX Config - 5	LPAR	5	5	6	6	6	6	7	7	7	8
sub-total P-Series (AIX) - Bronze			**90**	**94**	**101**	**105**	**110**	**114**	**121**	**127**	**132**	**140**
	Gold Tier											
	AIX Config - 1	LPAR	36	38	40	42	44	46	48	51	53	56
	AIX Config - 2	LPAR	26	27	29	30	32	33	35	37	38	40

Baseline Units - Volumetrics

Note: The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all inclusive representation of every service desired by the Commonwealth.

Resource Description	Service Tier / Configuration (6)	Units	Year 1 Qty	Year 2 Qty	Year 3 Qty	Year 4 Qty	Year 5 Qty	Year 6 Qty	Year 7 Qty	Opt - Year 8 Qty	Opt - Year 9 Qty	Opt - Year 10 Qty
	AIX Config - 3	LPAR	18	19	20	21	22	23	24	25	27	28
	AIX Config - 4	LPAR	5	5	6	6	6	6	7	7	7	8
	AIX Config - 5	LPAR	5	5	6	6	6	6	7	7	7	8
sub-total P-Series (AIX) - Gold			**90**	**94**	**101**	**105**	**110**	**114**	**121**	**127**	**132**	**140**
	Silver Tier											
	AIX Config - 1	LPAR	72	76	79	83	88	92	96	101	106	112
	AIX Config - 2	LPAR	52	55	57	60	63	66	70	73	77	81
	AIX Config - 3	LPAR	36	38	40	42	44	46	48	51	53	56
	AIX Config - 4	LPAR	10	11	11	12	12	13	13	14	15	16
	AIX Config - 5	LPAR	10	11	11	12	12	13	13	14	15	16
sub-total P-Series (AIX) - Silver			**180**	**191**	**198**	**209**	**219**	**230**	**240**	**253**	**266**	**281**
	Bronze Tier											
	AIX Config - 1	LPAR	24	25	26	28	29	31	32	34	35	37
	AIX Config - 2	LPAR	24	25	26	28	29	31	32	34	35	37
	AIX Config - 3	LPAR	8	8	9	9	10	10	11	11	12	12
	AIX Config - 4	LPAR	2	2	2	2	2	3	3	3	3	3
	AIX Config - 5	LPAR	2	2	2	2	2	3	3	3	3	3
sub-total P-Series (AIX) - Bronze			**60**	**62**	**65**	**69**	**72**	**78**	**81**	**85**	**88**	**92**
	Basic Tier											
	AIX Config - 1	LPAR	64	67	71	74	78	82	86	90	95	99
	AIX Config - 2	LPAR	64	67	71	74	78	82	86	90	95	99
	AIX Config - 3	LPAR	32	34	35	37	39	41	43	45	47	50
	AIX Config - 4	LPAR	10	11	11	12	12	13	13	14	15	16
	AIX Config - 5	LPAR	10	11	11	12	12	13	13	14	15	16
sub-total P-Series (AIX) - Basic			**180**	**190**	**199**	**209**	**219**	**231**	**241**	**253**	**267**	**280**
Total - Fully Managed - P-Series (AIX) - All Support Tiers (Window, Linux)			**600**	**631**	**664**	**697**	**730**	**767**	**804**	**845**	**885**	**933**
Server - Managed Only (2)												
x86 (Windows, Linux)												
	Platinum Tier	Server/Instance	100	60	36	22	50	50	50	50	50	50
	Gold Tier	Server/Instance	900	540	324	194	50	50	50	50	50	50
	Silver Tier	Server/Instance	1000	600	360	216	50	50	50	50	50	50
	Bronze Tier	Server/Instance	750	450	270	162	50	50	50	50	50	50
	Basic Tier	Server/Instance	1050	630	378	227	50	50	50	50	50	50
Total Managed Only- x86 - All Support Tiers (Window, Linux)			**3,800**	**2,280**	**1,368**	**821**	**250**	**250**	**250**	**250**	**250**	**250**
UNIX (IBM P-Series, AIX)												
	Platinum	LPAR	5	3	2	10	10	10	10	10	10	10
	Gold Tier	LPAR	15	9	5	10	10	10	10	10	10	10
	Silver Tier	LPAR	30	18	11	10	10	10	10	10	10	10
	Bronze Tier	LPAR	40	24	14	10	10	10	10	10	10	10
	Basic Tier	LPAR	30	18	11	10	10	10	10	10	10	10
Total Managed Only- P-Series - All Support Tiers (AIX)			**120**	**72**	**43**	**50**	**50**	**50**	**50**	**50**	**50**	**50**
Storage and Backup - Fully Managed (1)												

Baseline Units - Volumetrics

Note: The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all inclusive representation of every service desired by the Commonwealth.

Resource Description	Service Tier / Configuration (6)	Units	Year 1 Qty	Year 2 Qty	Year 3 Qty	Year 4 Qty	Year 5 Qty	Year 6 Qty	Year 7 Qty	Opt - Year 8 Qty	Opt - Year 9 Qty	Opt - Year 10 Qty
Enterprise Storage												
	* Dedicated - Config 1 - SAN Raid 5	GB	2300000	2530000	2783000	3061300	3367430	3704173	4074590	4482049	4930254	5423280
	* Dedicated - Config 2 - SAN Raid 10	GB	400000	440000	484000	532400	585640	644204	708624	779487	857436	943179
	Dedicated - Config 3 - Net Attached	GB	10000	11000	12100	13310	14641	16105	17716	19487	21436	23579
Total Enterprise Storage - Fully Managed			**2,710,000**	**2,981,000**	**3,279,100**	**3,607,010**	**3,967,711**	**4,364,482**	**4,800,930**	**5,281,023**	**5,809,126**	**6,390,038**
Tape and Backup												
	** Server Tape Stored	GB Stored	2700000	2970000	3267000	3593700	3953070	4348377	4783215	5261536	5787690	6366459
	** Offsite Tape Storage	Tapes	5000	5500	6050	6655	7321	8053	8858	9744	10718	11790
Total Tape and Backup - Fully Managed			**2,705,000**	**2,975,500**	**3,273,050**	**3,600,355**	**3,960,391**	**4,356,430**	**4,792,073**	**5,271,280**	**5,798,408**	**6,378,249**

Limited Co-Lo (Data Center Only Charge) (3)												
Server, Storage, Network, Security Equipment												
	Co-Lo Config - 1	Per Config	20	20	20	20	20	20	20	20	20	20
	Co-Lo Config - 2	Per Config	20	20	20	20	20	20	20	20	20	20
	Co-Lo Config - 3	Per Config	80	80	80	80	40	40	40	40	40	40
Total Limited Co-Lo (Data Center Only Charge)			**120**	**120**	**120**	**120**	**80**	**80**	**80**	**80**	**80**	**80**

Mainframe Services (4)												
IBM Services												
	*** IBM Mainframe Allocated DASD	GB	100000	100000	100000	100000	100000	100000	100000	100000	100000	100000
	IBM Tapes in Storage - VTS	GB	100000	100000	100000	100000	100000	100000	100000	100000	100000	100000
	IBM Offsite Tape Storage	Tape/Reel	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000
Total IBM Services			**201,000**	**201,000**	**201,000**	**201,000**	**201,000**	**201,000**	**201,000**	**201,000**	**201,000**	**201,000**
IBM Configurations												
	Platinum Tier											
	IBM Mainframe Config - 1	MIP	1705	1705	1705	1705	1705	1705	1705	1705	1705	1705
	IBM Mainframe Config - 2	MIP	141	141	141	141	141	141	141	141	141	141
	IBM Mainframe Config - 3	MIP	330	330	330	330	330	330	330	330	330	330
	IBM AS400 Config 1	CPW	364	364	364	364	364	364	364	364	364	364
	IBM AS400 Config 2	CPW	1460	1460	1460	1460	1460	1460	1460	1460	1460	1460
sub-total IBM Mainfram Services - Plantinum			**4000**	**4000**	**4000**	**4000**	**4000**	**4000**	**4000**	**4000**	**4000**	**4000**
	Gold Tier											
	IBM Mainframe Config - 1	MIP	213	213	213	213	213	213	213	213	213	213
	IBM Mainframe Config - 2	MIP	18	18	18	18	18	18	18	18	18	18
	IBM Mainframe Config - 3	MIP	41	41	41	41	41	41	41	41	41	41
	IBM AS400 Config 1	CPW	46	46	46	46	46	46	46	46	46	46
	IBM AS400 Config 2	CPW	182	182	182	182	182	182	182	182	182	182
sub-total IBM Mainfram Services - Gold			**500**	**500**	**500**	**500**	**500**	**500**	**500**	**500**	**500**	**500**
	Basic Tier											
	IBM Mainframe Config - 1	MIP	213	213	213	213	213	213	213	213	213	213
	IBM Mainframe Config - 2	MIP	18	18	18	18	18	18	18	18	18	18
	IBM Mainframe Config - 3	MIP	41	41	41	41	41	41	41	41	41	41
	IBM AS400 Config 1	CPW	46	46	46	46	46	46	46	46	46	46
	IBM AS400 Config 2	CPW	182	182	182	182	182	182	182	182	182	182
sub-total IBM Mainfram Services - Basic			**500**	**500**	**500**	**500**	**500**	**500**	**500**	**500**	**500**	**500**

Baseline Units - Volumetrics

Note: The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all inclusive representation of every service desired by the Commonwealth.

Resource Description	Service Tier / Configuration (6)	Units	Year 1 Qty	Year 2 Qty	Year 3 Qty	Year 4 Qty	Year 5 Qty	Year 6 Qty	Year 7 Qty	Opt - Year 8 Qty	Opt - Year 9 Qty	Opt - Year 10 Qty
Total - IBM Mainfram Services - All Support Tiers			**5,000**	**5,000**	**5,000**	**5,000**	**5,000**	**5,000**	**5,000**	**5,000**	**5,000**	**5,000**
Unisys Services												
	*** Unisys DASD	GB	100000	100000	100000	100000	100000	100000	100000	100000	100000	100000
	Unisys Tapes in Storage - VTS	GB	100000	100000	100000	100000	100000	100000	100000	100000	100000	100000
	Unisys Offsite Tape Storage	Tape/Reel	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000
Total Unisys Services			**201,000**	**201,000**	**201,000**	**201,000**	**201,000**	**201,000**	**201,000**	**201,000**	**201,000**	**201,000**
Unisys Configurations												
	Platinum Tier											
	Unisys Mainframe Config - 1	MIP	550	550	550	550	550	550	550	550	550	550
	Unisys Mainframe Config - 2	MIP	220	220	220	220	220	220	220	220	220	220
	Unisys Mainframe Config - 3	MIP	2882	2882	2882	2882	2882	2882	2882	2882	2882	2882
	Unisys Mainframe Config - 4	MIP	875	875	875	875	875	875	875	875	875	875
sub-total Unisys Mainfram Services - Plantinum			**4527**	**4527**	**4527**	**4527**	**4527**	**4527**	**4527**	**4527**	**4527**	**4527**
	Gold Tier											
	Unisys Mainframe Config - 1	MIP	44	44	44	44	44	44	44	44	44	44
	Unisys Mainframe Config - 2	MIP	27	27	27	27	27	27	27	27	27	27
	Unisys Mainframe Config - 3	MIP	176	176	176	176	176	176	176	176	176	176
	Unisys Mainframe Config - 4	MIP	110	110	110	110	110	110	110	110	110	110
sub-total Unisys Mainfram Services - Gold			**357**	**357**	**357**	**357**	**357**	**357**	**357**	**357**	**357**	**357**
	Basic Tier											
	Unisys Mainframe Config - 1	MIP	44	44	44	44	44	44	44	44	44	44
	Unisys Mainframe Config - 2	MIP	27	27	27	27	27	27	27	27	27	27
	Unisys Mainframe Config - 3	MIP	176	176	176	176	176	176	176	176	176	176
	Unisys Mainframe Config - 4	MIP	110	110	110	110	110	110	110	110	110	110
sub-total Unisys Mainfram Services - Basic			**357**	**357**	**357**	**357**	**357**	**357**	**357**	**357**	**357**	**357**
Total - Unisys Mainfram Services - All Support Tiers			**5,241**	**5,241**	**5,241**	**5,241**	**5,241**	**5,241**	**5,241**	**5,241**	**5,241**	**5,241**
On-Demand (IaaS) (5)												
IaaS Servers - x86 (Windows, Linux) - Virtual Servers												
	IaaS Windows vConfig - 1	Instance	40	48	58	69	84	100	120	143	172	188
	IaaS Windows vConfig - 2	Instance	40	48	58	69	84	100	120	143	172	188
	IaaS Windows vConfig - 3	Instance	40	48	58	69	84	100	120	143	172	188
	IaaS Windows vConfig - 4	Instance	15	18	21	25	30	36	44	54	65	72
	IaaS Windows vConfig - 5	Instance	15	18	21	25	30	36	44	54	65	72
	IaaS Linux vConfig - 1	Instance	20	24	29	34	42	50	60	72	86	94
	IaaS Linux vConfig - 2	Instance	20	24	29	34	42	50	60	72	86	94
	IaaS Linux vConfig - 3	Instance	20	24	29	34	42	50	60	72	86	94
	IaaS Linux vConfig - 4	Instance	7	9	11	13	15	18	23	27	32	36
	IaaS Linux vConfig - 5	Instance	7	9	11	13	15	18	23	27	32	36
Total IaaS Servers - x86 (Windows, Linux) - Virtual Servers			**224**	**270**	**325**	**385**	**468**	**558**	**674**	**807**	**968**	**1,062**
IaaS Storage On-Demand												
	IaaS Storage Config - 1	GB	1000	1200	1440	1728	2074	2488	2986	3583	4300	5160
	IaaS Storage Config - 2	GB	500	600	720	864	1037	1244	1493	1792	2150	2580
	IaaS Storage Config - 3	GB	50	50	50	50	50	50	50	50	50	50

Baseline Units - Volumetrics

Note: The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all inclusive representation of every service desired by the Commonwealth.

Resource Description	Service Tier / Configuration (6)	Units	Year 1 Qty	Year 2 Qty	Year 3 Qty	Year 4 Qty	Year 5 Qty	Year 6 Qty	Year 7 Qty	Opt - Year 8 Qty	Opt - Year 9 Qty	Opt - Year 10 Qty
Total IaaS Storage On-Demand			**1,550**	**1,850**	**2,210**	**2,642**	**3,161**	**3,782**	**4,529**	**5,425**	**6,500**	**7,790**
IaaS Backup On-Demand												
	IaaS Backup Config - 1	GB	2,000	2,400	2,880	3,456	4,147	4,977	5,972	7,166	8,600	10320
Total IaaS Backup On-Demand			**2,000**	**2,400**	**2,880**	**3,456**	**4,147**	**4,977**	**5,972**	**7,166**	**8,600**	**10,320**
Reserve Account												
		Mos Balance	1	1	1	1	1	1	1	1	1	1
Reserve Account			**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**

Notes:

For purposes of submitting a proposal, Offerors should assume that tapes are equivalent in capacity to LTO4 tapes.

* For purposes of submitting a proposal, Offerors should assume that the slower Tier1 RAID5 uses 10K drives and the Tier2 RAID10 uses 15K drives.

** The volume is expressed as native.

*** For purposes of evaluation DASD is expressed in Usable (not Raw)

Third Party Software

Third Party Software

Vendor	Product											
B & L	BL/LIB Tape Library Management System	License	1	1	1	1	1	1	1	1	1	1
B & L	BL/SCHED Scheduling & Monitoring System	License	1	1	1	1	1	1	1	1	1	1
BMC Software	BMC AppSight for Windows/.NET - Division Edition	License	1	1	1	1	1	1	1	1	1	1
BMC Software	BMC AppSight Named Users	License	50	50	50	50	50	50	50	50	50	50
BMC Software	BMC AppSight QA Users	License	20	20	20	20	20	20	20	20	20	20
BMC Software	CONTROL-M Enterprise Manager	License	1	1	1	1	1	1	1	1	1	1
BMC Software	CONTROL-M Full Admin User	License	5	5	5	5	5	5	5	5	5	5
BMC Software	CONTROL-M Tasks (100 Tasks per Unit)	License	6	6	6	6	6	6	6	6	6	6
BMC Software	Database Director (D2)	License	1	1	1	1	1	1	1	1	1	1
BMC Software	Eclipse iBuild	License	1	1	1	1	1	1	1	1	1	1
BMC Software	Eclipse iChange	License	1	1	1	1	1	1	1	1	1	1
BMC Software	Eclipse iCheck	License	1	1	1	1	1	1	1	1	1	1
BMC Software	Eclipse iCopy	License	1	1	1	1	1	1	1	1	1	1
BMC Software	Eclipse iExtract	License	1	1	1	1	1	1	1	1	1	1
BMC Software	Eclipse iLM	License	1	1	1	1	1	1	1	1	1	1
BMC Software	Eclipse iLoad	License	1	1	1	1	1	1	1	1	1	1
BMC Software	Eclipse iRecover	License	1	1	1	1	1	1	1	1	1	1
BMC Software	Eclipse iSurvey	License	1	1	1	1	1	1	1	1	1	1
BMC Software	Eclipse iUnload	License	1	1	1	1	1	1	1	1	1	1
BMC Software	Mission Control	License	1	1	1	1	1	1	1	1	1	1
Business Objects	Crystal Reports	License	4	4	4	4	4	4	4	4	4	4
Bytware Inc.	StandGuard Anti-Virus	License	1	1	1	1	1	1	1	1	1	1
Citrix	XenApp Advanced (User Counts)	License	100	100	100	100	100	100	100	100	100	100
Citrix	XenApp Enterprise (User Counts)	License	750	750	750	750	750	750	750	750	750	750
Computer Associates Interna ional, Inc.	CA-Explore for CICS	License	1	1	1	1	1	1	1	1	1	1

Baseline Units - Volumetrics

Note: The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all inclusive representation of every service desired by the Commonwealth.

Resource Description	Service Tier / Configuration (6)	Units	Year 1 Qty	Year 2 Qty	Year 3 Qty	Year 4 Qty	Year 5 Qty	Year 6 Qty	Year 7 Qty	Opt - Year 8 Qty	Opt - Year 9 Qty	Opt - Year 10 Qty
Computer Associates Interna ional, Inc.	SOA Security Manager	License	1	1	1	1	1	1	1	1	1	1
Computer Associates Interna ional, Inc.	SOA Security Manager Additional Secured Web Services	License	100	100	100	100	100	100	100	100	100	100
Computer Associates Interna ional, Inc.	SOA Security Manager Additional Users	License	50,000	50,000	50,000	50,000	50,000	50,000	50,000	50,000	50,000	50,000
Cor icon Technologies	Corticon Business Rules Server – Unlimited CPUs	License	1	1	1	1	1	1	1	1	1	1
Cor icon Technologies	Corticon Server – per Non-Production Server	License	2	2	2	2	2	2	2	2	2	2
Cor icon Technologies	Corticon Business Rules Modeling Studio – per Named User	License	12	12	12	12	12	12	12	12	12	12
CSI International	EPIC	License	1	1	1	1	1	1	1	1	1	1
CSI International	FAQS/PCS	License	1	1	1	1	1	1	1	1	1	1
CSI International	FAQS/ASO	License	1	1	1	1	1	1	1	1	1	1
EMC Corporation	PowerPath	License	83	83	83	83	83	83	83	83	83	83
EMC Corporation	PowerPath (per CPU)	License	252	252	252	252	252	252	252	252	252	252
EMC Corporation	Symmetrix® VMAX Fully Automated Storage Tiering for Virtual Pools (FAST VP)	License	1	1	1	1	1	1	1	1	1	1
EMC Corporation	Vsphere Enterprise Plus	License	24	24	24	24	24	24	24	24	24	24
Experian QAS	NameSearch - Production (Licensed per Server up to 8 CPU)	License	2	2	2	2	2	2	2	2	2	2
Experian QAS	NameSearch - Non-Production (Licensed per Server)	License	3	3	3	3	3	3	3	3	3	3
Formula Consultants, Inc.	Star 1100	License	3	3	3	3	3	3	3	3	3	3
GlobalScape	CuteFTP Pro 2.0	License	4	4	4	4	4	4	4	4	4	4
HELPSYS	Robot/Schedule	License	3	3	3	3	3	3	3	3	3	3
Idea Integration	XGEN	License	1	1	1	1	1	1	1	1	1	1
Informatica Corporation	SSA-Name 3	License	1	1	1	1	1	1	1	1	1	1
Infragistics	NetAdvantage for .NET	License	6	6	6	6	6	6	6	6	6	6
KMSYS Worldwide, Inc.	IQU Plus-1	License	2	2	2	2	2	2	2	2	2	2
Levi, Ray and Shoup	VPS/PCL	License	1	1	1	1	1	1	1	1	1	1
Levi, Ray and Shoup	VPS/TCP/IP	License	1	1	1	1	1	1	1	1	1	1
Levi, Ray and Shoup	VPS/DRS	License	1	1	1	1	1	1	1	1	1	1
Levi, Ray and Shoup	VPS	License	1	1	1	1	1	1	1	1	1	1
MacKinney Systems, Inc.	CICS Response Time Monitor	License	1	1	1	1	1	1	1	1	1	1
Marble Computer, Inc.	OS DCD III Data Correlation and Documenta ion System	License	1	1	1	1	1	1	1	1	1	1
Microsoft	BizTalk Adaptor for MQSeries	License	8	8	8	8	8	8	8	8	8	8
Microsoft	BizTalk Server Enterprise (Single Processor)	License	5	5	5	5	5	5	5	5	5	5
Microsoft	BizTalk Server Standard (Single Processor)	License	4	4	4	4	4	4	4	4	4	4
Microsoft	SQL Server CAL	License	10	10	10	10	10	10	10	10	10	10
Microsoft	SQL Server Enterprise (Single Processor)	License	10	10	10	10	10	10	10	10	10	10
Microsoft	SQL Server Enterprise	License	11	11	11	11	11	11	11	11	11	11
Microsoft	SQL Server Standard (Single Processor)	License	2	2	2	2	2	2	2	2	2	2
Microsoft	SQL Server Standard	License	8	8	8	8	8	8	8	8	8	8
Microsoft	SQL Server Standard per 2-Core	License	4	4	4	4	4	4	4	4	4	4
Microsoft	Visual Studio Foundation Server	License	1	1	1	1	1	1	1	1	1	1
Microsoft	Visual Studio Foundation Server CAL	License	6	6	6	6	6	6	6	6	6	6
Microsoft	Visual Studio Professional with MSDN	License	8	8	8	8	8	8	8	8	8	8

Baseline Units - Volumetrics

Note: The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all inclusive representation of every service desired by the Commonwealth.

Resource Description	Service Tier / Configuration (6)	Units	Year 1 Qty	Year 2 Qty	Year 3 Qty	Year 4 Qty	Year 5 Qty	Year 6 Qty	Year 7 Qty	Opt - Year 8 Qty	Opt - Year 9 Qty	Opt - Year 10 Qty
Microsoft	Windows Server Datacenter Edition (Single Processor)	License	284	284	284	284	284	284	284	284	284	284
Microsoft	Windows Server Enterprise Edition	License	318	318	318	318	318	318	318	318	318	318
Microsoft	Windows Server Standard Edition	License	221	221	221	221	221	221	221	221	221	221
Microsoft	Windows Terminal Service Client Access Licenses	License	100	100	100	100	100	100	100	100	100	100
Network Associates	McAfee Anti-Virus	License	420	420	420	420	420	420	420	420	420	420
Novell	Platespin Migrator	License	12	12	12	12	12	12	12	12	12	12
Novell	SuSE Linux	License	11	11	11	11	11	11	11	11	11	11
OpenText	Metastorm Integration Manager for CICS (MIM for CICS)	License	1	1	1	1	1	1	1	1	1	1
Oracle	Oracle Change Management Pack	License	10	10	10	10	10	10	10	10	10	10
Oracle	Oracle Database 10g Enterprise	License	3	3	3	3	3	3	3	3	3	3
Oracle	Oracle Database Enterprise Edition	License	18	18	18	18	18	18	18	18	18	18
Oracle	Oracle Diagnostic Pack	License	13	13	13	13	13	13	13	13	13	13
Oracle	Oracle Enterprise Linux	License	3	3	3	3	3	3	3	3	3	3
Oracle	Oracle Exadata Storage Software	License	1	1	1	1	1	1	1	1	1	1
Oracle	Oracle Partitioning	License	8	8	8	8	8	8	8	8	8	8
Oracle	Oracle Tuning Pack	License	13	13	13	13	13	13	13	13	13	13
Oracle	Real Application Cluster - Processor Perpetual	License	4	4	4	4	4	4	4	4	4	4
Oracle	Spatial and Graph - Processor Perpetual	License	4	4	4	4	4	4	4	4	4	4
Pitney Bowes	Finalist (Doc Sense)	License	1	1	1	1	1	1	1	1	1	1
Pitney Bowes	CODE-1 Plus	License	1	1	1	1	1	1	1	1	1	1
Pitney Bowes	CODE-1 Plus (Test / Development)	License	1	1	1	1	1	1	1	1	1	1
Pitney Bowes	Online Window for Finalist	License	1	1	1	1	1	1	1	1	1	1
Quest	Central Performance Suite for SQL Server, Tier A	License	2	2	2	2	2	2	2	2	2	2
Quest	Central Performance Suite for SQL Server, Tier B	License	10	10	10	10	10	10	10	10	10	10
Quest	Foglight Database Management Suite for SQL Server	License	8	8	8	8	8	8	8	8	8	8
Quest	Foglight for SQL Server per CPU Socket	License	42	42	42	42	42	42	42	42	42	42
Quest	Foglight OS Management per CPU Socket	License	47	47	47	47	47	47	47	47	47	47
Quest	Foglight Server for FSM	License	2	2	2	2	2	2	2	2	2	2
RealVNC	VNC Enterprise Edition for Windows	License	15	15	15	15	15	15	15	15	15	15
Red Hat	Red Hat Enterprise Linux	License	3	3	3	3	3	3	3	3	3	3
Schema Systems Limited	Q Editor Plus One	License	1	1	1	1	1	1	1	1	1	1
Segus Inc.	OPC/Graph	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG20	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG40	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG60	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG80	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG130	License	1	1	1	1	1	1	1	1	1	1

Baseline Units - Volumetrics

Note: The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all inclusive representation of every service desired by the Commonwealth.

Resource Description	Service Tier / Configuration (6)	Units	Year 1 Qty	Year 2 Qty	Year 3 Qty	Year 4 Qty	Year 5 Qty	Year 6 Qty	Year 7 Qty	Opt - Year 8 Qty	Opt - Year 9 Qty	Opt - Year 10 Qty
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG20	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG40	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG60	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG80	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG130	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG140	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - MAPPER, SWG20	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - MAPPER, SWG40	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - MAPPER, SWG60	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - MAPPER, SWG80	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - MAPPER, SWG130	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG20	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG40	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG60	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG80	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG130	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG140	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - System Log, SWG20	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - System Log, SWG40	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - System Log, SWG60	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - System Log, SWG80	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - System Log, SWG130	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - System Log, SWG140	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG20	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG40	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG60	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG80	License	1	1	1	1	1	1	1	1	1	1

Baseline Units - Volumetrics

Note: The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all inclusive representation of every service desired by the Commonwealth.

Resource Description	Service Tier / Configuration (6)	Units	Year 1 Qty	Year 2 Qty	Year 3 Qty	Year 4 Qty	Year 5 Qty	Year 6 Qty	Year 7 Qty	Opt - Year 8 Qty	Opt - Year 9 Qty	Opt - Year 10 Qty
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG130	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG140	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Power Agent, SWG20	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Power Agent, SWG40	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Power Agent, SWG60	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Power Agent, SWG80	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Power Agent, SWG130	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Power Agent, SWG140	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Torch Capacity Manager Power Agent, SWG40	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Torch Capacity Manager Power Agent, SWG60	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Torch Capacity Manager Power Agent, SWG130	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Torch Capacity Manager Power Agent, SWG140	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Torch Interface Agent - I/O TRACE, SWG40	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Torch Interface Agent - I/O TRACE, SWG60	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Torch Interface Agent - I/O TRACE, SWG130	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Torch Interface Agent - LOG, SWG40	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Torch Interface Agent - LOG, SWG60	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Torch Interface Agent - LOG, SWG130	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Torch Interface Agent - LOG, SWG140	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Torch Interface Agent - MAPPER, SWG40	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Torch Interface Agent - MAPPER, SWG60	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Torch Interface Agent - MAPPER, SWG130	License	1	1	1	1	1	1	1	1	1	1
Sightline	Windows 2000 Interface Agent - Internet Informa ion Server	License	7	7	7	7	7	7	7	7	7	7
Sightline	Windows 2000 Interface Agent - .NET	License	7	7	7	7	7	7	7	7	7	7
Sightline	Windows 2000 Interface Agent - SQL Server	License	4	4	4	4	4	4	4	4	4	4
Sightline	Windows 2000 Power Agent Upto 32 CPU's	License	3	3	3	3	3	3	3	3	3	3
SMA	OpCon/xps EXEC LSAM, Group 3	License	1	1	1	1	1	1	1	1	1	1
SMA	OpCon/xps EXEC LSAM, Group 12	License	1	1	1	1	1	1	1	1	1	1
SMA	OpCon/xps EXEC LSAM Development, Group 2	License	1	1	1	1	1	1	1	1	1	1
SMA	OpCon/xps EXEC LSAM Development, Group 12	License	1	1	1	1	1	1	1	1	1	1
SMA	OpCon/xps Production SAM	License	1	1	1	1	1	1	1	1	1	1

Baseline Units - Volumetrics

Note: The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all inclusive representation of every service desired by the Commonwealth.

Resource Description	Service Tier / Configuration (6)	Units	Year 1 Qty	Year 2 Qty	Year 3 Qty	Year 4 Qty	Year 5 Qty	Year 6 Qty	Year 7 Qty	Opt - Year 8 Qty	Opt - Year 9 Qty	Opt - Year 10 Qty
SMA	OpCon/xps Starter Kit	License	1	1	1	1	1	1	1	1	1	1
SMA	OpCon/xps User Interface	License	17	17	17	17	17	17	17	17	17	17
Sybase	EAServer Deploy Advanced - Active	License	2	2	2	2	2	2	2	2	2	2
Sybase	EAServer Deploy Advanced - Passive	License	2	2	2	2	2	2	2	2	2	2
Symantec	Backup Exec System Recovery Server	License	83	83	83	83	83	83	83	83	83	83
Symantec	EndPoint Protection	License	3	3	3	3	3	3	3	3	3	3
Symantec	Ghost Solution Suite	License	25	25	25	25	25	25	25	25	25	25
Symantec	NetBackup Client Application and Database Pack, UNX, Tier 3	License	3	3	3	3	3	3	3	3	3	3
Symantec	NetBackup Client Application and Database Pack, UNX, Tier 4	License	2	2	2	2	2	2	2	2	2	2
Symantec	NetBackup Client Application and Database Pack, WIN, Tier 2	License	7	7	7	7	7	7	7	7	7	7
Symantec	NetBackup Client Application and Database Pack, WIN, Tier 3	License	20	20	20	20	20	20	20	20	20	20
Symantec	NetBackup Client Application and Database Pack, WIN, Tier 4	License	1	1	1	1	1	1	1	1	1	1
Symantec	NetBackup Enterprise Client, UNX, Tier 4	License	1	1	1	1	1	1	1	1	1	1
Symantec	NetBackup Enterprise Client, WIN, Tier 1	License	3	3	3	3	3	3	3	3	3	3
Symantec	NetBackup Enterprise Client, WIN, Tier 2	License	10	10	10	10	10	10	10	10	10	10
Symantec	NetBackup Enterprise Client, WIN, Tier 3	License	18	18	18	18	18	18	18	18	18	18
Symantec	NetBackup Enterprise Server, WIN, Tier 2	License	3	3	3	3	3	3	3	3	3	3
Symantec	NetBackup Enterprise Server, WIN, Tier 3	License	16	16	16	16	16	16	16	16	16	16
Symantec	NetBackup Library Based Tape Drive Option, XPLAT	License	51	51	51	51	51	51	51	51	51	51
Symantec	NetBackup Media Server Encryption Option (MSEO) WIN, Tier 2	License	1	1	1	1	1	1	1	1	1	1
Symantec	NetBackup Platform Base, XPLAT (per Terabyte)	License	65	65	65	65	65	65	65	65	65	65
Symantec	NetBackup Shared Storage Option, XPLAT	License	56	56	56	56	56	56	56	56	56	56
Symantec	NetBackup Standard Client, XPLAT	License	133	133	133	133	133	133	133	133	133	133
Symantec	NetBackup Vault Additional Drive Option, XPLAT	License	6	6	6	6	6	6	6	6	6	6
Symantec	NetBackup Vault Base Option, XPLAT (4 tape drives per license)	License	6	6	6	6	6	6	6	6	6	6
Symantec	Veritas NetBackup Enterprise Server License, Tier 3	License	1	1	1	1	1	1	1	1	1	1
Symantec	Veritas NetBackup Windows Client, Tier 4	License	2	2	2	2	2	2	2	2	2	2
Tone Software Corp.	Dynastep	License	1	1	1	1	1	1	1	1	1	1
Unicon Group Ltd.	LOUIS II LCOM Host Module	License	1	1	1	1	1	1	1	1	1	1
Unicon Group Ltd.	LOUIS II Extract & Reporting Module	License	1	1	1	1	1	1	1	1	1	1
Unicon Group Ltd.	LOUIS II DERIVE Option	License	2	2	2	2	2	2	2	2	2	2
Unicon Group Ltd.	LOUIS II DMS Interface	License	1	1	1	1	1	1	1	1	1	1
Unicon Group Ltd.	LOUIS II RDMS Interface	License	1	1	1	1	1	1	1	1	1	1
Unicon Group Ltd.	LOUIS II RELATE Option	License	2	2	2	2	2	2	2	2	2	2
VanDyke Technologies	VShell Workgroup Server	License	6	6	6	6	6	6	6	6	6	6
Veeam	nWorks ESX Monitoring for SCOM	License	32	32	32	32	32	32	32	32	32	32
Veeam	nWorks Management Pack for VMWare	License	62	62	62	62	62	62	62	62	62	62
VMware, Inc.	VMware vSphere 4 Enterprise Plus for 1 Processor	License	8	8	8	8	8	8	8	8	8	8

Baseline Units - Volumetrics

Note: The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all inclusive representation of every service desired by the Commonwealth.

Resource Description	Service Tier / Configuration (6)	Units	Year 1 Qty	Year 2 Qty	Year 3 Qty	Year 4 Qty	Year 5 Qty	Year 6 Qty	Year 7 Qty	Opt - Year 8 Qty	Opt - Year 9 Qty	Opt - Year 10 Qty
VMware, Inc.	VMware vSphere 5 Enterprise Plus for 1 Processor	License	16	16	16	16	16	16	16	16	16	16
Western American Data	Rlist	License	1	1	1	1	1	1	1	1	1	1
Winternals	Winternals Administrator's Pak	License	1	1	1	1	1	1	1	1	1	1
WinZip Computing	Winzip	License	59	59	59	59	59	59	59	59	59	59
XtremeSoft	AppMetrics	License	1	1	1	1	1	1	1	1	1	1
USPS	Correct Address	License	1	1	1	1	1	1	1	1	1	1
IBM	FileNet	License	1	1	1	1	1	1	1	1	1	1
Microsoft	SharePoint (with SA)	License	2	2	2	2	2	2	2	2	2	2
IBM	WebSphere MQ (Procesor Value Unit)	License	1	1	1	1	1	1	1	1	1	1
Xerox	XeroxDocuShare	License	1	1	1	1	1	1	1	1	1	1
Hybrid Third Party Software												
Vendor	**Product**											
Computer Associates Interna ional, Inc.	CA 90's Services (freeware)	License	3	3	3	3	3	3	3	3	3	3
Computer Associates Interna ional, Inc.	Vision Builder	License	1	1	1	1	1	1	1	1	1	1
Computer Associates Interna ional, Inc.	Easytrieve Plus	License	1	1	1	1	1	1	1	1	1	1
Computer Associates Interna ional, Inc.	Easytrieve Plus MVS	License	1	1	1	1	1	1	1	1	1	1
Computer Associates Interna ional, Inc.	Easytrieve Plus IMS	License	1	1	1	1	1	1	1	1	1	1
Computer Associates Interna ional, Inc.	Easytrieve Plus IMS Option MVS	License	1	1	1	1	1	1	1	1	1	1
Computer Associates Interna ional, Inc.	Easytrieve Plus DB2 OPT	License	1	1	1	1	1	1	1	1	1	1
Computer Associates Interna ional, Inc.	Easytrieve Plus DB2 Option MVS	License	1	1	1	1	1	1	1	1	1	1
Computer Associates Interna ional, Inc.	Endevor/MVS Automated Configuration Mgr MVS	License	1	1	1	1	1	1	1	1	1	1
Computer Associates Interna ional, Inc.	Endevor/MVS External Security Int. MVS	License	1	1	1	1	1	1	1	1	1	1
Computer Associates Interna ional, Inc.	Endevor/MVS MVS	License	1	1	1	1	1	1	1	1	1	1
Computer Associates Interna ional, Inc.	Endevor/MVS Extended Processor	License	1	1	1	1	1	1	1	1	1	1
Computer Associates Interna ional, Inc.	CA-Librarian	License	1	1	1	1	1	1	1	1	1	1
Computer Associates Interna ional, Inc.	CA-META COBOL	License	1	1	1	1	1	1	1	1	1	1
Computer Associates Interna ional, Inc.	Panvalet	License	1	1	1	1	1	1	1	1	1	1
Computer Associates Interna ional, Inc.	Panvalet ISPF	License	1	1	1	1	1	1	1	1	1	1
Computer Associates Interna ional, Inc.	SORT (INCL DART)	License	1	1	1	1	1	1	1	1	1	1
Computer Associates Interna ional, Inc.	SRAM	License	1	1	1	1	1	1	1	1	1	1
dotJ Software Inc.	dotJ Custom Tag Library	License	1	1	1	1	1	1	1	1	1	1
Formula Consultants, Inc.	Star 1100	License	3	3	3	3	3	3	3	3	3	3
Idea Integration	XGEN	License	1	1	1	1	1	1	1	1	1	1
Informatica Corporation	Change DataMove for DB2 Source	License	1	1	1	1	1	1	1	1	1	1
Informatica Corporation	DataMove for DB2 Source	License	1	1	1	1	1	1	1	1	1	1
Informatica Corporation	Change DataMove	License	1	1	1	1	1	1	1	1	1	1
Informatica Corporation	DataMove for IMS Source	License	1	1	1	1	1	1	1	1	1	1
Informatica Corporation	Change DataMove for IMS Source	License	1	1	1	1	1	1	1	1	1	1
Informatica Corporation	DataMove	License	1	1	1	1	1	1	1	1	1	1
Informatica Corporation	Change DataMove DB2 Target	License	1	1	1	1	1	1	1	1	1	1
Informatica Corporation	DataMove DB2 Target	License	1	1	1	1	1	1	1	1	1	1
Informatica Corporation	Change DataMove/DataMove Target for UDB	License	1	1	1	1	1	1	1	1	1	1
Informatica Corporation	SSA - Name 3	License	1	1	1	1	1	1	1	1	1	1
KMSYS Worldwide, Inc.	IQU Plus-1	License	5	5	5	5	5	5	5	5	5	5

Baseline Units - Volumetrics

Note: The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all inclusive representation of every service desired by the Commonwealth.

Resource Description	Service Tier / Configuration (6)	Units	Year 1 Qty	Year 2 Qty	Year 3 Qty	Year 4 Qty	Year 5 Qty	Year 6 Qty	Year 7 Qty	Opt - Year 8 Qty	Opt - Year 9 Qty	Opt - Year 10 Qty
KMSYS Worldwide, Inc.	IQU Reorg Composer	License	1	1	1	1	1	1	1	1	1	1
KMSYS Worldwide, Inc.	QPLXSS	License	350	350	350	350	350	350	350	350	350	350
KMSYS Worldwide, Inc.	QPLXSV	License	1	1	1	1	1	1	1	1	1	1
KMSYS Worldwide, Inc.	QPLXV	License	1	1	1	1	1	1	1	1	1	1
Marble Computer Inc.	OS DCD III Data Correlation and Documenta ion System	License	1	1	1	1	1	1	1	1	1	1
Microsoft	SQL Server Enterprise	License	2	2	2	2	2	2	2	2	2	2
SAS Institute, Inc.	Base SAS	License	1	1	1	1	1	1	1	1	1	1
SAS Institute, Inc.	SAS/ACCESS Interface for IMS	License	1	1	1	1	1	1	1	1	1	1
SAS Institute, Inc.	SAS/ACCESS DB2	License	1	1	1	1	1	1	1	1	1	1
SAS Institute, Inc.	SAS/AF	License	1	1	1	1	1	1	1	1	1	1
SAS Institute, Inc.	SAS/FSP	License	1	1	1	1	1	1	1	1	1	1
SAS Institute, Inc.	SAS/GRAPH	License	1	1	1	1	1	1	1	1	1	1
SAS Institute, Inc.	SAS/SHARE	License	1	1	1	1	1	1	1	1	1	1
SAS Institute, Inc.	SAS/STAT	License	1	1	1	1	1	1	1	1	1	1
Schema Systems Limited	Q Editor Plus One	License	1	1	1	1	1	1	1	1	1	1
SMA	OpCon/xps EXEC LSAM, Group 3	License	1	1	1	1	1	1	1	1	1	1
SMA	OpCon/xps EXEC LSAM, Group 8	License	1	1	1	1	1	1	1	1	1	1
SMA	OpCon/xps EXEC LSAM, Group 14	License	1	1	1	1	1	1	1	1	1	1
SMA	OpCon/xps Microsoft LSAM	License	5	5	5	5	5	5	5	5	5	5
SMA	OpCon/xps User Interface	License	15	15	15	15	15	15	15	15	15	15
Sybase	EAServer Deploy Advanced - Active	License	2	2	2	2	2	2	2	2	2	2
Sybase	EAServer Deploy Advanced - Passive	License	2	2	2	2	2	2	2	2	2	2
TRILOGexport, Inc.	TriTune Automation Component (APC)	License	1	1	1	1	1	1	1	1	1	1
Unicon Group Ltd.	LOUIS II Database Gateway	License	2	2	2	2	2	2	2	2	2	2
Unicon Group Ltd.	LOUIS II DMS Interface	License	3	3	3	3	3	3	3	3	3	3
Unicon Group Ltd.	LOUIS II Extract & Reporting Module	License	1	1	1	1	1	1	1	1	1	1
Unicon Group Ltd.	LOUIS II LCOM Host Module	License	3	3	3	3	3	3	3	3	3	3
Unicon Group Ltd.	LOUIS II MAPPER Interface	License	1	1	1	1	1	1	1	1	1	1
Unicon Group Ltd.	LOUIS II RDMS Interface	License	3	3	3	3	3	3	3	3	3	3
Verisign	Secure Site Pro SSL	License	2	2	2	2	2	2	2	2	2	2
Western American Data	Rlist	License	2	2	2	2	2	2	2	2	2	2
WinZip	Self-Extractor 10-user license	License	2	2	2	2	2	2	2	2	2	2
Total Third Party Software			**54,390**	**54,390**	**54,390**	**54,390**	**54,390**	**54,390**	**54,390**	**54,390**	**54,390**	**54,390**

Baseline Units - Volumetrics

Note: The Commonwealth has established mult

Price per unit \ per month

Resource Description	Service Tier / Configuration (6)	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Server - Fully Managed (1)											
x86 (Windows, Linux) - Physical Servers											
	Platinum Tier										
	Windows pConfig - 1	$ 319 87	$ 316 54	$ 313 07	$ 309 75	$ 306 44	$ 303 16	$ 300 95	$ 300 95	$ 300 95	$ 300 95
	Windows pConfig - 2	$ 349 59	$ 345 52	$ 340 66	$ 336 29	$ 331 91	$ 327 51	$ 328 32	$ 328 32	$ 328 32	$ 328 32
	Windows pConfig - 3	$ 372 29	$ 363 76	$ 353 46	$ 345 08	$ 336 58	$ 327 97	$ 340 46	$ 340 46	$ 340 46	$ 340 46
	Windows pConfig - 4	$ 354 05	$ 350 11	$ 345 39	$ 341 17	$ 336 93	$ 332 68	$ 332 91	$ 332 91	$ 332 91	$ 332 91
	Windows pConfig - 5	$ 349 59	$ 345 52	$ 340 66	$ 336 29	$ 331 91	$ 327 51	$ 328 32	$ 328 32	$ 328 32	$ 328 32
	Linux pConfig - 1	$ 373 78	$ 361 82	$ 354 12	$ 346 59	$ 339 23	$ 332 03	$ 330 18	$ 330 18	$ 330 18	$ 330 18
	Linux pConfig - 2	$ 402 92	$ 390 47	$ 381 76	$ 373 18	$ 364 74	$ 356 41	$ 357 58	$ 357 58	$ 357 58	$ 357 58
	Linux pConfig - 3	$ 423 09	$ 407 19	$ 394 56	$ 381 97	$ 369 41	$ 356 88	$ 369 72	$ 369 72	$ 369 72	$ 369 72
	Linux pConfig - 4	$ 407 38	$ 395 06	$ 386 49	$ 378 06	$ 369 76	$ 361 58	$ 362 18	$ 362 18	$ 362 18	$ 362 18
	Linux pConfig - 5	$ 402 92	$ 390 47	$ 381 76	$ 373 18	$ 364 74	$ 356 41	$ 357 58	$ 357 58	$ 357 58	$ 357 58
sub-total x86 (Windows, Linux) - Physical Servers - Plantinum		**$ 3,755.46**	**$ 3,666.46**	**$ 3,591.93**	**$ 3,521.56**	**$ 3,451.65**	**$ 3,382.14**	**$ 3,408.19**	**$ 3,408.19**	**$ 3,408.19**	**$ 3,408.19**
	Gold Tier										
	Windows pConfig - 1	$ 316 36	$ 313 38	$ 310 07	$ 306 90	$ 303 74	$ 300 59	$ 298 50	$ 298 50	$ 298 50	$ 298 50
	Windows pConfig - 2	$ 346 13	$ 342 41	$ 337 71	$ 333 49	$ 329 24	$ 324 97	$ 325 91	$ 325 91	$ 325 91	$ 325 91
	Windows pConfig - 3	$ 368 83	$ 360 64	$ 350 51	$ 342 27	$ 333 92	$ 325 44	$ 338 05	$ 338 05	$ 338 05	$ 338 05
	Windows pConfig - 4	$ 350 59	$ 347 00	$ 342 44	$ 338 36	$ 334 26	$ 330 14	$ 330 50	$ 330 50	$ 330 50	$ 330 50
	Windows pConfig - 5	$ 346 13	$ 342 41	$ 337 71	$ 333 49	$ 329 24	$ 324 97	$ 325 91	$ 325 91	$ 325 91	$ 325 91
	Linux pConfig - 1	$ 357 47	$ 347 15	$ 340 18	$ 333 35	$ 326 65	$ 320 08	$ 318 82	$ 318 82	$ 318 82	$ 318 82
	Linux pConfig - 2	$ 386 61	$ 375 80	$ 367 82	$ 359 94	$ 352 16	$ 344 46	$ 346 23	$ 346 23	$ 346 23	$ 346 23
	Linux pConfig - 3	$ 406 79	$ 392 52	$ 380 62	$ 368 73	$ 356 83	$ 344 93	$ 358 37	$ 358 37	$ 358 37	$ 358 37
	Linux pConfig - 4	$ 391 07	$ 380 39	$ 372 55	$ 364 81	$ 357 18	$ 349 63	$ 350 82	$ 350 82	$ 350 82	$ 350 82
	Linux pConfig - 5	$ 386 61	$ 375 80	$ 367 82	$ 359 94	$ 352 16	$ 344 46	$ 346 23	$ 346 23	$ 346 23	$ 346 23
sub-total x86 (Windows, Linux) - Physical Servers - Gold		**$ 3,656.61**	**$ 3,577.50**	**$ 3,507.41**	**$ 3,441.27**	**$ 3,375.37**	**$ 3,309.68**	**$ 3,339.35**	**$ 3,339.35**	**$ 3,339.35**	**$ 3,339.35**
	Silver Tier										
	Windows pConfig - 1	$ 313 26	$ 310 59	$ 307 42	$ 304 38	$ 301 34	$ 298 32	$ 296 34	$ 296 34	$ 296 34	$ 296 34
	Windows pConfig - 2	$ 343 03	$ 339 62	$ 335 05	$ 330 97	$ 326 85	$ 322 70	$ 323 75	$ 323 75	$ 323 75	$ 323 75
	Windows pConfig - 3	$ 365 73	$ 357 85	$ 347 86	$ 339 75	$ 331 52	$ 323 17	$ 335 89	$ 335 89	$ 335 89	$ 335 89
	Windows pConfig - 4	$ 347 49	$ 344 21	$ 339 79	$ 335 84	$ 331 87	$ 327 87	$ 328 34	$ 328 34	$ 328 34	$ 328 34
	Windows pConfig - 5	$ 343 03	$ 339 62	$ 335 05	$ 330 97	$ 326 85	$ 322 70	$ 323 75	$ 323 75	$ 323 75	$ 323 75
	Linux pConfig - 1	$ 344 50	$ 335 47	$ 329 09	$ 322 81	$ 316 64	$ 310 57	$ 309 79	$ 309 79	$ 309 79	$ 309 79
	Linux pConfig - 2	$ 373 64	$ 364 12	$ 356 72	$ 349 40	$ 342 14	$ 334 95	$ 337 19	$ 337 19	$ 337 19	$ 337 19
	Linux pConfig - 3	$ 393 81	$ 380 84	$ 369 53	$ 358 19	$ 346 82	$ 335 42	$ 349 33	$ 349 33	$ 349 33	$ 349 33
	Linux pConfig - 4	$ 378 10	$ 368 71	$ 361 46	$ 354 27	$ 347 16	$ 340 12	$ 341 79	$ 341 79	$ 341 79	$ 341 79
	Linux pConfig - 5	$ 373 64	$ 364 12	$ 356 72	$ 349 40	$ 342 14	$ 334 95	$ 337 19	$ 337 19	$ 337 19	$ 337 19
sub-total x86 (Windows, Linux) - Physical Servers - Silver		**$ 3,576.22**	**$ 3,505.15**	**$ 3,438.68**	**$ 3,375.97**	**$ 3,313.34**	**$ 3,250.75**	**$ 3,283.36**	**$ 3,283.36**	**$ 3,283.36**	**$ 3,283.36**
	Bronze Tier										
	Windows pConfig - 1	$ 311 82	$ 309 30	$ 306 19	$ 303 21	$ 300 24	$ 297 26	$ 295 34	$ 295 34	$ 295 34	$ 295 34
	Windows pConfig - 2	$ 341 60	$ 338 32	$ 333 83	$ 329 80	$ 325 74	$ 321 65	$ 322 75	$ 322 75	$ 322 75	$ 322 75
	Windows pConfig - 3	$ 364 29	$ 356 56	$ 346 63	$ 338 59	$ 330 42	$ 322 11	$ 334 89	$ 334 89	$ 334 89	$ 334 89
	Windows pConfig - 4	$ 346 06	$ 342 92	$ 338 56	$ 334 67	$ 330 76	$ 326 82	$ 327 34	$ 327 34	$ 327 34	$ 327 34
	Windows pConfig - 5	$ 341 60	$ 338 32	$ 333 83	$ 329 80	$ 325 74	$ 321 65	$ 322 75	$ 322 75	$ 322 75	$ 322 75
	Linux pConfig - 1	$ 338 95	$ 330 48	$ 324 35	$ 318 31	$ 312 36	$ 306 50	$ 305 93	$ 305 93	$ 305 93	$ 305 93
	Linux pConfig - 2	$ 368 10	$ 359 13	$ 351 98	$ 344 90	$ 337 87	$ 330 89	$ 333 33	$ 333 33	$ 333 33	$ 333 33

Note: The Commonwealth has established mult

Baseline Units - Volumetrics

Price per unit \ per month

Resource Description	Service Tier / Configuration (6)	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
	Linux pConfig - 3	$ 388 27	$ 375 85	$ 364 79	$ 353 69	$ 342 54	$ 331 35	$ 345 47	$ 345 47	$ 345 47	$ 345 47
	Linux pConfig - 4	$ 372 56	$ 363 72	$ 356 72	$ 349 77	$ 342 89	$ 336 06	$ 337 93	$ 337 93	$ 337 93	$ 337 93
	Linux pConfig - 5	$ 368 10	$ 359 13	$ 351 98	$ 344 90	$ 337 87	$ 330 89	$ 333 33	$ 333 33	$ 333 33	$ 333 33
sub-total x86 (Windows, Linux) - Physical Servers - Bronze		**$ 3,541.34**	**$ 3,473.75**	**$ 3,408.85**	**$ 3,347.64**	**$ 3,286.42**	**$ 3,225.18**	**$ 3,259.07**	**$ 3,259.07**	**$ 3,259.07**	**$ 3,259.07**
	Basic Tier										
	Windows pConfig - 1	$ 310 46	$ 308 07	$ 305 02	$ 302 10	$ 299 18	$ 296 26	$ 294 39	$ 294 39	$ 294 39	$ 294 39
	Windows pConfig - 2	$ 340 23	$ 337 10	$ 332 66	$ 328 69	$ 324 69	$ 320 65	$ 321 80	$ 321 80	$ 321 80	$ 321 80
	Windows pConfig - 3	$ 362 93	$ 355 33	$ 345 46	$ 337 48	$ 329 36	$ 321 11	$ 333 94	$ 333 94	$ 333 94	$ 333 94
	Windows pConfig - 4	$ 344 69	$ 341 69	$ 337 39	$ 333 57	$ 329 71	$ 325 82	$ 326 39	$ 326 39	$ 326 39	$ 326 39
	Windows pConfig - 5	$ 340 23	$ 337 10	$ 332 66	$ 328 69	$ 324 69	$ 320 65	$ 321 80	$ 321 80	$ 321 80	$ 321 80
	Linux pConfig - 1	$ 333 92	$ 325 96	$ 320 05	$ 314 22	$ 308 48	$ 302 81	$ 302 42	$ 302 42	$ 302 42	$ 302 42
	Linux pConfig - 2	$ 363 07	$ 354 60	$ 347 68	$ 340 81	$ 333 99	$ 327 20	$ 329 83	$ 329 83	$ 329 83	$ 329 83
	Linux pConfig - 3	$ 383 24	$ 371 33	$ 360 49	$ 349 60	$ 338 66	$ 327 66	$ 341 97	$ 341 97	$ 341 97	$ 341 97
	Linux pConfig - 4	$ 367 53	$ 359 20	$ 352 42	$ 345 69	$ 339 01	$ 332 37	$ 334 42	$ 334 42	$ 334 42	$ 334 42
	Linux pConfig - 5	$ 363 07	$ 354 60	$ 347 68	$ 340 81	$ 333 99	$ 327 20	$ 329 83	$ 329 83	$ 329 83	$ 329 83
sub-total x86 (Windows, Linux) - Physical Servers - Basic		**$ 3,509.36**	**$ 3,444.98**	**$ 3,381.51**	**$ 3,321.67**	**$ 3,261.75**	**$ 3,201.74**	**$ 3,236.80**	**$ 3,236.80**	**$ 3,236.80**	**$ 3,236.80**
Total - Fully Managed - x86 Physical - All Support Tiers (Window, Linux)		**$ 18,039.00**	**$ 17,667.84**	**$ 17,328.38**	**$ 17,008.11**	**$ 16,688.54**	**$ 16,369.49**	**$ 16,526.76**	**$ 16,526.76**	**$ 16,526.76**	**$ 16,526.76**
x86 (Windows, Linux) - Virtual Servers											
	Platinum Tier										
	Windows vConfig - 1	$ 92 51	$ 86 63	$ 84 18	$ 81 95	$ 79 78	$ 77 39	$ 74 87	$ 74 87	$ 74 87	$ 74 87
	Windows vConfig - 2	$ 120 51	$ 114 57	$ 112 00	$ 109 65	$ 107 34	$ 103 82	$ 101 24	$ 101 24	$ 101 24	$ 101 24
	Windows vConfig - 3	$ 228 73	$ 222 57	$ 219 62	$ 216 86	$ 214 05	$ 206 61	$ 203 82	$ 203 82	$ 203 82	$ 203 82
	Windows vConfig - 4	$ 120 51	$ 114 59	$ 112 06	$ 109 65	$ 107 45	$ 103 85	$ 101 35	$ 101 35	$ 101 35	$ 101 35
	Windows vConfig - 5	$ 120 51	$ 114 59	$ 112 06	$ 109 65	$ 107 45	$ 103 85	$ 101 35	$ 101 35	$ 101 35	$ 101 35
	Linux vConfig - 1	$ 171 89	$ 157 39	$ 152 13	$ 146 17	$ 140 97	$ 134 91	$ 129 45	$ 129 45	$ 129 45	$ 129 45
	Linux vConfig - 2	$ 199 89	$ 185 33	$ 179 96	$ 173 87	$ 168 54	$ 161 35	$ 155 82	$ 155 82	$ 155 82	$ 155 82
	Linux vConfig - 3	$ 308 11	$ 293 33	$ 287 57	$ 281 08	$ 275 25	$ 264 13	$ 258 40	$ 258 40	$ 258 40	$ 258 40
	Linux vConfig - 4	$ 199 89	$ 185 39	$ 180 07	$ 174 06	$ 168 62	$ 161 43	$ 156 01	$ 156 01	$ 156 01	$ 156 01
	Linux vConfig - 5	$ 199 89	$ 185 39	$ 180 07	$ 174 06	$ 168 62	$ 161 43	$ 156 01	$ 156 01	$ 156 01	$ 156 01
sub-total x86 (Windows, Linux) - Virtual Servers - Platinum		**$ 1,762.44**	**$ 1,659.78**	**$ 1,619.73**	**$ 1,576.99**	**$ 1,538.06**	**$ 1,478.77**	**$ 1,438.32**	**$ 1,438.32**	**$ 1,438.32**	**$ 1,438.32**
	Gold Tier										
	Windows vConfig - 1	$ 89 05	$ 83 78	$ 81 58	$ 79 57	$ 77 60	$ 75 40	$ 73 04	$ 73 04	$ 73 04	$ 73 04
	Windows vConfig - 2	$ 117 05	$ 111 72	$ 109 41	$ 107 27	$ 105 17	$ 101 83	$ 99 41	$ 99 41	$ 99 41	$ 99 41
	Windows vConfig - 3	$ 225 27	$ 219 72	$ 217 02	$ 214 48	$ 211 88	$ 204 61	$ 201 99	$ 201 99	$ 201 99	$ 201 99
	Windows vConfig - 4	$ 117 05	$ 111 75	$ 109 47	$ 107 27	$ 105 28	$ 101 85	$ 99 52	$ 99 52	$ 99 52	$ 99 52
	Windows vConfig - 5	$ 117 05	$ 111 75	$ 109 47	$ 107 27	$ 105 28	$ 101 85	$ 99 52	$ 99 52	$ 99 52	$ 99 52
	Linux vConfig - 1	$ 155 59	$ 144 21	$ 140 08	$ 135 31	$ 131 12	$ 126 09	$ 121 47	$ 121 47	$ 121 47	$ 121 47
	Linux vConfig - 2	$ 183 59	$ 172 15	$ 167 91	$ 163 01	$ 158 69	$ 152 52	$ 147 84	$ 147 84	$ 147 84	$ 147 84
	Linux vConfig - 3	$ 291 81	$ 280 15	$ 275 52	$ 270 22	$ 265 40	$ 255 30	$ 250 42	$ 250 42	$ 250 42	$ 250 42
	Linux vConfig - 4	$ 183 59	$ 172 20	$ 168 02	$ 163 20	$ 158 77	$ 152 60	$ 148 03	$ 148 03	$ 148 03	$ 148 03
	Linux vConfig - 5	$ 183 59	$ 172 20	$ 168 02	$ 163 20	$ 158 77	$ 152 60	$ 148 03	$ 148 03	$ 148 03	$ 148 03
sub-total x86 (Windows, Linux) - Virtual Servers - Gold		**$ 1,663.64**	**$ 1,579.63**	**$ 1,546.50**	**$ 1,510.81**	**$ 1,477.95**	**$ 1,424.65**	**$ 1,389.29**	**$ 1,389.29**	**$ 1,389.29**	**$ 1,389.29**
	Silver Tier										
	Windows vConfig - 1	$ 85 95	$ 81 20	$ 79 22	$ 77 39	$ 75 61	$ 73 55	$ 71 35	$ 71 35	$ 71 35	$ 71 35
	Windows vConfig - 2	$ 113 95	$ 109 14	$ 107 04	$ 105 10	$ 103 17	$ 99 99	$ 97 72	$ 97 72	$ 97 72	$ 97 72

Note: The Commonwealth has established mult

Baseline Units - Volumetrics

Price per unit \ per month

Resource Description	Service Tier / Configuration (6)	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
	Windows vConfig - 3	$ 222 17	$ 217 14	$ 214 66	$ 212 30	$ 209 88	$ 202 77	$ 200 30	$ 200 30	$ 200 30	$ 200 30
	Windows vConfig - 4	$ 113 95	$ 109 17	$ 107 11	$ 105 10	$ 103 28	$ 100 01	$ 97 83	$ 97 83	$ 97 83	$ 97 83
	Windows vConfig - 5	$ 113 95	$ 109 17	$ 107 11	$ 105 10	$ 103 28	$ 100 01	$ 97 83	$ 97 83	$ 97 83	$ 97 83
	Linux vConfig - 1	$ 142 61	$ 133 46	$ 130 16	$ 126 27	$ 122 85	$ 118 59	$ 114 64	$ 114 64	$ 114 64	$ 114 64
	Linux vConfig - 2	$ 170 61	$ 161 40	$ 157 99	$ 153 98	$ 150 42	$ 145 03	$ 141 01	$ 141 01	$ 141 01	$ 141 01
	Linux vConfig - 3	$ 278 83	$ 269 40	$ 265 60	$ 261 18	$ 257 12	$ 247 81	$ 243 59	$ 243 59	$ 243 59	$ 243 59
	Linux vConfig - 4	$ 170 61	$ 161 46	$ 158 10	$ 154 17	$ 150 50	$ 145 11	$ 141 20	$ 141 20	$ 141 20	$ 141 20
	Linux vConfig - 5	$ 170 61	$ 161 46	$ 158 10	$ 154 17	$ 150 50	$ 145 11	$ 141 20	$ 141 20	$ 141 20	$ 141 20
sub-total x86 (Windows, Linux) - Virtual Servers - Silver		**$ 1,583.25**	**$ 1,513.01**	**$ 1,485.08**	**$ 1,454.75**	**$ 1,426.59**	**$ 1,377.99**	**$ 1,346.67**	**$ 1,346.67**	**$ 1,346.67**	**$ 1,346.67**
	Bronze Tier										
	Windows vConfig - 1	$ 84 52	$ 80 00	$ 78 11	$ 76 37	$ 74 67	$ 72 69	$ 70 55	$ 70 55	$ 70 55	$ 70 55
	Windows vConfig - 2	$ 112 52	$ 107 94	$ 105 94	$ 104 07	$ 102 23	$ 99 12	$ 96 92	$ 96 92	$ 96 92	$ 96 92
	Windows vConfig - 3	$ 220 73	$ 215 94	$ 213 55	$ 211 28	$ 208 94	$ 201 90	$ 199 50	$ 199 50	$ 199 50	$ 199 50
	Windows vConfig - 4	$ 112 52	$ 107 97	$ 106 00	$ 104 07	$ 102 34	$ 99 14	$ 97 03	$ 97 03	$ 97 03	$ 97 03
	Windows vConfig - 5	$ 112 52	$ 107 97	$ 106 00	$ 104 07	$ 102 34	$ 99 14	$ 97 03	$ 97 03	$ 97 03	$ 97 03
	Linux vConfig - 1	$ 137 07	$ 128 81	$ 125 83	$ 122 30	$ 119 19	$ 115 26	$ 111 58	$ 111 58	$ 111 58	$ 111 58
	Linux vConfig - 2	$ 165 07	$ 156 74	$ 153 66	$ 150 01	$ 146 76	$ 141 69	$ 137 95	$ 137 95	$ 137 95	$ 137 95
	Linux vConfig - 3	$ 273 29	$ 264 74	$ 261 27	$ 257 21	$ 253 47	$ 244 48	$ 240 53	$ 240 53	$ 240 53	$ 240 53
	Linux vConfig - 4	$ 165 07	$ 156 80	$ 153 77	$ 150 20	$ 146 84	$ 141 78	$ 138 14	$ 138 14	$ 138 14	$ 138 14
	Linux vConfig - 5	$ 165 07	$ 156 80	$ 153 77	$ 150 20	$ 146 84	$ 141 78	$ 138 14	$ 138 14	$ 138 14	$ 138 14
sub-total x86 (Windows, Linux) - Virtual Servers - Bronze		**$ 1,548.37**	**$ 1,483.71**	**$ 1,457.91**	**$ 1,429.79**	**$ 1,403.60**	**$ 1,356.97**	**$ 1,327.36**	**$ 1,327.36**	**$ 1,327.36**	**$ 1,327.36**
	Basic Tier										
	Windows vConfig - 1	$ 83 15	$ 78 85	$ 77 05	$ 75 39	$ 73 76	$ 71 85	$ 69 78	$ 69 78	$ 69 78	$ 69 78
	Windows vConfig - 2	$ 111 15	$ 106 79	$ 104 88	$ 103 09	$ 101 33	$ 98 28	$ 96 15	$ 96 15	$ 96 15	$ 96 15
	Windows vConfig - 3	$ 219 37	$ 214 79	$ 212 49	$ 210 30	$ 208 04	$ 201 07	$ 198 72	$ 198 72	$ 198 72	$ 198 72
	Windows vConfig - 4	$ 111 15	$ 106 82	$ 104 94	$ 103 09	$ 101 43	$ 98 31	$ 96 25	$ 96 25	$ 96 25	$ 96 25
	Windows vConfig - 5	$ 111 15	$ 106 82	$ 104 94	$ 103 09	$ 101 43	$ 98 31	$ 96 25	$ 96 25	$ 96 25	$ 96 25
	Linux vConfig - 1	$ 132 04	$ 124 54	$ 121 85	$ 118 64	$ 115 80	$ 112 16	$ 108 73	$ 108 73	$ 108 73	$ 108 73
	Linux vConfig - 2	$ 160 04	$ 152 48	$ 149 68	$ 146 35	$ 143 37	$ 138 59	$ 135 10	$ 135 10	$ 135 10	$ 135 10
	Linux vConfig - 3	$ 268 26	$ 260 48	$ 257 30	$ 253 55	$ 250 08	$ 241 37	$ 237 68	$ 237 68	$ 237 68	$ 237 68
	Linux vConfig - 4	$ 160 04	$ 152 54	$ 149 80	$ 146 53	$ 143 45	$ 138 67	$ 135 28	$ 135 28	$ 135 28	$ 135 28
	Linux vConfig - 5	$ 160 04	$ 152 54	$ 149 80	$ 146 53	$ 143 45	$ 138 67	$ 135 28	$ 135 28	$ 135 28	$ 135 28
sub-total x86 (Windows, Linux) - Virtual Servers - Basic		**$ 1,516.39**	**$ 1,456.65**	**$ 1,432.73**	**$ 1,406.57**	**$ 1,382.14**	**$ 1,337.28**	**$ 1,309.23**	**$ 1,309.23**	**$ 1,309.23**	**$ 1,309.23**
Total - Fully Managed - x86 Virtual - All Support Tiers (Window, Linux)		**$ 8,074.10**	**$ 7,692.79**	**$ 7,541.95**	**$ 7,378.91**	**$ 7,228.34**	**$ 6,975.66**	**$ 6,810.87**	**$ 6,810.87**	**$ 6,810.87**	**$ 6,810.87**
UNIX (IBM P-Series, AIX)											
	Platinum Tier										
	AIX Config - 1	$ 667 88	$ 660 97	$ 654 06	$ 647 15	$ 640 30	$ 634 26	$ 628 20	$ 622 15	$ 616 17	$ 610 12
	AIX Config - 2	$ 702 38	$ 695 44	$ 688 52	$ 681 59	$ 674 80	$ 667 87	$ 660 94	$ 654 01	$ 647 22	$ 640 29
	AIX Config - 3	$ 754 11	$ 746 30	$ 738 49	$ 730 69	$ 723 95	$ 717 00	$ 710 04	$ 703 10	$ 696 37	$ 689 42
	AIX Config - 4	$ 702 38	$ 695 44	$ 688 52	$ 681 59	$ 674 80	$ 667 87	$ 660 94	$ 654 01	$ 647 22	$ 640 29
	AIX Config - 5	$ 702 38	$ 695 44	$ 688 52	$ 681 59	$ 674 80	$ 667 87	$ 660 94	$ 654 01	$ 647 22	$ 640 29
sub-total P-Series (AIX) - Bronze		**$ 3,529.12**	**$ 3,493.60**	**$ 3,458.11**	**$ 3,422.62**	**$ 3,388.65**	**$ 3,354.88**	**$ 3,321.06**	**$ 3,287.30**	**$ 3,254.19**	**$ 3,220.42**
	Gold Tier										
	AIX Config - 1	$ 551 55	$ 546 35	$ 541 17	$ 535 99	$ 530 86	$ 525 68	$ 520 49	$ 515 30	$ 510 18	$ 505 00
	AIX Config - 2	$ 586 03	$ 579 97	$ 573 91	$ 567 84	$ 561 91	$ 555 85	$ 550 64	$ 545 44	$ 540 37	$ 535 16

Note: The Commonwealth has established mult

Baseline Units - Volumetrics

Price per unit \ per month

Resource Description	Service Tier / Configuration (6)	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
	AIX Config - 3	$ 637 76	$ 631 68	$ 625 61	$ 619 52	$ 613 64	$ 607 56	$ 601 47	$ 595 38	$ 589 51	$ 583 42
	AIX Config - 4	$ 586 03	$ 579 97	$ 573 91	$ 567 84	$ 561 91	$ 555 85	$ 550 64	$ 545 44	$ 540 37	$ 535 16
	AIX Config - 5	$ 586 03	$ 579 97	$ 573 91	$ 567 84	$ 561 91	$ 555 85	$ 550 64	$ 545 44	$ 540 37	$ 535 16
sub-total P-Series (AIX) - Gold		**$ 2,947.41**	**$ 2,917.93**	**$ 2,888.51**	**$ 2,859.04**	**$ 2,830.24**	**$ 2,800.79**	**$ 2,773.86**	**$ 2,747.00**	**$ 2,720.79**	**$ 2,693.89**
	Silver Tier										
	AIX Config - 1	$ 452 44	$ 448 12	$ 443 80	$ 439 47	$ 435 21	$ 430 89	$ 426 56	$ 422 23	$ 417 97	$ 413 65
	AIX Config - 2	$ 486 94	$ 481 73	$ 476 53	$ 471 32	$ 467 12	$ 462 78	$ 458 43	$ 454 09	$ 449 88	$ 445 53
	AIX Config - 3	$ 525 74	$ 520 51	$ 515 30	$ 510 08	$ 505 06	$ 499 84	$ 494 61	$ 489 39	$ 484 37	$ 479 15
	AIX Config - 4	$ 486 94	$ 481 73	$ 476 53	$ 471 32	$ 467 12	$ 462 78	$ 458 43	$ 454 09	$ 449 88	$ 445 53
	AIX Config - 5	$ 486 94	$ 481 73	$ 476 53	$ 471 32	$ 467 12	$ 462 78	$ 458 43	$ 454 09	$ 449 88	$ 445 53
sub-total P-Series (AIX) - Silver		**$ 2,439.00**	**$ 2,413.82**	**$ 2,388.69**	**$ 2,363.51**	**$ 2,341.62**	**$ 2,319.05**	**$ 2,296.46**	**$ 2,273.90**	**$ 2,251.97**	**$ 2,229.41**
	Bronze Tier										
	AIX Config - 1	$ 353 34	$ 349 88	$ 346 42	$ 342 96	$ 339 55	$ 336 09	$ 332 63	$ 329 16	$ 325 76	$ 322 31
	AIX Config - 2	$ 387 84	$ 384 35	$ 380 88	$ 377 39	$ 374 05	$ 370 57	$ 367 09	$ 363 60	$ 360 26	$ 356 78
	AIX Config - 3	$ 439 57	$ 435 19	$ 430 85	$ 426 49	$ 422 33	$ 417 98	$ 413 60	$ 409 25	$ 405 09	$ 400 73
	AIX Config - 4	$ 387 84	$ 384 35	$ 380 88	$ 377 39	$ 374 05	$ 370 57	$ 367 09	$ 363 60	$ 360 26	$ 356 78
	AIX Config - 5	$ 387 84	$ 384 35	$ 380 88	$ 377 39	$ 374 05	$ 370 57	$ 367 09	$ 363 60	$ 360 26	$ 356 78
sub-total P-Series (AIX) - Bronze		**$ 1,956.41**	**$ 1,938.13**	**$ 1,919.91**	**$ 1,901.62**	**$ 1,884.02**	**$ 1,865.79**	**$ 1,847.49**	**$ 1,829.22**	**$ 1,811.62**	**$ 1,793.38**
	Basic Tier										
	AIX Config - 1	$ 254 24	$ 251 63	$ 249 04	$ 246 43	$ 243 90	$ 241 31	$ 238 70	$ 236 10	$ 233 56	$ 230 96
	AIX Config - 2	$ 288 73	$ 286 12	$ 283 50	$ 280 88	$ 278 39	$ 275 78	$ 273 15	$ 270 53	$ 268 05	$ 265 44
	AIX Config - 3	$ 340 46	$ 336 96	$ 333 47	$ 329 98	$ 326 68	$ 323 18	$ 319 67	$ 316 18	$ 312 89	$ 309 38
	AIX Config - 4	$ 288 73	$ 286 12	$ 283 50	$ 280 88	$ 278 39	$ 275 78	$ 273 15	$ 270 53	$ 268 05	$ 265 44
	AIX Config - 5	$ 288 73	$ 286 12	$ 283 50	$ 280 88	$ 278 39	$ 275 78	$ 273 15	$ 270 53	$ 268 05	$ 265 44
sub-total P-Series (AIX) - Basic		**$ 1,460.90**	**$ 1,446.94**	**$ 1,433.01**	**$ 1,419.06**	**$ 1,405.75**	**$ 1,391.81**	**$ 1,377.81**	**$ 1,363.87**	**$ 1,350.60**	**$ 1,336.65**
Total - Fully Managed - P-Series (AIX) - All Support Tiers (Window, Linux)		**$ 12,332.85**	**$ 12,210.42**	**$ 12,088.22**	**$ 11,965.85**	**$ 11,850.29**	**$ 11,732.32**	**$ 11,616.69**	**$ 11,501.29**	**$ 11,389.17**	**$ 11,273.75**
Server - Managed Only (2)											
x86 (Windows, Linux)											
	Platinum Tier	$ 143 46	$ 129 22	$ 124 13	$ 118 36	$ 113 26	$ 107 71	$ 102 93	$ 102 93	$ 102 93	$ 102 93
	Gold Tier	$ 127 16	$ 116 03	$ 112 08	$ 107 50	$ 103 41	$ 98 88	$ 94 95	$ 94 95	$ 94 95	$ 94 95
	Silver Tier	$ 114 19	$ 105 29	$ 102 16	$ 98 47	$ 95 14	$ 91 39	$ 88 12	$ 88 12	$ 88 12	$ 88 12
	Bronze Tier	$ 108 64	$ 100 63	$ 97 83	$ 94 50	$ 91 48	$ 88 06	$ 85 06	$ 85 06	$ 85 06	$ 85 06
	Basic Tier	$ 103 61	$ 96 37	$ 93 85	$ 90 84	$ 88 09	$ 84 96	$ 82 21	$ 82 21	$ 82 21	$ 82 21
Total Managed Only- x86 - All Support Tiers (Window, Linux)		**$ 597.07**	**$ 547.54**	**$ 530.05**	**$ 509.67**	**$ 491.38**	**$ 471.00**	**$ 453.28**	**$ 453.28**	**$ 453.28**	**$ 453.28**
UNIX (IBM P-Series, AIX)											
	Platinum	$ 479 79	$ 474 95	$ 470 11	$ 465 28	$ 460 44	$ 455 60	$ 450 77	$ 445 93	$ 441 09	$ 436 26
	Gold Tier	$ 428 51	$ 424 65	$ 420 78	$ 416 91	$ 413 04	$ 409 17	$ 405 30	$ 401 43	$ 397 56	$ 393 70
	Silver Tier	$ 379 19	$ 375 32	$ 371 44	$ 367 57	$ 363 71	$ 359 84	$ 355 97	$ 352 10	$ 348 23	$ 344 36
	Bronze Tier	$ 320 18	$ 317 27	$ 314 38	$ 311 47	$ 308 57	$ 305 67	$ 302 77	$ 299 86	$ 296 97	$ 294 06
	Basic Tier	$ 206 04	$ 204 10	$ 202 17	$ 200 23	$ 198 30	$ 196 37	$ 194 43	$ 192 49	$ 190 55	$ 188 62
Total Managed Only- P-Series - All Support Tiers (AIX)		**$ 1,813.70**	**$ 1,796.29**	**$ 1,778.87**	**$ 1,761.47**	**$ 1,744.06**	**$ 1,726.64**	**$ 1,709.24**	**$ 1,691.81**	**$ 1,674.40**	**$ 1,656.99**
Storage and Backup - Fully Managed (1)											

Note: The Commonwealth has established mult

Baseline Units - Volumetrics

Price per unit \ per month

Resource Description	Service Tier / Configuration (6)	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Enterprise Storage											
	* Dedicated - Config 1 - SAN Raid 5	$ 0 06	$ 0 05	$ 0 05	$ 0 05	$ 0 05	$ 0 04	$ 0 04	$ 0 04	$ 0 03	$ 0 03
	* Dedicated - Config 2 - SAN Raid 10	$ 0 24	$ 0 24	$ 0 24	$ 0 23	$ 0 23	$ 0 23	$ 0 23	$ 0 21	$ 0 19	$ 0 17
	Dedicated - Config 3 - Net Attached	$ 0 07	$ 0 06	$ 0 06	$ 0 05	$ 0 05	$ 0 03	$ 0 03	$ 0 03	$ 0 03	$ 0 02
Total Enterprise Storage - Fully Managed		**$ 0.37**	**$ 0.36**	**$ 0.35**	**$ 0.34**	**$ 0.33**	**$ 0.31**	**$ 0.30**	**$ 0.27**	**$ 0.25**	**$ 0.23**
Tape and Backup											
	** Server Tape Stored	$ 0 07	$ 0 05	$ 0 05	$ 0 04	$ 0 04	$ 0 04	$ 0 04	$ 0 03	$ 0 03	$ 0 03
	** Offsite Tape Storage	$ 0 24	$ 0 24	$ 0 24	$ 0 23	$ 0 23	$ 0 23	$ 0 23	$ 0 21	$ 0 19	$ 0 17
Total Tape and Backup - Fully Managed		**$ 0.31**	**$ 0.29**	**$ 0.28**	**$ 0.28**	**$ 0.27**	**$ 0.26**	**$ 0.27**	**$ 0.24**	**$ 0.22**	**$ 0.20**
Limited Co-Lo (Data Center Only Charge) (3)											
Server, Storage, Network, Security Equipment											
	Co-Lo Config - 1	$ 49 85	$ 50 23	$ 50 63	$ 51 04	$ 53 10	$ 53 53	$ 53 98	$ 53 98	$ 53 98	$ 53 98
	Co-Lo Config - 2	$ 75 65	$ 76 42	$ 77 21	$ 78 03	$ 80 51	$ 81 38	$ 82 27	$ 82 27	$ 82 27	$ 82 27
	Co-Lo Config - 3	$ 135 48	$ 137 01	$ 138 59	$ 140 22	$ 144 55	$ 146 09	$ 147 67	$ 147 67	$ 147 67	$ 147 67
Total Limited Co-Lo (Data Center Only Charge)		**$ 260.98**	**$ 263.67**	**$ 266.44**	**$ 269.29**	**$ 278.16**	**$ 280.99**	**$ 283.91**	**$ 283.91**	**$ 283.91**	**$ 283.91**
Mainframe Services (4)											
IBM Services											
	*** IBM Mainframe Allocated DASD	$ 1 25	$ 1 19	$ 1 13	$ 1 07	$ 1 02	$ 0 97	$ 0 92	$ 0 92	$ 0 92	$ 0 92
	IBM Tapes in Storage - VTS	$ 0 29	$ 0 28	$ 0 28	$ 0 28	$ 0 27	$ 0 26	$ 0 26	$ 0 25	$ 0 25	$ 0 24
	IBM Offsite Tape Storage	$ 0 24	$ 0 24	$ 0 24	$ 0 23	$ 0 23	$ 0 23	$ 0 23	$ 0 21	$ 0 19	$ 0 17
Total IBM Services		**$ 1.78**	**$ 1.71**	**$ 1.64**	**$ 1.58**	**$ 1.52**	**$ 1.46**	**$ 1.41**	**$ 1.38**	**$ 1.36**	**$ 1.34**
IBM Configurations											
	Platinum Tier										
	IBM Mainframe Config - 1	$ 159 21	$ 151 26	$ 143 69	$ 136 52	$ 129 70	$ 123 21	$ 117 05	$ 117 05	$ 117 05	$ 117 05
	IBM Mainframe Config - 2	$ 139 89	$ 132 89	$ 126 25	$ 119 93	$ 113 94	$ 108 24	$ 102 83	$ 102 83	$ 102 83	$ 102 83
	IBM Mainframe Config - 3	$ 139 89	$ 132 89	$ 126 25	$ 119 93	$ 113 94	$ 108 24	$ 102 83	$ 102 83	$ 102 83	$ 102 83
	IBM AS400 Config 1	$ 17 37	$ 16 50	$ 15 68	$ 14 89	$ 14 15	$ 13 44	$ 12 77	$ 12 77	$ 12 77	$ 12 77
	IBM AS400 Config 2	$ 17 37	$ 16 50	$ 15 68	$ 14 89	$ 14 15	$ 13 44	$ 12 77	$ 12 77	$ 12 77	$ 12 77
sub-total IBM Mainfram Services - Plantinum		**$ 473.72**	**$ 450.04**	**$ 427.54**	**$ 406.17**	**$ 385.87**	**$ 366.58**	**$ 348.26**	**$ 348.26**	**$ 348.26**	**$ 348.26**
	Gold Tier										
	IBM Mainframe Config - 1	$ 148 50	$ 141 08	$ 134 03	$ 127 32	$ 120 95	$ 114 91	$ 109 17	$ 109 17	$ 109 17	$ 109 17
	IBM Mainframe Config - 2	$ 130 48	$ 123 96	$ 117 77	$ 111 88	$ 106 28	$ 100 97	$ 95 92	$ 95 92	$ 95 92	$ 95 92
	IBM Mainframe Config - 3	$ 130 48	$ 123 96	$ 117 77	$ 111 88	$ 106 28	$ 100 97	$ 95 92	$ 95 92	$ 95 92	$ 95 92
	IBM AS400 Config 1	$ 16 20	$ 15 39	$ 14 62	$ 13 89	$ 13 20	$ 12 54	$ 11 91	$ 11 91	$ 11 91	$ 11 91
	IBM AS400 Config 2	$ 16 20	$ 15 39	$ 14 62	$ 13 89	$ 13 20	$ 12 54	$ 11 91	$ 11 91	$ 11 91	$ 11 91
sub-total IBM Mainfram Services - Gold		**$ 441.86**	**$ 419.78**	**$ 398.81**	**$ 378.86**	**$ 359.92**	**$ 341.93**	**$ 324.84**	**$ 324.84**	**$ 324.84**	**$ 324.84**
	Basic Tier										
	IBM Mainframe Config - 1	$ 141 08	$ 134 03	$ 127 32	$ 120 95	$ 114 91	$ 109 17	$ 103 71	$ 103 71	$ 103 71	$ 103 71
	IBM Mainframe Config - 2	$ 123 96	$ 117 77	$ 111 88	$ 106 28	$ 100 97	$ 95 92	$ 91 13	$ 91 13	$ 91 13	$ 91 13
	IBM Mainframe Config - 3	$ 123 96	$ 117 77	$ 111 88	$ 106 28	$ 100 97	$ 95 92	$ 91 13	$ 91 13	$ 91 13	$ 91 13
	IBM AS400 Config 1	$ 15 39	$ 14 62	$ 13 89	$ 13 20	$ 12 54	$ 11 91	$ 11 32	$ 11 32	$ 11 32	$ 11 32
	IBM AS400 Config 2	$ 15 39	$ 14 62	$ 13 89	$ 13 20	$ 12 54	$ 11 91	$ 11 32	$ 11 32	$ 11 32	$ 11 32
sub-total IBM Mainfram Services - Basic		**$ 419.78**	**$ 398.81**	**$ 378.86**	**$ 359.92**	**$ 341.93**	**$ 324.84**	**$ 308.61**	**$ 308.61**	**$ 308.61**	**$ 308.61**

Note: The Commonwealth has established mult

Baseline Units - Volumetrics

Price per unit \ per month

Resource Description	Service Tier / Configuration (6)	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Total - IBM Mainfram Services - All Support Tiers		**$ 1,335.37**	**$ 1,268.64**	**$ 1,205.22**	**$ 1,144.95**	**$ 1,087.71**	**$ 1,033.34**	**$ 981.71**	**$ 981.71**	**$ 981.71**	**$ 981.71**
Unisys Services											
	*** Unisys DASD	$ 0 10	$ 0 10	$ 0 10	$ 0 10	$ 0 10	$ 0 07	$ 0 07	$ 0 07	$ 0 07	$ 0 07
	Unisys Tapes in Storage - VTS	$ 0 16	$ 0 16	$ 0 16	$ 0 16	$ 0 16	$ 0 15	$ 0 15	$ 0 15	$ 0 15	$ 0 15
	Unisys Offsite Tape Storage	$ 0 24	$ 0 24	$ 0 24	$ 0 23	$ 0 23	$ 0 23	$ 0 23	$ 0 21	$ 0 19	$ 0 17
Total Unisys Services		**$ 0.50**	**$ 0.49**	**$ 0.49**	**$ 0.49**	**$ 0.49**	**$ 0.44**	**$ 0.45**	**$ 0.43**	**$ 0.41**	**$ 0.39**
Unisys Configurations											
	Platinum Tier										
	Unisys Mainframe Config - 1	$ 1,007 63	$ 990 98	$ 982 84	$ 975 07	$ 965 22	$ 959 85	$ 943 16	$ 943 16	$ 943 16	$ 943 16
	Unisys Mainframe Config - 2	$ 986 88	$ 974 93	$ 969 96	$ 964 99	$ 955 52	$ 952 01	$ 943 16	$ 943 16	$ 943 16	$ 943 16
	Unisys Mainframe Config - 3	$ 9 83	$ 9 73	$ 9 69	$ 9 64	$ 9 56	$ 9 11	$ 9 05	$ 9 05	$ 9 05	$ 9 05
	Unisys Mainframe Config - 4	$ 14 32	$ 14 26	$ 14 23	$ 14 20	$ 14 14	$ 13 81	$ 13 48	$ 13 48	$ 13 48	$ 13 48
sub-total Unisys Mainfram Services - Plantinum		**$ 2,018.66**	**$ 1,989.90**	**$ 1,976.72**	**$ 1,963.90**	**$ 1,944.44**	**$ 1,934.79**	**$ 1,908.86**	**$ 1,908.86**	**$ 1,908.86**	**$ 1,908.86**
	Gold Tier										
	Unisys Mainframe Config - 1	$ 916 03	$ 900 89	$ 893 50	$ 886 42	$ 877 47	$ 872 60	$ 857 42	$ 857 42	$ 857 42	$ 857 42
	Unisys Mainframe Config - 2	$ 897 17	$ 886 30	$ 881 78	$ 877 26	$ 868 66	$ 865 46	$ 857 42	$ 857 42	$ 857 42	$ 857 42
	Unisys Mainframe Config - 3	$ 8 93	$ 8 85	$ 8 81	$ 8 77	$ 8 69	$ 8 28	$ 8 23	$ 8 23	$ 8 23	$ 8 23
	Unisys Mainframe Config - 4	$ 13 02	$ 12 96	$ 12 93	$ 12 91	$ 12 85	$ 12 55	$ 12 25	$ 12 25	$ 12 25	$ 12 25
sub-total Unisys Mainfram Services - Gold		**$ 1,835.15**	**$ 1,809.00**	**$ 1,797.02**	**$ 1,785.36**	**$ 1,767.67**	**$ 1,758.90**	**$ 1,735.32**	**$ 1,735.32**	**$ 1,735.32**	**$ 1,735.32**
	Basic Tier										
	Unisys Mainframe Config - 1	$ 839 69	$ 825 82	$ 819 04	$ 812 55	$ 804 35	$ 799 88	$ 785 96	$ 785 96	$ 785 96	$ 785 96
	Unisys Mainframe Config - 2	$ 822 40	$ 812 44	$ 804 16	$ 800 21	$ 796 27	$ 793 34	$ 785 97	$ 785 97	$ 785 97	$ 785 97
	Unisys Mainframe Config - 3	$ 8 19	$ 8 11	$ 8 04	$ 8 00	$ 7 97	$ 7 59	$ 7 55	$ 7 55	$ 7 55	$ 7 55
	Unisys Mainframe Config - 4	$ 11 94	$ 11 88	$ 11 83	$ 11 74	$ 11 68	$ 11 46	$ 11 23	$ 11 23	$ 11 23	$ 11 23
sub-total Unisys Mainfram Services - Basic		**$ 1,682.22**	**$ 1,658.25**	**$ 1,643.06**	**$ 1,632.51**	**$ 1,620.27**	**$ 1,612.27**	**$ 1,590.71**	**$ 1,590.71**	**$ 1,590.71**	**$ 1,590.71**
Total - Unisys Mainfram Services - All Support Tiers		**$ 5,536.03**	**$ 5,457.14**	**$ 5,416.80**	**$ 5,381.76**	**$ 5,332.38**	**$ 5,305.96**	**$ 5,234.89**	**$ 5,234.89**	**$ 5,234.89**	**$ 5,234.89**
On-Demand (IaaS) (5)											
IaaS Servers - x86 (Windows, Linux) - Virtual Servers											
	IaaS Windows vConfig - 1	$ 34 01	$ 32 62	$ 31 63	$ 31 55	$ 30 35	$ 30 29	$ 29 24	$ 29 24	$ 29 24	$ 29 24
	IaaS Windows vConfig - 2	$ 71 32	$ 67 67	$ 64 74	$ 63 03	$ 59 99	$ 57 82	$ 55 46	$ 55 46	$ 55 46	$ 55 46
	IaaS Windows vConfig - 3	$ 215 51	$ 203 31	$ 192 95	$ 184 96	$ 174 88	$ 164 81	$ 157 31	$ 157 31	$ 157 31	$ 157 31
	IaaS Windows vConfig - 4	$ 71 32	$ 67 67	$ 64 74	$ 63 03	$ 59 99	$ 57 82	$ 55 46	$ 55 46	$ 55 46	$ 55 46
	IaaS Windows vConfig - 5	$ 71 32	$ 67 67	$ 64 74	$ 63 03	$ 59 99	$ 57 82	$ 55 46	$ 55 46	$ 55 46	$ 55 46
	IaaS Linux vConfig - 1	$ 33 87	$ 32 48	$ 31 49	$ 31 41	$ 30 22	$ 30 16	$ 29 11	$ 29 11	$ 29 11	$ 34 42
	IaaS Linux vConfig - 2	$ 71 18	$ 67 53	$ 64 60	$ 62 90	$ 59 86	$ 57 69	$ 55 32	$ 55 32	$ 50 10	$ 71 34
	IaaS Linux vConfig - 3	$ 215 37	$ 203 17	$ 192 81	$ 184 82	$ 174 74	$ 164 68	$ 157 17	$ 157 17	$ 134 08	$ 219 02
	IaaS Linux vConfig - 4	$ 71 18	$ 67 53	$ 64 60	$ 62 90	$ 59 86	$ 57 69	$ 55 32	$ 55 32	$ 50 10	$ 71 34
	IaaS Linux vConfig - 5	$ 71 18	$ 67 53	$ 64 60	$ 62 90	$ 59 86	$ 57 69	$ 55 32	$ 55 32	$ 50 10	$ 71 34
Total IaaS Servers - x86 (Windows, Linux) - Virtual Servers		**$ 926.24**	**$ 877.20**	**$ 836.91**	**$ 810.52**	**$ 769.74**	**$ 736.45**	**$ 705.16**	**$ 705.16**	**$ 666.41**	**$ 820.36**
IaaS Storage On-Demand											
	IaaS Storage Config - 1	$ 0 06	$ 0 05	$ 0 05	$ 0 05	$ 0 05	$ 0 04	$ 0 04	$ 0 04	$ 0 03	$ 0 03
	IaaS Storage Config - 2	$ 0 24	$ 0 24	$ 0 24	$ 0 23	$ 0 23	$ 0 23	$ 0 23	$ 0 21	$ 0 19	$ 0 17
	IaaS Storage Config - 3	$ 0 07	$ 0 06	$ 0 06	$ 0 05	$ 0 05	$ 0 03	$ 0 03	$ 0 03	$ 0 03	$ 0 02

Baseline Units - Volumetrics

Note: The Commonwealth has established mult

Price per unit \ per month

Resource Description	Service Tier / Configuration (6)	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Total IaaS Storage On-Demand		**$ 0.37**	**$ 0.36**	**$ 0.35**	**$ 0.34**	**$ 0.33**	**$ 0.31**	**$ 0.30**	**$ 0.27**	**$ 0.25**	**$ 0.23**
IaaS Backup On-Demand											
	IaaS Backup Config - 1	$ 0 07	$ 0 05	$ 0 05	$ 0 04	$ 0 04	$ 0 04	$ 0 04	$ 0 03	$ 0 03	$ 0 03
Total IaaS Backup On-Demand		**$ 0.07**	**$ 0.05**	**$ 0.05**	**$ 0.04**	**$ 0.04**	**$ 0.04**	**$ 0.04**	**$ 0.03**	**$ 0.03**	**$ 0.03**
Reserve Account											
		$ 84,000 00	$ 84,000 00	$ 84,000 00	$ 84,000 00	$ 84,000 00	$ 84,000 00	$ 84,000 00	$ 84,000 00	$ 84,000 00	$ 84,000 00
Reserve Account		**$ 84,000.00**	**$ 84,000.00**	**$ 84,000.00**	**$ 84,000.00**	**$ 84,000.00**	**$ 84,000.00**	**$ 84,000.00**	**$ 84,000.00**	**$ 84,000.00**	**$ 84,000.00**

Notes:

For purposes of submitting a proposal, Offerors should assume that tapes are equivalent in ca

* For purposes of submitting a proposal, Offerors should assume that the slower Tier1 RAID

** The volume is expressed as native.

*** For purposes of evaluation DASD is expressed in Usable (not Raw)

Third Party Software

Third Party Software

Vendor	Product										
B & L	BL/LIB Tape Library Management System	$ 1,392.63	$ 1,459.61	$ 1,503.40	$ 1,548.51	$ 1,594.96	$ 1,642.81	$ 1,692.09	$ 1,692.09	$ 1,692.09	$ 1,692.09
B & L	BL/SCHED Scheduling & Monitoring System	$ 1,757.19	$ 1,841.71	$ 1,896.96	$ 1,953.87	$ 2,012.48	$ 2,072.86	$ 2,135.04	$ 2,135.04	$ 2,135.04	$ 2,135.04
BMC Software	BMC AppSight for Windows/.NET - Division Edition	$ 4,837.96	$ 4,983.10	$ 5,132.59	$ 5,286.57	$ 5,445.17	$ 5,608.53	$ 5,776.78	$ 5,776.78	$ 5,776.78	$ 5,776.78
BMC Software	BMC AppSight Named Users	$ 35.26	$ 36 31	$ 37.40	$ 38.53	$ 39.68	$ 40.87	$ 42.10	$ 42.10	$ 42.10	$ 42.10
BMC Software	BMC AppSight QA Users	$ 13.71	$ 14.12	$ 14.55	$ 14.98	$ 15.43	$ 15.90	$ 16.37	$ 16.37	$ 16.37	$ 16.37
BMC Software	CONTROL-M Enterprise Manager	$ 305.56	$ 314.72	$ 324.16	$ 333.89	$ 343.91	$ 354.22	$ 364.85	$ 364.85	$ 364.85	$ 364.85
BMC Software	CONTROL-M Full Admin User	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	CONTROL-M Tasks (100 Tasks per Unit)	$ 3,465.00	$ 3,568 95	$ 3,676.02	$ 3,786.30	$ 3,899.89	$ 4,016.88	$ 4,137.39	$ 4,137.39	$ 4,137.39	$ 4,137.39
BMC Software	Database Director (D2)	$ 36,631.86	$ 37,730 82	$ 38,862.75	$ 40,028.63	$ 41,229.49	$ 42,466.37	$ 43,740.37	$ 45,052.57	$ 46,404.15	$ 47,796.27
BMC Software	Eclipse iBuild	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iChange	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iCheck	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iCopy	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iExtract	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iLM	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iLoad	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iRecover	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iSurvey	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iUnload	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Mission Control	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Business Objects	Crystal Reports	$ 10.08	$ 10 39	$ 10.70	$ 11.02	$ 11.35	$ 11.69	$ 12.04	$ 12.04	$ 12.04	$ 12.04
Bytware Inc.	StandGuard Anti-Virus	$ 103.89	$ 107 01	$ 110.22	$ 113.52	$ 116.93	$ 120.44	$ 124.05	$ 124.05	$ 124.05	$ 124.05
Citrix	XenApp Advanced (User Counts)	$ -	$ 3 36	$ 3.46	$ 3.57	$ 3.68	$ 3.79	$ 3.90	$ 3.90	$ 3.90	$ 3.90
Citrix	XenApp Enterprise (User Counts)	$ -	$ 3.74	$ 3.85	$ 3.97	$ 4.08	$ 4.21	$ 4.33	$ 4.33	$ 4.33	$ 4.33
Computer Associates Interna ional, Inc.	CA-Explore for CICS	$ 734.41	$ 756.45	$ 779.14	$ 802.51	$ 826.59	$ 851.39	$ 876.93	$ 903.24	$ 930.33	$ 958.24

Note: The Commonwealth has established mult

Baseline Units - Volumetrics

Price per unit \ per month

Resource Description	Service Tier / Configuration (6)	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Computer Associates Interna ional, Inc.	SOA Security Manager	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates Interna ional, Inc.	SOA Security Manager Additional Secured Web Services	$ 81.48	$ 83 93	$ 86.44	$ 89.04	$ 91.71	$ 94.46	$ 97.29	$ 97.29	$ 97.29	$ 97.29
Computer Associates Interna ional, Inc.	SOA Security Manager Additional Users	$ 0.28	$ 0.29	$ 0.30	$ 0.31	$ 0.32	$ 0.32	$ 0.33	$ 0.33	$ 0.33	$ 0.33
Cor icon Technologies	Corticon Business Rules Server – Unlimited CPUs	$ 13,037.04	$ 13,428.15	$ 13,830.99	$ 14,245.92	$ 14,673.30	$ 15,113.50	$ 15,566.90	$ 15,566.90	$ 15,566.90	$ 15,566.90
Cor icon Technologies	Corticon Server – per Non-Production Server	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Cor icon Technologies	Corticon Business Rules Modeling Studio – per Named User	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
CSI International	EPIC	$ 2,078.62	$ 2,140 98	$ 2,205.21	$ 2,271.36	$ 2,339.51	$ 2,409.69	$ 2,481.98	$ 2,556.44	$ 2,633.13	$ 2,712.13
CSI International	FAQS/PCS	$ 1,263.91	$ 1,301 83	$ 1,340.89	$ 1,381.11	$ 1,422.55	$ 1,465.22	$ 1,509.18	$ 1,554.46	$ 1,601.09	$ 1,649.12
CSI International	FAQS/ASO	$ 1,549.50	$ 1,595 98	$ 1,643.86	$ 1,693.18	$ 1,743.97	$ 1,796.29	$ 1,850.18	$ 1,905.69	$ 1,962.86	$ 2,021.74
EMC Corporation	PowerPath	$ 2.87	$ 2.96	$ 3.05	$ 3.14	$ 3.23	$ 3.33	$ 3.43	$ 3.43	$ 3.43	$ 3.43
EMC Corporation	PowerPath (per CPU)	$ 2.87	$ 2.96	$ 3.05	$ 3.14	$ 3.23	$ 3.33	$ 3.43	$ 3.43	$ 3.43	$ 3.43
EMC Corporation	Symmetrix® VMAX Fully Automated Storage Tiering for Virtual Pools (FAST VP)	$ 189.70	$ 195 39	$ 201.25	$ 207.28	$ 213.50	$ 219.91	$ 226.51	$ 226.51	$ 226.51	$ 226.51
EMC Corporation	Vsphere Enterprise Plus	$ 73.33	$ 75 53	$ 77.80	$ 80.13	$ 82.54	$ 85.01	$ 87.56	$ 87.56	$ 87.56	$ 87.56
Experian QAS	NameSearch - Production (Licensed per Server up to 8 CPU)	$ 5,703.70	$ 5,874 81	$ 6,051.06	$ 6,232.59	$ 6,419.57	$ 6,612.16	$ 6,810.52	$ 6,810.52	$ 6,810.52	$ 6,810.52
Experian QAS	NameSearch - Non-Production (Licensed per Server)	$ 865.74	$ 891.71	$ 918.46	$ 946.02	$ 974.40	$ 1,003.63	$ 1,033.74	$ 1,033.74	$ 1,033.74	$ 1,033.74
Formula Consultants, Inc.	Star 1100	$ 198.00	$ 203 94	$ 210.06	$ 216.36	$ 222.85	$ 229.54	$ 236.42	$ 236.42	$ 236.42	$ 236.42
GlobalScape	CuteFTP Pro 2.0	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
HELPSYS	Robot/Schedule	$ 1,500.04	$ 1,545 05	$ 1,591.40	$ 1,639.14	$ 1,688.31	$ 1,738.96	$ 1,791.13	$ 1,844.87	$ 1,900.21	$ 1,957.22
Idea Integration	XGEN	$ 3,300.15	$ 3,399.16	$ 3,501.13	$ 3,606.17	$ 3,714.35	$ 3,825.78	$ 3,940.56	$ 3,940.56	$ 3,940.56	$ 3,940.56
Informatica Corporation	SSA-Name 3	$ 5,347.22	$ 5,507.64	$ 5,672.87	$ 5,843.05	$ 6,018.35	$ 6,198.90	$ 6,384.86	$ 6,384.86	$ 6,384.86	$ 6,384.86
Infragistics	NetAdvantage for .NET	$ 77.96	$ 80 30	$ 82.71	$ 85.19	$ 87.75	$ 90.38	$ 93.09	$ 93.09	$ 93.09	$ 93.09
KMSYS Worldwide, Inc.	IQU Plus-1	$ 488.89	$ 503 56	$ 518.66	$ 534.22	$ 550.25	$ 566.76	$ 583.76	$ 583.76	$ 583.76	$ 583.76
Levi, Ray and Shoup	VPS/PCL	$ 4,771.08	$ 4,914 21	$ 5,061.64	$ 5,213.49	$ 5,369.89	$ 5,530.99	$ 5,696.92	$ 5,867.83	$ 6,043.86	$ 6,225.18
Levi, Ray and Shoup	VPS/TCP/IP	$ 3,357.30	$ 3,458 02	$ 3,561.76	$ 3,668.61	$ 3,778.67	$ 3,892.03	$ 4,008.79	$ 4,129.06	$ 4,252.93	$ 4,380.52
Levi, Ray and Shoup	VPS/DRS	$ 1,698.67	$ 1,749.63	$ 1,802.12	$ 1,856.18	$ 1,911.87	$ 1,969.22	$ 2,028.30	$ 2,089.15	$ 2,151.83	$ 2,216.38
Levi, Ray and Shoup	VPS	$ 5,256.44	$ 5,414.13	$ 5,576.55	$ 5,743.85	$ 5,916.16	$ 6,093.65	$ 6,276.46	$ 6,464.75	$ 6,658.70	$ 6,858.46
MacKinney Systems, Inc.	CICS Response Time Monitor	$ 37.99	$ 39.13	$ 40.31	$ 41.52	$ 42.76	$ 44.04	$ 45.37	$ 46.73	$ 48.13	$ 49.57
Marble Computer, Inc.	OS DCD III Data Correlation and Documenta ion System	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	BizTalk Adaptor for MQSeries	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	BizTalk Server Enterprise (Single Processor)	$ 1,595.34	$ 1,643 20	$ 1,692.50	$ 1,743.28	$ 1,795.57	$ 1,849.44	$ 1,904.92	$ 1,904.92	$ 1,904.92	$ 1,904.92
Microsoft	BizTalk Server Standard (Single Processor)	$ 365.70	$ 376.67	$ 387.97	$ 399.61	$ 411.60	$ 423.95	$ 436.66	$ 436.66	$ 436.66	$ 436.66
Microsoft	SQL Server CAL	$ 129.32	$ 129 32	$ 129.32	$ 129.32	$ 129.32	$ 129.32	$ 129.32	$ 129.32	$ 129.32	$ 129.32
Microsoft	SQL Server Enterprise (Single Processor)	$ 495.94	$ 510 82	$ 526.15	$ 541.93	$ 558.19	$ 574.94	$ 592.18	$ 592.18	$ 592.18	$ 592.18
Microsoft	SQL Server Enterprise	$ 495.94	$ 510 82	$ 526.15	$ 541.93	$ 558.19	$ 574.94	$ 592.18	$ 592.18	$ 592.18	$ 592.18
Microsoft	SQL Server Standard (Single Processor)	$ 129.32	$ 133 20	$ 137.20	$ 141.31	$ 145.55	$ 149.92	$ 154.42	$ 154.42	$ 154.42	$ 154.42
Microsoft	SQL Server Standard	$ 129.32	$ 133 20	$ 137.20	$ 141.31	$ 145.55	$ 149.92	$ 154.42	$ 154.42	$ 154.42	$ 154.42
Microsoft	SQL Server Standard per 2-Core	$ 258.64	$ 266.40	$ 274.40	$ 282.63	$ 291.11	$ 299.84	$ 308.83	$ 308.83	$ 308.83	$ 308.83
Microsoft	Visual Studio Foundation Server	$ 14.90	$ 15 35	$ 15.81	$ 16.29	$ 16.77	$ 17.28	$ 17.80	$ 17.80	$ 17.80	$ 17.80
Microsoft	Visual Studio Foundation Server CAL	$ 17.15	$ 17.66	$ 18.19	$ 18.74	$ 19.30	$ 19.88	$ 20.47	$ 20.47	$ 20.47	$ 20.47
Microsoft	Visual Studio Professional with MSDN	$ 22.41	$ 23 08	$ 23.78	$ 24.49	$ 25.22	$ 25.98	$ 26.76	$ 26.76	$ 26.76	$ 26.76

Note: The Commonwealth has established mult

Baseline Units - Volumetrics

Price per unit \ per month

Resource Description	Service Tier / Configuration (6)	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Microsoft	Windows Server Datacenter Edition (Single Processor)	$ 70.06	$ 72.16	$ 74.32	$ 76.55	$ 78.85	$ 81.21	$ 83.65	$ 83.65	$ 83.65	$ 83.65
Microsoft	Windows Server Enterprise Edition	$ 50.09	$ 51 59	$ 53.14	$ 54.73	$ 56.38	$ 58.07	$ 59.81	$ 59.81	$ 59.81	$ 59.81
Microsoft	Windows Server Standard Edition	$ 13.21	$ 13.61	$ 14.02	$ 14.44	$ 14.87	$ 15.32	$ 15.77	$ 15.77	$ 15.77	$ 15.77
Microsoft	Windows Terminal Service Client Access Licenses	$ 3.72	$ 3.83	$ 3.95	$ 4.07	$ 4.19	$ 4.32	$ 4.44	$ 4.44	$ 4.44	$ 4.44
Network Associates	McAfee Anti-Virus	$ 0.89	$ 0.92	$ 0.95	$ 0.98	$ 1.01	$ 1.04	$ 1.07	$ 1.07	$ 1.07	$ 1.07
Novell	Platespin Migrator	$ 8.25	$ 8.50	$ 8.75	$ 9.01	$ 9.29	$ 9.56	$ 9.85	$ 9.85	$ 9.85	$ 9.85
Novell	SuSE Linux	$ 1,353.09	$ 1,393.68	$ 1,435.49	$ 1,478.55	$ 1,522.91	$ 1,568.60	$ 1,615.66	$ 1,664.13	$ 1,714.05	$ 1,765.47
OpenText	Metastorm Integration Manager for CICS (MIM for CICS)	$ 9,007.22	$ 9,277.44	$ 9,555.76	$ 9,842.43	$ 10,137.70	$ 10,441.84	$ 10,755.09	$ 11,077.74	$ 11,410.08	$ 11,752.38
Oracle	Oracle Change Management Pack	$ 134.44	$ 138.48	$ 142.63	$ 146.91	$ 151.32	$ 155.86	$ 160.53	$ 160.53	$ 160.53	$ 160.53
Oracle	Oracle Database 10g Enterprise	$ 948.55	$ 977 00	$ 1,006.31	$ 1,036.50	$ 1,067.60	$ 1,099.63	$ 1,132.62	$ 1,166.59	$ 1,201.59	$ 1,237.64
Oracle	Oracle Database Enterprise Edition	$ 532.18	$ 548.14	$ 564.59	$ 581.52	$ 598.97	$ 616.94	$ 635.45	$ 635.45	$ 635.45	$ 635.45
Oracle	Oracle Diagnostic Pack	$ 72.45	$ 74.63	$ 76.87	$ 79.17	$ 81.55	$ 83.99	$ 86.51	$ 87.10	$ 87.71	$ 88.33
Oracle	Oracle Enterprise Linux	$ 142.49	$ 146.77	$ 151.17	$ 155.70	$ 160.37	$ 165.19	$ 170.14	$ 170.14	$ 170.14	$ 170.14
Oracle	Oracle Exadata Storage Software	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Oracle	Oracle Partitioning	$ 128.84	$ 132.71	$ 136.69	$ 140.79	$ 145.01	$ 149.36	$ 153.84	$ 153.84	$ 153.84	$ 153.84
Oracle	Oracle Tuning Pack	$ 89.16	$ 90 84	$ 92.58	$ 94.36	$ 96.20	$ 98.09	$ 100.04	$ 100.04	$ 100.04	$ 100.04
Oracle	Real Application Cluster - Processor Perpetual	$ 442.17	$ 455.43	$ 469.10	$ 483.17	$ 497.66	$ 512.59	$ 527.97	$ 543.81	$ 560.12	$ 576.93
Oracle	Spatial and Graph - Processor Perpetual	$ 336.43	$ 346 52	$ 356.92	$ 367.63	$ 378.66	$ 390.02	$ 401.72	$ 413.77	$ 426.18	$ 438.97
Pitney Bowes	Finalist (Doc Sense)	$ 7,795.87	$ 8,029.75	$ 8,270.64	$ 8,518.76	$ 8,774.32	$ 9,037.55	$ 9,308.68	$ 9,587.94	$ 9,875.57	$ 10,171.84
Pitney Bowes	CODE-1 Plus	$ 733.33	$ 755 33	$ 777.99	$ 801.33	$ 825.37	$ 850.13	$ 875.64	$ 875.64	$ 875.64	$ 875.64
Pitney Bowes	CODE-1 Plus (Test / Development)	$ 336.11	$ 346.19	$ 356.58	$ 367.28	$ 378.30	$ 389.64	$ 401.33	$ 401.33	$ 401.33	$ 401.33
Pitney Bowes	Online Window for Finalist	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Quest	Central Performance Suite for SQL Server, Tier A	$ 44.11	$ 45.44	$ 46.80	$ 48.21	$ 49.65	$ 51.14	$ 52.68	$ 52.68	$ 52.68	$ 52.68
Quest	Central Performance Suite for SQL Server, Tier B	$ 44.11	$ 45.44	$ 46.80	$ 48.21	$ 49.65	$ 51.14	$ 52.68	$ 52.68	$ 52.68	$ 52.68
Quest	Foglight Database Management Suite for SQL Server	$ 44.11	$ 45.44	$ 46.80	$ 48.21	$ 49.65	$ 51.14	$ 52.68	$ 52.68	$ 52.68	$ 52.68
Quest	Foglight for SQL Server per CPU Socket	$ 22.06	$ 22.72	$ 23.40	$ 24.10	$ 24.83	$ 25.57	$ 26.34	$ 26.34	$ 26.34	$ 26.34
Quest	Foglight OS Management per CPU Socket	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Quest	Foglight Server for FSM	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
RealVNC	VNC Enterprise Edition for Windows	$ 1.18	$ 1 21	$ 1.25	$ 1.29	$ 1.32	$ 1.36	$ 1.40	$ 1.40	$ 1.40	$ 1.40
Red Hat	Red Hat Enterprise Linux	$ 319.87	$ 329.47	$ 339.35	$ 349.53	$ 360.02	$ 370.82	$ 381.94	$ 381.94	$ 381.94	$ 381.94
Schema Systems Limited	Q Editor Plus One	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Segus Inc.	OPC/Graph	$ 756.45	$ 779.14	$ 802.51	$ 826.59	$ 851.39	$ 876.93	$ 903.24	$ 930.33	$ 958.24	$ 986.99
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG20	$ 56.63	$ 58 33	$ 60.08	$ 61.88	$ 63.74	$ 65.65	$ 67.62	$ 67.62	$ 67.62	$ 67.62
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG40	$ 70.07	$ 72.18	$ 74.34	$ 76.57	$ 78.87	$ 81.24	$ 83.67	$ 83.67	$ 83.67	$ 83.67
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG60	$ 83.93	$ 86.44	$ 89.04	$ 91.71	$ 94.46	$ 97.29	$ 100.21	$ 100.21	$ 100.21	$ 100.21
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG80	$ 97.37	$ 1,203 50	$ 1,239.60	$ 1,276.79	$ 1,315.09	$ 1,354.55	$ 1,395.18	$ 1,395.18	$ 1,395.18	$ 1,395.18
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG130	$ 135.26	$ 139 32	$ 143.50	$ 147.80	$ 152.24	$ 156.80	$ 161.51	$ 161.51	$ 161.51	$ 161.51

Note: The Commonwealth has established mult

Baseline Units - Volumetrics

Price per unit \ per month

Resource Description	Service Tier / Configuration (6)	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG20	$ 56.63	$ 58 33	$ 60.08	$ 61.88	$ 63.74	$ 65.65	$ 67.62	$ 67.62	$ 67.62	$ 67.62
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG40	$ 70.07	$ 72.18	$ 74.34	$ 76.57	$ 78.87	$ 81.24	$ 83.67	$ 83.67	$ 83.67	$ 83.67
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG60	$ 83.93	$ 86.44	$ 89.04	$ 91.71	$ 94.46	$ 97.29	$ 100.21	$ 100.21	$ 100.21	$ 100.21
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG80	$ 97.37	$ 100 29	$ 103.30	$ 106.40	$ 109.59	$ 112.88	$ 116.27	$ 116.27	$ 116.27	$ 116.27
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG130	$ 135.26	$ 139 32	$ 143.50	$ 147.80	$ 152.24	$ 156.80	$ 161.51	$ 161.51	$ 161.51	$ 161.51
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG140	$ 155.63	$ 160 30	$ 165.11	$ 170.06	$ 175.16	$ 180.42	$ 185.83	$ 185.83	$ 185.83	$ 185.83
Sightline	OS 2200 Interface Agent - MAPPER, SWG20	$ 56.63	$ 58 33	$ 60.08	$ 61.88	$ 63.74	$ 65.65	$ 67.62	$ 67.62	$ 67.62	$ 67.62
Sightline	OS 2200 Interface Agent - MAPPER, SWG40	$ 70.07	$ 72.18	$ 74.34	$ 76.57	$ 78.87	$ 81.24	$ 83.67	$ 83.67	$ 83.67	$ 83.67
Sightline	OS 2200 Interface Agent - MAPPER, SWG60	$ 83.93	$ 86.44	$ 89.04	$ 91.71	$ 94.46	$ 97.29	$ 100.21	$ 100.21	$ 100.21	$ 100.21
Sightline	OS 2200 Interface Agent - MAPPER, SWG80	$ 97.37	$ 100 29	$ 103.30	$ 106.40	$ 109.59	$ 112.88	$ 116.27	$ 116.27	$ 116.27	$ 116.27
Sightline	OS 2200 Interface Agent - MAPPER, SWG130	$ 135.26	$ 139 32	$ 143.50	$ 147.80	$ 152.24	$ 156.80	$ 161.51	$ 161.51	$ 161.51	$ 161.51
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG20	$ 57.65	$ 59 38	$ 61.16	$ 62.99	$ 64.88	$ 66.83	$ 68.83	$ 68.83	$ 68.83	$ 68.83
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG40	$ 70.07	$ 72.18	$ 74.34	$ 76.57	$ 78.87	$ 81.24	$ 83.67	$ 83.67	$ 83.67	$ 83.67
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG60	$ 83.93	$ 86.44	$ 89.04	$ 91.71	$ 94.46	$ 97.29	$ 100.21	$ 100.21	$ 100.21	$ 100.21
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG80	$ 97.37	$ 100 29	$ 103.30	$ 106.40	$ 109.59	$ 112.88	$ 116.27	$ 116.27	$ 116.27	$ 116.27
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG130	$ 135.26	$ 139 32	$ 143.50	$ 147.80	$ 152.24	$ 156.80	$ 161.51	$ 161.51	$ 161.51	$ 161.51
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG140	$ 155.63	$ 160 30	$ 165.11	$ 170.06	$ 175.16	$ 180.42	$ 185.83	$ 185.83	$ 185.83	$ 185.83
Sightline	OS 2200 Interface Agent - System Log, SWG20	$ 56.63	$ 58 33	$ 60.08	$ 61.88	$ 63.74	$ 65.65	$ 67.62	$ 67.62	$ 67.62	$ 67.62
Sightline	OS 2200 Interface Agent - System Log, SWG40	$ 70.07	$ 72.18	$ 74.34	$ 76.57	$ 78.87	$ 81.24	$ 83.67	$ 83.67	$ 83.67	$ 83.67
Sightline	OS 2200 Interface Agent - System Log, SWG60	$ 83.93	$ 86.44	$ 89.04	$ 91.71	$ 94.46	$ 97.29	$ 100.21	$ 100.21	$ 100.21	$ 100.21
Sightline	OS 2200 Interface Agent - System Log, SWG80	$ 97.37	$ 100 29	$ 103.30	$ 106.40	$ 109.59	$ 112.88	$ 116.27	$ 116.27	$ 116.27	$ 116.27
Sightline	OS 2200 Interface Agent - System Log, SWG130	$ 135.26	$ 139 32	$ 143.50	$ 147.80	$ 152.24	$ 156.80	$ 161.51	$ 161.51	$ 161.51	$ 161.51
Sightline	OS 2200 Interface Agent - System Log, SWG140	$ 155.63	$ 160 30	$ 165.11	$ 170.06	$ 175.16	$ 180.42	$ 185.83	$ 185.83	$ 185.83	$ 185.83
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG20	$ 56.63	$ 58 33	$ 60.08	$ 61.88	$ 63.74	$ 65.65	$ 67.62	$ 67.62	$ 67.62	$ 67.62
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG40	$ 70.07	$ 72.18	$ 74.34	$ 76.57	$ 78.87	$ 81.24	$ 83.67	$ 83.67	$ 83.67	$ 83.67
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG60	$ 83.93	$ 86.44	$ 89.04	$ 91.71	$ 94.46	$ 97.29	$ 100.21	$ 100.21	$ 100.21	$ 100.21
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG80	$ 97.37	$ 100 29	$ 103.30	$ 106.40	$ 109.59	$ 112.88	$ 116.27	$ 116.27	$ 116.27	$ 116.27

Note: The Commonwealth has established mult

Baseline Units - Volumetrics

Price per unit \ per month

Resource Description	Service Tier / Configuration (6)	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG130	$ 135.26	$ 139 32	$ 143.50	$ 147.80	$ 152.24	$ 156.80	$ 161.51	$ 161.51	$ 161.51	$ 161.51
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG140	$ 155.63	$ 160 30	$ 165.11	$ 170.06	$ 175.16	$ 180.42	$ 185.83	$ 185.83	$ 185.83	$ 185.83
Sightline	OS 2200 Power Agent, SWG20	$ 113.26	$ 116.66	$ 120.16	$ 123.76	$ 127.47	$ 131.30	$ 135.24	$ 135.24	$ 135.24	$ 135.24
Sightline	OS 2200 Power Agent, SWG40	$ 140.15	$ 144 35	$ 148.68	$ 153.14	$ 157.74	$ 162.47	$ 167.34	$ 167.34	$ 167.34	$ 167.34
Sightline	OS 2200 Power Agent, SWG60	$ 167.85	$ 172 89	$ 178.07	$ 183.42	$ 188.92	$ 194.59	$ 200.42	$ 200.42	$ 200.42	$ 200.42
Sightline	OS 2200 Power Agent, SWG80	$ 194.74	$ 200 58	$ 206.60	$ 212.80	$ 219.18	$ 225.76	$ 232.53	$ 232.53	$ 232.53	$ 232.53
Sightline	OS 2200 Power Agent, SWG130	$ 270.52	$ 278.63	$ 286.99	$ 295.60	$ 304.47	$ 313.61	$ 323.01	$ 323.01	$ 323.01	$ 323.01
Sightline	OS 2200 Power Agent, SWG140	$ 311.26	$ 320.60	$ 330.21	$ 340.12	$ 350.33	$ 360.83	$ 371.66	$ 371.66	$ 371.66	$ 371.66
Sightline	OS 2200 Torch Capacity Manager Power Agent, SWG40	$ 574.44	$ 591.68	$ 609.43	$ 627.71	$ 646.54	$ 665.94	$ 685.92	$ 685.92	$ 685.92	$ 685.92
Sightline	OS 2200 Torch Capacity Manager Power Agent, SWG60	$ 658.78	$ 678 54	$ 698.90	$ 719.86	$ 741.46	$ 763.70	$ 786.62	$ 786.62	$ 786.62	$ 786.62
Sightline	OS 2200 Torch Capacity Manager Power Agent, SWG130	$ 1,043.37	$ 1,074.67	$ 1,106.91	$ 1,140.12	$ 1,174.32	$ 1,209.55	$ 1,245.84	$ 1,245.84	$ 1,245.84	$ 1,245.84
Sightline	OS 2200 Torch Capacity Manager Power Agent, SWG140	$ 1,197.37	$ 1,233 29	$ 1,270.29	$ 1,308.40	$ 1,347.65	$ 1,388.08	$ 1,429.72	$ 1,429.72	$ 1,429.72	$ 1,429.72
Sightline	OS 2200 Torch Interface Agent - I/O TRACE, SWG40	$ 239.56	$ 246.74	$ 254.14	$ 261.77	$ 269.62	$ 277.71	$ 286.04	$ 286.04	$ 286.04	$ 286.04
Sightline	OS 2200 Torch Interface Agent - I/O TRACE, SWG60	$ 290.89	$ 299.62	$ 308.60	$ 317.86	$ 327.40	$ 337.22	$ 347.34	$ 347.34	$ 347.34	$ 347.34
Sightline	OS 2200 Torch Interface Agent - I/O TRACE, SWG130	$ 483.19	$ 497.68	$ 512.61	$ 527.99	$ 543.83	$ 560.14	$ 576.95	$ 576.95	$ 576.95	$ 576.95
Sightline	OS 2200 Torch Interface Agent - LOG, SWG40	$ 239.56	$ 246.74	$ 254.14	$ 261.77	$ 269.62	$ 277.71	$ 286.04	$ 286.04	$ 286.04	$ 286.04
Sightline	OS 2200 Torch Interface Agent - LOG, SWG60	$ 290.89	$ 299.62	$ 308.60	$ 317.86	$ 327.40	$ 337.22	$ 347.34	$ 347.34	$ 347.34	$ 347.34
Sightline	OS 2200 Torch Interface Agent - LOG, SWG130	$ 483.19	$ 497.68	$ 512.61	$ 527.99	$ 543.83	$ 560.14	$ 576.95	$ 576.95	$ 576.95	$ 576.95
Sightline	OS 2200 Torch Interface Agent - LOG, SWG140	$ 560.19	$ 576 99	$ 594.30	$ 612.13	$ 630.49	$ 649.41	$ 668.89	$ 668.89	$ 668.89	$ 668.89
Sightline	OS 2200 Torch Interface Agent - MAPPER, SWG40	$ 239.56	$ 246.74	$ 254.14	$ 261.77	$ 269.62	$ 277.71	$ 286.04	$ 286.04	$ 286.04	$ 286.04
Sightline	OS 2200 Torch Interface Agent - MAPPER, SWG60	$ 290.89	$ 299.62	$ 308.60	$ 317.86	$ 327.40	$ 337.22	$ 347.34	$ 347.34	$ 347.34	$ 347.34
Sightline	OS 2200 Torch Interface Agent - MAPPER, SWG130	$ 483.19	$ 497.68	$ 512.61	$ 527.99	$ 543.83	$ 560.14	$ 576.95	$ 576.95	$ 576.95	$ 576.95
Sightline	Windows 2000 Interface Agent - Internet Informa ion Server	$ 24.44	$ 25.18	$ 25.93	$ 26.71	$ 27.51	$ 28.34	$ 29.19	$ 29.19	$ 29.19	$ 29.19
Sightline	Windows 2000 Interface Agent - .NET	$ 48.89	$ 50 36	$ 51.87	$ 53.42	$ 55.02	$ 56.68	$ 58.38	$ 58.38	$ 58.38	$ 58.38
Sightline	Windows 2000 Interface Agent - SQL Server	$ 81.48	$ 83 93	$ 86.44	$ 89.04	$ 91.71	$ 94.46	$ 97.29	$ 97.29	$ 97.29	$ 97.29
Sightline	Windows 2000 Power Agent Upto 32 CPU's	$ 268.89	$ 276 96	$ 285.26	$ 293.82	$ 302.64	$ 311.72	$ 321.07	$ 321.07	$ 321.07	$ 321.07
SMA	OpCon/xps EXEC LSAM, Group 3	$ 324.88	$ 333.71	$ 342.79	$ 352.16	$ 361.80	$ 371.73	$ 381.96	$ 381.96	$ 381.96	$ 381.96
SMA	OpCon/xps EXEC LSAM, Group 12	$ 1,983.73	$ 2,037.62	$ 2,093.11	$ 2,150.28	$ 2,209.16	$ 2,269.80	$ 2,332.26	$ 2,332.26	$ 2,332.26	$ 2,332.26
SMA	OpCon/xps EXEC LSAM Development, Group 2	$ 108.93	$ 111 89	$ 114.94	$ 118.07	$ 121.31	$ 124.64	$ 128.07	$ 128.07	$ 128.07	$ 128.07
SMA	OpCon/xps EXEC LSAM Development, Group 12	$ 991.82	$ 1,018.76	$ 1,046.51	$ 1,075.09	$ 1,104.52	$ 1,134.84	$ 1,166.07	$ 1,166.07	$ 1,166.07	$ 1,166.07
SMA	OpCon/xps Production SAM	$ 347.83	$ 357 28	$ 367.01	$ 377.03	$ 387.36	$ 397.99	$ 408.94	$ 408.94	$ 408.94	$ 408.94

Note: The Commonwealth has established mult

Baseline Units - Volumetrics

Price per unit \ per month

Resource Description	Service Tier / Configuration (6)	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
SMA	OpCon/xps Starter Kit	$ 595.93	$ 612.12	$ 628.79	$ 645.96	$ 663.65	$ 681.87	$ 700.63	$ 700.63	$ 700.63	$ 700.63
SMA	OpCon/xps User Interface	$ 5.49	$ 5.64	$ 5.79	$ 5.95	$ 6.11	$ 6.28	$ 6.45	$ 6.45	$ 6.45	$ 6.45
Sybase	EAServer Deploy Advanced - Active	$ 149.36	$ 153 84	$ 158.45	$ 163.20	$ 168.10	$ 173.14	$ 178.34	$ 178.34	$ 178.34	$ 178.34
Sybase	EAServer Deploy Advanced - Passive	$ 37.39	$ 38 51	$ 39.67	$ 40.86	$ 42.08	$ 43.35	$ 44.65	$ 44.65	$ 44.65	$ 44.65
Symantec	Backup Exec System Recovery Server	$ 0.97	$ 1.00	$ 1.03	$ 1.06	$ 1.09	$ 1.12	$ 1.16	$ 1.16	$ 1.16	$ 1.16
Symantec	EndPoint Protection	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	Ghost Solution Suite	$ 0.66	$ 0.68	$ 0.70	$ 0.72	$ 0.74	$ 0.76	$ 0.78	$ 0.78	$ 0.78	$ 0.78
Symantec	NetBackup Client Application and Database Pack, UNX, Tier 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Client Application and Database Pack, UNX, Tier 4	$ 175.15	$ 180.40	$ 185.81	$ 191.39	$ 197.13	$ 203.04	$ 209.13	$ 209.13	$ 209.13	$ 209.13
Symantec	NetBackup Client Application and Database Pack, WIN, Tier 2	$ 27.00	$ 27 81	$ 28.65	$ 29.50	$ 30.39	$ 31.30	$ 32.24	$ 32.24	$ 32.24	$ 32.24
Symantec	NetBackup Client Application and Database Pack, WIN, Tier 3	$ 34.97	$ 36 01	$ 37.09	$ 38.21	$ 39.35	$ 40.53	$ 41.75	$ 41.75	$ 41.75	$ 41.75
Symantec	NetBackup Client Application and Database Pack, WIN, Tier 4	$ 52.49	$ 54 06	$ 55.68	$ 57.36	$ 59.08	$ 60.85	$ 62.67	$ 62.67	$ 62.67	$ 62.67
Symantec	NetBackup Enterprise Client, UNX, Tier 4	$ 216.56	$ 223 06	$ 229.75	$ 236.64	$ 243.74	$ 251.06	$ 258.59	$ 258.59	$ 258.59	$ 258.59
Symantec	NetBackup Enterprise Client, WIN, Tier 1	$ 41.34	$ 42 58	$ 43.85	$ 45.17	$ 46.53	$ 47.92	$ 49.36	$ 49.36	$ 49.36	$ 49.36
Symantec	NetBackup Enterprise Client, WIN, Tier 2	$ 49.30	$ 50.78	$ 52.30	$ 53.87	$ 55.49	$ 57.15	$ 58.87	$ 58.87	$ 58.87	$ 58.87
Symantec	NetBackup Enterprise Client, WIN, Tier 3	$ 65.23	$ 67.19	$ 69.20	$ 71.28	$ 73.42	$ 75.62	$ 77.89	$ 77.89	$ 77.89	$ 77.89
Symantec	NetBackup Enterprise Server, WIN, Tier 2	$ 87.61	$ 90 24	$ 92.95	$ 95.74	$ 98.61	$ 101.57	$ 104.61	$ 104.61	$ 104.61	$ 104.61
Symantec	NetBackup Enterprise Server, WIN, Tier 3	$ 127.44	$ 131 26	$ 135.20	$ 139.25	$ 143.43	$ 147.73	$ 152.17	$ 152.17	$ 152.17	$ 152.17
Symantec	NetBackup Library Based Tape Drive Option, XPLAT	$ 47.79	$ 49 22	$ 50.70	$ 52.22	$ 53.79	$ 55.40	$ 57.06	$ 57.06	$ 57.06	$ 57.06
Symantec	NetBackup Media Server Encryption Option (MSEO) WIN, Tier 2	$ 95.74	$ 98.61	$ 101.57	$ 104.61	$ 104.61	$ 104.61	$ 104.61	$ 985.17	$ -	$ -
Symantec	NetBackup Platform Base, XPLAT (per Terabyte)	$ 199.12	$ 205 09	$ 211.25	$ 217.58	$ 224.11	$ 230.84	$ 237.76	$ 237.76	$ 237.76	$ 237.76
Symantec	NetBackup Shared Storage Option, XPLAT	$ 31.86	$ 32 82	$ 33.80	$ 34.81	$ 35.86	$ 36.93	$ 38.04	$ 38.04	$ 38.04	$ 38.04
Symantec	NetBackup Standard Client, XPLAT	$ 9.48	$ 9.76	$ 10.06	$ 10.36	$ 10.67	$ 10.99	$ 11.32	$ 11.32	$ 11.32	$ 11.32
Symantec	NetBackup Vault Additional Drive Option, XPLAT	$ 31.86	$ 32 82	$ 33.80	$ 34.81	$ 35.86	$ 36.93	$ 38.04	$ 38.04	$ 38.04	$ 38.04
Symantec	NetBackup Vault Base Option, XPLAT (4 tape drives per license)	$ 159.30	$ 164 08	$ 169.00	$ 174.07	$ 179.29	$ 184.67	$ 190.21	$ 190.21	$ 190.21	$ 190.21
Symantec	Veritas NetBackup Enterprise Server License, Tier 3	$ 127.44	$ 131 26	$ 135.20	$ 139.25	$ 143.43	$ 147.73	$ 152.17	$ 152.17	$ 152.17	$ 152.17
Symantec	Veritas NetBackup Windows Client, Tier 4	$ 52.49	$ 54 06	$ 55.68	$ 57.36	$ 59.08	$ 60.85	$ 62.67	$ 62.67	$ 62.67	$ 62.67
Tone Software Corp.	Dynastep	$ 1,471.15	$ 1,515 28	$ 1,560.74	$ 1,607.56	$ 1,655.79	$ 1,705.46	$ 1,756.63	$ 1,756.63	$ 1,756.63	$ 1,756.63
Unicon Group Ltd.	LOUIS II LCOM Host Module	$ 55.61	$ 57 28	$ 59.00	$ 60.77	$ 62.59	$ 64.47	$ 66.40	$ 66.40	$ 66.40	$ 66.40
Unicon Group Ltd.	LOUIS II Extract & Reporting Module	$ 893.44	$ 920 25	$ 947.86	$ 976.29	$ 1,005.58	$ 1,035.75	$ 1,066.82	$ 1,066.82	$ 1,066.82	$ 1,066.82
Unicon Group Ltd.	LOUIS II DERIVE Option	$ 62.44	$ 64 31	$ 66.24	$ 68.22	$ 70.27	$ 72.38	$ 74.55	$ 74.55	$ 74.55	$ 74.55
Unicon Group Ltd.	LOUIS II DMS Interface	$ 111.22	$ 114 56	$ 118.00	$ 121.54	$ 125.18	$ 128.94	$ 132.81	$ 132.81	$ 132.81	$ 132.81
Unicon Group Ltd.	LOUIS II RDMS Interface	$ 111.22	$ 114 56	$ 118.00	$ 121.54	$ 125.18	$ 128.94	$ 132.81	$ 132.81	$ 132.81	$ 132.81
Unicon Group Ltd.	LOUIS II RELATE Option	$ 89.12	$ 91.79	$ 94.55	$ 97.38	$ 100.31	$ 103.31	$ 106.41	$ 106.41	$ 106.41	$ 106.41
VanDyke Technologies	VShell Workgroup Server	$ 9.76	$ 10 05	$ 10.35	$ 10.66	$ 10.98	$ 11.31	$ 11.65	$ 11.65	$ 11.65	$ 11.65
Veeam	nWorks ESX Monitoring for SCOM	$ 12.89	$ 13 28	$ 13.68	$ 14.09	$ 14.51	$ 14.95	$ 15.39	$ 15.39	$ 15.39	$ 15.39
Veeam	nWorks Management Pack for VMWare	$ 154.71	$ 159 35	$ 164.13	$ 169.05	$ 174.13	$ 179.35	$ 184.73	$ 184.73	$ 184.73	$ 184.73
VMware, Inc.	VMware vSphere 4 Enterprise Plus for 1 Processor	$ 36.67	$ 37.77	$ 38.90	$ 40.07	$ 41.27	$ 42.51	$ 43.78	$ 43.78	$ 43.78	$ 43.78

Note: The Commonwealth has established mult

Baseline Units - Volumetrics

Price per unit \ per month

Resource Description	Service Tier / Configuration (6)	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
VMware, Inc.	VMware vSphere 5 Enterprise Plus for 1 Processor	$ 73.33	$ 75 53	$ 77.80	$ 80.13	$ 82.54	$ 85.01	$ 87.56	$ 87.56	$ 87.56	$ 87.56
Western American Data	Rlist	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Winternals	Winternals Administrator's Pak	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
WinZip Computing	Winzip	$ 0.26	$ 0.27	$ 0.27	$ 0.28	$ 0.29	$ 0.30	$ 0.31	$ 0.31	$ 0.31	$ 0.31
XtremeSoft	AppMetrics	$ 1,375.00	$ 1,416 25	$ 1,458.74	$ 1,502.50	$ 1,547.57	$ 1,594.00	$ 1,641.82	$ 1,641.82	$ 1,641.82	$ 1,641.82
USPS	Correct Address	$ 998.15	$ 1,028.09	$ 1,058.94	$ 1,090.70	$ 1,123.42	$ 1,157.13	$ 1,191.84	$ 1,191.84	$ 1,191.84	$ 1,191.84
IBM	FileNet	$ 66 51	$ 15.07	$ 15.52	$ 15.99	$ 16.47	$ 16.96	$ 17.47	$ 17.47	$ 17.47	$ 17.47
Microsoft	SharePoint (with SA)	$ 827 24	$ 852.06	$ 877.62	$ 903.95	$ 931.07	$ 959.00	$ 987.77	$ 987.77	$ 987.77	$ 987.77
IBM	WebSphere MQ (Procesor Value Unit)	$ 11.42	$ 2.59	$ 2.66	$ 2.74	$ 2.83	$ 2.91	$ 3.00	$ 3.00	$ 3.00	$ 3.00
Xerox	XeroxDocuShare	$ 52.08	$ 53.23	$ 54.41	$ 55.62	$ 56.88	$ 58.17	$ 59.50	$ 59.50	$ 59.50	$ 59.50
Hybrid Third Party Software											
Vendor	**Product**										
Computer Associates Interna ional, Inc.	CA 90's Services (freeware)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates Interna ional, Inc.	Vision Builder	$ 23,138.91	$ 23,833.08	$ 24,548.07	$ 25,284.51	$ 26,043.05	$ 26,824.34	$ 27,629.07	$ 28,457.94	$ 29,311.68	$ 30,191.03
Computer Associates Interna ional, Inc.	Easytrieve Plus	$ 33,157.62	$ 34,152.35	$ 35,176.92	$ 36,232.22	$ 37,319.19	$ 38,438.77	$ 39,591.93	$ 40,779.69	$ 42,003.08	$ 43,263.17
Computer Associates Interna ional, Inc.	Easytrieve Plus MVS	$ 18,620 96	$ 19,179.58	$ 19,754.97	$ 20,347.62	$ 20,958.05	$ 21,586.79	$ 22,234.39	$ 22,901.43	$ 23,588.47	$ 24,296.12
Computer Associates Interna ional, Inc.	Easytrieve Plus IMS	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates Interna ional, Inc.	Easytrieve Plus IMS Option MVS	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates Interna ional, Inc.	Easytrieve Plus DB2 OPT	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates Interna ional, Inc.	Easytrieve Plus DB2 Option MVS	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates Interna ional, Inc.	Endevor/MVS Automated Configuration Mgr MVS	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates Interna ional, Inc.	Endevor/MVS External Security Int. MVS	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates Interna ional, Inc.	Endevor/MVS MVS	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates Interna ional, Inc.	Endevor/MVS Extended Processor	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates Interna ional, Inc.	CA-Librarian	$ 27,824.48	$ 28,659.22	$ 29,518.99	$ 30,404.56	$ 31,316.70	$ 32,256.20	$ 33,223.89	$ 34,220.60	$ 35,247.22	$ 36,304.64
Computer Associates Interna ional, Inc.	CA-META COBOL	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates Interna ional, Inc.	Panvalet	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates Interna ional, Inc.	Panvalet ISPF	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates Interna ional, Inc.	SORT (INCL DART)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates Interna ional, Inc.	SRAM	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
dotJ Software Inc.	dotJ Custom Tag Library	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Formula Consultants, Inc.	Star 1100	$ 198.00	$ 203.94	$ 210.06	$ 216.36	$ 222.85	$ 229.54	$ 236.42	$ 236.42	$ 236.42	$ 236.42
Idea Integration	XGEN	$ 3,300.15	$ 3,399.16	$ 3,501.13	$ 3,606.17	$ 3,714.35	$ 3,825.78	$ 3,940.56	$ 3,940.56	$ 3,940.56	$ 3,940.56
Informatica Corporation	Change DataMove for DB2 Source	$ 16,892.13	$ 17,398.90	$ 17,920.86	$ 18,458.49	$ 19,012.24	$ 19,582.61	$ 20,170.09	$ 20,775.19	$ 21,398.45	$ 22,040.40
Informatica Corporation	DataMove for DB2 Source	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	Change DataMove	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	DataMove for IMS Source	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	Change DataMove for IMS Source	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	DataMove	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	Change DataMove DB2 Target	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	DataMove DB2 Target	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	Change DataMove/DataMove Target for UDB	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	SSA - Name 3	$ 5,347.22	$ 5,507.64	$ 5,672.87	$ 5,843.05	$ 6,018.35	$ 6,198.90	$ 6,384.86	$ 6,384.86	$ 6,384.86	$ 6,384.86
KMSYS Worldwide, Inc.	IQU Plus-1	$ 488.89	$ 503.56	$ 518.66	$ 534.22	$ 550.25	$ 566.76	$ 583.76	$ 583.76	$ 583.76	$ 583.76

Note: The Commonwealth has established mult

Baseline Units - Volumetrics

Price per unit \ per month

Resource Description	Service Tier / Configuration (6)	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
KMSYS Worldwide, Inc.	IQU Reorg Composer	$ 346.30	$ 356.69	$ 367.39	$ 378.41	$ 389.76	$ 401.45	$ 413.50	$ 413.50	$ 413.50	$ 413.50
KMSYS Worldwide, Inc.	QPLXSS	$ 0.99	$ 1.02	$ 1.05	$ 1.09	$ 1.12	$ 1.15	$ 1.19	$ 1.19	$ 1.19	$ 1.19
KMSYS Worldwide, Inc.	QPLXSV	$ 85 94	$ 88.52	$ 91.17	$ 93.91	$ 96.72	$ 99.63	$ 102.61	$ 102.61	$ 102.61	$ 102.61
KMSYS Worldwide, Inc.	QPLXV	$ 76.39	$ 78.68	$ 81.04	$ 83.47	$ 85.98	$ 88.56	$ 91.21	$ 91.21	$ 91.21	$ 91.21
Marble Computer Inc.	OS DCD III Data Correlation and Documenta ion System	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	SQL Server Enterprise	$ 105.78	$ 108.96	$ 112.23	$ 115.59	$ 119.06	$ 122.63	$ 126.31	$ 126.31	$ 126.31	$ 126.31
SAS Institute, Inc.	Base SAS	$ 70,983.91	$ 73,113.42	$ 75,306.83	$ 77,566.03	$ 79,893.01	$ 82,289.80	$ 84,758.50	$ 87,301.25	$ 89,920.29	$ 92,617.90
SAS Institute, Inc.	SAS/ACCESS Interface for IMS	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SAS Institute, Inc.	SAS/ACCESS DB2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SAS Institute, Inc.	SAS/AF	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SAS Institute, Inc.	SAS/FSP	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SAS Institute, Inc.	SAS/GRAPH	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SAS Institute, Inc.	SAS/SHARE	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SAS Institute, Inc.	SAS/STAT	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Schema Systems Limited	Q Editor Plus One	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SMA	OpCon/xps EXEC LSAM, Group 3	$ 296.54	$ 305.43	$ 314.60	$ 324.03	$ 333.76	$ 343.77	$ 354.08	$ 354.08	$ 354.08	$ 354.08
SMA	OpCon/xps EXEC LSAM, Group 8	$ 1,077.60	$ 1,109.93	$ 1,143.23	$ 1,177 52	$ 1,212.85	$ 1,249 23	$ 1,286.71	$ 1,286.71	$ 1,286.71	$ 1,286.71
SMA	OpCon/xps EXEC LSAM, Group 14	$ 2,783.45	$ 2,866.96	$ 2,952.96	$ 3,041.55	$ 3,132.80	$ 3,226.78	$ 3,323.59	$ 3,323.59	$ 3,323.59	$ 3,323.59
SMA	OpCon/xps Microsoft LSAM	$ 90.19	$ 92.89	$ 95.68	$ 98.55	$ 101.51	$ 104.55	$ 107.69	$ 107.69	$ 107.69	$ 107.69
SMA	OpCon/xps User Interface	$ 4.97	$ 5.12	$ 5.27	$ 5.43	$ 5.59	$ 5.76	$ 5.93	$ 5.93	$ 5.93	$ 5.93
Sybase	EAServer Deploy Advanced - Active	$ 149.36	$ 153.84	$ 158.45	$ 163.20	$ 168.10	$ 173.14	$ 178.34	$ 178.34	$ 178.34	$ 178.34
Sybase	EAServer Deploy Advanced - Passive	$ 37.39	$ 38.51	$ 39.67	$ 40.86	$ 42.08	$ 43.35	$ 44.65	$ 44.65	$ 44.65	$ 44.65
TRILOGexport, Inc.	TriTune Automation Component (APC)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unicon Group Ltd.	LOUIS II Database Gateway	$ 893.44	$ 920.25	$ 947.86	$ 976.29	$ 1,005.58	$ 1,035.75	$ 1,066.82	$ 1,066.82	$ 1,066.82	$ 1,066.82
Unicon Group Ltd.	LOUIS II DMS Interface	$ 111.22	$ 114.56	$ 118.00	$ 121.54	$ 125.18	$ 128.94	$ 132.81	$ 132.81	$ 132.81	$ 132.81
Unicon Group Ltd.	LOUIS II Extract & Reporting Module	$ 893.44	$ 920.25	$ 947.86	$ 976.29	$ 1,005.58	$ 1,035.75	$ 1,066.82	$ 1,066.82	$ 1,066.82	$ 1,066.82
Unicon Group Ltd.	LOUIS II LCOM Host Module	$ 55.61	$ 57.28	$ 59.00	$ 60.77	$ 62.59	$ 64.47	$ 66.40	$ 66.40	$ 66.40	$ 66.40
Unicon Group Ltd.	LOUIS II MAPPER Interface	$ -	$ 111.22	$ 114.56	$ 118.00	$ 121.54	$ 125.18	$ 128.94	$ 132.81	$ 132.81	$ 132.81
Unicon Group Ltd.	LOUIS II RDMS Interface	$ 111.22	$ 111.22	$ 114.56	$ 118.00	$ 121.54	$ 125.18	$ 128.94	$ 132.81	$ 132.81	$ 132.81
Verisign	Secure Site Pro SSL	$ 92.13	$ 97.74	$ 100.67	$ 103.69	$ 106.80	$ 110.01	$ 113.31	$ 113.31	$ 113.31	$ 113.31
Western American Data	Rlist	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
WinZip	Self-Extractor 10-user license	$ 0.66	$ 0.66	$ 0.68	$ 0.70	$ 0.72	$ 0.74	$ 0.76	$ 0.78	$ 0.78	$ 0.78
Total Third Party Software		**$ 358,990.67**	**$ 370,958.16**	**$ 382,069.25**	**$ 393,513.67**	**$ 405,298.28**	**$ 417,436.42**	**$ 429,938.72**	**$ 440,504.38**	**$ 449,486.86**	**$ 459,753.56**

Baseline Units - Volumetrics

Note: The Commonwealth has established mult

Annual Costs

Resource Description	Service Tier / Configuration (6)	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Server - Fully Managed (1)											
x86 (Windows, Linux) - Physical Servers											
	Platinum Tier										
	Windows pConfig - 1	$ 103,638 41	$ 98,760 75	$ 90,164 16	$ 85,490 12	$ 80,901 44	$ 76,397 29	$ 72,227 69	$ 68,616 30	$ 65,004 92	$ 61,393 53
	Windows pConfig - 2	$ 96,486 74	$ 91,216 72	$ 85,846 64	$ 80,710 34	$ 75,675 15	$ 70,741 63	$ 66,976 37	$ 63,036 59	$ 59,096 80	$ 55,157 01
	Windows pConfig - 3	$ 62,544 00	$ 56,745 88	$ 55,140 35	$ 49,691 60	$ 44,429 17	$ 43,292 55	$ 40,854 65	$ 40,854 65	$ 36,769 18	$ 36,769 18
	Windows pConfig - 4	$ 8,497 20	$ 8,402 69	$ 8,289 44	$ 8,188 01	$ 8,086 29	$ 7,984 28	$ 3,994 92	$ 3,994 92	$ 3,994 92	$ 3,994 92
	Windows pConfig - 5	$ 8,390 15	$ 8,292 43	$ 8,175 87	$ 8,071 03	$ 7,965 80	$ 7,860 18	$ 3,939 79	$ 3,939 79	$ 3,939 79	$ 3,939 79
	Linux pConfig - 1	$ 53,823 72	$ 47,760 54	$ 46,743 62	$ 41,590 94	$ 40,707 70	$ 35,859 02	$ 35,659 15	$ 31,697 03	$ 31,697 03	$ 31,697 03
	Linux pConfig - 2	$ 38,680 04	$ 37,485 10	$ 32,067 52	$ 31,347 27	$ 30,637 88	$ 25,661 64	$ 25,745 92	$ 25,745 92	$ 21,454 93	$ 21,454 93
	Linux pConfig - 3	$ 30,462 34	$ 29,317 91	$ 23,673 53	$ 22,918 15	$ 22,164 76	$ 21,412 68	$ 17,746 66	$ 17,746 66	$ 17,746 66	$ 17,746 66
	Linux pConfig - 4	$ 9,777 06	$ 9,481 54	$ 9,275 72	$ 9,073 34	$ 8,874 17	$ 8,677 98	$ 4,346 12	$ 4,346 12	$ 4,346 12	$ 4,346 12
	Linux pConfig - 5	$ 9,670 01	$ 9,371 27	$ 9,162 15	$ 8,956 36	$ 8,753 68	$ 8,553 88	$ 4,290 99	$ 4,290 99	$ 4,290 99	$ 4,290 99
sub-total x86 (Windows, Linux) - Physical Servers - Plantinum		**$ 421,969.69**	**$ 396,834.82**	**$ 368,539.01**	**$ 346,037.17**	**$ 328,196.05**	**$ 306,441.13**	**$ 275,782.25**	**$ 264,268.95**	**$ 248,341.33**	**$ 240,790.16**
	Gold Tier										
	Windows pConfig - 1	$ 930,100 27	$ 876,213 16	$ 822,300 58	$ 773,375 40	$ 728,965 52	$ 685,345 43	$ 644,767 83	$ 612,529 43	$ 583,873 09	$ 551,634 70
	Windows pConfig - 2	$ 868,102 10	$ 817,668 10	$ 765,917 27	$ 716,327 10	$ 671,652 52	$ 631,749 01	$ 602,278 89	$ 570,991 68	$ 543,615 36	$ 516,239 05
	Windows pConfig - 3	$ 539,966 10	$ 502,017 62	$ 462,671 29	$ 431,264 04	$ 396,694 00	$ 367,096 43	$ 365,092 18	$ 344,809 28	$ 328,582 96	$ 312,356 64
	Windows pConfig - 4	$ 75,728 25	$ 70,788 29	$ 65,748 13	$ 60,904 75	$ 60,167 12	$ 55,464 32	$ 51,558 44	$ 51,558 44	$ 47,592 41	$ 43,626 37
	Windows pConfig - 5	$ 74,764 77	$ 69,851 04	$ 64,839 56	$ 60,027 41	$ 59,263 46	$ 54,595 59	$ 50,841 72	$ 50,841 72	$ 46,930 82	$ 43,019 92
	Linux pConfig - 1	$ 463,285 20	$ 429,077 17	$ 395,968 93	$ 372,017 78	$ 344,943 53	$ 322,637 79	$ 302,245 26	$ 286,941 70	$ 275,464 03	$ 260,160 47
	Linux pConfig - 2	$ 334,034 86	$ 306,650 62	$ 286,897 60	$ 267,795 27	$ 249,327 06	$ 231,477 69	$ 220,201 63	$ 207,737 39	$ 199,427 89	$ 186,963 65
	Linux pConfig - 3	$ 263,596 88	$ 240,222 67	$ 223,804 53	$ 203,537 48	$ 188,407 80	$ 173,843 29	$ 172,017 02	$ 163,416 17	$ 154,815 32	$ 146,214 47
	Linux pConfig - 4	$ 84,472 19	$ 77,599 90	$ 71,529 52	$ 65,666 52	$ 64,291 90	$ 58,738 14	$ 54,728 44	$ 54,728 44	$ 50,518 56	$ 46,308 68
	Linux pConfig - 5	$ 83,508 71	$ 76,662 66	$ 70,620 95	$ 64,789 18	$ 63,388 24	$ 57,869 42	$ 54,011 72	$ 54,011 72	$ 49,856 97	$ 45,702 23
sub-total x86 (Windows, Linux) - Physical Servers - Gold		**$ 3,717,559.33**	**$ 3,466,751.23**	**$ 3,230,298.36**	**$ 3,015,704.93**	**$ 2,827,101.15**	**$ 2,638,817.12**	**$ 2,517,743.13**	**$ 2,397,565.97**	**$ 2,280,677.41**	**$ 2,152,226.17**
	Silver Tier										
	Windows pConfig - 1	$ 1,022,476 45	$ 961,584 26	$ 903,802 90	$ 851,033 80	$ 802,775 29	$ 751,756 88	$ 711,224 25	$ 675,663 04	$ 640,101 82	$ 672,106 92
	Windows pConfig - 2	$ 971,464 63	$ 912,886 06	$ 856,397 73	$ 802,261 77	$ 753,057 50	$ 708,648 96	$ 672,101 48	$ 641,021 64	$ 609,941 81	$ 637,136 66
	Windows pConfig - 3	$ 596,867 09	$ 553,956 62	$ 513,436 06	$ 477,013 93	$ 441,589 91	$ 407,189 43	$ 403,065 75	$ 382,912 46	$ 362,759 18	$ 382,912 46
	Windows pConfig - 4	$ 75,058 23	$ 70,218 78	$ 65,238 92	$ 60,451 24	$ 59,736 28	$ 55,082 31	$ 51,221 45	$ 51,221 45	$ 47,281 34	$ 51,221 45
	Windows pConfig - 5	$ 74,094 76	$ 69,281 53	$ 64,330 35	$ 59,573 89	$ 58,832 62	$ 54,213 58	$ 50,504 74	$ 50,504 74	$ 46,619 76	$ 50,504 74
	Linux pConfig - 1	$ 496,076 43	$ 458,925 36	$ 426,494 60	$ 398,992 93	$ 372,366 99	$ 346,590 90	$ 327,135 97	$ 312,266 15	$ 297,396 34	$ 312,266 15
	Linux pConfig - 2	$ 538,039 87	$ 498,115 16	$ 462,313 36	$ 431,858 93	$ 402,361 81	$ 373,803 07	$ 356,075 51	$ 339,890 26	$ 323,705 01	$ 339,890 26
	Linux pConfig - 3	$ 113,417 19	$ 105,112 57	$ 97,554 81	$ 90,263 34	$ 83,236 91	$ 76,474 69	$ 75,455 83	$ 71,263 84	$ 67,071 85	$ 71,263 84
	Linux pConfig - 4	$ 81,669 45	$ 75,217 58	$ 69,399 45	$ 63,769 42	$ 62,489 66	$ 57,140 15	$ 53,318 78	$ 53,318 78	$ 49,217 34	$ 53,318 78
	Linux pConfig - 5	$ 80,705 98	$ 74,280 33	$ 68,490 87	$ 62,892 08	$ 61,585 99	$ 56,271 43	$ 52,602 06	$ 52,602 06	$ 48,555 75	$ 52,602 06
sub-total x86 (Windows, Linux) - Physical Servers - Silver		**$ 4,049,870.09**	**$ 3,779,578.25**	**$ 3,527,459.04**	**$ 3,298,111.35**	**$ 3,098,032.94**	**$ 2,887,171.41**	**$ 2,752,705.82**	**$ 2,630,664.43**	**$ 2,492,650.18**	**$ 2,623,223.33**
	Bronze Tier										
	Windows pConfig - 1	$ 449,026 67	$ 423,119 74	$ 396,821 38	$ 374,767 78	$ 353,076 42	$ 331,747 24	$ 311,883 63	$ 297,707 11	$ 283,530 58	$ 269,354 05
	Windows pConfig - 2	$ 491,899 19	$ 462,827 47	$ 432,640 14	$ 407,633 78	$ 383,071 24	$ 358,959 42	$ 340,823 18	$ 325,331 21	$ 309,839 25	$ 294,347 29
	Windows pConfig - 3	$ 205,461 11	$ 192,543 45	$ 174,701 42	$ 162,522 35	$ 150,670 12	$ 139,153 48	$ 140,653 40	$ 132,616 06	$ 124,578 72	$ 120,560 05
	Windows pConfig - 4	$ 33,221 49	$ 32,920 18	$ 28,438 99	$ 28,112 69	$ 27,783 94	$ 23,530 98	$ 23,568 74	$ 23,568 74	$ 19,640 61	$ 19,640 61
	Windows pConfig - 5	$ 12,297 48	$ 12,179 67	$ 12,017 78	$ 11,872 83	$ 7,817 78	$ 7,719 56	$ 7,745 98	$ 7,745 98	$ 7,745 98	$ 7,745 98
	Linux pConfig - 1	$ 305,059 08	$ 281,571 57	$ 264,666 41	$ 244,460 18	$ 228,648 56	$ 213,325 40	$ 201,912 28	$ 190,898 88	$ 183,556 62	$ 172,543 22
	Linux pConfig - 2	$ 331,286 23	$ 305,979 26	$ 287,218 96	$ 264,881 77	$ 247,318 80	$ 230,296 43	$ 219,999 49	$ 207,999 52	$ 199,999 54	$ 187,999 57

Baseline Units - Volumetrics

Note: The Commonwealth has established mult

Resource Description	Service Tier / Configuration (6)	Annual Costs Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
	Linux pConfig - 3	$ 93,184 01	$ 85,694 70	$ 78,793 89	$ 72,151 86	$ 65,768 31	$ 59,643 36	$ 62,185 03	$ 58,039 36	$ 53,893 69	$ 53,893 69
	Linux pConfig - 4	$ 17,882 70	$ 17,458 80	$ 17,122 38	$ 12,591 80	$ 12,343 95	$ 12,098 04	$ 12,165 37	$ 12,165 37	$ 12,165 37	$ 12,165 37
	Linux pConfig - 5	$ 8,834 30	$ 8,619 13	$ 8,447 62	$ 8,277 56	$ 8,108 81	$ 7,941 26	$ 3,999 99	$ 3,999 99	$ 3,999 99	$ 3,999 99
sub-total x86 (Windows, Linux) - Physical Servers - Bronze		**$ 1,948,152.27**	**$ 1,822,913.97**	**$ 1,700,868.97**	**$ 1,587,272.61**	**$ 1,484,607.95**	**$ 1,384,415.16**	**$ 1,324,937.09**	**$ 1,260,072.22**	**$ 1,198,950.36**	**$ 1,142,249.83**
	Basic Tier										
	Windows pConfig - 1	$ 894,123 14	$ 842,879 16	$ 794,278 73	$ 746,795 50	$ 700,085 96	$ 661,261 66	$ 621,760 13	$ 593,498 31	$ 561,703 75	$ 533,441 93
	Windows pConfig - 2	$ 979,868 16	$ 922,294 62	$ 866,247 92	$ 812,527 49	$ 759,769 53	$ 715,686 01	$ 679,639 21	$ 648,746 52	$ 613,992 24	$ 583,099 55
	Windows pConfig - 3	$ 479,065 08	$ 447,720 53	$ 410,410 06	$ 380,677 20	$ 355,713 03	$ 327,536 46	$ 324,588 41	$ 308,559 35	$ 292,530 29	$ 276,501 24
	Windows pConfig - 4	$ 70,317 28	$ 65,604 54	$ 60,730 68	$ 60,041 97	$ 55,390 98	$ 50,827 74	$ 47,000 62	$ 47,000 62	$ 43,083 90	$ 43,083 90
	Windows pConfig - 5	$ 28,579 49	$ 28,316 06	$ 23,951 56	$ 23,665 85	$ 23,377 52	$ 19,238 87	$ 19,307 93	$ 19,307 93	$ 19,307 93	$ 15,446 35
	Linux pConfig - 1	$ 380,674 26	$ 352,032 80	$ 330,287 12	$ 305,423 90	$ 285,035 78	$ 268,899 65	$ 254,036 98	$ 239,520 58	$ 228,633 28	$ 217,745 98
	Linux pConfig - 2	$ 413,895 32	$ 382,972 12	$ 358,809 46	$ 331,269 97	$ 308,603 14	$ 290,552 35	$ 277,057 06	$ 261,225 23	$ 249,351 36	$ 237,477 48
	Linux pConfig - 3	$ 36,790 75	$ 35,647 41	$ 30,280 83	$ 29,366 41	$ 28,447 62	$ 23,591 87	$ 24,621 82	$ 24,621 82	$ 20,518 18	$ 20,518 18
	Linux pConfig - 4	$ 39,692 87	$ 38,793 40	$ 33,831 91	$ 33,185 94	$ 28,476 54	$ 27,919 04	$ 28,091 63	$ 24,078 54	$ 24,078 54	$ 24,078 54
	Linux pConfig - 5	$ 21,783 96	$ 21,276 23	$ 20,861 02	$ 16,359 01	$ 16,031 33	$ 15,705 53	$ 15,831 83	$ 11,873 87	$ 11,873 87	$ 11,873 87
sub-total x86 (Windows, Linux) - Physical Servers - Basic		**$ 3,344,790.31**	**$ 3,137,536.87**	**$ 2,929,689.29**	**$ 2,739,313.25**	**$ 2,560,931.43**	**$ 2,401,219.19**	**$ 2,291,935.62**	**$ 2,178,432.77**	**$ 2,065,073.36**	**$ 1,963,267.02**
Total - Fully Managed - x86 Physical - All Support Tiers (Window, Linux)		**$ 13,482,341.69**	**$ 12,603,615.14**	**$ 11,756,854.67**	**$ 10,986,439.30**	**$ 10,298,869.52**	**$ 9,618,064.00**	**$ 9,163,103.91**	**$ 8,731,004.34**	**$ 8,285,692.64**	**$ 8,121,756.51**
x86 (Windows, Linux) - Virtual Servers											
	Platinum Tier										
	Windows vConfig - 1	$ 31,083 09	$ 30,146 68	$ 31,313 76	$ 31,467 01	$ 32,548 76	$ 33,432 80	$ 34,141 22	$ 35,039 67	$ 36,836 57	$ 38,633 48
	Windows vConfig - 2	$ 33,260 83	$ 32,995 26	$ 33,601 18	$ 35,527 61	$ 36,066 79	$ 36,130 07	$ 37,661 83	$ 38,876 73	$ 41,306 53	$ 43,736 32
	Windows vConfig - 3	$ 38,426 13	$ 40,061 97	$ 39,531 19	$ 41,636 38	$ 43,666 45	$ 44,627 16	$ 46,470 47	$ 48,916 28	$ 51,362 09	$ 53,807 91
	Windows vConfig - 4	$ 4,338 37	$ 4,125 40	$ 4,034 32	$ 3,947 49	$ 5,157 52	$ 4,984 72	$ 4,864 74	$ 4,864 74	$ 4,864 74	$ 6,080 92
	Windows vConfig - 5	$ 2,892 25	$ 2,750 27	$ 2,689 55	$ 2,631 66	$ 2,578 76	$ 3,738 54	$ 3,648 55	$ 3,648 55	$ 3,648 55	$ 3,648 55
	Linux vConfig - 1	$ 24,752 16	$ 24,553 43	$ 23,732 24	$ 24,555 84	$ 25,374 91	$ 24,284 55	$ 24,854 99	$ 26,408 43	$ 27,961 87	$ 29,515 30
	Linux vConfig - 2	$ 23,986 93	$ 24,463 86	$ 23,754 31	$ 25,037 78	$ 24,269 33	$ 25,169 89	$ 24,308 46	$ 26,178 35	$ 28,048 23	$ 29,918 11
	Linux vConfig - 3	$ 22,183 76	$ 21,119 90	$ 24,155 94	$ 23,610 43	$ 23,120 71	$ 25,356 54	$ 24,806 38	$ 24,806 38	$ 27,907 18	$ 27,907 18
	Linux vConfig - 4	$ 4,797 39	$ 4,449 31	$ 4,321 70	$ 4,177 43	$ 4,046 84	$ 5,811 49	$ 5,616 30	$ 5,616 30	$ 5,616 30	$ 5,616 30
	Linux vConfig - 5	$ 2,398 69	$ 2,224 66	$ 2,160 85	$ 2,088 72	$ 2,023 42	$ 1,937 16	$ 1,872 10	$ 1,872 10	$ 1,872 10	$ 3,744 20
sub-total x86 (Windows, Linux) - Virtual Servers - Platinum		**$ 188,119.60**	**$ 186,890.73**	**$ 189,295.04**	**$ 194,680.35**	**$ 198,853.49**	**$ 205,472.92**	**$ 208,245.04**	**$ 216,227.53**	**$ 229,424.16**	**$ 242,608.28**
	Gold Tier										
	Windows vConfig - 1	$ 260,746 56	$ 257,383 77	$ 263,347 89	$ 269,253 13	$ 276,578 93	$ 281,379 56	$ 286,626 29	$ 300,650 82	$ 315,551 88	$ 332,206 00
	Windows vConfig - 2	$ 286,547 78	$ 286,902 77	$ 295,405 78	$ 303,800 87	$ 312,982 26	$ 317,702 56	$ 325,682 95	$ 342,384 64	$ 359,086 33	$ 376,981 00
	Windows vConfig - 3	$ 329,796 10	$ 337,492 82	$ 351,577 81	$ 362,895 62	$ 376,295 98	$ 383,035 42	$ 395,094 71	$ 416,909 76	$ 436,300 91	$ 458,115 95
	Windows vConfig - 4	$ 33,711 50	$ 33,524 96	$ 34,154 66	$ 36,044 01	$ 36,635 85	$ 37,889 68	$ 38,216 47	$ 40,605 00	$ 41,799 26	$ 44,187 79
	Windows vConfig - 5	$ 22,474 34	$ 22,796 97	$ 23,645 54	$ 24,458 43	$ 24,002 80	$ 24,444 96	$ 25,079 56	$ 27,468 09	$ 28,662 35	$ 29,856 61
	Linux vConfig - 1	$ 201,641 13	$ 195,546 27	$ 200,031 87	$ 202,960 33	$ 206,125 42	$ 208,797 43	$ 211,364 49	$ 221,568 30	$ 233,229 79	$ 244,891 28
	Linux vConfig - 2	$ 187,260 11	$ 183,852 62	$ 189,397 42	$ 191,705 26	$ 196,138 73	$ 197,661 64	$ 202,250 94	$ 212,895 72	$ 223,540 51	$ 234,185 29
	Linux vConfig - 3	$ 189,089 68	$ 191,620 05	$ 198,373 90	$ 204,284 56	$ 210,195 13	$ 211,389 96	$ 216,363 39	$ 228,383 58	$ 240,403 77	$ 252,423 96
	Linux vConfig - 4	$ 28,639 78	$ 28,930 01	$ 28,227 28	$ 29,376 15	$ 30,483 77	$ 31,130 71	$ 30,197 92	$ 31,974 27	$ 33,750 62	$ 35,526 97
	Linux vConfig - 5	$ 19,827 54	$ 18,597 86	$ 20,162 34	$ 19,584 10	$ 20,957 59	$ 20,143 40	$ 21,316 18	$ 23,092 53	$ 23,092 53	$ 24,868 88
sub-total x86 (Windows, Linux) - Virtual Servers - Gold		**$ 1,559,734.52**	**$ 1,556,648.12**	**$ 1,604,324.50**	**$ 1,644,362.47**	**$ 1,690,396.45**	**$ 1,713,575.32**	**$ 1,752,192.90**	**$ 1,845,932.69**	**$ 1,935,417.94**	**$ 2,033,243.73**
	Silver Tier										
	Windows vConfig - 1	$ 280,543 63	$ 278,691 41	$ 285,183 25	$ 292,528 40	$ 300,303 78	$ 306,282 96	$ 312,517 73	$ 327,929 56	$ 344,197 60	$ 361,321 86
	Windows vConfig - 2	$ 317,242 12	$ 319,568 59	$ 328,841 46	$ 339,250 72	$ 349,128 75	$ 355,151 25	$ 364,696 57	$ 382,286 44	$ 402,221 62	$ 422,156 80

Baseline Units - Volumetrics

Note: The Commonwealth has established mult

Resource Description	Service Tier / Configuration (6)	Annual Costs Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
	Windows vConfig - 3	$ 362,579 22	$ 372,615 51	$ 386,385 37	$ 399,971 80	$ 415,562 46	$ 423,386 83	$ 437,450 45	$ 459,082 61	$ 483,118 35	$ 507,154 09
	Windows vConfig - 4	$ 32,818 15	$ 32,750 97	$ 33,416 85	$ 35,312 18	$ 35,940 43	$ 37,204 66	$ 37,566 23	$ 39,914 11	$ 41,088 06	$ 43,435 95
	Windows vConfig - 5	$ 21,878 77	$ 22,270 66	$ 23,134 74	$ 23,961 84	$ 23,547 18	$ 24,003 00	$ 24,652 84	$ 27,000 72	$ 28,174 67	$ 29,348 61
	Linux vConfig - 1	$ 205,360 81	$ 201,798 04	$ 206,173 36	$ 210,623 50	$ 215,233 45	$ 217,739 18	$ 221,489 70	$ 232,495 40	$ 243,501 10	$ 255,882 52
	Linux vConfig - 2	$ 200,640 56	$ 199,493 86	$ 204,751 31	$ 208,798 06	$ 214,793 18	$ 217,538 43	$ 221,672 61	$ 233,517 71	$ 245,362 81	$ 257,207 91
	Linux vConfig - 3	$ 200,757 20	$ 203,668 24	$ 210,355 93	$ 216,260 25	$ 225,241 49	$ 228,977 19	$ 233,845 87	$ 245,538 17	$ 260,153 53	$ 271,845 83
	Linux vConfig - 4	$ 26,615 58	$ 27,125 04	$ 26,560 99	$ 27,750 07	$ 28,895 37	$ 29,602 53	$ 28,804 37	$ 30,498 75	$ 32,193 12	$ 33,887 49
	Linux vConfig - 5	$ 18,426 17	$ 17,437 53	$ 18,972 14	$ 18,500 05	$ 19,865 57	$ 19,154 58	$ 20,332 50	$ 22,026 87	$ 22,026 87	$ 23,721 25
sub-total x86 (Windows, Linux) - Virtual Servers - Silver		**$ 1,666,862.20**	**$ 1,675,419.85**	**$ 1,723,775.40**	**$ 1,772,956.86**	**$ 1,828,511.66**	**$ 1,859,040.62**	**$ 1,903,028.86**	**$ 2,000,290.34**	**$ 2,102,037.74**	**$ 2,205,962.31**
	Bronze Tier										
	Windows vConfig - 1	$ 92,291 72	$ 92,162 02	$ 93,734 34	$ 96,222 34	$ 99,453 81	$ 101,179 15	$ 103,285 10	$ 108,364 69	$ 113,444 29	$ 119,370 48
	Windows vConfig - 2	$ 122,868 86	$ 124,347 15	$ 127,126 95	$ 131,134 16	$ 136,170 72	$ 137,971 51	$ 141,891 37	$ 148,869 63	$ 155,847 90	$ 163,989 20
	Windows vConfig - 3	$ 116,547 55	$ 119,198 81	$ 125,569 12	$ 129,301 97	$ 132,885 76	$ 135,678 59	$ 141,243 65	$ 148,425 53	$ 155,607 41	$ 162,789 29
	Windows vConfig - 4	$ 1,350 21	$ 1,295 61	$ 1,272 00	$ 1,248 89	$ 1,228 04	$ 1,189 72	$ 1,164 33	$ 1,164 33	$ 1,164 33	$ 2,328 66
	Windows vConfig - 5	$ 1,350 21	$ 1,295 61	$ 1,272 00	$ 1,248 89	$ 1,228 04	$ 1,189 72	$ 1,164 33	$ 1,164 33	$ 1,164 33	$ 2,328 66
	Linux vConfig - 1	$ 62,503 32	$ 61,826 63	$ 63,418 90	$ 64,575 76	$ 65,793 42	$ 66,389 12	$ 68,288 75	$ 70,966 74	$ 74,983 72	$ 79,000 71
	Linux vConfig - 2	$ 75,271 80	$ 75,237 10	$ 77,443 80	$ 79,205 47	$ 81,009 44	$ 81,613 54	$ 84,427 43	$ 87,738 31	$ 92,704 63	$ 97,670 95
	Linux vConfig - 3	$ 59,029 88	$ 60,361 54	$ 62,705 31	$ 64,817 77	$ 66,914 98	$ 67,475 20	$ 69,272 54	$ 72,158 90	$ 77,931 61	$ 80,817 97
	Linux vConfig - 4	$ 1,980 84	$ 1,881 60	$ 1,845 27	$ 1,802 36	$ 1,762 05	$ 1,701 30	$ 1,657 66	$ 1,657 66	$ 1,657 66	$ 3,315 31
	Linux vConfig - 5	$ 1,980 84	$ 1,881 60	$ 1,845 27	$ 1,802 36	$ 1,762 05	$ 1,701 30	$ 1,657 66	$ 1,657 66	$ 1,657 66	$ 3,315 31
sub-total x86 (Windows, Linux) - Virtual Servers - Bronze		**$ 535,175.22**	**$ 539,487.67**	**$ 556,232.95**	**$ 571,359.97**	**$ 588,208.31**	**$ 596,089.16**	**$ 614,052.82**	**$ 642,167.78**	**$ 676,163.54**	**$ 714,926.56**
	Basic Tier										
	Windows vConfig - 1	$ 180,605 22	$ 179,785 15	$ 184,927 62	$ 189,974 65	$ 194,729 46	$ 199,166 59	$ 203,469 71	$ 213,517 59	$ 223,565 48	$ 235,288 01
	Windows vConfig - 2	$ 241,423 48	$ 243,484 90	$ 251,712 85	$ 259,798 28	$ 267,501 73	$ 272,434 13	$ 280,365 80	$ 294,211 03	$ 308,056 25	$ 324,209 01
	Windows vConfig - 3	$ 236,918 89	$ 244,862 03	$ 252,443 04	$ 262,451 35	$ 272,111 10	$ 277,470 95	$ 288,546 87	$ 302,854 97	$ 317,163 08	$ 333,855 88
	Windows vConfig - 4	$ 1,333 83	$ 1,281 83	$ 1,259 29	$ 1,237 13	$ 1,217 20	$ 1,179 68	$ 1,155 06	$ 1,155 06	$ 1,155 06	$ 2,310 11
	Windows vConfig - 5	$ 1,333 83	$ 1,281 83	$ 1,259 29	$ 1,237 13	$ 1,217 20	$ 1,179 68	$ 1,155 06	$ 1,155 06	$ 1,155 06	$ 2,310 11
	Linux vConfig - 1	$ 126,757 39	$ 125,537 79	$ 128,678 15	$ 132,402 09	$ 134,794 53	$ 137,281 80	$ 139,607 39	$ 147,435 84	$ 153,959 55	$ 161,788 00
	Linux vConfig - 2	$ 153,638 39	$ 153,699 78	$ 158,063 64	$ 163,323 99	$ 166,880 48	$ 169,633 70	$ 173,466 98	$ 183,194 10	$ 191,300 04	$ 201,027 16
	Linux vConfig - 3	$ 128,763 22	$ 131,281 70	$ 135,851 90	$ 139,959 96	$ 147,045 69	$ 147,721 39	$ 154,013 55	$ 159,717 76	$ 168,274 07	$ 176,830 38
	Linux vConfig - 4	$ 1,920 48	$ 1,830 43	$ 1,797 55	$ 1,758 41	$ 1,721 39	$ 1,664 09	$ 1,623 40	$ 1,623 40	$ 1,623 40	$ 3,246 81
	Linux vConfig - 5	$ 1,920 48	$ 1,830 43	$ 1,797 55	$ 1,758 41	$ 1,721 39	$ 1,664 09	$ 1,623 40	$ 1,623 40	$ 1,623 40	$ 3,246 81
sub-total x86 (Windows, Linux) - Virtual Servers - Basic		**$ 1,074,615.21**	**$ 1,084,875.88**	**$ 1,117,790.88**	**$ 1,153,901.40**	**$ 1,188,940.16**	**$ 1,209,396.11**	**$ 1,245,027.22**	**$ 1,306,488.22**	**$ 1,367,875.39**	**$ 1,444,112.28**
Total - Fully Managed - x86 Virtual - All Support Tiers (Window, Linux)		**$ 5,024,506.75**	**$ 5,043,322.25**	**$ 5,191,418.76**	**$ 5,337,261.04**	**$ 5,494,910.06**	**$ 5,583,574.13**	**$ 5,722,546.83**	**$ 6,011,106.56**	**$ 6,310,918.77**	**$ 6,640,853.16**
UNIX (IBM P-Series, AIX)											
	Platinum Tier										
	AIX Config - 1	$ 288,523 93	$ 301,403 52	$ 313,948 80	$ 326,162 27	$ 338,080 62	$ 350,111 52	$ 361,845 63	$ 380,758 38	$ 391,886 46	$ 410,003 12
	AIX Config - 2	$ 219,142 23	$ 225,323 58	$ 239,604 59	$ 245,374 11	$ 259,122 39	$ 264,477 98	$ 277,593 92	$ 290,382 08	$ 295,130 88	$ 307,340 46
	AIX Config - 3	$ 162,887 31	$ 170,155 92	$ 177,238 48	$ 184,133 75	$ 191,122 94	$ 197,892 87	$ 204,492 73	$ 210,930 79	$ 225,623 71	$ 231,643 88
	AIX Config - 4	$ 42,142 74	$ 41,726 59	$ 49,573 36	$ 49,074 82	$ 48,585 45	$ 48,086 91	$ 55,518 78	$ 54,937 15	$ 54,366 21	$ 61,468 09
	AIX Config - 5	$ 42,142 74	$ 41,726 59	$ 49,573 36	$ 49,074 82	$ 48,585 45	$ 48,086 91	$ 55,518 78	$ 54,937 15	$ 54,366 21	$ 61,468 09
sub-total P-Series (AIX) - Bronze		**$ 754,838.94**	**$ 780,336.20**	**$ 829,938.61**	**$ 853,819.77**	**$ 885,496.85**	**$ 908,656.18**	**$ 954,969.84**	**$ 991,945.54**	**$ 1,021,373.48**	**$ 1,071,923.65**
	Gold Tier										
	AIX Config - 1	$ 238,267 78	$ 249,136 80	$ 259,759 33	$ 270,138 69	$ 280,294 08	$ 290,177 68	$ 299,799 51	$ 315,365 85	$ 324,474 48	$ 339,358 94
	AIX Config - 2	$ 182,842 51	$ 187,909 09	$ 199,720 86	$ 204,423 54	$ 215,775 26	$ 220,115 56	$ 231,267 47	$ 242,174 43	$ 246,407 04	$ 256,874 78

Note: The Commonwealth has established mult

Baseline Units - Volumetrics

Resource Description	Service Tier / Configuration (6)	Annual Costs Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
	AIX Config - 3	$ 137,756 73	$ 144,022 56	$ 150,146 53	$ 156,119 04	$ 162,000 40	$ 167,686 27	$ 173,222 91	$ 178,615 11	$ 191,000 39	$ 196,030 00
	AIX Config - 4	$ 35,162 02	$ 34,797 98	$ 41,321 56	$ 40,884 71	$ 40,457 86	$ 40,021 01	$ 46,253 49	$ 45,816 78	$ 45,390 77	$ 51,374 96
	AIX Config - 5	$ 35,162 02	$ 34,797 98	$ 41,321 56	$ 40,884 71	$ 40,457 86	$ 40,021 01	$ 46,253 49	$ 45,816 78	$ 45,390 77	$ 51,374 96
sub-total P-Series (AIX) - Gold		**$ 629,191.06**	**$ 650,664.40**	**$ 692,269.83**	**$ 712,450.69**	**$ 738,985.47**	**$ 758,021.53**	**$ 796,796.88**	**$ 827,788.95**	**$ 852,663.45**	**$ 895,013.63**
	Silver Tier										
	AIX Config - 1	$ 390,909 52	$ 408,682 56	$ 420,720 40	$ 437,709 50	$ 459,577 87	$ 475,699 65	$ 491,393 48	$ 511,745 31	$ 531,651 81	$ 555,948 43
	AIX Config - 2	$ 303,851 22	$ 317,942 15	$ 325,947 60	$ 339,351 16	$ 353,141 13	$ 366,518 43	$ 385,084 29	$ 397,784 22	$ 415,686 20	$ 433,059 76
	AIX Config - 3	$ 227,118 09	$ 237,351 84	$ 247,342 99	$ 257,078 20	$ 266,672 79	$ 275,911 68	$ 284,893 24	$ 299,506 68	$ 308,059 65	$ 321,991 63
	AIX Config - 4	$ 58,432 93	$ 63,588 43	$ 62,902 17	$ 67,870 23	$ 67,264 98	$ 72,193 02	$ 71,515 65	$ 76,287 39	$ 80,977 83	$ 85,542 67
	AIX Config - 5	$ 58,432 93	$ 63,588 43	$ 62,902 17	$ 67,870 23	$ 67,264 98	$ 72,193 02	$ 71,515 65	$ 76,287 39	$ 80,977 83	$ 85,542 67
sub-total P-Series (AIX) - Silver		**$ 1,038,744.68**	**$ 1,091,153.41**	**$ 1,119,815.33**	**$ 1,169,879.32**	**$ 1,213,921.74**	**$ 1,262,515.81**	**$ 1,304,402.32**	**$ 1,361,610.99**	**$ 1,417,353.33**	**$ 1,482,085.16**
	Bronze Tier										
	AIX Config - 1	$ 101,761 16	$ 104,964 32	$ 108,082 71	$ 115,233 50	$ 118,164 32	$ 125,025 68	$ 127,729 31	$ 134,297 49	$ 136,820 08	$ 143,103 77
	AIX Config - 2	$ 111,697 01	$ 115,305 47	$ 118,833 90	$ 126,803 92	$ 130,168 12	$ 137,853 02	$ 140,961 55	$ 148,349 66	$ 151,307 43	$ 158,411 25
	AIX Config - 3	$ 42,198 32	$ 41,778 69	$ 46,532 08	$ 46,060 64	$ 50,679 66	$ 50,157 22	$ 54,595 20	$ 54,021 28	$ 58,332 88	$ 57,705 12
	AIX Config - 4	$ 9,308 08	$ 9,224 44	$ 9,141 07	$ 9,057 42	$ 8,977 11	$ 13,340 61	$ 13,215 15	$ 13,089 68	$ 12,969 21	$ 12,844 16
	AIX Config - 5	$ 9,308 08	$ 9,224 44	$ 9,141 07	$ 9,057 42	$ 8,977 11	$ 13,340 61	$ 13,215 15	$ 13,089 68	$ 12,969 21	$ 12,844 16
sub-total P-Series (AIX) - Bronze		**$ 274,272.66**	**$ 280,497.36**	**$ 291,730.84**	**$ 306,212.91**	**$ 316,966.32**	**$ 339,717.15**	**$ 349,716.35**	**$ 362,847.78**	**$ 372,398.82**	**$ 384,908.46**
	Basic Tier										
	AIX Config - 1	$ 195,259 96	$ 202,313 48	$ 212,182 08	$ 218,834 05	$ 228,289 41	$ 237,444 38	$ 246,338 40	$ 254,988 57	$ 266,257 20	$ 274,379 85
	AIX Config - 2	$ 221,746 66	$ 230,037 09	$ 241,541 10	$ 249,423 31	$ 260,575 50	$ 271,363 38	$ 281,888 08	$ 292,172 97	$ 305,580 00	$ 315,337 72
	AIX Config - 3	$ 130,737 25	$ 137,479 25	$ 140,058 95	$ 146,509 72	$ 152,884 76	$ 159,004 56	$ 164,950 53	$ 170,737 48	$ 176,467 88	$ 185,630 21
	AIX Config - 4	$ 34,647 92	$ 37,767 28	$ 37,421 86	$ 40,447 02	$ 40,088 54	$ 43,021 02	$ 42,610 99	$ 45,449 13	$ 48,249 47	$ 50,963 67
	AIX Config - 5	$ 34,647 92	$ 37,767 28	$ 37,421 86	$ 40,447 02	$ 40,088 54	$ 43,021 02	$ 42,610 99	$ 45,449 13	$ 48,249 47	$ 50,963 67
sub-total P-Series (AIX) - Basic		**$ 617,039.70**	**$ 645,364.40**	**$ 668,625.85**	**$ 695,661.12**	**$ 721,926.76**	**$ 753,854.36**	**$ 778,399.00**	**$ 808,797.28**	**$ 844,804.03**	**$ 877,275.13**
Total - Fully Managed - P-Series (AIX) - All Support Tiers (Window, Linux)		**$ 3,314,087.04**	**$ 3,448,015.77**	**$ 3,602,380.46**	**$ 3,738,023.80**	**$ 3,877,297.14**	**$ 4,022,765.03**	**$ 4,184,284.40**	**$ 4,352,990.54**	**$ 4,508,593.11**	**$ 4,711,206.03**
Server - Managed Only (2)											
x86 (Windows, Linux)											
	Platinum Tier	$ 172,156 56	$ 93,037 82	$ 53,623 81	$ 31,247 33	$ 67,955 95	$ 64,626 60	$ 61,759 27	$ 61,759 27	$ 61,759 27	$ 61,759 27
	Gold Tier	$ 1,373,339 83	$ 751,897 52	$ 435,758 51	$ 250,265 30	$ 62,046 73	$ 59,329 34	$ 56,971 73	$ 56,971 73	$ 56,971 73	$ 56,971 73
	Silver Tier	$ 1,370,225 68	$ 758,085 97	$ 441,328 68	$ 255,230 28	$ 57,083 00	$ 54,834 69	$ 52,873 05	$ 52,873 05	$ 52,873 05	$ 52,873 05
	Bronze Tier	$ 977,782 40	$ 543,406 76	$ 316,971 24	$ 183,704 05	$ 54,887 50	$ 52,833 42	$ 51,037 18	$ 51,037 18	$ 51,037 18	$ 51,037 18
	Basic Tier	$ 1,305,520 58	$ 728,533 47	$ 425,720 72	$ 247,435 24	$ 52,854 63	$ 50,973 09	$ 49,324 52	$ 49,324 52	$ 49,324 52	$ 49,324 52
Total Managed Only- x86 - All Support Tiers (Window, Linux)		**$ 5,199,025.06**	**$ 2,874,961.54**	**$ 1,673,402.96**	**$ 967,882.19**	**$ 294,827.80**	**$ 282,597.14**	**$ 271,965.75**	**$ 271,965.75**	**$ 271,965.75**	**$ 271,965.75**
UNIX (IBM P-Series, AIX)											
	Platinum	$ 28,787 12	$ 17,098 03	$ 11,282 53	$ 55,833 22	$ 55,252 42	$ 54,671 62	$ 54,092 21	$ 53,511 41	$ 52,930 61	$ 52,351 20
	Gold Tier	$ 77,132 46	$ 45,861 80	$ 25,246 74	$ 50,029 39	$ 49,565 31	$ 49,099 83	$ 48,635 75	$ 48,171 66	$ 47,707 58	$ 47,243 49
	Silver Tier	$ 136,507 45	$ 81,069 12	$ 49,030 22	$ 44,108 84	$ 43,644 76	$ 43,180 67	$ 42,716 59	$ 42,252 51	$ 41,787 03	$ 41,322 95
	Bronze Tier	$ 153,686 91	$ 91,375 12	$ 52,815 84	$ 37,376 84	$ 37,028 08	$ 36,680 72	$ 36,331 96	$ 35,983 20	$ 35,635 83	$ 35,287 07
	Basic Tier	$ 74,172 88	$ 44,086 05	$ 26,686 23	$ 24,028 17	$ 23,796 13	$ 23,564 08	$ 23,332 04	$ 23,098 61	$ 22,866 57	$ 22,634 53
Total Managed Only- P-Series - All Support Tiers (AIX)		**$ 470,286.82**	**$ 279,490.13**	**$ 165,061.55**	**$ 211,376.46**	**$ 209,286.69**	**$ 207,196.93**	**$ 205,108.55**	**$ 203,017.39**	**$ 200,927.62**	**$ 198,839.24**
Storage and Backup - Fully Managed (1)											

Note: The Commonwealth has established mult

Baseline Units - Volumetrics

Resource Description	Service Tier / Configuration (6)	Annual Costs Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Enterprise Storage											
	* Dedicated - Config 1 - SAN Raid 5	$ 1,562,534 63	$ 1,639,821 86	$ 1,714,140 32	$ 1,793,457 16	$ 1,878,034 18	$ 1,978,486 65	$ 2,035,170 81	$ 2,035,221 38	$ 2,035,266 99	$ 2,035,308 05
	* Dedicated - Config 2 - SAN Raid 10	$ 1,154,680 43	$ 1,256,547 20	$ 1,367,724 99	$ 1,488,735 98	$ 1,620,363 03	$ 1,762,471 03	$ 1,918,571 06	$ 1,918,579 86	$ 1,918,587 79	$ 1,918,594 93
	Dedicated - Config 3 - Net Attached	$ 8,450 84	$ 8,523 50	$ 8,573 65	$ 8,635 59	$ 8,710 12	$ 6,748 41	$ 6,863 52	$ 6,863 73	$ 6,863 93	$ 6,864 11
Total Enterprise Storage - Fully Managed		**$ 2,725,665.90**	**$ 2,904,892.56**	**$ 3,090,438.96**	**$ 3,290,828.74**	**$ 3,507,107.33**	**$ 3,747,706.09**	**$ 3,960,605.39**	**$ 3,960,664.97**	**$ 3,960,718.72**	**$ 3,960,767.08**
Tape and Backup											
	** Server Tape Stored	$ 2,359,875 98	$ 1,843,848 25	$ 1,850,919 93	$ 1,895,679 66	$ 1,935,907 88	$ 1,955,897 88	$ 2,049,647 37	$ 2,049,706 72	$ 2,049,760 28	$ 2,049,808 46
	** Offsite Tape Storage	$ 14,421 81	$ 15,668 75	$ 17,120 44	$ 18,703 83	$ 20,435 00	$ 21,892 84	$ 24,385 06	$ 24,385 17	$ 24,385 27	$ 24,385 36
Total Tape and Backup - Fully Managed		**$ 2,374,297.79**	**$ 1,859,517.00**	**$ 1,868,040.37**	**$ 1,914,383.49**	**$ 1,956,342.88**	**$ 1,977,790.72**	**$ 2,074,032.43**	**$ 2,074,091.90**	**$ 2,074,145.55**	**$ 2,074,193.82**
Limited Co-Lo (Data Center Only Charge) (3)											
Server, Storage, Network, Security Equipment											
	Co-Lo Config - 1	$ 11,963 60	$ 12,055 76	$ 12,150 68	$ 12,248 46	$ 12,743 79	$ 12,847 52	$ 12,954 36	$ 12,954 36	$ 12,954 36	$ 12,954 36
	Co-Lo Config - 2	$ 18,157 05	$ 18,341 37	$ 18,531 22	$ 18,726 77	$ 19,322 81	$ 19,530 26	$ 19,743 94	$ 19,743 94	$ 19,743 94	$ 19,743 94
	Co-Lo Config - 3	$ 130,057 48	$ 131,532 04	$ 133,050 83	$ 134,615 19	$ 69,383 80	$ 70,120 81	$ 70,879 69	$ 70,879 69	$ 70,879 69	$ 70,879 69
Total Limited Co-Lo (Data Center Only Charge)		**$ 160,178.13**	**$ 161,929.17**	**$ 163,732.74**	**$ 165,590.42**	**$ 101,450.41**	**$ 102,498.59**	**$ 103,577.99**	**$ 103,577.99**	**$ 103,577.99**	**$ 103,577.99**
Mainframe Services (4)											
IBM Services											
	*** IBM Mainframe Allocated DASD	$ 1,502,021 05	$ 1,426,989 47	$ 1,355,709 47	$ 1,287,903 16	$ 1,223,570 53	$ 1,162,433 68	$ 1,104,353 68	$ 1,104,353 68	$ 1,104,353 68	$ 1,104,353 68
	IBM Tapes in Storage - VTS	$ 346,256 84	$ 340,837 89	$ 334,446 32	$ 331,111 58	$ 320,412 63	$ 316,105 26	$ 308,463 16	$ 303,322 11	$ 297,625 26	$ 292,206 32
	IBM Offsite Tape Storage	$ 2,884 36	$ 2,848 86	$ 2,829 82	$ 2,810 49	$ 2,791 29	$ 2,718 59	$ 2,752 89	$ 2,502 58	$ 2,275 17	$ 2,068 31
Total IBM Services		**$ 1,851,162.26**	**$ 1,770,676.23**	**$ 1,692,985.61**	**$ 1,621,825.23**	**$ 1,546,774.44**	**$ 1,481,257.54**	**$ 1,415,569.73**	**$ 1,410,178.37**	**$ 1,404,254.12**	**$ 1,398,628.31**
IBM Configurations											
	Platinum Tier										
	IBM Mainframe Config - 1	$ 3,257,447 37	$ 3,094,693 45	$ 2,939,994 32	$ 2,793,113 05	$ 2,653,575 85	$ 2,520,908 91	$ 2,394,875 31	$ 2,394,875 31	$ 2,394,875 31	$ 2,394,875 31
	IBM Mainframe Config - 2	$ 236,685 87	$ 224,852 55	$ 213,606 99	$ 202,929 57	$ 192,781 14	$ 183,142 08	$ 173,992 81	$ 173,992 81	$ 173,992 81	$ 173,992 81
	IBM Mainframe Config - 3	$ 553,945 64	$ 526,250 65	$ 499,931 24	$ 474,941 56	$ 451,189 89	$ 428,630 40	$ 407,217 22	$ 407,217 22	$ 407,217 22	$ 407,217 22
	IBM AS400 Config 1	$ 75,865 26	$ 72,072 00	$ 68,481 04	$ 65,041 82	$ 61,804 90	$ 58,719 71	$ 55,786 26	$ 55,786 26	$ 55,786 26	$ 55,786 26
	IBM AS400 Config 2	$ 304,294 74	$ 289,080 00	$ 274,676 72	$ 260,882 02	$ 247,898 78	$ 235,524 13	$ 223,758 06	$ 223,758 06	$ 223,758 06	$ 223,758 06
sub-total IBM Mainfram Services - Plantinum		**$ 4,428,238.88**	**$ 4,206,948.66**	**$ 3,996,690.30**	**$ 3,796,908.03**	**$ 3,607,250.56**	**$ 3,426,925.23**	**$ 3,255,629.66**	**$ 3,255,629.66**	**$ 3,255,629.66**	**$ 3,255,629.66**
	Gold Tier										
	IBM Mainframe Config - 1	$ 379,566 00	$ 360,595 10	$ 342,571 26	$ 325,435 30	$ 309,157 62	$ 293,708 61	$ 279,029 10	$ 279,029 10	$ 279,029 10	$ 279,029 10
	IBM Mainframe Config - 2	$ 28,184 36	$ 26,776 27	$ 25,438 21	$ 24,165 17	$ 22,957 16	$ 21,809 18	$ 20,718 72	$ 20,718 72	$ 20,718 72	$ 20,718 72
	IBM Mainframe Config - 3	$ 64,197 71	$ 60,990 39	$ 57,942 58	$ 55,042 89	$ 52,291 31	$ 49,676 46	$ 47,192 64	$ 47,192 64	$ 47,192 64	$ 47,192 64
	IBM AS400 Config 1	$ 8,941 82	$ 8,494 41	$ 8,072 56	$ 7,669 89	$ 7,286 40	$ 6,922 08	$ 6,576 93	$ 6,576 93	$ 6,576 93	$ 6,576 93
	IBM AS400 Config 2	$ 35,378 50	$ 33,608 31	$ 31,939 28	$ 30,346 11	$ 28,828 80	$ 27,387 36	$ 26,021 79	$ 26,021 79	$ 26,021 79	$ 26,021 79
sub-total IBM Mainfram Services - Gold		**$ 516,268.40**	**$ 490,464.48**	**$ 465,963.89**	**$ 442,659.36**	**$ 420,521.29**	**$ 399,503.70**	**$ 379,539.18**	**$ 379,539.18**	**$ 379,539.18**	**$ 379,539.18**
	Basic Tier										
	IBM Mainframe Config - 1	$ 360,595 10	$ 342,571 26	$ 325,435 30	$ 309,157 62	$ 293,708 61	$ 279,029 10	$ 265,089 49	$ 265,089 49	$ 265,089 49	$ 265,089 49
	IBM Mainframe Config - 2	$ 26,776 27	$ 25,438 21	$ 24,165 17	$ 22,957 16	$ 21,809 18	$ 20,718 72	$ 19,683 28	$ 19,683 28	$ 19,683 28	$ 19,683 28
	IBM Mainframe Config - 3	$ 60,990 39	$ 57,942 58	$ 55,042 89	$ 52,291 31	$ 49,676 46	$ 47,192 64	$ 44,834 15	$ 44,834 15	$ 44,834 15	$ 44,834 15
	IBM AS400 Config 1	$ 8,494 41	$ 8,072 56	$ 7,669 89	$ 7,286 40	$ 6,922 08	$ 6,576 93	$ 6,250 96	$ 6,250 96	$ 6,250 96	$ 6,250 96
	IBM AS400 Config 2	$ 33,608 31	$ 31,939 28	$ 30,346 11	$ 28,828 80	$ 27,387 36	$ 26,021 79	$ 24,732 08	$ 24,732 08	$ 24,732 08	$ 24,732 08
sub-total IBM Mainfram Services - Basic		**$ 490,464.48**	**$ 465,963.89**	**$ 442,659.36**	**$ 420,521.29**	**$ 399,503.70**	**$ 379,539.18**	**$ 360,589.96**	**$ 360,589.96**	**$ 360,589.96**	**$ 360,589.96**

Note: The Commonwealth has established mult

Baseline Units - Volumetrics

Resource Description	Service Tier / Configuration (6)	Annual Costs Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Total - IBM Mainfram Services - All Support Tiers		**$ 5,434,971.75**	**$ 5,163,377.03**	**$ 4,905,313.55**	**$ 4,660,088.68**	**$ 4,427,275.55**	**$ 4,205,968.11**	**$ 3,995,758.80**	**$ 3,995,758.80**	**$ 3,995,758.80**	**$ 3,995,758.80**
Unisys Services											
	*** Unisys DASD	$ 117,415 63	$ 117,492 26	$ 117,354 43	$ 117,325 22	$ 117,301 29	$ 83,610 17	$ 83,571 87	$ 83,509 60	$ 83,452 79	$ 83,400 97
	Unisys Tapes in Storage - VTS	$ 191,086 73	$ 186,753 27	$ 188,861 25	$ 191,134 41	$ 193,470 85	$ 178,345 58	$ 180,788 22	$ 180,725 96	$ 180,669 15	$ 180,617 33
	Unisys Offsite Tape Storage	$ 2,884 36	$ 2,848 86	$ 2,829 82	$ 2,810 49	$ 2,791 29	$ 2,718 59	$ 2,752 89	$ 2,502 58	$ 2,275 17	$ 2,068 31
Total Unisys Services		**$ 311,386.72**	**$ 307,094.39**	**$ 309,045.51**	**$ 311,270.12**	**$ 313,563.42**	**$ 264,674.34**	**$ 267,112.98**	**$ 266,738.14**	**$ 266,397.10**	**$ 266,086.61**
Unisys Configurations											
	Platinum Tier										
	Unisys Mainframe Config - 1	$ 6,650,365 60	$ 6,540,459 11	$ 6,486,773 84	$ 6,435,430 23	$ 6,370,451 40	$ 6,335,042 93	$ 6,224,840 24	$ 6,224,840 24	$ 6,224,840 24	$ 6,224,840 24
	Unisys Mainframe Config - 2	$ 2,605,367 88	$ 2,573,806 36	$ 2,560,689 70	$ 2,547,573 04	$ 2,522,582 65	$ 2,513,307 96	$ 2,489,952 64	$ 2,489,952 64	$ 2,489,952 64	$ 2,489,952 64
	Unisys Mainframe Config - 3	$ 339,837 19	$ 336,621 55	$ 335,091 25	$ 333,560 96	$ 330,642 60	$ 315,179 25	$ 313,137 79	$ 313,137 79	$ 313,137 79	$ 313,137 79
	Unisys Mainframe Config - 4	$ 150,390 97	$ 149,710 15	$ 149,387 00	$ 149,063 85	$ 148,447 28	$ 144,991 38	$ 141,535 49	$ 141,535 49	$ 141,535 49	$ 141,535 49
sub-total Unisys Mainfram Services - Plantinum		**$ 9,745,961.64**	**$ 9,600,597.16**	**$ 9,531,941.79**	**$ 9,465,628.08**	**$ 9,372,123.93**	**$ 9,308,521.53**	**$ 9,169,466.16**	**$ 9,169,466.16**	**$ 9,169,466.16**	**$ 9,169,466.16**
	Gold Tier										
	Unisys Mainframe Config - 1	$ 483,662 95	$ 475,669 75	$ 471,765 37	$ 468,031 29	$ 463,305 56	$ 460,730 39	$ 452,715 65	$ 452,715 65	$ 452,715 65	$ 452,715 65
	Unisys Mainframe Config - 2	$ 290,681 54	$ 287,160 21	$ 285,696 78	$ 284,233 36	$ 281,445 17	$ 280,410 39	$ 277,804 63	$ 277,804 63	$ 277,804 63	$ 277,804 63
	Unisys Mainframe Config - 3	$ 18,866 74	$ 18,688 22	$ 18,603 26	$ 18,518 30	$ 18,356 29	$ 17,497 81	$ 17,384 47	$ 17,384 47	$ 17,384 47	$ 17,384 47
	Unisys Mainframe Config - 4	$ 17,187 54	$ 17,109 73	$ 17,072 80	$ 17,035 87	$ 16,965 40	$ 16,570 44	$ 16,175 48	$ 16,175 48	$ 16,175 48	$ 16,175 48
sub-total Unisys Mainfram Services - Gold		**$ 810,398.77**	**$ 798,627.92**	**$ 793,138.22**	**$ 787,818.82**	**$ 780,072.42**	**$ 775,209.04**	**$ 764,080.24**	**$ 764,080.24**	**$ 764,080.24**	**$ 764,080.24**
	Basic Tier										
	Unisys Mainframe Config - 1	$ 443,357 71	$ 436,030 61	$ 432,451 59	$ 429,028 68	$ 424,696 76	$ 422,336 20	$ 414,989 35	$ 414,989 35	$ 414,989 35	$ 414,989 35
	Unisys Mainframe Config - 2	$ 266,458 08	$ 263,230 20	$ 260,547 24	$ 259,269 33	$ 257,991 41	$ 257,042 86	$ 254,654 25	$ 254,654 25	$ 254,654 25	$ 254,654 25
	Unisys Mainframe Config - 3	$ 17,294 51	$ 17,130 87	$ 16,974 95	$ 16,900 77	$ 16,826 60	$ 16,039 66	$ 15,935 77	$ 15,935 77	$ 15,935 77	$ 15,935 77
	Unisys Mainframe Config - 4	$ 15,755 24	$ 15,683 92	$ 15,616 21	$ 15,491 52	$ 15,419 62	$ 15,123 57	$ 14,827 53	$ 14,827 53	$ 14,827 53	$ 14,827 53
sub-total Unisys Mainfram Services - Basic		**$ 742,865.54**	**$ 732,075.59**	**$ 725,589.99**	**$ 720,690.30**	**$ 714,934.38**	**$ 710,542.29**	**$ 700,406.89**	**$ 700,406.89**	**$ 700,406.89**	**$ 700,406.89**
Total - Unisys Mainfram Services - All Support Tiers		**$ 11,299,225.96**	**$ 11,131,300.67**	**$ 11,050,670.01**	**$ 10,974,137.20**	**$ 10,867,130.72**	**$ 10,794,272.85**	**$ 10,633,953.29**	**$ 10,633,953.29**	**$ 10,633,953.29**	**$ 10,633,953.29**
On-Demand (IaaS) (5)											
IaaS Servers - x86 (Windows, Linux) - Virtual Servers											
	IaaS Windows vConfig - 1	$ 16,324 64	$ 18,791 28	$ 22,016 08	$ 26,119 64	$ 30,596 84	$ 36,348 40	$ 42,109 68	$ 50,180 71	$ 60,357 21	$ 65,971 84
	IaaS Windows vConfig - 2	$ 34,231 75	$ 38,978 75	$ 45,058 58	$ 52,191 37	$ 60,472 95	$ 69,384 00	$ 79,856 52	$ 95,162 35	$ 114,461 01	$ 125,108 54
	IaaS Windows vConfig - 3	$ 103,444 81	$ 117,107 66	$ 134,293 15	$ 153,144 02	$ 176,275 91	$ 197,774 78	$ 226,522 59	$ 269,939 42	$ 324,682 38	$ 354,885 39
	IaaS Windows vConfig - 4	$ 12,836 91	$ 14,617 03	$ 16,314 31	$ 18,909 92	$ 21,597 48	$ 24,978 24	$ 29,280 72	$ 35,935 43	$ 43,255 61	$ 47,913 91
	IaaS Windows vConfig - 5	$ 12,836 91	$ 14,617 03	$ 16,314 31	$ 18,909 92	$ 21,597 48	$ 24,978 24	$ 29,280 72	$ 35,935 43	$ 43,255 61	$ 47,913 91
	IaaS Linux vConfig - 1	$ 8,128 93	$ 9,355 57	$ 10,959 93	$ 12,814 49	$ 15,229 83	$ 18,093 38	$ 20,957 87	$ 25,149 45	$ 30,039 62	$ 38,822 10
	IaaS Linux vConfig - 2	$ 17,082 48	$ 19,449 31	$ 22,481 18	$ 25,661 43	$ 30,167 88	$ 34,611 17	$ 39,831 29	$ 47,797 55	$ 51,705 66	$ 80,467 90
	IaaS Linux vConfig - 3	$ 51,689 01	$ 58,513 77	$ 67,098 46	$ 75,406 21	$ 88,069 36	$ 98,806 57	$ 113,164 33	$ 135,797 19	$ 138,369 82	$ 247,051 08
	IaaS Linux vConfig - 4	$ 5,978 87	$ 7,293 49	$ 8,527 34	$ 9,811 72	$ 10,774 24	$ 12,460 02	$ 15,268 66	$ 17,924 08	$ 19,239 31	$ 30,817 49
	IaaS Linux vConfig - 5	$ 5,978 87	$ 7,293 49	$ 8,527 34	$ 9,811 72	$ 10,774 24	$ 12,460 02	$ 15,268 66	$ 17,924 08	$ 19,239 31	$ 30,817 49
Total IaaS Servers - x86 (Windows, Linux) - Virtual Servers		**$ 268,533.18**	**$ 306,017.39**	**$ 351,590.69**	**$ 402,780.44**	**$ 465,556.22**	**$ 529,894.83**	**$ 611,541.05**	**$ 731,745.69**	**$ 844,605.55**	**$ 1,069,769.66**
IaaS Storage On-Demand											
	IaaS Storage Config - 1	$ 679 36	$ 777 78	$ 886 94	$ 1,012 35	$ 1,156 68	$ 1,328 90	$ 1,491 44	$ 1,626 98	$ 1,775 09	$ 1,936 50
	IaaS Storage Config - 2	$ 1,443 35	$ 1,713 47	$ 2,034 63	$ 2,415 98	$ 2,869 20	$ 3,403 45	$ 4,042 24	$ 4,410 72	$ 4,810 81	$ 5,248 18
	IaaS Storage Config - 3	$ 42 25	$ 38 74	$ 35 43	$ 32 44	$ 29 75	$ 20 95	$ 19 37	$ 17 61	$ 16 01	$ 14 56

Note: The Commonwealth has established mult

Baseline Units - Volumetrics

Resource Description	Service Tier / Configuration (6)	Annual Costs Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Total IaaS Storage On-Demand		**$ 2,164.97**	**$ 2,530.00**	**$ 2,957.00**	**$ 3,460.77**	**$ 4,055.62**	**$ 4,753.30**	**$ 5,553.05**	**$ 6,055.30**	**$ 6,601.91**	**$ 7,199.24**
IaaS Backup On-Demand											
	IaaS Backup Config - 1	$ 1,748 06	$ 1,489 98	$ 1,631 66	$ 1,823 04	$ 2,030 88	$ 2,238 65	$ 2,559 05	$ 2,791 62	$ 3,045 76	$ 3,322 73
Total IaaS Backup On-Demand		**$ 1,748.06**	**$ 1,489.98**	**$ 1,631.66**	**$ 1,823.04**	**$ 2,030.88**	**$ 2,238.65**	**$ 2,559.05**	**$ 2,791.62**	**$ 3,045.76**	**$ 3,322.73**
Reserve Account											
		$ 1,008,000 00	$ 1,008,000 00	$ 1,008,000 00	$ 1,008,000 00	$ 1,008,000 00	$ 1,008,000 00	$ 1,008,000 00	$ 1,008,000 00	$ 1,008,000 00	$ 1,008,000 00
Reserve Account		**$ 1,008,000.00**	**$ 1,008,000.00**	**$ 1,008,000.00**	**$ 1,008,000.00**	**$ 1,008,000.00**	**$ 1,008,000.00**	**$ 1,008,000.00**	**$ 1,008,000.00**	**$ 1,008,000.00**	**$ 1,008,000.00**

Notes:

For purposes of submitting a proposal, Offerors should assume that tapes are equivalent in ca

* For purposes of submitting a proposal, Offerors should assume that the slower Tier1 RAID!

** The volume is expressed as native.

*** For purposes of evaluation DASD is expressed in Usable (not Raw)

Third Party Software

Third Party Software

Vendor	Product										
B & L	BL/LIB Tape Library Management System	$ 16,711 56	$ 17,515 38	$ 18,040 84	$ 18,582 07	$ 19,139 53	$ 19,713 71	$ 20,305 12	$ 20,305 12	$ 20,305 12	$ 20,305 12
B & L	BL/SCHED Scheduling & Monitoring System	$ 21,086 22	$ 22,100 49	$ 22,763 51	$ 23,446 41	$ 24,149 80	$ 24,874 30	$ 25,620 53	$ 25,620 53	$ 25,620 53	$ 25,620 53
BMC Software	BMC AppSight for Windows/.NET - Division Edition	$ 58,055 56	$ 59,797 22	$ 61,591 14	$ 63,438 87	$ 65,342 04	$ 67,302 30	$ 69,321 37	$ 69,321 37	$ 69,321 37	$ 69,321 37
BMC Software	BMC AppSight Named Users	$ 21,153 73	$ 21,788 35	$ 22,442 00	$ 23,115 26	$ 23,808 71	$ 24,522 97	$ 25,258 66	$ 25,258 66	$ 25,258 66	$ 25,258 66
BMC Software	BMC AppSight QA Users	$ 3,290 71	$ 3,389 43	$ 3,491 12	$ 3,595 85	$ 3,703 72	$ 3,814 84	$ 3,929 28	$ 3,929 28	$ 3,929 28	$ 3,929 28
BMC Software	CONTROL-M Enterprise Manager	$ 3,666 67	$ 3,776 67	$ 3,889 97	$ 4,006 67	$ 4,126 87	$ 4,250 67	$ 4,378 19	$ 4,378 19	$ 4,378 19	$ 4,378 19
BMC Software	CONTROL-M Full Admin User	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	CONTROL-M Tasks (100 Tasks per Unit)	$ 249,480 00	$ 256,964 40	$ 264,673 33	$ 272,613 53	$ 280,791 94	$ 289,215 70	$ 297,892 17	$ 297,892 17	$ 297,892 17	$ 297,892 17
BMC Software	Database Director (D2)	$ 439,582 37	$ 452,769 87	$ 466,352 94	$ 480,343 55	$ 494,753 92	$ 509,596 42	$ 524,884 38	$ 540,630 87	$ 556,849 78	$ 573,555 28
BMC Software	Eclipse iBuild	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iChange	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iCheck	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iCopy	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iExtract	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iLM	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iLoad	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iRecover	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iSurvey	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iUnload	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Mission Control	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Business Objects	Crystal Reports	$ 484 00	$ 498 52	$ 513 48	$ 528 88	$ 544 75	$ 561 09	$ 577 92	$ 577 92	$ 577 92	$ 577 92
Bytware Inc.	StandGuard Anti-Virus	$ 1,246 67	$ 1,284 07	$ 1,322 59	$ 1,362 27	$ 1,403 13	$ 1,445 23	$ 1,488 59	$ 1,488 59	$ 1,488 59	$ 1,488 59
Citrix	XenApp Advanced (User Counts)	$ -	$ 4,036 00	$ 4,157 08	$ 4,281 79	$ 4,410 24	$ 4,542 55	$ 4,678 83	$ 4,678 83	$ 4,678 83	$ 4,678 83
Citrix	XenApp Enterprise (User Counts)	$ -	$ 33,640 66	$ 34,649 88	$ 35,689 37	$ 36,760 06	$ 37,862 86	$ 38,998 74	$ 38,998 74	$ 38,998 74	$ 38,998 74
Computer Associates Interna ional, Inc.	CA-Explore for CICS	$ 8,812 95	$ 9,077 34	$ 9,349 66	$ 9,630 15	$ 9,919 06	$ 10,216 63	$ 10,523 13	$ 10,838 82	$ 11,163 99	$ 11,498 91

Note: The Commonwealth has established mult

Baseline Units - Volumetrics

Resource Description	Service Tier / Configuration (6)	Annual Costs Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Computer Associates Interna ional, Inc.	SOA Security Manager	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates Interna ional, Inc.	SOA Security Manager Additional Secured Web Services	$ 97,777 78	$ 100,711 11	$ 103,732 44	$ 106,844 42	$ 110,049 75	$ 113,351 24	$ 116,751 78	$ 116,751 78	$ 116,751 78	$ 116,751 78
Computer Associates Interna ional, Inc.	SOA Security Manager Additional Users	$ 168,055 56	$ 173,097 22	$ 178,290 14	$ 183,638 84	$ 189,148 01	$ 194,822 45	$ 200,667 12	$ 200,667 12	$ 200,667 12	$ 200,667 12
Cor icon Technologies	Corticon Business Rules Server – Unlimited CPUs	$ 156,444 44	$ 161,137 78	$ 165,971 91	$ 170,951 07	$ 176,079 60	$ 181,361 99	$ 186,802 85	$ 186,802 85	$ 186,802 85	$ 186,802 85
Cor icon Technologies	Corticon Server – per Non-Production Server	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Cor icon Technologies	Corticon Business Rules Modeling Studio – per Named User	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
CSI International	EPIC	$ 24,943 44	$ 25,691 74	$ 26,462 50	$ 27,256 37	$ 28,074 06	$ 28,916 28	$ 29,783 77	$ 30,677 29	$ 31,597 60	$ 32,545 53
CSI International	FAQS/PCS	$ 15,166 97	$ 15,621 98	$ 16,090 64	$ 16,573 36	$ 17,070 56	$ 17,582 68	$ 18,110 16	$ 18,653 46	$ 19,213 07	$ 19,789 46
CSI International	FAQS/ASO	$ 18,593 98	$ 19,151 80	$ 19,726 35	$ 20,318 14	$ 20,927 69	$ 21,555 52	$ 22,202 18	$ 22,868 25	$ 23,554 30	$ 24,260 93
EMC Corporation	PowerPath	$ 2,860 73	$ 2,946 56	$ 3,034 95	$ 3,126 00	$ 3,219 78	$ 3,316 37	$ 3,415 87	$ 3,415 87	$ 3,415 87	$ 3,415 87
EMC Corporation	PowerPath (per CPU)	$ 8,685 60	$ 8,946 17	$ 9,214 55	$ 9,490 99	$ 9,775 72	$ 10,068 99	$ 10,371 06	$ 10,371 06	$ 10,371 06	$ 10,371 06
EMC Corporation	Symmetrix® VMAX Fully Automated Storage Tiering for Virtual Pools (FAST VP)	$ 2,276 34	$ 2,344 63	$ 2,414 97	$ 2,487 42	$ 2,562 04	$ 2,638 90	$ 2,718 07	$ 2,718 07	$ 2,718 07	$ 2,718 07
EMC Corporation	Vsphere Enterprise Plus	$ 21,120 00	$ 21,753 60	$ 22,406 21	$ 23,078 39	$ 23,770 75	$ 24,483 87	$ 25,218 38	$ 25,218 38	$ 25,218 38	$ 25,218 38
Experian QAS	NameSearch - Production (Licensed per Server up to 8 CPU)	$ 136,888 89	$ 140,995 56	$ 145,225 42	$ 149,582 18	$ 154,069 65	$ 158,691 74	$ 163,452 49	$ 163,452 49	$ 163,452 49	$ 163,452 49
Experian QAS	NameSearch - Non-Production (Licensed per Server)	$ 31,166 67	$ 32,101 67	$ 33,064 72	$ 34,056 66	$ 35,078 36	$ 36,130 71	$ 37,214 63	$ 37,214 63	$ 37,214 63	$ 37,214 63
Formula Consultants, Inc.	Star 1100	$ 7,128 00	$ 7,341 84	$ 7,562 10	$ 7,788 96	$ 8,022 63	$ 8,263 31	$ 8,511 20	$ 8,511 20	$ 8,511 20	$ 8,511 20
GlobalScape	CuteFTP Pro 2.0	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
HELPSYS	Robot/Schedule	$ 54,001 62	$ 55,621 66	$ 57,290 31	$ 59,009 02	$ 60,779 29	$ 62,602 67	$ 64,480 75	$ 66,415 18	$ 68,407 63	$ 70,459 86
Idea Integration	XGEN	$ 39,601 83	$ 40,789 89	$ 42,013 58	$ 43,273 99	$ 44,572 21	$ 45,909 38	$ 47,286 66	$ 47,286 66	$ 47,286 66	$ 47,286 66
Informatica Corporation	SSA-Name 3	$ 64,166 67	$ 66,091 67	$ 68,074 42	$ 70,116 65	$ 72,220 15	$ 74,386 75	$ 76,618 36	$ 76,618 36	$ 76,618 36	$ 76,618 36
Infragistics	NetAdvantage for .NET	$ 5,613 15	$ 5,781 55	$ 5,954 99	$ 6,133 64	$ 6,317 65	$ 6,507 18	$ 6,702 40	$ 6,702 40	$ 6,702 40	$ 6,702 40
KMSYS Worldwide, Inc.	IQU Plus-1	$ 11,733 33	$ 12,085 33	$ 12,447 89	$ 12,821 33	$ 13,205 97	$ 13,602 15	$ 14,010 21	$ 14,010 21	$ 14,010 21	$ 14,010 21
Levi, Ray and Shoup	VPS/PCL	$ 57,252 99	$ 58,970 57	$ 60,739 69	$ 62,561 88	$ 64,438 74	$ 66,371 90	$ 68,363 06	$ 70,413 95	$ 72,526 37	$ 74,702 16
Levi, Ray and Shoup	VPS/TCP/IP	$ 40,287 62	$ 41,496 24	$ 42,741 13	$ 44,023 37	$ 45,344 07	$ 46,704 39	$ 48,105 52	$ 49,548 69	$ 51,035 15	$ 52,566 20
Levi, Ray and Shoup	VPS/DRS	$ 20,384 05	$ 20,995 57	$ 21,625 44	$ 22,274 20	$ 22,942 43	$ 23,630 70	$ 24,339 62	$ 25,069 81	$ 25,821 90	$ 26,596 56
Levi, Ray and Shoup	VPS	$ 63,077 22	$ 64,969 54	$ 66,918 63	$ 68,926 19	$ 70,993 97	$ 73,123 79	$ 75,317 51	$ 77,577 03	$ 79,904 34	$ 82,301 47
MacKinney Systems, Inc.	CICS Response Time Monitor	$ 455 92	$ 469 60	$ 483 69	$ 498 20	$ 513 14	$ 528 54	$ 544 39	$ 560 73	$ 577 55	$ 594 87
Marble Computer, Inc.	OS DCD III Data Correlation and Documenta ion System	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	BizTalk Adaptor for MQSeries	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	BizTalk Server Enterprise (Single Processor)	$ 95,720 67	$ 98,592 29	$ 101,550 06	$ 104,596 56	$ 107,734 45	$ 110,966 49	$ 114,295 48	$ 114,295 48	$ 114,295 48	$ 114,295 48
Microsoft	BizTalk Server Standard (Single Processor)	$ 17,553 60	$ 18,080 21	$ 18,622 61	$ 19,181 29	$ 19,756 73	$ 20,349 43	$ 20,959 92	$ 20,959 92	$ 20,959 92	$ 20,959 92
Microsoft	SQL Server CAL	$ 15,518 67	$ 15,518 67	$ 15,518 67	$ 15,518 67	$ 15,518 67	$ 15,518 67	$ 15,518 67	$ 15,518 67	$ 15,518 67	$ 15,518 67
Microsoft	SQL Server Enterprise (Single Processor)	$ 59,513 33	$ 61,298 73	$ 63,137 70	$ 65,031 83	$ 66,982 78	$ 68,992 26	$ 71,062 03	$ 71,062 03	$ 71,062 03	$ 71,062 03
Microsoft	SQL Server Enterprise	$ 65,464 67	$ 67,428 61	$ 69,451 46	$ 71,535 01	$ 73,681 06	$ 75,891 49	$ 78,168 24	$ 78,168 24	$ 78,168 24	$ 78,168 24
Microsoft	SQL Server Standard (Single Processor)	$ 3,103 73	$ 3,196 85	$ 3,292 75	$ 3,391 53	$ 3,493 28	$ 3,598 08	$ 3,706 02	$ 3,706 02	$ 3,706 02	$ 3,706 02
Microsoft	SQL Server Standard	$ 12,414 93	$ 12,787 38	$ 13,171 00	$ 13,566 13	$ 13,973 12	$ 14,392 31	$ 14,824 08	$ 14,824 08	$ 14,824 08	$ 14,824 08
Microsoft	SQL Server Standard per 2-Core	$ 12,414 93	$ 12,787 38	$ 13,171 00	$ 13,566 13	$ 13,973 12	$ 14,392 31	$ 14,824 08	$ 14,824 08	$ 14,824 08	$ 14,824 08
Microsoft	Visual Studio Foundation Server	$ 178 85	$ 184 21	$ 189 74	$ 195 43	$ 201 29	$ 207 33	$ 213 55	$ 213 55	$ 213 55	$ 213 55
Microsoft	Visual Studio Foundation Server CAL	$ 1,234 49	$ 1,271 53	$ 1,309 67	$ 1,348 96	$ 1,389 43	$ 1,431 12	$ 1,474 05	$ 1,474 05	$ 1,474 05	$ 1,474 05
Microsoft	Visual Studio Professional with MSDN	$ 2,151 47	$ 2,216 01	$ 2,282 49	$ 2,350 97	$ 2,421 49	$ 2,494 14	$ 2,568 96	$ 2,568 96	$ 2,568 96	$ 2,568 96

Note: The Commonwealth has established mult

Baseline Units - Volumetrics

Resource Description	Service Tier / Configuration (6)	Annual Costs Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Microsoft	Windows Server Datacenter Edition (Single Processor)	$ 238,749 33	$ 245,911 81	$ 253,289 17	$ 260,887 84	$ 268,714 48	$ 276,775 91	$ 285,079 19	$ 285,079 19	$ 285,079 19	$ 285,079 19
Microsoft	Windows Server Enterprise Edition	$ 191,139 20	$ 196,873 38	$ 202,779 58	$ 208,862 96	$ 215,128 85	$ 221,582 72	$ 228,230 20	$ 228,230 20	$ 228,230 20	$ 228,230 20
Microsoft	Windows Server Standard Edition	$ 35,035 87	$ 36,086 94	$ 37,169 55	$ 38,284 64	$ 39,433 18	$ 40,616 17	$ 41,834 66	$ 41,834 66	$ 41,834 66	$ 41,834 66
Microsoft	Windows Terminal Service Client Access Licenses	$ 4,466 67	$ 4,600 67	$ 4,738 69	$ 4,880 85	$ 5,027 27	$ 5,178 09	$ 5,333 43	$ 5,333 43	$ 5,333 43	$ 5,333 43
Network Associates	McAfee Anti-Virus	$ 4,508 05	$ 4,643 29	$ 4,782 59	$ 4,926 07	$ 5,073 85	$ 5,226 07	$ 5,382 85	$ 5,382 85	$ 5,382 85	$ 5,382 85
Novell	Platespin Migrator	$ 1,188 00	$ 1,223 64	$ 1,260 35	$ 1,298 16	$ 1,337 10	$ 1,377 22	$ 1,418 53	$ 1,418 53	$ 1,418 53	$ 1,418 53
Novell	SuSE Linux	$ 178,607 39	$ 183,965 61	$ 189,484 58	$ 195,169 12	$ 201,024 19	$ 207,054 92	$ 213,266 57	$ 219,664 56	$ 226,254 50	$ 233,042 13
OpenText	Metastorm Integration Manager for CICS (MIM for CICS)	$ 108,086 63	$ 111,329 23	$ 114,669 11	$ 118,109 18	$ 121,652 46	$ 125,302 03	$ 129,061 09	$ 132,932 92	$ 136,920 91	$ 141,028 54
Oracle	Oracle Change Management Pack	$ 16,133 33	$ 16,617 33	$ 17,115 85	$ 17,629 33	$ 18,158 21	$ 18,702 96	$ 19,264 04	$ 19,264 04	$ 19,264 04	$ 19,264 04
Oracle	Oracle Database 10g Enterprise	$ 34,147 71	$ 35,172 14	$ 36,227 31	$ 37,314 13	$ 38,433 55	$ 39,586 56	$ 40,774 15	$ 41,997 38	$ 43,257 30	$ 44,555 02
Oracle	Oracle Database Enterprise Edition	$ 114,950 00	$ 118,398 50	$ 121,950 46	$ 125,608 97	$ 129,377 24	$ 133,258 55	$ 137,256 31	$ 137,256 31	$ 137,256 31	$ 137,256 31
Oracle	Oracle Diagnostic Pack	$ 11,302 91	$ 11,642 00	$ 11,991 26	$ 12,350 99	$ 12,721 52	$ 13,103 17	$ 13,496 26	$ 13,587 80	$ 13,682 08	$ 13,779 19
Oracle	Oracle Enterprise Linux	$ 5,129 67	$ 5,283 56	$ 5,442 06	$ 5,605 33	$ 5,773 49	$ 5,946 69	$ 6,125 09	$ 6,125 09	$ 6,125 09	$ 6,125 09
Oracle	Oracle Exadata Storage Software	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Oracle	Oracle Partitioning	$ 12,368 89	$ 12,739 96	$ 13,122 15	$ 13,515 82	$ 13,921 29	$ 14,338 93	$ 14,769 10	$ 14,769 10	$ 14,769 10	$ 14,769 10
Oracle	Oracle Tuning Pack	$ 13,909 31	$ 14,171 74	$ 14,442 04	$ 14,720 45	$ 15,007 21	$ 15,302 58	$ 15,606 81	$ 15,606 81	$ 15,606 81	$ 15,606 81
Oracle	Real Application Cluster - Processor Perpetual	$ 21,224 04	$ 21,860 76	$ 22,516 58	$ 23,192 08	$ 23,887 84	$ 24,604 48	$ 25,342 61	$ 26,102 89	$ 26,885 97	$ 27,692 55
Oracle	Spatial and Graph - Processor Perpetual	$ 16,148 72	$ 16,633 19	$ 17,132 18	$ 17,646 15	$ 18,175 53	$ 18,720 80	$ 19,282 42	$ 19,860 89	$ 20,456 72	$ 21,070 42
Pitney Bowes	Finalist (Doc Sense)	$ 93,550 44	$ 96,356 95	$ 99,247 66	$ 102,225 09	$ 105,291 85	$ 108,450 60	$ 111,704 12	$ 115,055 24	$ 118,506 90	$ 122,062 11
Pitney Bowes	CODE-1 Plus	$ 8,800 00	$ 9,064 00	$ 9,335 92	$ 9,616 00	$ 9,904 48	$ 10,201 61	$ 10,507 66	$ 10,507 66	$ 10,507 66	$ 10,507 66
Pitney Bowes	CODE-1 Plus (Test / Development)	$ 4,033 33	$ 4,154 33	$ 4,278 96	$ 4,407 33	$ 4,539 55	$ 4,675 74	$ 4,816 01	$ 4,816 01	$ 4,816 01	$ 4,816 01
Pitney Bowes	Online Window for Finalist	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Quest	Central Performance Suite for SQL Server, Tier A	$ 1,058 75	$ 1,090 52	$ 1,123 23	$ 1,156 93	$ 1,191 64	$ 1,227 39	$ 1,264 21	$ 1,264 21	$ 1,264 21	$ 1,264 21
Quest	Central Performance Suite for SQL Server, Tier B	$ 5,293 77	$ 5,452 58	$ 5,616 16	$ 5,784 65	$ 5,958 19	$ 6,136 93	$ 6,321 04	$ 6,321 04	$ 6,321 04	$ 6,321 04
Quest	Foglight Database Management Suite for SQL Server	$ 4,235 02	$ 4,362 07	$ 4,492 93	$ 4,627 72	$ 4,766 55	$ 4,909 54	$ 5,056 83	$ 5,056 83	$ 5,056 83	$ 5,056 83
Quest	Foglight for SQL Server per CPU Socket	$ 11,116 92	$ 11,450 43	$ 11,793 94	$ 12,147 76	$ 12,512 19	$ 12,887 55	$ 13,274 18	$ 13,274 18	$ 13,274 18	$ 13,274 18
Quest	Foglight OS Management per CPU Socket	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Quest	Foglight Server for FSM	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
RealVNC	VNC Enterprise Edition for Windows	$ 211 75	$ 218 10	$ 224 65	$ 231 38	$ 238 33	$ 245 48	$ 252 84	$ 252 84	$ 252 84	$ 252 84
Red Hat	Red Hat Enterprise Linux	$ 11,515 31	$ 11,860 77	$ 12,216 60	$ 12,583 09	$ 12,960 59	$ 13,349 40	$ 13,749 89	$ 13,749 89	$ 13,749 89	$ 13,749 89
Schema Systems Limited	Q Editor Plus One	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Segus Inc.	OPC/Graph	$ 9,077 34	$ 9,349 66	$ 9,630 15	$ 9,919 06	$ 10,216 63	$ 10,523 13	$ 10,838 82	$ 11,163 99	$ 11,498 91	$ 11,843 87
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG20	$ 679 56	$ 699 94	$ 720 94	$ 742 57	$ 764 85	$ 787 79	$ 811 42	$ 811 42	$ 811 42	$ 811 42
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG40	$ 840 89	$ 866 12	$ 892 10	$ 918 86	$ 946 43	$ 974 82	$ 1,004 07	$ 1,004 07	$ 1,004 07	$ 1,004 07
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG60	$ 1,007 11	$ 1,037 32	$ 1,068 44	$ 1,100 50	$ 1,133 51	$ 1,167 52	$ 1,202 54	$ 1,202 54	$ 1,202 54	$ 1,202 54
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG80	$ 1,168 44	$ 14,441 97	$ 14,875 23	$ 15,321 49	$ 15,781 13	$ 16,254 57	$ 16,742 21	$ 16,742 21	$ 16,742 21	$ 16,742 21
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG130	$ 1,623 11	$ 1,671 80	$ 1,721 96	$ 1,773 62	$ 1,826 83	$ 1,881 63	$ 1,938 08	$ 1,938 08	$ 1,938 08	$ 1,938 08

Note: The Commonwealth has established mult

Baseline Units - Volumetrics

		Annual Costs									
Resource Description	**Service Tier / Configuration (6)**	**Year 1**	**Year 2**	**Year 3**	**Year 4**	**Year 5**	**Year 6**	**Year 7**	**Opt - Year 8**	**Opt - Year 9**	**Opt - Year 10**
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG20	$ 679 56	$ 699 94	$ 720 94	$ 742 57	$ 764 85	$ 787 79	$ 811 42	$ 811 42	$ 811 42	$ 811 42
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG40	$ 840 89	$ 866 12	$ 892 10	$ 918 86	$ 946 43	$ 974 82	$ 1,004 07	$ 1,004 07	$ 1,004 07	$ 1,004 07
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG60	$ 1,007 11	$ 1,037 32	$ 1,068 44	$ 1,100 50	$ 1,133 51	$ 1,167 52	$ 1,202 54	$ 1,202 54	$ 1,202 54	$ 1,202 54
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG80	$ 1,168 44	$ 1,203 50	$ 1,239 60	$ 1,276 79	$ 1,315 09	$ 1,354 55	$ 1,395 18	$ 1,395 18	$ 1,395 18	$ 1,395 18
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG130	$ 1,623 11	$ 1,671 80	$ 1,721 96	$ 1,773 62	$ 1,826 83	$ 1,881 63	$ 1,938 08	$ 1,938 08	$ 1,938 08	$ 1,938 08
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG140	$ 1,867 56	$ 1,923 58	$ 1,981 29	$ 2,040 73	$ 2,101 95	$ 2,165 01	$ 2,229 96	$ 2,229 96	$ 2,229 96	$ 2,229 96
Sightline	OS 2200 Interface Agent - MAPPER, SWG20	$ 679 56	$ 699 94	$ 720 94	$ 742 57	$ 764 85	$ 787 79	$ 811 42	$ 811 42	$ 811 42	$ 811 42
Sightline	OS 2200 Interface Agent - MAPPER, SWG40	$ 840 89	$ 866 12	$ 892 10	$ 918 86	$ 946 43	$ 974 82	$ 1,004 07	$ 1,004 07	$ 1,004 07	$ 1,004 07
Sightline	OS 2200 Interface Agent - MAPPER, SWG60	$ 1,007 11	$ 1,037 32	$ 1,068 44	$ 1,100 50	$ 1,133 51	$ 1,167 52	$ 1,202 54	$ 1,202 54	$ 1,202 54	$ 1,202 54
Sightline	OS 2200 Interface Agent - MAPPER, SWG80	$ 1,168 44	$ 1,203 50	$ 1,239 60	$ 1,276 79	$ 1,315 09	$ 1,354 55	$ 1,395 18	$ 1,395 18	$ 1,395 18	$ 1,395 18
Sightline	OS 2200 Interface Agent - MAPPER, SWG130	$ 1,623 11	$ 1,671 80	$ 1,721 96	$ 1,773 62	$ 1,826 83	$ 1,881 63	$ 1,938 08	$ 1,938 08	$ 1,938 08	$ 1,938 08
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG20	$ 691 78	$ 712 53	$ 733 91	$ 755 92	$ 778 60	$ 801 96	$ 826 02	$ 826 02	$ 826 02	$ 826 02
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG40	$ 840 89	$ 866 12	$ 892 10	$ 918 86	$ 946 43	$ 974 82	$ 1,004 07	$ 1,004 07	$ 1,004 07	$ 1,004 07
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG60	$ 1,007 11	$ 1,037 32	$ 1,068 44	$ 1,100 50	$ 1,133 51	$ 1,167 52	$ 1,202 54	$ 1,202 54	$ 1,202 54	$ 1,202 54
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG80	$ 1,168 44	$ 1,203 50	$ 1,239 60	$ 1,276 79	$ 1,315 09	$ 1,354 55	$ 1,395 18	$ 1,395 18	$ 1,395 18	$ 1,395 18
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG130	$ 1,623 11	$ 1,671 80	$ 1,721 96	$ 1,773 62	$ 1,826 83	$ 1,881 63	$ 1,938 08	$ 1,938 08	$ 1,938 08	$ 1,938 08
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG140	$ 1,867 56	$ 1,923 58	$ 1,981 29	$ 2,040 73	$ 2,101 95	$ 2,165 01	$ 2,229 96	$ 2,229 96	$ 2,229 96	$ 2,229 96
Sightline	OS 2200 Interface Agent - System Log, SWG20	$ 679 56	$ 699 94	$ 720 94	$ 742 57	$ 764 85	$ 787 79	$ 811 42	$ 811 42	$ 811 42	$ 811 42
Sightline	OS 2200 Interface Agent - System Log, SWG40	$ 840 89	$ 866 12	$ 892 10	$ 918 86	$ 946 43	$ 974 82	$ 1,004 07	$ 1,004 07	$ 1,004 07	$ 1,004 07
Sightline	OS 2200 Interface Agent - System Log, SWG60	$ 1,007 11	$ 1,037 32	$ 1,068 44	$ 1,100 50	$ 1,133 51	$ 1,167 52	$ 1,202 54	$ 1,202 54	$ 1,202 54	$ 1,202 54
Sightline	OS 2200 Interface Agent - System Log, SWG80	$ 1,168 44	$ 1,203 50	$ 1,239 60	$ 1,276 79	$ 1,315 09	$ 1,354 55	$ 1,395 18	$ 1,395 18	$ 1,395 18	$ 1,395 18
Sightline	OS 2200 Interface Agent - System Log, SWG130	$ 1,623 11	$ 1,671 80	$ 1,721 96	$ 1,773 62	$ 1,826 83	$ 1,881 63	$ 1,938 08	$ 1,938 08	$ 1,938 08	$ 1,938 08
Sightline	OS 2200 Interface Agent - System Log, SWG140	$ 1,867 56	$ 1,923 58	$ 1,981 29	$ 2,040 73	$ 2,101 95	$ 2,165 01	$ 2,229 96	$ 2,229 96	$ 2,229 96	$ 2,229 96
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG20	$ 679 56	$ 699 94	$ 720 94	$ 742 57	$ 764 85	$ 787 79	$ 811 42	$ 811 42	$ 811 42	$ 811 42
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG40	$ 840 89	$ 866 12	$ 892 10	$ 918 86	$ 946 43	$ 974 82	$ 1,004 07	$ 1,004 07	$ 1,004 07	$ 1,004 07
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG60	$ 1,007 11	$ 1,037 32	$ 1,068 44	$ 1,100 50	$ 1,133 51	$ 1,167 52	$ 1,202 54	$ 1,202 54	$ 1,202 54	$ 1,202 54
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG80	$ 1,168 44	$ 1,203 50	$ 1,239 60	$ 1,276 79	$ 1,315 09	$ 1,354 55	$ 1,395 18	$ 1,395 18	$ 1,395 18	$ 1,395 18

Note: The Commonwealth has established mult

Baseline Units - Volumetrics

Resource Description	Service Tier / Configuration (6)	Annual Costs									
		Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG130	$ 1,623 11	$ 1,671 80	$ 1,721 96	$ 1,773 62	$ 1,826 83	$ 1,881 63	$ 1,938 08	$ 1,938 08	$ 1,938 08	$ 1,938 08
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG140	$ 1,867 56	$ 1,923 58	$ 1,981 29	$ 2,040 73	$ 2,101 95	$ 2,165 01	$ 2,229 96	$ 2,229 96	$ 2,229 96	$ 2,229 96
Sightline	OS 2200 Power Agent, SWG20	$ 1,359 11	$ 1,399 88	$ 1,441 88	$ 1,485 14	$ 1,529 69	$ 1,575 58	$ 1,622 85	$ 1,622 85	$ 1,622 85	$ 1,622 85
Sightline	OS 2200 Power Agent, SWG40	$ 1,681 78	$ 1,732 23	$ 1,784 20	$ 1,837 72	$ 1,892 86	$ 1,949 64	$ 2,008 13	$ 2,008 13	$ 2,008 13	$ 2,008 13
Sightline	OS 2200 Power Agent, SWG60	$ 2,014 22	$ 2,074 65	$ 2,136 89	$ 2,201 00	$ 2,267 02	$ 2,335 04	$ 2,405 09	$ 2,405 09	$ 2,405 09	$ 2,405 09
Sightline	OS 2200 Power Agent, SWG80	$ 2,336 89	$ 2,407 00	$ 2,479 21	$ 2,553 58	$ 2,630 19	$ 2,709 09	$ 2,790 37	$ 2,790 37	$ 2,790 37	$ 2,790 37
Sightline	OS 2200 Power Agent, SWG130	$ 3,246 22	$ 3,343 61	$ 3,443 92	$ 3,547 23	$ 3,653 65	$ 3,763 26	$ 3,876 16	$ 3,876 16	$ 3,876 16	$ 3,876 16
Sightline	OS 2200 Power Agent, SWG140	$ 3,735 11	$ 3,847 16	$ 3,962 58	$ 4,081 46	$ 4,203 90	$ 4,330 02	$ 4,459 92	$ 4,459 92	$ 4,459 92	$ 4,459 92
Sightline	OS 2200 Torch Capacity Manager Power Agent, SWG40	$ 6,893 33	$ 7,100 13	$ 7,313 14	$ 7,532 53	$ 7,758 51	$ 7,991 26	$ 8,231 00	$ 8,231 00	$ 8,231 00	$ 8,231 00
Sightline	OS 2200 Torch Capacity Manager Power Agent, SWG60	$ 7,905 33	$ 8,142 49	$ 8,386 77	$ 8,638 37	$ 8,897 52	$ 9,164 45	$ 9,439 38	$ 9,439 38	$ 9,439 38	$ 9,439 38
Sightline	OS 2200 Torch Capacity Manager Power Agent, SWG130	$ 12,520 44	$ 12,896 06	$ 13,282 94	$ 13,681 43	$ 14,091 87	$ 14,514 63	$ 14,950 07	$ 14,950 07	$ 14,950 07	$ 14,950 07
Sightline	OS 2200 Torch Capacity Manager Power Agent, SWG140	$ 14,368 44	$ 14,799 50	$ 15,243 48	$ 15,700 79	$ 16,171 81	$ 16,656 97	$ 17,156 67	$ 17,156 67	$ 17,156 67	$ 17,156 67
Sightline	OS 2200 Torch Interface Agent - I/O TRACE, SWG40	$ 2,874 67	$ 2,960 91	$ 3,049 73	$ 3,141 23	$ 3,235 46	$ 3,332 53	$ 3,432 50	$ 3,432 50	$ 3,432 50	$ 3,432 50
Sightline	OS 2200 Torch Interface Agent - I/O TRACE, SWG60	$ 3,490 67	$ 3,595 39	$ 3,703 25	$ 3,814 35	$ 3,928 78	$ 4,046 64	$ 4,168 04	$ 4,168 04	$ 4,168 04	$ 4,168 04
Sightline	OS 2200 Torch Interface Agent - I/O TRACE, SWG130	$ 5,798 22	$ 5,972 17	$ 6,151 33	$ 6,335 87	$ 6,525 95	$ 6,721 73	$ 6,923 38	$ 6,923 38	$ 6,923 38	$ 6,923 38
Sightline	OS 2200 Torch Interface Agent - LOG, SWG40	$ 2,874 67	$ 2,960 91	$ 3,049 73	$ 3,141 23	$ 3,235 46	$ 3,332 53	$ 3,432 50	$ 3,432 50	$ 3,432 50	$ 3,432 50
Sightline	OS 2200 Torch Interface Agent - LOG, SWG60	$ 3,490 67	$ 3,595 39	$ 3,703 25	$ 3,814 35	$ 3,928 78	$ 4,046 64	$ 4,168 04	$ 4,168 04	$ 4,168 04	$ 4,168 04
Sightline	OS 2200 Torch Interface Agent - LOG, SWG130	$ 5,798 22	$ 5,972 17	$ 6,151 33	$ 6,335 87	$ 6,525 95	$ 6,721 73	$ 6,923 38	$ 6,923 38	$ 6,923 38	$ 6,923 38
Sightline	OS 2200 Torch Interface Agent - LOG, SWG140	$ 6,722 22	$ 6,923 89	$ 7,131 61	$ 7,345 55	$ 7,565 92	$ 7,792 90	$ 8,026 68	$ 8,026 68	$ 8,026 68	$ 8,026 68
Sightline	OS 2200 Torch Interface Agent - MAPPER, SWG40	$ 2,874 67	$ 2,960 91	$ 3,049 73	$ 3,141 23	$ 3,235 46	$ 3,332 53	$ 3,432 50	$ 3,432 50	$ 3,432 50	$ 3,432 50
Sightline	OS 2200 Torch Interface Agent - MAPPER, SWG60	$ 3,490 67	$ 3,595 39	$ 3,703 25	$ 3,814 35	$ 3,928 78	$ 4,046 64	$ 4,168 04	$ 4,168 04	$ 4,168 04	$ 4,168 04
Sightline	OS 2200 Torch Interface Agent - MAPPER, SWG130	$ 5,798 22	$ 5,972 17	$ 6,151 33	$ 6,335 87	$ 6,525 95	$ 6,721 73	$ 6,923 38	$ 6,923 38	$ 6,923 38	$ 6,923 38
Sightline	Windows 2000 Interface Agent - Internet Informa ion Server	$ 2,053 33	$ 2,114 93	$ 2,178 38	$ 2,243 73	$ 2,311 04	$ 2,380 38	$ 2,451 79	$ 2,451 79	$ 2,451 79	$ 2,451 79
Sightline	Windows 2000 Interface Agent - .NET	$ 4,106 67	$ 4,229 87	$ 4,356 76	$ 4,487 47	$ 4,622 09	$ 4,760 75	$ 4,903 57	$ 4,903 57	$ 4,903 57	$ 4,903 57
Sightline	Windows 2000 Interface Agent - SQL Server	$ 3,911 11	$ 4,028 44	$ 4,149 30	$ 4,273 78	$ 4,401 99	$ 4,534 05	$ 4,670 07	$ 4,670 07	$ 4,670 07	$ 4,670 07
Sightline	Windows 2000 Power Agent Upto 32 CPU's	$ 9,680 00	$ 9,970 40	$ 10,269 51	$ 10,577 60	$ 10,894 93	$ 11,221 77	$ 11,558 43	$ 11,558 43	$ 11,558 43	$ 11,558 43
SMA	OpCon/xps EXEC LSAM, Group 3	$ 3,898 57	$ 4,004 46	$ 4,113 53	$ 4,225 87	$ 4,341 58	$ 4,460 76	$ 4,583 52	$ 4,583 52	$ 4,583 52	$ 4,583 52
SMA	OpCon/xps EXEC LSAM, Group 12	$ 23,804 81	$ 24,451 40	$ 25,117 37	$ 25,803 33	$ 26,509 87	$ 27,237 60	$ 27,987 17	$ 27,987 17	$ 27,987 17	$ 27,987 17
SMA	OpCon/xps EXEC LSAM Development, Group 2	$ 1,307 16	$ 1,342 66	$ 1,379 23	$ 1,416 90	$ 1,455 70	$ 1,495 66	$ 1,536 82	$ 1,536 82	$ 1,536 82	$ 1,536 82
SMA	OpCon/xps EXEC LSAM Development, Group 12	$ 11,901 82	$ 12,225 09	$ 12,558 07	$ 12,901 03	$ 13,254 28	$ 13,618 13	$ 13,992 89	$ 13,992 89	$ 13,992 89	$ 13,992 89
SMA	OpCon/xps Production SAM	$ 4,173 98	$ 4,287 35	$ 4,404 12	$ 4,524 40	$ 4,648 28	$ 4,775 89	$ 4,907 32	$ 4,907 32	$ 4,907 32	$ 4,907 32

Baseline Units - Volumetrics

Note: The Commonwealth has established mult

Annual Costs

Resource Description	Service Tier / Configuration (6)	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
SMA	OpCon/xps Starter Kit	$ 7,151 19	$ 7,345 43	$ 7,545 50	$ 7,751 57	$ 7,963 82	$ 8,182 43	$ 8,407 61	$ 8,407 61	$ 8,407 61	$ 8,407 61
SMA	OpCon/xps User Interface	$ 1,119 32	$ 1,149 72	$ 1,181 04	$ 1,213 29	$ 1,246 51	$ 1,280 73	$ 1,315 98	$ 1,315 98	$ 1,315 98	$ 1,315 98
Sybase	EAServer Deploy Advanced - Active	$ 3,584 53	$ 3,692 07	$ 3,802 83	$ 3,916 92	$ 4,034 42	$ 4,155 46	$ 4,280 12	$ 4,280 12	$ 4,280 12	$ 4,280 12
Sybase	EAServer Deploy Advanced - Passive	$ 897 40	$ 924 33	$ 952 06	$ 980 62	$ 1,010 04	$ 1,040 34	$ 1,071 55	$ 1,071 55	$ 1,071 55	$ 1,071 55
Symantec	Backup Exec System Recovery Server	$ 966 26	$ 995 25	$ 1,025 10	$ 1,055 86	$ 1,087 53	$ 1,120 16	$ 1,153 76	$ 1,153 76	$ 1,153 76	$ 1,153 76
Symantec	EndPoint Protection	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	Ghost Solution Suite	$ 197 08	$ 203 00	$ 209 09	$ 215 36	$ 221 82	$ 228 47	$ 235 33	$ 235 33	$ 235 33	$ 235 33
Symantec	NetBackup Client Application and Database Pack, UNX, Tier 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Client Application and Database Pack, UNX, Tier 4	$ 4,203 51	$ 4,329 62	$ 4,459 50	$ 4,593 29	$ 4,731 09	$ 4,873 02	$ 5,019 21	$ 5,019 21	$ 5,019 21	$ 5,019 21
Symantec	NetBackup Client Application and Database Pack, WIN, Tier 2	$ 2,268 06	$ 2,336 10	$ 2,406 19	$ 2,478 37	$ 2,552 72	$ 2,629 30	$ 2,708 18	$ 2,708 18	$ 2,708 18	$ 2,708 18
Symantec	NetBackup Client Application and Database Pack, WIN, Tier 3	$ 8,391 73	$ 8,643 48	$ 8,902 79	$ 9,169 87	$ 9,444 96	$ 9,728 31	$ 10,020 16	$ 10,020 16	$ 10,020 16	$ 10,020 16
Symantec	NetBackup Client Application and Database Pack, WIN, Tier 4	$ 629 86	$ 648 75	$ 668 22	$ 688 26	$ 708 91	$ 730 18	$ 752 08	$ 752 08	$ 752 08	$ 752 08
Symantec	NetBackup Enterprise Client, UNX, Tier 4	$ 2,598 76	$ 2,676 72	$ 2,757 02	$ 2,839 73	$ 2,924 93	$ 3,012 67	$ 3,103 06	$ 3,103 06	$ 3,103 06	$ 3,103 06
Symantec	NetBackup Enterprise Client, WIN, Tier 1	$ 1,488 15	$ 1,532 79	$ 1,578 77	$ 1,626 14	$ 1,674 92	$ 1,725 17	$ 1,776 92	$ 1,776 92	$ 1,776 92	$ 1,776 92
Symantec	NetBackup Enterprise Client, WIN, Tier 2	$ 5,916 26	$ 6,093 75	$ 6,276 56	$ 6,464 86	$ 6,658 81	$ 6,858 57	$ 7,064 33	$ 7,064 33	$ 7,064 33	$ 7,064 33
Symantec	NetBackup Enterprise Client, WIN, Tier 3	$ 14,090 08	$ 14,512 78	$ 14,948 16	$ 15,396 61	$ 15,858 50	$ 16,334 26	$ 16,824 29	$ 16,824 29	$ 16,824 29	$ 16,824 29
Symantec	NetBackup Enterprise Server, WIN, Tier 2	$ 3,154 07	$ 3,248 69	$ 3,346 15	$ 3,446 53	$ 3,549 93	$ 3,656 43	$ 3,766 12	$ 3,766 12	$ 3,766 12	$ 3,766 12
Symantec	NetBackup Enterprise Server, WIN, Tier 3	$ 24,467 91	$ 25,201 95	$ 25,958 01	$ 26,736 75	$ 27,538 85	$ 28,365 02	$ 29,215 97	$ 29,215 97	$ 29,215 97	$ 29,215 97
Symantec	NetBackup Library Based Tape Drive Option, XPLAT	$ 29,246 80	$ 30,124 20	$ 31,027 93	$ 31,958 77	$ 32,917 53	$ 33,905 06	$ 34,922 21	$ 34,922 21	$ 34,922 21	$ 34,922 21
Symantec	NetBackup Media Server Encryption Option (MSEO) WIN, Tier 2	$ 1,148 84	$ 1,183 31	$ 1,218 81	$ 1,255 37	$ 1,255 37	$ 1,255 37	$ 1,255 37	$ 11,822 09	$ -	$ -
Symantec	NetBackup Platform Base, XPLAT (per Terabyte)	$ 155,313 89	$ 159,973 31	$ 164,772 50	$ 169,715 68	$ 174,807 15	$ 180,051 36	$ 185,452 91	$ 185,452 91	$ 185,452 91	$ 185,452 91
Symantec	NetBackup Shared Storage Option, XPLAT	$ 21,409 42	$ 22,051 70	$ 22,713 26	$ 23,394 65	$ 24,096 49	$ 24,819 39	$ 25,563 97	$ 25,563 97	$ 25,563 97	$ 25,563 97
Symantec	NetBackup Standard Client, XPLAT	$ 15,127 09	$ 15,580 91	$ 16,048 33	$ 16,529 79	$ 17,025 68	$ 17,536 45	$ 18,062 54	$ 18,062 54	$ 18,062 54	$ 18,062 54
Symantec	NetBackup Vault Additional Drive Option, XPLAT	$ 2,293 87	$ 2,362 68	$ 2,433 56	$ 2,506 57	$ 2,581 77	$ 2,659 22	$ 2,739 00	$ 2,739 00	$ 2,739 00	$ 2,739 00
Symantec	NetBackup Vault Base Option, XPLAT (4 tape drives per license)	$ 11,469 33	$ 11,813 41	$ 12,167 82	$ 12,532 85	$ 12,908 84	$ 13,296 10	$ 13,694 98	$ 13,694 98	$ 13,694 98	$ 13,694 98
Symantec	Veritas NetBackup Enterprise Server License, Tier 3	$ 1,529 24	$ 1,575 12	$ 1,622 38	$ 1,671 05	$ 1,721 18	$ 1,772 81	$ 1,826 00	$ 1,826 00	$ 1,826 00	$ 1,826 00
Symantec	Veritas NetBackup Windows Client, Tier 4	$ 1,259 72	$ 1,297 51	$ 1,336 43	$ 1,376 52	$ 1,417 82	$ 1,460 36	$ 1,504 17	$ 1,504 17	$ 1,504 17	$ 1,504 17
Tone Software Corp.	Dynastep	$ 17,653 78	$ 18,183 39	$ 18,728 89	$ 19,290 76	$ 19,869 48	$ 20,465 57	$ 21,079 53	$ 21,079 53	$ 21,079 53	$ 21,079 53
Unicon Group Ltd.	LOUIS II LCOM Host Module	$ 667 33	$ 687 35	$ 707 97	$ 729 21	$ 751 09	$ 773 62	$ 796 83	$ 796 83	$ 796 83	$ 796 83
Unicon Group Ltd.	LOUIS II Extract & Reporting Module	$ 10,721 33	$ 11,042 97	$ 11,374 26	$ 11,715 49	$ 12,066 96	$ 12,428 96	$ 12,801 83	$ 12,801 83	$ 12,801 83	$ 12,801 83
Unicon Group Ltd.	LOUIS II DERIVE Option	$ 1,498 44	$ 1,543 40	$ 1,589 70	$ 1,637 39	$ 1,686 51	$ 1,737 11	$ 1,789 22	$ 1,789 22	$ 1,789 22	$ 1,789 22
Unicon Group Ltd.	LOUIS II DMS Interface	$ 1,334 67	$ 1,374 71	$ 1,415 95	$ 1,458 43	$ 1,502 18	$ 1,547 24	$ 1,593 66	$ 1,593 66	$ 1,593 66	$ 1,593 66
Unicon Group Ltd.	LOUIS II RDMS Interface	$ 1,334 67	$ 1,374 71	$ 1,415 95	$ 1,458 43	$ 1,502 18	$ 1,547 24	$ 1,593 66	$ 1,593 66	$ 1,593 66	$ 1,593 66
Unicon Group Ltd.	LOUIS II RELATE Option	$ 2,138 89	$ 2,203 06	$ 2,269 15	$ 2,337 22	$ 2,407 34	$ 2,479 56	$ 2,553 95	$ 2,553 95	$ 2,553 95	$ 2,553 95
VanDyke Technologies	VShell Workgroup Server	$ 702 53	$ 723 61	$ 745 32	$ 767 68	$ 790 71	$ 814 43	$ 838 86	$ 838 86	$ 838 86	$ 838 86
Veeam	nWorks ESX Monitoring for SCOM	$ 4,950 68	$ 5,099 20	$ 5,252 18	$ 5,409 75	$ 5,572 04	$ 5,739 20	$ 5,911 38	$ 5,911 38	$ 5,911 38	$ 5,911 38
Veeam	nWorks Management Pack for VMWare	$ 115,103 41	$ 118,556 52	$ 122,113 21	$ 125,776 61	$ 129,549 91	$ 133,436 40	$ 137,439 50	$ 137,439 50	$ 137,439 50	$ 137,439 50
VMware, Inc.	VMware vSphere 4 Enterprise Plus for 1 Processor	$ 3,520 00	$ 3,625 60	$ 3,734 37	$ 3,846 40	$ 3,961 79	$ 4,080 64	$ 4,203 06	$ 4,203 06	$ 4,203 06	$ 4,203 06

Note: The Commonwealth has established mult

Baseline Units - Volumetrics

		Annual Costs									
Resource Description	**Service Tier / Configuration (6)**	**Year 1**	**Year 2**	**Year 3**	**Year 4**	**Year 5**	**Year 6**	**Year 7**	**Opt - Year 8**	**Opt - Year 9**	**Opt - Year 10**
VMware, Inc.	VMware vSphere 5 Enterprise Plus for 1 Processor	$ 14,080 00	$ 14,502 40	$ 14,937 47	$ 15,385 60	$ 15,847 16	$ 16,322 58	$ 16,812 26	$ 16,812 26	$ 16,812 26	$ 16,812 26
Western American Data	Rlist	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Winternals	Winternals Administrator's Pak	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
WinZip Computing	Winzip	$ 182 44	$ 187 91	$ 193 55	$ 199 36	$ 205 34	$ 211 50	$ 217 84	$ 217 84	$ 217 84	$ 217 84
XtremeSoft	AppMetrics	$ 16,500 00	$ 16,995 00	$ 17,504 85	$ 18,030 00	$ 18,570 90	$ 19,128 02	$ 19,701 86	$ 19,701 86	$ 19,701 86	$ 19,701 86
USPS	Correct Address	$ 11,977 78	$ 12,337 11	$ 12,707 22	$ 13,088 44	$ 13,481 09	$ 13,885 53	$ 14,302 09	$ 14,302 09	$ 14,302 09	$ 14,302 09
IBM	FileNet	$ 798 11	$ 180 85	$ 186 28	$ 191 87	$ 197 62	$ 203 55	$ 209 66	$ 209 66	$ 209 66	$ 209 66
Microsoft	SharePoint (with SA)	$ 19,853 87	$ 20,449 48	$ 21,062 97	$ 21,694 86	$ 22,345 70	$ 23,016 07	$ 23,706 56	$ 23,706 56	$ 23,706 56	$ 23,706 56
IBM	WebSphere MQ (Procesor Value Unit)	$ 137 00	$ 31 04	$ 31 98	$ 32 93	$ 33 92	$ 34 94	$ 35 99	$ 35 99	$ 35 99	$ 35 99
Xerox	XeroxDocuShare	$ 625 00	$ 638 75	$ 652 91	$ 667 50	$ 682 52	$ 698 00	$ 713 94	$ 713 94	$ 713 94	$ 713 94
Hybrid Third Party Software											
Vendor	**Product**										
Computer Associates Interna ional, Inc.	CA 90's Services (freeware)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates Interna ional, Inc.	Vision Builder	$ 277,666 94	$ 285,996 95	$ 294,576 86	$ 303,414 16	$ 312,516 59	$ 321,892 08	$ 331,548 85	$ 341,495 31	$ 351,740 17	$ 362,292 38
Computer Associates Interna ional, Inc.	Easytrieve Plus	$ 397,891 42	$ 409,828 16	$ 422,123 01	$ 434,786 70	$ 447,830 30	$ 461,265 21	$ 475,103 17	$ 489,356 26	$ 504,036 95	$ 519,158 06
Computer Associates Interna ional, Inc.	Easytrieve Plus MVS	$ 223,451 47	$ 230,155 01	$ 237,059 66	$ 244,171 45	$ 251,496 59	$ 259,041 49	$ 266,812 74	$ 274,817 12	$ 283,061 63	$ 291,553 48
Computer Associates Interna ional, Inc.	Easytrieve Plus IMS	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates Interna ional, Inc.	Easytrieve Plus IMS Option MVS	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates Interna ional, Inc.	Easytrieve Plus DB2 OPT	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates Interna ional, Inc.	Easytrieve Plus DB2 Option MVS	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates Interna ional, Inc.	Endevor/MVS Automated Configuration Mgr MVS	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates Interna ional, Inc.	Endevor/MVS External Security Int. MVS	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates Interna ional, Inc.	Endevor/MVS MVS	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates Interna ional, Inc.	Endevor/MVS Extended Processor	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates Interna ional, Inc.	CA-Librarian	$ 333,893 78	$ 343,910 60	$ 354,227 91	$ 364,854 75	$ 375,800 39	$ 387,074 41	$ 398,686 64	$ 410,647 24	$ 422,966 65	$ 435,655 65
Computer Associates Interna ional, Inc.	CA-META COBOL	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates Interna ional, Inc.	Panvalet	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates Interna ional, Inc.	Panvalet ISPF	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates Interna ional, Inc.	SORT (INCL DART)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates Interna ional, Inc.	SRAM	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
dotJ Software Inc.	dotJ Custom Tag Library	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Formula Consultants, Inc.	Star 1100	$ 7,128 00	$ 7,341 84	$ 7,562 10	$ 7,788 96	$ 8,022 63	$ 8,263 31	$ 8,511 20	$ 8,511 20	$ 8,511 20	$ 8,511 20
Idea Integration	XGEN	$ 39,601 83	$ 40,789 89	$ 42,013 58	$ 43,273 99	$ 44,572 21	$ 45,909 38	$ 47,286 66	$ 47,286 66	$ 47,286 66	$ 47,286 66
Informatica Corporation	Change DataMove for DB2 Source	$ 202,705 60	$ 208,786 77	$ 215,050 37	$ 221,501 88	$ 228,146 94	$ 234,991 35	$ 242,041 09	$ 249,302 32	$ 256,781 39	$ 264,484 83
Informatica Corporation	DataMove for DB2 Source	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	Change DataMove	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	DataMove for IMS Source	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	Change DataMove for IMS Source	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	DataMove	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	Change DataMove DB2 Target	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	DataMove DB2 Target	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	Change DataMove/DataMove Target for UDB	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	SSA - Name 3	$ 64,166 67	$ 66,091 67	$ 68,074 42	$ 70,116 65	$ 72,220 15	$ 74,386 75	$ 76,618 36	$ 76,618 36	$ 76,618 36	$ 76,618 36
KMSYS Worldwide, Inc.	IQU Plus-1	$ 29,333 33	$ 30,213 33	$ 31,119 73	$ 32,053 33	$ 33,014 93	$ 34,005 37	$ 35,025 53	$ 35,025 53	$ 35,025 53	$ 35,025 53

Note: The Commonwealth has established mult

Baseline Units - Volumetrics

Resource Description	Service Tier / Configuration (6)	Annual Costs Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
KMSYS Worldwide, Inc.	IQU Reorg Composer	$ 4,155 56	$ 4,280 22	$ 4,408 63	$ 4,540 89	$ 4,677 11	$ 4,817 43	$ 4,961 95	$ 4,961 95	$ 4,961 95	$ 4,961 95
KMSYS Worldwide, Inc.	QPLXSS	$ 4,170 83	$ 4,295 96	$ 4,424 84	$ 4,557 58	$ 4,694 31	$ 4,835 14	$ 4,980 19	$ 4,980 19	$ 4,980 19	$ 4,980 19
KMSYS Worldwide, Inc.	QPLXSV	$ 1,031 25	$ 1,062 19	$ 1,094 05	$ 1,126 87	$ 1,160 68	$ 1,195 50	$ 1,231 37	$ 1,231 37	$ 1,231 37	$ 1,231 37
KMSYS Worldwide, Inc.	QPLXV	$ 916 67	$ 944 17	$ 972 49	$ 1,001 67	$ 1,031 72	$ 1,062 67	$ 1,094 55	$ 1,094 55	$ 1,094 55	$ 1,094 55
Marble Computer Inc.	OS DCD III Data Correlation and Documenta ion System	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	SQL Server Enterprise	$ 2,538 80	$ 2,614 96	$ 2,693 41	$ 2,774 22	$ 2,857 44	$ 2,943 17	$ 3,031 46	$ 3,031 46	$ 3,031 46	$ 3,031 46
SAS Institute, Inc.	Base SAS	$ 851,806 88	$ 877,361 08	$ 903,681 92	$ 930,792 37	$ 958,716 14	$ 987,477 63	$ 1,017,101 96	$ 1,047,615 02	$ 1,079,043 47	$ 1,111,414 77
SAS Institute, Inc.	SAS/ACCESS Interface for IMS	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SAS Institute, Inc.	SAS/ACCESS DB2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SAS Institute, Inc.	SAS/AF	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SAS Institute, Inc.	SAS/FSP	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SAS Institute, Inc.	SAS/GRAPH	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SAS Institute, Inc.	SAS/SHARE	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SAS Institute, Inc.	SAS/STAT	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Schema Systems Limited	Q Editor Plus One	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SMA	OpCon/xps EXEC LSAM, Group 3	$ 3,558 45	$ 3,665 20	$ 3,775 15	$ 3,888 41	$ 4,005 06	$ 4,125 21	$ 4,248 97	$ 4,248 97	$ 4,248 97	$ 4,248 97
SMA	OpCon/xps EXEC LSAM, Group 8	$ 12,931 20	$ 13,319 13	$ 13,718 71	$ 14,130 27	$ 14,554 18	$ 14,990 80	$ 15,440 53	$ 15,440 53	$ 15,440 53	$ 15,440 53
SMA	OpCon/xps EXEC LSAM, Group 14	$ 33,401 43	$ 34,403 47	$ 35,435 57	$ 36,498 64	$ 37,593 60	$ 38,721 41	$ 39,883 05	$ 39,883 05	$ 39,883 05	$ 39,883 05
SMA	OpCon/xps Microsoft LSAM	$ 5,411 30	$ 5,573 64	$ 5,740 85	$ 5,913 08	$ 6,090 47	$ 6,273 18	$ 6,461 38	$ 6,461 38	$ 6,461 38	$ 6,461 38
SMA	OpCon/xps User Interface	$ 894 20	$ 921 02	$ 948 65	$ 977 11	$ 1,006 43	$ 1,036 62	$ 1,067 72	$ 1,067 72	$ 1,067 72	$ 1,067 72
Sybase	EAServer Deploy Advanced - Active	$ 3,584 53	$ 3,692 07	$ 3,802 83	$ 3,916 92	$ 4,034 42	$ 4,155 46	$ 4,280 12	$ 4,280 12	$ 4,280 12	$ 4,280 12
Sybase	EAServer Deploy Advanced - Passive	$ 897 40	$ 924 33	$ 952 06	$ 980 62	$ 1,010 04	$ 1,040 34	$ 1,071 55	$ 1,071 55	$ 1,071 55	$ 1,071 55
TRILOGexport, Inc.	TriTune Automation Component (APC)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unicon Group Ltd.	LOUIS II Database Gateway	$ 21,442 67	$ 22,085 95	$ 22,748 53	$ 23,430 98	$ 24,133 91	$ 24,857 93	$ 25,603 67	$ 25,603 67	$ 25,603 67	$ 25,603 67
Unicon Group Ltd.	LOUIS II DMS Interface	$ 4,004 00	$ 4,124 12	$ 4,247 84	$ 4,375 28	$ 4,506 54	$ 4,641 73	$ 4,780 99	$ 4,780 99	$ 4,780 99	$ 4,780 99
Unicon Group Ltd.	LOUIS II Extract & Reporting Module	$ 10,721 33	$ 11,042 97	$ 11,374 26	$ 11,715 49	$ 12,066 96	$ 12,428 96	$ 12,801 83	$ 12,801 83	$ 12,801 83	$ 12,801 83
Unicon Group Ltd.	LOUIS II LCOM Host Module	$ 2,002 00	$ 2,062 06	$ 2,123 92	$ 2,187 64	$ 2,253 27	$ 2,320 87	$ 2,390 49	$ 2,390 49	$ 2,390 49	$ 2,390 49
Unicon Group Ltd.	LOUIS II MAPPER Interface	$ -	$ 1,334 67	$ 1,374 71	$ 1,415 95	$ 1,458 43	$ 1,502 18	$ 1,547 24	$ 1,593 66	$ 1,593 66	$ 1,593 66
Unicon Group Ltd.	LOUIS II RDMS Interface	$ 4,004 00	$ 4,004 00	$ 4,124 12	$ 4,247 84	$ 4,375 28	$ 4,506 54	$ 4,641 73	$ 4,780 99	$ 4,780 99	$ 4,780 99
Verisign	Secure Site Pro SSL	$ 2,211 11	$ 2,345 77	$ 2,416 14	$ 2,488 63	$ 2,563 28	$ 2,640 18	$ 2,719 39	$ 2,719 39	$ 2,719 39	$ 2,719 39
Western American Data	Rlist	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
WinZip	Self-Extractor 10-user license	$ 15 74	$ 15 74	$ 16 21	$ 16 70	$ 17 20	$ 17 72	$ 18 25	$ 18 80	$ 18 80	$ 18 80
Total Third Party Software		**$ 6,605,259.98**	**$ 6,854,771.37**	**$ 7,059,637.65**	**$ 7,270,649.95**	**$ 7,487,955.00**	**$ 7,711,779.02**	**$ 7,942,317.95**	**$ 8,078,208.94**	**$ 8,195,279.07**	**$ 8,328,038.08**

Datacenter Architecture Charges

Description	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Total Base Term	Opt - Year 8	Opt - Year 8	Opt - Year 10	Total Opt Years	Total Base Term + Opt Years
DC Architecture Charges - One Time Startup (a)													
Data Center Network Setup	$80,796 70	$0 00	$0 00					**$80,796.70**				**$0.00**	**$80,796.70**
Data Center Security (Firewall/IDS) Setup	$0 00	$0 00	$0 00					**$0.00**				**$0.00**	**$0.00**
Internet Setup	$0 00	$0 00	$0 00					**$0.00**				**$0.00**	**$0.00**
Capacity on Demand Server Base Infrastructure	$0 00	$0 00	$0 00					**$0.00**				**$0.00**	**$0.00**
Capacity on Demand Storage Base Infrastructure	$0 00	$0 00	$0 00					**$0.00**				**$0.00**	**$0.00**
Enterprise Systems Management	$113,296 30	$0 00	$0 00					**$113,296.30**				**$0.00**	**$113,296.30**
Data Center Facility Management	$9,403,289 08	$1,128,107 08	$293,930 96					**$10,825,327.12**				**$0.00**	**$10,825,327.12**
IT Service Management Platform	$2,749,476 17	$0 00	$0 00					**$2,749,476.17**				**$0.00**	**$2,749,476.17**
Mainframe Managed Services Base Infrastructure	$121,970 20	$0 00	$0 00					**$121,970.20**				**$0.00**	**$121,970.20**
Server Managed Services Base Infrastructure	$299,549 98	$0 00	$0 00					**$299,549.98**				**$0.00**	**$299,549.98**
Storage Managed Services Base Infrastructure	$2,790,562 78	$0 00	$0 00					**$2,790,562.78**				**$0.00**	**$2,790,562.78**
Program Management Office and Office Space	$51,844 55	$0 00	$0 00					**$51,844.55**				**$0.00**	**$51,844.55**
Security Services	$1,893,193 53	$293,253 88	$51,493 74					**$2,237,941.15**				**$0.00**	**$2,237,941.15**
Service Desk	$401,035 87	$0 00	$0 00					**$401,035.87**				**$0.00**	**$401,035.87**
Service Portal - Operational Dashboard & Reporting	$56,255 53	$0 00	$0 00					**$56,255.53**				**$0.00**	**$56,255.53**
Service Portal - Service Catalog	$691,048 01	$0 00	$0 00					**$691,048.01**				**$0.00**	**$691,048.01**
Service Portal - Base Services Portal	$0 00	$0 00	$0 00					**$0.00**				**$0.00**	**$0.00**
Technical Services - DR Planning & Testing	$125,477 28	$0 00	$0 00					**$125,477.28**				**$0.00**	**$125,477.28**
Data Center Utilities	$0 00	$0 00	$0 00					**$0.00**				**$0.00**	**$0.00**
Other (insert description)								**$0.00**				**$0.00**	**$0.00**
One Time Datacenter Startup Total	*$18,777,795.99*	*$1,421,360.96*	*$345,424.70*	*$0.00*	*$0.00*	*$0.00*	*$0.00*	***$20,544,581.65***	*$0.00*	*$0.00*	*$0.00*	***$0.00***	***$20,544,581.65***
DC Architecture Charges - Monthly Reccuring (c)													
Data Center Network (WAN) recurring	$152,640 43	$149,338 70	$148,258 03	$141,994 68	$141,145 17	$139,980 23	$139,193 94	**$1,012,551.17**	$139,193 94	$139,193 94	$139,193 94	**$417,581.81**	**$1,430,132.98**
Data Center Security (Firewall/IDS Management)	$67,567 60	$67,179 45	$67,783 19	$68,447 63	$69,164 50	$69,736 68	$70,508 17	**$480,387.21**	$70,508 17	$70,508 17	$70,508 17	**$211,524.50**	**$691,911.71**
Internet Recurring Charges	$30,443 42	$16,674 98	$16,551 68	$16,425 03	$16,311 64	$16,188 47	$16,081 46	**$128,676.69**	$15,646 33	$15,192 28	$14,794 98	**$45,633.59**	**$174,310.28**
Capacity on Demand Server Base Infrastructure	$1,108 21	$1,683 67	$1,683 67	$1,683 67	$2,166 36	$2,014 33	$1,977 73	**$12,317.64**	$1,977 73	$1,977 73	$1,977 73	**$5,933.19**	**$18,250.82**
Capacity on Demand Storage Base Infrastructure	$636 80	$636 80	$636 80	$636 80	$636 80	$636 80	$636 80	**$4,457.62**	$636 80	$636 80	$636 80	**$1,910.41**	**$6,368.03**
Enterprise Systems Management	$144,593 69	$104,805 68	$101,759 18	$100,958 98	$100,378 23	$103,442 06	$107,064 64	**$763,002.47**	$106,534 91	$106,043 02	$106,497 08	**$319,075.02**	**$1,082,077.48**
Data Center Facility Management	$821,614 96	$1,405,912 65	$1,532,625 37	$1,573,764 83	$1,603,861 91	$1,634,713 94	$1,666,343 13	**$10,238,836.79**	$1,666,343 13	$1,666,343 13	$1,666,343 13	**$4,999,029.39**	**$15,237,866.18**
IT Service Management Platform	$195,628 03	$295,250 97	$299,459 42	$283,835 75	$288,706 79	$272,969 96	$278,530 37	**$1,914,381.27**	$279,116 86	$279,618 21	$280,233 07	**$838,968.13**	**$2,753,349.41**
Mainframe Managed Services Base Infrastructure	$248,417 21	$201,852 37	$207,325 93	$210,542 04	$215,969 00	$249,948 05	$223,730 64	**$1,557,785.24**	$222,330 64	$221,469 84	$219,417 15	**$663,217.63**	**$2,221,002.86**
Server Managed Services Base Infrastructure	$369,650 40	$361,056 76	$396,796 35	$428,288 99	$459,407 89	$327,194 10	$347,806 78	**$2,690,201.27**	$384,954 34	$423,835 05	$436,295 74	**$1,245,085.14**	**$3,935,286.40**
Storage Managed Services Base Infrastructure	$351,473 65	$334,253 04	$358,351 15	$381,405 74	$408,957 57	$961,828 43	$464,605 20	**$3,260,874.78**	$463,801 15	$463,432 24	$462,145 76	**$1,389,379.15**	**$4,650,253.93**
Program Management Office and Office Space	$272,525 04	$1,127,819 27	$1,164,786 18	$1,229,880 01	$1,253,143 29	$1,275,615 57	$1,300,584 24	**$7,624,353.61**	$1,302,797 75	$1,304,349 09	$1,306,808 54	**$3,913,955.38**	**$11,538,308.98**
Security Services	$387,356 95	$400,418 42	$428,209 19	$439,372 87	$449,719 23	$467,132 49	$470,482 78	**$3,042,691.92**	$470,605 75	$470,359 81	$470,624 67	**$1,411,590.23**	**$4,454,282.14**
Service Desk	$43,100 07	$84,568 37	$84,902 90	$86,203 54	$86,966 14	$85,803 21	$87,812 69	**$559,356.92**	$87,812 69	$87,812 69	$87,812 69	**$263,438.08**	**$822,795.00**
Service Portal - Operational Dashboard & Reporting	$7,821 11	$4,571 13	$4,760 76	$4,862 94	$5,108 37	$4,611 27	$4,949 88	**$36,685.45**	$4,949 88	$4,949 88	$4,949 88	**$14,849.63**	**$51,535.08**
Service Portal - Service Catalog	$67,368 48	$76,500 28	$78,970 60	$81,584 14	$84,332 76	$87,013 15	$90,649 53	**$566,418.93**	$91,661 68	$92,494 11	$93,563 02	**$277,718.82**	**$844,137.74**
Service Portal - Base Services Portal	$5,936 45	$6,430 38	$6,397 15	$6,375 28	$6,342 73	$6,323 00	$6,291 08	**$44,096.07**	$6,291 08	$6,291 08	$6,291 08	**$18,873.24**	**$62,969.31**
Technical Services - DR Planning & Testing	$31,497 44	$27,381 72	$27,547 43	$27,740 13	$28,067 37	$28,632 22	$29,493 30	**$200,359.60**	$29,531 13	$29,521 67	$29,587 89	**$88,640.70**	**$289,000.30**
Data Center Utilities	$293,154 28	$632,165 30	$646,491 02	$661,174 79	$676,224 23	$691,630 58	$707,434 64	**$4,308,274.84**	$707,434 64	$707,434 64	$707,434 64	**$2,122,303.91**	**$6,430,578.75**
Other (insert description)								**$0.00**				**$0.00**	**$0.00**
DC Architecture Charges - Monthly Reccuring Total	*$3,492,534.23*	*$5,298,499.92*	*$5,573,295.98*	*$5,745,177.84*	*$5,896,609.97*	*$6,425,414.55*	*$6,014,176.99*	*$38,445,709.47*	*$6,052,128.60*	*$6,091,463.36*	*$6,105,115.94*	*$18,248,707.90*	*$56,694,417.37*
DC Architecture Charges - Yearly Reccuring Total	*$41,910,410.71*	*$63,581,999.03*	*$66,879,551.70*	*$68,942,134.08*	*$70,759,319.61*	*$77,104,974.61*	*$72,170,123.86*	***$461,348,513.60***	*$72,625,543.24*	*$73,097,560.35*	*$73,261,391.23*	***$218,984,494.82***	***$680,333,008.42***
DC Architecture Charges - Yearly Totals	**$60,688,206.69**	**$65,003,359.99**	**$67,224,976.41**	**$68,942,134.08**	**$70,759,319.61**	**$77,104,974.61**	**$72,170,123.86**	**$481,893,095.25**	**$72,625,543.24**	**$73,097,560.35**	**$73,261,391.23**	**$218,984,494.82**	**$700,877,590.07**

Notes:
(a) Enter initial setup charges in the appropriate year when they occcur
(b) Enter additional items as needed
(c) Enter Monthly Recurring Charge within each approapriate year

(a) Transition Charges

Milestone Number	Transition Milestone	Cost
M-1	Key Staffing	$ 2,379,908.78
M-2	Contract Management Plan	$ 1,318,811.12
M-3	Staffing	$ 6,706,666.96
M-4	Datacenter Architecture Plan and Roadmap	$ 3,532,760.78
M-5	Data Gathering	$ 3,436,691.42
M-6	Detailed Transition Plan	$ 2,455,038.41
M-7	Commonwealth Compute Process Manual (CCPM)	$ 4,685,754.82
M-8	Network Connectivity	$ 879,329.54
M-9	Security	$ 6,505,835.86
M-10	ITSM System Integration	$ 2,549,611.31
M-11	Financial Management	$ 2,265,872.16
M-12	Operational Readiness	$ 4,371,379.27
M-13	SSAE 16 Audit of EDC	$ 4,238,497.24
M-14 (A)	DPH Transition Completed	$ 18,632,155.38
M-14 (B)	DPH Transition Completed	$ -
M-15	EDC Operational Transition Completed	$ 5,194,813.81
M-16	Department of Labor and Industry Datacenter Transition Completed	$ 955,537.27
M-17	Department of Revenue Datacenter Transition Completed	$ 672,221.65
M-18	Pennsylvania State Police Datacenter Transition Completed	$ 949,747.23
M-19	Department of Public Welfare Datacenter Transition Completed	$ 608,739.51
M-20	Department of Health Datacenter Transition Completed	$ 808,552.21
	Total Transition Costs	$ 73,147,924.76

(a) Transition Milestone Acceptance Criteria/Deliverables are described in Schedule D - Transition Milestones

Total Charges

Description	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Total Base Term	Opt - Year 8	Opt - Year 9	Opt - Year 10
Total Charges Summary											
Datacenter Architecture Charges											
DC Architecture Charges - Yearly Totals	$60,688,206 69	$65,003,359 99	$67,224,976 41	$68,942,134 08	$70,759,319 61	$77,104,974 61	$72,170,123 86	$481,893,095 25	$72,625,543 24	$73,097,560 35	$73,261,391 23
Server - Fully Managed											
Total - Fully Managed - x86 Physical - All Support Tiers (Window, Linux)	$13,482,341 69	$12,603,615 14	$11,756,854 67	$10,986,439 30	$10,298,869 52	$9,618,064 00	$9,163,103 91	$77,909,288 25	$8,731,004 34	$8,285,692 64	$8,121,756 51
Total - Fully Managed - x86 Virtual - All Support Tiers (Window, Linux)	$5,024,506 75	$5,043,322 25	$5,191,418 76	$5,337,261 04	$5,494,910 06	$5,583,574 13	$5,722,546 83	$37,397,539 82	$6,011,106 56	$6,310,918 77	$6,640,853 16
Total - Fully Managed - P-Series (AIX) - All Support Tiers (Window, Linux)	$3,314,087 04	$3,448,015 77	$3,602,380 46	$3,738,023 80	$3,877,297 14	$4,022,765 03	$4,184,284 40	$26,186,853 63	$4,352,990 54	$4,508,593 11	$4,711,206 03
Server - Managed Only											
Total Managed Only- x86 - All Support Tiers (Window, Linux)	$5,199,025 06	$2,874,961 54	$1,673,402 96	$967,882 19	$294,827 80	$282,597 14	$271,965 75	$11,564,662 44	$271,965 75	$271,965 75	$271,965 75
Total Managed Only- P-Series - All Support Tiers (AIX)	$470,286 82	$279,490 13	$165,061 55	$211,376 46	$209,286 69	$207,196 93	$205,108 55	$1,747,807 14	$203,017 39	$200,927 62	$198,839 24
Storage and Backup - Fully Managed											
Total Enterprise Storage - Fully Managed	$2,725,665 90	$2,904,892 56	$3,090,438 96	$3,290,828 74	$3,507,107 33	$3,747,706 09	$3,960,605 39	$23,227,244 95	$3,960,664 97	$3,960,718 72	$3,960,767 08
Total Tape and Backup - Fully Managed	$2,374,297 79	$1,859,517 00	$1,868,040 37	$1,914,383 49	$1,956,342 88	$1,977,790 72	$2,074,032 43	$14,024,404 67	$2,074,091 90	$2,074,145 55	$2,074,193 82
Limited Co-Lo (Data Center Only Charge)											
Total Limited Co-Lo (Data Center Only Charge)	$160,178 13	$161,929 17	$163,732 74	$165,590 42	$101,450 41	$102,498 59	$103,577 99	$958,957 45	$103,577 99	$103,577 99	$103,577 99
Mainframe Services											
Total IBM Services	$1,851,162 26	$1,770,676 23	$1,692,985 61	$1,621,825 23	$1,546,774 44	$1,481,257 54	$1,415,569 73	$11,380,251 04	$1,410,178 37	$1,404,254 12	$1,398,628 31
Total - IBM Mainfram Services - All Support Tiers	$5,434,971 75	$5,163,377 03	$4,905,313 55	$4,660,088 68	$4,427,275 55	$4,205,968 11	$3,995,758 80	$32,792,753 47	$3,995,758 80	$3,995,758 80	$3,995,758 80
Total Unisys Services	$311,386 72	$307,094 39	$309,045 51	$311,270 12	$313,563 42	$264,674 34	$267,112 98	$2,084,147 47	$266,738 14	$266,397 10	$266,086 61
Total - Unisys Mainfram Services - All Support Tiers	$11,299,225 96	$11,131,300 67	$11,050,670 01	$10,974,137 20	$10,867,130 72	$10,794,272 85	$10,633,953 29	$76,750,690 70	$10,633,953 29	$10,633,953 29	$10,633,953 29
On-Demand (IaaS)											
Total IaaS Servers - x86 (Windows, Linux) - Virtual Servers	$268,533 18	$306,017 39	$351,590 69	$402,780 44	$465,556 22	$529,894 83	$611,541 05	$2,935,913 79	$731,745 69	$844,605 55	$1,069,769 66
Total IaaS Storage On-Demand	$2,164 97	$2,530 00	$2,957 00	$3,460 77	$4,055 62	$4,753 30	$5,553 05	$25,474 71	$6,055 30	$6,601 91	$7,199 24
Total IaaS Backup On-Demand	$1,748 06	$1,489 98	$1,631 66	$1,823 04	$2,030 88	$2,238 65	$2,559 05	$13,521 33	$2,791 62	$3,045 76	$3,322 73
Reserve Account											
Reserve Account	$1,008,000 00	$1,008,000 00	$1,008,000 00	$1,008,000 00	$1,008,000 00	$1,008,000 00	$1,008,000 00	$7,056,000 00	$1,008,000 00	$1,008,000 00	$1,008,000 00
Third Party Software											
Total Third Party Software	$6,605,259 98	$6,854,771 37	$7,059,637 65	$7,270,649 95	$7,487,955 00	$7,711,779 02	$7,942,317 95	$50,932,370 92	$8,078,208 94	$8,195,279 07	$8,328,038 08
Yearly Total	**$120,221,048.73**	**$120,724,360.60**	**$121,118,138.55**	**$121,807,954.95**	**$122,621,753.31**	**$128,650,005.88**	**$123,737,715.00**	**$858,880,977.02**	**$124,467,392.83**	**$125,171,996.09**	**$126,055,307.53**

Total Transition Charges	**$73,147,924.76**
Services (Base Term)	**$858,880,977.02**

Grand Total Base Term: Transition + Services	**$932,028,901.77**
Services (Renewal Years)	**$375,694,696.44**
Grand Total w/ Renewal Years	**$1,307,723,598.21**

Technical Staff Rate Card

	S aff Hourly Rate									
Resource Description	Year 1	Year 2	Year 3	Year	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Inf astructure (mainframe m d-range and x86) Architects Engineers	$133.78	$137.19	$120.71	$12 .33	$128.06	$131.90	$135.86	$139.93	$1 .13	$1 .8
M crosoft Product Spec alists (e.g. Exchange SharePo nt)	$132.18	$135.5	$119.01	$122.58	$126.25	$130.0	$133.9	$137.96	$1 2.10	$1 6.36
Basis and SAP Oracle support	N/A	N/A	N/A	N A	N/A	N/A	N/A	N/A	N/A	N/A
Performance Specialists	$112.18	$115.5	$119.01	$122.58	$126.25	$130.0	$133.9	$137.96	$1 2.10	$1 6.36
Ma nframe Systems Programmers	$238.87	$2 6.0	$253 .2	$261.02	$268.85	$276.92	$285.22	$293.78	$302 59	$311.67
Batch Administrators	$ 03.9	$ 16.05	$ 28.5	$ 1.39	$ 5 .63	$ 68.27	$ 82.32	$ 96.79	$511.70	$527.05
Ind Pur v Software Product Specialis s	$112.18	$115.5	$119.01	$122.58	$126.25	$130.0	$133.9	$137.96	$1 2.10	$1 6.36
System Adm nistrator (W ndows AIX Linux)	$186.26	$191.85	$197.60	$203.53	$209.6	$215.92	$222. 0	$229.07	$235.95	$2 3.02
System Adm nistrator (Middleware support)	$168.77	$173.83	$179.05	$18 . 2	$189.95	$195.65	$201.52	$207.56	$213.79	$220.20
S storage Administrator	$203.71	$209.86	$216.16	$222.6	$229.32	$236.20	$2 3.29	$250.59	$258.10	$265.84
Data Backup Adm n s ra or	$258.66	$266. 2	$27 . 1	$282.65	$291 13	$299.86	$308.86	$318 12	$327.66	$337. 9
Da abase Administrator	$181.99	$187. 5	$193.07	$198.87	$20 .83	$210.98	$217.31	$223.83	$230 5	$237. 3
Da abase Architects	$152.10	$155.63	$160.30	$165.11	$170.06	$175.16	$180. 2	$185.83	$191. 0	$197. 4
Database Analysts	$87.73	$90.36	$93.08	$95.87	$98.7	$101.71	$10 .76	$107.90	$111.1	$11 . 7
Project Management Support	$2 5.17	$252.53	$260.10	$267.91	$275.9	$28 .22	$292.75	$301.53	$310.58	$319.90
Network Adm n s ra or	$190. 0	$196.11	$202.00	$208.06	$21 .30	$220.73	$227.35	$23 .17	$2 1.19	$2 8. 1
Facil ties Administrator	$1 8.98	$153. 5	$158.05	$162.79	$167.67	$172.70	$177.88	$183.22	$188.72	$19 .38
Secur ty Administrator	$168.77	$173.83	$179.05	$18 . 2	$189.95	$195.65	$201.52	$207.56	$213.79	$220.20
Secur ty Architects	$151.10	$155.63	$160.30	$165.11	$170.06	$175.16	$180. 2	$185.83	$191. 0	$197. 4
Secur ty Analysts	$87.73	$90.36	$93.08	$95.87	$98.7	$101.71	$10 .76	$107.90	$111.1	$11 . 7
Asset Management Adm n stra or	$222.69	$229.37	$236.25	$2 3.3	$250.6	$258.16	$265.90	$273.88	$282.10	$290.56
Qual ty Assurance Support	$12 .89	$128.63	$132. 9	$136. 7	$1 0.56	$1 .78	$1 9.12	$153.60	$158.20	$162.96
Remedy Support Spec alist	$136.21	$1 0.30	$1 .53	$1 8.8	$153.31	$157.91	$162.65	$167.52	$172.51	$177.73
IT Ser ce Continui y Specialist	$399.87	$ 11.86	$ 2 .22	$ 36.92	$ 50.86	$ 63.56	$ 77. 6	$ 91.79	$106 5	$121. 8
Inf ast uctu e (mai f ame mid- range and x86) A chitects/Enginee s - Jun o	$133.78	$137.19	$120.71	$12 .33	$128.06	$131.90	$135.86	$139.93	$1 .13	$1 8. 8
M c osoft P oduct Specialists (e.g. Exchange Sha ePoint) - Junio	$89.7	$92. 3	$95.21	$98.06	$101.00	$10 .03	$107.15	$110.37	$113.68	$117.09
Basis and SAP O acle suppo t – Junio	N/A	N/A	N/A	N A	N/A	N/A	N/A	N/A	N/A	N/A
Pe fo mance Specialists - Junio	$89.7	$92. 3	$95.21	$98.06	$101 00	$10 .03	$107.15	$110.37	$113 68	$117.09
Un ux Main f ame Systems P og amme s - Junio	$1 9.13	$153.60	$158.21	$162.96	$167.85	$172.88	$178.07	$183. 1	$188.91	$19 .58
Batch Administ a o s – Junio	$153.8	$158. 4	$163.25	$168.15	$173.15	$178.3	$183.69	$189.20	$19 .88	$200.54
Un ux Main f ame Batch Administ ato - Senio	$62.50	$6 .37	$66.30	$68.29	$70.3	$72. 5	$7 .63	$76.86	$79.17	$81.55
Un ux Main f ame Batch Administ ato – Junio	$62.50	$6 .37	$66.30	$68.29	$70.3	$72. 5	$7 .63	$76.86	$79.17	$81.55
3 d Pa ty S ftwa e P oduct Specialists - Junio.	$112.18	$115.5	$119.01	$122.58	$126.25	$130.0	$133.9	$137.96	$1 2.10	$1 6.36
System Administ ato (Windows AIX Linux) - Junio	$1 6.52	$150.92	$155.	$160.11	$16 .91	$169.86	$17 .95	$180.20	$185.61	$191.18
System Administ ato (Middlewa e suppo) - Junio	$80.13	$82.53	$85.00	$87.55	$90.18	$92.89	$95.67	$98 5	$101.50	$10 .55
Da a Backup Administ ato – Junio	$239.69	$2 6.88	$25 .28	$261.91	$269.77	$277.86	$286.20	$29 .79	$303.63	$312.7
Da abase Administ ato – Junio	$138.	$1 2.59	$1 6.87	$151.28	$155.81	$160. 9	$165.30	$170.26	$175.37	$180.63
Da abase A ch itects – Junio	$115.35	$118.81	$122.38	$126.05	$129.83	$133.72	$137.7	$1 1.87	$1 6.12	$150.54
Da abase Analysts – Junio	$81.23	$83.67	$86.18	$88.77	$91. 3	$9 .17	$97.00	$99.91	$102 90	$105.99
P oject Management Suppo t – Junio	$190.23	$195.95	$201.83	$207.89	$21 .12	$220.55	$227.17	$233.98	$2 1.00	$2 8.23
Fac ilities Administ ato – Junio	$125.0	$128.79	$132.66	$136.6	$1 0.7	$1 .96	$1 9.31	$153.79	$158. 0	$163.15
Netwo k Administ a o – Jun o	$1 8.82	$153.29	$157.89	$162.62	$167.50	$172.53	$177.70	$183.03	$188.52	$19 .18
Secu ity Administ ato – Junio	$1 6.52	$150.92	$155.	$160.11	$16 .91	$169.86	$17 .95	$180.20	$185.61	$191.18
Secu ity A chitec t – Junio	$30 .87	$31 .5	$318.37	$325.36	$332.51	$339.8	$3 7.35	$355.03	$362 90	$370.96
Secu ity Analysts – Junio	$87.73	$90.36	$93.08	$95.87	$98.7	$101.71	$10 .76	$107 90	$111.1	$11 . 7
Sma t Hands and Feet Suppo t	$ 0.88	$ 9.52	$51.00	$52.53	$5 .11	$55.73	$57. 0	$59.13	$60.90	$62.73
Un ux Main f ame Use Account Administ ato	$89.7	$92. 3	$95.21	$98.06	$101 00	$10 .03	$107.15	$110.37	$113.68	$117.09
Messaging A chitect	$113.78	$117.19	$120.71	$12 .33	$128.06	$131.90	$135.86	$139.93	$1 .13	$1 8. 5
Senio Messaging Consultant	$112.18	$115.5	$119.01	$122.58	$126.25	$130.0	$133.9	$137.96	$1 2.10	$1 6.36
Messaging Consul ant	$89.7	$92. 3	$95.21	$98.06	$101 00	$10 .03	$107.15	$110.37	$113.68	$117.09
Senio Ac tve Dr ecto y Consultant	$89.7	$92. 3	$95.21	$98.06	$101 00	$10 .03	$107.15	$110.37	$113.68	$117.09
Active Di ecto y Consul ant	$89.7	$92. 3	$95.21	$98.06	$101 00	$10 .03	$107.15	$110.37	$113.68	$117.09
Appl cation Suppo t Consul ant	$169.87	$17 .96	$180.23	$185.62	$191 18	$196.92	$202.83	$208.91	$215.18	$221.6
Technicol W ite	$80.13	$82.53	$85.00	$87.55	$90.18	$92.89	$95.67	$98.5	$101.50	$10 .55
Automation Engineer – Senio	$112.18	$115.5	$119.01	$122.58	$126.25	$130.0	$133.9	$137.96	$1 2.10	$1 6.36
Automation Engineer – Junio	$89.7	$92. 3	$95.21	$98.06	$101 00	$10 .03	$107.15	$110.37	$113.68	$117.09
Senio Technology Consultant 1 - 2200 Database Suppo t	$122.91	$126.60	$130. 0	$13 .31	$138.3	$1 2. 9	$1 6.76	$151.17	$155.70	$160.37
Senio Technology Consultant 2 – Window 2000 and Middlewa e	$168. 1	$173. 7	$178.67	$18 .03	$189.53	$195. 2	$201.09	$207.13	$213.3	$219. 7
Senio Technology Consultant 3 - 2200 Main f ame Applications Pe fo mance and Secu ity	$36 .58	$169.51	$17 .60	$179.8	$185.23	$190.79	$196.51	$202. 1	$208. 8	$21 .
Senio Technology Consultant 4 - Middlewa e P oducts and Appl cations	$193.7	$199.55	$205.5	$211.71	$218.06	$22 .60	$231.3	$238.28	$2 5. 3	$252.79
Senio Technology Consultant 5 - 2200 Database Design and Maintenance	$222.10	$228.76	$235.62	$2 2.69	$2 9.97	$297. 7	$306.20	$273.15	$281 35	$289.79
Senio Technology Consultant 6 - Data Wa ehouse Systems and O acle Database Se ve s	$161.26	$166.10	$171.08	$176.21	$181 50	$186.9	$192.55	$198.33	$20 .28	$210. 6
SPC P ine pal Eng nee	$238.32	$266.07	$27 .06	$282.28	$290.75	$299. 7	$308. 5	$317.71	$327 2	$337.05
SPC Consulting Enginee	$139.26	$3 .3	$1 7.7	$152.17	$156.7	$161.	$166.28	$171.27	$176. 1	$181.70
Consultant 1	$3 0.37	$350.58	$361.10	$371.93	$383.09	$39 .58	$ 06. 2	$ 18.61	$ 31.17	$. 1
Consultant 2	$311.52	$320.87	$330.50	$3 0. 1	$350.63	$361.1	$371.90	$383.1	$39 .63	$ 06. 9
Consultant 3	$259.61	$267.39	$275. 2	$283.68	$292.19	$300.95	$309.98	$319.28	$328.86	$338.73
Consultant 4	$213. 3	$219.86	$226. 5	$233.25	$2 0.2	$2 7. 5	$25 .87	$262.52	$270. 0	$278.51
In eg at on A chi ect	$193.7	$199.55	$205.5	$211.71	$218.06	$22 .60	$231.3	$238.28	$2 5. 3	$252.79
P og am Analyst	$93.75	$96.56	$99. 6	$102.	$105.51	$108.68	$111.9	$115.30	$118.76	$122.32
P og amme	$93.75	$96.56	$99. 6	$102.	$105.51	$108.68	$111.9	$115.30	$118.76	$122.32
Senio P og amme	$3 0.37	$350.58	$361.10	$371.93	$383.09	$39 .58	$ 06. 2	$ 18.61	$ 31.17	$. 1
Senio Systems Analyst	$122.91	$126.60	$130. 0	$13 .31	$138.3	$1 2. 9	$1 6.76	$151.17	$155.70	$160.37
Senio Systems A chitect	$258.32	$266.07	$27 .06	$282.28	$290.75	$299. 7	$308. 5	$317.71	$327 2	$337.05
S Engagement Manage	$361.32	$372.16	$383.32	$39 .82	$ 06.66	$ 18.86	$ 31. 3	$. 37	$ 57.70	$ 71.
Systems Analyst	$132.50	$115.87	$119.35	$122.93	$126.61	$130. 1	$13 .33	$138.36	$1 2.51	$1 6.78
Systems A ch tect	$1 7.91	$152.35	$156.92	$161.63	$166. 8	$171. 7	$176.61	$181.91	$187 37	$192.99
Technology A chitect	$1 7.91	$152.35	$156.92	$161.63	$166. 8	$171. 7	$176.61	$181.91	$187 37	$192.99
Solutions A chitect	$361.32	$372.16	$383.32	$39 .82	$ 06.66	$ 18.86	$ 31. 3	$. 37	$ 57.70	$ 71.
System Administ ato (AIX Linux) - Junio	$168.77	$173.83	$179.05	$18 . 2	$189.95	$195.65	$201.52	$207.56	$213.79	$220.20
S s tem Administ ato – Junio	$181.81	$187.26	$192.88	$198.67	$20 .63	$210.77	$217.09	$223.60	$230.31	$237.22
Solutions A chitect - Junio	$29 .58	$303. 1	$312.52	$321.89	$331.55	$3 1. 9	$351.7	$362.29	$373.16	$38 .36
Asset Management Administ ato – Junio	$123.0	$128.79	$132.66	$136.6	$1 0.7	$1 .96	$1 9.31	$153.79	$158. 0	$163.15
Quality Assu ance Suppo t - Junio	$107. 0	$110.62	$113.9	$117.36	$120.88	$12 .50	$128.2	$132.09	$136.05	$1 0.13
Remedy Suppo t Spec ali st – Junio	$107. 0	$110.62	$113.9	$117.36	$120.88	$12 .50	$128.2	$132.09	$136.05	$1 0.13
IT Se vice Cont nuity Special st – Junio	$171.07	$176.20	$181. 9	$186.93	$192. 1	$198.02	$20 .27	$210.39	$216.71	$223.21
Mul f ame System P og amme (IBM) – Junio	$1 6.52	$150.92	$155.	$160.11	$16 .91	$169.86	$17 .95	$180.20	$185.61	$191.18
P oject Manage – ERP	$238.86	$5 .73	$561.07	$577.90	$595.2	$613.10	$631. 9	$650.	$669.95	$690.05
Functional Team Lead - ERP	$ 82.20	$ 92.7	$933.5	$1 .59	$525.92	$537.51	$5 9.38	$561.53	$573.98	$586.77
Senio Func tonal Spec alist ERP	$ 12.20	$ 21.22	$ 30. 5	$ 39.90	$ 9.57	$ 59. 8	$ 69.63	$ 80.02	$ 90.66	$501.56
Junio Func tonal Spec alist - ERP	$3 2.21	$3 9.69	$357.35	$365.20	$373.23	$381. 6	$389.88	$398.51	$ 07.3	$ 16.39
Testing / Documentation Specialist - ERP	$295.5	$302.00	$308.62	$315. 0	$322.3	$329.	$336.72	$3 .17	$351.79	$359.61
T ainr	$295.5	$302.00	$308.62	$315. 0	$322.3	$329.	$336.72	$3 .17	$351.79	$359.61
Technical Team Lead	$ 82.20	$ 92.7	$933.5	$1 .59	$525.92	$537.51	$5 9.38	$561.53	$573.98	$586.77
Senio Develope	$ 12.20	$ 21.22	$ 30. 5	$ 39.90	$ 9.57	$ 59. 8	$ 69.63	$ 80.02	$ 90.66	$501.56
Junio Develope	$139.99	$1 3.05	$1 6.19	$1 9. 0	$152.69	$156.05	$159.50	$163.03	$166.6	$170.3
Du abase Administ ato Team Lead	$528.86	$5 .3	$552.27	$56 .39	$576.81	$589.52	$602.5	$615.80	$629.53	$6 3.51
Senio System Administ ation Specialist	$ 82.20	$ 92.7	$933.5	$1 .59	$525.92	$537.51	$5 9.38	$561.53	$573.98	$586.77
Junio System Administ ation Specialist	$ 12.20	$ 21.22	$ 30. 5	$ 39.90	$ 9.57	$ 59. 8	$ 69.63	$ 80.02	$ 90.66	$501.56
Senio Secu ity Special st	$ 12.20	$ 21.22	$ 30. 5	$ 39.90	$ 9.57	$ 59. 8	$ 69.63	$ 80.02	$ 90.66	$501.56
Junio Secu ity Special st	$30 .87	$31 .5	$318.37	$325.36	$332.51	$339.8	$3 7.35	$355.03	$362 90	$370.96
P og am Manage – Onsite	$273.77	$281.98	$290.	$299.15	$308.13	$317.37	$326.89	$336.70	$3 6.80	$357.20
Senio Func tonal Analyst - Onsi e	$209.99	$216.29	$222.78	$229. 6	$236.35	$2 3.	$250.7	$258.26	$266.01	$273.99
Junio Func tonal Analyst - Onsi e	$209.99	$216.29	$222.78	$229. 6	$236.35	$2 3.	$250.7	$258.26	$266.01	$273.99
Testing / Documentation Specialist - Onsite	$180.	$185.85	$191. 2	$197.17	$203.08	$209.17	$215. 5	$221.91	$228.57	$235. 3
A ch tect - Onsite	$209.99	$216.29	$222.78	$229. 6	$236.35	$2 3.	$250.7	$258.26	$266.01	$273.99
Senio Develope – Onsi e	$209.99	$216.29	$222.78	$229. 6	$236.35	$2 3.	$250.7	$258.26	$266.01	$273.99
Junio Develope – Onsi e	$168.51	$173.33	$178.30	$183. 1	$188.67	$19 .08	$199.65	$205.38	$211.28	$217.36
Automated Teste – Ons te	$180.	$185.85	$191. 2	$197.17	$203.08	$209.17	$215. 5	$221.91	$228.57	$235. 3
Du abase Administ ato Team Lead - Onsi e	$273.77	$281.98	$290.	$299.15	$308.13	$317.37	$326.89	$336.70	$3 6.80	$357.20
Senio Database Administ ato Specialist - Onsite	$209.99	$216.29	$222.78	$229. 6	$236.35	$2 3.	$250.7	$258.26	$266.01	$273.99
Junio Database Administ ato Specialist - Onsi e	$180.	$185.85	$191. 2	$197.17	$203.08	$209.17	$215. 5	$221.91	$228.57	$235. 3
Secu ity Specialist - Onsite	$139.99	$1 .19	$1 8.52	$152.97	$157.56	$162.29	$167.16	$172.17	$177.3	$182.66
Configu ation Analyst - Onsite	$139.99	$1 3.05	$1 6.19	$1 9. 0	$152.69	$156.05	$159.50	$163.03	$166.6	$170.3
Othe f ena t desc ipt on)										
Othe ftma t desc ipt on)										

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	Product Name	Unit	Qty per config	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
* Note: This data is sample data provided as an example. The data contained do not contain actual prices or product information.																			
* Sample Data ==>	Mainframe_Dorado_MIPS	Per MIP		ABC51323698	45687	1245	rv 5.0.1	FDCFG12599	XYZ123	$0.001	$0.001	$0.001	$0.001	$0.001	$0.001	$0.001	$0.001	$0.001	$0.001
* Sample Data ==>	VirtualServer_Windows2008_vCPU	Per VCPU		ABC51323699	45688	1246	rv 5.0.2	FDCFG12600	XYZ124	$0.002	$0.002	$0.002	$0.002	$0.002	$0.002	$0.002	$0.002	$0.002	$0.002
* Sample Data ==>	VirtualServer_Windows2008_vRAM	Per Gig		ABC51323700	45689	1247	rv 5.0.3	FDCFG12601	XYZ125	$0.003	$0.003	$0.003	$0.003	$0.003	$0.003	$0.003	$0.003	$0.003	$0.003
* Sample Data ==>	VirtualServer_Windows2008_Gig_Diskspace_Tier1	Per Gig		ABC51323701	45690	1248	rv 5.0.4	FDCFG12602	XYZ126	$0.004	$0.004	$0.004	$0.004	$0.004	$0.004	$0.004	$0.004	$0.004	$0.004
* Sample Data ==>	VirtualServer_Windows2008_Gig_Diskspace_Tier2	Per Gig		ABC51323702	45691	1249	rv 5.0.5	FDCFG12603	XYZ127	$0.005	$0.005	$0.005	$0.005	$0.005	$0.005	$0.005	$0.005	$0.005	$0.005
* Sample Data ==>	VirtualServer_Windows2008_IIS_Feature	Per Instance		ABC51323703	45692	1250	rv 5.0.6	FDCFG12604	XYZ128	$0.006	$0.006	$0.006	$0.006	$0.006	$0.006	$0.006	$0.006	$0.006	$0.006
* Sample Data ==>	VirtualServer_Windows2008_WebServer_Feature	Per Instance		ABC51323704	45693	1251	rv 5.0.7	FDCFG12605	XYZ129	$0.007	$0.007	$0.007	$0.007	$0.007	$0.007	$0.007	$0.007	$0.007	$0.007
* Sample Data ==>	Backup_Service_Disk	Per Server		ABC51323705	45694	1252	rv 5.0.8	FDCFG12606	XYZ130	$0.008	$0.008	$0.008	$0.008	$0.008	$0.008	$0.008	$0.008	$0.008	$0.008
* Sample Data ==>	SSL_Certificate	Per Cert		ABC51323706	45695	1253	rv 5.0.9	FDCFG12607	XYZ131	$0.009	$0.009	$0.009	$0.009	$0.009	$0.009	$0.009	$0.009	$0.009	$0.009
Server - Fully Managed (1)																			
x86 Server Configurations (Windows)																			
Windows pConfig - 1	2-way Quad-Core 2.0 GHz	Per Server		CCSU13310001-A	N/A	N/A	A			$ 39.34	$ 38.20	$ 35.12	$ 31.89	$ 28.51	$ 24.99	$ 36.95	$ 36.95	$ 36.95	$ 36.95
Windows pConfig - 2 4 5	2-way Six-Core 2.4 GHz	Per Server		CCSU13310002-A	N/A	N/A	A			$ 57.96	$ 56.63	$ 53.37	$ 49.95	$ 46.39	$ 42.69	$ 54.47	$ 54.47	$ 54.47	$ 54.47
Windows pConfig - 3	4-way Six-Core 2.0 GHz	Per Server		CCSU13310003-A	N/A	N/A	A			$ 51.66	$ 46.58	$ 39.49	$ 32.17	$ 24.62	$ 16.85	$ 40.10	$ 40.10	$ 40.10	$ 40.10
Windows pConfig - 1, 2, 3, 4, 5	GB RAM	Per GB		CCSU13310004-A	N/A	N/A	A			$ 0.93	$ 0.88	$ 0.78	$ 0.71	$ 0.64	$ 0.56	$ 0.82	$ 0.82	$ 0.82	$ 0.82
Windows pConfig - 1 2 4 5	Mirrored 146 15K Hard Drives	Per Primary Mirror drive		CCSU13310005-A	N/A	N/A	A			$ 33.72	$ 32.75	$ 30.10	$ 27.34	$ 24.44	$ 21.42	$ 31.67	$ 31.67	$ 31.67	$ 31.67
Windows pConfig - 3	SAN Attached Storage	Per GB		CCSU13310006-A	N/A	N/A	A			$ 0.04	$ 0.04	$ 0.04	$ 0.04	$ 0.04	$ 0.04	$ 0.04	$ 0.04	$ 0.04	$ 0.04
Windows pConfig - 1 2 3 4 5	Windows Server 2008 R2	Per License		CCSU13310007-A	2008	R2	A			$ 179.09	$ 184.46	$ 189.99	$ 195.69	$ 201.57	$ 207.61	$ 184.46	$ 184.46	$ 184.46	$ 184.46
Windows pConfig - 4	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization Site's Local SAN Storage from hourly data synchronization	Per Service		CCSU13310008-A	N/A	N/A	A			$ 4.46	$ 4.59	$ 4.73	$ 4.87	$ 5.02	$ 5.17	$ 4.59	$ 4.59	$ 4.59	$ 4.59
Windows pConfig - 5	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Service		CCSU13310009-A	N/A	N/A	A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 1	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310010-A	N/A	N/A	A			$ 64.00	$ 57.60	$ 54.72	$ 51.98	$ 49.38	$ 46.91	$ 44.57	$ 44.57	$ 44.57	$ 44.57
Windows pConfig - 1	Fully Managed (1) - Gold Tier	Per Config		CCSU13310011-A	N/A	N/A	A			$ 60.49	$ 54.44	$ 51.72	$ 49.13	$ 46.67	$ 44.34	$ 42.12	$ 42.12	$ 42.12	$ 42.12
Windows pConfig - 1	Fully Managed (1) - Silver Tier	Per Config		CCSU13310012-A	N/A	N/A	A			$ 57.39	$ 51.65	$ 49.06	$ 46.61	$ 44.28	$ 42.07	$ 39.96	$ 39.96	$ 39.96	$ 39.96
Windows pConfig - 1	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310013-A	N/A	N/A	A			$ 55.95	$ 50.36	$ 47.84	$ 45.45	$ 43.17	$ 41.02	$ 38.96	$ 38.96	$ 38.96	$ 38.96
Windows pConfig - 1	Fully Managed (1) - Basic Tier	Per Config		CCSU13310014-A	N/A	N/A	A			$ 54.59	$ 49.13	$ 46.67	$ 44.34	$ 42.12	$ 40.01	$ 38.01	$ 38.01	$ 38.01	$ 38.01
Windows pConfig - 2	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310015-A	N/A	N/A	A			$ 63.94	$ 57.55	$ 54.67	$ 51.94	$ 49.34	$ 46.87	$ 44.53	$ 44.53	$ 44.53	$ 44.53
Windows pConfig - 2	Fully Managed (1) - Gold Tier	Per Config		CCSU13310016-A	N/A	N/A	A			$ 60.49	$ 54.44	$ 51.72	$ 49.13	$ 46.67	$ 44.34	$ 42.12	$ 42.12	$ 42.12	$ 42.12
Windows pConfig - 2	Fully Managed (1) - Silver Tier	Per Config		CCSU13310017-A	N/A	N/A	A			$ 57.39	$ 51.65	$ 49.06	$ 46.61	$ 44.28	$ 42.07	$ 39.96	$ 39.96	$ 39.96	$ 39.96
Windows pConfig - 2	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310018-A	N/A	N/A	A			$ 55.95	$ 50.36	$ 47.84	$ 45.45	$ 43.17	$ 41.02	$ 38.96	$ 38.96	$ 38.96	$ 38.96
Windows pConfig - 2	Fully Managed (1) - Basic Tier	Per Config		CCSU13310019-A	N/A	N/A	A			$ 54.59	$ 49.13	$ 46.67	$ 44.34	$ 42.12	$ 40.01	$ 38.01	$ 38.01	$ 38.01	$ 38.01
Windows pConfig - 3	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310020-A	N/A	N/A	A			$ 63.94	$ 57.55	$ 54.67	$ 51.94	$ 49.34	$ 46.87	$ 44.53	$ 44.53	$ 44.53	$ 44.53
Windows pConfig - 3	Fully Managed (1) - Gold Tier	Per Config		CCSU13310021-A	N/A	N/A	A			$ 60.49	$ 54.44	$ 51.72	$ 49.13	$ 46.67	$ 44.34	$ 42.12	$ 42.12	$ 42.12	$ 42.12
Windows pConfig - 3	Fully Managed (1) - Silver Tier	Per Config		CCSU13310022-A	N/A	N/A	A			$ 57.39	$ 51.65	$ 49.06	$ 46.61	$ 44.28	$ 42.07	$ 39.96	$ 39.96	$ 39.96	$ 39.96
Windows pConfig - 3	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310023-A	N/A	N/A	A			$ 55.95	$ 50.36	$ 47.84	$ 45.45	$ 43.17	$ 41.02	$ 38.96	$ 38.96	$ 38.96	$ 38.96
Windows pConfig - 3	Fully Managed (1) - Basic Tier	Per Config		CCSU13310024-A	N/A	N/A	A			$ 54.59	$ 49.13	$ 46.67	$ 44.34	$ 42.12	$ 40.01	$ 38.01	$ 38.01	$ 38.01	$ 38.01
Windows pConfig - 4	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310025-A	N/A	N/A	A			$ 63.94	$ 57.55	$ 54.67	$ 51.94	$ 49.34	$ 46.87	$ 44.53	$ 44.53	$ 44.53	$ 44.53
Windows pConfig - 4	Fully Managed (1) - Gold Tier	Per Config		CCSU13310026-A	N/A	N/A	A			$ 60.49	$ 54.44	$ 51.72	$ 49.13	$ 46.67	$ 44.34	$ 42.12	$ 42.12	$ 42.12	$ 42.12
Windows pConfig - 4	Fully Managed (1) - Silver Tier	Per Config		CCSU13310027-A	N/A	N/A	A			$ 57.39	$ 51.65	$ 49.06	$ 46.61	$ 44.28	$ 42.07	$ 39.96	$ 39.96	$ 39.96	$ 39.96
Windows pConfig - 4	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310028-A	N/A	N/A	A			$ 55.95	$ 50.36	$ 47.84	$ 45.45	$ 43.17	$ 41.02	$ 38.96	$ 38.96	$ 38.96	$ 38.96
Windows pConfig - 4	Fully Managed (1) - Basic Tier	Per Config		CCSU13310029-A	N/A	N/A	A			$ 54.59	$ 49.13	$ 46.67	$ 44.34	$ 42.12	$ 40.01	$ 38.01	$ 38.01	$ 38.01	$ 38.01
Windows pConfig - 5	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310030-A	N/A	N/A	A			$ 63.94	$ 57.55	$ 54.67	$ 51.94	$ 49.34	$ 46.87	$ 44.53	$ 44.53	$ 44.53	$ 44.53
Windows pConfig - 5	Fully Managed (1) - Gold Tier	Per Config		CCSU13310031-A	N/A	N/A	A			$ 60.49	$ 54.44	$ 51.72	$ 49.13	$ 46.67	$ 44.34	$ 42.12	$ 42.12	$ 42.12	$ 42.12
Windows pConfig - 5	Fully Managed (1) - Silver Tier	Per Config		CCSU13310032-A	N/A	N/A	A			$ 57.39	$ 51.65	$ 49.06	$ 46.61	$ 44.28	$ 42.07	$ 39.96	$ 39.96	$ 39.96	$ 39.96
Windows pConfig - 5	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310033-A	N/A	N/A	A			$ 55.95	$ 50.36	$ 47.84	$ 45.45	$ 43.17	$ 41.02	$ 38.96	$ 38.96	$ 38.96	$ 38.96
Windows pConfig - 5	Fully Managed (1) - Basic Tier	Per Config		CCSU13310034-A	N/A	N/A	A			$ 54.59	$ 49.13	$ 46.67	$ 44.34	$ 42.12	$ 40.01	$ 38.01	$ 38.01	$ 38.01	$ 38.01
Windows pConfig - 1	2-way Quad-Core 2.0 GHz		1							$ 39.34	$ 38.20	$ 35.12	$ 31.89	$ 28.51	$ 24.99	$ 36.95	$ 36.95	$ 36.95	$ 36.95
	GB RAM		4							$ 3.72	$ 3.53	$ 3.13	$ 2.84	$ 2.54	$ 2.23	$ 3.29	$ 3.29	$ 3.29	$ 3.29
	Mirrored 146 15K Hard Drives		1							$ 33.72	$ 32.75	$ 30.10	$ 27.34	$ 24.44	$ 21.42	$ 31.67	$ 31.67	$ 31.67	$ 31.67
	Windows Server 2008 R2		1							$ 179.09	$ 184.46	$ 189.99	$ 195.69	$ 201.57	$ 207.61	$ 184.46	$ 184.46	$ 184.46	$ 184.46
	Sub-Total									**$ 255.87**	**$ 258.94**	**$ 258.35**	**$ 257.76**	**$ 257.06**	**$ 256.25**	**$ 256.38**	**$ 256.38**	**$ 256.38**	**$ 256.38**
Windows pConfig - 1	Fully Managed (1) - Platinum Tier		1							$ 319.87	$ 316.54	$ 313.07	$ 309.75	$ 306.44	$ 303.16	$ 300.95	$ 300.95	$ 300.95	$ 300.95
Windows pConfig - 1	Fully Managed (1) - Gold Tier		1							$ 316.36	$ 313.38	$ 310.07	$ 306.90	$ 303.74	$ 300.59	$ 298.50	$ 298.50	$ 298.50	$ 298.50
Windows pConfig - 1	Fully Managed (1) - Silver Tier		1							$ 313.26	$ 310.59	$ 307.42	$ 304.38	$ 301.34	$ 298.32	$ 296.34	$ 296.34	$ 296.34	$ 296.34
Windows pConfig - 1	Fully Managed (1) - Bronze Tier		1							$ 311.82	$ 309.30	$ 306.19	$ 303.21	$ 300.24	$ 297.26	$ 295.34	$ 295.34	$ 295.34	$ 295.34
Windows pConfig - 1	Fully Managed (1) - Basic Tier		1							$ 310.46	$ 308.07	$ 305.02	$ 302.10	$ 299.18	$ 296.26	$ 294.39	$ 294.39	$ 294.39	$ 294.39
Windows pConfig - 2	2-way Six-Core 2.4 GHz		1							$ 57.96	$ 56.63	$ 53.37	$ 49.95	$ 46.39	$ 42.69	$ 54.47	$ 54.47	$ 54.47	$ 54.47
	GB RAM		16							$ 14.87	$ 14.13	$ 12.52	$ 11.37	$ 10.17	$ 8.91	$ 13.18	$ 13.18	$ 13.18	$ 13.18
	Mirrored 146 15K Hard Drives		1							$ 33.72	$ 32.75	$ 30.10	$ 27.34	$ 24.44	$ 21.42	$ 31.67	$ 31.67	$ 31.67	$ 31.67
	Windows Server 2008 R2		1							$ 179.09	$ 184.46	$ 189.99	$ 195.69	$ 201.57	$ 207.61	$ 184.46	$ 184.46	$ 184.46	$ 184.46
	Sub-Total									**$ 285.65**	**$ 287.97**	**$ 285.99**	**$ 284.35**	**$ 282.57**	**$ 280.63**	**$ 283.78**	**$ 283.78**	**$ 283.78**	**$ 283.78**

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	**Product Name**	**Unit**	**Qty per config**	**Provider Part Number**	**Version Major**	**Version Minor**	**Version Build**	**Manufacturer ID**	**Equipment Code**	**Price per unit \ Per Month**									
Description / Use *>*	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Windows pConfig - 2	Fully Managed (1) - Platinum Tier		1							$ 349.59	$ 345.52	$ 340.66	$ 336.29	$ 331.91	$ 327.51	$ 328.32	$ 328.32	$ 328.32	$ 328.32
Windows pConfig - 2	Fully Managed (1) - Gold Tier		1							$ 346.13	$ 342.41	$ 337.71	$ 333.49	$ 329.24	$ 324.97	$ 325.91	$ 325.91	$ 325.91	$ 325.91
Windows pConfig - 2	Fully Managed (1) - Silver Tier		1							$ 343.03	$ 339.62	$ 335.05	$ 330.97	$ 326.85	$ 322.70	$ 323.75	$ 323.75	$ 323.75	$ 323.75
Windows pConfig - 2	Fully Managed (1) - Bronze Tier		1							$ 341.60	$ 338.32	$ 333.83	$ 329.80	$ 325.74	$ 321.65	$ 322.75	$ 322.75	$ 322.75	$ 322.75
Windows pConfig - 2	Fully Managed (1) - Basic Tier		1							$ 340.23	$ 337.10	$ 332.66	$ 328.69	$ 324.69	$ 320.65	$ 321.80	$ 321.80	$ 321.80	$ 321.80
Windows pConfig - 3	4-way Six-Core 2.0 GHz		1							$ 51.66	$ 46.58	$ 39.49	$ 32.17	$ 24.62	$ 16.85	$ 40.10	$ 40.10	$ 40.10	$ 40.10
	GB RAM		64							$ 59.48	$ 56.51	$ 50.09	$ 45.49	$ 40.67	$ 35.64	$ 52.70	$ 52.70	$ 52.70	$ 52.70
	SAN Attached Storage		500							$ 18.11	$ 18.66	$ 19.22	$ 19.79	$ 20.39	$ 21.00	$ 18.66	$ 18.66	$ 18.66	$ 18.66
	Windows Server 2008 R2		1							$ 179.09	$ 184.46	$ 189.99	$ 195.69	$ 201.57	$ 207.61	$ 184.46	$ 184.46	$ 184.46	$ 184.46
	Sub-Total									**$ 308.34**	**$ 306.21**	**$ 298.79**	**$ 293.14**	**$ 287.24**	**$ 281.10**	**$ 295.92**	**$ 295.92**	**$ 295.92**	**$ 295.92**
Windows pConfig - 3	Fully Managed (1) - Platinum Tier		1							$ 372.29	$ 363.76	$ 353.46	$ 345.08	$ 336.58	$ 327.97	$ 340.46	$ 340.46	$ 340.46	$ 340.46
Windows pConfig - 3	Fully Managed (1) - Gold Tier		1							$ 368.83	$ 360.64	$ 350.51	$ 342.27	$ 333.92	$ 325.44	$ 338.05	$ 338.05	$ 338.05	$ 338.05
Windows pConfig - 3	Fully Managed (1) - Silver Tier		1							$ 365.73	$ 357.85	$ 347.86	$ 339.75	$ 331.52	$ 323.17	$ 335.89	$ 335.89	$ 335.89	$ 335.89
Windows pConfig - 3	Fully Managed (1) - Bronze Tier		1							$ 364.29	$ 356.56	$ 346.63	$ 338.59	$ 330.42	$ 322.11	$ 334.89	$ 334.89	$ 334.89	$ 334.89
Windows pConfig - 3	Fully Managed (1) - Basic Tier		1							$ 362.93	$ 355.33	$ 345.46	$ 337.48	$ 329.36	$ 321.11	$ 333.94	$ 333.94	$ 333.94	$ 333.94
Windows pConfig - 4	2-way Six-Core 2.4 GHz		1							$ 57.96	$ 56.63	$ 53.37	$ 49.95	$ 46.39	$ 42.69	$ 54.47	$ 54.47	$ 54.47	$ 54.47
	GB RAM		16							$ 14.87	$ 14.13	$ 12.52	$ 11.37	$ 10.17	$ 8.91	$ 13.18	$ 13.18	$ 13.18	$ 13.18
	Mirrored 146 15K Hard Drives		1							$ 33.72	$ 32.75	$ 30.10	$ 27.34	$ 24.44	$ 21.42	$ 31.67	$ 31.67	$ 31.67	$ 31.67
	Windows Server 2008 R2		1							$ 179.09	$ 184.46	$ 189.99	$ 195.69	$ 201.57	$ 207.61	$ 184.46	$ 184.46	$ 184.46	$ 184.46
	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization Site's Local SAN Storage from hourly data synchronization		1							$ 4.46	$ 4.59	$ 4.73	$ 4.87	$ 5.02	$ 5.17	$ 4.59	$ 4.59	$ 4.59	$ 4.59
	Sub-Total									**$ 290.11**	**$ 292.56**	**$ 290.72**	**$ 289.23**	**$ 287.59**	**$ 285.80**	**$ 288.38**	**$ 288.38**	**$ 288.38**	**$ 288.38**
Windows pConfig - 4	Fully Managed (1) - Platinum Tier		1							$ 354.05	$ 350.11	$ 345.39	$ 341.17	$ 336.93	$ 332.68	$ 332.91	$ 332.91	$ 332.91	$ 332.91
Windows pConfig - 4	Fully Managed (1) - Gold Tier		1							$ 350.59	$ 347.00	$ 342.44	$ 338.36	$ 334.26	$ 330.14	$ 330.50	$ 330.50	$ 330.50	$ 330.50
Windows pConfig - 4	Fully Managed (1) - Silver Tier		1							$ 347.49	$ 344.21	$ 339.79	$ 335.84	$ 331.87	$ 327.87	$ 328.34	$ 328.34	$ 328.34	$ 328.34
Windows pConfig - 4	Fully Managed (1) - Bronze Tier		1							$ 346.06	$ 342.92	$ 338.56	$ 334.67	$ 330.76	$ 326.82	$ 327.34	$ 327.34	$ 327.34	$ 327.34
Windows pConfig - 4	Fully Managed (1) - Basic Tier		1							$ 344.69	$ 341.69	$ 337.39	$ 333.57	$ 329.71	$ 325.82	$ 326.39	$ 326.39	$ 326.39	$ 326.39
Windows pConfig - 5	2-way Six-Core 2.4 GHz		1							$ 57.96	$ 56.63	$ 53.37	$ 49.95	$ 46.39	$ 42.69	$ 54.47	$ 54.47	$ 54.47	$ 54.47
	GB RAM		16							$ 14.87	$ 14.13	$ 12.52	$ 11.37	$ 10.17	$ 8.91	$ 13.18	$ 13.18	$ 13.18	$ 13.18
	Mirrored 146 15K Hard Drives		1							$ 33.72	$ 32.75	$ 30.10	$ 27.34	$ 24.44	$ 21.42	$ 31.67	$ 31.67	$ 31.67	$ 31.67
	Windows Server 2008 R2		1							$ 179.09	$ 184.46	$ 189.99	$ 195.69	$ 201.57	$ 207.61	$ 184.46	$ 184.46	$ 184.46	$ 184.46
	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from Backup off-site tape Backups		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Sub-Total									**$ 285.65**	**$ 287.97**	**$ 285.99**	**$ 284.35**	**$ 282.57**	**$ 280.63**	**$ 283.78**	**$ 283.78**	**$ 283.78**	**$ 283.78**
Windows pConfig - 5	Fully Managed (1) - Platinum Tier		1							$ 349.59	$ 345.52	$ 340.66	$ 336.29	$ 331.91	$ 327.51	$ 328.32	$ 328.32	$ 328.32	$ 328.32
Windows pConfig - 5	Fully Managed (1) - Gold Tier		1							$ 346.13	$ 342.41	$ 337.71	$ 333.49	$ 329.24	$ 324.97	$ 325.91	$ 325.91	$ 325.91	$ 325.91
Windows pConfig - 5	Fully Managed (1) - Silver Tier		1							$ 343.03	$ 339.62	$ 335.05	$ 330.97	$ 326.85	$ 322.70	$ 323.75	$ 323.75	$ 323.75	$ 323.75
Windows pConfig - 5	Fully Managed (1) - Bronze Tier		1							$ 341.60	$ 338.32	$ 333.83	$ 329.80	$ 325.74	$ 321.65	$ 322.75	$ 322.75	$ 322.75	$ 322.75
Windows pConfig - 5	Fully Managed (1) - Basic Tier		1							$ 340.23	$ 337.10	$ 332.66	$ 328.69	$ 324.69	$ 320.65	$ 321.80	$ 321.80	$ 321.80	$ 321.80
x86 Server Configurations (Linux)																			
Linux pConfig - 1	2-way Quad-Core 2.0 GHz	Per Server		CCSU13310035-A	N/A	N/A	A			$ 39.34	$ 38.20	$ 35.12	$ 31.89	$ 28.51	$ 24.99	$ 36.95	$ 36.95	$ 36.95	$ 36.95
Linux pConfig - 2, 4, 5	2-way Six-Core 2.4 GHz	Per Server		CCSU13310036-A	N/A	N/A	A			$ 57.96	$ 56.63	$ 53.37	$ 49.95	$ 46.39	$ 42.69	$ 54.47	$ 54.47	$ 54.47	$ 54.47
Linux pConfig - 3	4-way Six-Core 2.0 GHz	Per Server		CCSU13310037-A	N/A	N/A	A			$ 51.66	$ 46.58	$ 39.49	$ 32.17	$ 24.62	$ 16.85	$ 40.10	$ 40.10	$ 40.10	$ 40.10
Linux pConfig - 1	GB RAM	Per GB		CCSU13310038-A	N/A	N/A	A			$ 0.88	$ 0.85	$ 0.78	$ 0.71	$ 0.64	$ 0.56	$ 0.82	$ 0.82	$ 0.82	$ 0.82
Linux pConfig - 1, 2, 4, 5	Mirrored 146 15K Hard Drives	Per Primary Mirror drive		CCSU13310039-A	N/A	N/A	A			$ 33.72	$ 32.75	$ 30.10	$ 27.34	$ 24.44	$ 21.42	$ 31.67	$ 31.67	$ 31.67	$ 31.67
Linux pConfig - 3	SAN Attached Storage	Per GB		CCSU13310040-A	N/A	N/A	A			$ 0.04	$ 0.04	$ 0.04	$ 0.04	$ 0.04	$ 0.04	$ 0.04	$ 0.04	$ 0.04	$ 0.04
Linux pConfig - 1, 2, 3, 4 , 5	RedHat or SUSE	Per License		CCSU13310041-A	N/A	N/A	A			$ 153.74	$ 158.35	$ 163.10	$ 167.99	$ 173.03	$ 178.22	$ 158.35	$ 158.35	$ 158.35	$ 158.35
Linux pConfig - 4	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Service		CCSU13310042-A	N/A	N/A	A			$ 4.46	$ 4.59	$ 4.73	$ 4.87	$ 5.02	$ 5.17	$ 4.59	$ 4.59	$ 4.59	$ 4.59
Linux pConfig - 5	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Service		CCSU13310043-A	N/A	N/A	A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 1	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310044-A	N/A	N/A	A			$ 143.46	$ 129.12	$ 122.66	$ 116.53	$ 110.70	$ 105.17	$ 99.91	$ 99.91	$ 99.91	$ 99.91
Linux pConfig - 1	Fully Managed (1) - Gold Tier	Per Config		CCSU13310045-A	N/A	N/A	A			$ 127.16	$ 114.44	$ 108.72	$ 103.29	$ 98.12	$ 93.22	$ 88.56	$ 88.56	$ 88.56	$ 88.56
Linux pConfig - 1	Fully Managed (1) - Silver Tier	Per Config		CCSU13310046-A	N/A	N/A	A			$ 114.19	$ 102.77	$ 97.63	$ 92.75	$ 88.11	$ 83.70	$ 79.52	$ 79.52	$ 79.52	$ 79.52
Linux pConfig - 1	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310047-A	N/A	N/A	A			$ 108.64	$ 97.78	$ 92.89	$ 88.24	$ 83.83	$ 79.64	$ 75.66	$ 75.66	$ 75.66	$ 75.66
Linux pConfig - 1	Fully Managed (1) - Basic Tier	Per Config		CCSU13310048-A	N/A	N/A	A			$ 103.61	$ 93.25	$ 88.59	$ 84.16	$ 79.95	$ 75.95	$ 72.16	$ 72.16	$ 72.16	$ 72.16
Linux pConfig - 2	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310049-A	N/A	N/A	A			$ 143.46	$ 129.12	$ 122.66	$ 116.53	$ 110.70	$ 105.17	$ 99.91	$ 99.91	$ 99.91	$ 99.91
Linux pConfig - 2	Fully Managed (1) - Gold Tier	Per Config		CCSU13310050-A	N/A	N/A	A			$ 127.16	$ 114.44	$ 108.72	$ 103.29	$ 98.12	$ 93.22	$ 88.56	$ 88.56	$ 88.56	$ 88.56
Linux pConfig - 2	Fully Managed (1) - Silver Tier	Per Config		CCSU13310051-A	N/A	N/A	A			$ 114.19	$ 102.77	$ 97.63	$ 92.75	$ 88.11	$ 83.70	$ 79.52	$ 79.52	$ 79.52	$ 79.52
Linux pConfig - 2	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310052-A	N/A	N/A	A			$ 108.64	$ 97.78	$ 92.89	$ 88.24	$ 83.83	$ 79.64	$ 75.66	$ 75.66	$ 75.66	$ 75.66
Linux pConfig - 2	Fully Managed (1) - Basic Tier	Per Config		CCSU13310053-A	N/A	N/A	A			$ 103.61	$ 93.25	$ 88.59	$ 84.16	$ 79.95	$ 75.95	$ 72.16	$ 72.16	$ 72.16	$ 72.16
Linux pConfig - 3	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310054-A	N/A	N/A	A			$ 143.46	$ 129.12	$ 122.66	$ 116.53	$ 110.70	$ 105.17	$ 99.91	$ 99.91	$ 99.91	$ 99.91
Linux pConfig - 3	Fully Managed (1) - Gold Tier	Per Config		CCSU13310055-A	N/A	N/A	A			$ 127.16	$ 114.44	$ 108.72	$ 103.29	$ 98.12	$ 93.22	$ 88.56	$ 88.56	$ 88.56	$ 88.56
Linux pConfig - 3	Fully Managed (1) - Silver Tier	Per Config		CCSU13310056-A	N/A	N/A	A			$ 114.19	$ 102.77	$ 97.63	$ 92.75	$ 88.11	$ 83.70	$ 79.52	$ 79.52	$ 79.52	$ 79.52
Linux pConfig - 3	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310057-A	N/A	N/A	A			$ 108.64	$ 97.78	$ 92.89	$ 88.24	$ 83.83	$ 79.64	$ 75.66	$ 75.66	$ 75.66	$ 75.66
Linux pConfig - 3	Fully Managed (1) - Basic Tier	Per Config		CCSU13310058-A	N/A	N/A	A			$ 103.61	$ 93.25	$ 88.59	$ 84.16	$ 79.95	$ 75.95	$ 72.16	$ 72.16	$ 72.16	$ 72.16

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	**Product Name**	**Unit**	**Qty per config**	**Provider Part Number**	**Version Major**	**Version Minor**	**Version Build**	**Manufacturer ID**	**Equipment Code**	**Price per unit \ Per Month**									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Linux pConfig - 4	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310059-A	N/A	N/A	A			$ 143.46	$ 129.12	$ 122.66	$ 116.53	$ 110.70	$ 105.17	$ 99.91	$ 99.91	$ 99.91	$ 99.91
Linux pConfig - 4	Fully Managed (1) - Gold Tier	Per Config		CCSU13310060-A	N/A	N/A	A			$ 127.16	$ 114.44	$ 108.72	$ 103.29	$ 98.12	$ 93.22	$ 88.56	$ 88.56	$ 88.56	$ 88.56
Linux pConfig - 4	Fully Managed (1) - Silver Tier	Per Config		CCSU13310061-A	N/A	N/A	A			$ 114.19	$ 102.77	$ 97.63	$ 92.75	$ 88.11	$ 83.70	$ 79.52	$ 79.52	$ 79.52	$ 79.52
Linux pConfig - 4	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310062-A	N/A	N/A	A			$ 108.64	$ 97.78	$ 92.89	$ 88.24	$ 83.83	$ 79.64	$ 75.66	$ 75.66	$ 75.66	$ 75.66
Linux pConfig - 4	Fully Managed (1) - Basic Tier	Per Config		CCSU13310063-A	N/A	N/A	A			$ 103.61	$ 93.25	$ 88.59	$ 84.16	$ 79.95	$ 75.95	$ 72.16	$ 72.16	$ 72.16	$ 72.16
Linux pConfig - 5	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310064-A	N/A	N/A	A			$ 143.46	$ 129.12	$ 122.66	$ 116.53	$ 110.70	$ 105.17	$ 99.91	$ 99.91	$ 99.91	$ 99.91
Linux pConfig - 5	Fully Managed (1) - Gold Tier	Per Config		CCSU13310065-A	N/A	N/A	A			$ 127.16	$ 114.44	$ 108.72	$ 103.29	$ 98.12	$ 93.22	$ 88.56	$ 88.56	$ 88.56	$ 88.56
Linux pConfig - 5	Fully Managed (1) - Silver Tier	Per Config		CCSU13310066-A	N/A	N/A	A			$ 114.19	$ 102.77	$ 97.63	$ 92.75	$ 88.11	$ 83.70	$ 79.52	$ 79.52	$ 79.52	$ 79.52
Linux pConfig - 5	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310067-A	N/A	N/A	A			$ 108.64	$ 97.78	$ 92.89	$ 88.24	$ 83.83	$ 79.64	$ 75.66	$ 75.66	$ 75.66	$ 75.66
Linux pConfig - 5	Fully Managed (1) - Basic Tier	Per Config		CCSU13310068-A	N/A	N/A	A			$ 103.61	$ 93.25	$ 88.59	$ 84.16	$ 79.95	$ 75.95	$ 72.16	$ 72.16	$ 72.16	$ 72.16
Linux pConfig - 1	2-way Quad-Core 2.0 GHz		1							$ 39.34	$ 38.20	$ 35.12	$ 31.89	$ 28.51	$ 24.99	$ 36.95	$ 36.95	$ 36.95	$ 36.95
	4 GB RAM		4							$ 3.51	$ 3.41	$ 3.13	$ 2.84	$ 2.54	$ 2.23	$ 3.29	$ 3.29	$ 3.29	$ 3.29
	Mirrored 146 15K Hard Drives		1							$ 33.72	$ 32.75	$ 30.10	$ 27.34	$ 24.44	$ 21.42	$ 31.67	$ 31.67	$ 31.67	$ 31.67
	RedHat or SUSE		1							$ 153.74	$ 158.35	$ 163.10	$ 167.99	$ 173.03	$ 178.22	$ 158.35	$ 158.35	$ 158.35	$ 158.35
	Sub-Total									**$ 230.31**	**$ 232.70**	**$ 231.46**	**$ 230.06**	**$ 228.53**	**$ 226.86**	**$ 230.27**	**$ 230.27**	**$ 230.27**	**$ 230.27**
Linux pConfig - 1	Fully Managed (1) - Platinum Tier		1							$ 373.78	$ 361.82	$ 354.12	$ 346.59	$ 339.23	$ 332.03	$ 330.18	$ 330.18	$ 330.18	$ 330.18
Linux pConfig - 1	Fully Managed (1) - Gold Tier		1							$ 357.47	$ 347.15	$ 340.18	$ 333.35	$ 326.65	$ 320.08	$ 318.82	$ 318.82	$ 318.82	$ 318.82
Linux pConfig - 1	Fully Managed (1) - Silver Tier		1							$ 344.50	$ 335.47	$ 329.09	$ 322.81	$ 316.64	$ 310.57	$ 309.79	$ 309.79	$ 309.79	$ 309.79
Linux pConfig - 1	Fully Managed (1) - Bronze Tier		1							$ 338.95	$ 330.48	$ 324.35	$ 318.31	$ 312.36	$ 306.50	$ 305.93	$ 305.93	$ 305.93	$ 305.93
Linux pConfig - 1	Fully Managed (1) - Basic Tier		1							$ 333.92	$ 325.96	$ 320.05	$ 314.22	$ 308.48	$ 302.81	$ 302.42	$ 302.42	$ 302.42	$ 302.42
Linux pConfig - 2	2-way Six-Core 2.4 GHz		1							$ 57.96	$ 56.63	$ 53.37	$ 49.95	$ 46.39	$ 42.69	$ 54.47	$ 54.47	$ 54.47	$ 54.47
	16 GB RAM		16							$ 14.03	$ 13.62	$ 12.52	$ 11.37	$ 10.17	$ 8.91	$ 13.18	$ 13.18	$ 13.18	$ 13.18
	Mirrored 146 15K Hard Drives		1							$ 33.72	$ 32.75	$ 30.10	$ 27.34	$ 24.44	$ 21.42	$ 31.67	$ 31.67	$ 31.67	$ 31.67
	RedHat or SUSE		1							$ 153.74	$ 158.35	$ 163.10	$ 167.99	$ 173.03	$ 178.22	$ 158.35	$ 158.35	$ 158.35	$ 158.35
	Sub-Total									**$ 259.45**	**$ 261.35**	**$ 259.09**	**$ 256.65**	**$ 254.03**	**$ 251.24**	**$ 257.67**	**$ 257.67**	**$ 257.67**	**$ 257.67**
Linux pConfig - 2	Fully Managed (1) - Platinum Tier		1							$ 402.92	$ 390.47	$ 381.76	$ 373.18	$ 364.74	$ 356.41	$ 357.58	$ 357.58	$ 357.58	$ 357.58
Linux pConfig - 2	Fully Managed (1) - Gold Tier		1							$ 386.61	$ 375.80	$ 367.82	$ 359.94	$ 352.16	$ 344.46	$ 346.23	$ 346.23	$ 346.23	$ 346.23
Linux pConfig - 2	Fully Managed (1) - Silver Tier		1							$ 373.64	$ 364.12	$ 356.72	$ 349.40	$ 342.14	$ 334.95	$ 337.19	$ 337.19	$ 337.19	$ 337.19
Linux pConfig - 2	Fully Managed (1) - Bronze Tier		1							$ 368.10	$ 359.13	$ 351.98	$ 344.90	$ 337.87	$ 330.89	$ 333.33	$ 333.33	$ 333.33	$ 333.33
Linux pConfig - 2	Fully Managed (1) - Basic Tier		1							$ 363.07	$ 354.60	$ 347.68	$ 340.81	$ 333.99	$ 327.20	$ 329.83	$ 329.83	$ 329.83	$ 329.83
Linux pConfig - 3	4-way Six-Core 2.0 GHz		1							$ 51.66	$ 46.58	$ 39.49	$ 32.17	$ 24.62	$ 16.85	$ 40.10	$ 40.10	$ 40.10	$ 40.10
	64 GB RAM		64							$ 56.12	$ 54.49	$ 50.09	$ 45.49	$ 40.67	$ 35.64	$ 52.70	$ 52.70	$ 52.70	$ 52.70
	SAN Attached Storage		500							$ 18.11	$ 18.66	$ 19.22	$ 19.79	$ 20.39	$ 21.00	$ 18.66	$ 18.66	$ 18.66	$ 18.66
	RedHat or SUSE		1							$ 153.74	$ 158.35	$ 163.10	$ 167.99	$ 173.03	$ 178.22	$ 158.35	$ 158.35	$ 158.35	$ 158.35
	Sub-Total									**$ 279.62**	**$ 278.08**	**$ 271.90**	**$ 265.44**	**$ 258.71**	**$ 251.71**	**$ 269.81**	**$ 269.81**	**$ 269.81**	**$ 269.81**
Linux pConfig - 3	Fully Managed (1) - Platinum Tier		1							$ 423.09	$ 407.19	$ 394.56	$ 381.97	$ 369.41	$ 356.88	$ 369.72	$ 369.72	$ 369.72	$ 369.72
Linux pConfig - 3	Fully Managed (1) - Gold Tier		1							$ 406.79	$ 392.52	$ 380.62	$ 368.73	$ 356.83	$ 344.93	$ 358.37	$ 358.37	$ 358.37	$ 358.37
Linux pConfig - 3	Fully Managed (1) - Silver Tier		1							$ 393.81	$ 380.84	$ 369.53	$ 358.19	$ 346.82	$ 335.42	$ 349.33	$ 349.33	$ 349.33	$ 349.33
Linux pConfig - 3	Fully Managed (1) - Bronze Tier		1							$ 388.27	$ 375.85	$ 364.79	$ 353.69	$ 342.54	$ 331.35	$ 345.47	$ 345.47	$ 345.47	$ 345.47
Linux pConfig - 3	Fully Managed (1) - Basic Tier		1							$ 383.24	$ 371.33	$ 360.49	$ 349.60	$ 338.66	$ 327.66	$ 341.97	$ 341.97	$ 341.97	$ 341.97
Linux pConfig - 4	2-way Six-Core 2.4 GHz		1							$ 57.96	$ 56.63	$ 53.37	$ 49.95	$ 46.39	$ 42.69	$ 54.47	$ 54.47	$ 54.47	$ 54.47
	16 GB RAM		16							$ 14.03	$ 13.62	$ 12.52	$ 11.37	$ 10.17	$ 8.91	$ 13.18	$ 13.18	$ 13.18	$ 13.18
	Mirrored 146 15K Hard Drives		1							$ 33.72	$ 32.75	$ 30.10	$ 27.34	$ 24.44	$ 21.42	$ 31.67	$ 31.67	$ 31.67	$ 31.67
	RedHat or SUSE		1							$ 153.74	$ 158.35	$ 163.10	$ 167.99	$ 173.03	$ 178.22	$ 158.35	$ 158.35	$ 158.35	$ 158.35
	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization		1							$ 4.46	$ 4.59	$ 4.73	$ 4.87	$ 5.02	$ 5.17	$ 4.59	$ 4.59	$ 4.59	$ 4.59
	Sub-Total									**$ 263.91**	**$ 265.95**	**$ 263.83**	**$ 261.53**	**$ 259.05**	**$ 256.42**	**$ 262.27**	**$ 262.27**	**$ 262.27**	**$ 262.27**
Linux pConfig - 4	Fully Managed (1) - Platinum Tier		1							$ 407.38	$ 395.06	$ 386.49	$ 378.06	$ 369.76	$ 361.58	$ 362.18	$ 362.18	$ 362.18	$ 362.18
Linux pConfig - 4	Fully Managed (1) - Gold Tier		1							$ 391.07	$ 380.39	$ 372.55	$ 364.81	$ 357.18	$ 349.63	$ 350.82	$ 350.82	$ 350.82	$ 350.82
Linux pConfig - 4	Fully Managed (1) - Silver Tier		1							$ 378.10	$ 368.71	$ 361.46	$ 354.27	$ 347.16	$ 340.12	$ 341.79	$ 341.79	$ 341.79	$ 341.79
Linux pConfig - 4	Fully Managed (1) - Bronze Tier		1							$ 372.56	$ 363.72	$ 356.72	$ 349.77	$ 342.89	$ 336.06	$ 337.93	$ 337.93	$ 337.93	$ 337.93
Linux pConfig - 4	Fully Managed (1) - Basic Tier		1							$ 367.53	$ 359.20	$ 352.42	$ 345.69	$ 339.01	$ 332.37	$ 334.42	$ 334.42	$ 334.42	$ 334.42
Linux pConfig - 5	2-way Six-Core 2.4 GHz		1							$ 57.96	$ 56.63	$ 53.37	$ 49.95	$ 46.39	$ 42.69	$ 54.47	$ 54.47	$ 54.47	$ 54.47
	16 GB RAM		16							$ 14.03	$ 13.62	$ 12.52	$ 11.37	$ 10.17	$ 8.91	$ 13.18	$ 13.18	$ 13.18	$ 13.18
	Mirrored 146 15K Hard Drives		1							$ 33.72	$ 32.75	$ 30.10	$ 27.34	$ 24.44	$ 21.42	$ 31.67	$ 31.67	$ 31.67	$ 31.67
	RedHat or SUSE		1							$ 153.74	$ 158.35	$ 163.10	$ 167.99	$ 173.03	$ 178.22	$ 158.35	$ 158.35	$ 158.35	$ 158.35
	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Sub-Total									**$ 259.45**	**$ 261.35**	**$ 259.09**	**$ 256.65**	**$ 254.03**	**$ 251.24**	**$ 257.67**	**$ 257.67**	**$ 257.67**	**$ 257.67**
Linux pConfig - 5	Fully Managed (1) - Platinum Tier		1							$ 402.92	$ 390.47	$ 381.76	$ 373.18	$ 364.74	$ 356.41	$ 357.58	$ 357.58	$ 357.58	$ 357.58
Linux pConfig - 5	Fully Managed (1) - Gold Tier		1							$ 386.61	$ 375.80	$ 367.82	$ 359.94	$ 352.16	$ 344.46	$ 346.23	$ 346.23	$ 346.23	$ 346.23
Linux pConfig - 5	Fully Managed (1) - Silver Tier		1							$ 373.64	$ 364.12	$ 356.72	$ 349.40	$ 342.14	$ 334.95	$ 337.19	$ 337.19	$ 337.19	$ 337.19
Linux pConfig - 5	Fully Managed (1) - Bronze Tier		1							$ 368.10	$ 359.13	$ 351.98	$ 344.90	$ 337.87	$ 330.89	$ 333.33	$ 333.33	$ 333.33	$ 333.33
Linux pConfig - 5	Fully Managed (1) - Basic Tier		1							$ 363.07	$ 354.60	$ 347.68	$ 340.81	$ 333.99	$ 327.20	$ 329.83	$ 329.83	$ 329.83	$ 329.83
x86 (Windows) - Virtual Servers																			
Windows vConfig - 1	2vCPU	Per Instance		CCSU13310069-A	N/A	N/A	A			$ 4.24	$ 4.06	$ 3.99	$ 3.92	$ 3.87	$ 3.25	$ 3.10	$ 3.10	$ 3.10	$ 3.10
Windows vConfig - 2 4 5	4vCPU	Per Instance		CCSU13310070-A	N/A	N/A	A			$ 11.24	$ 11.00	$ 10.82	$ 10.63	$ 10.44	$ 8.68	$ 8.47	$ 8.47	$ 8.47	$ 8.47
Windows vConfig - 3	8vCPU	Per Instance		CCSU13310071-A	N/A	N/A	A			$ 35.46	$ 35.00	$ 34.43	$ 33.83	$ 33.15	$ 27.47	$ 27.04	$ 27.04	$ 27.04	$ 27.04
Windows vConfig - 1, 2, 3, 4, 5	GB Ram	Per GB		CCSU13310072-A	N/A	N/A	A			$ 1.75	$ 1.75	$ 1.75	$ 1.75	$ 1.75	$ 1.75	$ 1.75	$ 1.75	$ 1.75	$ 1.75

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	**Product Name**	**Unit**	**Qty per config**	**Provider Part Number**	**Version Major**	**Version Minor**	**Version Build**	**Manufacturer ID**	**Equipment Code**	**Price per unit \ Per Month**									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Windows vConfig - 1, 2, 3, 4, 5	Windows Server 2008 R2	Per License		CCSU13310073-A	2008	R2	A			$ 12.65	$ 12.23	$ 12.08	$ 11.89	$ 11.80	$ 11.81	$ 11.21	$ 11.21	$ 11.21	$ 11.21
Windows vConfig - 1 2 3 4 5	Firewall/IDS	Per Config		CCSU13310074-A	N/A	N/A	A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 1 2 3 4 5	Site-Site VPN	Per Config		CCSU13310075-A	N/A	N/A	A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 1, 2, 3, 4, 5	VPN Client	Per Config		CCSU13310076-A	N/A	N/A	A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 1, 2, 3, 4, 5	VLAN	Per Config		CCSU13310077-A	N/A	N/A	A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 4	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Config		CCSU13310078-A	N/A	N/A	A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 5	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Config		CCSU13310079-A	N/A	N/A	A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 1	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310080-A	N/A	N/A	A			$ 68.62	$ 63.33	$ 61.10	$ 59.13	$ 57.10	$ 55.33	$ 53.56	$ 53.56	$ 53.56	$ 53.56
Windows vConfig - 1	Fully Managed (1) - Gold Tier	Per Config		CCSU13310081-A	N/A	N/A	A			$ 65.16	$ 60.49	$ 58.51	$ 56.76	$ 54.93	$ 53.33	$ 51.74	$ 51.74	$ 51.74	$ 51.74
Windows vConfig - 1	Fully Managed (1) - Silver Tier	Per Config		CCSU13310082-A	N/A	N/A	A			$ 62.06	$ 57.91	$ 56.14	$ 54.58	$ 52.93	$ 51.49	$ 50.04	$ 50.04	$ 50.04	$ 50.04
Windows vConfig - 1	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310083-A	N/A	N/A	A			$ 60.62	$ 56.71	$ 55.04	$ 53.56	$ 51.99	$ 50.62	$ 49.24	$ 49.24	$ 49.24	$ 49.24
Windows vConfig - 1	Fully Managed (1) - Basic Tier	Per Config		CCSU13310084-A	N/A	N/A	A			$ 59.26	$ 55.56	$ 53.98	$ 52.58	$ 51.09	$ 49.78	$ 48.47	$ 48.47	$ 48.47	$ 48.47
Windows vConfig - 2	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310085-A	N/A	N/A	A			$ 68.62	$ 63.33	$ 61.10	$ 59.13	$ 57.10	$ 55.33	$ 53.56	$ 53.56	$ 53.56	$ 53.56
Windows vConfig - 2	Fully Managed (1) - Gold Tier	Per Config		CCSU13310086-A	N/A	N/A	A			$ 65.16	$ 60.49	$ 58.51	$ 56.76	$ 54.93	$ 53.33	$ 51.74	$ 51.74	$ 51.74	$ 51.74
Windows vConfig - 2	Fully Managed (1) - Silver Tier	Per Config		CCSU13310087-A	N/A	N/A	A			$ 62.06	$ 57.91	$ 56.14	$ 54.58	$ 52.93	$ 51.49	$ 50.04	$ 50.04	$ 50.04	$ 50.04
Windows vConfig - 2	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310088-A	N/A	N/A	A			$ 60.62	$ 56.71	$ 55.04	$ 53.56	$ 51.99	$ 50.62	$ 49.24	$ 49.24	$ 49.24	$ 49.24
Windows vConfig - 2	Fully Managed (1) - Basic Tier	Per Config		CCSU13310089-A	N/A	N/A	A			$ 59.26	$ 55.56	$ 53.98	$ 52.58	$ 51.09	$ 49.78	$ 48.47	$ 48.47	$ 48.47	$ 48.47
Windows vConfig - 3	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310090-A	N/A	N/A	A			$ 68.62	$ 63.33	$ 61.10	$ 59.13	$ 57.10	$ 55.33	$ 53.56	$ 53.56	$ 53.56	$ 53.56
Windows vConfig - 3	Fully Managed (1) - Gold Tier	Per Config		CCSU13310091-A	N/A	N/A	A			$ 65.16	$ 60.49	$ 58.51	$ 56.76	$ 54.93	$ 53.33	$ 51.74	$ 51.74	$ 51.74	$ 51.74
Windows vConfig - 3	Fully Managed (1) - Silver Tier	Per Config		CCSU13310092-A	N/A	N/A	A			$ 62.06	$ 57.91	$ 56.14	$ 54.58	$ 52.93	$ 51.49	$ 50.04	$ 50.04	$ 50.04	$ 50.04
Windows vConfig - 3	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310093-A	N/A	N/A	A			$ 60.62	$ 56.71	$ 55.04	$ 53.56	$ 51.99	$ 50.62	$ 49.24	$ 49.24	$ 49.24	$ 49.24
Windows vConfig - 3	Fully Managed (1) - Basic Tier	Per Config		CCSU13310094-A	N/A	N/A	A			$ 59.26	$ 55.56	$ 53.98	$ 52.58	$ 51.09	$ 49.78	$ 48.47	$ 48.47	$ 48.47	$ 48.47
Windows vConfig - 4	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310095-A	N/A	N/A	A			$ 68.62	$ 63.36	$ 61.16	$ 59.13	$ 57.21	$ 55.35	$ 53.67	$ 53.67	$ 53.67	$ 53.67
Windows vConfig - 4	Fully Managed (1) - Gold Tier	Per Config		CCSU13310096-A	N/A	N/A	A			$ 65.16	$ 60.52	$ 58.57	$ 56.75	$ 55.04	$ 53.36	$ 51.84	$ 51.84	$ 51.84	$ 51.84
Windows vConfig - 4	Fully Managed (1) - Silver Tier	Per Config		CCSU13310097-A	N/A	N/A	A			$ 62.06	$ 57.94	$ 56.20	$ 54.58	$ 53.04	$ 51.52	$ 50.15	$ 50.15	$ 50.15	$ 50.15
Windows vConfig - 4	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310098-A	N/A	N/A	A			$ 60.62	$ 56.74	$ 55.10	$ 53.55	$ 52.10	$ 50.65	$ 49.35	$ 49.35	$ 49.35	$ 49.35
Windows vConfig - 4	Fully Managed (1) - Basic Tier	Per Config		CCSU13310099-A	N/A	N/A	A			$ 59.26	$ 55.59	$ 54.04	$ 52.57	$ 51.20	$ 49.81	$ 48.58	$ 48.58	$ 48.58	$ 48.58
Windows vConfig - 5	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310100-A	N/A	N/A	A			$ 68.62	$ 63.36	$ 61.16	$ 59.13	$ 57.21	$ 55.35	$ 53.67	$ 53.67	$ 53.67	$ 53.67
Windows vConfig - 5	Fully Managed (1) - Gold Tier	Per Config		CCSU13310101-A	N/A	N/A	A			$ 65.16	$ 60.52	$ 58.57	$ 56.75	$ 55.04	$ 53.36	$ 51.84	$ 51.84	$ 51.84	$ 51.84
Windows vConfig - 5	Fully Managed (1) - Silver Tier	Per Config		CCSU13310102-A	N/A	N/A	A			$ 62.06	$ 57.94	$ 56.20	$ 54.58	$ 53.04	$ 51.52	$ 50.15	$ 50.15	$ 50.15	$ 50.15
Windows vConfig - 5	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310103-A	N/A	N/A	A			$ 60.62	$ 56.74	$ 55.10	$ 53.55	$ 52.10	$ 50.65	$ 49.35	$ 49.35	$ 49.35	$ 49.35
Windows vConfig - 5	Fully Managed (1) - Basic Tier	Per Config		CCSU13310104-A	N/A	N/A	A			$ 59.26	$ 55.59	$ 54.04	$ 52.57	$ 51.20	$ 49.81	$ 48.58	$ 48.58	$ 48.58	$ 48.58
Windows vConfig - 1	2vCPU		1							$ 4.24	$ 4.06	$ 3.99	$ 3.92	$ 3.87	$ 3.25	$ 3.10	$ 3.10	$ 3.10	$ 3.10
	GB Ram		4							$ 7.00	$ 7.00	$ 7.00	$ 7.00	$ 7.00	$ 7.00	$ 7.00	$ 7.00	$ 7.00	$ 7.00
	Windows Server 2008 R2		1							$ 12.65	$ 12.23	$ 12.08	$ 11.89	$ 11.80	$ 11.81	$ 11.21	$ 11.21	$ 11.21	$ 11.21
	Firewall/IDS		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Site-Site VPN		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	VPN Client		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	VLAN		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Sub-Total									**$ 23.89**	**$ 23.29**	**$ 23.08**	**$ 22.81**	**$ 22.67**	**$ 22.06**	**$ 21.31**	**$ 21.31**	**$ 21.31**	**$ 21.31**
Windows vConfig - 1	Fully Managed (1) - Platinum Tier		1							$ 92.51	$ 86.63	$ 84.18	$ 81.95	$ 79.78	$ 77.39	$ 74.87	$ 74.87	$ 74.87	$ 74.87
Windows vConfig - 1	Fully Managed (1) - Gold Tier		1							$ 89.05	$ 83.78	$ 81.58	$ 79.57	$ 77.60	$ 75.40	$ 73.04	$ 73.04	$ 73.04	$ 73.04
Windows vConfig - 1	Fully Managed (1) - Silver Tier		1							$ 85.95	$ 81.20	$ 79.22	$ 77.39	$ 75.61	$ 73.55	$ 71.35	$ 71.35	$ 71.35	$ 71.35
Windows vConfig - 1	Fully Managed (1) - Bronze Tier		1							$ 84.52	$ 80.00	$ 78.11	$ 76.37	$ 74.67	$ 72.69	$ 70.55	$ 70.55	$ 70.55	$ 70.55
Windows vConfig - 1	Fully Managed (1) - Basic Tier		1							$ 83.15	$ 78.85	$ 77.05	$ 75.39	$ 73.76	$ 71.85	$ 69.78	$ 69.78	$ 69.78	$ 69.78
Windows vConfig - 2	4vCPU		1							$ 11.24	$ 11.00	$ 10.82	$ 10.63	$ 10.44	$ 8.68	$ 8.47	$ 8.47	$ 8.47	$ 8.47
	GB Ram		16							$ 28.00	$ 28.00	$ 28.00	$ 28.00	$ 28.00	$ 28.00	$ 28.00	$ 28.00	$ 28.00	$ 28.00
	Windows Server 2008 R2		1							$ 12.65	$ 12.23	$ 12.08	$ 11.89	$ 11.80	$ 11.81	$ 11.21	$ 11.21	$ 11.21	$ 11.21
	Firewall/IDS		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Site-Site VPN		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	VPN Client		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	VLAN		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Sub-Total									**$ 51.90**	**$ 51.23**	**$ 50.90**	**$ 50.52**	**$ 50.24**	**$ 48.50**	**$ 47.68**	**$ 47.68**	**$ 47.68**	**$ 47.68**
Windows vConfig - 2	Fully Managed (1) - Platinum Tier		1							$ 120.51	$ 114.57	$ 112.00	$ 109.65	$ 107.34	$ 103.82	$ 101.24	$ 101.24	$ 101.24	$ 101.24
Windows vConfig - 2	Fully Managed (1) - Gold Tier		1							$ 117.05	$ 111.72	$ 109.41	$ 107.27	$ 105.17	$ 101.83	$ 99.41	$ 99.41	$ 99.41	$ 99.41
Windows vConfig - 2	Fully Managed (1) - Silver Tier		1							$ 113.95	$ 109.14	$ 107.04	$ 105.10	$ 103.17	$ 99.99	$ 97.72	$ 97.72	$ 97.72	$ 97.72
Windows vConfig - 2	Fully Managed (1) - Bronze Tier		1							$ 112.52	$ 107.94	$ 105.94	$ 104.07	$ 102.23	$ 99.12	$ 96.92	$ 96.92	$ 96.92	$ 96.92
Windows vConfig - 2	Fully Managed (1) - Basic Tier		1							$ 111.15	$ 106.79	$ 104.88	$ 103.09	$ 101.33	$ 98.28	$ 96.15	$ 96.15	$ 96.15	$ 96.15
Windows vConfig - 3	8vCPU		1							$ 35.46	$ 35.00	$ 34.43	$ 33.83	$ 33.15	$ 27.47	$ 27.04	$ 27.04	$ 27.04	$ 27.04
	GB Ram		64							$ 112.00	$ 112.00	$ 112.00	$ 112.00	$ 112.00	$ 112.00	$ 112.00	$ 112.00	$ 112.00	$ 112.00
	Windows Server 2008 R2		1							$ 12.65	$ 12.23	$ 12.08	$ 11.89	$ 11.80	$ 11.81	$ 11.21	$ 11.21	$ 11.21	$ 11.21
	Firewall/IDS		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Site-Site VPN		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	VPN Client		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	VLAN		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Sub-Total									**$ 160.11**	**$ 159.23**	**$ 158.52**	**$ 157.72**	**$ 156.95**	**$ 151.28**	**$ 150.26**	**$ 150.26**	**$ 150.26**	**$ 150.26**
Windows vConfig - 3	Fully Managed (1) - Platinum Tier		1							$ 228.73	$ 222.57	$ 219.62	$ 216.86	$ 214.05	$ 206.61	$ 203.82	$ 203.82	$ 203.82	$ 203.82
Windows vConfig - 3	Fully Managed (1) - Gold Tier		1							$ 225.27	$ 219.72	$ 217.02	$ 214.48	$ 211.88	$ 204.61	$ 201.99	$ 201.99	$ 201.99	$ 201.99

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	**Product Name**	**Unit**	**Qty per config**	**Provider Part Number**	**Version Major**	**Version Minor**	**Version Build**	**Manufacturer ID**	**Equipment Code**	**Price per unit \ Per Month**									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Windows vConfig - 3	Fully Managed (1) - Silver Tier		1							$ 222.17	$ 217.14	$ 214.66	$ 212.30	$ 209.88	$ 202.77	$ 200.30	$ 200.30	$ 200.30	$ 200.30
Windows vConfig - 3	Fully Managed (1) - Bronze Tier		1							$ 220.73	$ 215.94	$ 213.55	$ 211.28	$ 208.94	$ 201.90	$ 199.50	$ 199.50	$ 199.50	$ 199.50
Windows vConfig - 3	Fully Managed (1) - Basic Tier		1							$ 219.37	$ 214.79	$ 212.49	$ 210.30	$ 208.04	$ 201.07	$ 198.72	$ 198.72	$ 198.72	$ 198.72
Windows vConfig - 4	4vCPU		1							$ 11.24	$ 11.00	$ 10.82	$ 10.63	$ 10.44	$ 8.68	$ 8.47	$ 8.47	$ 8.47	$ 8.47
	GB Ram		16							$ 28.00	$ 28.00	$ 28.00	$ 28.00	$ 28.00	$ 28.00	$ 28.00	$ 28.00	$ 28.00	$ 28.00
	Windows Server 2008 R2		1							$ 12.65	$ 12.23	$ 12.08	$ 11.89	$ 11.80	$ 11.81	$ 11.21	$ 11.21	$ 11.21	$ 11.21
	Firewall/IDS		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Site-Site VPN		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	VPN Client		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	VLAN		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Sub-Total									**$ 51.90**	**$ 51.23**	**$ 50.90**	**$ 50.52**	**$ 50.24**	**$ 48.50**	**$ 47.68**	**$ 47.68**	**$ 47.68**	**$ 47.68**
Windows vConfig - 4	Fully Managed (1) - Platinum Tier		1							$ 120.51	$ 114.59	$ 112.06	$ 109.65	$ 107.45	$ 103.85	$ 101.35	$ 101.35	$ 101.35	$ 101.35
Windows vConfig - 4	Fully Managed (1) - Gold Tier		1							$ 117.05	$ 111.75	$ 109.47	$ 107.27	$ 105.28	$ 101.85	$ 99.52	$ 99.52	$ 99.52	$ 99.52
Windows vConfig - 4	Fully Managed (1) - Silver Tier		1							$ 113.95	$ 109.17	$ 107.11	$ 105.10	$ 103.28	$ 100.01	$ 97.83	$ 97.83	$ 97.83	$ 97.83
Windows vConfig - 4	Fully Managed (1) - Bronze Tier		1							$ 112.52	$ 107.97	$ 106.00	$ 104.07	$ 102.34	$ 99.14	$ 97.03	$ 97.03	$ 97.03	$ 97.03
Windows vConfig - 4	Fully Managed (1) - Basic Tier		1							$ 111.15	$ 106.82	$ 104.94	$ 103.09	$ 101.43	$ 98.31	$ 96.25	$ 96.25	$ 96.25	$ 96.25
Windows vConfig - 5	4vCPU		1							$ 11.24	$ 11.00	$ 10.82	$ 10.63	$ 10.44	$ 8.68	$ 8.47	$ 8.47	$ 8.47	$ 8.47
	GB Ram		16							$ 28.00	$ 28.00	$ 28.00	$ 28.00	$ 28.00	$ 28.00	$ 28.00	$ 28.00	$ 28.00	$ 28.00
	Windows Server 2008 R2		1							$ 12.65	$ 12.23	$ 12.08	$ 11.89	$ 11.80	$ 11.81	$ 11.21	$ 11.21	$ 11.21	$ 11.21
	Firewall/IDS		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Site-Site VPN		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	VPN Client		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	VLAN		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Sub-Total									**$ 51.90**	**$ 51.23**	**$ 50.90**	**$ 50.52**	**$ 50.24**	**$ 48.50**	**$ 47.68**	**$ 47.68**	**$ 47.68**	**$ 47.68**
Windows vConfig - 5	Fully Managed (1) - Platinum Tier		1							$ 120.51	$ 114.59	$ 112.06	$ 109.65	$ 107.45	$ 103.85	$ 101.35	$ 101.35	$ 101.35	$ 101.35
Windows vConfig - 5	Fully Managed (1) - Gold Tier		1							$ 117.05	$ 111.75	$ 109.47	$ 107.27	$ 105.28	$ 101.85	$ 99.52	$ 99.52	$ 99.52	$ 99.52
Windows vConfig - 5	Fully Managed (1) - Silver Tier		1							$ 113.95	$ 109.17	$ 107.11	$ 105.10	$ 103.28	$ 100.01	$ 97.83	$ 97.83	$ 97.83	$ 97.83
Windows vConfig - 5	Fully Managed (1) - Bronze Tier		1							$ 112.52	$ 107.97	$ 106.00	$ 104.07	$ 102.34	$ 99.14	$ 97.03	$ 97.03	$ 97.03	$ 97.03
Windows vConfig - 5	Fully Managed (1) - Basic Tier		1							$ 111.15	$ 106.82	$ 104.94	$ 103.09	$ 101.43	$ 98.31	$ 96.25	$ 96.25	$ 96.25	$ 96.25
x86 (Linux) - Virtual Servers																			
Linux vConfig - 1	2vCPU	Per Instance		CCSU13310105-A	N/A	N/A	A			$ 4.24	$ 4.06	$ 3.99	$ 3.92	$ 3.87	$ 3.25	$ 3.10	$ 3.10	$ 3.10	$ 3.10
Linux vConfig - 2, 4, 5	4vCPU	Per Instance		CCSU13310106-A	N/A	N/A	A			$ 11.24	$ 11.00	$ 10.82	$ 10.63	$ 10.44	$ 8.68	$ 8.47	$ 8.47	$ 8.47	$ 8.47
Linux vConfig - 3	8vCPU	Per Instance		CCSU13310107-A	N/A	N/A	A			$ 35.46	$ 35.00	$ 34.43	$ 33.83	$ 33.15	$ 27.47	$ 27.04	$ 27.04	$ 27.04	$ 27.04
Linux vConfig - 1 2 3 4 5	GB Ram	Per GB		CCSU13310108-A	N/A	N/A	A			$ 1.75	$ 1.75	$ 1.75	$ 1.75	$ 1.75	$ 1.75	$ 1.75	$ 1.75	$ 1.75	$ 1.75
Linux vConfig - 1 2 3 4 5	RedHat or SUSE	Per License		CCSU13310109-A	N/A	N/A	A			$ 12.51	$ 12.10	$ 11.94	$ 11.75	$ 11.66	$ 11.68	$ 11.08	$ 11.08	$ 11.08	$ 11.08
Linux vConfig - 1, 2, 3, 4, 5	Firewall/IDS	Per Config		CCSU13310110-A	N/A	N/A	A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 1, 2, 3, 4, 5	Site-Site VPN	Per Config		CCSU13310111-A	N/A	N/A	A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 1 2 3 4 5	VPN Client	Per Config		CCSU13310112-A	N/A	N/A	A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 1 2 3 4 5	VLAN	Per Config		CCSU13310113-A	N/A	N/A	A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 4	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Config		CCSU13310114-A	N/A	N/A	A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 5	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Config		CCSU13310115-A	N/A	N/A	A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 1	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310116-A	N/A	N/A	A			$ 148.14	$ 134.24	$ 129.19	$ 123.49	$ 118.44	$ 112.98	$ 108.28	$ 108.28	$ 108.28	$ 108.28
Linux vConfig - 1	Fully Managed (1) - Gold Tier	Per Config		CCSU13310117-A	N/A	N/A	A			$ 131.83	$ 121.05	$ 117.14	$ 112.63	$ 108.59	$ 104.16	$ 100.30	$ 100.30	$ 100.30	$ 100.30
Linux vConfig - 1	Fully Managed (1) - Silver Tier	Per Config		CCSU13310118-A	N/A	N/A	A			$ 118.86	$ 110.31	$ 107.22	$ 103.60	$ 100.31	$ 96.66	$ 93.47	$ 93.47	$ 93.47	$ 93.47
Linux vConfig - 1	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310119-A	N/A	N/A	A			$ 113.31	$ 105.65	$ 102.89	$ 99.63	$ 96.66	$ 93.33	$ 90.41	$ 90.41	$ 90.41	$ 90.41
Linux vConfig - 1	Fully Managed (1) - Basic Tier	Per Config		CCSU13310120-A	N/A	N/A	A			$ 108.28	$ 101.39	$ 98.92	$ 95.97	$ 93.27	$ 90.23	$ 87.55	$ 87.55	$ 87.55	$ 87.55
Linux vConfig - 2	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310121-A	N/A	N/A	A			$ 148.14	$ 134.24	$ 129.19	$ 123.49	$ 118.44	$ 112.98	$ 108.28	$ 108.28	$ 108.28	$ 108.28
Linux vConfig - 2	Fully Managed (1) - Gold Tier	Per Config		CCSU13310122-A	N/A	N/A	A			$ 131.83	$ 121.05	$ 117.14	$ 112.63	$ 108.59	$ 104.16	$ 100.30	$ 100.30	$ 100.30	$ 100.30
Linux vConfig - 2	Fully Managed (1) - Silver Tier	Per Config		CCSU13310123-A	N/A	N/A	A			$ 118.86	$ 110.31	$ 107.22	$ 103.60	$ 100.31	$ 96.66	$ 93.47	$ 93.47	$ 93.47	$ 93.47
Linux vConfig - 2	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310124-A	N/A	N/A	A			$ 113.31	$ 105.65	$ 102.89	$ 99.63	$ 96.66	$ 93.33	$ 90.41	$ 90.41	$ 90.41	$ 90.41
Linux vConfig - 2	Fully Managed (1) - Basic Tier	Per Config		CCSU13310125-A	N/A	N/A	A			$ 108.28	$ 101.39	$ 98.92	$ 95.97	$ 93.27	$ 90.23	$ 87.55	$ 87.55	$ 87.55	$ 87.55
Linux vConfig - 3	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310126-A	N/A	N/A	A			$ 148.14	$ 134.24	$ 129.19	$ 123.49	$ 118.44	$ 112.98	$ 108.28	$ 108.28	$ 108.28	$ 108.28
Linux vConfig - 3	Fully Managed (1) - Gold Tier	Per Config		CCSU13310127-A	N/A	N/A	A			$ 131.83	$ 121.05	$ 117.14	$ 112.63	$ 108.59	$ 104.16	$ 100.30	$ 100.30	$ 100.30	$ 100.30
Linux vConfig - 3	Fully Managed (1) - Silver Tier	Per Config		CCSU13310128-A	N/A	N/A	A			$ 118.86	$ 110.31	$ 107.22	$ 103.60	$ 100.31	$ 96.66	$ 93.47	$ 93.47	$ 93.47	$ 93.47
Linux vConfig - 3	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310129-A	N/A	N/A	A			$ 113.31	$ 105.65	$ 102.89	$ 99.63	$ 96.66	$ 93.33	$ 90.41	$ 90.41	$ 90.41	$ 90.41
Linux vConfig - 3	Fully Managed (1) - Basic Tier	Per Config		CCSU13310130-A	N/A	N/A	A			$ 108.28	$ 101.39	$ 98.92	$ 95.97	$ 93.27	$ 90.23	$ 87.55	$ 87.55	$ 87.55	$ 87.55
Linux vConfig - 4	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310131-A	N/A	N/A	A			$ 148.14	$ 134.29	$ 129.31	$ 123.68	$ 118.52	$ 113.07	$ 108.46	$ 108.46	$ 108.46	$ 108.46
Linux vConfig - 4	Fully Managed (1) - Gold Tier	Per Config		CCSU13310132-A	N/A	N/A	A			$ 131.83	$ 121.11	$ 117.26	$ 112.82	$ 108.67	$ 104.24	$ 100.48	$ 100.48	$ 100.48	$ 100.48
Linux vConfig - 4	Fully Managed (1) - Silver Tier	Per Config		CCSU13310133-A	N/A	N/A	A			$ 118.86	$ 110.36	$ 107.34	$ 103.79	$ 100.40	$ 96.75	$ 93.65	$ 93.65	$ 93.65	$ 93.65
Linux vConfig - 4	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310134-A	N/A	N/A	A			$ 113.31	$ 105.71	$ 103.01	$ 99.81	$ 96.74	$ 93.41	$ 90.59	$ 90.59	$ 90.59	$ 90.59
Linux vConfig - 4	Fully Managed (1) - Basic Tier	Per Config		CCSU13310135-A	N/A	N/A	A			$ 108.28	$ 101.44	$ 99.03	$ 96.15	$ 93.35	$ 90.31	$ 87.74	$ 87.74	$ 87.74	$ 87.74
Linux vConfig - 5	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310136-A	N/A	N/A	A			$ 148.14	$ 134.29	$ 129.31	$ 123.68	$ 118.52	$ 113.07	$ 108.46	$ 108.46	$ 108.46	$ 108.46
Linux vConfig - 5	Fully Managed (1) - Gold Tier	Per Config		CCSU13310137-A	N/A	N/A	A			$ 131.83	$ 121.11	$ 117.26	$ 112.82	$ 108.67	$ 104.24	$ 100.48	$ 100.48	$ 100.48	$ 100.48

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	**Product Name**	**Unit**	**Qty per config**	**Provider Part Number**	**Version Major**	**Version Minor**	**Version Build**	**Manufacturer ID**	**Equipment Code**	**Price per unit \ Per Month**									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Linux vConfig - 5	Fully Managed (1) - Silver Tier	Per Config		CCSU13310138-A	N/A	N/A	A			$ 118.86	$ 110.36	$ 107.34	$ 103.79	$ 100.40	$ 96.75	$ 93.65	$ 93.65	$ 93.65	$ 93.65
Linux vConfig - 5	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310139-A	N/A	N/A	A			$ 113.31	$ 105.71	$ 103.01	$ 99.81	$ 96.74	$ 93.41	$ 90.59	$ 90.59	$ 90.59	$ 90.59
Linux vConfig - 5	Fully Managed (1) - Basic Tier	Per Config		CCSU13310140-A	N/A	N/A	A			$ 108.28	$ 101.44	$ 99.03	$ 96.15	$ 93.35	$ 90.31	$ 87.74	$ 87.74	$ 87.74	$ 87.74
Linux vConfig - 1	2vCPU		1							$ 4.24	$ 4.06	$ 3.99	$ 3.92	$ 3.87	$ 3.25	$ 3.10	$ 3.10	$ 3.10	$ 3.10
	GB Ram		4							$ 7.00	$ 7.00	$ 7.00	$ 7.00	$ 7.00	$ 7.00	$ 7.00	$ 7.00	$ 7.00	$ 7.00
	RedHat or SUSE		1							$ 12.51	$ 12.10	$ 11.94	$ 11.75	$ 11.66	$ 11.68	$ 11.08	$ 11.08	$ 11.08	$ 11.08
	Firewall/IDS		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Site-Site VPN		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	VPN Client		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	VLAN		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Sub-Total									**$ 23.75**	**$ 23.16**	**$ 22.94**	**$ 22.67**	**$ 22.54**	**$ 21.93**	**$ 21.17**	**$ 21.17**	**$ 21.17**	**$ 21.17**
Linux vConfig - 1	Fully Managed (1) - Platinum Tier		1							$ 171.89	$ 157.39	$ 152.13	$ 146.17	$ 140.97	$ 134.91	$ 129.45	$ 129.45	$ 129.45	$ 129.45
Linux vConfig - 1	Fully Managed (1) - Gold Tier		1							$ 155.59	$ 144.21	$ 140.08	$ 135.31	$ 131.12	$ 126.09	$ 121.47	$ 121.47	$ 121.47	$ 121.47
Linux vConfig - 1	Fully Managed (1) - Silver Tier		1							$ 142.61	$ 133.46	$ 130.16	$ 126.27	$ 122.85	$ 118.59	$ 114.64	$ 114.64	$ 114.64	$ 114.64
Linux vConfig - 1	Fully Managed (1) - Bronze Tier		1							$ 137.07	$ 128.81	$ 125.83	$ 122.30	$ 119.19	$ 115.26	$ 111.58	$ 111.58	$ 111.58	$ 111.58
Linux vConfig - 1	Fully Managed (1) - Basic Tier		1							$ 132.04	$ 124.54	$ 121.85	$ 118.64	$ 115.80	$ 112.16	$ 108.73	$ 108.73	$ 108.73	$ 108.73
Linux vConfig - 2	4vCPU		1							$ 11.24	$ 11.00	$ 10.82	$ 10.63	$ 10.44	$ 8.68	$ 8.47	$ 8.47	$ 8.47	$ 8.47
	GB Ram		16							$ 28.00	$ 28.00	$ 28.00	$ 28.00	$ 28.00	$ 28.00	$ 28.00	$ 28.00	$ 28.00	$ 28.00
	RedHat or SUSE		1							$ 12.51	$ 12.10	$ 11.94	$ 11.75	$ 11.66	$ 11.68	$ 11.08	$ 11.08	$ 11.08	$ 11.08
	Firewall/IDS		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Site-Site VPN		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	VPN Client		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	VLAN		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Sub-Total									**$ 51.76**	**$ 51.09**	**$ 50.76**	**$ 50.38**	**$ 50.10**	**$ 48.36**	**$ 47.54**	**$ 47.54**	**$ 47.54**	**$ 47.54**
Linux vConfig - 2	Fully Managed (1) - Platinum Tier		1							$ 199.89	$ 185.33	$ 179.96	$ 173.87	$ 168.54	$ 161.35	$ 155.82	$ 155.82	$ 155.82	$ 155.82
Linux vConfig - 2	Fully Managed (1) - Gold Tier		1							$ 183.59	$ 172.15	$ 167.91	$ 163.01	$ 158.69	$ 152.52	$ 147.84	$ 147.84	$ 147.84	$ 147.84
Linux vConfig - 2	Fully Managed (1) - Silver Tier		1							$ 170.61	$ 161.40	$ 157.99	$ 153.98	$ 150.42	$ 145.03	$ 141.01	$ 141.01	$ 141.01	$ 141.01
Linux vConfig - 2	Fully Managed (1) - Bronze Tier		1							$ 165.07	$ 156.74	$ 153.66	$ 150.01	$ 146.76	$ 141.69	$ 137.95	$ 137.95	$ 137.95	$ 137.95
Linux vConfig - 2	Fully Managed (1) - Basic Tier		1							$ 160.04	$ 152.48	$ 149.68	$ 146.35	$ 143.37	$ 138.59	$ 135.10	$ 135.10	$ 135.10	$ 135.10
Linux vConfig - 3	8vCPU		1							$ 35.46	$ 35.00	$ 34.43	$ 33.83	$ 33.15	$ 27.47	$ 27.04	$ 27.04	$ 27.04	$ 27.04
	GB Ram		64							$ 112.00	$ 112.00	$ 112.00	$ 112.00	$ 112.00	$ 112.00	$ 112.00	$ 112.00	$ 112.00	$ 112.00
	RedHat or SUSE		1							$ 12.51	$ 12.10	$ 11.94	$ 11.75	$ 11.66	$ 11.68	$ 11.08	$ 11.08	$ 11.08	$ 11.08
	Firewall/IDS		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Site-Site VPN		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	VPN Client		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	VLAN		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Sub-Total									**$ 159.97**	**$ 159.09**	**$ 158.38**	**$ 157.58**	**$ 156.81**	**$ 151.15**	**$ 150.12**	**$ 150.12**	**$ 150.12**	**$ 150.12**
Linux vConfig - 3	Fully Managed (1) - Platinum Tier		1							$ 308.11	$ 293.33	$ 287.57	$ 281.08	$ 275.25	$ 264.13	$ 258.40	$ 258.40	$ 258.40	$ 258.40
Linux vConfig - 3	Fully Managed (1) - Gold Tier		1							$ 291.81	$ 280.15	$ 275.52	$ 270.22	$ 265.40	$ 255.30	$ 250.42	$ 250.42	$ 250.42	$ 250.42
Linux vConfig - 3	Fully Managed (1) - Silver Tier		1							$ 278.83	$ 269.40	$ 265.60	$ 261.18	$ 257.12	$ 247.81	$ 243.59	$ 243.59	$ 243.59	$ 243.59
Linux vConfig - 3	Fully Managed (1) - Bronze Tier		1							$ 273.29	$ 264.74	$ 261.27	$ 257.21	$ 253.47	$ 244.48	$ 240.53	$ 240.53	$ 240.53	$ 240.53
Linux vConfig - 3	Fully Managed (1) - Basic Tier		1							$ 268.26	$ 260.48	$ 257.30	$ 253.55	$ 250.08	$ 241.37	$ 237.68	$ 237.68	$ 237.68	$ 237.68
Linux vConfig - 4	4vCPU		1							$ 11.24	$ 11.00	$ 10.82	$ 10.63	$ 10.44	$ 8.68	$ 8.47	$ 8.47	$ 8.47	$ 8.47
	GB Ram		16							$ 28.00	$ 28.00	$ 28.00	$ 28.00	$ 28.00	$ 28.00	$ 28.00	$ 28.00	$ 28.00	$ 28.00
	RedHat or SUSE		1							$ 12.51	$ 12.10	$ 11.94	$ 11.75	$ 11.66	$ 11.68	$ 11.08	$ 11.08	$ 11.08	$ 11.08
	Firewall/IDS		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Site-Site VPN		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	VPN Client		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	VLAN		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Sub-Total									**$ 51.76**	**$ 51.09**	**$ 50.76**	**$ 50.38**	**$ 50.10**	**$ 48.36**	**$ 47.54**	**$ 47.54**	**$ 47.54**	**$ 47.54**
Linux vConfig - 4	Fully Managed (1) - Platinum Tier		1							$ 199.89	$ 185.39	$ 180.07	$ 174.06	$ 168.62	$ 161.43	$ 156.01	$ 156.01	$ 156.01	$ 156.01
Linux vConfig - 4	Fully Managed (1) - Gold Tier		1							$ 183.59	$ 172.20	$ 168.02	$ 163.20	$ 158.77	$ 152.60	$ 148.03	$ 148.03	$ 148.03	$ 148.03
Linux vConfig - 4	Fully Managed (1) - Silver Tier		1							$ 170.61	$ 161.46	$ 158.10	$ 154.17	$ 150.50	$ 145.11	$ 141.20	$ 141.20	$ 141.20	$ 141.20
Linux vConfig - 4	Fully Managed (1) - Bronze Tier		1							$ 165.07	$ 156.80	$ 153.77	$ 150.20	$ 146.84	$ 141.78	$ 138.14	$ 138.14	$ 138.14	$ 138.14
Linux vConfig - 4	Fully Managed (1) - Basic Tier		1							$ 160.04	$ 152.54	$ 149.80	$ 146.53	$ 143.45	$ 138.67	$ 135.28	$ 135.28	$ 135.28	$ 135.28
Linux vConfig - 5	4vCPU		1							$ 11.24	$ 11.00	$ 10.82	$ 10.63	$ 10.44	$ 8.68	$ 8.47	$ 8.47	$ 8.47	$ 8.47
	GB Ram		16							$ 28.00	$ 28.00	$ 28.00	$ 28.00	$ 28.00	$ 28.00	$ 28.00	$ 28.00	$ 28.00	$ 28.00
	RedHat or SUSE		1							$ 12.51	$ 12.10	$ 11.94	$ 11.75	$ 11.66	$ 11.68	$ 11.08	$ 11.08	$ 11.08	$ 11.08
	Firewall/IDS		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Site-Site VPN		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	VPN Client		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	VLAN		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Sub-Total									**$ 51.76**	**$ 51.09**	**$ 50.76**	**$ 50.38**	**$ 50.10**	**$ 48.36**	**$ 47.54**	**$ 47.54**	**$ 47.54**	**$ 47.54**
Linux vConfig - 5	Fully Managed (1) - Platinum Tier		1							$ 199.89	$ 185.39	$ 180.07	$ 174.06	$ 168.62	$ 161.43	$ 156.01	$ 156.01	$ 156.01	$ 156.01
Linux vConfig - 5	Fully Managed (1) - Gold Tier		1							$ 183.59	$ 172.20	$ 168.02	$ 163.20	$ 158.77	$ 152.60	$ 148.03	$ 148.03	$ 148.03	$ 148.03
Linux vConfig - 5	Fully Managed (1) - Silver Tier		1							$ 170.61	$ 161.46	$ 158.10	$ 154.17	$ 150.50	$ 145.11	$ 141.20	$ 141.20	$ 141.20	$ 141.20

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	**Product Name**	**Unit**	**Qty per config**	**Provider Part Number**	**Version Major**	**Version Minor**	**Version Build**	**Manufacturer ID**	**Equipment Code**	**Price per unit \ Per Month**									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Linux vConfig - 5	Fully Managed (1) - Bronze Tier		1							$ 165.07	$ 156.80	$ 153.77	$ 150.20	$ 146.84	$ 141.78	$ 138.14	$ 138.14	$ 138.14	$ 138.14
Linux vConfig - 5	Fully Managed (1) - Basic Tier		1							$ 160.04	$ 152.54	$ 149.80	$ 146.53	$ 143.45	$ 138.67	$ 135.28	$ 135.28	$ 135.28	$ 135.28
P-Series Server Configurations																			
AIX Config - 1 2 3 4 5	3.0GHz POWER7	Per Server		CCSI13310141-A	N/A	N/A	A			$ 99.96	$ 98.97	$ 97.97	$ 96.99	$ 96.01	$ 95.06	$ 94.11	$ 93.18	$ 92.24	$ 91.32
AIX Config - 1	Cores	Per .5 Core		CCSI13310142-A	N/A	N/A	A			$ 31.02	$ 30.71	$ 30.41	$ 30.11	$ 29.80	$ 29.50	$ 29.20	$ 28.91	$ 28.62	$ 28.33
AIX Config - 1, 2, 3, 4, 5	GB RAM	Per GB		CCSI13310143-A	N/A	N/A	A			$ 1.30	$ 1.29	$ 1.27	$ 1.26	$ 1.26	$ 1.25	$ 1.24	$ 1.23	$ 1.23	$ 1.22
AIX Config - 1 2 3 4 5	AIX	Per License		CCSI13310144-A	N/A	N/A	A			$ 48.26	$ 50.84	$ 52.57	$ 56.02	$ 58.60	$ 61.18	$ 64.63	$ 68.94	$ 68.94	$ 68.94
AIX Config - 4	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Config		CCSI13310145-A	N/A	N/A	A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 5	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Config		CCSI13310146-A	N/A	N/A	A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 1	Fully Managed (1) - Platinum Tier	Per Config		CCSI13310147-A	N/A	N/A	A			$ 496.37	$ 488.10	$ 480.68	$ 471.52	$ 463.22	$ 455.76	$ 447.42	$ 438.22	$ 433.32	$ 428.40
AIX Config - 1	Fully Managed (1) - Gold Tier	Per Config		CCSI13310148-A	N/A	N/A	A			$ 380.03	$ 373.48	$ 367.78	$ 360.36	$ 353.77	$ 347.18	$ 339.70	$ 331.37	$ 327.33	$ 323.27
AIX Config - 1	Fully Managed (1) - Silver Tier	Per Config		CCSI13310149-A	N/A	N/A	A			$ 280.93	$ 275.24	$ 270.41	$ 263.84	$ 258.12	$ 252.39	$ 245.77	$ 238.29	$ 235.11	$ 231.93
AIX Config - 1	Fully Managed (1) - Bronze Tier	Per Config		CCSI13310150-A	N/A	N/A	A			$ 181.82	$ 177.01	$ 173.04	$ 167.33	$ 162.46	$ 157.59	$ 151.85	$ 145.22	$ 142.91	$ 140.58
AIX Config - 1	Fully Managed (1) - Basic Tier	Per Config		CCSI13310151-A	N/A	N/A	A			$ 82.73	$ 78.76	$ 75.66	$ 70.81	$ 66.81	$ 62.80	$ 57.92	$ 52.16	$ 50.70	$ 49.23
AIX Config - 2	Fully Managed (1) - Platinum Tier	Per Config		CCSI13310152-A	N/A	N/A	A			$ 507.57	$ 499.50	$ 492.29	$ 483.34	$ 475.23	$ 467.12	$ 458.12	$ 448.26	$ 442.69	$ 437.11
AIX Config - 2	Fully Managed (1) - Gold Tier	Per Config		CCSI13310153-A	N/A	N/A	A			$ 391.23	$ 384.03	$ 377.68	$ 369.59	$ 362.35	$ 355.09	$ 347.82	$ 339.68	$ 335.84	$ 331.97
AIX Config - 2	Fully Managed (1) - Silver Tier	Per Config		CCSI13310154-A	N/A	N/A	A			$ 292.14	$ 285.79	$ 280.30	$ 273.07	$ 267.55	$ 262.02	$ 255.62	$ 248.33	$ 245.35	$ 242.35
AIX Config - 2	Fully Managed (1) - Bronze Tier	Per Config		CCSI13310155-A	N/A	N/A	A			$ 193.03	$ 188.41	$ 184.65	$ 179.14	$ 174.48	$ 169.82	$ 164.27	$ 157.84	$ 155.73	$ 153.59
AIX Config - 2	Fully Managed (1) - Basic Tier	Per Config		CCSI13310156-A	N/A	N/A	A			$ 93.93	$ 90.18	$ 87.27	$ 82.63	$ 78.83	$ 75.02	$ 70.33	$ 64.77	$ 63.52	$ 62.25
AIX Config - 3	Fully Managed (1) - Platinum Tier	Per Config		CCSI13310157-A	N/A	N/A	A			$ 536.01	$ 527.29	$ 519.42	$ 509.81	$ 501.91	$ 493.99	$ 485.19	$ 475.52	$ 470.16	$ 464.77
AIX Config - 3	Fully Managed (1) - Gold Tier	Per Config		CCSI13310158-A	N/A	N/A	A			$ 419.67	$ 412.67	$ 406.54	$ 398.64	$ 391.60	$ 384.55	$ 376.62	$ 367.81	$ 363.30	$ 358.77
AIX Config - 3	Fully Managed (1) - Silver Tier	Per Config		CCSI13310159-A	N/A	N/A	A			$ 307.64	$ 301.50	$ 296.22	$ 289.20	$ 283.02	$ 276.83	$ 269.75	$ 261.81	$ 258.16	$ 254.51
AIX Config - 3	Fully Managed (1) - Bronze Tier	Per Config		CCSI13310160-A	N/A	N/A	A			$ 221.47	$ 216.19	$ 211.78	$ 205.61	$ 200.29	$ 194.97	$ 188.75	$ 181.67	$ 178.88	$ 176.08
AIX Config - 3	Fully Managed (1) - Basic Tier	Per Config		CCSI13310161-A	N/A	N/A	A			$ 122.37	$ 117.95	$ 114.40	$ 109.10	$ 104.64	$ 100.17	$ 94.82	$ 88.60	$ 86.68	$ 84.73
AIX Config - 4	Fully Managed (1) - Platinum Tier	Per Config		CCSI13310162-A	N/A	N/A	A			$ 507.57	$ 499.50	$ 492.29	$ 483.34	$ 475.23	$ 467.12	$ 458.12	$ 448.26	$ 442.69	$ 437.11
AIX Config - 4	Fully Managed (1) - Gold Tier	Per Config		CCSI13310163-A	N/A	N/A	A			$ 391.23	$ 384.03	$ 377.68	$ 369.59	$ 362.35	$ 355.09	$ 347.82	$ 339.68	$ 335.84	$ 331.97
AIX Config - 4	Fully Managed (1) - Silver Tier	Per Config		CCSI13310164-A	N/A	N/A	A			$ 292.14	$ 285.79	$ 280.30	$ 273.07	$ 267.55	$ 262.02	$ 255.62	$ 248.33	$ 245.35	$ 242.35
AIX Config - 4	Fully Managed (1) - Bronze Tier	Per Config		CCSI13310165-A	N/A	N/A	A			$ 193.03	$ 188.41	$ 184.65	$ 179.14	$ 174.48	$ 169.82	$ 164.27	$ 157.84	$ 155.73	$ 153.59
AIX Config - 4	Fully Managed (1) - Basic Tier	Per Config		CCSI13310166-A	N/A	N/A	A			$ 93.93	$ 90.18	$ 87.27	$ 82.63	$ 78.83	$ 75.02	$ 70.33	$ 64.77	$ 63.52	$ 62.25
AIX Config - 5	Fully Managed (1) - Platinum Tier	Per Config		CCSI13310167-A	N/A	N/A	A			$ 507.57	$ 499.50	$ 492.29	$ 483.34	$ 475.23	$ 467.12	$ 458.12	$ 448.26	$ 442.69	$ 437.11
AIX Config - 5	Fully Managed (1) - Gold Tier	Per Config		CCSI13310168-A	N/A	N/A	A			$ 391.23	$ 384.03	$ 377.68	$ 369.59	$ 362.35	$ 355.09	$ 347.82	$ 339.68	$ 335.84	$ 331.97
AIX Config - 5	Fully Managed (1) - Silver Tier	Per Config		CCSI13310169-A	N/A	N/A	A			$ 292.14	$ 285.79	$ 280.30	$ 273.07	$ 267.55	$ 262.02	$ 255.62	$ 248.33	$ 245.35	$ 242.35
AIX Config - 5	Fully Managed (1) - Bronze Tier	Per Config		CCSI13310170-A	N/A	N/A	A			$ 193.03	$ 188.41	$ 184.65	$ 179.14	$ 174.48	$ 169.82	$ 164.27	$ 157.84	$ 155.73	$ 153.59
AIX Config - 5	Fully Managed (1) - Basic Tier	Per Config		CCSI13310171-A	N/A	N/A	A			$ 93.93	$ 90.18	$ 87.27	$ 82.63	$ 78.83	$ 75.02	$ 70.33	$ 64.77	$ 63.52	$ 62.25
AIX Config - 1	3.0GHz POWER7		1							$ 99.96	$ 98.97	$ 97.97	$ 96.99	$ 96.01	$ 95.06	$ 94.11	$ 93.18	$ 92.24	$ 91.32
	0.5 Cores		0.5							$ 15.51	$ 15.35	$ 15.20	$ 15.05	$ 14.90	$ 14.75	$ 14.60	$ 14.46	$ 14.31	$ 14.17
	6 GB RAM		6							$ 7.78	$ 7.71	$ 7.64	$ 7.57	$ 7.57	$ 7.50	$ 7.43	$ 7.36	$ 7.36	$ 7.29
	AIX		1							$ 48.26	$ 50.84	$ 52.57	$ 56.02	$ 58.60	$ 61.18	$ 64.63	$ 68.94	$ 68.94	$ 68.94
	Sub-Total									**$ 171.51**	**$ 172.87**	**$ 173.38**	**$ 175.63**	**$ 177.09**	**$ 178.50**	**$ 180.78**	**$ 183.94**	**$ 182.85**	**$ 181.73**
AIX Config - 1	Fully Managed (1) - Platinum Tier		1							$ 667.88	$ 660.97	$ 654.06	$ 647.15	$ 640.30	$ 634.26	$ 628.20	$ 622.15	$ 616.17	$ 610.12
AIX Config - 1	Fully Managed (1) - Gold Tier		1							$ 551.55	$ 546.35	$ 541.17	$ 535.99	$ 530.86	$ 525.68	$ 520.49	$ 515.30	$ 510.18	$ 505.00
AIX Config - 1	Fully Managed (1) - Silver Tier		1							$ 452.44	$ 448.12	$ 443.80	$ 439.47	$ 435.21	$ 430.89	$ 426.56	$ 422.23	$ 417.97	$ 413.65
AIX Config - 1	Fully Managed (1) - Bronze Tier		1							$ 353.34	$ 349.88	$ 346.42	$ 342.96	$ 339.55	$ 336.09	$ 332.63	$ 329.16	$ 325.76	$ 322.31
AIX Config - 1	Fully Managed (1) - Basic Tier		1							$ 254.24	$ 251.63	$ 249.04	$ 246.43	$ 243.90	$ 241.31	$ 238.70	$ 236.10	$ 233.56	$ 230.96
AIX Config - 2	3.0GHz POWER7		1							$ 99.96	$ 98.97	$ 97.97	$ 96.99	$ 96.01	$ 95.06	$ 94.11	$ 93.18	$ 92.24	$ 91.32
	1.0 Cores		1							$ 31.02	$ 30.71	$ 30.41	$ 30.11	$ 29.80	$ 29.50	$ 29.20	$ 28.91	$ 28.62	$ 28.33
	12 GB RAM		12							$ 15.56	$ 15.42	$ 15.28	$ 15.15	$ 15.15	$ 15.01	$ 14.87	$ 14.73	$ 14.73	$ 14.59
	AIX		1							$ 48.26	$ 50.84	$ 52.57	$ 56.02	$ 58.60	$ 61.18	$ 64.63	$ 68.94	$ 68.94	$ 68.94
	Sub-Total									**$ 194.80**	**$ 195.94**	**$ 196.23**	**$ 198.25**	**$ 199.56**	**$ 200.76**	**$ 202.82**	**$ 205.76**	**$ 204.53**	**$ 203.19**
AIX Config - 2	Fully Managed (1) - Platinum Tier		1							$ 702.38	$ 695.44	$ 688.52	$ 681.59	$ 674.80	$ 667.87	$ 660.94	$ 654.01	$ 647.22	$ 640.29
AIX Config - 2	Fully Managed (1) - Gold Tier		1							$ 586.03	$ 579.97	$ 573.91	$ 567.84	$ 561.91	$ 555.85	$ 550.64	$ 545.44	$ 540.37	$ 535.16
AIX Config - 2	Fully Managed (1) - Silver Tier		1							$ 486.94	$ 481.73	$ 476.53	$ 471.32	$ 467.12	$ 462.78	$ 458.43	$ 454.09	$ 449.88	$ 445.53
AIX Config - 2	Fully Managed (1) - Bronze Tier		1							$ 387.84	$ 384.35	$ 380.88	$ 377.39	$ 374.05	$ 370.57	$ 367.09	$ 363.60	$ 360.26	$ 356.78
AIX Config - 2	Fully Managed (1) - Basic Tier		1							$ 288.73	$ 286.12	$ 283.50	$ 280.88	$ 278.39	$ 275.78	$ 273.15	$ 270.53	$ 268.05	$ 265.44
AIX Config - 3	3.0GHz POWER7		1							$ 99.96	$ 98.97	$ 97.97	$ 96.99	$ 96.01	$ 95.06	$ 94.11	$ 93.18	$ 92.24	$ 91.32
	1.5 Cores		1.5							$ 46.53	$ 46.06	$ 45.61	$ 45.16	$ 44.71	$ 44.25	$ 43.80	$ 43.37	$ 42.93	$ 42.50
	18 GB RAM		18							$ 23.34	$ 23.13	$ 22.93	$ 22.72	$ 22.72	$ 22.51	$ 22.30	$ 22.09	$ 22.09	$ 21.88
	AIX		1							$ 48.26	$ 50.84	$ 52.57	$ 56.02	$ 58.60	$ 61.18	$ 64.63	$ 68.94	$ 68.94	$ 68.94
	Sub-Total									**$ 218.10**	**$ 219.00**	**$ 219.07**	**$ 220.88**	**$ 222.04**	**$ 223.01**	**$ 224.85**	**$ 227.58**	**$ 226.21**	**$ 224.65**
AIX Config - 3	Fully Managed (1) - Platinum Tier		1							$ 754.11	$ 746.30	$ 738.49	$ 730.69	$ 723.95	$ 717.00	$ 710.04	$ 703.10	$ 696.37	$ 689.42
AIX Config - 3	Fully Managed (1) - Gold Tier		1							$ 637.76	$ 631.68	$ 625.61	$ 619.52	$ 613.64	$ 607.56	$ 601.47	$ 595.38	$ 589.51	$ 583.42
AIX Config - 3	Fully Managed (1) - Silver Tier		1							$ 525.74	$ 520.51	$ 515.30	$ 510.08	$ 505.06	$ 499.84	$ 494.61	$ 489.39	$ 484.37	$ 479.15
AIX Config - 3	Fully Managed (1) - Bronze Tier		1							$ 439.57	$ 435.19	$ 430.85	$ 426.49	$ 422.33	$ 417.98	$ 413.60	$ 409.25	$ 405.09	$ 400.73
AIX Config - 3	Fully Managed (1) - Basic Tier		1							$ 340.46	$ 336.96	$ 333.47	$ 329.98	$ 326.68	$ 323.18	$ 319.67	$ 316.18	$ 312.89	$ 309.38
AIX Config - 4	3.0GHz POWER7		1							$ 99.96	$ 98.97	$ 97.97	$ 96.99	$ 96.01	$ 95.06	$ 94.11	$ 93.18	$ 92.24	$ 91.32
	1.0 Cores		1							$ 31.02	$ 30.71	$ 30.41	$ 30.11	$ 29.80	$ 29.50	$ 29.20	$ 28.91	$ 28.62	$ 28.33
	12 GB RAM		12							$ 15.56	$ 15.42	$ 15.28	$ 15.15	$ 15.15	$ 15.01	$ 14.87	$ 14.73	$ 14.73	$ 14.59
	AIX		1							$ 48.26	$ 50.84	$ 52.57	$ 56.02	$ 58.60	$ 61.18	$ 64.63	$ 68.94	$ 68.94	$ 68.94

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	**Product Name**	**Unit**	**Qty per config**	**Provider Part Number**	**Version Major**	**Version Minor**	**Version Build**	**Manufacturer ID**	**Equipment Code**	**Price per unit \ Per Month**									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Sub-Total									**$ 194.80**	**$ 195.94**	**$ 196.23**	**$ 198.25**	**$ 199.56**	**$ 200.76**	**$ 202.82**	**$ 205.76**	**$ 204.53**	**$ 203.19**
AIX Config - 4	Fully Managed (1) - Platinum Tier		1							$ 702.38	$ 695.44	$ 688.52	$ 681.59	$ 674.80	$ 667.87	$ 660.94	$ 654.01	$ 647.22	$ 640.29
AIX Config - 4	Fully Managed (1) - Gold Tier		1							$ 586.03	$ 579.97	$ 573.91	$ 567.84	$ 561.91	$ 555.85	$ 550.64	$ 545.44	$ 540.37	$ 535.16
AIX Config - 4	Fully Managed (1) - Silver Tier		1							$ 486.94	$ 481.73	$ 476.53	$ 471.32	$ 467.12	$ 462.78	$ 458.43	$ 454.09	$ 449.88	$ 445.53
AIX Config - 4	Fully Managed (1) - Bronze Tier		1							$ 387.84	$ 384.35	$ 380.88	$ 377.39	$ 374.05	$ 370.57	$ 367.09	$ 363.60	$ 360.26	$ 356.78
AIX Config - 4	Fully Managed (1) - Basic Tier		1							$ 288.73	$ 286.12	$ 283.50	$ 280.88	$ 278.39	$ 275.78	$ 273.15	$ 270.53	$ 268.05	$ 265.44
AIX Config - 5	3.0GHz POWER7		1							$ 99.96	$ 98.97	$ 97.97	$ 96.99	$ 96.01	$ 95.06	$ 94.11	$ 93.18	$ 92.24	$ 91.32
	1.0 Cores		1							$ 31.02	$ 30.71	$ 30.41	$ 30.11	$ 29.80	$ 29.50	$ 29.20	$ 28.91	$ 28.62	$ 28.33
	12 GB RAM		12							$ 15.56	$ 15.42	$ 15.28	$ 15.15	$ 15.15	$ 15.01	$ 14.87	$ 14.73	$ 14.73	$ 14.59
	AIX		1							$ 48.26	$ 50.84	$ 52.57	$ 56.02	$ 58.60	$ 61.18	$ 64.63	$ 68.94	$ 68.94	$ 68.94
	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Sub-Total									**$ 194.80**	**$ 195.94**	**$ 196.23**	**$ 198.25**	**$ 199.56**	**$ 200.76**	**$ 202.82**	**$ 205.76**	**$ 204.53**	**$ 203.19**
AIX Config - 5	Fully Managed (1) - Platinum Tier		1							$ 702.38	$ 695.44	$ 688.52	$ 681.59	$ 674.80	$ 667.87	$ 660.94	$ 654.01	$ 647.22	$ 640.29
AIX Config - 5	Fully Managed (1) - Gold Tier		1							$ 586.03	$ 579.97	$ 573.91	$ 567.84	$ 561.91	$ 555.85	$ 550.64	$ 545.44	$ 540.37	$ 535.16
AIX Config - 5	Fully Managed (1) - Silver Tier		1							$ 486.94	$ 481.73	$ 476.53	$ 471.32	$ 467.12	$ 462.78	$ 458.43	$ 454.09	$ 449.88	$ 445.53
AIX Config - 5	Fully Managed (1) - Bronze Tier		1							$ 387.84	$ 384.35	$ 380.88	$ 377.39	$ 374.05	$ 370.57	$ 367.09	$ 363.60	$ 360.26	$ 356.78
AIX Config - 5	Fully Managed (1) - Basic Tier		1							$ 288.73	$ 286.12	$ 283.50	$ 280.88	$ 278.39	$ 275.78	$ 273.15	$ 270.53	$ 268.05	$ 265.44
AIX Config - 5	**Total**									**$ 2,841.53**	**$ 2,819.49**	**$ 2,795.79**	**$ 2,775.54**	**$ 2,755.40**	**$ 2,734.36**	**$ 2,715.88**	**$ 2,699.19**	**$ 2,674.83**	**$ 2,649.58**
Server - Managed Only (2)																			
Server - Managed Only x86 (Windows, Linux)																			
	Platinum Tier	Server/Instance		CCSU13320001-A	N/A	N/A	A			$ 143.46	$ 129.22	$ 124.13	$ 118.36	$ 113.26	$ 107.71	$ 102.93	$ 102.93	$ 102.93	$ 102.93
	Gold Tier	Server/Instance		CCSU13320002-A	N/A	N/A	A			$ 127.16	$ 116.03	$ 112.08	$ 107.50	$ 103.41	$ 98.88	$ 94.95	$ 94.95	$ 94.95	$ 94.95
	Silver Tier	Server/Instance		CCSU13320003-A	N/A	N/A	A			$ 114.19	$ 105.29	$ 102.16	$ 98.47	$ 95.14	$ 91.39	$ 88.12	$ 88.12	$ 88.12	$ 88.12
	Bronze Tier	Server/Instance		CCSU13320004-A	N/A	N/A	A			$ 108.64	$ 100.63	$ 97.83	$ 94.50	$ 91.48	$ 88.06	$ 85.06	$ 85.06	$ 85.06	$ 85.06
	Basic Tier	Server/Instance		CCSU13320005-A	N/A	N/A	A			$ 103.61	$ 96.37	$ 93.85	$ 90.84	$ 88.09	$ 84.96	$ 82.21	$ 82.21	$ 82.21	$ 82.21
Server - Managed Only UNIX (IBM P-Series, AIX)																			
	Platinum	LPAR		CCSI13320006-A	N/A	N/A	A			$ 479.79	$ 474.95	$ 470.11	$ 465.28	$ 460.44	$ 455.60	$ 450.77	$ 445.93	$ 441.09	$ 436.26
	Gold Tier	LPAR		CCSI13320007-A	N/A	N/A	A			$ 428.51	$ 424.65	$ 420.78	$ 416.91	$ 413.04	$ 409.17	$ 405.30	$ 401.43	$ 397.56	$ 393.70
	Silver Tier	LPAR		CCSI13320008-A	N/A	N/A	A			$ 379.19	$ 375.32	$ 371.44	$ 367.57	$ 363.71	$ 359.84	$ 355.97	$ 352.10	$ 348.23	$ 344.36
	Bronze Tier	LPAR		CCSI13320009-A	N/A	N/A	A			$ 320.18	$ 317.27	$ 314.38	$ 311.47	$ 308.57	$ 305.67	$ 302.77	$ 299.86	$ 296.97	$ 294.06
	Basic Tier	LPAR		CCSI13320010-A	N/A	N/A	A			$ 206.04	$ 204.10	$ 202.17	$ 200.23	$ 198.30	$ 196.37	$ 194.43	$ 192.49	$ 190.55	$ 188.62
Storage and Backup - Fully Managed (1)																			
Enterprise Storage																			
	* Dedicated - Config 1 - SAN Raid 5	GB		CCSZ13310172-A	N/A	N/A	A			$ 0.06	$ 0.05	$ 0.05	$ 0.05	$ 0.05	$ 0.04	$ 0.04	$ 0.04	$ 0.03	$ 0.03
	* Dedicated - Config 2 - SAN Raid 10	GB		CCSZ13310173-A	N/A	N/A	A			$ 0.24	$ 0.24	$ 0.24	$ 0.23	$ 0.23	$ 0.23	$ 0.23	$ 0.21	$ 0.19	$ 0.17
	Dedicated - Config 3 - Net Attached	GB		CCSZ13310174-A	N/A	N/A	A			$ 0.07	$ 0.06	$ 0.06	$ 0.05	$ 0.05	$ 0.03	$ 0.03	$ 0.03	$ 0.03	$ 0.02
Tape and Backup																			
	** Server Tape Stored	GB Stored		CCSU13310175-A	N/A	N/A	A			$ 0.07	$ 0.05	$ 0.05	$ 0.04	$ 0.04	$ 0.04	$ 0.04	$ 0.03	$ 0.03	$ 0.03
	** Offsite Tape Storage	Tapes		CCSU13310176-A	N/A	N/A	A			$ 0.24	$ 0.24	$ 0.24	$ 0.23	$ 0.23	$ 0.23	$ 0.23	$ 0.21	$ 0.19	$ 0.17
Limited Co-Lo (Data Center Only Charge) (3)																			
Limited Co-Lo Configurations																			
Co-Lo Config - 1	1/4 Rack Configuration includes: 10U Cabinet Space	Per Config		CCSU13330001-A	N/A	N/A	A			$ 49.85	$ 50.23	$ 50.63	$ 51.04	$ 53.10	$ 53.53	$ 53.98	$ 53.98	$ 53.98	$ 53.98
Co-Lo Config - 2	1/2 Rack Configuration includes: 21U Cabinet Space	Per Config		CCSU13330002-A	N/A	N/A	A			$ 75.65	$ 76.42	$ 77.21	$ 78.03	$ 80.51	$ 81.38	$ 82.27	$ 82.27	$ 82.27	$ 82.27
Co-Lo Config - 3	Full Rack Configuration includes: 42U Cabinet Space	Per Config		CCSU13330003-A	N/A	N/A	A			$ 135.48	$ 137.01	$ 138.59	$ 140.22	$ 144.55	$ 146.09	$ 147.67	$ 147.67	$ 147.67	$ 147.67
Co-Lo Config - 1, 2, 3	Network Bandwidth	Per GB		CCSU13330004-A	N/A	N/A	A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Co-Lo Config - 1 2 3	100Mb/s Uplink	Each		CCSU13330005-A	N/A	N/A	A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Co-Lo Config - 1, 2, 3	IP Addresses	Each		CCSU13330006-A	N/A	N/A	A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Co-Lo Config - 1	110V AC Circuits	Per Circuit		CCSU13330007-A	N/A	N/A	A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Co-Lo Config - 1	1/4 Rack Configuration includes: 10U Cabinet Space		1							$ 49.85	$ 50.23	$ 50.63	$ 51.04	$ 53.10	$ 53.53	$ 53.98	$ 53.98	$ 53.98	$ 53.98
	GB Network Bandwidth		5000							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	100Mb/s Uplink		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IP Addresses		6							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	110V AC Circuits		5							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Co-Lo Config - 1	**Total**									**$ 49.85**	**$ 50.23**	**$ 50.63**	**$ 51.04**	**$ 53.10**	**$ 53.53**	**$ 53.98**	**$ 53.98**	**$ 53.98**	**$ 53.98**
Co-Lo Config - 2	1/2 Rack Configuration includes: 21U Cabinet Space		1							$ 75.65	$ 76.42	$ 77.21	$ 78.03	$ 80.51	$ 81.38	$ 82.27	$ 82.27	$ 82.27	$ 82.27
	10,000 GB Network Bandwidth		10000							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	100Mb/s Uplink		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IP Addresses		14							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	110V AC Circuits		10							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Co-Lo Config - 2	**Total**									**$ 75.65**	**$ 76.42**	**$ 77.21**	**$ 78.03**	**$ 80.51**	**$ 81.38**	**$ 82.27**	**$ 82.27**	**$ 82.27**	**$ 82.27**
Co-Lo Config - 3	Full Rack Configuration includes: 42U Cabinet Space		1							$ 135.48	$ 137.01	$ 138.59	$ 140.22	$ 144.55	$ 146.09	$ 147.67	$ 147.67	$ 147.67	$ 147.67
	GB Network Bandwidth		20000							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	100Mb/s Uplink		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	Product Name	Unit	Qty per config	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
	IP Addresses		30							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	110V AC Circuits		20							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Co-Lo Config - 3	**Total**									**$ 135.48**	**$ 137.01**	**$ 138.59**	**$ 140.22**	**$ 144.55**	**$ 146.09**	**$ 147.67**	**$ 147.67**	**$ 147.67**	**$ 147.67**
Mainframe Services (4)																			
IBM Mainframe																			
	*** IBM Mainframe Allocated DASD	GB		CCSI13310177-A	N/A	N/A	A			$ 1.25	$ 1.19	$ 1.13	$ 1.07	$ 1.02	$ 0.97	$ 0.92	$ 0.92	$ 0.92	$ 0.92
	IBM Tapes in Storage - VTS	GB		CCSI13310178-A	N/A	N/A	A			$ 0.29	$ 0.28	$ 0.28	$ 0.28	$ 0.27	$ 0.26	$ 0.26	$ 0.25	$ 0.25	$ 0.24
	IBM Offsite Tape Storage	Tape/Reel		CCSI13310179-A	N/A	N/A	A			$ 0.24	$ 0.24	$ 0.24	$ 0.23	$ 0.23	$ 0.23	$ 0.23	$ 0.21	$ 0.19	$ 0.17
IBM Mainframe Configurations																			
IBM Mainframe Config - 1	IBM System zEnterprise Processor z/OS	Per MIP		CCSI13310180-A	N/A	N/A	A			$ 75.03	$ 71.28	$ 67.72	$ 64.33	$ 61.11	$ 58.06	$ 55.16	$ 55.16	$ 55.16	$ 55.16
IBM Mainframe Config - 2, 3	IBM System zEnterprise Processor Virtual Linux Prod IFL	Per MIP		CCSI13310181-A	N/A	N/A	A			$ 65.93	$ 62.63	$ 59.50	$ 56.52	$ 53.70	$ 51.01	$ 48.46	$ 48.46	$ 48.46	$ 48.46
IBM AS400 Config 1, 2	IBM i Series / AS400	Per CPW		CCSI13310182-A	N/A	N/A	A			$ 8.19	$ 7.78	$ 7.39	$ 7.02	$ 6.67	$ 6.33	$ 6.02	$ 6.02	$ 6.02	$ 6.02
IBM Mainframe Config - 3	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Config		CCSI13310183-A	N/A	N/A	A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IBM AS400 Config 2	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Config		CCSI13310184-A	N/A	N/A	A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IBM Mainframe Config - 1	Mainframe Services (4) - Platinum Tier	Per Config		CCSI13310185-A	N/A	N/A	A			$ 84.18	$ 79.98	$ 75.98	$ 72.19	$ 68.58	$ 65.15	$ 61.90	$ 61.90	$ 61.90	$ 61.90
IBM Mainframe Config - 1	Mainframe Services (4) - Gold Tier	Per Config		CCSI13310186-A	N/A	N/A	A			$ 73.47	$ 69.80	$ 66.31	$ 62.99	$ 59.84	$ 56.85	$ 54.01	$ 54.01	$ 54.01	$ 54.01
IBM Mainframe Config - 1	Mainframe Services (4) - Basic Tier	Per Config		CCSI13310187-A	N/A	N/A	A			$ 66.05	$ 62.75	$ 59.61	$ 56.62	$ 53.80	$ 51.11	$ 48.56	$ 48.56	$ 48.56	$ 48.56
IBM Mainframe Config - 2	Mainframe Services (4) - Platinum Tier	Per Config		CCSI13310188-A	N/A	N/A	A			$ 73.96	$ 70.26	$ 66.75	$ 63.41	$ 60.24	$ 57.23	$ 54.37	$ 54.37	$ 54.37	$ 54.37
IBM Mainframe Config - 2	Mainframe Services (4) - Gold Tier	Per Config		CCSI13310189-A	N/A	N/A	A			$ 64.56	$ 61.33	$ 58.27	$ 55.35	$ 52.58	$ 49.95	$ 47.46	$ 47.46	$ 47.46	$ 47.46
IBM Mainframe Config - 2	Mainframe Services (4) - Basic Tier	Per Config		CCSI13310190-A	N/A	N/A	A			$ 58.04	$ 55.14	$ 52.38	$ 49.76	$ 47.27	$ 44.91	$ 42.66	$ 42.66	$ 42.66	$ 42.66
IBM Mainframe Config - 3	Mainframe Services (4) - Platinum Tier	Per Config		CCSI13310191-A	N/A	N/A	A			$ 73.96	$ 70.26	$ 66.75	$ 63.41	$ 60.24	$ 57.23	$ 54.37	$ 54.37	$ 54.37	$ 54.37
IBM Mainframe Config - 3	Mainframe Services (4) - Gold Tier	Per Config		CCSI13310192-A	N/A	N/A	A			$ 64.56	$ 61.33	$ 58.27	$ 55.35	$ 52.58	$ 49.95	$ 47.46	$ 47.46	$ 47.46	$ 47.46
IBM Mainframe Config - 3	Mainframe Services (4) - Basic Tier	Per Config		CCSI13310193-A	N/A	N/A	A			$ 58.04	$ 55.14	$ 52.38	$ 49.76	$ 47.27	$ 44.91	$ 42.66	$ 42.66	$ 42.66	$ 42.66
IBM AS400 Config 1	Mainframe Services (4) - Platinum Tier	Per Config		CCSI13310194-A	N/A	N/A	A			$ 9.18	$ 8.72	$ 8.29	$ 7.87	$ 7.48	$ 7.11	$ 6.75	$ 6.75	$ 6.75	$ 6.75
IBM AS400 Config 1	Mainframe Services (4) - Gold Tier	Per Config		CCSI13310195-A	N/A	N/A	A			$ 8.01	$ 7.61	$ 7.24	$ 6.88	$ 6.53	$ 6.21	$ 5.90	$ 5.90	$ 5.90	$ 5.90
IBM AS400 Config 1	Mainframe Services (4) - Basic Tier	Per Config		CCSI13310196-A	N/A	N/A	A			$ 7.20	$ 6.85	$ 6.51	$ 6.18	$ 5.87	$ 5.58	$ 5.31	$ 5.31	$ 5.31	$ 5.31
IBM AS400 Config 2	Mainframe Services (4) - Platinum Tier	Per Config		CCSI13310197-A	N/A	N/A	A			$ 9.18	$ 8.72	$ 8.29	$ 7.87	$ 7.48	$ 7.11	$ 6.75	$ 6.75	$ 6.75	$ 6.75
IBM AS400 Config 2	Mainframe Services (4) - Gold Tier	Per Config		CCSI13310198-A	N/A	N/A	A			$ 8.01	$ 7.61	$ 7.24	$ 6.88	$ 6.53	$ 6.21	$ 5.90	$ 5.90	$ 5.90	$ 5.90
IBM AS400 Config 2	Mainframe Services (4) - Basic Tier	Per Config		CCSI13310199-A	N/A	N/A	A			$ 7.20	$ 6.85	$ 6.51	$ 6.18	$ 5.87	$ 5.58	$ 5.31	$ 5.31	$ 5.31	$ 5.31
IBM Mainframe Config - 1	IBM System zEnterprise Processor z/OS		1							$ 75.03	$ 71.28	$ 67.72	$ 64.33	$ 61.11	$ 58.06	$ 55.16	$ 55.16	$ 55.16	$ 55.16
	Sub-Total									**$ 75.03**	**$ 71.28**	**$ 67.72**	**$ 64.33**	**$ 61.11**	**$ 58.06**	**$ 55.16**	**$ 55.16**	**$ 55.16**	**$ 55.16**
IBM Mainframe Config - 1	Mainframe Services (4) - Platinum Tier		1							$ 159.21	$ 151.26	$ 143.69	$ 136.52	$ 129.70	$ 123.21	$ 117.05	$ 117.05	$ 117.05	$ 117.05
IBM Mainframe Config - 1	Mainframe Services (4) - Gold Tier		1							$ 148.50	$ 141.08	$ 134.03	$ 127.32	$ 120.95	$ 114.91	$ 109.17	$ 109.17	$ 109.17	$ 109.17
IBM Mainframe Config - 1	Mainframe Services (4) - Basic Tier		1							$ 141.08	$ 134.03	$ 127.32	$ 120.95	$ 114.91	$ 109.17	$ 103.71	$ 103.71	$ 103.71	$ 103.71
IBM Mainframe Config - 2	IBM System zEnterprise Processor Virtual Linux Prod IFL		1							$ 65.93	$ 62.63	$ 59.50	$ 56.52	$ 53.70	$ 51.01	$ 48.46	$ 48.46	$ 48.46	$ 48.46
	Sub-Total									**$ 65.93**	**$ 62.63**	**$ 59.50**	**$ 56.52**	**$ 53.70**	**$ 51.01**	**$ 48.46**	**$ 48.46**	**$ 48.46**	**$ 48.46**
IBM Mainframe Config - 2	Mainframe Services (4) - Platinum Tier		1							$ 139.89	$ 132.89	$ 126.25	$ 119.93	$ 113.94	$ 108.24	$ 102.83	$ 102.83	$ 102.83	$ 102.83
IBM Mainframe Config - 2	Mainframe Services (4) - Gold Tier		1							$ 130.48	$ 123.96	$ 117.77	$ 111.88	$ 106.28	$ 100.97	$ 95.92	$ 95.92	$ 95.92	$ 95.92
IBM Mainframe Config - 2	Mainframe Services (4) - Basic Tier		1							$ 123.96	$ 117.77	$ 111.88	$ 106.28	$ 100.97	$ 95.92	$ 91.13	$ 91.13	$ 91.13	$ 91.13
IBM Mainframe Config - 3	IBM System zEnterprise Processor Virtual Linux Prod IFL		1							$ 65.93	$ 62.63	$ 59.50	$ 56.52	$ 53.70	$ 51.01	$ 48.46	$ 48.46	$ 48.46	$ 48.46
	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Sub-Total									**$ 65.93**	**$ 62.63**	**$ 59.50**	**$ 56.52**	**$ 53.70**	**$ 51.01**	**$ 48.46**	**$ 48.46**	**$ 48.46**	**$ 48.46**
IBM Mainframe Config - 3	Mainframe Services (4) - Platinum Tier		1							$ 139.89	$ 132.89	$ 126.25	$ 119.93	$ 113.94	$ 108.24	$ 102.83	$ 102.83	$ 102.83	$ 102.83
IBM Mainframe Config - 3	Mainframe Services (4) - Gold Tier		1							$ 130.48	$ 123.96	$ 117.77	$ 111.88	$ 106.28	$ 100.97	$ 95.92	$ 95.92	$ 95.92	$ 95.92
IBM Mainframe Config - 3	Mainframe Services (4) - Basic Tier		1							$ 123.96	$ 117.77	$ 111.88	$ 106.28	$ 100.97	$ 95.92	$ 91.13	$ 91.13	$ 91.13	$ 91.13
IBM AS400 Config 1	IBM i Series / AS400		1							$ 8.19	$ 7.78	$ 7.39	$ 7.02	$ 6.67	$ 6.33	$ 6.02	$ 6.02	$ 6.02	$ 6.02
	Sub-Total									**$ 8.19**	**$ 7.78**	**$ 7.39**	**$ 7.02**	**$ 6.67**	**$ 6.33**	**$ 6.02**	**$ 6.02**	**$ 6.02**	**$ 6.02**
IBM AS400 Config 1	Mainframe Services (4) - Platinum Tier		1							$ 17.37	$ 16.50	$ 15.68	$ 14.89	$ 14.15	$ 13.44	$ 12.77	$ 12.77	$ 12.77	$ 12.77
IBM AS400 Config 1	Mainframe Services (4) - Gold Tier		1							$ 16.20	$ 15.39	$ 14.62	$ 13.89	$ 13.20	$ 12.54	$ 11.91	$ 11.91	$ 11.91	$ 11.91
IBM AS400 Config 1	Mainframe Services (4) - Basic Tier		1							$ 15.39	$ 14.62	$ 13.89	$ 13.20	$ 12.54	$ 11.91	$ 11.32	$ 11.32	$ 11.32	$ 11.32
IBM AS400 Config 2	IBM i Series / AS400		1							$ 8.19	$ 7.78	$ 7.39	$ 7.02	$ 6.67	$ 6.33	$ 6.02	$ 6.02	$ 6.02	$ 6.02
	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Sub-Total									**$ 8.19**	**$ 7.78**	**$ 7.39**	**$ 7.02**	**$ 6.67**	**$ 6.33**	**$ 6.02**	**$ 6.02**	**$ 6.02**	**$ 6.02**
IBM AS400 Config 2	Mainframe Services (4) - Platinum Tier		1							$ 17.37	$ 16.50	$ 15.68	$ 14.89	$ 14.15	$ 13.44	$ 12.77	$ 12.77	$ 12.77	$ 12.77
IBM AS400 Config 2	Mainframe Services (4) - Gold Tier		1							$ 16.20	$ 15.39	$ 14.62	$ 13.89	$ 13.20	$ 12.54	$ 11.91	$ 11.91	$ 11.91	$ 11.91
IBM AS400 Config 2	Mainframe Services (4) - Basic Tier		1							$ 15.39	$ 14.62	$ 13.89	$ 13.20	$ 12.54	$ 11.91	$ 11.32	$ 11.32	$ 11.32	$ 11.32
Unisys Mainframe																			
	*** Unisys DASD	GB		CCSU13310200-A	N/A	N/A	A			$ 0.10	$ 0.10	$ 0.10	$ 0.10	$ 0.10	$ 0.07	$ 0.07	$ 0.07	$ 0.07	$ 0.07
	Unisys Tapes in Storage - VTS	GB		CCSU13310201-A	N/A	N/A	A			$ 0.16	$ 0.16	$ 0.16	$ 0.16	$ 0.16	$ 0.15	$ 0.15	$ 0.15	$ 0.15	$ 0.15
	Unisys Offsite Tape Storage	Tape/Reel		CCSU13310202-A	N/A	N/A	A			$ 0.24	$ 0.24	$ 0.24	$ 0.23	$ 0.23	$ 0.23	$ 0.23	$ 0.21	$ 0.19	$ 0.17

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	Product Name	Unit	Qty per config	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Unisys Mainframe Configurations																			
Unisys Mainframe Config - 1, 3	Unisys (Clearpath / Dorado)	Per MIP		CCSU13310203-A	N/A	N/A	A			$ 761.89	$ 751.54	$ 748.05	$ 744.76	$ 739.62	$ 738.04	$ 727.07	$ 727.07	$ 727.07	$ 727.07
Unisys Mainframe Config - 2 4	Unisys (Clearpath / Libra)	Per Mip		CCSU13310204-A	N/A	N/A	A			$ 746.21	$ 739.37	$ 734.46	$ 733.45	$ 732.19	$ 732.01	$ 727.08	$ 727.08	$ 727.08	$ 727.08
Unisys Mainframe Config - 3	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Config		CCSU13310205-A	N/A	N/A	A			$ 7.43	$ 7.38	$ 7.34	$ 7.33	$ 7.33	$ 7.01	$ 6.98	$ 6.98	$ 6.98	$ 6.98
Unisys Mainframe Config - 4	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Config		CCSU13310206-A	N/A	N/A	A			$ 10.83	$ 10.81	$ 10.81	$ 10.76	$ 10.74	$ 10.57	$ 10.39	$ 10.39	$ 10.39	$ 10.39
Unisys Mainframe Config - 1	Mainframe Services (4) - Platinum Tier	Per Config		CCSU13310207-A	N/A	N/A	A			$ 245.74	$ 239.44	$ 234.80	$ 230.30	$ 225.60	$ 221.81	$ 216.08	$ 216.08	$ 216.08	$ 216.08
Unisys Mainframe Config - 1	Mainframe Services (4) - Gold Tier	Per Config		CCSU13310208-A	N/A	N/A	A			$ 154.13	$ 149.35	$ 145.45	$ 141.66	$ 137.85	$ 134.55	$ 130.34	$ 130.34	$ 130.34	$ 130.34
Unisys Mainframe Config - 1	Mainframe Services (4) - Basic Tier	Per Config		CCSU13310209-A	N/A	N/A	A			$ 77.80	$ 74.27	$ 70.99	$ 67.79	$ 64.73	$ 61.84	$ 58.89	$ 58.89	$ 58.89	$ 58.89
Unisys Mainframe Config - 2	Mainframe Services (4) - Platinum Tier	Per Config		CCSU13310210-A	N/A	N/A	A			$ 240.68	$ 235.56	$ 235.50	$ 231.54	$ 223.33	$ 220.00	$ 216.09	$ 216.09	$ 216.09	$ 216.09
Unisys Mainframe Config - 2	Mainframe Services (4) - Gold Tier	Per Config		CCSU13310211-A	N/A	N/A	A			$ 150.96	$ 146.93	$ 147.32	$ 143.81	$ 136.47	$ 133.45	$ 130.34	$ 130.34	$ 130.34	$ 130.34
Unisys Mainframe Config - 2	Mainframe Services (4) - Basic Tier	Per Config		CCSU13310212-A	N/A	N/A	A			$ 76.20	$ 73.07	$ 69.70	$ 66.76	$ 64.08	$ 61.33	$ 58.89	$ 58.89	$ 58.89	$ 58.89
Unisys Mainframe Config - 3	Mainframe Services (4) - Platinum Tier	Per Config		CCSU13310213-A	N/A	N/A	A			$ 2.40	$ 2.35	$ 2.35	$ 2.31	$ 2.23	$ 2.11	$ 2.07	$ 2.07	$ 2.07	$ 2.07
Unisys Mainframe Config - 3	Mainframe Services (4) - Gold Tier	Per Config		CCSU13310214-A	N/A	N/A	A			$ 1.50	$ 1.47	$ 1.47	$ 1.43	$ 1.37	$ 1.28	$ 1.25	$ 1.25	$ 1.25	$ 1.25
Unisys Mainframe Config - 3	Mainframe Services (4) - Basic Tier	Per Config		CCSU13310215-A	N/A	N/A	A			$ 0.76	$ 0.73	$ 0.70	$ 0.67	$ 0.64	$ 0.59	$ 0.57	$ 0.57	$ 0.57	$ 0.57
Unisys Mainframe Config - 4	Mainframe Services (4) - Platinum Tier	Per Config		CCSU13310216-A	N/A	N/A	A			$ 3.49	$ 3.45	$ 3.42	$ 3.44	$ 3.40	$ 3.24	$ 3.09	$ 3.09	$ 3.09	$ 3.09
Unisys Mainframe Config - 4	Mainframe Services (4) - Gold Tier	Per Config		CCSU13310217-A	N/A	N/A	A			$ 2.19	$ 2.15	$ 2.13	$ 2.15	$ 2.11	$ 1.98	$ 1.86	$ 1.86	$ 1.86	$ 1.86
Unisys Mainframe Config - 4	Mainframe Services (4) - Basic Tier	Per Config		CCSU13310218-A	N/A	N/A	A			$ 1.11	$ 1.07	$ 1.03	$ 0.98	$ 0.94	$ 0.89	$ 0.84	$ 0.84	$ 0.84	$ 0.84
Unisys Mainframe Config - 1	Unisys (Clearpath / Dorado)		1							$ 761.89	$ 751.54	$ 748.05	$ 744.76	$ 739.62	$ 738.04	$ 727.07	$ 727.07	$ 727.07	$ 727.07
	Sub-Total									**$ 761.89**	**$ 751.54**	**$ 748.05**	**$ 744.76**	**$ 739.62**	**$ 738.04**	**$ 727.07**	**$ 727.07**	**$ 727.07**	**$ 727.07**
Unisys Mainframe Config - 1	Mainframe Services (4) - Platinum Tier		1							$ 1,007.63	$ 990.98	$ 982.84	$ 975.07	$ 965.22	$ 959.85	$ 943.16	$ 943.16	$ 943.16	$ 943.16
Unisys Mainframe Config - 1	Mainframe Services (4) - Gold Tier		1							$ 916.03	$ 900.89	$ 893.50	$ 886.42	$ 877.47	$ 872.60	$ 857.42	$ 857.42	$ 857.42	$ 857.42
Unisys Mainframe Config - 1	Mainframe Services (4) - Basic Tier		1							$ 839.69	$ 825.82	$ 819.04	$ 812.55	$ 804.35	$ 799.88	$ 785.96	$ 785.96	$ 785.96	$ 785.96
Unisys Mainframe Config - 2	Unisys (Clearpath / Libra)		1							$ 746.21	$ 739.37	$ 734.46	$ 733.45	$ 732.19	$ 732.01	$ 727.08	$ 727.08	$ 727.08	$ 727.08
	Sub-Total									**$ 746.21**	**$ 739.37**	**$ 734.46**	**$ 733.45**	**$ 732.19**	**$ 732.01**	**$ 727.08**	**$ 727.08**	**$ 727.08**	**$ 727.08**
Unisys Mainframe Config - 2	Mainframe Services (4) - Platinum Tier		1							$ 986.88	$ 974.93	$ 969.96	$ 964.99	$ 955.52	$ 952.01	$ 943.16	$ 943.16	$ 943.16	$ 943.16
Unisys Mainframe Config - 2	Mainframe Services (4) - Gold Tier		1							$ 897.17	$ 886.30	$ 881.78	$ 877.26	$ 868.66	$ 865.46	$ 857.42	$ 857.42	$ 857.42	$ 857.42
Unisys Mainframe Config - 2	Mainframe Services (4) - Basic Tier		1							$ 822.40	$ 812.44	$ 804.16	$ 800.21	$ 796.27	$ 793.34	$ 785.97	$ 785.97	$ 785.97	$ 785.97
Unisys Mainframe Config - 3	Unisys (Clearpath / Dorado)		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization		1							$ 7.43	$ 7.38	$ 7.34	$ 7.33	$ 7.33	$ 7.01	$ 6.98	$ 6.98	$ 6.98	$ 6.98
	Sub-Total									**$ 7.43**	**$ 7.38**	**$ 7.34**	**$ 7.33**	**$ 7.33**	**$ 7.01**	**$ 6.98**	**$ 6.98**	**$ 6.98**	**$ 6.98**
Unisys Mainframe Config - 3	Mainframe Services (4) - Platinum Tier		1							$ 9.83	$ 9.73	$ 9.69	$ 9.64	$ 9.56	$ 9.11	$ 9.05	$ 9.05	$ 9.05	$ 9.05
Unisys Mainframe Config - 3	Mainframe Services (4) - Gold Tier		1							$ 8.93	$ 8.85	$ 8.81	$ 8.77	$ 8.69	$ 8.28	$ 8.23	$ 8.23	$ 8.23	$ 8.23
Unisys Mainframe Config - 3	Mainframe Services (4) - Basic Tier		1							$ 8.19	$ 8.11	$ 8.04	$ 8.00	$ 7.97	$ 7.59	$ 7.55	$ 7.55	$ 7.55	$ 7.55
Unisys Mainframe Config - 4	Unisys (Clearpath / Libra)		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization		1							$ 10.83	$ 10.81	$ 10.81	$ 10.76	$ 10.74	$ 10.57	$ 10.39	$ 10.39	$ 10.39	$ 10.39
	Sub-Total									**$ 10.83**	**$ 10.81**	**$ 10.81**	**$ 10.76**	**$ 10.74**	**$ 10.57**	**$ 10.39**	**$ 10.39**	**$ 10.39**	**$ 10.39**
Unisys Mainframe Config - 4	Mainframe Services (4) - Platinum Tier		1							$ 14.32	$ 14.26	$ 14.23	$ 14.20	$ 14.14	$ 13.81	$ 13.48	$ 13.48	$ 13.48	$ 13.48
Unisys Mainframe Config - 4	Mainframe Services (4) - Gold Tier		1							$ 13.02	$ 12.96	$ 12.93	$ 12.91	$ 12.85	$ 12.55	$ 12.25	$ 12.25	$ 12.25	$ 12.25
Unisys Mainframe Config - 4	Mainframe Services (4) - Basic Tier		1							$ 11.94	$ 11.88	$ 11.83	$ 11.74	$ 11.68	$ 11.46	$ 11.23	$ 11.23	$ 11.23	$ 11.23
IaaS x86 Server Configurations (Windows)																			
IaaS Windows vConfig - 1	2vCPU	Per Server		CCSU13340001-A	N/A	N/A	A			$ 5.24	$ 4.65	$ 4.34	$ 4.15	$ 3.85	$ 3.31	$ 3.08	$ 3.08	$ 3.08	$ 3.08
IaaS Windows vConfig - 2 4 5	4vCPU	Per Server		CCSU13340002-A	N/A	N/A	A			$ 13.98	$ 12.57	$ 11.67	$ 11.15	$ 10.23	$ 8.74	$ 8.30	$ 8.30	$ 8.30	$ 8.30
IaaS Windows vConfig - 3	8vCPU	Per Server		CCSU13340003-A	N/A	N/A	A			$ 43.94	$ 39.68	$ 36.78	$ 35.13	$ 32.06	$ 27.34	$ 26.17	$ 26.17	$ 26.17	$ 26.17
IaaS Windows vConfig - 1, 2, 3, 4, 5	GB Ram	Per GB		CCSU13340004-A	N/A	N/A	A			$ 2.38	$ 2.26	$ 2.15	$ 2.04	$ 1.94	$ 1.84	$ 1.75	$ 1.75	$ 1.75	$ 1.75
IaaS Windows vConfig - 1 2 3 4 5	Windows Server 2008 R2	Per License		CCSU13340005-A	2008	R2	A			$ 19.25	$ 18.93	$ 18.70	$ 19.23	$ 18.75	$ 19.61	$ 19.17	$ 19.17	$ 19.17	$ 19.17
IaaS Windows vConfig - 1 2 3 4 5	Firewall/IDS	Per Config		CCSU13340006-A	N/A	N/A	A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Windows vConfig - 1, 2, 3, 4, 5	Site-Site VPN	Per Config		CCSU13340007-A	N/A	N/A	A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Windows vConfig - 1, 2, 3, 4, 5	VPN Client	Per Config		CCSU13340008-A	N/A	N/A	A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Windows vConfig - 1 2 3 4 5	VLAN	Per Config		CCSU13340009-A	N/A	N/A	A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Windows vConfig - 4	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Config		CCSU13340010-A	N/A	N/A	A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Windows vConfig - 5	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Config		CCSU13340011-A	N/A	N/A	A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Windows vConfig - 1	2vCPU		1							$ 5.24	$ 4.65	$ 4.34	$ 4.15	$ 3.85	$ 3.31	$ 3.08	$ 3.08	$ 3.08	$ 3.08
	GB Ram		4							$ 9.52	$ 9.04	$ 8.59	$ 8.16	$ 7.75	$ 7.37	$ 7.00	$ 7.00	$ 7.00	$ 7.00
	Windows Server 2008 R2		1							$ 19.25	$ 18.93	$ 18.70	$ 19.23	$ 18.75	$ 19.61	$ 19.17	$ 19.17	$ 19.17	$ 19.17
	Firewall/IDS		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Site-Site VPN		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	VPN Client		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	VLAN		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	**Product Name**	**Unit**	**Qty per config**	**Provider Part Number**	**Version Major**	**Version Minor**	**Version Build**	**Manufacturer ID**	**Equipment Code**	**Price per unit \ Per Month**									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
IaaS Windows vConfig - 1	Total									$ 34.01	$ 32.62	$ 31.63	$ 31.55	$ 30.35	$ 30.29	$ 29.24	$ 29.24	$ 29.24	$ 29.24
IaaS Windows vConfig - 2	4vCPU		1							$ 13.98	$ 12.57	$ 11.67	$ 11.15	$ 10.23	$ 8.74	$ 8.30	$ 8.30	$ 8.30	$ 8.30
	GB Ram		16							$ 38.08	$ 36.18	$ 34.37	$ 32.65	$ 31.02	$ 29.47	$ 27.99	$ 27.99	$ 27.99	$ 27.99
	Windows Server 2008 R2		1							$ 19.25	$ 18.93	$ 18.70	$ 19.23	$ 18.75	$ 19.61	$ 19.17	$ 19.17	$ 19.17	$ 19.17
	Firewall/IDS		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Site-Site VPN		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	VPN Client		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	VLAN		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Windows vConfig - 2	Total									$ 71.32	$ 67.67	$ 64.74	$ 63.03	$ 59.99	$ 57.82	$ 55.46	$ 55.46	$ 55.46	$ 55.46
IaaS Windows vConfig - 3	8vCPU		1							$ 43.94	$ 39.68	$ 36.78	$ 35.13	$ 32.06	$ 27.34	$ 26.17	$ 26.17	$ 26.17	$ 26.17
	GB Ram		64							$ 152.32	$ 144.70	$ 137.47	$ 130.60	$ 124.07	$ 117.86	$ 111.97	$ 111.97	$ 111.97	$ 111.97
	Windows Server 2008 R2		1							$ 19.25	$ 18.93	$ 18.70	$ 19.23	$ 18.75	$ 19.61	$ 19.17	$ 19.17	$ 19.17	$ 19.17
	Firewall/IDS		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Site-Site VPN		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	VPN Client		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	VLAN		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Windows vConfig - 3	Total									$ 215.51	$ 203.31	$ 192.95	$ 184.96	$ 174.88	$ 164.81	$ 157.31	$ 157.31	$ 157.31	$ 157.31
IaaS Windows vConfig - 4	4vCPU		1							$ 13.98	$ 12.57	$ 11.67	$ 11.15	$ 10.23	$ 8.74	$ 8.30	$ 8.30	$ 8.30	$ 8.30
	GB Ram		16							$ 38.08	$ 36.18	$ 34.37	$ 32.65	$ 31.02	$ 29.47	$ 27.99	$ 27.99	$ 27.99	$ 27.99
	Windows Server 2008 R2		1							$ 19.25	$ 18.93	$ 18.70	$ 19.23	$ 18.75	$ 19.61	$ 19.17	$ 19.17	$ 19.17	$ 19.17
	Firewall/IDS		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Site-Site VPN		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	VPN Client		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	VLAN		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Windows vConfig - 4	Total									$ 71.32	$ 67.67	$ 64.74	$ 63.03	$ 59.99	$ 57.82	$ 55.46	$ 55.46	$ 55.46	$ 55.46
IaaS Windows vConfig - 5	4vCPU		1							$ 13.98	$ 12.57	$ 11.67	$ 11.15	$ 10.23	$ 8.74	$ 8.30	$ 8.30	$ 8.30	$ 8.30
	GB Ram		16							$ 38.08	$ 36.18	$ 34.37	$ 32.65	$ 31.02	$ 29.47	$ 27.99	$ 27.99	$ 27.99	$ 27.99
	Windows Server 2008 R2		1							$ 19.25	$ 18.93	$ 18.70	$ 19.23	$ 18.75	$ 19.61	$ 19.17	$ 19.17	$ 19.17	$ 19.17
	Firewall/IDS		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Site-Site VPN		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	VPN Client		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	VLAN		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Windows vConfig - 5	Total									$ 71.32	$ 67.67	$ 64.74	$ 63.03	$ 59.99	$ 57.82	$ 55.46	$ 55.46	$ 55.46	$ 55.46
IaaS x86 Server Configurations (Linux)																			
IaaS Linux vConfig - 1	2vCPU	Per Server		CCSU13340012-A	N/A	N/A	A			$ 5.24	$ 4.65	$ 4.34	$ 4.15	$ 3.85	$ 3.31	$ 3.08	$ 3.08	$ 3.08	$ 3.08
IaaS Linux vConfig - 2 4 5	4vCPU	Per Server		CCSU13340013-A	N/A	N/A	A			$ 13.98	$ 12.57	$ 11.67	$ 11.15	$ 10.23	$ 8.74	$ 8.30	$ 8.30	$ 3.08	$ 3.08
IaaS Linux vConfig - 3	8vCPU	Per Server		CCSU13340014-A	N/A	N/A	A			$ 43.94	$ 39.68	$ 36.78	$ 35.13	$ 32.06	$ 27.34	$ 26.17	$ 26.17	$ 3.08	$ 3.08
IaaS Linux vConfig - 1, 2, 3, 4, 5	GB Ram	Per GB		CCSU13340015-A	N/A	N/A	A			$ 2.38	$ 2.26	$ 2.15	$ 2.04	$ 1.94	$ 1.84	$ 1.75	$ 1.75	$ 1.75	$ 3.08
IaaS Linux vConfig - 1, 2, 3, 4, 5	RedHat or SUSE	Per License		CCSU13340016-A	N/A	N/A	A			$ 19.11	$ 18.79	$ 18.57	$ 19.09	$ 18.61	$ 19.48	$ 19.03	$ 19.03	$ 19.03	$ 19.03
IaaS Linux vConfig - 1 2 3 4 5	Firewall/IDS	Per Config		CCSU13340017-A	N/A	N/A	A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Linux vConfig - 1 2 3 4 5	Site-Site VPN	Per Config		CCSU13340018-A	N/A	N/A	A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Linux vConfig - 1, 2, 3, 4, 5	VPN Client	Per Config		CCSU13340019-A	N/A	N/A	A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Linux vConfig - 1, 2, 3, 4, 5	VLAN	Per Config		CCSU13340020-A	N/A	N/A	A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Linux vConfig - 4	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Config		CCSU13340021-A	N/A	N/A	A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Linux vConfig - 5	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Config		CCSU13340022-A	N/A	N/A	A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Linux vConfig - 1	2vCPU		1							$ 5.24	$ 4.65	$ 4.34	$ 4.15	$ 3.85	$ 3.31	$ 3.08	$ 3.08	$ 3.08	$ 3.08
	4 GB Ram		4							$ 9.52	$ 9.04	$ 8.59	$ 8.16	$ 7.75	$ 7.37	$ 7.00	$ 7.00	$ 7.00	$ 12.31
	RedHat or SUSE		1							$ 19.11	$ 18.79	$ 18.57	$ 19.09	$ 18.61	$ 19.48	$ 19.03	$ 19.03	$ 19.03	$ 19.03
	Firewall/IDS		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Site-Site VPN		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	VPN Client		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	VLAN		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Linux vConfig - 1	Total									$ 33.87	$ 32.48	$ 31.49	$ 31.41	$ 30.22	$ 30.16	$ 29.11	$ 29.11	$ 29.11	$ 34.42
IaaS Linux vConfig - 2	4vCPU		1							$ 13.98	$ 12.57	$ 11.67	$ 11.15	$ 10.23	$ 8.74	$ 8.30	$ 8.30	$ 3.08	$ 3.08
	16 GB Ram		16							$ 38.08	$ 36.18	$ 34.37	$ 32.65	$ 31.02	$ 29.47	$ 27.99	$ 27.99	$ 27.99	$ 49.23
	RedHat or SUSE		1							$ 19.11	$ 18.79	$ 18.57	$ 19.09	$ 18.61	$ 19.48	$ 19.03	$ 19.03	$ 19.03	$ 19.03
	Firewall/IDS		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Site-Site VPN		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	VPN Client		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	VLAN		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Linux vConfig - 2	Total									$ 71.18	$ 67.53	$ 64.60	$ 62.90	$ 59.86	$ 57.69	$ 55.32	$ 55.32	$ 50.10	$ 71.34

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	Product Name	Unit	Qty per config	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
IaaS Linux vConfig - 3	8vCPU		1							$ 43.94	$ 39.68	$ 36.78	$ 35.13	$ 32.06	$ 27.34	$ 26.17	$ 26.17	$ 3.08	$ 3.08
	64 GB Ram		64							$ 152.32	$ 144.70	$ 137.47	$ 130.60	$ 124.07	$ 117.86	$ 111.97	$ 111.97	$ 111.97	$ 196.91
	RedHat or SUSE		1							$ 19.11	$ 18.79	$ 18.57	$ 19.09	$ 18.61	$ 19.48	$ 19.03	$ 19.03	$ 19.03	$ 19.03
	Firewall/IDS		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Site-Site VPN		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	VPN Client		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	VLAN		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Linux vConfig - 3	Total									$ 215.37	$ 203.17	$ 192.81	$ 184.82	$ 174.74	$ 164.68	$ 157.17	$ 157.17	$ 134.08	$ 219.02
IaaS Linux vConfig - 4	4vCPU		1							$ 13.98	$ 12.57	$ 11.67	$ 11.15	$ 10.23	$ 8.74	$ 8.30	$ 8.30	$ 3.08	$ 3.08
	16 GB Ram		16							$ 38.08	$ 36.18	$ 34.37	$ 32.65	$ 31.02	$ 29.47	$ 27.99	$ 27.99	$ 27.99	$ 49.23
	RedHat or SUSE		1							$ 19.11	$ 18.79	$ 18.57	$ 19.09	$ 18.61	$ 19.48	$ 19.03	$ 19.03	$ 19.03	$ 19.03
	Firewall/IDS		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Site-Site VPN		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	VPN Client		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	VLAN		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Linux vConfig - 4	Total									$ 71.18	$ 67.53	$ 64.60	$ 62.90	$ 59.86	$ 57.69	$ 55.32	$ 55.32	$ 50.10	$ 71.34
IaaS Linux vConfig - 5	4vCPU		1							$ 13.98	$ 12.57	$ 11.67	$ 11.15	$ 10.23	$ 8.74	$ 8.30	$ 8.30	$ 3.08	$ 3.08
	16 GB Ram		16							$ 38.08	$ 36.18	$ 34.37	$ 32.65	$ 31.02	$ 29.47	$ 27.99	$ 27.99	$ 27.99	$ 49.23
	RedHat or SUSE		1							$ 19.11	$ 18.79	$ 18.57	$ 19.09	$ 18.61	$ 19.48	$ 19.03	$ 19.03	$ 19.03	$ 19.03
	Firewall/IDS		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Site-Site VPN		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	VPN Client		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	VLAN		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Linux vConfig - 5	Total									$ 71.18	$ 67.53	$ 64.60	$ 62.90	$ 59.86	$ 57.69	$ 55.32	$ 55.32	$ 50.10	$ 71.34
IaaS Storage Configurations																			
IaaS Storage Config - 1, 2	SAN attached storage	Per GB		CCSU13340023-A	N/A	N/A	A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Storage Config - 3	Network Attached Storage	Per GB		CCSU13340024-A	N/A	N/A	A			$ 0.07	$ 0.06	$ 0.06	$ 0.05	$ 0.05	$ 0.03	$ 0.03	$ 0.03	$ 0.03	$ 0.02
IaaS Storage Config - 1	Raid 5	Per GB		CCSU13340025-A	N/A	N/A	A			$ 0.06	$ 0.05	$ 0.05	$ 0.05	$ 0.05	$ 0.04	$ 0.04	$ 0.04	$ 0.03	$ 0.03
IaaS Storage Config - 2	Raid 10	Per GB		CCSU13340026-A	N/A	N/A	A			$ 0.24	$ 0.24	$ 0.24	$ 0.23	$ 0.23	$ 0.23	$ 0.23	$ 0.21	$ 0.19	$ 0.17
IaaS Storage Config - 1, 2	10K - 15K RPM discs	Per GB		CCSU13340027-A	N/A	N/A	A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Storage Config - 1	SAN attached storage		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Raid 5		1							$ 0.06	$ 0.05	$ 0.05	$ 0.05	$ 0.05	$ 0.04	$ 0.04	$ 0.04	$ 0.03	$ 0.03
	10K - 15K RPM discs		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Storage Config - 1	Total									$ 0.06	$ 0.05	$ 0.05	$ 0.05	$ 0.05	$ 0.04	$ 0.04	$ 0.04	$ 0.03	$ 0.03
IaaS Storage Config - 2	SAN attached storage		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Raid 10		1							$ 0.24	$ 0.24	$ 0.24	$ 0.23	$ 0.23	$ 0.23	$ 0.23	$ 0.21	$ 0.19	$ 0.17
	10K - 15K RPM discs		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Storage Config - 2	Total									$ 0.24	$ 0.24	$ 0.24	$ 0.23	$ 0.23	$ 0.23	$ 0.23	$ 0.21	$ 0.19	$ 0.17
IaaS Storage Config - 3	Network Attached Storage		1							$ 0.07	$ 0.06	$ 0.06	$ 0.05	$ 0.05	$ 0.03	$ 0.03	$ 0.03	$ 0.03	$ 0.02
IaaS Storage Config - 3	Total									$ 0.07	$ 0.06	$ 0.06	$ 0.05	$ 0.05	$ 0.03	$ 0.03	$ 0.03	$ 0.03	$ 0.02
IaaS Backup Configurations																			
IaaS Backup Config - 1	Remote Offsite backup per GB	Per GB		CCSU13340028-A	N/A	N/A	A			$ 0.07	$ 0.05	$ 0.05	$ 0.04	$ 0.04	$ 0.04	$ 0.04	$ 0.03	$ 0.03	$ 0.03
Reserve Account																			
	Reserve Account - Enterprise Datacenter									$84 000.00	$84 000.00	$84 000.00	$84 000.00	$84 000.00	$84 000.00	$84 000.00	$84 000.00	$84 000.00	$84 000.00
Third Party Software																			
Third Party Software																			
Vendor	**Product**																		
B & L	BL/LIB Tape Library Management System	License		CCSU13350001-A			A			$ 1 392.63	$ 1 459.61	$ 1 503.40	$ 1 548.51	$ 1 594.96	$ 1 642.81	$ 1 692.09	$ 1 692.09	$ 1 692.09	$ 1 692.09
B & L	BL/SCHED Schedu ing & Monitoring System	License		CCSU13350002-A			A			$ 1,757.19	$ 1,841.71	$ 1,896.96	$ 1,953.87	$ 2,012.48	$ 2,072.86	$ 2,135.04	$ 2,135.04	$ 2,135.04	$ 2,135.04
BMC Software	BMC AppSight for Windows/.NET - Division Edition	License		CCSU13350003-A			A			$ 4,837.96	$ 4,983.10	$ 5,132.59	$ 5,286.57	$ 5,445.17	$ 5,608.53	$ 5,776.78	$ 5,776.78	$ 5,776.78	$ 5,776.78
BMC Software	BMC AppSight Named Users	License		CCSU13350004-A			A			$ 35.26	$ 36.31	$ 37.40	$ 38.53	$ 39.68	$ 40.87	$ 42.10	$ 42.10	$ 42.10	$ 42.10
BMC Software	BMC AppSight QA Users	License		CCSU13350005-A			A			$ 13.71	$ 14.12	$ 14.55	$ 14.98	$ 15.43	$ 15.90	$ 16.37	$ 16.37	$ 16.37	$ 16.37
BMC Software	CONTROL-M Enterprise Manager	License		CCSU13350006-A			A			$ 305.56	$ 314.72	$ 324.16	$ 333.89	$ 343.91	$ 354.22	$ 364.85	$ 364.85	$ 364.85	$ 364.85
BMC Software	CONTROL-M Full Admin User	License		CCSU13350007-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	CONTROL-M Tasks (100 Tasks per Unit)	License		CCSU13350008-A			A			$ 3 465.00	$ 3 568.95	$ 3 676.02	$ 3 786.30	$ 3 899.89	$ 4 016.88	$ 4 137.39	$ 4 137.39	$ 4 137.39	$ 4 137.39
BMC Software	Database Director (D2)	License		CCSI13350009-A			A			$ 36 631.86	$ 37 730.82	$ 38 862.75	$ 40 028.63	$ 41 229.49	$ 42 466.37	$ 43 740.37	$ 45 052.57	$ 46 404.15	$ 47 796.27
BMC Software	Eclipse iBuild	License		CCSI13350010-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iChange	License		CCSI13350011-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iCheck	License		CCSI13350012-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iCopy	License		CCSI13350013-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iExtract	License		CCSI13350014-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iLM	License		CCSI13350015-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iLoad	License		CCSI13350016-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iRecover	License		CCSI13350017-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iSurvey	License		CCSI13350018-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	**Product Name**	**Unit**	**Qty per config**	**Provider Part Number**	**Version Major**	**Version Minor**	**Version Build**	**Manufacturer ID**	**Equipment Code**	**Price per unit \ Per Month**									
Description / Use *>*	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
BMC Software	Eclipse iUnload	License		CCSI13350019-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Mission Control	License		CCSI13350020-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Business Objects	Crystal Reports	License		CCSU13350021-A			A			$ 10.08	$ 10.39	$ 10.70	$ 11.02	$ 11.35	$ 11.69	$ 12.04	$ 12.04	$ 12.04	$ 12.04
Bytware Inc.	StandGuard Anti-Virus	License		CCSU13350022-A			A			$ 103.89	$ 107.01	$ 110.22	$ 113.52	$ 116.93	$ 120.44	$ 124.05	$ 124.05	$ 124.05	$ 124.05
Citrix	XenApp Advanced (User Counts)	License		CCSU13350023-A			A			$ -	$ 3.36	$ 3.46	$ 3.57	$ 3.68	$ 3.79	$ 3.90	$ 3.90	$ 3.90	$ 3.90
Citrix	XenApp Enterprise (User Counts)	License		CCSU13350024-A			A			$ -	$ 3.74	$ 3.85	$ 3.97	$ 4.08	$ 4.21	$ 4.33	$ 4.33	$ 4.33	$ 4.33
Computer Associates International, Inc.	CA-Explore for CICS	License		CCSI13350025-A			A			$ 734.41	$ 756.45	$ 779.14	$ 802.51	$ 826.59	$ 851.39	$ 876.93	$ 903.24	$ 930.33	$ 958.24
Computer Associates International, Inc.	SOA Security Manager	License		CCSU13350026-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	SOA Security Manager Additional Secured Web Services	License		CCSU13350027-A			A			$ 81.48	$ 83.93	$ 86.44	$ 89.04	$ 91.71	$ 94.46	$ 97.29	$ 97.29	$ 97.29	$ 97.29
Computer Associates International Inc.	SOA Security Manager Additional Users	License		CCSU13350028-A			A			$ 0.28	$ 0.29	$ 0.30	$ 0.31	$ 0.32	$ 0.32	$ 0.33	$ 0.33	$ 0.33	$ 0.33
Corticon Technologies	Corticon Business Rules Server – Un imited CPUs	License		CCSU13350029-A			A			$ 13 037.04	$ 13 428.15	$ 13 830.99	$ 14 245.92	$ 14 673.30	$ 15 113.50	$ 15 566.90	$ 15 566.90	$ 15 566.90	$ 15 566.90
Corticon Technologies	Corticon Server – per Non-Production Server	License		CCSU13350030-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Corticon Technologies	Corticon Business Rules Mode ing Studio – per Named User	License		CCSU13350031-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
CSI International	EPIC	License		CCSI13350032-A			A			$ 2,078.62	$ 2,140.98	$ 2,205.21	$ 2,271.36	$ 2,339.51	$ 2,409.69	$ 2,481.98	$ 2,556.44	$ 2,633.13	$ 2,712.13
CSI International	FAQS/PCS	License		CCSI13350033-A			A			$ 1 263.91	$ 1 301.83	$ 1 340.89	$ 1 381.11	$ 1 422.55	$ 1 465.22	$ 1 509.18	$ 1 554.46	$ 1 601.09	$ 1 649.12
CSI International	FAQS/ASO	License		CCSU13350034-A			A			$ 1 549.50	$ 1 595.98	$ 1 643.86	$ 1 693.18	$ 1 743.97	$ 1 796.29	$ 1 850.18	$ 1 905.69	$ 1 962.86	$ 2 021.74
EMC Corporation	PowerPath	License		CCSU13350035-A			A			$ 2.87	$ 2.96	$ 3.05	$ 3.14	$ 3.23	$ 3.33	$ 3.43	$ 3.43	$ 3.43	$ 3.43
EMC Corporation	PowerPath (per CPU)	License		CCSU13350036-A			A			$ 2.87	$ 2.96	$ 3.05	$ 3.14	$ 3.23	$ 3.33	$ 3.43	$ 3.43	$ 3.43	$ 3.43
EMC Corporation	Symmetrix® VMAX Fully Automated Storage Tiering for Virtual Pools (FAST VP)	License		CCSU13350037-A			A			$ 189.70	$ 195.39	$ 201.25	$ 207.28	$ 213.50	$ 219.91	$ 226.51	$ 226.51	$ 226.51	$ 226.51
EMC Corporation	Vsphere Enterprise Plus	License		CCSU13350038-A			A			$ 73.33	$ 75.53	$ 77.80	$ 80.13	$ 82.54	$ 85.01	$ 87.56	$ 87.56	$ 87.56	$ 87.56
Experian QAS	NameSearch - Production (Licensed per Server up to 8 CPU)	License		CCSU13350039-A			A			$ 5,703.70	$ 5,874.81	$ 6,051.06	$ 6,232.59	$ 6,419.57	$ 6,612.16	$ 6,810.52	$ 6,810.52	$ 6,810.52	$ 6,810.52
Experian QAS	NameSearch - Non-Production (Licensed per Server)	License		CCSU13350040-A			A			$ 865.74	$ 891.71	$ 918.46	$ 946.02	$ 974.40	$ 1,003.63	$ 1,033.74	$ 1,033.74	$ 1,033.74	$ 1,033.74
Formula Consultants, Inc.	Star 1100	License		CCSU13350041-A			A			$ 198.00	$ 203.94	$ 210.06	$ 216.36	$ 222.85	$ 229.54	$ 236.42	$ 236.42	$ 236.42	$ 236.42
GlobalScape	CuteFTP Pro 2.0	License		CCSU13350042-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
HELPSYS	Robot/Schedule	License		CCSI13350043-A			A			$ 1 500.04	$ 1 545.05	$ 1 591.40	$ 1 639.14	$ 1 688.31	$ 1 738.96	$ 1 791.13	$ 1 844.87	$ 1 900.21	$ 1 957.22
Idea Integration	XGEN	License		CCSU13350044-A			A			$ 3,300.15	$ 3,399.16	$ 3,501.13	$ 3,606.17	$ 3,714.35	$ 3,825.78	$ 3,940.56	$ 3,940.56	$ 3,940.56	$ 3,940.56
Informatica Corporation	SSA-Name 3	License		CCSU13350045-A			A			$ 5,347.22	$ 5,507.64	$ 5,672.87	$ 5,843.05	$ 6,018.35	$ 6,198.90	$ 6,384.86	$ 6,384.86	$ 6,384.86	$ 6,384.86
Infragistics	NetAdvantage for .NET	License		CCSU13350046-A			A			$ 77.96	$ 80.30	$ 82.71	$ 85.19	$ 87.75	$ 90.38	$ 93.09	$ 93.09	$ 93.09	$ 93.09
KMSYS Worldwide, Inc.	IQU Plus-1	License		CCSU13350047-A			A			$ 488.89	$ 503.56	$ 518.66	$ 534.22	$ 550.25	$ 566.76	$ 583.76	$ 583.76	$ 583.76	$ 583.76
Levi, Ray and Shoup	VPS/PCL	License		CCSI13350048-A			A			$ 4,771.08	$ 4,914.21	$ 5,061.64	$ 5,213.49	$ 5,369.89	$ 5,530.99	$ 5,696.92	$ 5,867.83	$ 6,043.86	$ 6,225.18
Levi, Ray and Shoup	VPS/TCP/IP	License		CCSI13350049-A			A			$ 3,357.30	$ 3,458.02	$ 3,561.76	$ 3,668.61	$ 3,778.67	$ 3,892.03	$ 4,008.79	$ 4,129.06	$ 4,252.93	$ 4,380.52
Levi, Ray and Shoup	VPS/DRS	License		CCSI13350050-A			A			$ 1 698.67	$ 1 749.63	$ 1 802.12	$ 1 856.18	$ 1 911.87	$ 1 969.22	$ 2 028.30	$ 2 089.15	$ 2 151.83	$ 2 216.38
Levi, Ray and Shoup	VPS	License		CCSI13350051-A			A			$ 5 256.44	$ 5 414.13	$ 5 576.55	$ 5 743.85	$ 5 916.16	$ 6 093.65	$ 6 276.46	$ 6 464.75	$ 6 658.70	$ 6 858.46
MacKinney Systems, Inc.	CICS Response Time Monitor	License		CCSI13350052-A			A			$ 37.99	$ 39.13	$ 40.31	$ 41.52	$ 42.76	$ 44.04	$ 45.37	$ 46.73	$ 48.13	$ 49.57
Marble Computer, Inc.	OS DCD III Data Correlation and Documentation System	License		CCSU13350053-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	BizTalk Adaptor for MQSeries	License		CCSU13350054-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	BizTalk Server Enterprise (Single Processor)	License		CCSU13350055-A			A			$ 1 595.34	$ 1 643.20	$ 1 692.50	$ 1 743.28	$ 1 795.57	$ 1 849.44	$ 1 904.92	$ 1 904.92	$ 1 904.92	$ 1 904.92
Microsoft	BizTalk Server Standard (Single Processor)	License		CCSU13350056-A			A			$ 365.70	$ 376.67	$ 387.97	$ 399.61	$ 411.60	$ 423.95	$ 436.66	$ 436.66	$ 436.66	$ 436.66
Microsoft	SQL Server CAL	License		CCSU13350057-A			A			$ 129.32	$ 129.32	$ 129.32	$ 129.32	$ 129.32	$ 129.32	$ 129.32	$ 129.32	$ 129.32	$ 129.32
Microsoft	SQL Server Enterprise (Single Processor)	License		CCSU13350058-A			A			$ 495.94	$ 510.82	$ 526.15	$ 541.93	$ 558.19	$ 574.94	$ 592.18	$ 592.18	$ 592.18	$ 592.18
Microsoft	SQL Server Enterprise	License		CCSU13350059-A			A			$ 495.94	$ 510.82	$ 526.15	$ 541.93	$ 558.19	$ 574.94	$ 592.18	$ 592.18	$ 592.18	$ 592.18
Microsoft	SQL Server Standard (Single Processor)	License		CCSU13350060-A			A			$ 129.32	$ 133.20	$ 137.20	$ 141.31	$ 145.55	$ 149.92	$ 154.42	$ 154.42	$ 154.42	$ 154.42
Microsoft	SQL Server Standard	License		CCSU13350061-A			A			$ 129.32	$ 133.20	$ 137.20	$ 141.31	$ 145.55	$ 149.92	$ 154.42	$ 154.42	$ 154.42	$ 154.42
Microsoft	SQL Server Standard per 2-Core	License		CCSU13350062-A			A			$ 258.64	$ 266.40	$ 274.40	$ 282.63	$ 291.11	$ 299.84	$ 308.83	$ 308.83	$ 308.83	$ 308.83
Microsoft	Visual Studio Foundation Server	License		CCSU13350063-A			A			$ 14.90	$ 15.35	$ 15.81	$ 16.29	$ 16.77	$ 17.28	$ 17.80	$ 17.80	$ 17.80	$ 17.80
Microsoft	Visual Studio Foundation Server CAL	License		CCSU13350064-A			A			$ 17.15	$ 17.66	$ 18.19	$ 18.74	$ 19.30	$ 19.88	$ 20.47	$ 20.47	$ 20.47	$ 20.47
Microsoft	Visual Studio Professional with MSDN	License		CCSU13350065-A			A			$ 22.41	$ 23.08	$ 23.78	$ 24.49	$ 25.22	$ 25.98	$ 26.76	$ 26.76	$ 26.76	$ 26.76
Microsoft	Windows Server Datacenter Edition (Single Processor)	License		CCSU13350066-A			A			$ 70.06	$ 72.16	$ 74.32	$ 76.55	$ 78.85	$ 81.21	$ 83.65	$ 83.65	$ 83.65	$ 83.65
Microsoft	Windows Server Enterprise Edition	License		CCSU13350067-A			A			$ 50.09	$ 51.59	$ 53.14	$ 54.73	$ 56.38	$ 58.07	$ 59.81	$ 59.81	$ 59.81	$ 59.81
Microsoft	Windows Server Standard Edition	License		CCSU13350068-A			A			$ 13.21	$ 13.61	$ 14.02	$ 14.44	$ 14.87	$ 15.32	$ 15.77	$ 15.77	$ 15.77	$ 15.77
Microsoft	Windows Terminal Service Client Access Licenses	License		CCSU13350069-A			A			$ 3.72	$ 3.83	$ 3.95	$ 4.07	$ 4.19	$ 4.32	$ 4.44	$ 4.44	$ 4.44	$ 4.44
Network Associates	McAfee Anti-Virus	License		CCSU13350070-A			A			$ 0.89	$ 0.92	$ 0.95	$ 0.98	$ 1.01	$ 1.04	$ 1.07	$ 1.07	$ 1.07	$ 1.07
Novell	Platespin Migrator	License		CCSU13350071-A			A			$ 8.25	$ 8.50	$ 8.75	$ 9.01	$ 9.29	$ 9.56	$ 9.85	$ 9.85	$ 9.85	$ 9.85
Novell	SuSE Linux	License		CCSI13350072-A			A			$ 1 353.09	$ 1 393.68	$ 1 435.49	$ 1 478.55	$ 1 522.91	$ 1 568.60	$ 1 615.66	$ 1 664.13	$ 1 714.05	$ 1 765.47
OpenText	Metastorm Integration Manager for CICS (MIM for CICS)	License		CCSI13350073-A			A			$ 9,007.22	$ 9,277.44	$ 9,555.76	$ 9,842.43	$ 10,137.70	$ 10,441.84	$ 10,755.09	$ 11,077.74	$ 11,410.08	$ 11,752.38
Oracle	Oracle Change Management Pack	License		CCSU13350074-A			A			$ 134.44	$ 138.48	$ 142.63	$ 146.91	$ 151.32	$ 155.86	$ 160.53	$ 160.53	$ 160.53	$ 160.53
Oracle	Oracle Database 10g Enterprise	License		CCSU13350075-A			A			$ 948.55	$ 977.00	$ 1,006.31	$ 1,036.50	$ 1,067.60	$ 1,099.63	$ 1,132.62	$ 1,166.59	$ 1,201.59	$ 1,237.64
Oracle	Oracle Database Enterprise Edition	License		CCSU13350076-A			A			$ 532.18	$ 548.14	$ 564.59	$ 581.52	$ 598.97	$ 616.94	$ 635.45	$ 635.45	$ 635.45	$ 635.45
Oracle	Oracle Diagnostic Pack	License		CCSU13350077-A			A			$ 72.45	$ 74.63	$ 76.87	$ 79.17	$ 81.55	$ 83.99	$ 86.51	$ 87.10	$ 87.71	$ 88.33
Oracle	Oracle Enterprise Linux	License		CCSU13350078-A			A			$ 142.49	$ 146.77	$ 151.17	$ 155.70	$ 160.37	$ 165.19	$ 170.14	$ 170.14	$ 170.14	$ 170.14
Oracle	Oracle Exadata Storage Software	License		CCSU13350079-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Oracle	Oracle Partitioning	License		CCSU13350080-A			A			$ 128.84	$ 132.71	$ 136.69	$ 140.79	$ 145.01	$ 149.36	$ 153.84	$ 153.84	$ 153.84	$ 153.84
Oracle	Oracle Tuning Pack	License		CCSU13350081-A			A			$ 89.16	$ 90.84	$ 92.58	$ 94.36	$ 96.20	$ 98.09	$ 100.04	$ 100.04	$ 100.04	$ 100.04
Oracle	Real Application Cluster - Processor Perpetual	License		CCSU13350082-A			A			$ 442.17	$ 455.43	$ 469.10	$ 483.17	$ 497.66	$ 512.59	$ 527.97	$ 543.81	$ 560.12	$ 576.93
Oracle	Spatial and Graph - Processor Perpetual	License		CCSU13350083-A			A			$ 336.43	$ 346.52	$ 356.92	$ 367.63	$ 378.66	$ 390.02	$ 401.72	$ 413.77	$ 426.18	$ 438.97
P tney Bowes	Finalist (Doc Sense)	License		CCSI13350084-A			A			$ 7,795.87	$ 8,029.75	$ 8,270.64	$ 8,518.76	$ 8,774.32	$ 9,037.55	$ 9,308.68	$ 9,587.94	$ 9,875.57	$ 10,171.84
P tney Bowes	CODE-1 Plus	License		CCSU13350085-A			A			$ 733.33	$ 755.33	$ 777.99	$ 801.33	$ 825.37	$ 850.13	$ 875.64	$ 875.64	$ 875.64	$ 875.64
P tney Bowes	CODE-1 Plus (Test / Development)	License		CCSU13350086-A			A			$ 336.11	$ 346.19	$ 356.58	$ 367.28	$ 378.30	$ 389.64	$ 401.33	$ 401.33	$ 401.33	$ 401.33

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	**Product Name**	**Unit**	**Qty per config**	**Provider Part Number**	**Version Major**	**Version Minor**	**Version Build**	**Manufacturer ID**	**Equipment Code**	**Price per unit \ Per Month**									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
P tney Bowes	Online Window for Finalist	License		CCSI13350087-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Quest	Central Performance Suite for SQL Server, Tier A	License		CCSU13350088-A			A			$ 44.11	$ 45.44	$ 46.80	$ 48.21	$ 49.65	$ 51.14	$ 52.68	$ 52.68	$ 52.68	$ 52.68
Quest	Central Performance Suite for SQL Server, Tier B	License		CCSU13350089-A			A			$ 44.11	$ 45.44	$ 46.80	$ 48.21	$ 49.65	$ 51.14	$ 52.68	$ 52.68	$ 52.68	$ 52.68
Quest	Foglight Database Management Suite for SQL Server	License		CCSU13350090-A			A			$ 44.11	$ 45.44	$ 46.80	$ 48.21	$ 49.65	$ 51.14	$ 52.68	$ 52.68	$ 52.68	$ 52.68
Quest	Foglight for SQL Server per CPU Socket	License		CCSU13350091-A			A			$ 22.06	$ 22.72	$ 23.40	$ 24.10	$ 24.83	$ 25.57	$ 26.34	$ 26.34	$ 26.34	$ 26.34
Quest	Foglight OS Management per CPU Socket	License		CCSU13350092-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Quest	Foglight Server for FSM	License		CCSU13350093-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
RealVNC	VNC Enterprise Ed tion for Windows	License		CCSU13350094-A			A			$ 1.18	$ 1.21	$ 1.25	$ 1.29	$ 1.32	$ 1.36	$ 1.40	$ 1.40	$ 1.40	$ 1.40
Red Hat	Red Hat Enterprise Linux	License		CCSU13350095-A			A			$ 319.87	$ 329.47	$ 339.35	$ 349.53	$ 360.02	$ 370.82	$ 381.94	$ 381.94	$ 381.94	$ 381.94
Schema Systems Limited	Q Ed tor Plus One	License		CCSU13350096-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Segus Inc.	OPC/Graph	License		CCSI13350097-A			A			$ 756.45	$ 779.14	$ 802.51	$ 826.59	$ 851.39	$ 876.93	$ 903.24	$ 930.33	$ 958.24	$ 986.99
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG20	License		CCSU13350098-A			A			$ 56.63	$ 58.33	$ 60.08	$ 61.88	$ 63.74	$ 65.65	$ 67.62	$ 67.62	$ 67.62	$ 67.62
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG40	License		CCSU13350099-A			A			$ 70.07	$ 72.18	$ 74.34	$ 76.57	$ 78.87	$ 81.24	$ 83.67	$ 83.67	$ 83.67	$ 83.67
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG60	License		CCSU13350100-A			A			$ 83.93	$ 86.44	$ 89.04	$ 91.71	$ 94.46	$ 97.29	$ 100.21	$ 100.21	$ 100.21	$ 100.21
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG80	License		CCSU13350101-A			A			$ 97.37	$ 1 203.50	$ 1 239.60	$ 1 276.79	$ 1 315.09	$ 1 354.55	$ 1 395.18	$ 1 395.18	$ 1 395.18	$ 1 395.18
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG130	License		CCSU13350102-A			A			$ 135.26	$ 139.32	$ 143.50	$ 147.80	$ 152.24	$ 156.80	$ 161.51	$ 161.51	$ 161.51	$ 161.51
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG20	License		CCSU13350103-A			A			$ 56.63	$ 58.33	$ 60.08	$ 61.88	$ 63.74	$ 65.65	$ 67.62	$ 67.62	$ 67.62	$ 67.62
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG40	License		CCSU13350104-A			A			$ 70.07	$ 72.18	$ 74.34	$ 76.57	$ 78.87	$ 81.24	$ 83.67	$ 83.67	$ 83.67	$ 83.67
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG60	License		CCSU13350105-A			A			$ 83.93	$ 86.44	$ 89.04	$ 91.71	$ 94.46	$ 97.29	$ 100.21	$ 100.21	$ 100.21	$ 100.21
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG80	License		CCSU13350106-A			A			$ 97.37	$ 100.29	$ 103.30	$ 106.40	$ 109.59	$ 112.88	$ 116.27	$ 116.27	$ 116.27	$ 116.27
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG130	License		CCSU13350107-A			A			$ 135.26	$ 139.32	$ 143.50	$ 147.80	$ 152.24	$ 156.80	$ 161.51	$ 161.51	$ 161.51	$ 161.51
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG140	License		CCSU13350108-A			A			$ 155.63	$ 160.30	$ 165.11	$ 170.06	$ 175.16	$ 180.42	$ 185.83	$ 185.83	$ 185.83	$ 185.83
Sightline	OS 2200 Interface Agent - MAPPER, SWG20	License		CCSU13350109-A			A			$ 56.63	$ 58.33	$ 60.08	$ 61.88	$ 63.74	$ 65.65	$ 67.62	$ 67.62	$ 67.62	$ 67.62
Sightline	OS 2200 Interface Agent - MAPPER, SWG40	License		CCSU13350110-A			A			$ 70.07	$ 72.18	$ 74.34	$ 76.57	$ 78.87	$ 81.24	$ 83.67	$ 83.67	$ 83.67	$ 83.67
Sightline	OS 2200 Interface Agent - MAPPER, SWG60	License		CCSU13350111-A			A			$ 83.93	$ 86.44	$ 89.04	$ 91.71	$ 94.46	$ 97.29	$ 100.21	$ 100.21	$ 100.21	$ 100.21
Sightline	OS 2200 Interface Agent - MAPPER, SWG80	License		CCSU13350112-A			A			$ 97.37	$ 100.29	$ 103.30	$ 106.40	$ 109.59	$ 112.88	$ 116.27	$ 116.27	$ 116.27	$ 116.27
Sightline	OS 2200 Interface Agent - MAPPER, SWG130	License		CCSU13350113-A			A			$ 135.26	$ 139.32	$ 143.50	$ 147.80	$ 152.24	$ 156.80	$ 161.51	$ 161.51	$ 161.51	$ 161.51
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG20	License		CCSU13350114-A			A			$ 57.65	$ 59.38	$ 61.16	$ 62.99	$ 64.88	$ 66.83	$ 68.83	$ 68.83	$ 68.83	$ 68.83
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG40	License		CCSU13350115-A			A			$ 70.07	$ 72.18	$ 74.34	$ 76.57	$ 78.87	$ 81.24	$ 83.67	$ 83.67	$ 83.67	$ 83.67
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG60	License		CCSU13350116-A			A			$ 83.93	$ 86.44	$ 89.04	$ 91.71	$ 94.46	$ 97.29	$ 100.21	$ 100.21	$ 100.21	$ 100.21
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG80	License		CCSU13350117-A			A			$ 97.37	$ 100.29	$ 103.30	$ 106.40	$ 109.59	$ 112.88	$ 116.27	$ 116.27	$ 116.27	$ 116.27
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG130	License		CCSU13350118-A			A			$ 135.26	$ 139.32	$ 143.50	$ 147.80	$ 152.24	$ 156.80	$ 161.51	$ 161.51	$ 161.51	$ 161.51
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG140	License		CCSU13350119-A			A			$ 155.63	$ 160.30	$ 165.11	$ 170.06	$ 175.16	$ 180.42	$ 185.83	$ 185.83	$ 185.83	$ 185.83
Sightline	OS 2200 Interface Agent - System Log, SWG20	License		CCSU13350120-A			A			$ 56.63	$ 58.33	$ 60.08	$ 61.88	$ 63.74	$ 65.65	$ 67.62	$ 67.62	$ 67.62	$ 67.62
Sightline	OS 2200 Interface Agent - System Log, SWG40	License		CCSU13350121-A			A			$ 70.07	$ 72.18	$ 74.34	$ 76.57	$ 78.87	$ 81.24	$ 83.67	$ 83.67	$ 83.67	$ 83.67
Sightline	OS 2200 Interface Agent - System Log, SWG60	License		CCSU13350122-A			A			$ 83.93	$ 86.44	$ 89.04	$ 91.71	$ 94.46	$ 97.29	$ 100.21	$ 100.21	$ 100.21	$ 100.21
Sightline	OS 2200 Interface Agent - System Log, SWG80	License		CCSU13350123-A			A			$ 97.37	$ 100.29	$ 103.30	$ 106.40	$ 109.59	$ 112.88	$ 116.27	$ 116.27	$ 116.27	$ 116.27
Sightline	OS 2200 Interface Agent - System Log, SWG130	License		CCSU13350124-A			A			$ 135.26	$ 139.32	$ 143.50	$ 147.80	$ 152.24	$ 156.80	$ 161.51	$ 161.51	$ 161.51	$ 161.51
Sightline	OS 2200 Interface Agent - System Log, SWG140	License		CCSU13350125-A			A			$ 155.63	$ 160.30	$ 165.11	$ 170.06	$ 175.16	$ 180.42	$ 185.83	$ 185.83	$ 185.83	$ 185.83
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG20	License		CCSU13350126-A			A			$ 56.63	$ 58.33	$ 60.08	$ 61.88	$ 63.74	$ 65.65	$ 67.62	$ 67.62	$ 67.62	$ 67.62
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG40	License		CCSU13350127-A			A			$ 70.07	$ 72.18	$ 74.34	$ 76.57	$ 78.87	$ 81.24	$ 83.67	$ 83.67	$ 83.67	$ 83.67
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG60	License		CCSU13350128-A			A			$ 83.93	$ 86.44	$ 89.04	$ 91.71	$ 94.46	$ 97.29	$ 100.21	$ 100.21	$ 100.21	$ 100.21
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG80	License		CCSU13350129-A			A			$ 97.37	$ 100.29	$ 103.30	$ 106.40	$ 109.59	$ 112.88	$ 116.27	$ 116.27	$ 116.27	$ 116.27
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG130	License		CCSU13350130-A			A			$ 135.26	$ 139.32	$ 143.50	$ 147.80	$ 152.24	$ 156.80	$ 161.51	$ 161.51	$ 161.51	$ 161.51
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG140	License		CCSU13350131-A			A			$ 155.63	$ 160.30	$ 165.11	$ 170.06	$ 175.16	$ 180.42	$ 185.83	$ 185.83	$ 185.83	$ 185.83
Sightline	OS 2200 Power Agent, SWG20	License		CCSU13350132-A			A			$ 113.26	$ 116.66	$ 120.16	$ 123.76	$ 127.47	$ 131.30	$ 135.24	$ 135.24	$ 135.24	$ 135.24
Sightline	OS 2200 Power Agent SWG40	License		CCSU13350133-A			A			$ 140.15	$ 144.35	$ 148.68	$ 153.14	$ 157.74	$ 162.47	$ 167.34	$ 167.34	$ 167.34	$ 167.34
Sightline	OS 2200 Power Agent, SWG60	License		CCSU13350134-A			A			$ 167.85	$ 172.89	$ 178.07	$ 183.42	$ 188.92	$ 194.59	$ 200.42	$ 200.42	$ 200.42	$ 200.42
Sightline	OS 2200 Power Agent, SWG80	License		CCSU13350135-A			A			$ 194.74	$ 200.58	$ 206.60	$ 212.80	$ 219.18	$ 225.76	$ 232.53	$ 232.53	$ 232.53	$ 232.53
Sightline	OS 2200 Power Agent, SWG130	License		CCSU13350136-A			A			$ 270.52	$ 278.63	$ 286.99	$ 295.60	$ 304.47	$ 313.61	$ 323.01	$ 323.01	$ 323.01	$ 323.01
Sightline	OS 2200 Power Agent, SWG140	License		CCSU13350137-A			A			$ 311.26	$ 320.60	$ 330.21	$ 340.12	$ 350.33	$ 360.83	$ 371.66	$ 371.66	$ 371.66	$ 371.66
Sightline	OS 2200 Torch Capacity Manager Power Agent, SWG40	License		CCSU13350138-A			A			$ 574.44	$ 591.68	$ 609.43	$ 627.71	$ 646.54	$ 665.94	$ 685.92	$ 685.92	$ 685.92	$ 685.92
Sightline	OS 2200 Torch Capacity Manager Power Agent, SWG60	License		CCSU13350139-A			A			$ 658.78	$ 678.54	$ 698.90	$ 719.86	$ 741.46	$ 763.70	$ 786.62	$ 786.62	$ 786.62	$ 786.62
Sightline	OS 2200 Torch Capacity Manager Power Agent, SWG130	License		CCSU13350140-A			A			$ 1,043.37	$ 1,074.67	$ 1,106.91	$ 1,140.12	$ 1,174.32	$ 1,209.55	$ 1,245.84	$ 1,245.84	$ 1,245.84	$ 1,245.84
Sightline	OS 2200 Torch Capacity Manager Power Agent, SWG140	License		CCSU13350141-A			A			$ 1,197.37	$ 1,233.29	$ 1,270.29	$ 1,308.40	$ 1,347.65	$ 1,388.08	$ 1,429.72	$ 1,429.72	$ 1,429.72	$ 1,429.72
Sightline	OS 2200 Torch Interface Agent - I/O TRACE, SWG40	License		CCSU13350142-A			A			$ 239.56	$ 246.74	$ 254.14	$ 261.77	$ 269.62	$ 277.71	$ 286.04	$ 286.04	$ 286.04	$ 286.04
Sightline	OS 2200 Torch Interface Agent - I/O TRACE, SWG60	License		CCSU13350143-A			A			$ 290.89	$ 299.62	$ 308.60	$ 317.86	$ 327.40	$ 337.22	$ 347.34	$ 347.34	$ 347.34	$ 347.34
Sightline	OS 2200 Torch Interface Agent - I/O TRACE, SWG130	License		CCSU13350144-A			A			$ 483.19	$ 497.68	$ 512.61	$ 527.99	$ 543.83	$ 560.14	$ 576.95	$ 576.95	$ 576.95	$ 576.95
Sightline	OS 2200 Torch Interface Agent - LOG, SWG40	License		CCSU13350145-A			A			$ 239.56	$ 246.74	$ 254.14	$ 261.77	$ 269.62	$ 277.71	$ 286.04	$ 286.04	$ 286.04	$ 286.04
Sightline	OS 2200 Torch Interface Agent - LOG, SWG60	License		CCSU13350146-A			A			$ 290.89	$ 299.62	$ 308.60	$ 317.86	$ 327.40	$ 337.22	$ 347.34	$ 347.34	$ 347.34	$ 347.34
Sightline	OS 2200 Torch Interface Agent - LOG, SWG130	License		CCSU13350147-A			A			$ 483.19	$ 497.68	$ 512.61	$ 527.99	$ 543.83	$ 560.14	$ 576.95	$ 576.95	$ 576.95	$ 576.95

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	**Product Name**	**Unit**	**Qty per config**	**Provider Part Number**	**Version Major**	**Version Minor**	**Version Build**	**Manufacturer ID**	**Equipment Code**	**Price per unit \ Per Month**									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Sightline	OS 2200 Torch Interface Agent - LOG, SWG140	License		CCSU13350148-A			A			$ 560.19	$ 576.99	$ 594.30	$ 612.13	$ 630.49	$ 649.41	$ 668.89	$ 668.89	$ 668.89	$ 668.89
Sightline	OS 2200 Torch Interface Agent - MAPPER, SWG40	License		CCSU13350149-A			A			$ 239.56	$ 246.74	$ 254.14	$ 261.77	$ 269.62	$ 277.71	$ 286.04	$ 286.04	$ 286.04	$ 286.04
Sightline	OS 2200 Torch Interface Agent - MAPPER, SWG60	License		CCSU13350150-A			A			$ 290.89	$ 299.62	$ 308.60	$ 317.86	$ 327.40	$ 337.22	$ 347.34	$ 347.34	$ 347.34	$ 347.34
Sightline	OS 2200 Torch Interface Agent - MAPPER, SWG130	License		CCSU13350151-A			A			$ 483.19	$ 497.68	$ 512.61	$ 527.99	$ 543.83	$ 560.14	$ 576.95	$ 576.95	$ 576.95	$ 576.95
Sightline	Windows 2000 Interface Agent - Internet Information Server	License		CCSU13350152-A			A			$ 24.44	$ 25.18	$ 25.93	$ 26.71	$ 27.51	$ 28.34	$ 29.19	$ 29.19	$ 29.19	$ 29.19
Sightline	Windows 2000 Interface Agent - .NET	License		CCSU13350153-A			A			$ 48.89	$ 50.36	$ 51.87	$ 53.42	$ 55.02	$ 56.68	$ 58.38	$ 58.38	$ 58.38	$ 58.38
Sightline	Windows 2000 Interface Agent - SQL Server	License		CCSU13350154-A			A			$ 81.48	$ 83.93	$ 86.44	$ 89.04	$ 91.71	$ 94.46	$ 97.29	$ 97.29	$ 97.29	$ 97.29
Sightline	Windows 2000 Power Agent Upto 32 CPU's	License		CCSU13350155-A			A			$ 268.89	$ 276.96	$ 285.26	$ 293.82	$ 302.64	$ 311.72	$ 321.07	$ 321.07	$ 321.07	$ 321.07
SMA	OpCon/xps EXEC LSAM, Group 3	License		CCSU13350156-A			A			$ 324.88	$ 333.71	$ 342.79	$ 352.16	$ 361.80	$ 371.73	$ 381.96	$ 381.96	$ 381.96	$ 381.96
SMA	OpCon/xps EXEC LSAM Group 12	License		CCSU13350157-A			A			$ 1 983.73	$ 2 037.62	$ 2 093.11	$ 2 150.28	$ 2 209.16	$ 2 269.80	$ 2 332.26	$ 2 332.26	$ 2 332.26	$ 2 332.26
SMA	OpCon/xps EXEC LSAM Development, Group 2	License		CCSU13350158-A			A			$ 108.93	$ 111.89	$ 114.94	$ 118.07	$ 121.31	$ 124.64	$ 128.07	$ 128.07	$ 128.07	$ 128.07
SMA	OpCon/xps EXEC LSAM Development, Group 12	License		CCSU13350159-A			A			$ 991.82	$ 1 018.76	$ 1 046.51	$ 1 075.09	$ 1 104.52	$ 1 134.84	$ 1 166.07	$ 1 166.07	$ 1 166.07	$ 1 166.07
SMA	OpCon/xps Production SAM	License		CCSU13350160-A			A			$ 347.83	$ 357.28	$ 367.01	$ 377.03	$ 387.36	$ 397.99	$ 408.94	$ 408.94	$ 408.94	$ 408.94
SMA	OpCon/xps Starter Kit	License		CCSU13350161-A			A			$ 595.93	$ 612.12	$ 628.79	$ 645.96	$ 663.65	$ 681.87	$ 700.63	$ 700.63	$ 700.63	$ 700.63
SMA	OpCon/xps User Interface	License		CCSU13350162-A			A			$ 5.49	$ 5.64	$ 5.79	$ 5.95	$ 6.11	$ 6.28	$ 6.45	$ 6.45	$ 6.45	$ 6.45
Sybase	EAServer Deploy Advanced - Active	License		CCSU13350163-A			A			$ 149.36	$ 153.84	$ 158.45	$ 163.20	$ 168.10	$ 173.14	$ 178.34	$ 178.34	$ 178.34	$ 178.34
Sybase	EAServer Deploy Advanced - Passive	License		CCSU13350164-A			A			$ 37.39	$ 38.51	$ 39.67	$ 40.86	$ 42.08	$ 43.35	$ 44.65	$ 44.65	$ 44.65	$ 44.65
Symantec	Backup Exec System Recovery Server	License		CCSU13350165-A			A			$ 0.97	$ 1.00	$ 1.03	$ 1.06	$ 1.09	$ 1.12	$ 1.16	$ 1.16	$ 1.16	$ 1.16
Symantec	EndPoint Protection	License		CCSU13350166-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	Ghost Solution Suite	License		CCSU13350167-A			A			$ 0.66	$ 0.68	$ 0.70	$ 0.72	$ 0.74	$ 0.76	$ 0.78	$ 0.78	$ 0.78	$ 0.78
Symantec	NetBackup Client Application and Database Pack, UNX, Tier 3	License		CCSU13350168-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Client Application and Database Pack, UNX, Tier 4	License		CCSU13350169-A			A			$ 175.15	$ 180.40	$ 185.81	$ 191.39	$ 197.13	$ 203.04	$ 209.13	$ 209.13	$ 209.13	$ 209.13
Symantec	NetBackup Client Application and Database Pack, WIN, Tier 2	License		CCSU13350170-A			A			$ 27.00	$ 27.81	$ 28.65	$ 29.50	$ 30.39	$ 31.30	$ 32.24	$ 32.24	$ 32.24	$ 32.24
Symantec	NetBackup Client Application and Database Pack, WIN, Tier 3	License		CCSU13350171-A			A			$ 34.97	$ 36.01	$ 37.09	$ 38.21	$ 39.35	$ 40.53	$ 41.75	$ 41.75	$ 41.75	$ 41.75
Symantec	NetBackup Client Application and Database Pack, WIN, Tier 4	License		CCSU13350172-A			A			$ 52.49	$ 54.06	$ 55.68	$ 57.36	$ 59.08	$ 60.85	$ 62.67	$ 62.67	$ 62.67	$ 62.67
Symantec	NetBackup Enterprise Client, UNX, Tier 4	License		CCSU13350173-A			A			$ 216.56	$ 223.06	$ 229.75	$ 236.64	$ 243.74	$ 251.06	$ 258.59	$ 258.59	$ 258.59	$ 258.59
Symantec	NetBackup Enterprise Client, WIN, Tier 1	License		CCSU13350174-A			A			$ 41.34	$ 42.58	$ 43.85	$ 45.17	$ 46.53	$ 47.92	$ 49.36	$ 49.36	$ 49.36	$ 49.36
Symantec	NetBackup Enterprise Client, WIN, Tier 2	License		CCSU13350175-A			A			$ 49.30	$ 50.78	$ 52.30	$ 53.87	$ 55.49	$ 57.15	$ 58.87	$ 58.87	$ 58.87	$ 58.87
Symantec	NetBackup Enterprise Client, WIN, Tier 3	License		CCSU13350176-A			A			$ 65.23	$ 67.19	$ 69.20	$ 71.28	$ 73.42	$ 75.62	$ 77.89	$ 77.89	$ 77.89	$ 77.89
Symantec	NetBackup Enterprise Server, WIN, Tier 2	License		CCSU13350177-A			A			$ 87.61	$ 90.24	$ 92.95	$ 95.74	$ 98.61	$ 101.57	$ 104.61	$ 104.61	$ 104.61	$ 104.61
Symantec	NetBackup Enterprise Server, WIN, Tier 3	License		CCSU13350178-A			A			$ 127.44	$ 131.26	$ 135.20	$ 139.25	$ 143.43	$ 147.73	$ 152.17	$ 152.17	$ 152.17	$ 152.17
Symantec	NetBackup Library Based Tape Drive Option, XPLAT	License		CCSU13350179-A			A			$ 47.79	$ 49.22	$ 50.70	$ 52.22	$ 53.79	$ 55.40	$ 57.06	$ 57.06	$ 57.06	$ 57.06
Symantec	NetBackup Media Server Encryption Option (MSEO) WIN, Tier 2	License		CCSU13350180-A			A			$ 95.74	$ 98.61	$ 101.57	$ 104.61	$ 104.61	$ 104.61	$ 104.61	$ 985.17	$ -	$ -
Symantec	NetBackup Platform Base, XPLAT (per Terabyte)	License		CCSU13350181-A			A			$ 199.12	$ 205.09	$ 211.25	$ 217.58	$ 224.11	$ 230.84	$ 237.76	$ 237.76	$ 237.76	$ 237.76
Symantec	NetBackup Shared Storage Option, XPLAT	License		CCSU13350182-A			A			$ 31.86	$ 32.82	$ 33.80	$ 34.81	$ 35.86	$ 36.93	$ 38.04	$ 38.04	$ 38.04	$ 38.04
Symantec	NetBackup Standard Client, XPLAT	License		CCSU13350183-A			A			$ 9.48	$ 9.76	$ 10.06	$ 10.36	$ 10.67	$ 10.99	$ 11.32	$ 11.32	$ 11.32	$ 11.32
Symantec	NetBackup Vault Additional Drive Option XPLAT	License		CCSU13350184-A			A			$ 31.86	$ 32.82	$ 33.80	$ 34.81	$ 35.86	$ 36.93	$ 38.04	$ 38.04	$ 38.04	$ 38.04
Symantec	NetBackup Vault Base Option, XPLAT (4 tape drives per icense)	License		CCSU13350185-A			A			$ 159.30	$ 164.08	$ 169.00	$ 174.07	$ 179.29	$ 184.67	$ 190.21	$ 190.21	$ 190.21	$ 190.21
Symantec	Ver tas NetBackup Enterprise Server License, Tier 3	License		CCSU13350186-A			A			$ 127.44	$ 131.26	$ 135.20	$ 139.25	$ 143.43	$ 147.73	$ 152.17	$ 152.17	$ 152.17	$ 152.17
Symantec	Ver tas NetBackup Windows Client, Tier 4	License		CCSU13350187-A			A			$ 52.49	$ 54.06	$ 55.68	$ 57.36	$ 59.08	$ 60.85	$ 62.67	$ 62.67	$ 62.67	$ 62.67
Tone Software Corp.	Dynastep	License		CCSU13350188-A			A			$ 1,471.15	$ 1,515.28	$ 1,560.74	$ 1,607.56	$ 1,655.79	$ 1,705.46	$ 1,756.63	$ 1,756.63	$ 1,756.63	$ 1,756.63
Unicon Group Ltd.	LOUIS II LCOM Host Module	License		CCSU13350189-A			A			$ 55.61	$ 57.28	$ 59.00	$ 60.77	$ 62.59	$ 64.47	$ 66.40	$ 66.40	$ 66.40	$ 66.40
Unicon Group Ltd.	LOUIS II Extract & Reporting Module	License		CCSU13350190-A			A			$ 893.44	$ 920.25	$ 947.86	$ 976.29	$ 1 005.58	$ 1 035.75	$ 1 066.82	$ 1 066.82	$ 1 066.82	$ 1 066.82
Unicon Group Ltd.	LOUIS II DERIVE Option	License		CCSU13350191-A			A			$ 62.44	$ 64.31	$ 66.24	$ 68.22	$ 70.27	$ 72.38	$ 74.55	$ 74.55	$ 74.55	$ 74.55
Unicon Group Ltd.	LOUIS II DMS Interface	License		CCSU13350192-A			A			$ 111.22	$ 114.56	$ 118.00	$ 121.54	$ 125.18	$ 128.94	$ 132.81	$ 132.81	$ 132.81	$ 132.81
Unicon Group Ltd.	LOUIS II RDMS Interface	License		CCSU13350193-A			A			$ 111.22	$ 114.56	$ 118.00	$ 121.54	$ 125.18	$ 128.94	$ 132.81	$ 132.81	$ 132.81	$ 132.81
Unicon Group Ltd.	LOUIS II RELATE Option	License		CCSU13350194-A			A			$ 89.12	$ 91.79	$ 94.55	$ 97.38	$ 100.31	$ 103.31	$ 106.41	$ 106.41	$ 106.41	$ 106.41
VanDyke Technologies	VShell Workgroup Server	License		CCSU13350195-A			A			$ 9.76	$ 10.05	$ 10.35	$ 10.66	$ 10.98	$ 11.31	$ 11.65	$ 11.65	$ 11.65	$ 11.65
Veeam	nWorks ESX Monitoring for SCOM	License		CCSU13350196-A			A			$ 12.89	$ 13.28	$ 13.68	$ 14.09	$ 14.51	$ 14.95	$ 15.39	$ 15.39	$ 15.39	$ 15.39
Veeam	nWorks Management Pack for VMWare	License		CCSU13350197-A			A			$ 154.71	$ 159.35	$ 164.13	$ 169.05	$ 174.13	$ 179.35	$ 184.73	$ 184.73	$ 184.73	$ 184.73
VMware, Inc.	VMware vSphere 4 Enterprise Plus for 1 Processor	License		CCSU13350198-A			A			$ 36.67	$ 37.77	$ 38.90	$ 40.07	$ 41.27	$ 42.51	$ 43.78	$ 43.78	$ 43.78	$ 43.78
VMware, Inc.	VMware vSphere 5 Enterprise Plus for 1 Processor	License		CCSU13350199-A			A			$ 73.33	$ 75.53	$ 77.80	$ 80.13	$ 82.54	$ 85.01	$ 87.56	$ 87.56	$ 87.56	$ 87.56
Western American Data	Rlist	License		CCSU13350200-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Winternals	Winternals Administrator's Pak	License		CCSU13350201-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
WinZip Computing	Winzip	License		CCSU13350202-A			A			$ 0.26	$ 0.27	$ 0.27	$ 0.28	$ 0.29	$ 0.30	$ 0.31	$ 0.31	$ 0.31	$ 0.31
XtremeSoft	AppMetrics	License		CCSU13350203-A			A			$ 1 375.00	$ 1 416.25	$ 1 458.74	$ 1 502.50	$ 1 547.57	$ 1 594.00	$ 1 641.82	$ 1 641.82	$ 1 641.82	$ 1 641.82
USPS	Correct Address	License		CCSU13350204-A			A			$ 998.15	$ 1,028.09	$ 1,058.94	$ 1,090.70	$ 1,123.42	$ 1,157.13	$ 1,191.84	$ 1,191.84	$ 1,191.84	$ 1,191.84
IBM	FileNet	License		CCSU13350205-A			A			$ 66.51	$ 15.07	$ 15.52	$ 15.99	$ 16.47	$ 16.96	$ 17.47	$ 17.47	$ 17.47	$ 17.47
Microsoft	SharePoint (w th SA)	License		CCSU13350206-A			A			$ 827.24	$ 852.06	$ 877.62	$ 903.95	$ 931.07	$ 959.00	$ 987.77	$ 987.77	$ 987.77	$ 987.77
IBM	WebSphere MQ (Procesor Value Unit)	License		CCSU13350207-A			A			$ 11.42	$ 2.59	$ 2.66	$ 2.74	$ 2.83	$ 2.91	$ 3.00	$ 3.00	$ 3.00	$ 3.00
Xerox	XeroxDocuShare	License		CCSU13350208-A			A			$ 52.08	$ 53.23	$ 54.41	$ 55.62	$ 56.88	$ 58.17	$ 59.50	$ 59.50	$ 59.50	$ 59.50
Hybrid Third Party Software																			
Vendor	**Product**																		
Computer Associates International, Inc.	CA 90's Services (freeware)	License		CCSI13350209-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	Vision Builder	License		CCSI13350210-A			A			$ 23 138.91	$ 23 833.08	$ 24 548.07	$ 25 284.51	$ 26 043.05	$ 26 824.34	$ 27 629.07	$ 28 457.94	$ 29 311.68	$ 30 191.03
Computer Associates International, Inc.	Easytrieve Plus	License		CCSI13350211-A			A			$ 33,157.62	$ 34,152.35	$ 35,176.92	$ 36,232.22	$ 37,319.19	$ 38,438.77	$ 39,591.93	$ 40,779.69	$ 42,003.08	$ 43,263.17
Computer Associates International, Inc.	Easytrieve Plus MVS	License		CCSI13350212-A			A			$ 18,620.96	$ 19,179.58	$ 19,754.97	$ 20,347.62	$ 20,958.05	$ 21,586.79	$ 22,234.39	$ 22,901.43	$ 23,588.47	$ 24,296.12

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	**Product Name**	**Unit**	**Qty per config**	**Provider Part Number**	**Version Major**	**Version Minor**	**Version Build**	**Manufacturer ID**	**Equipment Code**	**Price per unit \ Per Month**									
Description / Use *>*	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Computer Associates International, Inc.	Easytrieve Plus IMS	License		CCSI13350213-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	Easytrieve Plus IMS Option MVS	License		CCSI13350214-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	Easytrieve Plus DB2 OPT	License		CCSI13350215-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	Easytrieve Plus DB2 Option MVS	License		CCSI13350216-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	Endevor/MVS Automated Configuration Mgr MVS	License		CCSI13350217-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	Endevor/MVS External Secur ty Int. MVS	License		CCSI13350218-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	Endevor/MVS MVS	License		CCSI13350219-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	Endevor/MVS Extended Processor	License		CCSI13350220-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	CA-L brarian	License		CCSI13350221-A			A			$ 27,824.48	$ 28,659.22	$ 29,518.99	$ 30,404.56	$ 31,316.70	$ 32,256.20	$ 33,223.89	$ 34,220.60	$ 35,247.22	$ 36,304.64
Computer Associates International, Inc.	CA-META COBOL	License		CCSI13350222-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	Panvalet	License		CCSI13350223-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	Panvalet ISPF	License		CCSI13350224-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	SORT (INCL DART)	License		CCSI13350225-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	SRAM	License		CCSI13350226-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
dotJ Software Inc.	dotJ Custom Tag Library	License		CCSU13350227-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Formula Consultants, Inc.	Star 1100	License		CCSU13350228-A			A			$ 198.00	$ 203.94	$ 210.06	$ 216.36	$ 222.85	$ 229.54	$ 236.42	$ 236.42	$ 236.42	$ 236.42
Idea Integration	XGEN	License		CCSU13350229-A			A			$ 3,300.15	$ 3,399.16	$ 3,501.13	$ 3,606.17	$ 3,714.35	$ 3,825.78	$ 3,940.56	$ 3,940.56	$ 3,940.56	$ 3,940.56
Informatica Corporation	Change DataMove for DB2 Source	License		CCSI13350230-A			A			$ 16 892.13	$ 17 398.90	$ 17 920.86	$ 18 458.49	$ 19 012.24	$ 19 582.61	$ 20 170.09	$ 20 775.19	$ 21 398.45	$ 22 040.40
Informatica Corporation	DataMove for DB2 Source	License		CCSI13350231-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	Change DataMove	License		CCSI13350232-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	DataMove for IMS Source	License		CCSI13350233-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	Change DataMove for IMS Source	License		CCSI13350234-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	DataMove	License		CCSI13350235-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	Change DataMove DB2 Target	License		CCSI13350236-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	DataMove DB2 Target	License		CCSI13350237-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	Change DataMove/DataMove Target for UDB	License		CCSI13350238-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	SSA - Name 3	License		CCSU13350239-A			A			$ 5 347.22	$ 5 507.64	$ 5 672.87	$ 5 843.05	$ 6 018.35	$ 6 198.90	$ 6 384.86	$ 6 384.86	$ 6 384.86	$ 6 384.86
KMSYS Worldwide, Inc.	IQU Plus-1	License		CCSU13350240-A			A			$ 488.89	$ 503.56	$ 518.66	$ 534.22	$ 550.25	$ 566.76	$ 583.76	$ 583.76	$ 583.76	$ 583.76
KMSYS Worldwide, Inc.	IQU Reorg Composer	License		CCSU13350241-A			A			$ 346.30	$ 356.69	$ 367.39	$ 378.41	$ 389.76	$ 401.45	$ 413.50	$ 413.50	$ 413.50	$ 413.50
KMSYS Worldwide, Inc.	QPLXSS	License		CCSU13350242-A			A			$ 0.99	$ 1.02	$ 1.05	$ 1.09	$ 1.12	$ 1.15	$ 1.19	$ 1.19	$ 1.19	$ 1.19
KMSYS Worldwide Inc.	QPLXSV	License		CCSU13350243-A			A			$ 85.94	$ 88.52	$ 91.17	$ 93.91	$ 96.72	$ 99.63	$ 102.61	$ 102.61	$ 102.61	$ 102.61
KMSYS Worldwide, Inc.	QPLXV	License		CCSU13350244-A			A			$ 76.39	$ 78.68	$ 81.04	$ 83.47	$ 85.98	$ 88.56	$ 91.21	$ 91.21	$ 91.21	$ 91.21
Marble Computer Inc.	OS DCD III Data Correlation and Documentation System	License		CCSU13350245-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	SQL Server Enterprise	License		CCSU13350246-A			A			$ 105.78	$ 108.96	$ 112.23	$ 115.59	$ 119.06	$ 122.63	$ 126.31	$ 126.31	$ 126.31	$ 126.31
SAS Institute Inc.	Base SAS	License		CCSI13350247-A			A			$ 70 983.91	$ 73 113.42	$ 75 306.83	$ 77 566.03	$ 79 893.01	$ 82 289.80	$ 84 758.50	$ 87 301.25	$ 89 920.29	$ 92 617.90
SAS Institute, Inc.	SAS/ACCESS Interface for IMS	License		CCSI13350248-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SAS Institute, Inc.	SAS/ACCESS DB2	License		CCSI13350249-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SAS Institute, Inc.	SAS/AF	License		CCSI13350250-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SAS Institute, Inc.	SAS/FSP	License		CCSI13350251-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SAS Institute, Inc.	SAS/GRAPH	License		CCSI13350252-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SAS Institute, Inc.	SAS/SHARE	License		CCSI13350253-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SAS Institute, Inc.	SAS/STAT	License		CCSI13350254-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Schema Systems Limited	Q Ed tor Plus One	License		CCSU13350255-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SMA	OpCon/xps EXEC LSAM, Group 3	License		CCSU13350256-A			A			$ 296.54	$ 305.43	$ 314.60	$ 324.03	$ 333.76	$ 343.77	$ 354.08	$ 354.08	$ 354.08	$ 354.08
SMA	OpCon/xps EXEC LSAM, Group 8	License		CCSU13350257-A			A			$ 1 077.60	$ 1 109.93	$ 1 143.23	$ 1 177.52	$ 1 212.85	$ 1 249.23	$ 1 286.71	$ 1 286.71	$ 1 286.71	$ 1 286.71
SMA	OpCon/xps EXEC LSAM, Group 14	License		CCSU13350258-A			A			$ 2,783.45	$ 2,866.96	$ 2,952.96	$ 3,041.55	$ 3,132.80	$ 3,226.78	$ 3,323.59	$ 3,323.59	$ 3,323.59	$ 3,323.59
SMA	OpCon/xps Microsoft LSAM	License		CCSU13350259-A			A			$ 90.19	$ 92.89	$ 95.68	$ 98.55	$ 101.51	$ 104.55	$ 107.69	$ 107.69	$ 107.69	$ 107.69
SMA	OpCon/xps User Interface	License		CCSU13350260-A			A			$ 4.97	$ 5.12	$ 5.27	$ 5.43	$ 5.59	$ 5.76	$ 5.93	$ 5.93	$ 5.93	$ 5.93
Sybase	EAServer Deploy Advanced - Active	License		CCSU13350261-A			A			$ 149.36	$ 153.84	$ 158.45	$ 163.20	$ 168.10	$ 173.14	$ 178.34	$ 178.34	$ 178.34	$ 178.34
Sybase	EAServer Deploy Advanced - Passive	License		CCSU13350262-A			A			$ 37.39	$ 38.51	$ 39.67	$ 40.86	$ 42.08	$ 43.35	$ 44.65	$ 44.65	$ 44.65	$ 44.65
TRILOGexport, Inc.	TriTune Automation Component (APC)	License		CCSI13350263-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unicon Group Ltd.	LOUIS II Database Gateway	License		CCSU13350264-A			A			$ 893.44	$ 920.25	$ 947.86	$ 976.29	$ 1 005.58	$ 1 035.75	$ 1 066.82	$ 1 066.82	$ 1 066.82	$ 1 066.82
Unicon Group Ltd.	LOUIS II DMS Interface	License		CCSU13350265-A			A			$ 111.22	$ 114.56	$ 118.00	$ 121.54	$ 125.18	$ 128.94	$ 132.81	$ 132.81	$ 132.81	$ 132.81
Unicon Group Ltd.	LOUIS II Extract & Reporting Module	License		CCSU13350266-A			A			$ 893.44	$ 920.25	$ 947.86	$ 976.29	$ 1,005.58	$ 1,035.75	$ 1,066.82	$ 1,066.82	$ 1,066.82	$ 1,066.82
Unicon Group Ltd.	LOUIS II LCOM Host Module	License		CCSU13350267-A			A			$ 55.61	$ 57.28	$ 59.00	$ 60.77	$ 62.59	$ 64.47	$ 66.40	$ 66.40	$ 66.40	$ 66.40
Unicon Group Ltd.	LOUIS II MAPPER Interface	License		CCSU13350268-A			A			$ -	$ 111.22	$ 114.56	$ 118.00	$ 121.54	$ 125.18	$ 128.94	$ 132.81	$ 132.81	$ 132.81
Unicon Group Ltd.	LOUIS II RDMS Interface	License		CCSU13350269-A			A			$ 111.22	$ 111.22	$ 114.56	$ 118.00	$ 121.54	$ 125.18	$ 128.94	$ 132.81	$ 132.81	$ 132.81
Verisign	Secure Site Pro SSL	License		CCSU13350270-A			A			$ 92.13	$ 97.74	$ 100.67	$ 103.69	$ 106.80	$ 110.01	$ 113.31	$ 113.31	$ 113.31	$ 113.31
Western American Data	Rlist	License		CCSU13350271-A			A			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
WinZip	Self-Extractor 10-user license	License		CCSU13350272-A			A			$ 0.66	$ 0.66	$ 0.68	$ 0.70	$ 0.72	$ 0.74	$ 0.76	$ 0.78	$ 0.78	$ 0.78
Additional Services																			
Infrastructure (mainframe, mid-range and x86) Architects/Engineers		Per Hour		CCSZ13360001-A	N/A	N/A	A			$ 113.78	$ 117.19	$ 120.71	$ 124.33	$ 128.06	$ 131.90	$ 135.86	$ 139.93	$ 144.13	$ 148.45
Microsoft Product Specialists (e.g. Exchange, SharePoint)		Per Hour		CCSZ13360002-A	N/A	N/A	A			$ 112.18	$ 115.54	$ 119.01	$ 122.58	$ 126.25	$ 130.04	$ 133.94	$ 137.96	$ 142.10	$ 146.36
Basis and SAP Oracle support		Per Hour		CCSD13360003-A	N/A	N/A	A			N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Performance Specialists		Per Hour		CCSZ13360004-A	N/A	N/A	A			$ 112.18	$ 115.54	$ 119.01	$ 122.58	$ 126.25	$ 130.04	$ 133.94	$ 137.96	$ 142.10	$ 146.36
Mainframe Systems Programmers		Per Hour		CCSZ13360005-A	N/A	N/A	A			$ 238.87	$ 246.04	$ 253.42	$ 261.02	$ 268.85	$ 276.92	$ 285.22	$ 293.78	$ 302.59	$ 311.67
Batch Administrators		Per Hour		CCSZ13360006-A	N/A	N/A	A			$ 403.94	$ 416.05	$ 428.54	$ 441.39	$ 454.63	$ 468.27	$ 482.32	$ 496.79	$ 511.70	$ 527.05
3rd Party Software Product Specialists		Per Hour		CCSZ13360007-A	N/A	N/A	A			$ 112.18	$ 115.54	$ 119.01	$ 122.58	$ 126.25	$ 130.04	$ 133.94	$ 137.96	$ 142.10	$ 146.36
System Administrator (Windows, AIX, Linux)		Per Hour		CCSZ13360008-A	N/A	N/A	A			$ 186.26	$ 191.85	$ 197.60	$ 203.53	$ 209.64	$ 215.92	$ 222.40	$ 229.07	$ 235.95	$ 243.02
System Administrator (Middleware support)		Per Hour		CCSZ13360009-A	N/A	N/A	A			$ 168.77	$ 173.83	$ 179.05	$ 184.42	$ 189.95	$ 195.65	$ 201.52	$ 207.56	$ 213.79	$ 220.20
Storage Administrator		Per Hour		CCSZ13360010-A	N/A	N/A	A			$ 203.75	$ 209.86	$ 216.16	$ 222.64	$ 229.32	$ 236.20	$ 243.29	$ 250.59	$ 258.10	$ 265.85
Data Backup Administrator		Per Hour		CCSZ13360011-A	N/A	N/A	A			$ 258.66	$ 266.42	$ 274.41	$ 282.65	$ 291.13	$ 299.86	$ 308.86	$ 318.12	$ 327.66	$ 337.49

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	Product Name	Unit	Qty per config	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Database Administrator		Per Hour		CCSZ13360012-A	N/A	N/A	A			$ 181.99	$ 187.45	$ 193.07	$ 198.87	$ 204.83	$ 210.98	$ 217.31	$ 223.83	$ 230.54	$ 237.46
Database Architects		Per Hour		CCSZ13360013-A	N/A	N/A	A			$ 151.10	$ 155.63	$ 160.30	$ 165.11	$ 170.06	$ 175.16	$ 180.42	$ 185.83	$ 191.40	$ 197.14
Database Analysts		Per Hour		CCSZ13360014-A	N/A	N/A	A			$ 87.73	$ 90.36	$ 93.08	$ 95.87	$ 98.74	$ 101.71	$ 104.76	$ 107.90	$ 111.14	$ 114.47
Project Management Support		Per Hour		CCSZ13360015-A	N/A	N/A	A			$ 245.17	$ 252.53	$ 260.10	$ 267.91	$ 275.94	$ 284.22	$ 292.75	$ 301.53	$ 310.58	$ 319.90
Network Administrator		Per Hour		CCSZ13360016-A	N/A	N/A	A			$ 190.40	$ 196.11	$ 202.00	$ 208.06	$ 214.30	$ 220.73	$ 227.35	$ 234.17	$ 241.19	$ 248.43
Facilities Administrator		Per Hour		CCSZ13360017-A	N/A	N/A	A			$ 148.98	$ 153.45	$ 158.05	$ 162.79	$ 167.67	$ 172.70	$ 177.88	$ 183.22	$ 188.72	$ 194.38
Security Administrator		Per Hour		CCSZ13360018-A	N/A	N/A	A			$ 168.77	$ 173.83	$ 179.05	$ 184.42	$ 189.95	$ 195.65	$ 201.52	$ 207.56	$ 213.79	$ 220.20
Security Architects		Per Hour		CCSZ13360019-A	N/A	N/A	A			$ 151.10	$ 155.63	$ 160.30	$ 165.11	$ 170.06	$ 175.16	$ 180.42	$ 185.83	$ 191.40	$ 197.14
Security Analysts		Per Hour		CCSZ13360020-A	N/A	N/A	A			$ 87.73	$ 90.36	$ 93.08	$ 95.87	$ 98.74	$ 101.71	$ 104.76	$ 107.90	$ 111.14	$ 114.47
Asset Management Administrator		Per Hour		CCSZ13360021-A	N/A	N/A	A			$ 222.69	$ 229.37	$ 236.25	$ 243.34	$ 250.64	$ 258.16	$ 265.90	$ 273.88	$ 282.10	$ 290.56
Quality Assurance Support		Per Hour		CCSZ13360022-A	N/A	N/A	A			$ 124.89	$ 128.63	$ 132.49	$ 136.47	$ 140.56	$ 144.78	$ 149.12	$ 153.60	$ 158.20	$ 162.95
Remedy Support Specialist		Per Hour		CCSZ13360023-A	N/A	N/A	A			$ 136.21	$ 140.30	$ 144.51	$ 148.84	$ 153.31	$ 157.91	$ 162.65	$ 167.52	$ 172.55	$ 177.73
IT Service Continuity Specialist		Per Hour		CCSZ13360024-A	N/A	N/A	A			$ 399.87	$ 411.86	$ 424.22	$ 436.95	$ 450.06	$ 463.56	$ 477.46	$ 491.79	$ 506.54	$ 521.74
Infrastructure (mainframe, mid-range and x86) Architects/Engineers - Junior		Per Hour		CCSZ13360025-A	N/A	N/A	A			$ 113.78	$ 117.19	$ 120.71	$ 124.33	$ 128.06	$ 131.90	$ 135.86	$ 139.93	$ 144.13	$ 148.45
Microsoft Product Specialists (e.g. Exchange, SharePoint) - Junior		Per Hour		CCSZ13360026-A	N/A	N/A	A			$ 89.74	$ 92.43	$ 95.21	$ 98.06	$ 101.00	$ 104.03	$ 107.15	$ 110.37	$ 113.68	$ 117.09
Basis and SAP Oracle support - Junior		Per Hour		CCSD13360027-A	N/A	N/A	A			N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Performance Specialists - Junior		Per Hour		CCSZ13360028-A	N/A	N/A	A			$ 89.74	$ 92.43	$ 95.21	$ 98.06	$ 101.00	$ 104.03	$ 107.15	$ 110.37	$ 113.68	$ 117.09
Unisys Mainframe Systems Programmers - Junior		Per Hour		CCSU13360029-A	N/A	N/A	A			$ 149.13	$ 153.60	$ 158.21	$ 162.96	$ 167.85	$ 172.88	$ 178.07	$ 183.41	$ 188.91	$ 194.58
Batch Administrators - Junior		Per Hour		CCSZ13360030-A	N/A	N/A	A			$ 153.84	$ 158.46	$ 163.21	$ 168.11	$ 173.15	$ 178.34	$ 183.69	$ 189.20	$ 194.88	$ 200.73
Unisys Mainframe Batch Administrator - Senior		Per Hour		CCSU13360031-A	N/A	N/A	A			$ 62.50	$ 64.37	$ 66.30	$ 68.29	$ 70.34	$ 72.45	$ 74.63	$ 76.86	$ 79.17	$ 81.55
Unisys Mainframe Batch Administrator - Junior		Per Hour		CCSU13360032-A	N/A	N/A	A			$ 62.50	$ 64.37	$ 66.30	$ 68.29	$ 70.34	$ 72.45	$ 74.63	$ 76.86	$ 79.17	$ 81.55
3rd Party Software Product Specialists - Junior		Per Hour		CCSZ13360033-A	N/A	N/A	A			$ 112.18	$ 115.54	$ 119.01	$ 122.58	$ 126.25	$ 130.04	$ 133.94	$ 137.96	$ 142.10	$ 146.36
System Administrator (Windows, AIX, Linux) - Junior		Per Hour		CCSZ13360034-A	N/A	N/A	A			$ 146.52	$ 150.92	$ 155.44	$ 160.11	$ 164.91	$ 169.86	$ 174.95	$ 180.20	$ 185.61	$ 191.18
System Administrator (Middleware support) - Junior		Per Hour		CCSZ13360035-A	N/A	N/A	A			$ 80.13	$ 82.53	$ 85.00	$ 87.55	$ 90.18	$ 92.89	$ 95.67	$ 98.54	$ 101.50	$ 104.55
Data Backup Administrator - Junior		Per Hour		CCSZ13360036-A	N/A	N/A	A			$ 239.69	$ 246.88	$ 254.28	$ 261.91	$ 269.77	$ 277.86	$ 286.20	$ 294.79	$ 303.63	$ 312.74
Database Administrator - Junior		Per Hour		CCSZ13360037-A	N/A	N/A	A			$ 138.44	$ 142.59	$ 146.87	$ 151.28	$ 155.81	$ 160.49	$ 165.30	$ 170.26	$ 175.37	$ 180.63
Database Architects - Junior		Per Hour		CCSZ13360038-A	N/A	N/A	A			$ 115.35	$ 118.81	$ 122.38	$ 126.05	$ 129.83	$ 133.72	$ 137.74	$ 141.87	$ 146.12	$ 150.51
Database Analysts - Junior		Per Hour		CCSZ13360039-A	N/A	N/A	A			$ 81.23	$ 83.67	$ 86.18	$ 88.77	$ 91.43	$ 94.17	$ 97.00	$ 99.91	$ 102.90	$ 105.99
Project Management Support - Junior		Per Hour		CCSZ13360040-A	N/A	N/A	A			$ 190.25	$ 195.95	$ 201.83	$ 207.89	$ 214.12	$ 220.55	$ 227.17	$ 233.98	$ 241.00	$ 248.23
Facilities Administrator - Junior		Per Hour		CCSZ13360041-A	N/A	N/A	A			$ 125.04	$ 128.79	$ 132.66	$ 136.64	$ 140.74	$ 144.96	$ 149.31	$ 153.79	$ 158.40	$ 163.15
Network Administrator - Junior		Per Hour		CCSZ13360042-A	N/A	N/A	A			$ 148.82	$ 153.29	$ 157.89	$ 162.62	$ 167.50	$ 172.53	$ 177.70	$ 183.03	$ 188.52	$ 194.18
Security Administrator - Junior		Per Hour		CCSZ13360043-A	N/A	N/A	A			$ 146.52	$ 150.92	$ 155.44	$ 160.11	$ 164.91	$ 169.86	$ 174.95	$ 180.20	$ 185.61	$ 191.18
Security Architects - Junior		Per Hour		CCSZ13360044-A	N/A	N/A	A			$ 304.87	$ 311.54	$ 318.37	$ 325.36	$ 332.51	$ 339.84	$ 347.35	$ 355.03	$ 362.90	$ 370.96
Security Analysts - Junior		Per Hour		CCSZ13360045-A	N/A	N/A	A			$ 87.73	$ 90.36	$ 93.08	$ 95.87	$ 98.74	$ 101.71	$ 104.76	$ 107.90	$ 111.14	$ 114.47
Smart Hands and Feet Support		Per Hour		CCSU13360046-A	N/A	N/A	A			$ 48.08	$ 49.52	$ 51.00	$ 52.53	$ 54.11	$ 55.73	$ 57.40	$ 59.13	$ 60.90	$ 62.73
Unisys Mainframe User Account Administrator		Per Hour		CCSU13360047-A	N/A	N/A	A			$ 89.74	$ 92.43	$ 95.21	$ 98.06	$ 101.00	$ 104.03	$ 107.15	$ 110.37	$ 113.68	$ 117.09
Messaging Architect		Per Hour		CCSU13360048-A	N/A	N/A	A			$ 113.78	$ 117.19	$ 120.71	$ 124.33	$ 128.06	$ 131.90	$ 135.86	$ 139.93	$ 144.13	$ 148.45
Senior Messaging Consultant		Per Hour		CCSU13360049-A	N/A	N/A	A			$ 112.18	$ 115.54	$ 119.01	$ 122.58	$ 126.25	$ 130.04	$ 133.94	$ 137.96	$ 142.10	$ 146.36
Messaging Consultant		Per Hour		CCSU13360050-A	N/A	N/A	A			$ 89.74	$ 92.43	$ 95.21	$ 98.06	$ 101.00	$ 104.03	$ 107.15	$ 110.37	$ 113.68	$ 117.09
Senior Active Directory Consultant		Per Hour		CCSU13360051-A	N/A	N/A	A			$ 89.74	$ 92.43	$ 95.21	$ 98.06	$ 101.00	$ 104.03	$ 107.15	$ 110.37	$ 113.68	$ 117.09
Active Directory Consultant		Per Hour		CCSU13360052-A	N/A	N/A	A			$ 89.74	$ 92.43	$ 95.21	$ 98.06	$ 101.00	$ 104.03	$ 107.15	$ 110.37	$ 113.68	$ 117.09
Application Support Consultant		Per Hour		CCSU13360053-A	N/A	N/A	A			$ 169.87	$ 174.96	$ 180.21	$ 185.62	$ 191.18	$ 196.92	$ 202.83	$ 208.91	$ 215.18	$ 221.64
Technical Writer		Per Hour		CCSU13360054-A	N/A	N/A	A			$ 80.13	$ 82.53	$ 85.00	$ 87.55	$ 90.18	$ 92.89	$ 95.67	$ 98.54	$ 101.50	$ 104.55
Automation Engineer - Senior		Per Hour		CCSU13360055-A	N/A	N/A	A			$ 112.18	$ 115.54	$ 119.01	$ 122.58	$ 126.25	$ 130.04	$ 133.94	$ 137.96	$ 142.10	$ 146.36
Automation Engineer - Junior		Per Hour		CCSU13360056-A	N/A	N/A	A			$ 89.74	$ 92.43	$ 95.21	$ 98.06	$ 101.00	$ 104.03	$ 107.15	$ 110.37	$ 113.68	$ 117.09
Senior Technology Consultant 1 - 2200 Database Support		Per Hour		CCSU13360057-A	N/A	N/A	A			$ 122.91	$ 126.60	$ 130.40	$ 134.31	$ 138.34	$ 142.49	$ 146.76	$ 151.17	$ 155.70	$ 160.37
Senior Technology Consultant 2 - Windows 2000 and Middleware		Per Hour		CCSU13360058-A	N/A	N/A	A			$ 168.41	$ 173.47	$ 178.67	$ 184.03	$ 189.55	$ 195.24	$ 201.09	$ 207.13	$ 213.34	$ 219.74
Senior Technology Consultant 3 - 2200 Mainframe Applications, Performance, and Security		Per Hour		CCSU13360059-A	N/A	N/A	A			$ 164.58	$ 169.51	$ 174.60	$ 179.84	$ 185.23	$ 190.79	$ 196.51	$ 202.41	$ 208.48	$ 214.74
Senior Technology Consultant 4 - Middleware Products and Applications		Per Hour		CCSU13360060-A	N/A	N/A	A			$ 193.74	$ 199.55	$ 205.54	$ 211.71	$ 218.06	$ 224.60	$ 231.34	$ 238.28	$ 245.43	$ 252.79
Senior Technology Consultant 5 - 2200 Database Design and Maintenance		Per Hour		CCSU13360061-A	N/A	N/A	A			$ 222.10	$ 228.76	$ 235.62	$ 242.69	$ 249.97	$ 257.47	$ 265.20	$ 273.15	$ 281.35	$ 289.79
Senior Technology Consultant 6 – Data Warehouse Systems and Oracle Database Servers		Per Hour		CCSU13360062-A	N/A	N/A	A			$ 161.26	$ 166.10	$ 171.08	$ 176.21	$ 181.50	$ 186.94	$ 192.55	$ 198.33	$ 204.28	$ 210.40
SPC Principal Engineer		Per Hour		CCSU13360063-A	N/A	N/A	A			$ 258.32	$ 266.07	$ 274.06	$ 282.28	$ 290.75	$ 299.47	$ 308.45	$ 317.71	$ 327.24	$ 337.05
SPC Consulting Engineer		Per Hour		CCSU13360064-A	N/A	N/A	A			$ 139.26	$ 143.44	$ 147.74	$ 152.17	$ 156.74	$ 161.44	$ 166.28	$ 171.27	$ 176.41	$ 181.70
Consultant 1		Per Hour		CCSU13360065-A	N/A	N/A	A			$ 340.37	$ 350.58	$ 361.10	$ 371.93	$ 383.09	$ 394.58	$ 406.42	$ 418.61	$ 431.17	$ 444.11
Consultant 2		Per Hour		CCSU13360066-A	N/A	N/A	A			$ 311.53	$ 320.87	$ 330.50	$ 340.41	$ 350.63	$ 361.14	$ 371.98	$ 383.14	$ 394.63	$ 406.47
Consultant 3		Per Hour		CCSU13360067-A	N/A	N/A	A			$ 259.61	$ 267.39	$ 275.42	$ 283.68	$ 292.19	$ 300.95	$ 309.98	$ 319.28	$ 328.86	$ 338.73
Consultant 4		Per Hour		CCSU13360068-A	N/A	N/A	A			$ 213.45	$ 219.86	$ 226.45	$ 233.25	$ 240.24	$ 247.45	$ 254.87	$ 262.52	$ 270.40	$ 278.51
Integration Architect		Per Hour		CCSU13360069-A	N/A	N/A	A			$ 193.74	$ 199.55	$ 205.54	$ 211.71	$ 218.06	$ 224.60	$ 231.34	$ 238.28	$ 245.43	$ 252.79
Program Analyst		Per Hour		CCSU13360070-A	N/A	N/A	A			$ 93.75	$ 96.56	$ 99.46	$ 102.44	$ 105.51	$ 108.68	$ 111.94	$ 115.30	$ 118.76	$ 122.32
Programmer		Per Hour		CCSU13360071-A	N/A	N/A	A			$ 93.75	$ 96.56	$ 99.46	$ 102.44	$ 105.51	$ 108.68	$ 111.94	$ 115.30	$ 118.76	$ 122.32
Senior Programmer		Per Hour		CCSU13360072-A	N/A	N/A	A			$ 340.37	$ 350.58	$ 361.10	$ 371.93	$ 383.09	$ 394.58	$ 406.42	$ 418.61	$ 431.17	$ 444.11
Senior Systems Analyst		Per Hour		CCSU13360073-A	N/A	N/A	A			$ 122.91	$ 126.60	$ 130.40	$ 134.31	$ 138.34	$ 142.49	$ 146.76	$ 151.17	$ 155.70	$ 160.37
Senior Systems Architect		Per Hour		CCSU13360074-A	N/A	N/A	A			$ 258.32	$ 266.07	$ 274.06	$ 282.28	$ 290.75	$ 299.47	$ 308.45	$ 317.71	$ 327.24	$ 337.05
Sr. Engagement Manager		Per Hour		CCSU13360075-A	N/A	N/A	A			$ 361.32	$ 372.16	$ 383.32	$ 394.82	$ 406.66	$ 418.86	$ 431.43	$ 444.37	$ 457.70	$ 471.44
Systems Analyst		Per Hour		CCSU13360076-A	N/A	N/A	A			$ 112.50	$ 115.87	$ 119.35	$ 122.93	$ 126.61	$ 130.41	$ 134.33	$ 138.36	$ 142.51	$ 146.78
Systems Architect		Per Hour		CCSU13360077-A	N/A	N/A	A			$ 147.91	$ 152.35	$ 156.92	$ 161.63	$ 166.48	$ 171.47	$ 176.61	$ 181.91	$ 187.37	$ 192.99
Technology Architect		Per Hour		CCSU13360078-A	N/A	N/A	A			$ 147.91	$ 152.35	$ 156.92	$ 161.63	$ 166.48	$ 171.47	$ 176.61	$ 181.91	$ 187.37	$ 192.99
Solutions Architect		Per Hour		CCSI13360079-A	N/A	N/A	A			$ 361.32	$ 372.16	$ 383.32	$ 394.82	$ 406.66	$ 418.86	$ 431.43	$ 444.37	$ 457.70	$ 471.44
System Administrator (AIX, Linux) - Junior		Per Hour		CCSI13360080-A	N/A	N/A	A			$ 168.77	$ 173.83	$ 179.05	$ 184.42	$ 189.95	$ 195.65	$ 201.52	$ 207.56	$ 213.79	$ 220.20
Storage Administrator - Junior		Per Hour		CCSI13360081-A	N/A	N/A	A			$ 181.81	$ 187.26	$ 192.88	$ 198.67	$ 204.63	$ 210.77	$ 217.09	$ 223.60	$ 230.31	$ 237.22
Solutions Architect - Junior		Per Hour		CCSI13360082-A	N/A	N/A	A			$ 294.58	$ 303.41	$ 312.52	$ 321.89	$ 331.55	$ 341.49	$ 351.74	$ 362.29	$ 373.16	$ 384.36
Asset Management Administrator - Junior		Per Hour		CCSI13360083-A	N/A	N/A	A			$ 125.04	$ 128.79	$ 132.66	$ 136.64	$ 140.74	$ 144.96	$ 149.31	$ 153.79	$ 158.40	$ 163.15
Quality Assurance Support - Junior		Per Hour		CCSI13360084-A	N/A	N/A	A			$ 107.40	$ 110.62	$ 113.94	$ 117.36	$ 120.88	$ 124.50	$ 128.24	$ 132.09	$ 136.05	$ 140.13

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	Product Name	Unit	Qty per config	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Remedy Support Specialist - Junior		Per Hour		CCSI13360085-A	N/A	N/A	A			$ 107.40	$ 110.62	$ 113.94	$ 117.36	$ 120.88	$ 124.50	$ 128.24	$ 132.09	$ 136.05	$ 140.13
IT Service Continuity Specialist - Junior		Per Hour		CCSI13360086-A	N/A	N/A	A			$ 171.07	$ 176.20	$ 181.49	$ 186.93	$ 192.54	$ 198.32	$ 204.27	$ 210.39	$ 216.71	$ 223.21
Mainframe System Programmer (IBM) - Junior		Per Hour		CCSI13360087-A	N/A	N/A	A			$ 146.52	$ 150.92	$ 155.44	$ 160.11	$ 164.91	$ 169.86	$ 174.95	$ 180.20	$ 185.61	$ 191.18
Project Manager - ERP		Per Hour		CCSD13360088-A	N/A	N/A	A			$ 528.86	$ 544.73	$ 561.07	$ 577.90	$ 595.24	$ 613.10	$ 631.49	$ 650.44	$ 669.95	$ 690.05
Functional Team Lead - ERP		Per Hour		CCSD13360089-A	N/A	N/A	A			$ 482.20	$ 492.74	$ 503.54	$ 514.59	$ 525.92	$ 537.51	$ 549.38	$ 561.53	$ 573.98	$ 586.73
Senior Functional Specialist ERP		Per Hour		CCSD13360090-A	N/A	N/A	A			$ 412.20	$ 421.22	$ 430.45	$ 439.90	$ 449.57	$ 459.48	$ 469.63	$ 480.02	$ 490.66	$ 501.56
Junior Functional Specialist - ERP		Per Hour		CCSD13360091-A	N/A	N/A	A			$ 342.21	$ 349.69	$ 357.35	$ 365.20	$ 373.23	$ 381.46	$ 389.88	$ 398.51	$ 407.34	$ 416.39
Testing / Documentation Specialist - ERP		Per Hour		CCSD13360092-A	N/A	N/A	A			$ 295.54	$ 302.00	$ 308.62	$ 315.40	$ 322.34	$ 329.44	$ 336.72	$ 344.17	$ 351.79	$ 359.61
Trainer		Per Hour		CCSD13360093-A	N/A	N/A	A			$ 295.54	$ 302.00	$ 308.62	$ 315.40	$ 322.34	$ 329.44	$ 336.72	$ 344.17	$ 351.79	$ 359.61
Technical Team Lead		Per Hour		CCSD13360094-A	N/A	N/A	A			$ 482.20	$ 492.74	$ 503.54	$ 514.59	$ 525.92	$ 537.51	$ 549.38	$ 561.53	$ 573.98	$ 586.73
Senior Developer		Per Hour		CCSD13360095-A	N/A	N/A	A			$ 412.20	$ 421.22	$ 430.45	$ 439.90	$ 449.57	$ 459.48	$ 469.63	$ 480.02	$ 490.66	$ 501.56
Junior Developer		Per Hour		CCSD13360096-A	N/A	N/A	A			$ 139.99	$ 143.05	$ 146.19	$ 149.40	$ 152.69	$ 156.05	$ 159.50	$ 163.03	$ 166.64	$ 170.34
Database Administrator Team Lead		Per Hour		CCSD13360097-A	N/A	N/A	A			$ 528.86	$ 540.43	$ 552.27	$ 564.39	$ 576.81	$ 589.52	$ 602.54	$ 615.88	$ 629.53	$ 643.51
Senior System Administration Specialist		Per Hour		CCSD13360098-A	N/A	N/A	A			$ 482.20	$ 492.74	$ 503.54	$ 514.59	$ 525.92	$ 537.51	$ 549.38	$ 561.53	$ 573.98	$ 586.73
Junior System Administration Specialist		Per Hour		CCSD13360099-A	N/A	N/A	A			$ 412.20	$ 421.22	$ 430.45	$ 439.90	$ 449.57	$ 459.48	$ 469.63	$ 480.02	$ 490.66	$ 501.56
Senior Security Specialist		Per Hour		CCSD13360100-A	N/A	N/A	A			$ 412.20	$ 421.22	$ 430.45	$ 439.90	$ 449.57	$ 459.48	$ 469.63	$ 480.02	$ 490.66	$ 501.56
Junior Security Specialist		Per Hour		CCSD13360101-A	N/A	N/A	A			$ 304.87	$ 311.54	$ 318.37	$ 325.36	$ 332.51	$ 339.84	$ 347.35	$ 355.03	$ 362.90	$ 370.96
Program Manager - Onsite		Per Hour		CCSD13360102-A	N/A	N/A	A			$ 273.77	$ 281.98	$ 290.44	$ 299.15	$ 308.13	$ 317.37	$ 326.89	$ 336.70	$ 346.80	$ 357.20
Senior Functional Analyst - Onsite		Per Hour		CCSD13360103-A	N/A	N/A	A			$ 209.99	$ 216.29	$ 222.78	$ 229.46	$ 236.35	$ 243.44	$ 250.74	$ 258.26	$ 266.01	$ 273.99
Junior Functional Analyst - Onsite		Per Hour		CCSD13360104-A	N/A	N/A	A			$ 209.99	$ 216.29	$ 222.78	$ 229.46	$ 236.35	$ 243.44	$ 250.74	$ 258.26	$ 266.01	$ 273.99
Testing / Documentation Specialist - Onsite		Per Hour		CCSD13360105-A	N/A	N/A	A			$ 180.44	$ 185.85	$ 191.42	$ 197.17	$ 203.08	$ 209.17	$ 215.45	$ 221.91	$ 228.57	$ 235.43
Architect - Onsite		Per Hour		CCSD13360106-A	N/A	N/A	A			$ 209.99	$ 216.29	$ 222.78	$ 229.46	$ 236.35	$ 243.44	$ 250.74	$ 258.26	$ 266.01	$ 273.99
Senior Developer - Onsite		Per Hour		CCSD13360107-A	N/A	N/A	A			$ 209.99	$ 216.29	$ 222.78	$ 229.46	$ 236.35	$ 243.44	$ 250.74	$ 258.26	$ 266.01	$ 273.99
Junior Developer - Onsite		Per Hour		CCSD13360108-A	N/A	N/A	A			$ 168.51	$ 173.33	$ 178.30	$ 183.41	$ 188.67	$ 194.08	$ 199.65	$ 205.38	$ 211.28	$ 217.36
Automated Tester - Onsite		Per Hour		CCSD13360109-A	N/A	N/A	A			$ 180.44	$ 185.85	$ 191.42	$ 197.17	$ 203.08	$ 209.17	$ 215.45	$ 221.91	$ 228.57	$ 235.43
Database Administrator Team Lead - Onsite		Per Hour		CCSD13360110-A	N/A	N/A	A			$ 273.77	$ 281.98	$ 290.44	$ 299.15	$ 308.13	$ 317.37	$ 326.89	$ 336.70	$ 346.80	$ 357.20
Senior Database Adminstrator Specialist - Onsite		Per Hour		CCSD13360111-A	N/A	N/A	A			$ 209.99	$ 216.29	$ 222.78	$ 229.46	$ 236.35	$ 243.44	$ 250.74	$ 258.26	$ 266.01	$ 273.99
Junior Database Administrator Specialist - Onsite		Per Hour		CCSD13360112-A	N/A	N/A	A			$ 180.44	$ 185.85	$ 191.42	$ 197.17	$ 203.08	$ 209.17	$ 215.45	$ 221.91	$ 228.57	$ 235.43
Security Specialist - Onsite		Per Hour		CCSD13360113-A	N/A	N/A	A			$ 139.99	$ 144.19	$ 148.52	$ 152.97	$ 157.56	$ 162.29	$ 167.16	$ 172.17	$ 177.34	$ 182.66
Configuration Analyst - Onsite		Per Hour		CCSD13360114-A	N/A	N/A	A			$ 139.99	$ 143.05	$ 146.19	$ 149.40	$ 152.69	$ 156.05	$ 159.50	$ 163.03	$ 166.64	$ 170.34
Additional Technical Services																			
Database Management Service	Database Management Service - Database Support Resources - Platinum (Up to 500 hours per month)	Per Request		CCSD13370001-A	N/A	N/A	A			$ 122,906.92	$ 131,873.96	$ 141,501.55	$ 151,838.67	$ 162,937.94	$ 174,855.94	$ 187,653.42	$ 201,395.68	$ 216,152.90	$ 232,000.48
Database Management Service	Database Management Service - Database Support Resources - Gold (Up to 375 hours per month)	Per Request		CCSD13370002-A	N/A	N/A	A			$ 90,235.46	$ 96,818.86	$ 103,887.21	$ 111,476.49	$ 119,625.33	$ 128,375.24	$ 137,770.86	$ 147,860.12	$ 158,694.53	$ 170,329.46
Database Management Service	Database Management Service - Database Support Resources - Silver (Up to 250 hours per month)	Per Request		CCSD13370003-A	N/A	N/A	A			$ 64,176.08	$ 68,858.24	$ 73,885.30	$ 79,282.85	$ 85,078.36	$ 91,301.36	$ 97,983.59	$ 105,159.14	$ 112,864.65	$ 121,139.49
Database Management Service	Database Management Service - Database Support Resources - Bronze (Up to 160 hours per month)	Per Request		CCSD13370004-A	N/A	N/A	A			$ 34,227.24	$ 36,724.39	$ 39,405.50	$ 42,284.19	$ 45,375.12	$ 48,694.06	$ 52,257.91	$ 56,084.87	$ 60,194.48	$ 64,607.73
Database Management Service	Database Management Service - Database Support Resources - Basic (Up to 80 hours per month)	Per Request		CCSD13370005-A	N/A	N/A	A			$ 15,557.84	$ 16,692.91	$ 17,911.59	$ 19,220.08	$ 20,625.06	$ 22,133.66	$ 23,753.60	$ 25,493.12	$ 27,361.13	$ 29,367.15
Database Management Service	Database Software - Microsoft SQL 2012 Enterprise - Physical Server using Windows pConfig-3	Per Server Instance		CCSU13370006-A	N/A	N/A	A			$ 8,042.29	$ 8,283.56	$ 8,532.07	$ 8,788.03	$ 9,051.67	$ 9,323.22	$ 9,602.92	$ 9,891.01	$ 10,187.74	$ 10,493.37
Database Management Service	Database Software - Microsoft SQL 2012 Standad - Physical Server using Windows pConfig-3	Per Server Instance		CCSU13370007-A	N/A	N/A	A			$ 1,906.46	$ 1,963.65	$ 2,022.56	$ 2,083.24	$ 2,145.74	$ 2,210.11	$ 2,276.41	$ 2,344.70	$ 2,415.04	$ 2,487.50
Database Management Service	Database Software - Microsoft SQL 2012 Enterprise - Virtual Server using Windows vConfig-3	Per Server Instance		CCSU13370008-A	N/A	N/A	A			$ 2,437.06	$ 2,510.17	$ 2,585.48	$ 2,663.04	$ 2,742.93	$ 2,825.22	$ 2,909.98	$ 2,997.27	$ 3,087.19	$ 3,179.81
Database Management Service	Database Software - Microsoft SQL 2012 Standard - Virtual Server using Windows vConfig-3	Per Server Instance		CCSU13370009-A	N/A	N/A	A			$ 635.49	$ 654.55	$ 674.19	$ 694.41	$ 715.25	$ 736.70	$ 758.80	$ 781.57	$ 805.01	$ 829.17
Database Management Service	Database Software - Oracle 11g Enterprise - Physical Server using Windows pConfig-3	Per Server Instance		CCSU13370010-A	N/A	N/A	A			$ 311,218.38	$ 320,554.93	$ 330,171.58	$ 340,076.72	$ 350,279.02	$ 360,787.39	$ 371,611.02	$ 382,759.35	$ 394,242.13	$ 406,069.39
Database Management Service	Database Software - Oracle 11g Real Application Server - Physical Server using Windows pConfig-3	Per Server Instance		CCSU13370011-A	N/A	N/A	A			$ 150,695.21	$ 155,216.07	$ 159,872.55	$ 164,668.73	$ 169,608.79	$ 174,697.05	$ 179,937.97	$ 185,336.11	$ 190,896.19	$ 196,623.07
Database Management Service	Database Software - Oracle 11g Standard - Physical Server using Windows pConfig-3	Per Server Instance		CCSU13370012-A	N/A	N/A	A			$ 38,219.80	$ 39,366.39	$ 40,547.39	$ 41,763.81	$ 43,016.72	$ 44,307.22	$ 45,636.44	$ 47,005.53	$ 48,415.70	$ 49,868.17
Database Management Service	Database Software - Oracle 11g Enterprise - Physical Server using Windows pConfig-3 - Annual Maintenance	Per Server Instance		CCSU13370505-A	N/A	N/A	A			$ 5,705.67	$ 6,276.24	$ 6,903.86	$ 7,594.25	$ 8,353.67	$ 9,189.04	$ 10,107.94	$ 11,118.74	$ 12,230.61	$ 13,453.67
Database Management Service	Database Software - Oracle 11g Real Application Server - Physical Server using Windows pConfig-3 - Annual Maintenance	Per Server Instance		CCSU13370506-A	N/A	N/A	A			$ 2,762.75	$ 3,039.02	$ 3,342.92	$ 3,677.21	$ 4,044.94	$ 4,449.43	$ 4,894.37	$ 5,383.81	$ 5,922.19	$ 6,514.41
Database Management Service	Database Software - Oracle 11g Standard - Physical Server using Windows pConfig-3 - Annual Maintenance	Per Server Instance		CCSU13370507-A	N/A	N/A	A			$ 700.70	$ 770.77	$ 847.84	$ 932.63	$ 1,025.89	$ 1,128.48	$ 1,241.33	$ 1,365.46	$ 1,502.00	$ 1,652.21
Database Management Service	Database Software - Sybase ASE Enterprise - Physical Server using Windows pConfig-3	Per Server Instance		CCSU13370013-A	N/A	N/A	A			$ 83,753.23	$ 86,265.83	$ 88,853.80	$ 91,519.42	$ 94,265.00	$ 97,092.95	$ 100,005.74	$ 103,005.91	$ 106,096.09	$ 109,278.97
Database Management Service	Database Software - Sybase Replication Server using Windows pConfig-3	Per Server Instance		CCSU13370014-A	N/A	N/A	A			$ 94,570.09	$ 97,407.19	$ 100,329.41	$ 103,339.29	$ 106,439.47	$ 109,632.66	$ 112,921.64	$ 116,309.28	$ 119,798.56	$ 123,392.52
Database Management Service	Database Software - Sybase ASE Standard - Physical Server using Windows pConfig-3	Per Server Instance		CCSU13370015-A	N/A	N/A				$ 18,500.29	$ 19,055.30	$ 19,626.96	$ 20,215.77	$ 20,822.24	$ 21,446.91	$ 22,090.32	$ 22,753.03	$ 23,435.62	$ 24,138.69

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	Product Name	Unit	Qty per config	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Database Management Service	Database Software - Sybase ASE Enterprise - Physical Server using Windows pConfig-3 - Annual Maintenance	Per Server Instance		CCSU13370508-A	N/A	N/A	A			$ 16,750.65	$ 18,425.71	$ 20,268.28	$ 22,295.11	$ 24,524.62	$ 26,977.08	$ 29,674.79	$ 32,642.27	$ 35,906.50	$ 39,497.15
Database Management Service	Database Software - Sybase Replication Server using Windows pConfig-3 - Annual Maintenance	Per Server Instance		CCSU13370509-A	N/A	N/A	A			$ 20,868.01	$ 22,954.81	$ 25,250.29	$ 27,775.32	$ 30,552.86	$ 33,608.14	$ 36,968.95	$ 40,665.85	$ 44,732.44	$ 49,205.68
Database Management Service	Database Software - Sybase ASE Standard - Physical Server using Windows pConfig-3 - Annual Maintenance	Per Server Instance		CCSU13370510-A	N/A	N/A				$ 3,700.06	$ 4,070.06	$ 4,477.07	$ 4,924.78	$ 5,417.26	$ 5,958.98	$ 6,554.88	$ 7,210.37	$ 7,931.40	$ 8,724.55
Database Management Service	Oracle Build p-Series Standard (1 server)	Per Request		CCSI13370016-A	N/A	N/A	A			$ 53 492.00	$ 55 096.76	$ 56 749.66	$ 58 452.15	$ 60 205.72	$ 62 011.89	$ 63 872.25	$ 65 788.41	$ 67 762.07	$ 69 794.93
Database Management Service	Oracle Build p-Series Complex (2 servers in clustered pair)	Per Request		CCSI13370017-A	N/A	N/A	A			$ 84,142.00	$ 86,666.26	$ 89,266.25	$ 91,944.24	$ 94,702.56	$ 97,543.64	$ 100,469.95	$ 103,484.05	$ 106,588.57	$ 109,786.23
Database Management Service	Oracle Upgrade p-Series Standard (1 server)	Per Request		CCSI13370018-A	N/A	N/A	A			$ 49 423.00	$ 50 905.69	$ 52 432.86	$ 54 005.85	$ 55 626.02	$ 57 294.80	$ 59 013.65	$ 60 784.06	$ 62 607.58	$ 64 485.81
Database Management Service	Oracle Upgrade p-Series Complex (2 servers in clustered pair)	Per Request		CCSI13370019-A	N/A	N/A	A			$ 63,525.00	$ 65,430.75	$ 67,393.67	$ 69,415.48	$ 71,497.95	$ 73,642.89	$ 75,852.17	$ 78,127.74	$ 80,471.57	$ 82,885.72
Database Management Service	DB2 Build p-Series Standard (1 server)	Per Request		CCSI13370020-A	N/A	N/A	A			$ 62,646.00	$ 64,525.38	$ 66,461.14	$ 68,454.98	$ 70,508.62	$ 72,623.88	$ 74,802.60	$ 77,046.68	$ 79,358.08	$ 81,738.82
Database Management Service	DB2 Build p-Series Complex (2 servers)	Per Request		CCSI13370021-A	N/A	N/A	A			$ 102,445.00	$ 105,518.35	$ 108,683.90	$ 111,944.42	$ 115,302.75	$ 118,761.83	$ 122,324.69	$ 125,994.43	$ 129,774.26	$ 133,667.49
Database Management Service	DB2 Upgrade p-Series Standard (1 server)	Per Request		CCSI13370022-A	N/A	N/A	A			$ 56 749.00	$ 58 451.47	$ 60 205.01	$ 62 011.16	$ 63 871.50	$ 65 787.64	$ 67 761.27	$ 69 794.11	$ 71 887.94	$ 74 044.57
Database Management Service	DB2 Upgrade p-Series Complex (2 servers)	Per Request		CCSI13370023-A	N/A	N/A	A			$ 78 859.00	$ 81 224.77	$ 83 661.51	$ 86 171.36	$ 88 756.50	$ 91 419.19	$ 94 161.77	$ 96 986.62	$ 99 896.22	$ 102 893.11
Database Management Service	p-Series Database Administrator for Oracle (3TB)	Per Database		CCSI13370024-A	N/A	N/A	A			$ 28,415.00	$ 29,267.45	$ 30,145.47	$ 31,049.84	$ 31,981.33	$ 32,940.77	$ 33,929.00	$ 34,946.87	$ 35,995.27	$ 37,075.13
Database Management Service	p-Series Database Administrator for Oracle (7TB)	Per Database		CCSI13370025-A	N/A	N/A	A			$ 56,830.00	$ 58,534.90	$ 60,290.95	$ 62,099.68	$ 63,962.67	$ 65,881.55	$ 67,857.99	$ 69,893.73	$ 71,990.54	$ 74,150.26
Database Management Service	p-Series Database Administrator for Oracle (12TB)	Per Database		CCSI13370026-A	N/A	N/A	A			$ 85 245.00	$ 87 802.35	$ 90 436.42	$ 93 149.51	$ 95 944.00	$ 98 822.32	$ 101 786.99	$ 104 840.60	$ 107 985.82	$ 111 225.39
Database Management Service	p-Series Database Administrator for DB2 (3TB)	Per Database		CCSI13370027-A	N/A	N/A	A			$ 28 415.00	$ 29 267.45	$ 30 145.47	$ 31 049.84	$ 31 981.33	$ 32 940.77	$ 33 929.00	$ 34 946.87	$ 35 995.27	$ 37 075.13
Database Management Service	p-Series Database Administrator for DB2 (7TB)	Per Database		CCSI13370028-A	N/A	N/A	A			$ 56,830.00	$ 58,534.90	$ 60,290.95	$ 62,099.68	$ 63,962.67	$ 65,881.55	$ 67,857.99	$ 69,893.73	$ 71,990.54	$ 74,150.26
Database Management Service	p-Series Database Administrator for DB2 (12TB)	Per Database		CCSI13370029-A	N/A	N/A	A			$ 85,245.00	$ 87,802.35	$ 90,436.42	$ 93,149.51	$ 95,944.00	$ 98,822.32	$ 101,786.99	$ 104,840.60	$ 107,985.82	$ 111,225.39
Database Management Service	p-Series Database Administrator for High Availability Databases: Oracle RAC or DB2 Clusters (20 databases)	Per Database		CCSI13370030-A	N/A	N/A	A			$ 28,415.00	$ 29,267.45	$ 30,145.47	$ 31,049.84	$ 31,981.33	$ 32,940.77	$ 33,929.00	$ 34,946.87	$ 35,995.27	$ 37,075.13
Database Management Service	p-Series Database Administrator for High Availability Databases: Oracle RAC or DB2 Clusters (40 databases)	Per Database		CCSI13370031-A	N/A	N/A	A			$ 56,830.00	$ 58,534.90	$ 60,290.95	$ 62,099.68	$ 63,962.67	$ 65,881.55	$ 67,857.99	$ 69,893.73	$ 71,990.54	$ 74,150.26
Database Management Service	p-Series Database Administrator for High Availability Databases: Oracle RAC or DB2 Clusters (60 databases)	Per Database		CCSI13370032-A	N/A	N/A	A			$ 85,245.00	$ 87,802.35	$ 90,436.42	$ 93,149.51	$ 95,944.00	$ 98,822.32	$ 101,786.99	$ 104,840.60	$ 107,985.82	$ 111,225.39
Database Management Service	IMS Upgrade z-Series Standard (1 subsystem without data sharing or clustering)	Per Request		CCSI13370033-A	N/A	N/A	A			$ 62,646.00	$ 64,525.38	$ 66,461.14	$ 68,454.98	$ 70,508.62	$ 72,623.88	$ 74,802.60	$ 77,046.68	$ 79,358.08	$ 81,738.82
Database Management Service	IMS Upgrade z-Series Complex (2 subsystems with data sharing and clustering across multiple CECs)	Per Request		CCSI13370034-A	N/A	N/A	A			$ 102,445.00	$ 105,518.35	$ 108,683.90	$ 111,944.42	$ 115,302.75	$ 118,761.83	$ 122,324.69	$ 125,994.43	$ 129,774.26	$ 133,667.49
Database Management Service	IMS Maintenance z-Series Standard (1 subsystem without data sharing or clustering)	Per Request		CCSI13370035-A	N/A	N/A	A			$ 56,749.00	$ 58,451.47	$ 60,205.01	$ 62,011.16	$ 63,871.50	$ 65,787.64	$ 67,761.27	$ 69,794.11	$ 71,887.94	$ 74,044.57
Database Management Service	IMS Maintenance z-Series Complex (2 subsystems with data sharing and clustering across multiple CECs)	Per Request		CCSI13370036-A	N/A	N/A	A			$ 78,859.00	$ 81,224.77	$ 83,661.51	$ 86,171.36	$ 88,756.50	$ 91,419.19	$ 94,161.77	$ 96,986.62	$ 99,896.22	$ 102,893.11
Database Management Service	DB2 Upgrade z Series Standard (1 subsystem without data sharing or clustering)	Per Request		CCSI13370037-A	N/A	N/A	A			$ 67,067.00	$ 69,079.01	$ 71,151.38	$ 73,285.92	$ 75,484.50	$ 77,749.03	$ 80,081.51	$ 82,483.95	$ 84,958.47	$ 87,507.22
Database Management Service	DB2 Upgrade z-Series Complex (2 subsystems with data sharing and clustering across multiple CECs)	Per Request		CCSI13370038-A	N/A	N/A	A			$ 110,551.00	$ 113,867.53	$ 117,283.56	$ 120,802.06	$ 124,426.12	$ 128,158.91	$ 132,003.68	$ 135,963.79	$ 140,042.70	$ 144,243.98
Database Management Service	DB2 Maintenance z-Series Standard (1 subsystem without data sharing or clustering)	Per Request		CCSI13370039-A	N/A	N/A	A			$ 61,909.00	$ 63,766.27	$ 65,679.26	$ 67,649.64	$ 69,679.12	$ 71,769.50	$ 73,922.58	$ 76,140.26	$ 78,424.47	$ 80,777.20
Database Management Service	DB2 Maintenance z-Series Complex (2 subsystems with data sharing and clustering across multiple CECs)	Per Request		CCSI13370040-A	N/A	N/A	A			$ 75,174.00	$ 77,429.22	$ 79,752.10	$ 82,144.66	$ 84,609.00	$ 87,147.27	$ 89,761.69	$ 92,454.54	$ 95,228.17	$ 98,085.02
Database Management Service	z-Series Database Administrator for DB2 (5TB)	Per Database		CCSI13370041-A	N/A	N/A	A			$ 25 890.00	$ 26 666.70	$ 27 466.70	$ 28 290.70	$ 29 139.42	$ 30 013.61	$ 30 914.01	$ 31 841.43	$ 32 796.68	$ 33 780.58
Database Management Service	z-Series Database Administrator for DB2 (10TB)	Per Database		CCSI13370042-A	N/A	N/A	A			$ 51 775.00	$ 53 328.25	$ 54 928.10	$ 56 575.94	$ 58 273.22	$ 60 021.42	$ 61 822.06	$ 63 676.72	$ 65 587.02	$ 67 554.63
Database Management Service	z-Series Database Administrator for DB2 (15TB)	Per Database		CCSI13370043-A	N/A	N/A	A			$ 77,660.00	$ 79,989.80	$ 82,389.49	$ 84,861.18	$ 87,407.01	$ 90,029.22	$ 92,730.10	$ 95,512.00	$ 98,377.36	$ 101,328.69
Database Management Service	z-Series Database Administrator for IMS (5TB)	Per Database		CCSI13370044-A	N/A	N/A	A			$ 25,890.00	$ 26,666.70	$ 27,466.70	$ 28,290.70	$ 29,139.42	$ 30,013.61	$ 30,914.01	$ 31,841.43	$ 32,796.68	$ 33,780.58
Database Management Service	z-Series Database Administrator for IMS (10TB)	Per Database		CCSI13370045-A	N/A	N/A	A			$ 51 775.00	$ 53 328.25	$ 54 928.10	$ 56 575.94	$ 58 273.22	$ 60 021.42	$ 61 822.06	$ 63 676.72	$ 65 587.02	$ 67 554.63
Database Management Service	z-Series Database Administrator for IMS (15TB)	Per Database		CCSI13370046-A	N/A	N/A	A			$ 77 660.00	$ 79 989.80	$ 82 389.49	$ 84 861.18	$ 87 407.01	$ 90 029.22	$ 92 730.10	$ 95 512.00	$ 98 377.36	$ 101 328.69
Database Management Service	z-Series High Availability Databases: IMS or DB2 DataSharing (25 databases)	Per Database		CCSI13370047-A	N/A	N/A	A			$ 25,890.00	$ 26,666.70	$ 27,466.70	$ 28,290.70	$ 29,139.42	$ 30,013.61	$ 30,914.01	$ 31,841.43	$ 32,796.68	$ 33,780.58
Database Management Service	z-Series High Availability Databases: IMS or DB2 DataSharing (50 databases)	Per Database		CCSI13370048-A	N/A	N/A	A			$ 51,775.00	$ 53,328.25	$ 54,928.10	$ 56,575.94	$ 58,273.22	$ 60,021.42	$ 61,822.06	$ 63,676.72	$ 65,587.02	$ 67,554.63
Database Management Service	z-Series High Availability Databases: IMS or DB2 DataSharing (75 databases)	Per Database		CCSI13370049-A	N/A	N/A	A			$ 77,660.00	$ 79,989.80	$ 82,389.49	$ 84,861.18	$ 87,407.01	$ 90,029.22	$ 92,730.10	$ 95,512.00	$ 98,377.36	$ 101,328.69
Batch and Job Scheduling	Batch and Job Scheduling- Job Creation or Modification - Small (Up to 25 Steps in Job Script)	Per Job Script		CCSU13370050-A	N/A	N/A	A			$ 2,243.50	$ 2,310.81	$ 2,380.13	$ 2,451.54	$ 2,525.08	$ 2,600.83	$ 2,678.86	$ 2,759.22	$ 2,842.00	$ 2,927.26
Batch and Job Scheduling	Batch and Job Scheduling- Job Creation or Modification - Medium (Up to 50 Steps in Job Script)	Per Job Script		CCSU13370051-A	N/A	N/A	A			$ 3,516.22	$ 3,621.71	$ 3,730.36	$ 3,842.27	$ 3,957.54	$ 4,076.26	$ 4,198.55	$ 4,324.51	$ 4,454.24	$ 4,587.87
Batch and Job Scheduling	Batch and Job Scheduling- Job Creation or Modification - Large (Up to 100 Steps in Job Script)	Per Job Script		CCSU13370052-A	N/A	N/A	A			$ 8,790.55	$ 9,054.27	$ 9,325.90	$ 9,605.68	$ 9,893.85	$ 10,190.66	$ 10,496.38	$ 10,811.27	$ 11,135.61	$ 11,469.68
Batch and Job Scheduling	Batch and Job Scheduling- Scheduling and Monitoring - Small (Up to 25 Steps in Job Script)	Per Job Script		CCSU13370053-A	N/A	N/A	A			$ 111.72	$ 114.17	$ 116.67	$ 119.23	$ 121.85	$ 124.54	$ 127.29	$ 130.10	$ 132.99	$ 135.94

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	Product Name	Unit	Qty per config	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Batch and Job Scheduling	Batch and Job Scheduling- Scheduling and Monitoring - Medium (Up to 50 Steps in Job Script)	Per Job Script		CCSU13370054-A	N/A	N/A	A			$ 178.76	$ 182.66	$ 186.67	$ 190.77	$ 194.96	$ 199.26	$ 203.66	$ 208.17	$ 212.78	$ 217.51
Batch and Job Scheduling	Batch and Job Scheduling- Scheduling and Monitoring - Large (Up to 100 Steps in Job Script)	Per Job Script		CCSU13370055-A	N/A	N/A	A			$ 268.13	$ 274.00	$ 280.00	$ 286.15	$ 292.44	$ 298.89	$ 305.49	$ 312.25	$ 319.17	$ 326.26
Batch and Job Scheduling	Batch and Job Scheduling- Scheduling and Monitoring - Small (Up to 25 Steps in Job Script) - Control M Software	Per Job Script		CCSU13370511-A	N/A	N/A	A			$ 268.73	$ 276.79	$ 285.10	$ 293.65	$ 302.46	$ 311.54	$ 320.88	$ 330.51	$ 340.42	$ 350.64
Batch and Job Scheduling	Batch and Job Scheduling- Scheduling and Monitoring - Medium (Up to 50 Steps in Job Script) - Control M Software	Per Job Script		CCSU13370512-A	N/A	N/A	A			$ 537.47	$ 553.59	$ 570.20	$ 587.30	$ 604.92	$ 623.07	$ 641.76	$ 661.02	$ 680.85	$ 701.27
Batch and Job Scheduling	Batch and Job Scheduling- Scheduling and Monitoring - Large (Up to 100 Steps in Job Script) - Control M Software	Per Job Script		CCSU13370513-A	N/A	N/A	A			$ 1,074.93	$ 1,107.18	$ 1,140.40	$ 1,174.61	$ 1,209.85	$ 1,246.14	$ 1,283.52	$ 1,322.03	$ 1,361.69	$ 1,402.54
Batch and Job Scheduling	AIX Production Batch Operations Support (50,000 jobs per year)	Per Month		CCSI13370056-A	N/A	N/A	A			$ 8,824.77	$ 9,089.52	$ 9,362.20	$ 9,643.07	$ 9,932.36	$ 10,230.33	$ 10,537.24	$ 10,853.36	$ 11,178.96	$ 11,514.33
Batch and Job Scheduling	IBM Mainframe Production Batch Operations Support (50,000 jobs per year)	Per Month		CCSI13370057-A	N/A	N/A	A			$ 25,749.96	$ 26,522.46	$ 27,318.13	$ 28,137.68	$ 28,981.81	$ 29,851.26	$ 30,746.80	$ 31,669.20	$ 32,619.28	$ 33,597.86
Service Management	Service Management Custom Report - Small (4 hours to create report)	Per Report		CCSU13370058-A	N/A	N/A	A			$ 230.76	$ 237.68	$ 244.81	$ 252.16	$ 259.72	$ 267.51	$ 275.54	$ 283.81	$ 292.32	$ 301.09
Service Management	Service Management Custom Report - Medium (8 hours to create report)	Per Report		CCSU13370059-A	N/A	N/A	A			$ 461.52	$ 475.37	$ 489.63	$ 504.32	$ 519.45	$ 535.03	$ 551.08	$ 567.61	$ 584.64	$ 602.18
Service Management	Service Management Custom Report - Large (20 hours to create report)	Per Report		CCSU13370060-A	N/A	N/A	A			$ 1,153.80	$ 1,188.42	$ 1,224.07	$ 1,260.79	$ 1,298.61	$ 1,337.57	$ 1,377.70	$ 1,419.03	$ 1,461.60	$ 1,505.45
Service Management	ITSM Named Licenses - Agency Access to ITSM, license supports 1 user	Per License		CCSU13370061-A	N/A	N/A	A			$ 47.09	$ 48.51	$ 49.96	$ 51.46	$ 53.00	$ 54.59	$ 56.23	$ 57.92	$ 59.66	$ 61.44
Service Management	ITSM Floating Licenses - Agency Access to ITSM, license supports 10 users	Per License		CCSU13370062-A	N/A	N/A	A			$ 117.73	$ 121.26	$ 124.90	$ 128.65	$ 132.51	$ 136.48	$ 140.58	$ 144.79	$ 149.14	$ 153.61
Service Management	Application Mapping (ADDM) Discovery Script Setup - Small	Per Application Discovery Script		CCSU13370063-A	N/A	N/A	A			$ 901.57	$ 4.26	$ 4.35	$ 4.44	$ 4.53	$ 4.63	$ 4.73	$ 4.83	$ 4.93	$ 5.04
Service Management	Application Mapping (ADDM) Discovery Script Setup - Medium	Per Application Discovery Script		CCSU13370064-A	N/A	N/A	A			$ 905.74	$ 8.52	$ 8.69	$ 8.88	$ 9.06	$ 9.26	$ 9.45	$ 9.65	$ 9.86	$ 10.07
Service Management	Application Mapping (ADDM) Discovery Script Setup - Large	Per Application Discovery Script		CCSU13370065-A	N/A	N/A	A			$ 914.08	$ 17.03	$ 17.39	$ 17.75	$ 18.13	$ 18.51	$ 18.91	$ 19.31	$ 19.72	$ 20.14
Service Management	Application Mapping (ADDM) Discovery Script Maintenance - Small	Per Application Discovery Script		CCSU13370066-A	N/A	N/A	A			$ 4.17	$ 4.26	$ 4.35	$ 4.44	$ 4.53	$ 4.63	$ 4.73	$ 4.83	$ 4.93	$ 5.04
Service Management	Application Mapping (ADDM) Discovery Script Maintenance - Medium	Per Application Discovery Script		CCSU13370067-A	N/A	N/A	A			$ 8.34	$ 8.52	$ 8.69	$ 8.88	$ 9.06	$ 9.26	$ 9.45	$ 9.65	$ 9.86	$ 10.07
Service Management	Application Mapping (ADDM) Discovery Script Maintenance - Large	Per Application Discovery Script		CCSU13370068-A	N/A	N/A	A			$ 16.68	$ 17.03	$ 17.39	$ 17.75	$ 18.13	$ 18.51	$ 18.91	$ 19.31	$ 19.72	$ 20.14
Compute Services - Infrastructure Monitoring	Microsoft System Center 2012 (SCOM) - Standard	Per Server		CCSU13370069-A	N/A	N/A	A			$ 2.29	$ 2.36	$ 2.43	$ 2.50	$ 2.58	$ 2.66	$ 2.74	$ 2.82	$ 2.90	$ 2.99
Fully Managed	Fully Managed – Physical – Platinum – Comm/Decomm	Per Server		CCSU13370070-A	N/A	N/A	A			$ 897.57	$ 916.36	$ 935.60	$ 955.31	$ 975.48	$ 996.14	$ 1,017.29	$ 1,038.96	$ 1,061.14	$ 1,083.86
Fully Managed	Fully Managed – Physical – Gold – Comm/Decomm	Per Server		CCSU13370071-A	N/A	N/A	A			$ 897.57	$ 916.36	$ 935.60	$ 955.31	$ 975.48	$ 996.14	$ 1,017.29	$ 1,038.96	$ 1,061.14	$ 1,083.86
Fully Managed	Fully Managed – Physical – Silver – Comm/Decomm	Per Server		CCSU13370072-A	N/A	N/A	A			$ 583.42	$ 595.64	$ 608.14	$ 620.95	$ 634.06	$ 647.49	$ 661.24	$ 675.32	$ 689.74	$ 704.51
Fully Managed	Fully Managed – Physical – Bronze – Comm/Decomm	Per Server		CCSU13370073-A	N/A	N/A	A			$ 583.42	$ 595.64	$ 608.14	$ 620.95	$ 634.06	$ 647.49	$ 661.24	$ 675.32	$ 689.74	$ 704.51
Fully Managed	Fully Managed – Physical – Basic – Comm/Decomm	Per Server		CCSU13370074-A	N/A	N/A	A			$ 583.42	$ 595.64	$ 608.14	$ 620.95	$ 634.06	$ 647.49	$ 661.24	$ 675.32	$ 689.74	$ 704.51
Fully Managed	Fully Managed – Virtual – Platinum – Comm/Decomm	Per Server		CCSU13370075-A	N/A	N/A	A			$ 897.57	$ 916.36	$ 935.60	$ 955.31	$ 975.48	$ 996.14	$ 1,017.29	$ 1,038.96	$ 1,061.14	$ 1,083.86
Fully Managed	Fully Managed – Virtual – Gold – Comm/Decomm	Per Server		CCSU13370076-A	N/A	N/A	A			$ 897.57	$ 916.36	$ 935.60	$ 955.31	$ 975.48	$ 996.14	$ 1 017.29	$ 1 038.96	$ 1 061.14	$ 1 083.86
Fully Managed	Fully Managed – Virtual – Silver – Comm/Decomm	Per Server		CCSU13370077-A	N/A	N/A	A			$ 583.42	$ 595.64	$ 608.14	$ 620.95	$ 634.06	$ 647.49	$ 661.24	$ 675.32	$ 689.74	$ 704.51
Fully Managed	Fully Managed – Virtual – Bronze – Comm/Decomm	Per Server		CCSU13370078-A	N/A	N/A	A			$ 583.42	$ 595.64	$ 608.14	$ 620.95	$ 634.06	$ 647.49	$ 661.24	$ 675.32	$ 689.74	$ 704.51
Fully Managed	Fully Managed – Virtual – Basic – Comm/Decomm	Per Server		CCSU13370079-A	N/A	N/A	A			$ 583.42	$ 595.64	$ 608.14	$ 620.95	$ 634.06	$ 647.49	$ 661.24	$ 675.32	$ 689.74	$ 704.51
Fully Managed	Platinum AIX Service Level Package	Per Package		CCSI13370080-A	N/A	N/A	A			$ 240 748.38	$ 247 970.83	$ 255 409.96	$ 263 072.25	$ 270 964.42	$ 279 093.35	$ 287 466.15	$ 296 090.14	$ 304 972.84	$ 314 122.03
Fully Managed	Gold AIX Service Level Package	Per Package		CCSI13370081-A	N/A	N/A	A			$ 136,368.72	$ 140,459.78	$ 144,673.58	$ 149,013.78	$ 153,484.20	$ 158,088.72	$ 162,831.39	$ 167,716.33	$ 172,747.82	$ 177,930.25
Fully Managed	Disaster Recovery - AIX (271 images)	Per Server		CCSI13370082-A	N/A	N/A	A			$ 28,818.39	$ 29,682.94	$ 30,573.43	$ 31,490.63	$ 32,435.35	$ 33,408.41	$ 34,410.66	$ 35,442.98	$ 36,506.27	$ 37,601.46
Storage and Backup Service	Archive Services: Archive storage that provides record-level content management and replication to DR	Per GB of Protected Data		CCSU13370083-A	N/A	N/A	A			$ 0.19	$ 0.19	$ 0.19	$ 0.19	$ 0.19	$ 0.15	$ 0.15	$ 0.15	$ 0.15	$ 0.15
Storage and Backup Service	EMC PowerPath Storage Load Balancing S/W for Physical Servers.	Per CPU per Server		CCSU13370085-A	N/A	N/A	A			$ 4.67	$ 4.67	$ 4.67	$ 4.67	$ 4.67	$ 4.67	$ 4.67	$ 4.67	$ 4.67	$ 4.67
Storage and Backup Service	EMC PowerPath Storage Load Balancing S/W forVirtual Server Hosts UNITS : 322 CPUs ESX Virtual Servers	Per Server		CCSU13370086-A	N/A	N/A	A			$ 21.02	$ 21.02	$ 21.02	$ 21.02	$ 21.02	$ 23.72	$ 24.22	$ 24.73	$ 25.26	$ 25.80
Storage and Backup Service	Archive Services: Cost Effective Archive storage with replication to DR.	Per GB of Protected Data		CCSU13370088-A	N/A	N/A	A			$ 0.02	$ 0.02	$ 0.02	$ 0.02	$ 0.02	$ 0.01	$ 0.01	$ 0.01	$ 0.01	$ 0.01
Storage and Backup Service	IBM Storwize V7000 High Performance Tier	Per System	1	CCSI13370558-A	N/A	N/A	A			$ 284 844.29	$ 270 602.07	$ 257 071.97	$ 244 218.37	$ 232 007.45	$ 220 407.08	$ 209 386.73	$ 198 917.39	$ 188 971.52	$ 179 522.94
Storage and Backup Service	IBM Storwize V7000 Standard Performance Tier	Per System	1	CCSI13370559-A	N/A	N/A	A			$ 225 343.89	$ 214 076.69	$ 203 372.86	$ 193 204.22	$ 183 544.01	$ 174 366.80	$ 165 648.46	$ 157 366.04	$ 149 497.74	$ 142 022.85
Storage and Backup Service	IBM XIV Standard Performance Tier	Per System	1	CCSI13370560-A	N/A	N/A	A			$ 598,742.39	$ 568,805.27	$ 540,365.00	$ 513,346.75	$ 487,679.42	$ 463,295.45	$ 440,130.67	$ 418,124.14	$ 397,217.93	$ 377,357.04

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	Product Name	Unit	Qty per config	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Storage and Backup Service	IBM XIV High Performance Tier	Per System	1	CCSI13370561-A	N/A	N/A	A			$ 549,408.13	$ 521,937.73	$ 495,840.84	$ 471,048.80	$ 447,496.36	$ 425,121.54	$ 403,865.46	$ 383,672.19	$ 364,488.58	$ 346,264.15
Storage and Backup Service	IBM Storwize V7000 Unified NAS Tier	Per System	1	CCSI13370562-A	N/A	N/A	A			$ 41 381.46	$ 39 312.39	$ 37 346.77	$ 35 479.43	$ 33 705.46	$ 32 020.19	$ 30 419.18	$ 28 898.22	$ 27 453.31	$ 26 080.64
Storage and Backup Service	IBM Standard Rack	Per System	1	CCSI13370563-A	N/A	N/A	A			$ 6 230.18	$ 6 417.08	$ 6 609.59	$ 6 807.88	$ 7 012.12	$ 7 222.48	$ 7 439.16	$ 7 662.33	$ 7 892.20	$ 8 128.97
Managed Only	Managed Only – Platinum – Comm/Decomm	Per Server		CCSI13370091-A	N/A	N/A	A			$ 897.57	$ 916.36	$ 935.60	$ 955.31	$ 975.48	$ 996.14	$ 1,017.29	$ 1,038.96	$ 1,061.14	$ 1,083.86
Managed Only	Managed Only – Gold – Comm/Decomm	Per Server		CCSU13370092-A	N/A	N/A	A			$ 897.57	$ 916.36	$ 935.60	$ 955.31	$ 975.48	$ 996.14	$ 1,017.29	$ 1,038.96	$ 1,061.14	$ 1,083.86
Managed Only	Managed Only – Silver – Comm/Decomm	Per Server		CCSU13370093-A	N/A	N/A	A			$ 583.42	$ 595.64	$ 608.14	$ 620.95	$ 634.06	$ 647.49	$ 661.24	$ 675.32	$ 689.74	$ 704.51
Managed Only	Managed Only – Bronze – Comm/Decomm	Per Server		CCSU13370094-A	N/A	N/A	A			$ 583.42	$ 595.64	$ 608.14	$ 620.95	$ 634.06	$ 647.49	$ 661.24	$ 675.32	$ 689.74	$ 704.51
Managed Only	Managed Only – Basic – Comm/Decomm	Per Server		CCSU13370095-A	N/A	N/A	A			$ 583.42	$ 595.64	$ 608.14	$ 620.95	$ 634.06	$ 647.49	$ 661.24	$ 675.32	$ 689.74	$ 704.51
IBM Mainframe Services	Platinum IBM Mainframe Service Level Package	Per Package		CCSI13370096-A	N/A	N/A	A			$ 168,974.90	$ 174,044.14	$ 179,265.47	$ 184,643.43	$ 190,182.73	$ 195,888.22	$ 201,764.86	$ 207,817.81	$ 214,052.34	$ 220,473.91
IBM Mainframe Services	Gold IBM Mainframe and i-Series Service Level Package	Per Package		CCSI13370097-A	N/A	N/A	A			$ 460,791.89	$ 474,615.65	$ 488,854.12	$ 503,519.74	$ 518,625.33	$ 534,184.09	$ 550,209.61	$ 566,715.90	$ 583,717.38	$ 601,228.90
IBM Mainframe Services	DPH IBM Mainframe Services	Per Package		CCSI13370098-A	N/A	N/A	A			$ 560 471.30	$ 577 285.44	$ 594 604.00	$ 612 442.12	$ 630 815.38	$ 649 739.85	$ 669 232.04	$ 689 309.00	$ 709 988.27	$ 731 287.92
IBM Mainframe Services	Disaster Recovery - Mainframe / i-series (134 images)	Per Package		CCSI13370099-A	N/A	N/A	A			$ 57,168.00	$ 58,883.04	$ 60,649.54	$ 62,469.02	$ 64,343.09	$ 66,273.39	$ 68,261.59	$ 70,309.43	$ 72,418.72	$ 74,591.28
Unisys Mainframe - Storage and Backup Service	Mainframe Services: EMC RecoverPoint Replication	Per 50 TB of replicated storage		CCSU13370100-A	N/A	N/A	A			$ 173.75	$ 173.75	$ 173.75	$ 173.75	$ 173.75	$ 138.80	$ 138.80	$ 138.80	$ 138.80	$ 138.80
Unisys Mainframe - Storage and Backup Service	Mainframe Services: EMC SRDF Replication	Per 50 TB of replicated storage		CCSU13370101-A	N/A	N/A	A			$ 173.75	$ 173.75	$ 173.75	$ 173.75	$ 173.75	$ 138.80	$ 138.80	$ 138.80	$ 138.80	$ 138.80
Unisys Mainframe Configuration - Add-On Software Run Pack	Unisys Mainframe (Clearpath Dorado) – Config-1 – Run Pack(Add-on software run pack for Config - 1)	Per Config		CCSU13370102-A	N/A	N/A	A			$ 231,485.73	$ 231,485.73	$ 231,485.73	$ 231,485.73	$ 231,485.73	$ 231,485.73	$ 231,485.73	$ 231,485.73	$ 231,485.73	$ 231,485.73
Unisys Mainframe Configuration - Add-On Software Run Pack	Unisys Mainframe (Clearpath Libra) – Config-2 – Run Pack(Add-on software run pack for Config - 2)	Per Config		CCSU13370103-A	N/A	N/A	A			$ 8,469.72	$ 8,469.72	$ 8,469.72	$ 8,469.72	$ 8,469.72	$ 8,469.72	$ 8,469.72	$ 8,469.72	$ 8,469.72	$ 8,469.72
Unisys Mainframe Configuration - Add-On Software Run Pack	Unisys Mainframe (Clearpath Dorado) – Config-3 – Run Pack(Add-on software run pack for Config - 3)	Per Config		CCSU13370104-A	N/A	N/A	A			$ 1,159.90	$ 1,159.90	$ 1,159.90	$ 1,159.90	$ 1,159.90	$ 1,159.90	$ 1,159.90	$ 1,159.90	$ 1,159.90	$ 1,159.90
Unisys Mainframe Configuration - Exhibit Based Replacement	Unisys Mainframe (Clearpath Dorado) – DPW Production System(Provides technology replacement of DPW mainframe as described in the Exhibits)	Per Config		CCSU13370106-A	N/A	N/A	A			$ 520,409.52	$ 527,666.28	$ 535,288.18	$ 543,287.59	$ 551,689.48	$ 509,680.27	$ 516,938.55	$ 524,557.40	$ 532,558.34	$ 540,960.23
Unisys Mainframe Configuration - Exhibit Based Replacement	Unisys Mainframe (Clearpath Dorado) – PSP Production System(Provides technology replacement of PSP mainframe as described in the Exhibits)	Per Config		CCSU13370107-A	N/A	N/A	A			$ 113,151.09	$ 114,721.94	$ 116,373.11	$ 118,104.10	$ 119,923.49	$ 113,594.65	$ 115,167.03	$ 116,815.15	$ 118,547.66	$ 120,367.05
Unisys Mainframe Configuration - Exhibit Based Replacement	Unisys Mainframe (Clearpath Dorado) – DPW/PSP DR(Provides technology replacement of DPW/PSP DR mainframe as described in the Exhibits)	Per Config		CCSU13370108-A	N/A	N/A	A			$ 30,452.89	$ 31,143.88	$ 31,871.69	$ 32,633.22	$ 33,434.80	$ 30,726.59	$ 31,419.10	$ 32,143.86	$ 32,906.91	$ 33,708.49
Unisys Mainframe Configuration - Exhibit Based Replacement	Unisys Mainframe (Clearpath Libra) – PA Game Production(Provides technology replacement of PA Game Production mainframe as described in the Exhibits)	Per Config		CCSU13370109-A	N/A	N/A	A			$ 16,126.09	$ 16,197.03	$ 16,272.05	$ 16,350.57	$ 16,432.59	$ 16,706.72	$ 73,786.31	$ 72,210.86	$ 69,724.44	$ 67,340.45
Unisys Mainframe Configuration - Exhibit Based Replacement	Unisys Mainframe (Clearpath Libra) – PA Game Development(Provides technology replacement of PA Game Development mainframe as described in the Exhibits)	Per Config		CCSU13370110-A	N/A	N/A	A			$ 3,550.33	$ 3,583.88	$ 3,619.13	$ 3,656.30	$ 3,694.60	$ 3,929.41	$ 12,424.77	$ 8,365.71	$ 8,399.61	$ 8,435.21
Unisys Mainframe Configuration - Exhibit Based Replacement	Unisys Mainframe (Clearpath Libra) – PA Game DR(Provides technology replacement of PA Game DR mainframe as described in the Exhibits)	Per Config		CCSU13370111-A	N/A	N/A	A			$ 12,443.90	$ 12,465.37	$ 12,488.08	$ 12,511.80	$ 12,536.66	$ 12,660.76	$ 66,992.85	$ 63,209.46	$ 63,228.01	$ 63,247.65
Microsoft Cloud Compute Services	Microsoft SharePoint Online Plan 1 (Govt Cloud) - per user monthly subscription	Per User		CCSM13370113-A	N/A	N/A	A			$ 45.95	$ 47.32	$ 48.74	$ 50.21	$ 51.71	$ 53.26	$ 54.86	$ 56.51	$ 58.20	$ 59.95
Microsoft Cloud Compute Services	Microsoft SharePoint Online Plan 2 (Govt Cloud) - per user monthly subscription	Per User		CCSM13370114-A	N/A	N/A	A			$ 107.21	$ 110.42	$ 113.74	$ 117.15	$ 120.66	$ 124.28	$ 128.01	$ 131.85	$ 135.81	$ 139.88
Microsoft Cloud Compute Services	Microsoft Office 365 Plan 1 (Govt Cloud) - per user monthly subscription	Per User		CCSM13370115-A	N/A	N/A	A			$ 8.75	$ 9.02	$ 9.29	$ 9.57	$ 9.85	$ 10.15	$ 10.45	$ 10.77	$ 11.09	$ 11.42
Microsoft Cloud Compute Services	Microsoft Office 365 Plan 3 (Govt Cloud) - per user monthly subscription	Per User		CCSM13370116-A	N/A	N/A	A			$ 24.82	$ 25.56	$ 26.33	$ 27.12	$ 27.93	$ 28.77	$ 29.64	$ 30.53	$ 31.44	$ 32.38
Microsoft Cloud Compute Services	Microsoft Project Server Online (Govt Cloud) - per user monthly subscription	Per User		CCSM13370117-A	N/A	N/A	A			$ 41.53	$ 42.78	$ 44.06	$ 45.38	$ 46.74	$ 48.15	$ 49.59	$ 51.08	$ 52.61	$ 54.19
Microsoft Cloud Compute Services	Microsoft Project Server Online w/ Project Pro (Govt Cloud) - per user monthly subscription	Per User		CCSM13370118-A	N/A	N/A	A			$ 72.99	$ 75.18	$ 77.43	$ 79.76	$ 82.15	$ 84.61	$ 87.15	$ 89.77	$ 92.46	$ 95.23
Microsoft Cloud Compute Services	Microsoft Dynamics CRM Online - per user monthly subscription	Per User		CCSM13370119-A	N/A	N/A	A			$ 58.29	$ 60.04	$ 61.84	$ 63.69	$ 65.60	$ 67.57	$ 69.60	$ 71.69	$ 73.84	$ 76.05
Microsoft Cloud Compute Services	Microsoft Compute Svr VM - 1 Core-1.75GB RAM-2x1TB Disk Storage Non-Windows OS 1	Per Server for 100 Hours		CCSM13370120-A	N/A	N/A	A			$ 63.24	$ 65.14	$ 67.09	$ 69.11	$ 71.18	$ 73.32	$ 75.52	$ 77.78	$ 80.11	$ 82.52
Microsoft Cloud Compute Services	Microsoft Compute Svr VM - 1 Core-1.75GB RAM-2x1TB Disk Storage Windows OS 1	Per Server for 100 Hours		CCSM13370121-A	N/A	N/A	A			$ 85.72	$ 88.29	$ 90.94	$ 93.67	$ 96.48	$ 99.37	$ 102.35	$ 105.43	$ 108.59	$ 111.85
Microsoft Cloud Compute Services	Microsoft Hi Mem Compute Svr VM- 4 Core-28GB RAM-8x1TB Disk Storage Non-Windows OS	Per Server for 100 Hours		CCSM13370122-A	N/A	N/A	A			$ 670.04	$ 690.14	$ 710.85	$ 732.17	$ 754.14	$ 776.76	$ 800.06	$ 824.07	$ 848.79	$ 874.25
Microsoft Cloud Compute Services	Microsoft Hi Mem Compute Svr VM - 4 Core-28GB RAM-8x1TB Disk Storage Windows OS	Per Server for 100 Hours		CCSM13370123-A	N/A	N/A	A			$ 848.81	$ 874.27	$ 900.50	$ 927.52	$ 955.34	$ 984.00	$ 1,013.52	$ 1,043.93	$ 1,075.25	$ 1,107.50
Microsoft Cloud Compute Services	Microsoft Hi Mem Compute Svr VM - 8 Core-56GB RAM-16x1TB Disk Storage Non-Windows OS	Per Server for 100 Hours		CCSM13370124-A	N/A	N/A	A			$ 1,340.29	$ 1,380.50	$ 1,421.92	$ 1,464.57	$ 1,508.51	$ 1,553.77	$ 1,600.38	$ 1,648.39	$ 1,697.84	$ 1,748.78
Microsoft Cloud Compute Services	Microsoft Hi Mem Compute Svr VM - 8 Core-56GB RAM-16x1TB Disk Storage Windows OS	Per Server for 100 Hours		CCSM13370125-A	N/A	N/A	A			$ 1,697.62	$ 1,748.55	$ 1,801.00	$ 1,855.03	$ 1,910.68	$ 1,968.00	$ 2,027.04	$ 2,087.85	$ 2,150.49	$ 2,215.01
Microsoft Cloud Compute Services	Microsoft Hi Mem Compute Svr - 4 Core-28GB RAM-Cloud Services	Per Server for 100 Hours		CCSM13370126-A	N/A	N/A	A			$ 893.42	$ 920.22	$ 947.83	$ 976.26	$ 1,005.55	$ 1,035.72	$ 1,066.79	$ 1,098.79	$ 1,131.76	$ 1,165.71

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	Product Name	Unit	Qty per config	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Microsoft Cloud Compute Services	Microsoft Hi Mem Compute Svr - 8 Core-56GB RAM-Cloud Services	Per Server for 100 Hours		CCSM13370127-A	N/A	N/A	A			$ 1,786.96	$ 1,840.56	$ 1,895.78	$ 1,952.65	$ 2,011.23	$ 2,071.57	$ 2,133.72	$ 2,197.73	$ 2,263.66	$ 2,331.57
Microsoft Cloud Compute Services	Microsoft Azure Storage Geo Redundancy 100 GB	Per Month		CCSM13370128-A	N/A	N/A	A			$ 9.70	$ 9.99	$ 10.29	$ 10.60	$ 10.92	$ 11.24	$ 11.58	$ 11.93	$ 12.29	$ 12.66
Microsoft Cloud Compute Services	Microsoft Azure Storage Local Redundancy 100 GB	Per Month		CCSM13370129-A	N/A	N/A	A			$ 7.13	$ 7.35	$ 7.57	$ 7.79	$ 8.03	$ 8.27	$ 8.52	$ 8.77	$ 9.03	$ 9.31
Microsoft Cloud Compute Services	Microsoft Azure Backup Service 10 GB	Per Month		CCSM13370130-A	N/A	N/A	A			$ 5.11	$ 5.26	$ 5.42	$ 5.58	$ 5.75	$ 5.92	$ 6.10	$ 6.28	$ 6.47	$ 6.66
Microsoft Cloud Compute Services	Office 365 Migration Service	Per Month		CCSM13370131-A	N/A	N/A	A			$ 90 458.01	$ 93 171.75	$ 95 966.91	$ 98 845.91	$101 811.29	$104 865.63	$ 108 011.60	$ 111 251.95	$ 114 589.50	$ 118 027.19
Microsoft Cloud Compute Services	Office 365 Migration Tool	Per User		CCSM13370132-A	N/A	N/A	A			$ 8.19	$ 8.44	$ 8.69	$ 8.95	$ 9.22	$ 9.49	$ 9.78	$ 10.07	$ 10.37	$ 10.69
Microsoft Cloud Compute Services	Office 365 Management Service	Per Month		CCSM13370133-A	N/A	N/A	A			$ 13 174.14	$ 13 569.36	$ 13 976.44	$ 14 395.74	$ 14 827.61	$ 15 272.44	$ 15 730.61	$ 16 202.53	$ 16 688.60	$ 17 189.26
Microsoft Cloud Compute Services	Microsoft Sharepoint Online Migration	Per Month		CCSM13370134-A	N/A	N/A	A			$ 7,538.17	$ 7,764.31	$ 7,997.24	$ 8,237.16	$ 8,484.27	$ 8,738.80	$ 9,000.97	$ 9,271.00	$ 9,549.13	$ 9,835.60
Microsoft Cloud Compute Services	Microsoft Sharepoint Management Service	Per Month		CCSM13370135-A	N/A	N/A	A			$ 13,174.14	$ 13,449.92	$ 13,732.32	$ 14,021.50	$ 14,317.62	$ 14,620.84	$ 14,931.34	$ 15,249.30	$ 15,574.88	$ 15,908.28
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Dedicated Cloud - Base Service	Per Month		CCSV13370136-A	N/A	N/A	A			$ 23,179.29	$ 23,874.66	$ 24,590.90	$ 25,328.63	$ 26,088.49	$ 26,871.14	$ 27,677.28	$ 28,507.60	$ 29,362.83	$ 30,243.71
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Dedicated Cloud - Compute add-on (1 additional)	Per Month		CCSV13370137-A	N/A	N/A	A			$ 17,234.13	$ 17,751.15	$ 18,283.69	$ 18,832.20	$ 19,397.16	$ 19,979.08	$ 20,578.45	$ 21,195.80	$ 21,831.68	$ 22,486.63
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Dedicated Cloud - Compute add-on (2-3 additional)	Per Month		CCSV13370138-A	N/A	N/A	A			$ 16,662.96	$ 17,162.85	$ 17,677.73	$ 18,208.07	$ 18,754.31	$ 19,316.94	$ 19,896.45	$ 20,493.34	$ 21,108.14	$ 21,741.38
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Dedicated Cloud - Compute add-on (4-5 additional)	Per Month		CCSV13370139-A	N/A	N/A	A			$ 16,070.17	$ 16,552.28	$ 17,048.84	$ 17,560.31	$ 18,087.12	$ 18,629.73	$ 19,188.62	$ 19,764.28	$ 20,357.21	$ 20,967.93
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Dedicated Cloud - Compute add-on (6-7 additional)	Per Month		CCSV13370140-A	N/A	N/A	A			$ 15,315.22	$ 15,774.68	$ 16,247.92	$ 16,735.35	$ 17,237.42	$ 17,754.54	$ 18,287.17	$ 18,835.79	$ 19,400.86	$ 19,982.89
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Dedicated Cloud - Compute add-on (8 additional)	Per Month		CCSV13370141-A	N/A	N/A	A			$ 14,480.99	$ 14,915.42	$ 15,362.88	$ 15,823.77	$ 16,298.48	$ 16,787.44	$ 17,291.06	$ 17,809.79	$ 18,344.09	$ 18,894.41
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Dedicated Cloud - Support add-on (1 additional)	Per Month		CCSV13370142-A	N/A	N/A	A			$ 2,585.57	$ 2,663.14	$ 2,743.03	$ 2,825.32	$ 2,910.08	$ 2,997.38	$ 3,087.31	$ 3,179.92	$ 3,275.32	$ 3,373.58
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Dedicated Cloud - Support add-on (2-3 additional)	Per Month		CCSV13370143-A	N/A	N/A	A			$ 2,165.75	$ 2,230.72	$ 2,297.65	$ 2,366.58	$ 2,437.57	$ 2,510.70	$ 2,586.02	$ 2,663.60	$ 2,743.51	$ 2,825.82
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Dedicated Cloud - Support add-on (4-5 additional)	Per Month		CCSV13370144-A	N/A	N/A	A			$ 1,767.56	$ 1,820.58	$ 1,875.20	$ 1,931.46	$ 1,989.40	$ 2,049.08	$ 2,110.55	$ 2,173.87	$ 2,239.09	$ 2,306.26
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Dedicated Cloud - Support add-on (6-7 additional)	Per Month		CCSV13370145-A	N/A	N/A	A			$ 1,531.52	$ 1,577.47	$ 1,624.79	$ 1,673.54	$ 1,723.74	$ 1,775.45	$ 1,828.72	$ 1,883.58	$ 1,940.09	$ 1,998.29
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Dedicated Cloud - Support add-on (8 additional)	Per Month		CCSV13370146-A	N/A	N/A	A			$ 1,374.77	$ 1,416.01	$ 1,458.49	$ 1,502.24	$ 1,547.31	$ 1,593.73	$ 1,641.54	$ 1,690.79	$ 1,741.51	$ 1,793.76
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Dedicated Cloud - Storage add-on (1 additional)	Per Month		CCSV13370147-A	N/A	N/A	A			$ 1,531.52	$ 1,577.47	$ 1,624.79	$ 1,673.54	$ 1,723.74	$ 1,775.45	$ 1,828.72	$ 1,883.58	$ 1,940.09	$ 1,998.29
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Dedicated Cloud - Storage add-on (2-3 additional)	Per Month		CCSV13370148-A	N/A	N/A	A			$ 1,459.45	$ 1,503.23	$ 1,548.33	$ 1,594.78	$ 1,642.62	$ 1,691.90	$ 1,742.66	$ 1,794.94	$ 1,848.79	$ 1,904.25
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Dedicated Cloud - Storage add-on (4-5 additional)	Per Month		CCSV13370149-A	N/A	N/A	A			$ 1,378.37	$ 1,419.72	$ 1,462.31	$ 1,506.18	$ 1,551.37	$ 1,597.91	$ 1,645.85	$ 1,695.22	$ 1,746.08	$ 1,798.46
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Dedicated Cloud - Storage add-on (6 additional)	Per Month		CCSV13370150-A	N/A	N/A	A			$ 1,306.30	$ 1,345.49	$ 1,385.85	$ 1,427.43	$ 1,470.25	$ 1,514.36	$ 1,559.79	$ 1,606.58	$ 1,654.78	$ 1,704.42
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Dedicated Cloud - Bandwidth add-on	Per Month		CCSV13370151-A	N/A	N/A	A			$ 1,715.45	$ 1,766.92	$ 1,819.93	$ 1,874.52	$ 1,930.76	$ 1,988.68	$ 2,048.34	$ 2,109.79	$ 2,173.09	$ 2,238.28
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Dedicated Cloud - Public IP add-on	Per Month		CCSV13370152-A	N/A	N/A	A			$ 37.54	$ 38.66	$ 39.82	$ 41.02	$ 42.25	$ 43.52	$ 44.82	$ 46.17	$ 47.55	$ 48.98
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Virtual Cloud - Base Service	Per Month		CCSV13370153-A	N/A	N/A	A			$ 2,084.82	$ 2,147.37	$ 2,211.79	$ 2,278.14	$ 2,346.49	$ 2,416.88	$ 2,489.39	$ 2,564.07	$ 2,640.99	$ 2,720.22
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Virtual Cloud - Compute add-on (1-5 additional)	Per Month		CCSV13370154-A	N/A	N/A	A			$ 963.36	$ 992.26	$ 1,022.03	$ 1,052.69	$ 1,084.27	$ 1,116.80	$ 1,150.30	$ 1,184.81	$ 1,220.35	$ 1,256.96
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Virtual Cloud - Compute add-on (6-11 additional)	Per Month		CCSV13370155-A	N/A	N/A	A			$ 944.14	$ 972.46	$ 1,001.64	$ 1,031.69	$ 1,062.64	$ 1,094.52	$ 1,127.35	$ 1,161.17	$ 1,196.01	$ 1,231.89
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Virtual Cloud - Compute add-on (12-17 additional)	Per Month		CCSV13370156-A	N/A	N/A	A			$ 936.63	$ 964.73	$ 993.67	$ 1,023.48	$ 1,054.19	$ 1,085.81	$ 1,118.39	$ 1,151.94	$ 1,186.50	$ 1,222.09
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Virtual Cloud - Compute add-on (18-23 additional)	Per Month		CCSV13370157-A	N/A	N/A	A			$ 922.52	$ 950.19	$ 978.70	$ 1,008.06	$ 1,038.30	$ 1,069.45	$ 1,101.53	$ 1,134.58	$ 1,168.62	$ 1,203.68
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Virtual Cloud - Compute add-on (24 additional)	Per Month		CCSV13370158-A	N/A	N/A	A			$ 906.00	$ 933.18	$ 961.18	$ 990.01	$ 1,019.71	$ 1,050.30	$ 1,081.81	$ 1,114.27	$ 1,147.69	$ 1,182.12
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Virtual Cloud - Support add-on (1-5 additional)	Per Month		CCSV13370159-A	N/A	N/A	A			$ 192.79	$ 198.58	$ 204.53	$ 210.67	$ 216.99	$ 223.50	$ 230.20	$ 237.11	$ 244.22	$ 251.55
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Virtual Cloud - Support add-on (6-11 additional)	Per Month		CCSV13370160-A	N/A	N/A	A			$ 188.89	$ 194.55	$ 200.39	$ 206.40	$ 212.59	$ 218.97	$ 225.54	$ 232.31	$ 239.28	$ 246.46
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Virtual Cloud - Support add-on (12-17 additional)	Per Month		CCSV13370161-A	N/A	N/A	A			$ 173.27	$ 178.47	$ 183.82	$ 189.34	$ 195.02	$ 200.87	$ 206.90	$ 213.10	$ 219.50	$ 226.08
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Virtual Cloud - Support add-on (18-23 additional)	Per Month		CCSV13370162-A	N/A	N/A	A			$ 164.26	$ 169.19	$ 174.27	$ 179.49	$ 184.88	$ 190.43	$ 196.14	$ 202.02	$ 208.08	$ 214.33
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Virtual Cloud - Support add-on (24 additional)	Per Month		CCSV13370163-A	N/A	N/A	A			$ 157.66	$ 162.39	$ 167.26	$ 172.28	$ 177.44	$ 182.77	$ 188.25	$ 193.90	$ 199.71	$ 205.71
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Virtual Cloud - Storage add-on (1-5 additional)	Per Month		CCSV13370164-A	N/A	N/A	A			$ 510.51	$ 525.82	$ 541.60	$ 557.85	$ 574.58	$ 591.82	$ 609.57	$ 627.86	$ 646.70	$ 666.10
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Virtual Cloud - Storage add-on (6-11 additional)	Per Month		CCSV13370165-A	N/A	N/A	A			$ 486.48	$ 501.08	$ 516.11	$ 531.59	$ 547.54	$ 563.97	$ 580.89	$ 598.31	$ 616.26	$ 634.75
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Virtual Cloud - Storage add-on (12-17 additional)	Per Month		CCSV13370166-A	N/A	N/A	A			$ 459.46	$ 473.24	$ 487.44	$ 502.06	$ 517.12	$ 532.64	$ 548.62	$ 565.07	$ 582.03	$ 599.49

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	Product Name	Unit	Qty per config	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Virtual Cloud - Storage add-on (18 additional)	Per Month		CCSV13370167-A	N/A	N/A	A			$ 435.43	$ 448.50	$ 461.95	$ 475.81	$ 490.00	$ 504.79	$ 519.93	$ 535.53	$ 551.59	$ 568.14
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Virtual Cloud - Bandwidth add-on	Per Month		CCSV13370168-A	N/A	N/A	A			$ 343.09	$ 353.38	$ 363.99	$ 374.90	$ 386.15	$ 397.74	$ 409.67	$ 421.96	$ 434.62	$ 447.66
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Virtual Cloud - Public IP add-on	Per Month		CCSV13370169-A	N/A	N/A	A			$ 37.54	$ 38.66	$ 39.82	$ 41.02	$ 42.25	$ 43.52	$ 44.82	$ 46.17	$ 47.55	$ 48.98
Identity and Access Management Service	Active Directory Support - Small	Per Month		CCSU13370170-A	N/A	N/A	A			$ 2 634.83	$ 2 713.87	$ 2 795.29	$ 2 879.15	$ 2 965.52	$ 3 054.49	$ 3 146.12	$ 3 240.51	$ 3 337.72	$ 3 437.85
Identity and Access Management Service	Active Directory Support - Medium	Per Month		CCSU13370171-A	N/A	N/A	A			$ 4 391.38	$ 4 523.12	$ 4 658.81	$ 4 798.58	$ 4 942.54	$ 5 090.81	$ 5 243.54	$ 5 400.84	$ 5 562.87	$ 5 729.75
Identity and Access Management Service	Active Directory Support - Large	Per Month		CCSU13370172-A	N/A	N/A	A			$ 13 174.14	$ 13 569.36	$ 13 976.44	$ 14 395.74	$ 14 827.61	$ 15 272.44	$ 15 730.61	$ 16 202.53	$ 16 688.60	$ 17 189.26
Identity and Access Management Service	Active Directory Support - Very Large	Per Month		CCSU13370173-A	N/A	N/A	A			$ 27,995.04	$ 28,834.90	$ 29,699.94	$ 30,590.94	$ 31,508.67	$ 32,453.93	$ 33,427.55	$ 34,430.37	$ 35,463.28	$ 36,527.18
Identity and Access Management Service	PKI Support - Small	Per Month		CCSU13370174-A	N/A	N/A	A			$ 2,634.83	$ 2,713.87	$ 2,795.29	$ 2,879.15	$ 2,965.52	$ 3,054.49	$ 3,146.12	$ 3,240.51	$ 3,337.72	$ 3,437.85
Identity and Access Management Service	PKI Support - Medium	Per Month		CCSU13370175-A	N/A	N/A	A			$ 6 587.07	$ 6 784.68	$ 6 988.22	$ 7 197.87	$ 7 413.80	$ 7 636.22	$ 7 865.31	$ 8 101.26	$ 8 344.30	$ 8 594.63
Identity and Access Management Service	PKI Support - Large	Per Month		CCSU13370176-A	N/A	N/A	A			$ 13 174.14	$ 13 569.36	$ 13 976.44	$ 14 395.74	$ 14 827.61	$ 15 272.44	$ 15 730.61	$ 16 202.53	$ 16 688.60	$ 17 189.26
Business Continuity and Disaster Recovery	Development of Data Center Disaster Recovery Plan	Per Plan		CCSI13370177-A	N/A	N/A	A			$ 33,800.00	$ 34,814.00	$ 35,858.42	$ 36,934.17	$ 38,042.20	$ 39,183.46	$ 40,358.97	$ 41,569.74	$ 42,816.83	$ 44,101.33
Business Continuity and Disaster Recovery	Business Impact Assessment Workshop	Per Workshop		CCSI13370178-A	N/A	N/A	A			$ 33 800.00	$ 34 814.00	$ 35 858.42	$ 36 934.17	$ 38 042.20	$ 39 183.46	$ 40 358.97	$ 41 569.74	$ 42 816.83	$ 44 101.33
Business Continuity and Disaster Recovery	Resilient Strategy Development Workshop	Per Workshop		CCSI13370179-A	N/A	N/A	A			$ 124 500.00	$ 128 235.00	$ 132 082.05	$ 136 044.51	$ 140 125.85	$ 144 329.62	$ 148 659.51	$ 153 119.30	$ 157 712.88	$ 162 444.26
Business Continuity and Disaster Recovery	Labor for Tier 3 to Tier 6 DR Service Testing (Disk-based)	Per Server		CCSU13370180-A	N/A	N/A	A			$ 214.16	$ 220.58	$ 227.20	$ 234.02	$ 241.04	$ 248.27	$ 255.72	$ 263.39	$ 271.29	$ 279.43
Business Continuity and Disaster Recovery	Labor for Tier 1 & Tier 2 DR Service Testing (Tape-based)	Per Server		CCSU13370181-A	N/A	N/A	A			$ 917.41	$ 944.93	$ 973.28	$ 1,002.48	$ 1,032.55	$ 1,063.53	$ 1,095.43	$ 1,128.29	$ 1,162.14	$ 1,197.01
Business Continuity and Disaster Recovery	DR Config-1 Storage	Per GB		CCSU13370182-A	N/A	N/A	A			$ 0.06	$ 0.05	$ 0.05	$ 0.05	$ 0.05	$ 0.04	$ 0.04	$ 0.04	$ 0.03	$ 0.03
Business Continuity and Disaster Recovery	DR Config-2 Storage	Per GB		CCSU13370183-A	N/A	N/A	A			$ 0.24	$ 0.24	$ 0.24	$ 0.23	$ 0.23	$ 0.23	$ 0.23	$ 0.21	$ 0.19	$ 0.17
Business Continuity and Disaster Recovery	Tape Library Resources to 100,000 GB to Tier1 DR RTO	Per GB of Protected Data		CCSU13370184-A	N/A	N/A	A			$ 0.13	$ 0.13	$ 0.13	$ 0.13	$ 0.13	$ 0.13	$ 0.13	$ 0.13	$ 0.13	$ 0.13
Business Continuity and Disaster Recovery	Tape Library Resources to 100,000 GB to Tier2 DR RTO	Per GB of Protected Data		CCSU13370185-A	N/A	N/A	A			$ 0.58	$ 0.58	$ 0.58	$ 0.58	$ 0.58	$ 0.58	$ 0.58	$ 0.58	$ 0.58	$ 0.58
Business Continuity and Disaster Recovery	Backup to Disk for 255,000 GBs of deduplicated data	Per Gb of Protected Data		CCSU13370186-A	N/A	N/A	A			$ 0.01	$ 0.01	$ 0.01	$ 0.01	$ 0.01	$ 0.01	$ 0.01	$ 0.01	$ 0.01	$ 0.01
Business Continuity and Disaster Recovery	Mainframe Services: EMC RecoverPoint Data Replication for 27,000 GBs of VMAX10K Storage	Per GB of Replicated Data		CCSU13370187-A	N/A	N/A	A			$ 0.12	$ 0.12	$ 0.12	$ 0.12	$ 0.12	$ 0.10	$ 0.10	$ 0.10	$ 0.10	$ 0.10
Business Continuity and Disaster Recovery	EMC RecoverPoint SnapShot & Replication for 32,256 GBs of Config2 Storage	Per GB of Replicated Data		CCSU13370188-A	N/A	N/A	A			$ 0.03	$ 0.03	$ 0.03	$ 0.03	$ 0.03	$ 0.47	$ 0.48	$ 0.50	$ 0.51	$ 0.52
Business Continuity and Disaster Recovery	EMC RecoverPoint SnapShot & Replication for 84,700 GBs of Config1 Storage	Per GB of Replicated Data		CCSU13370189-A	N/A	N/A	A			$ 0.01	$ 0.01	$ 0.01	$ 0.01	$ 0.01	$ 0.01	$ 0.01	$ 0.01	$ 0.01	$ 0.01
Business Continuity and Disaster Recovery	Mainframe Services: EMC SRDF Data Replication for 50 000 GB of VMAX Storage	Per GB of Replicated Data		CCSU13370190-A	N/A	N/A	A			$ 173.75	$ 173.75	$ 173.75	$ 173.75	$ 173.75	$ 138.80	$ 138.80	$ 138.80	$ 138.80	$ 138.80
Business Continuity and Disaster Recovery	Open Systems Services: EMC VPlex Metro Replication for 150,000 GBs	Per GB of Replicated Data		CCSU13370192-A	N/A	N/A	A			$ 0.11	$ 0.11	$ 0.11	$ 0.11	$ 0.11	$ 0.09	$ 0.09	$ 0.09	$ 0.09	$ 0.09
Business Continuity and Disaster Recovery	SAN Switch Port, purchased in pairs, for SAN-attached Servers	Per SAN Port		CCSU13370193-A	N/A	N/A	A			$ 47.31	$ 47.31	$ 47.31	$ 47.31	$ 47.31	$ 34.90	$ 34.90	$ 34.90	$ 34.90	$ 34.90
Business Continuity and Disaster Recovery	IBM Storwize V7000 Disaster Recovery System	Per System	1	CCSI13370564-A	N/A	N/A	A			$ 204,532.91	$ 194,306.27	$ 184,590.95	$ 175,361.41	$ 166,593.34	$ 158,263.67	$ 150,350.49	$ 142,832.96	$ 135,691.31	$ 128,906.75
Business Continuity and Disaster Recovery	IBM XIV High Performance Disaster Recovery Tier	Per System	1	CCSI13370565-A	N/A	N/A	A			$ 549,408.13	$ 521,937.73	$ 495,840.84	$ 471,048.80	$ 447,496.36	$ 425,121.54	$ 403,865.46	$ 383,672.19	$ 364,488.58	$ 346,264.15
Application Performance Monitoring Services	Application Performance Monitoring Service - Setup – Small	Per Application		CCSU13370194-A	N/A	N/A	A			$ 1,435.84	$ 1,478.92	$ 1,523.28	$ 1,568.98	$ 1,616.05	$ 1,664.53	$ 1,714.47	$ 1,765.90	$ 1,818.88	$ 1,873.45
Application Performance Monitoring Services	Application Performance Monitoring Service - Setup – Medium	Per Application		CCSU13370195-A	N/A	N/A	A			$ 2,153.76	$ 2,218.38	$ 2,284.93	$ 2,353.47	$ 2,424.08	$ 2,496.80	$ 2,571.70	$ 2,648.86	$ 2,728.32	$ 2,810.17
Application Performance Monitoring Services	Application Performance Monitoring Service - Setup - Large	Per Application		CCSU13370196-A	N/A	N/A	A			$ 2,871.68	$ 2,957.83	$ 3,046.57	$ 3,137.97	$ 3,232.10	$ 3,329.07	$ 3,428.94	$ 3,531.81	$ 3,637.76	$ 3,746.89
Application Performance Monitoring Services	Application Performance Monitoring Service - Ongoing Support – Small	Per Application		CCSU13370197-A	N/A	N/A	A			$ 208.15	$ 214.40	$ 220.83	$ 227.45	$ 234.28	$ 241.30	$ 248.54	$ 256.00	$ 263.68	$ 271.59
Application Performance Monitoring Services	Application Performance Monitoring Service - Ongoing Support – Medium	Per Application		CCSU13370198-A	N/A	N/A	A			$ 316.18	$ 325.66	$ 335.43	$ 345.50	$ 355.86	$ 366.54	$ 377.53	$ 388.86	$ 400.53	$ 412.54
Application Performance Monitoring Services	Application Performance Monitoring Service - Ongoing Support - Large	Per Application		CCSU13370199-A	N/A	N/A	A			$ 421.57	$ 434.22	$ 447.25	$ 460.66	$ 474.48	$ 488.72	$ 503.38	$ 518.48	$ 534.04	$ 550.06
Application Capacity Management Services	Application Capacity Management - Setup – Small	Per Application		CCSU13370200-A	N/A	N/A	A			$ 5,025.45	$ 5,176.21	$ 5,331.49	$ 5,491.44	$ 5,656.18	$ 5,825.87	$ 6,000.64	$ 6,180.66	$ 6,366.08	$ 6,557.07
Application Capacity Management Services	Application Capacity Management - Setup – Medium	Per Application		CCSU13370201-A	N/A	N/A	A			$ 9,332.97	$ 9,612.96	$ 9,901.35	$ 10,198.39	$ 10,504.34	$ 10,819.47	$ 11,144.05	$ 11,478.38	$ 11,822.73	$ 12,177.41
Application Capacity Management Services	Application Capacity Management – Setup - Large	Per Application		CCSU13370202-A	N/A	N/A	A			$ 13 640.49	$ 14 049.71	$ 14 471.20	$ 14 905.34	$ 15 352.50	$ 15 813.07	$ 16 287.46	$ 16 776.09	$ 17 279.37	$ 17 797.75
Application Capacity Management Services	Application Capacity Management - Ongoing Support – Small	Per Application		CCSU13370203-A	N/A	N/A	A			$ 1,470.01	$ 1,500.78	$ 1,532.29	$ 1,564.56	$ 1,597.60	$ 1,631.43	$ 1,666.08	$ 1,701.56	$ 1,737.89	$ 1,775.09
Application Capacity Management Services	Application Capacity Management - Ongoing Support – Medium	Per Application		CCSU13370204-A	N/A	N/A	A			$ 41.70	$ 42.58	$ 43.47	$ 44.39	$ 45.32	$ 46.28	$ 47.27	$ 48.27	$ 49.30	$ 50.36
Application Capacity Management Services	Application Capacity Management – Ongoing Support - Large	Per Application		CCSU13370205-A	N/A	N/A	A			$ 1,449.16	$ 1,479.49	$ 1,510.56	$ 1,542.36	$ 1,574.94	$ 1,608.29	$ 1,642.45	$ 1,677.42	$ 1,713.24	$ 1,749.91
Application Capacity Management Services	Application Capacity Management - Appdynamics Agent License – Small	Per Application		CCSU13370555-A	N/A	N/A	A			$ 31,041.64	$ 31,972.89	$ 32,932.08	$ 33,920.04	$ 34,937.64	$ 35,985.77	$ 37,065.35	$ 38,177.31	$ 39,322.63	$ 40,502.31
Application Capacity Management Services	Application Capacity Management - Appdynamics Agent License – Medium	Per Application		CCSU13370556-A	N/A	N/A	A			$ 58,865.32	$ 60,631.28	$ 62,450.22	$ 64,323.72	$ 66,253.43	$ 68,241.04	$ 70,288.27	$ 72,396.92	$ 74,568.82	$ 76,805.89
Application Capacity Management Services	Application Capacity Management – Appdynamics Agent License - Large	Per Application		CCSU13370557-A	N/A	N/A	A			$ 103,602.96	$ 106,711.05	$ 109,912.38	$ 113,209.75	$ 116,606.04	$ 120,104.22	$ 123,707.35	$ 127,418.57	$ 131,241.13	$ 135,178.36

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	Product Name	Unit	Qty per config	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Application Architecture	Review Application Architecture - Small	Per Assessment		CCSD13370206-A	N/A	N/A	A			$ 34,597.07	$ 35,634.98	$ 36,704.03	$ 37,805.15	$ 38,939.31	$ 40,107.49	$ 41,310.71	$ 42,550.03	$ 43,826.53	$ 45,141.33
Application Architecture	Review Application Architecture - Medium	Per Assessment		CCSD13370207-A	N/A	N/A	A			$ 83 032.97	$ 85 523.96	$ 88 089.67	$ 90 732.36	$ 93 454.34	$ 96 257.97	$ 99 145.70	$ 102 120.08	$ 105 183.68	$ 108 339.19
Application Architecture	Review Application Architecture - Large	Per Assessment		CCSD13370208-A	N/A	N/A	A			$ 166 065.93	$ 171 047.91	$ 176 179.35	$ 181 464.73	$ 186 908.67	$ 192 515.93	$ 198 291.41	$ 204 240.15	$ 210 367.36	$ 216 678.38
Application Assessment	Application Performance Impact Assessment (Follow-on for 5 applications)	Per Assessment		CCSI13370209-A	N/A	N/A	A			$ 125,000.00	$ 128,750.00	$ 132,612.50	$ 136,590.88	$ 140,688.60	$ 144,909.26	$ 149,256.54	$ 153,734.23	$ 158,346.26	$ 163,096.65
Application Assessment	Open System Database Performance Assessment - Small (Up to 100 objects)	Per Assessment		CCSD13370210-A	N/A	N/A	A			$ 4,843.59	$ 4,988.90	$ 5,138.56	$ 5,292.72	$ 5,451.50	$ 5,615.05	$ 5,783.50	$ 5,957.00	$ 6,135.71	$ 6,319.79
Application Assessment	Open System Database Performance Assessment - Medium (Up to 500 objects)	Per Assessment		CCSD13370211-A	N/A	N/A	A			$ 6,919.41	$ 7,127.00	$ 7,340.81	$ 7,561.03	$ 7,787.86	$ 8,021.50	$ 8,262.14	$ 8,510.01	$ 8,765.31	$ 9,028.27
Application Assessment	Open System Database Performance Assessment - Large (Up to 1,000 objects)	Per Assessment		CCSD13370212-A	N/A	N/A	A			$ 10,379.12	$ 10,690.49	$ 11,011.21	$ 11,341.55	$ 11,681.79	$ 12,032.25	$ 12,393.21	$ 12,765.01	$ 13,147.96	$ 13,542.40
Application Assessment	Open System Configuration Management Assessment - Small (Up to 10 Application Pages)	Per Assessment		CCSD13370213-A	N/A	N/A	A			$ 4,843.59	$ 4,988.90	$ 5,138.56	$ 5,292.72	$ 5,451.50	$ 5,615.05	$ 5,783.50	$ 5,957.00	$ 6,135.71	$ 6,319.79
Application Assessment	Open System Configuration Management Assessment - Medium (Up to 25 Application Pages)	Per Assessment		CCSD13370214-A	N/A	N/A	A			$ 6,919.41	$ 7,127.00	$ 7,340.81	$ 7,561.03	$ 7,787.86	$ 8,021.50	$ 8,262.14	$ 8,510.01	$ 8,765.31	$ 9,028.27
Application Assessment	Open System Configuration Management Assessment - Small (Up to 50 Application Pages)	Per Assessment		CCSD13370215-A	N/A	N/A	A			$ 10,379.12	$ 10,690.49	$ 11,011.21	$ 11,341.55	$ 11,681.79	$ 12,032.25	$ 12,393.21	$ 12,765.01	$ 13,147.96	$ 13,542.40
Application Assessment	Mobile Wireframe Assessment - Small (Up to 10 Pages)	Per Assessment		CCSD13370216-A	N/A	N/A	A			$ 48,435.90	$ 49,888.97	$ 51,385.64	$ 52,927.21	$ 54,515.03	$ 56,150.48	$ 57,834.99	$ 59,570.04	$ 61,357.15	$ 63,197.86
Application Assessment	Mobile Wireframe Assessment - Medium (Up to 25 Pages)	Per Assessment		CCSD13370217-A	N/A	N/A	A			$ 69,194.14	$ 71,269.96	$ 73,408.06	$ 75,610.30	$ 77,878.61	$ 80,214.97	$ 82,621.42	$ 85,100.06	$ 87,653.07	$ 90,282.66
Application Assessment	Mobile Wireframe Assessment - Small (Up to 50 Pages)	Per Assessment		CCSD13370218-A	N/A	N/A	A			$ 103,791.21	$ 106,904.94	$ 110,112.09	$ 113,415.46	$ 116,817.92	$ 120,322.46	$ 123,932.13	$ 127,650.09	$ 131,479.60	$ 135,423.99
Application Assessment	Application Management Innovation Workshop	Per Workshop		CCSU13370219-A	N/A	N/A	A			$ 71 311.48	$ 73 450.82	$ 75 654.35	$ 77 923.98	$ 80 261.70	$ 82 669.55	$ 85 149.64	$ 87 704.13	$ 90 335.25	$ 93 045.31
Application Assessment	Application Modernization Assessment - 1 Week	Per Assessment		CCSU13370220-A	N/A	N/A	A			$ 113 893.55	$ 117 310.36	$ 120 829.67	$ 124 454.56	$ 128 188.20	$ 132 033.84	$ 135 994.86	$ 140 074.70	$ 144 276.95	$ 148 605.25
Application Assessment	Application Modernization Assessment - 4 Week	Per Assessment		CCSU13370221-A	N/A	N/A	A			$ 298,199.06	$ 307,145.03	$ 316,359.38	$ 325,850.17	$ 335,625.67	$ 345,694.44	$ 356,065.27	$ 366,747.23	$ 377,749.65	$ 389,082.14
Application Testing Services	Test Assessment	Per Assessment		CCSD13370222-A	N/A	N/A	A			$ 30,445.42	$ 31,358.78	$ 32,299.55	$ 33,268.53	$ 34,266.59	$ 35,294.59	$ 36,353.43	$ 37,444.03	$ 38,567.35	$ 39,724.37
Application Testing Services	Test Estimation and Test Approach Planning	Per Assessment		CCSD13370223-A	N/A	N/A	A			$ 30 445.42	$ 31 358.78	$ 32 299.55	$ 33 268.53	$ 34 266.59	$ 35 294.59	$ 36 353.43	$ 37 444.03	$ 38 567.35	$ 39 724.37
Application Testing Services	System Integration and Acceptance Testing, UAT Support - Small	Per Request		CCSD13370224-A	N/A	N/A	A			$ 83,032.97	$ 85,523.96	$ 88,089.67	$ 90,732.36	$ 93,454.34	$ 96,257.97	$ 99,145.70	$ 102,120.08	$ 105,183.68	$ 108,339.19
Application Testing Services	System Integration and Acceptance Testing, UAT Support - Medium	Per Request		CCSD13370225-A	N/A	N/A	A			$ 276,776.56	$ 285,079.85	$ 293,632.25	$ 302,441.22	$ 311,514.45	$ 320,859.89	$ 330,485.68	$ 340,400.25	$ 350,612.26	$ 361,130.63
Application Testing Services	System Integration and Acceptance Testing, UAT Support - Large	Per Request		CCSD13370226-A	N/A	N/A	A			$ 415,164.83	$ 427,619.78	$ 440,448.37	$ 453,661.82	$ 467,271.68	$ 481,289.83	$ 495,728.52	$ 510,600.38	$ 525,918.39	$ 541,695.94
Application Testing Services	Automated Regression Testing - Small	Per Request		CCSD13370227-A	N/A	N/A	A			$ 13,838.83	$ 14,253.99	$ 14,681.61	$ 15,122.06	$ 15,575.72	$ 16,042.99	$ 16,524.28	$ 17,020.01	$ 17,530.61	$ 18,056.53
Application Testing Services	Automated Regression Testing - Medium	Per Request		CCSD13370228-A	N/A	N/A	A			$ 27,677.66	$ 28,507.99	$ 29,363.22	$ 30,244.12	$ 31,151.45	$ 32,085.99	$ 33,048.57	$ 34,040.03	$ 35,061.23	$ 36,113.06
Application Testing Services	Automated Regression Testing - Large	Per Request		CCSD13370229-A	N/A	N/A	A			$ 41 516.48	$ 42 761.98	$ 44 044.84	$ 45 366.18	$ 46 727.17	$ 48 128.98	$ 49 572.85	$ 51 060.04	$ 52 591.84	$ 54 169.59
Application Testing Services	Test Data Management - Small	Per Request		CCSD13370230-A	N/A	N/A	A			$ 27 677.66	$ 28 507.99	$ 29 363.22	$ 30 244.12	$ 31 151.45	$ 32 085.99	$ 33 048.57	$ 34 040.03	$ 35 061.23	$ 36 113.06
Application Testing Services	Test Data Management - Medium	Per Request		CCSD13370231-A	N/A	N/A	A			$ 41 516.48	$ 42 761.98	$ 44 044.84	$ 45 366.18	$ 46 727.17	$ 48 128.98	$ 49 572.85	$ 51 060.04	$ 52 591.84	$ 54 169.59
Application Testing Services	Test Data Management - Large	Per Request		CCSD13370232-A	N/A	N/A	A			$ 69,194.14	$ 71,269.96	$ 73,408.06	$ 75,610.30	$ 77,878.61	$ 80,214.97	$ 82,621.42	$ 85,100.06	$ 87,653.07	$ 90,282.66
Application Testing Services	ADA Compliance Testing - Small	Per Request		CCSD13370233-A	N/A	N/A	A			$ 13,838.83	$ 14,253.99	$ 14,681.61	$ 15,122.06	$ 15,575.72	$ 16,042.99	$ 16,524.28	$ 17,020.01	$ 17,530.61	$ 18,056.53
Application Testing Services	ADA Compliance Testing - Medium	Per Request		CCSD13370234-A	N/A	N/A	A			$ 27 677.66	$ 28 507.99	$ 29 363.22	$ 30 244.12	$ 31 151.45	$ 32 085.99	$ 33 048.57	$ 34 040.03	$ 35 061.23	$ 36 113.06
Application Testing Services	ADA Compliance Testing - Large	Per Request		CCSD13370235-A	N/A	N/A	A			$ 41 516.48	$ 42 761.98	$ 44 044.84	$ 45 366.18	$ 46 727.17	$ 48 128.98	$ 49 572.85	$ 51 060.04	$ 52 591.84	$ 54 169.59
Application Load/Availability Testing	Application Load Testing - Script Creation - Small (Up to 20 Application Pages)	Per Script		CCSD13370236-A	N/A	N/A	A			$ 20,758.24	$ 21,380.99	$ 22,022.42	$ 22,683.09	$ 23,363.58	$ 24,064.49	$ 24,786.43	$ 25,530.02	$ 26,295.92	$ 27,084.80
Application Load/Availability Testing	Application Load Testing - Script Creation - Medium (Up to 50 Application Pages)	Per Script		CCSD13370237-A	N/A	N/A	A			$ 58,123.08	$ 59,866.77	$ 61,662.77	$ 63,512.66	$ 65,418.03	$ 67,380.58	$ 69,401.99	$ 71,484.05	$ 73,628.57	$ 75,837.43
Application Load/Availability Testing	Application Load Testing - Script Creation - Large (Up to 100 Application Pages)	Per Script		CCSD13370238-A	N/A	N/A	A			$ 166,065.93	$ 171,047.91	$ 176,179.35	$ 181,464.73	$ 186,908.67	$ 192,515.93	$ 198,291.41	$ 204,240.15	$ 210,367.36	$ 216,678.38
Application Load/Availability Testing	Application Load Testing - Script Maintenance - Small (Up to 10 of Application Pages)	Per Script		CCSD13370239-A	N/A	N/A	A			$ 13,838.83	$ 14,253.99	$ 14,681.61	$ 15,122.06	$ 15,575.72	$ 16,042.99	$ 16,524.28	$ 17,020.01	$ 17,530.61	$ 18,056.53
Application Load/Availability Testing	Application Load Testing - Script Maintenance - Medium (Up To 25 of Application Pages)	Per Script		CCSD13370240-A	N/A	N/A	A			$ 34,597.07	$ 35,634.98	$ 36,704.03	$ 37,805.15	$ 38,939.31	$ 40,107.49	$ 41,310.71	$ 42,550.03	$ 43,826.53	$ 45,141.33
Application Load/Availability Testing	Application Load Testing - Script Maintenance - Large (Up to 50 Application Pages)	Per Script		CCSD13370241-A	N/A	N/A	A			$ 62,274.73	$ 64,142.97	$ 66,067.26	$ 68,049.27	$ 70,090.75	$ 72,193.47	$ 74,359.28	$ 76,590.06	$ 78,887.76	$ 81,254.39
Application Load/Availability Testing	Application Load Testing - Execution and Analysis - Small (Up to 25 Application Test Scripts)	Per Test		CCSD13370242-A	N/A	N/A	A			$ 13,838.83	$ 14,253.99	$ 14,681.61	$ 15,122.06	$ 15,575.72	$ 16,042.99	$ 16,524.28	$ 17,020.01	$ 17,530.61	$ 18,056.53
Application Load/Availability Testing	Application Load Testing - Execution and Analysis - Medium (Up to 50 Application Test Scripts)	Per Test		CCSD13370243-A	N/A	N/A	A			$ 20,758.24	$ 21,380.99	$ 22,022.42	$ 22,683.09	$ 23,363.58	$ 24,064.49	$ 24,786.43	$ 25,530.02	$ 26,295.92	$ 27,084.80
Application Load/Availability Testing	Application Load Testing - Execution and Analysis - Large (100 Application Test Scripts)	Per Test		CCSD13370244-A	N/A	N/A	A			$ 27,677.66	$ 28,507.99	$ 29,363.22	$ 30,244.12	$ 31,151.45	$ 32,085.99	$ 33,048.57	$ 34,040.03	$ 35,061.23	$ 36,113.06
Application Load/Availability Testing	Synthetic Transaction Modeling - Small	Per Test		CCSD13370245-A	N/A	N/A	A			$ 13,838.83	$ 14,253.99	$ 14,681.61	$ 15,122.06	$ 15,575.72	$ 16,042.99	$ 16,524.28	$ 17,020.01	$ 17,530.61	$ 18,056.53
Application Load/Availability Testing	Synthetic Transaction Modeling - Medium	Per Test		CCSD13370246-A	N/A	N/A	A			$ 20 758.24	$ 21 380.99	$ 22 022.42	$ 22 683.09	$ 23 363.58	$ 24 064.49	$ 24 786.43	$ 25 530.02	$ 26 295.92	$ 27 084.80
Application Load/Availability Testing	Synthetic Transaction Modeling - Large	Per Test		CCSD13370247-A	N/A	N/A	A			$ 27 677.66	$ 28 507.99	$ 29 363.22	$ 30 244.12	$ 31 151.45	$ 32 085.99	$ 33 048.57	$ 34 040.03	$ 35 061.23	$ 36 113.06
Middleware Service	WebSphere Build p-Series Standard (1 server)	Per Request		CCSI13370255-A	N/A	N/A	A			$ 47,347.00	$ 48 767.41	$ 50 230.43	$ 51 737.35	$ 53 289.47	$ 54 888.15	$ 56 534.79	$ 58 230.84	$ 59 977.76	$ 61 777.10

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	Product Name	Unit	Qty per config	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Middleware Service	WebSphere Build p-Series Complex (2 servers)	Per Request		CCSI13370256-A	N/A	N/A	A			$ 85,363.00	$ 87,923.89	$ 90,561.61	$ 93,278.45	$ 96,076.81	$ 98,959.11	$ 101,927.89	$ 104,985.72	$ 108,135.29	$ 111,379.35
Middleware Service	WebSphere Upgrade p-Series Standard (1 server)	Per Request		CCSI13370257-A	N/A	N/A	A			$ 44 147.00	$ 45 471.41	$ 46 835.55	$ 48 240.62	$ 49 687.84	$ 51 178.47	$ 52 713.83	$ 54 295.24	$ 55 924.10	$ 57 601.82
Middleware Service	WebSphere Upgrade p-Series Complex (2 servers)	Per Request		CCSI13370258-A	N/A	N/A	A			$ 58 818.00	$ 60 582.54	$ 62 400.02	$ 64 272.02	$ 66 200.18	$ 68 186.18	$ 70 231.77	$ 72 338.72	$ 74 508.88	$ 76 744.15
Middleware Service	DataPower Quickstart Services	Per Request		CCSI13370259-A	N/A	N/A	A			$ 44,066.00	$ 45,387.98	$ 46,749.62	$ 48,152.11	$ 49,596.67	$ 51,084.57	$ 52,617.11	$ 54,195.62	$ 55,821.49	$ 57,496.14
Middleware Service	p-Series Support for WebSphere App Server (10 Instances)	Per Month		CCSI13370260-A	N/A	N/A	A			$ 28,415.00	$ 29,267.45	$ 30,145.47	$ 31,049.84	$ 31,981.33	$ 32,940.77	$ 33,929.00	$ 34,946.87	$ 35,995.27	$ 37,075.13
Middleware Service	p-Series Support for WebSphere App Server (25 Instances)	Per Month		CCSI13370261-A	N/A	N/A	A			$ 56,830.00	$ 58,534.90	$ 60,290.95	$ 62,099.68	$ 63,962.67	$ 65,881.55	$ 67,857.99	$ 69,893.73	$ 71,990.54	$ 74,150.26
Middleware Service	p-Series Support for WebSphere App Server (40 Instances)	Per Month		CCSI13370262-A	N/A	N/A	A			$ 85,245.00	$ 87,802.35	$ 90,436.42	$ 93,149.51	$ 95,944.00	$ 98,822.32	$ 101,786.99	$ 104,840.60	$ 107,985.82	$ 111,225.39
Middleware Service	p-Series Support for WebSphere MQ Queue Managers (40 Instances)	Per Month		CCSI13370263-A	N/A	N/A	A			$ 28,415.00	$ 29,267.45	$ 30,145.47	$ 31,049.84	$ 31,981.33	$ 32,940.77	$ 33,929.00	$ 34,946.87	$ 35,995.27	$ 37,075.13
Middleware Service	p-Series Support for WebSphere MQ Queue Managers (80 Instances)	Per Month		CCSI13370264-A	N/A	N/A	A			$ 56,830.00	$ 58,534.90	$ 60,290.95	$ 62,099.68	$ 63,962.67	$ 65,881.55	$ 67,857.99	$ 69,893.73	$ 71,990.54	$ 74,150.26
Middleware Service	p-Series Support for WebSphere MQ Queue Managers (120 Instances)	Per Month		CCSI13370265-A	N/A	N/A	A			$ 85,245.00	$ 87,802.35	$ 90,436.42	$ 93,149.51	$ 95,944.00	$ 98,822.32	$ 101,786.99	$ 104,840.60	$ 107,985.82	$ 111,225.39
Middleware Service	WebSphere Build z-Series Standard (1 subsystem without data sharing or clustering)	Per Month		CCSI13370266-A	N/A	N/A	A			$ 64,119.00	$ 66,042.57	$ 68,023.85	$ 70,064.56	$ 72,166.50	$ 74,331.49	$ 76,561.44	$ 78,858.28	$ 81,224.03	$ 83,660.75
Middleware Service	WebSphere Build z-Series Complex (2 subsystems with data sharing and clustering across multiple CECs)	Per Month		CCSI13370267-A	N/A	N/A	A			$ 71,489.00	$ 73,633.67	$ 75,842.68	$ 78,117.96	$ 80,461.50	$ 82,875.34	$ 85,361.60	$ 87,922.45	$ 90,560.13	$ 93,276.93
Middleware Service	WebSphere Upgrade z-Series Standard (1 subsystem without data sharing or clustering)	Per Request		CCSI13370268-A	N/A	N/A	A			$ 53,802.00	$ 55,416.06	$ 57,078.54	$ 58,790.90	$ 60,554.62	$ 62,371.26	$ 64,242.40	$ 66,169.67	$ 68,154.76	$ 70,199.41
Middleware Service	WebSphere Upgrade z-Series Complex (2 subsystems with data sharing and clustering across multiple CECs)	Per Request		CCSI13370269-A	N/A	N/A	A			$ 65,594.00	$ 67,561.82	$ 69,588.67	$ 71,676.33	$ 73,826.62	$ 76,041.42	$ 78,322.67	$ 80,672.35	$ 83,092.52	$ 85,585.29
Middleware Service	z-Series Support for WebSphere App Server (10 Instances)	Per Month		CCSI13370272-A	N/A	N/A	A			$ 25,890.00	$ 26,666.70	$ 27,466.70	$ 28,290.70	$ 29,139.42	$ 30,013.61	$ 30,914.01	$ 31,841.43	$ 32,796.68	$ 33,780.58
Middleware Service	z-Series Support for WebSphere App Server (25 Instances)	Per Month		CCSI13370273-A	N/A	N/A	A			$ 51,775.00	$ 53,328.25	$ 54,928.10	$ 56,575.94	$ 58,273.22	$ 60,021.42	$ 61,822.06	$ 63,676.72	$ 65,587.02	$ 67,554.63
Middleware Service	z-Series Support for WebSphere App Server (40 Instances)	Per Month		CCSI13370274-A	N/A	N/A	A			$ 77,660.00	$ 79,989.80	$ 82,389.49	$ 84,861.18	$ 87,407.01	$ 90,029.22	$ 92,730.10	$ 95,512.00	$ 98,377.36	$ 101,328.69
Middleware Service	z-Series Support for WebSphere MQ Queue Managers (40 Queue Managers)	Per Month		CCSI13370275-A	N/A	N/A	A			$ 25,890.00	$ 26,666.70	$ 27,466.70	$ 28,290.70	$ 29,139.42	$ 30,013.61	$ 30,914.01	$ 31,841.43	$ 32,796.68	$ 33,780.58
Middleware Service	z-Series Support for WebSphere MQ Queue Managers (80 Queue Managers)	Per Month		CCSI13370276-A	N/A	N/A	A			$ 51,775.00	$ 53,328.25	$ 54,928.10	$ 56,575.94	$ 58,273.22	$ 60,021.42	$ 61,822.06	$ 63,676.72	$ 65,587.02	$ 67,554.63
Middleware Service	z-Series Support for WebSphere MQ Queue Managers (120 Queue Managers)	Per Month		CCSI13370277-A	N/A	N/A	A			$ 77,660.00	$ 79,989.80	$ 82,389.49	$ 84,861.18	$ 87,407.01	$ 90,029.22	$ 92,730.10	$ 95,512.00	$ 98,377.36	$ 101,328.69
Application User Experience	User Experience Strategy - Small	Per Request		CCSD13370278-A	N/A	N/A	A			$ 27 677.66	$ 28 507.99	$ 29 363.22	$ 30 244.12	$ 31 151.45	$ 32 085.99	$ 33 048.57	$ 34 040.03	$ 35 061.23	$ 36 113.06
Application User Experience	User Experience Strategy - Medium	Per Request		CCSD13370279-A	N/A	N/A	A			$ 62 274.73	$ 64 142.97	$ 66 067.26	$ 68 049.27	$ 70 090.75	$ 72 193.47	$ 74 359.28	$ 76 590.06	$ 78 887.76	$ 81 254.39
Application User Experience	User Experience Strategy - Large	Per Request		CCSD13370280-A	N/A	N/A	A			$ 124,549.45	$ 128,285.93	$ 132,134.51	$ 136,098.55	$ 140,181.50	$ 144,386.95	$ 148,718.56	$ 153,180.11	$ 157,775.52	$ 162,508.78
Application User Experience	User Experience Design - Small	Per Request		CCSD13370281-A	N/A	N/A	A			$ 41,516.48	$ 42,761.98	$ 44,044.84	$ 45,366.18	$ 46,727.17	$ 48,128.98	$ 49,572.85	$ 51,060.04	$ 52,591.84	$ 54,169.59
Application User Experience	User Experience Design - Medium	Per Request		CCSD13370282-A	N/A	N/A	A			$ 88 568.50	$ 91 225.55	$ 93 962.32	$ 96 781.19	$ 99 684.62	$ 102 675.16	$ 105 755.42	$ 108 928.08	$ 112 195.92	$ 115 561.80
Application User Experience	User Experience Design - Large	Per Request		CCSD13370283-A	N/A	N/A	A			$ 166 065.93	$ 171 047.91	$ 176 179.35	$ 181 464.73	$ 186 908.67	$ 192 515.93	$ 198 291.41	$ 204 240.15	$ 210 367.36	$ 216 678.38
Application User Experience	User Experience Prototype Development - Small	Per Request		CCSD13370284-A	N/A	N/A	A			$ 27,677.66	$ 28,507.99	$ 29,363.22	$ 30,244.12	$ 31,151.45	$ 32,085.99	$ 33,048.57	$ 34,040.03	$ 35,061.23	$ 36,113.06
Application User Experience	User Experience Prototype Development - Medium	Per Request		CCSD13370285-A	N/A	N/A	A			$ 55,355.31	$ 57,015.97	$ 58,726.45	$ 60,488.24	$ 62,302.89	$ 64,171.98	$ 66,097.14	$ 68,080.05	$ 70,122.45	$ 72,226.13
Application User Experience	User Experience Prototype Development - Large	Per Request		CCSD13370286-A	N/A	N/A	A			$ 103 791.21	$ 106 904.94	$ 110 112.09	$ 113 415.46	$ 116 817.92	$ 120 322.46	$ 123 932.13	$ 127 650.09	$ 131 479.60	$ 135 423.99
Data Quality Management	Data Quality Management Assessment - Small	Per Assessment		CCSD13370287-A	N/A	N/A	A			$ 110 710.62	$ 114 031.94	$ 117 452.90	$ 120 976.49	$ 124 605.78	$ 128 343.95	$ 132 194.27	$ 136 160.10	$ 140 244.90	$ 144 452.25
Data Quality Management	Data Quality Management Assessment - Medium	Per Assessment		CCSD13370288-A	N/A	N/A	A			$ 196,511.35	$ 202,406.70	$ 208,478.90	$ 214,733.26	$ 221,175.26	$ 227,810.52	$ 234,644.83	$ 241,684.18	$ 248,934.70	$ 256,402.75
Data Quality Management	Data Quality Management Assessment - Large	Per Assessment		CCSD13370289-A	N/A	N/A	A			$ 243,563.37	$ 250,870.27	$ 258,396.38	$ 266,148.27	$ 274,132.72	$ 282,356.70	$ 290,827.40	$ 299,552.22	$ 308,538.79	$ 317,794.95
Data Quality Management	Data Quality Management Assessment - Very Large	Per Assessment		CCSD13370290-A	N/A	N/A	A			$ 290,615.38	$ 299,333.85	$ 308,313.86	$ 317,563.28	$ 327,090.17	$ 336,902.88	$ 347,009.97	$ 357,420.27	$ 368,142.87	$ 379,187.16
Information Management Strategy	Information Management Strategy - Small	Per Assessment		CCSD13370291-A	N/A	N/A	A			$ 110 710.62	$ 114 031.94	$ 117 452.90	$ 120 976.49	$ 124 605.78	$ 128 343.95	$ 132 194.27	$ 136 160.10	$ 140 244.90	$ 144 452.25
Information Management Strategy	Information Management Strategy - Medium	Per Assessment		CCSD13370292-A	N/A	N/A	A			$ 196,511.35	$ 202,406.70	$ 208,478.90	$ 214,733.26	$ 221,175.26	$ 227,810.52	$ 234,644.83	$ 241,684.18	$ 248,934.70	$ 256,402.75
Information Management Strategy	Information Management Strategy - Large	Per Assessment		CCSD13370293-A	N/A	N/A	A			$ 243,563.37	$ 250,870.27	$ 258,396.38	$ 266,148.27	$ 274,132.72	$ 282,356.70	$ 290,827.40	$ 299,552.22	$ 308,538.79	$ 317,794.95
Information Management Strategy	Information Management Strategy - Very Large	Per Assessment		CCSD13370294-A	N/A	N/A	A			$ 257 402.20	$ 265 124.26	$ 273 077.99	$ 281 270.33	$ 289 708.44	$ 298 399.69	$ 307 351.68	$ 316 572.23	$ 326 069.40	$ 335 851.48
Information Management Strategy	Information Management Full Implementation Lifecycle - Small	Per Assessment		CCSD13370295-A	N/A	N/A	A			$ 471,907.00	$ 486,064.21	$ 500,646.14	$ 515,665.52	$ 531,135.49	$ 547,069.55	$ 563,481.64	$ 580,386.09	$ 597,797.67	$ 615,731.60
Information Management Strategy	Information Management Full Implementation Lifecycle - Medium	Per Assessment		CCSD13370296-A	N/A	N/A	A			$ 532,798.23	$ 548,782.18	$ 565,245.64	$ 582,203.01	$ 599,669.10	$ 617,659.17	$ 636,188.95	$ 655,274.62	$ 674,932.86	$ 695,180.84
Information Management Strategy	Information Management Full Implementation Lifecycle - Large	Per Assessment		CCSD13370297-A	N/A	N/A	A			$ 624,135.07	$ 642,859.12	$ 662,144.89	$ 682,009.24	$ 702,469.52	$ 723,543.60	$ 745,249.91	$ 767,607.41	$ 790,635.63	$ 814,354.70
Information Management Strategy	Information Management Full Implementation Lifecycle - Very Large	Per Assessment		CCSD13370298-A	N/A	N/A	A			$ 745,917.52	$ 768,295.05	$ 791,343.90	$ 815,084.21	$ 839,536.74	$ 864,722.84	$ 890,664.53	$ 917,384.46	$ 944,906.00	$ 973,253.18
ERP Services	ERP Fit/Gap Analysis (4 week duration)	Per Assessment		CCSD13370299-A	N/A	N/A	A			$ 297,534.80	$ 306,460.84	$ 315,654.67	$ 325,124.31	$ 334,878.04	$ 344,924.38	$ 355,272.11	$ 365,930.27	$ 376,908.18	$ 388,215.43
ERP Services	ERP Product Selection	Per Assessment		CCSD13370300-A	N/A	N/A	A			$ 242 179.49	$ 249 444.87	$ 256 928.22	$ 264 636.06	$ 272 575.15	$ 280 752.40	$ 289 174.97	$ 297 850.22	$ 306 785.73	$ 315 989.30
ERP Services	ERP Security Review and Segregation of Duties Analysis - Small (Up to 25 users and roles)	Per Assessment		CCSD13370302-A	N/A	N/A	A			$ 58,815.02	$ 60,579.47	$ 62,396.85	$ 64,268.76	$ 66,196.82	$ 68,182.73	$ 70,228.21	$ 72,335.05	$ 74,505.11	$ 76,740.26
ERP Services	ERP Security Review and Segregation of Duties Analysis - Small (Up to 100 users and roles)	Per Assessment		CCSD13370303-A	N/A	N/A	A			$ 117,630.04	$ 121,158.94	$ 124,793.71	$ 128,537.52	$ 132,393.64	$ 136,365.45	$ 140,456.41	$ 144,670.11	$ 149,010.21	$ 153,480.52
ERP Services	ERP Security Review and Segregation of Duties Analysis - Small (Up to 500 users and roles)	Per Assessment		CCSD13370304-A	N/A	N/A	A			$ 204,814.65	$ 210,959.09	$ 217,287.86	$ 223,806.50	$ 230,520.69	$ 237,436.32	$ 244,559.40	$ 251,896.19	$ 259,453.07	$ 267,236.66

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	Product Name	Unit	Qty per config	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
ERP Services	ERP Governance Risk, and Compliance (GRC) Review - Small (Agency System Configuration and Parameters for 1 GRC Capability)	Per Assessment		CCSD13370305-A	N/A	N/A	A			$ 51,203.66	$ 52,739.77	$ 54,321.97	$ 55,951.62	$ 57,630.17	$ 59,359.08	$ 61,139.85	$ 62,974.05	$ 64,863.27	$ 66,809.17
ERP Services	ERP Governance Risk, and Compliance (GRC) Review - Medium (Agency System Configuration and Parameters for 3 GRC Capability)	Per Assessment		CCSD13370306-A	N/A	N/A	A			$ 94,104.03	$ 96,927.15	$ 99,834.96	$102,830.01	$105,914.91	$109,092.36	$ 112,365.13	$ 115,736.09	$ 119,208.17	$ 122,784.41
ERP Services	ERP Governance Risk, and Compliance (GRC) Review - Large (Agency System Configuration and Parameters for 5 GRC Capability)	Per Assessment		CCSD13370307-A	N/A	N/A	A			$ 131,468.86	$135,412.93	$139,475.32	$143,659.58	$147,969.36	$152,408.45	$ 156,980.70	$ 161,690.12	$ 166,540.82	$ 171,537.05
Communications Strategy	Stakeholder Analysis	Per Assessment		CCSD13370308-A	N/A	N/A	A			$ 55,355.31	$ 57,015.97	$ 58,726.45	$ 60,488.24	$ 62,302.89	$ 64,171.98	$ 66,097.14	$ 68,080.05	$ 70,122.45	$ 72,226.13
Communications Strategy	Communications Plan	Per Request		CCSD13370309-A	N/A	N/A	A			$ 110,710.62	$ 114,031.94	$ 117,452.90	$120,976.49	$124,605.78	$128,343.95	$ 132,194.27	$ 136,160.10	$ 140,244.90	$ 144,452.25
Communications Strategy	Communications Delivery	Per Request		CCSD13370310-A	N/A	N/A	A			$ 110 710.62	$ 114 031.94	$ 117 452.90	$120 976.49	$124 605.78	$128 343.95	$ 132 194.27	$ 136 160.10	$ 140 244.90	$ 144 452.25
Infrastructure Virtualization and Migration Services	Cirba Software for Application and Infrastructure Mapping (includes 6 months of Support)	Per Server Instance		CCSU13370311-A	N/A	N/A	A			$ 66.75	$ 68.75	$ 70.82	$ 72.94	$ 75.13	$ 77.38	$ 79.70	$ 82.09	$ 84.56	$ 87.09
Infrastructure Virtualization and Migration Services	Application and Infrastructure Mapping with CIRBA (Up to 100 Servers)	Per Request		CCSU13370312-A	N/A	N/A	A			$ 28,854.00	$ 29,719.62	$ 30,611.21	$ 31,529.54	$ 32,475.43	$ 33,449.69	$ 34,453.18	$ 35,486.78	$ 36,551.38	$ 37,647.93
Infrastructure Virtualization and Migration Services	Application and Infrastructure Mapping and Consolidation Planning with CIRBA (Up to 100 Servers)	Per Request		CCSU13370313-A	N/A	N/A	A			$ 33,309.33	$ 34,308.61	$ 35,337.87	$ 36,398.00	$ 37,489.94	$ 38,614.64	$ 39,773.08	$ 40,966.27	$ 42,195.26	$ 43,461.12
Data Center Facility Services	Security Cage - EDC - Small	Per Cage		CCSU13370501-A	N/A	N/A	A			$ 4,089.59	$ 3,264.76	$ 3,298.53	$ 3,333.31	$ 3,369.13	$ 3,406.03	$ 3,444.04	$ 3,483.18	$ 3,523.50	$ 3,565.03
Data Center Facility Services	Security Cage - EDC - Medium	Per Cage		CCSU13370502-A	N/A	N/A	A			$ 4 768.42	$ 3 806.12	$ 3 845.51	$ 3 886.09	$ 3 927.89	$ 3 970.93	$ 4 015.27	$ 4 060.95	$ 4 107.99	$ 4 156.44
Data Center Facility Services	Security Cage - EDC - Large	Per Cage		CCSU13370503-A	N/A	N/A	A			$ 7 483.74	$ 5 971.55	$ 6 033.46	$ 6 097.22	$ 6 162.90	$ 6 230.55	$ 6 300.23	$ 6 371.99	$ 6 445.92	$ 6 522.05
Data Center Facility Services	Security Cage - EDC - Very Large	Per Cage		CCSU13370504-A	N/A	N/A	A			$ 10 461.29	$ 8 344.23	$ 8 430.90	$ 8 520.17	$ 8 612.12	$ 8 706.82	$ 8 804.37	$ 8 904.85	$ 9 008.34	$ 9 114.93
Data Center Facility Services	Security Cage - [redacted] - Small	Per Cage		CCSU13370314-A	N/A	N/A	A			$ 1,347.29	$ 1,246.06	$ 1,281.75	$ 1,318.51	$ 1,356.37	$ 1,395.36	$ 1,435.53	$ 1,476.90	$ 1,519.52	$ 1,563.41
Data Center Facility Services	Security Cage - [redacted] - Medium	Per Cage		CCSU13370315-A	N/A	N/A	A			$ 1,569.07	$ 1,450.97	$ 1,492.60	$ 1,535.49	$ 1,579.66	$ 1,625.16	$ 1,672.02	$ 1,720.28	$ 1,770.00	$ 1,821.21
Data Center Facility Services	Security Cage - [redacted] - Large	Per Cage		CCSU13370316-A	N/A	N/A	A			$ 2 456.19	$ 2 270.60	$ 2 336.03	$ 2 403.42	$ 2 472.83	$ 2 544.33	$ 2 617.97	$ 2 693.81	$ 2 771.94	$ 2 852.41
Data Center Facility Services	Security Cage - [redacted] - Very Large	Per Cage		CCSU13370317-A	N/A	N/A	A			$ 3 422.72	$ 3 162.90	$ 3 254.50	$ 3 348.84	$ 3 446.02	$ 3 546.11	$ 3 649.21	$ 3 755.40	$ 3 864.77	$ 3 977.42
Data Center Facility Services	Security Cage - [redacted] - Small	Per Cage		CCSU13370318-A	N/A	N/A	A			$ 2,505.03	$ 5,581.82	$ 5,745.79	$ 5,914.67	$ 6,088.62	$ 6,267.79	$ 6,452.34	$ 6,642.42	$ 6,838.21	$ 7,039.87
Data Center Facility Services	Security Cage - [redacted] - Medium	Per Cage		CCSU13370319-A	N/A	N/A	A			$ 6,509.35	$ 6,509.35	$ 6,700.65	$ 6,897.68	$ 7,100.63	$ 7,309.66	$ 7,524.96	$ 7,746.72	$ 7,975.14	$ 8,210.41
Data Center Facility Services	Security Cage - [redacted] - Large	Per Cage		CCSU13370320-A	N/A	N/A	A			$ 10 219.49	$ 10 219.49	$ 10 520.10	$ 10 829.72	$ 11 148.64	$ 11 477.12	$ 11 815.45	$ 12 163.93	$ 12 522.87	$ 12 892.58
Data Center Facility Services	Security Cage - [redacted] - Very Large	Per Cage		CCSU13370321-A	N/A	N/A	A			$ 14 291.35	$ 14 291.35	$ 14 712.19	$ 15 145.67	$ 15 592.15	$ 16 052.02	$ 16 525.69	$ 17 013.56	$ 17 516.08	$ 18 033.67
Data Center Facility Services	Security Cage - EDC - Small - Setup	Per Cage		CCSU13370514-A	N/A	N/A	A			$ 2,923.18	$ 3,010.88	$ 3,101.20	$ 3,194.24	$ 3,290.07	$ 3,388.77	$ 3,490.43	$ 3,595.15	$ 3,703.00	$ 3,814.09
Data Center Facility Services	Security Cage - EDC - Medium - Setup	Per Cage		CCSU13370515-A	N/A	N/A	A			$ 4,384.77	$ 4,516.32	$ 4,651.81	$ 4,791.36	$ 4,935.10	$ 5,083.15	$ 5,235.65	$ 5,392.72	$ 5,554.50	$ 5,721.13
Data Center Facility Services	Security Cage - EDC - Large - Setup	Per Cage		CCSU13370516-A	N/A	N/A	A			$ 7 307.95	$ 7 527.19	$ 7 753.01	$ 7 985.60	$ 8 225.17	$ 8 471.92	$ 8 726.08	$ 8 987.86	$ 9 257.50	$ 9 535.22
Data Center Facility Services	Security Cage - EDC - Very Large - Setup	Per Cage		CCSU13370517-A	N/A	N/A	A			$ 14 615.91	$ 15 054.39	$ 15 506.02	$ 15 971.20	$ 16 450.33	$ 16 943.84	$ 17 452.16	$ 17 975.73	$ 18 515.00	$ 19 070.45
Data Center Facility Services	Security Cage - [redacted] - Small - Setup	Per Cage		CCSU13370518-A	N/A	N/A	A			$ 2,923.18	$ 3,010.88	$ 3,101.20	$ 3,194.24	$ 3,290.07	$ 3,388.77	$ 3,490.43	$ 3,595.15	$ 3,703.00	$ 3,814.09
Data Center Facility Services	Security Cage - [redacted] - Medium - Setup	Per Cage		CCSU13370519-A	N/A	N/A	A			$ 4,384.77	$ 4,516.32	$ 4,651.81	$ 4,791.36	$ 4,935.10	$ 5,083.15	$ 5,235.65	$ 5,392.72	$ 5,554.50	$ 5,721.13
Data Center Facility Services	Security Cage - [redacted] - Large - Setup	Per Cage		CCSU13370520-A	N/A	N/A	A			$ 7 307.95	$ 7 527.19	$ 7 753.01	$ 7 985.60	$ 8 225.17	$ 8 471.92	$ 8 726.08	$ 8 987.86	$ 9 257.50	$ 9 535.22
Data Center Facility Services	Security Cage - [redacted] - Very Large - Setup	Per Cage		CCSU13370521-A	N/A	N/A	A			$ 14 615.91	$ 15 054.39	$ 15 506.02	$ 15 971.20	$ 16 450.33	$ 16 943.84	$ 17 452.16	$ 17 975.73	$ 18 515.00	$ 19 070.45
Data Center Facility Services	Security Cage - [redacted] - Small - Setup	Per Cage		CCSU13370522-A	N/A	N/A	A			$ 2,923.18	$ 3,010.88	$ 3,101.20	$ 3,194.24	$ 3,290.07	$ 3,388.77	$ 3,490.43	$ 3,595.15	$ 3,703.00	$ 3,814.09
Data Center Facility Services	Security Cage - [redacted] - Medium - Setup	Per Cage		CCSU13370523-A	N/A	N/A	A			$ 4,384.77	$ 4,516.32	$ 4,651.81	$ 4,791.36	$ 4,935.10	$ 5,083.15	$ 5,235.65	$ 5,392.72	$ 5,554.50	$ 5,721.13
Data Center Facility Services	Security Cage - [redacted] - Large - Setup	Per Cage		CCSU13370524-A	N/A	N/A	A			$ 7 307.95	$ 7 527.19	$ 7 753.01	$ 7 985.60	$ 8 225.17	$ 8 471.92	$ 8 726.08	$ 8 987.86	$ 9 257.50	$ 9 535.22
Data Center Facility Services	Security Cage - [redacted] - Very Large - setup	Per Cage		CCSU13370525-A	N/A	N/A	A			$ 7 307.95	$ 7 527.19	$ 7 753.01	$ 7 985.60	$ 8 225.17	$ 8 471.92	$ 8 726.08	$ 8 987.86	$ 9 257.50	$ 9 535.22
Data Center Facility Services	Enclosed Network Security Conduit	Per Foot		CCSU13370322-A	N/A	N/A	A			$ 85.30	$ 85.30	$ 85.30	$ 85.30	$ 85.30	$ 85.30	$ 85.30	$ 85.30	$ 85.30	$ 85.30
Data Center Facility Services	Enclosed Security Cable Tray	Per Foot		CCSU13370323-A	N/A	N/A	A			$ 41.46	$ 41.46	$ 41.46	$ 41.46	$ 41.46	$ 41.46	$ 41.46	$ 41.46	$ 41.46	$ 41.46
Data Center Facility Services	Security Camera	Per Camera		CCSU13370324-A	N/A	N/A	A			$ 9 965.39	$ 9 965.39	$ 9 965.39	$ 9 965.39	$ 9 965.39	$ 9 965.39	$ 9 965.39	$ 9 965.39	$ 9 965.39	$ 9 965.39
Data Center Facility Services	Access Control Panel	Per Panel		CCSU13370325-A	N/A	N/A	A			$ 10 878.63	$ 10 878.63	$ 10 878.63	$ 10 878.63	$ 10 878.63	$ 10 878.63	$ 10 878.63	$ 10 878.63	$ 10 878.63	$ 10 878.63
Data Center Facility Services	Security Cabinet	Per Cabinet		CCSU13370326-A	N/A	N/A	A			$ 2 262.04	$ 2 262.04	$ 2 262.04	$ 2 262.04	$ 2 262.04	$ 2 262.04	$ 2 262.04	$ 2 262.04	$ 2 262.04	$ 2 262.04
Data Center Relocation Services	Lift and Ship of Server Hardware	Per Server		CCSU13370327-A	N/A	N/A	A			$ 3,377.81	$ 3,386.97	$ 3,396.35	$ 3,405.95	$ 3,415.79	$ 3,425.86	$ 3,436.17	$ 3,446.73	$ 3,457.54	$ 3,468.61
Data Center Relocation Services	Data Center Relocation Services	Per Request		CCSI13370328-A	N/A	N/A	A			$ 59,339.00	$ 61,119.17	$ 62,952.75	$ 64,841.33	$ 66,786.57	$ 68,790.16	$ 70,853.87	$ 72,979.49	$ 75,168.87	$ 77,423.94
Data Center Relocation Services	Transition Tools: EMC RecoverPoint Solution for migrations for 10,000 GB of SAN-attached Storage	Per GB		CCSU13370329-A	N/A	N/A	A			$ 1.23	$ 1.23	$ 1.23	$ 1.23	$ 1.23	$ 1.23	$ 1.23	$ 1.23	$ 1.23	$ 1.23
Network and Security Service	IPV6 Strategy	Per Assessment		CCSP13370330-A	N/A	N/A	A			$ 91,105.62	$ 93,838.78	$ 96,653.95	$ 99,553.57	$102,540.17	$105,616.38	$ 108,784.87	$ 112,048.42	$ 115,409.87	$ 118,872.17
Network and Security Service	LAN Switch install for new Managed Racks	Per Rack		CCSU13370331-A	N/A	N/A	A			$ 386.80	$ 398.40	$ 410.35	$ 422.66	$ 435.34	$ 448.40	$ 461.86	$ 475.71	$ 489.98	$ 504.68
Network and Security Service	VPN Planning - Business Partner	Per VPN Request		CCSU13370332-A	N/A	N/A	A			$ 2 243.50	$ 2 310.81	$ 2 380.13	$ 2 451.54	$ 2 525.08	$ 2 600.83	$ 2 678.86	$ 2 759.22	$ 2 842.00	$ 2 927.26
Network and Security Service	VPN Implementation - Business Partner	Per VPN Request		CCSU13370333-A	N/A	N/A	A			$ 2 243.50	$ 2 310.81	$ 2 380.13	$ 2 451.54	$ 2 525.08	$ 2 600.83	$ 2 678.86	$ 2 759.22	$ 2 842.00	$ 2 927.26
Network and Security Service	VPN Modification - Business Partner	Per VPN Request		CCSU13370334-A	N/A	N/A	A			$ 2,243.50	$ 2,310.81	$ 2,380.13	$ 2,451.54	$ 2,525.08	$ 2,600.83	$ 2,678.86	$ 2,759.22	$ 2,842.00	$ 2,927.26
Network and Security Service	VPN Decommission - Business Partner	Per VPN Request		CCSU13370335-A	N/A	N/A	A			$ 2,243.50	$ 2,310.81	$ 2,380.13	$ 2,451.54	$ 2,525.08	$ 2,600.83	$ 2,678.86	$ 2,759.22	$ 2,842.00	$ 2,927.26
Network and Security Service	VPN Planning - Agency	Per VPN Request		CCSU13370336-A	N/A	N/A	A			$ 2 243.50	$ 2 310.81	$ 2 380.13	$ 2 451.54	$ 2 525.08	$ 2 600.83	$ 2 678.86	$ 2 759.22	$ 2 842.00	$ 2 927.26
Network and Security Service	VPN Implementation - Agency	Per VPN Request		CCSU13370337-A	N/A	N/A	A			$ 2 243.50	$ 2 310.81	$ 2 380.13	$ 2 451.54	$ 2 525.08	$ 2 600.83	$ 2 678.86	$ 2 759.22	$ 2 842.00	$ 2 927.26
Network and Security Service	VPN Modification - Agency	Per VPN Request		CCSU13370338-A	N/A	N/A	A			$ 2 243.50	$ 2 310.81	$ 2 380.13	$ 2 451.54	$ 2 525.08	$ 2 600.83	$ 2 678.86	$ 2 759.22	$ 2 842.00	$ 2 927.26
Network and Security Service	VPN Decommission- Agency	Per VPN Request		CCSU13370339-A	N/A	N/A	A			$ 2,243.50	$ 2,310.81	$ 2,380.13	$ 2,451.54	$ 2,525.08	$ 2,600.83	$ 2,678.86	$ 2,759.22	$ 2,842.00	$ 2,927.26
Network and Security Service	Hardware Network Load Balancer - Design and Implement - Small	Per Request		CCSU13370340-A	N/A	N/A	A			$ 378.08	$ 389.43	$ 401.11	$ 413.14	$ 425.54	$ 438.30	$ 451.45	$ 465.00	$ 478.95	$ 493.31
Network and Security Service	Hardware Network Load Balancer - Design and Implement - Medium	Per Request		CCSU13370341-A	N/A	N/A	A			$ 604.93	$ 623.08	$ 641.78	$ 661.03	$ 680.86	$ 701.29	$ 722.32	$ 743.99	$ 766.31	$ 789.30
Network and Security Service	Hardware Network Load Balancer - Design and Implement - Large	Per Request		CCSU13370342-A	N/A	N/A	A			$ 907.40	$ 934.62	$ 962.66	$ 991.54	$ 1,021.29	$ 1,051.93	$ 1,083.49	$ 1,115.99	$ 1,149.47	$ 1,183.95
Network and Security Service	Hardware Network Load Balancer - Modify - Small	Per Request		CCSU13370343-A	N/A	N/A	A			$ 378.08	$ 389.43	$ 401.11	$ 413.14	$ 425.54	$ 438.30	$ 451.45	$ 465.00	$ 478.95	$ 493.31
Network and Security Service	Hardware Network Load Balancer - Modify - Medium	Per Request		CCSU13370344-A	N/A	N/A	A			$ 604.93	$ 623.08	$ 641.78	$ 661.03	$ 680.86	$ 701.29	$ 722.32	$ 743.99	$ 766.31	$ 789.30
Network and Security Service	Hardware Network Load Balancer - Modify - Large	Per Request		CCSU13370345-A	N/A	N/A	A			$ 907.40	$ 934.62	$ 962.66	$ 991.54	$ 1,021.29	$ 1,051.93	$ 1,083.49	$ 1,115.99	$ 1,149.47	$ 1,183.95

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	Product Name	Unit	Qty per config	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Network and Security Service	SSL Offloading on Network Load Balancer - Design and Implement	Per Request		CCSU13370346-A	N/A	N/A	A			$ 1,512.34	$ 1,557.71	$ 1,604.44	$ 1,652.57	$ 1,702.15	$ 1,753.21	$ 1,805.81	$ 1,859.98	$ 1,915.78	$ 1,973.26
Network and Security Service	SSL Offloading on Network Load Balancer - Modify	Per Request		CCSU13370349-A	N/A	N/A	A			$ 1 512.34	$ 1 557.71	$ 1 604.44	$ 1 652.57	$ 1 702.15	$ 1 753.21	$ 1 805.81	$ 1 859.98	$ 1 915.78	$ 1 973.26
Network and Security Service	Multi-Site Global Network Load Balancer - Design and Implement - Small	Per Request		CCSU13370352-A	N/A	N/A	A			$ 756.17	$ 778.85	$ 802.22	$ 826.29	$ 851.07	$ 876.61	$ 902.90	$ 929.99	$ 957.89	$ 986.63
Network and Security Service	Multi-Site Global Network Load Balancer - Design and Implement - Medium	Per Request		CCSU13370353-A	N/A	N/A	A			$ 1,134.25	$ 1,168.28	$ 1,203.33	$ 1,239.43	$ 1,276.61	$ 1,314.91	$ 1,354.36	$ 1,394.99	$ 1,436.84	$ 1,479.94
Network and Security Service	Multi-Site Global Network Load Balancer - Design and Implement - Large	Per Request		CCSU13370354-A	N/A	N/A	A			$ 1,512.34	$ 1,557.71	$ 1,604.44	$ 1,652.57	$ 1,702.15	$ 1,753.21	$ 1,805.81	$ 1,859.98	$ 1,915.78	$ 1,973.26
Network and Security Service	Multi-Site Global Network Load Balancer - Modify - Small	Per Request		CCSU13370355-A	N/A	N/A	A			$ 756.17	$ 778.85	$ 802.22	$ 826.29	$ 851.07	$ 876.61	$ 902.90	$ 929.99	$ 957.89	$ 986.63
Network and Security Service	Multi-Site Global Network Load Balancer - Modify - Medium	Per Request		CCSU13370356-A	N/A	N/A	A			$ 1,134.25	$ 1,168.28	$ 1,203.33	$ 1,239.43	$ 1,276.61	$ 1,314.91	$ 1,354.36	$ 1,394.99	$ 1,436.84	$ 1,479.94
Network and Security Service	Multi-Site Global Network Load Balancer - Modify - Large	Per Request		CCSU13370357-A	N/A	N/A	A			$ 1,512.34	$ 1,557.71	$ 1,604.44	$ 1,652.57	$ 1,702.15	$ 1,753.21	$ 1,805.81	$ 1,859.98	$ 1,915.78	$ 1,973.26
Network and Security Service	Reverse Proxy - Design & Implement - Proxy Platform - Small	Per Proxy		CCSU13370358-A	N/A	N/A	A			$ 8,233.84	$ 8,477.30	$ 8,728.01	$ 8,986.20	$ 9,252.08	$ 9,525.88	$ 9,807.84	$ 10,098.21	$ 10,397.23	$ 10,705.16
Network and Security Service	Reverse Proxy - Design & Implement - Proxy Platform - Medium	Per Proxy		CCSU13370359-A	N/A	N/A	A			$ 9,932.88	$ 10,226.13	$ 10,528.11	$ 10,839.08	$ 11,159.31	$ 11,489.08	$ 11,828.66	$ 12,178.37	$ 12,538.48	$ 12,909.33
Network and Security Service	Reverse Proxy - Design & Implement - Proxy Platform - Large	Per Proxy		CCSU13370360-A	N/A	N/A	A			$ 11,631.93	$ 11,974.96	$ 12,328.20	$ 12,691.96	$ 13,066.54	$ 13,452.27	$ 13,849.48	$ 14,258.52	$ 14,679.73	$ 15,113.49
Network and Security Service	Reverse Proxy - Design & Implement - Application Service - Small	Per Request		CCSU13370361-A	N/A	N/A	A			$ 1,274.28	$ 1,311.62	$ 1,350.07	$ 1,389.66	$ 1,430.42	$ 1,472.40	$ 1,515.62	$ 1,560.12	$ 1,605.94	$ 1,653.12
Network and Security Service	Reverse Proxy - Design & Implement - Application Service - Medium	Per Request		CCSU13370362-A	N/A	N/A	A			$ 1,699.05	$ 1,748.83	$ 1,800.10	$ 1,852.88	$ 1,907.23	$ 1,963.20	$ 2,020.82	$ 2,080.16	$ 2,141.25	$ 2,204.16
Network and Security Service	Reverse Proxy - Design & Implement - Application Service - Large	Per Request		CCSU13370363-A	N/A	N/A	A			$ 2,123.81	$ 2,186.04	$ 2,250.12	$ 2,316.10	$ 2,384.04	$ 2,453.99	$ 2,526.03	$ 2,600.19	$ 2,676.56	$ 2,755.20
Network and Security Service	Reverse Proxy - Modify - Application Service - Small	Per Request		CCSU13370364-A	N/A	N/A	A			$ 1,176.26	$ 1,211.55	$ 1,247.90	$ 1,285.33	$ 1,323.89	$ 1,363.61	$ 1,404.52	$ 1,446.65	$ 1,490.05	$ 1,534.76
Network and Security Service	Reverse Proxy - Modify - Application Service - Medium	Per Request		CCSU13370365-A	N/A	N/A	A			$ 1,568.35	$ 1,615.40	$ 1,663.86	$ 1,713.78	$ 1,765.19	$ 1,818.15	$ 1,872.69	$ 1,928.87	$ 1,986.74	$ 2,046.34
Network and Security Service	Reverse Proxy - Modify - Application Service - Large	Per Request		CCSU13370366-A	N/A	N/A	A			$ 1,960.44	$ 2,019.25	$ 2,079.83	$ 2,142.22	$ 2,206.49	$ 2,272.68	$ 2,340.86	$ 2,411.09	$ 2,483.42	$ 2,557.93
Network and Security Service	Stealth Starter Plan (2 week)	Per Request		CCSU13370367-A	N/A	N/A	A			$ 68,796.88	$ 70,860.78	$ 72,986.61	$ 75,176.21	$ 77,431.49	$ 79,754.44	$ 82,147.07	$ 84,611.48	$ 87,149.83	$ 89,764.32
Network and Security Service	Stealth Secure Virtual Terminal (SSVT) Started Plan Add-On (2 week)	Per Request		CCSU13370368-A	N/A	N/A	A			$ 2,907.63	$ 2,994.86	$ 3,084.71	$ 3,177.25	$ 3,272.57	$ 3,370.74	$ 3,471.87	$ 3,576.02	$ 3,683.30	$ 3,793.80
Network and Security Service	Stealth Service - Discovery	Per Engagement		CCSU13370369-A	N/A	N/A	A			$ 72,722.27	$ 74,903.94	$ 77,151.06	$ 79,465.59	$ 81,849.56	$ 84,305.05	$ 86,834.20	$ 89,439.22	$ 92,122.40	$ 94,886.07
Network and Security Service	Stealth Service - Design	Per Engagement		CCSU13370370-A	N/A	N/A	A			$ 70,042.24	$ 72,143.51	$ 74,307.82	$ 76,537.05	$ 78,833.16	$ 81,198.16	$ 83,634.10	$ 86,143.13	$ 88,727.42	$ 91,389.24
Network and Security Service	Stealth Service - Deployment	Per Engagement		CCSU13370371-A	N/A	N/A	A			$ 52 348.08	$ 53 918.52	$ 55 536.08	$ 57 202.16	$ 58 918.23	$ 60 685.77	$ 62 506.35	$ 64 381.54	$ 66 312.98	$ 68 302.37
Network and Security Service	Stealth Network Appliance (1000 Licenses, 300 Mbps)	Per Appliance		CCSU13370372-A	N/A	N/A	A			$ 2,694.26	$ 2,773.51	$ 2,855.13	$ 2,939.21	$ 3,025.80	$ 3,115.00	$ 3,206.87	$ 3,301.50	$ 3,398.96	$ 3,499.35
Network and Security Service	Stealth Network Appliance (1000 Licenses, 800 Mbps)	Per Appliance		CCSU13370373-A	N/A	N/A	A			$ 6,515.76	$ 6,707.98	$ 6,905.98	$ 7,109.91	$ 7,319.96	$ 7,536.32	$ 7,759.16	$ 7,988.69	$ 8,225.11	$ 8,468.62
Network and Security Service	Stealth Network Appliance (RPS, 1 Gbps)	Per Appliance		CCSU13370374-A	N/A	N/A	A			$ 23,243.52	$ 23,940.82	$ 24,659.05	$ 25,398.82	$ 26,160.78	$ 26,945.61	$ 27,753.97	$ 28,586.59	$ 29,444.19	$ 30,327.52
Network and Security Service	Stealth Network Appliance (1000 Licenses, 300 Mbps) - Annual Maintenance	Per Appliance		CCSU13370526-A	N/A	N/A	A			$ 3,398.78	$ 3,398.78	$ 3,398.78	$ 3,398.78	$ 3,398.78	$ 3,398.78	$ 3,398.78	$ 3,398.78	$ 3,398.78	$ 3,398.78
Network and Security Service	Stealth Network Appliance (1000 Licenses, 800 Mbps) - Annual Maintenance	Per Appliance		CCSU13370527-A	N/A	N/A	A			$ 3,398.78	$ 3,398.78	$ 3,398.78	$ 3,398.78	$ 3,398.78	$ 3,398.78	$ 3,398.78	$ 3,398.78	$ 3,398.78	$ 3,398.78
Network and Security Service	Stealth Network Appliance (RPS, 1 Gbps) - Annual Maintenance	Per Appliance		CCSU13370528-A	N/A	N/A	A			$ 283.23	$ 283.23	$ 283.23	$ 283.23	$ 283.23	$ 283.23	$ 283.23	$ 283.23	$ 283.23	$ 283.23
Network and Security Service	Stealth Client License (1-24)	Per License		CCSU13370375-A	N/A	N/A	A			$ 757.18	$ 779.90	$ 803.30	$ 827.39	$ 852.22	$ 877.78	$ 904.12	$ 931.24	$ 959.18	$ 987.95
Network and Security Service	Stealth Client License (25-49)	Per License		CCSU13370376-A	N/A	N/A	A			$ 721.60	$ 743.25	$ 765.55	$ 788.51	$ 812.17	$ 836.53	$ 861.63	$ 887.48	$ 914.10	$ 941.53
Network and Security Service	Stealth Client License (50-99)	Per License		CCSU13370377-A	N/A	N/A	A			$ 670.36	$ 690.47	$ 711.19	$ 732.52	$ 754.50	$ 777.13	$ 800.45	$ 824.46	$ 849.20	$ 874.67
Network and Security Service	Stealth Client License (100-249)	Per License		CCSU13370378-A	N/A	N/A	A			$ 620.55	$ 639.16	$ 658.34	$ 678.09	$ 698.43	$ 719.39	$ 740.97	$ 763.20	$ 786.09	$ 809.67
Network and Security Service	Stealth Client License (250-499)	Per License		CCSU13370379-A	N/A	N/A	A			$ 573.58	$ 590.79	$ 608.51	$ 626.77	$ 645.57	$ 664.94	$ 684.88	$ 705.43	$ 726.59	$ 748.39
Network and Security Service	Stealth Client License (500-999)	Per License		CCSU13370380-A	N/A	N/A	A			$ 519.50	$ 535.08	$ 551.13	$ 567.67	$ 584.70	$ 602.24	$ 620.30	$ 638.91	$ 658.08	$ 677.82
Network and Security Service	Stealth Client License (1000)	Per License		CCSU13370381-A	N/A	N/A	A			$ 401.36	$ 413.40	$ 425.81	$ 438.58	$ 451.74	$ 465.29	$ 479.25	$ 493.63	$ 508.44	$ 523.69
Network and Security Service	Stealth Client License (1-24) - Annual Maintenance	Per License		CCSU13370529-A	N/A	N/A	A			$ 14.30	$ 14.30	$ 14.30	$ 14.30	$ 14.30	$ 14.30	$ 14.30	$ 14.30	$ 14.30	$ 14.30
Network and Security Service	Stealth Client License (25-49) - Annual Maintenance	Per License		CCSU13370530-A	N/A	N/A	A			$ 11.53	$ 11.53	$ 11.53	$ 11.53	$ 11.53	$ 11.53	$ 11.53	$ 11.53	$ 11.53	$ 11.53
Network and Security Service	Stealth Client License (50-99) - Annual Maintenance	Per License		CCSU13370531-A	N/A	N/A	A			$ 7.19	$ 7.19	$ 7.19	$ 7.19	$ 7.19	$ 7.19	$ 7.19	$ 7.19	$ 7.19	$ 7.19
Network and Security Service	Stealth Client License (100-249) - Annual Maintenance	Per License		CCSU13370532-A	N/A	N/A	A			$ 13.59	$ 13.59	$ 13.59	$ 13.59	$ 13.59	$ 13.59	$ 13.59	$ 13.59	$ 13.59	$ 13.59
Network and Security Service	Stealth Client License (250-499) - Annual Maintenance	Per License		CCSU13370533-A	N/A	N/A	A			$ 10.60	$ 10.60	$ 10.60	$ 10.60	$ 10.60	$ 10.60	$ 10.60	$ 10.60	$ 10.60	$ 10.60
Network and Security Service	Stealth Client License (500-999) - Annual Maintenance	Per License		CCSU13370534-A	N/A	N/A	A			$ 12.60	$ 12.60	$ 12.60	$ 12.60	$ 12.60	$ 12.60	$ 12.60	$ 12.60	$ 12.60	$ 12.60
Network and Security Service	Stealth Client License (1000) - Annual Maintenance	Per License		CCSU13370535-A	N/A	N/A	A			$ 9.54	$ 9.54	$ 9.54	$ 9.54	$ 9.54	$ 9.54	$ 9.54	$ 9.54	$ 9.54	$ 9.54
Network and Security Service	Stealth Client Expansion License (1-24)	Per License		CCSU13370382-A	N/A	N/A	A			$ 758.61	$ 781.36	$ 804.81	$ 828.95	$ 853.82	$ 879.43	$ 905.82	$ 932.99	$ 960.98	$ 989.81
Network and Security Service	Stealth Client Expansion License (25-49)	Per License		CCSU13370383-A	N/A	N/A	A			$ 723.02	$ 744.71	$ 767.06	$ 790.07	$ 813.77	$ 838.18	$ 863.33	$ 889.23	$ 915.91	$ 943.38

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	Product Name	Unit	Qty per config	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Network and Security Service	Stealth Client Expansion License (50-99)	Per License		CCSU13370384-A	N/A	N/A	A			$ 671.79	$ 691.94	$ 712.70	$ 734.08	$ 756.10	$ 778.78	$ 802.15	$ 826.21	$ 851.00	$ 876.53
Network and Security Service	Stealth Client Expansion License (100-249)	Per License		CCSU13370385-A	N/A	N/A	A			$ 621.97	$ 640.63	$ 659.85	$ 679.65	$ 700.03	$ 721.04	$ 742.67	$ 764.95	$ 787.89	$ 811.53
Network and Security Service	Stealth Client Expansion License (250-499)	Per License		CCSU13370386-A	N/A	N/A	A			$ 575.00	$ 592.25	$ 610.02	$ 628.32	$ 647.17	$ 666.59	$ 686.58	$ 707.18	$ 728.40	$ 750.25
Network and Security Service	Stealth Client Expansion License (500-999)	Per License		CCSU13370387-A	N/A	N/A	A			$ 520.92	$ 536.55	$ 552.64	$ 569.22	$ 586.30	$ 603.89	$ 622.00	$ 640.66	$ 659.88	$ 679.68
Network and Security Service	Stealth Client Expansion License (1000)	Per License		CCSU13370388-A	N/A	N/A	A			$ 402.79	$ 414.87	$ 427.32	$ 440.14	$ 453.34	$ 466.94	$ 480.95	$ 495.38	$ 510.24	$ 525.55
Network and Security Service	Stealth Client Expansion License (1-24) - Annual Maintenance	Per License		CCSU13370536-A	N/A	N/A	A			$ 171.65	$ 171.65	$ 171.65	$ 171.65	$ 171.65	$ 171.65	$ 171.65	$ 171.65	$ 171.65	$ 171.65
Network and Security Service	Stealth Client Expansion License (25-49) - Annual Maintenance	Per License		CCSU13370537-A	N/A	N/A	A			$ 138.34	$ 138.34	$ 138.34	$ 138.34	$ 138.34	$ 138.34	$ 138.34	$ 138.34	$ 138.34	$ 138.34
Network and Security Service	Stealth Client Expansion License (50-99) - Annual Maintenance	Per License		CCSU13370538-A	N/A	N/A	A			$ 86.25	$ 86.25	$ 86.25	$ 86.25	$ 86.25	$ 86.25	$ 86.25	$ 86.25	$ 86.25	$ 86.25
Network and Security Service	Stealth Client Expansion License (100-249) - Annual Maintenance	Per License		CCSU13370539-A	N/A	N/A	A			$ 163.11	$ 163.11	$ 163.11	$ 163.11	$ 163.11	$ 163.11	$ 163.11	$ 163.11	$ 163.11	$ 163.11
Network and Security Service	Stealth Client Expansion License (250-499) - Annual Maintenance	Per License		CCSU13370540-A	N/A	N/A	A			$ 127.24	$ 127.24	$ 127.24	$ 127.24	$ 127.24	$ 127.24	$ 127.24	$ 127.24	$ 127.24	$ 127.24
Network and Security Service	Stealth Client Expansion License (500-999) - Annual Maintenance	Per License		CCSU13370541-A	N/A	N/A	A			$ 151.15	$ 151.15	$ 151.15	$ 151.15	$ 151.15	$ 151.15	$ 151.15	$ 151.15	$ 151.15	$ 151.15
Network and Security Service	Stealth Client Expansion License (1000) - Annual Maintenance	Per License		CCSU13370542-A	N/A	N/A	A			$ 114.43	$ 114.43	$ 114.43	$ 114.43	$ 114.43	$ 114.43	$ 114.43	$ 114.43	$ 114.43	$ 114.43
Network and Security Service	Stealth Server License (1-4)	Per License		CCSU13370389-A	N/A	N/A	A			$ 23,761.59	$ 24,474.44	$ 25,208.67	$ 25,964.93	$ 26,743.88	$ 27,546.19	$ 28,372.58	$ 29,223.76	$ 30,100.47	$ 31,003.48
Network and Security Service	Stealth Server License (5-9)	Per License		CCSU13370390-A	N/A	N/A	A			$ 17,124.85	$ 17,638.60	$ 18,167.76	$ 18,712.79	$ 19,274.17	$ 19,852.40	$ 20,447.97	$ 21,061.41	$ 21,693.25	$ 22,344.05
Network and Security Service	Stealth Server License (10-24)	Per License		CCSU13370391-A	N/A	N/A	A			$ 11 386.21	$ 11 727.79	$ 12 079.63	$ 12 442.01	$ 12 815.27	$ 13 199.73	$ 13 595.73	$ 14 003.60	$ 14 423.70	$ 14 856.42
Network and Security Service	Stealth Server License (25-49)	Per License		CCSU13370392-A	N/A	N/A	A			$ 7 116.38	$ 7 329.87	$ 7 549.77	$ 7 776.26	$ 8 009.55	$ 8 249.83	$ 8 497.33	$ 8 752.25	$ 9 014.82	$ 9 285.26
Network and Security Service	Stealth Server License (50-99)	Per License		CCSU13370393-A	N/A	N/A	A			$ 4,269.83	$ 4,397.92	$ 4,529.86	$ 4,665.76	$ 4,805.73	$ 4,949.90	$ 5,098.40	$ 5,251.35	$ 5,408.89	$ 5,571.16
Network and Security Service	Stealth Server License (100)	Per License		CCSU13370394-A	N/A	N/A	A			$ 2,846.55	$ 2,931.95	$ 3,019.91	$ 3,110.50	$ 3,203.82	$ 3,299.93	$ 3,398.93	$ 3,500.90	$ 3,605.93	$ 3,714.10
Network and Security Service	Stealth Server License (1-4) - Annual Maintenance	Per License		CCSU13370543-A	N/A	N/A	A			$ 475.37	$ 489.64	$ 504.32	$ 519.45	$ 535.04	$ 551.09	$ 567.62	$ 584.65	$ 602.19	$ 620.26
Network and Security Service	Stealth Server License (5-9) - Annual Maintenance	Per License		CCSU13370544-A	N/A	N/A	A			$ 227.72	$ 234.56	$ 241.59	$ 248.84	$ 256.31	$ 263.99	$ 271.91	$ 280.07	$ 288.47	$ 297.13
Network and Security Service	Stealth Server License (10-24) - Annual Maintenance	Per License		CCSU13370545-A	N/A	N/A	A			$ 56.93	$ 58.64	$ 60.40	$ 62.21	$ 64.08	$ 66.00	$ 67.98	$ 70.02	$ 72.12	$ 74.28
Network and Security Service	Stealth Server License (25-49) - Annual Maintenance	Per License		CCSU13370546-A	N/A	N/A	A			$ 142.33	$ 146.60	$ 151.00	$ 155.53	$ 160.19	$ 165.00	$ 169.95	$ 175.04	$ 180.30	$ 185.71
Network and Security Service	Stealth Server License (50-99) - Annual Maintenance	Per License		CCSU13370547-A	N/A	N/A	A			$ 341.59	$ 351.83	$ 362.39	$ 373.26	$ 384.46	$ 395.99	$ 407.87	$ 420.11	$ 432.71	$ 445.69
Network and Security Service	Stealth Server License (100) - Annual Maintenance	Per License		CCSU13370548-A	N/A	N/A	A			$ 85.40	$ 87.96	$ 90.60	$ 93.32	$ 96.11	$ 99.00	$ 101.97	$ 105.03	$ 108.18	$ 111.42
Network and Security Service	Stealth Server Expansion License (1-4)	Per License		CCSU13370395-A	N/A	N/A	A			$ 23 761.59	$ 24 474.44	$ 25 208.67	$ 25 964.93	$ 26 743.88	$ 27 546.19	$ 28 372.58	$ 29 223.76	$ 30 100.47	$ 31 003.48
Network and Security Service	Stealth Server Expansion License (5-9)	Per License		CCSU13370396-A	N/A	N/A	A			$ 17 079.31	$ 17 591.69	$ 18 119.44	$ 18 663.02	$ 19 222.91	$ 19 799.60	$ 20 393.59	$ 21 005.40	$ 21 635.56	$ 22 284.62
Network and Security Service	Stealth Server Expansion License (10-24)	Per License		CCSU13370397-A	N/A	N/A	A			$ 11 386.21	$ 11 727.79	$ 12 079.63	$ 12 442.01	$ 12 815.27	$ 13 199.73	$ 13 595.73	$ 14 003.60	$ 14 423.70	$ 14 856.42
Network and Security Service	Stealth Server Expansion License (25-49)	Per License		CCSU13370398-A	N/A	N/A	A			$ 7,116.38	$ 7,329.87	$ 7,549.77	$ 7,776.26	$ 8,009.55	$ 8,249.83	$ 8,497.33	$ 8,752.25	$ 9,014.82	$ 9,285.26
Network and Security Service	Stealth Server Expansion License (50-99)	Per License		CCSU13370399-A	N/A	N/A	A			$ 4,269.83	$ 4,397.92	$ 4,529.86	$ 4,665.76	$ 4,805.73	$ 4,949.90	$ 5,098.40	$ 5,251.35	$ 5,408.89	$ 5,571.16
Network and Security Service	Stealth Server Expansion License (100)	Per License		CCSU13370400-A	N/A	N/A	A			$ 2 846.55	$ 2 931.95	$ 3 019.91	$ 3 110.50	$ 3 203.82	$ 3 299.93	$ 3 398.93	$ 3 500.90	$ 3 605.93	$ 3 714.10
Network and Security Service	Stealth Server Expansion License (1-4) - Annual Maintenance	Per License		CCSU13370549-A	N/A	N/A	A			$ 475.37	$ 475.37	$ 475.37	$ 475.37	$ 475.37	$ 475.37	$ 475.37	$ 475.37	$ 475.37	$ 475.37
Network and Security Service	Stealth Server Expansion License (5-9) - Annual Maintenance	Per License		CCSU13370550-A	N/A	N/A	A			$ 227.72	$ 227.72	$ 227.72	$ 227.72	$ 227.72	$ 227.72	$ 227.72	$ 227.72	$ 227.72	$ 227.72
Network and Security Service	Stealth Server Expansion License (10-24) - Annual Maintenance	Per License		CCSU13370551-A	N/A	N/A	A			$ 56.93	$ 56.93	$ 56.93	$ 56.93	$ 56.93	$ 56.93	$ 56.93	$ 56.93	$ 56.93	$ 56.93
Network and Security Service	Stealth Server Expansion License (25-49) - Annual Maintenance	Per License		CCSU13370552-A	N/A	N/A	A			$ 142.33	$ 142.33	$ 142.33	$ 142.33	$ 142.33	$ 142.33	$ 142.33	$ 142.33	$ 142.33	$ 142.33
Network and Security Service	Stealth Server Expansion License (50-99) - Annual Maintenance	Per License		CCSU13370553-A	N/A	N/A	A			$ 341.59	$ 341.59	$ 341.59	$ 341.59	$ 341.59	$ 341.59	$ 341.59	$ 341.59	$ 341.59	$ 341.59
Network and Security Service	Stealth Server Expansion License (100) - Annual Maintenance	Per License		CCSU13370554-A	N/A	N/A	A			$ 85.40	$ 85.40	$ 85.40	$ 85.40	$ 85.40	$ 85.40	$ 85.40	$ 85.40	$ 85.40	$ 85.40
Network and Security Service	Stealth Authorization Service Stand Alone License	Per License		CCSU13370401-A	N/A	N/A	A			$ 14,232.76	$ 14,659.74	$ 15,099.53	$ 15,552.52	$ 16,019.09	$ 16,499.67	$ 16,994.66	$ 17,504.50	$ 18,029.63	$ 18,570.52
Network and Security Service	Stealth Authorization Service with AD/LDAP License	Per License		CCSU13370402-A	N/A	N/A	A			$ 21,349.14	$ 21,989.61	$ 22,649.30	$ 23,328.78	$ 24,028.64	$ 24,749.50	$ 25,491.98	$ 26,256.74	$ 27,044.45	$ 27,855.78
Network and Security Service	Stealth Authorization Service with RADIUS License	Per License		CCSU13370403-A	N/A	N/A	A			$ 28 465.51	$ 29 319.48	$ 30 199.06	$ 31 105.04	$ 32 038.19	$ 32 999.33	$ 33 989.31	$ 35 008.99	$ 36 059.26	$ 37 141.04
Network and Security Service	Stealth Secure Virtual Terminal 4GB Windows Boot Device	Per Device		CCSU13370404-A	N/A	N/A	A			$ 533.73	$ 549.74	$ 566.23	$ 583.22	$ 600.72	$ 618.74	$ 637.30	$ 656.42	$ 676.11	$ 696.39
Security Services	Vulnerability Assessment - Infrastructure - Small	Per Assessment		CCSD13370405-A	N/A	N/A	A			$ 38,748.72	$ 39,911.18	$ 41,108.51	$ 42,341.77	$ 43,612.02	$ 44,920.38	$ 46,268.00	$ 47,656.04	$ 49,085.72	$ 50,558.29
Security Services	Vulnerability Assessment - Infrastructure - Medium	Per Assessment		CCSD13370406-A	N/A	N/A	A			$ 68 502.20	$ 70 557.26	$ 72 673.98	$ 74 854.20	$ 77 099.83	$ 79 412.82	$ 81 795.21	$ 84 249.06	$ 86 776.53	$ 89 379.83
Security Services	Vulnerability Assessment - Infrastructure - Large	Per Assessment		CCSD13370407-A	N/A	N/A	A			$ 106 558.97	$ 109 755.74	$ 113 048.42	$ 116 439.87	$ 119 933.06	$ 123 531.06	$ 127 236.99	$ 131 054.10	$ 134 985.72	$ 139 035.29
Security Services	Vulnerability Assessment - Infrastructure - Very Large	Per Assessment		CCSD13370408-A	N/A	N/A	A			$ 210,350.18	$ 216,660.69	$ 223,160.51	$ 229,855.32	$ 236,750.98	$ 243,853.51	$ 251,169.12	$ 258,704.19	$ 266,465.32	$ 274,459.28
Security Services	Vulnerability Assessment - Web / mobile Application - Small (Up to 35 Custom Web Application Pages)	Per Assessment		CCSD13370409-A	N/A	N/A	A			$ 53,279.49	$ 54,877.87	$ 56,524.21	$ 58,219.93	$ 59,966.53	$ 61,765.53	$ 63,618.49	$ 65,527.05	$ 67,492.86	$ 69,517.65
Security Services	Vulnerability Assessment - Web / mobile Application - Medium (Up to 70 Custom Web Application Pages)	Per Assessment		CCSD13370410-A	N/A	N/A	A			$ 78,881.32	$ 81,247.76	$ 83,685.19	$ 86,195.75	$ 88,781.62	$ 91,445.07	$ 94,188.42	$ 97,014.07	$ 99,924.49	$ 102,922.23
Security Services	Vulnerability Assessment - Web / mobile Application - Large (Up to 100 Custom Web Application Pages)	Per Assessment		CCSD13370411-A	N/A	N/A	A			$ 117,906.81	$ 121,444.02	$ 125,087.34	$ 128,839.96	$ 132,705.16	$ 136,686.31	$ 140,786.90	$ 145,010.51	$ 149,360.82	$ 153,841.65

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	Product Name	Unit	Qty per config	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Security Services	Vulnerability Assessment - Web / mobile Application - Very Large (Up to 175 Custom Web Application Pages)	Per Assessment		CCSD13370412-A	N/A	N/A	A			$ 200,663.00	$206,682.89	$212,883.38	$219,269.88	$225,847.98	$232,623.42	$ 239,602.12	$ 246,790.18	$ 254,193.89	$ 261,819.71
Security Services	Vulnerability Assessment - Database - Small (Up to 3 Database Server with up to 5 database instances or Oracle SIDs)	Per Assessment		CCSD13370413-A	N/A	N/A	A			$ 23,526.01	$ 24,231.79	$ 24,958.74	$ 25,707.50	$ 26,478.73	$ 27,273.09	$ 28,091.28	$ 28,934.02	$ 29,802.04	$ 30,696.10
Security Services	Vulnerability Assessment - Database - Medium (Up to 5 database servers with up to ten database instances or Oracle SIDs)	Per Assessment		CCSD13370414-A	N/A	N/A	A			$ 34,597.07	$ 35,634.98	$ 36,704.03	$ 37,805.15	$ 38,939.31	$ 40,107.49	$ 41,310.71	$ 42,550.03	$ 43,826.53	$ 45,141.33
Security Services	Vulnerability Assessment - Database - Large (Up to 10 Database Servers with up to 15 database instances or Oracle SIDs)	Per Assessment		CCSD13370415-A	N/A	N/A	A			$ 49,127.84	$ 50,601.67	$ 52,119.72	$ 53,683.32	$ 55,293.82	$ 56,952.63	$ 58,661.21	$ 60,421.04	$ 62,233.68	$ 64,100.69
Security Services	Vulnerability Assessment - Database - Very Large (Up to 20 database servers with up to 30 database instances or Oracle SIDs)	Per Assessment		CCSD13370416-A	N/A	N/A	A			$ 96,871.79	$ 99,777.95	$102,771.29	$105,854.43	$109,030.06	$112,300.96	$ 115,669.99	$ 119,140.09	$ 122,714.29	$ 126,395.72
Security Services	Vulnerability Assessment - Wireless - Small (Up to 2 locations with up to 25 wireless access points)	Per Assessment		CCSD13370417-A	N/A	N/A	A			$ 24,909.89	$ 25,657.19	$ 26,426.90	$ 27,219.71	$ 28,036.30	$ 28,877.39	$ 29,743.71	$ 30,636.02	$ 31,555.10	$ 32,501.76
Security Services	Vulnerability Assessment - Wireless - Medium (Up to 3 locations with up to 50 wireless access points)	Per Assessment		CCSD13370418-A	N/A	N/A	A			$ 41,516.48	$ 42,761.98	$ 44,044.84	$ 45,366.18	$ 46,727.17	$ 48,128.98	$ 49,572.85	$ 51,060.04	$ 52,591.84	$ 54,169.59
Security Services	Vulnerability Assessment - Wireless - Large (Up to 4 locations with up to 75 wireless access points)	Per Assessment		CCSD13370419-A	N/A	N/A	A			$ 89,952.38	$ 92,650.95	$ 95,430.48	$ 98,293.40	$101,242.20	$104,279.46	$ 107,407.85	$ 110,630.08	$ 113,948.98	$ 117,367.45
Security Services	Security Code Review - Small (Up to 500,000 Lines of Code for one web application custom source code; includes manual verification on up to 15 vulnerabilities with up to 4 instances per vulnerability assimilated)	Per Assessment		CCSD13370420-A	N/A	N/A	A			$ 44,976.19	$ 46,325.48	$ 47,715.24	$ 49,146.70	$ 50,621.10	$ 52,139.73	$ 53,703.92	$ 55,315.04	$ 56,974.49	$ 58,683.73
Security Services	Security Code Review - Medium (Up to 1,000,000 Lines of Code for one web application custom source code; includes manual verification on up to 20 vulnerabilities with up to 6 instances per vulnerability assimilated)	Per Assessment		CCSD13370421-A	N/A	N/A	A			$ 74,729.67	$ 76,971.56	$ 79,280.71	$ 81,659.13	$ 84,108.90	$ 86,632.17	$ 89,231.13	$ 91,908.07	$ 94,665.31	$ 97,505.27
Security Services	Security Code Review - Large (Up to 2,000,000 Lines of Code for one web application custom source code; includes manual verification on up to 25 vulnerabilities with up to 8 instances per vulnerability assimilated)	Per Assessment		CCSD13370422-A	N/A	N/A	A			$ 115,554.21	$119,020.84	$122,591.46	$126,269.21	$130,057.28	$133,959.00	$ 137,977.77	$ 142,117.11	$ 146,380.62	$ 150,772.04
Security Services	Security Code Review - Very Large (Up to 3,500,000 Lines of Code for one web application custom source code; includes manual verification on up to 35 vulnerabilities with up to 10 instances per vulnerability assimilated)	Per Assessment		CCSD13370423-A	N/A	N/A	A			$ 159,146.52	$163,920.92	$168,838.54	$173,903.70	$179,120.81	$184,494.43	$ 190,029.27	$ 195,730.15	$ 201,602.05	$ 207,650.11
Security Services	Security Risk Assessment - Small (An Agency or Office with up to 99 employees & 1 Security Guidelines)	Per Assessment		CCSD13370424-A	N/A	N/A	A			$ 79,573.26	$ 81,960.46	$ 84,419.27	$ 86,951.85	$ 89,560.40	$ 92,247.22	$ 95,014.63	$ 97,865.07	$ 100,801.02	$ 103,825.06
Security Services	Security Risk Assessment - Medium (An Agency or Office with up to 999 employees & 2 Security Guidelines)	Per Assessment		CCSD13370425-A	N/A	N/A	A			$ 163,298.17	$168,197.11	$173,243.03	$178,440.32	$183,793.53	$189,307.33	$ 194,986.55	$ 200,836.15	$ 206,861.23	$ 213,067.07
Security Services	Security Risk Assessment - Large (An Agency or Office with up to 9,999 employees & 5 Security Guidelines)	Per Assessment		CCSD13370426-A	N/A	N/A	A			$ 242,179.49	$249,444.87	$256,928.22	$264,636.06	$272,575.15	$280,752.40	$ 289,174.97	$ 297,850.22	$ 306,785.73	$ 315,989.30
Security Services	Security Risk Assessment - Very Large (An Agency or Office with 10,000 employees & 10 Security Guidelines)	Per Assessment		CCSD13370427-A	N/A	N/A	A			$ 371,572.53	$382,719.70	$394,201.29	$406,027.33	$418,208.15	$430,754.40	$ 443,677.03	$ 456,987.34	$ 470,696.96	$ 484,817.87
Security Services	eGRC Solution - Install and initial setup	Per Implementation		CCSD13370428-A	N/A	N/A	A			$ 37 364.84	$ 38 485.78	$ 39 640.35	$ 40 829.56	$ 42 054.45	$ 43 316.08	$ 44 615.57	$ 45 954.03	$ 47 332.66	$ 48 752.63
Security Services	eGRC Solution - Design and Configure - Small	Per Request		CCSD13370429-A	N/A	N/A	A			$ 45 668.13	$ 47 038.18	$ 48 449.32	$ 49 902.80	$ 51 399.88	$ 52 941.88	$ 54 530.14	$ 56 166.04	$ 57 851.02	$ 59 586.55
Security Services	eGRC Solution - Design and Configure - Medium	Per Request		CCSD13370430-A	N/A	N/A	A			$ 104,483.15	$107,617.64	$110,846.17	$114,171.56	$117,596.71	$121,124.61	$ 124,758.35	$ 128,501.10	$ 132,356.13	$ 136,326.81
Security Services	eGRC Solution - Design and Configure - Large	Per Request		CCSD13370431-A	N/A	N/A	A			$ 138,388.28	$ 142,539.93	$146,816.12	$151,220.61	$155,757.23	$160,429.94	$ 165,242.84	$ 170,200.13	$ 175,306.13	$ 180,565.31
Security Services	eGRC Solution - Design and Configure - Very Large	Per Request		CCSD13370432-A	N/A	N/A	A			$ 179 212.82	$ 184 589.20	$190 126.88	$195 830.69	$201 705.61	$207 756.78	$ 213 989.48	$ 220 409.16	$ 227 021.44	$ 233 832.08
Security Services	eGRC Solution - Develop risk assessment templates - Small	Per Request		CCSD13370433-A	N/A	N/A	A			$ 26,293.77	$ 27,082.59	$ 27,895.06	$ 28,731.92	$ 29,593.87	$ 30,481.69	$ 31,396.14	$ 32,338.02	$ 33,308.16	$ 34,307.41
Security Services	eGRC Solution - Develop risk assessment templates - Medium	Per Request		CCSD13370434-A	N/A	N/A	A			$ 62,274.73	$ 64,142.97	$ 66,067.26	$ 68,049.27	$ 70,090.75	$ 72,193.47	$ 74,359.28	$ 76,590.06	$ 78,887.76	$ 81,254.39
Security Services	eGRC Solution - Develop risk assessment templates - Large	Per Request		CCSD13370435-A	N/A	N/A	A			$ 89,260.44	$ 91,938.25	$ 94,696.40	$ 97,537.29	$100,463.41	$103,477.31	$ 106,581.63	$ 109,779.08	$ 113,072.45	$ 116,464.63
Security Services	eGRC Solution - Develop risk assessment templates - Very Large	Per Request		CCSD13370436-A	N/A	N/A	A			$ 119,013.92	$122,584.34	$126,261.87	$130,049.72	$133,951.21	$137,969.75	$ 142,108.84	$ 146,372.11	$ 150,763.27	$ 155,286.17
Security Services	Security Configuration Review (Standard OS Platform - up to 3 information Systems	Per Request		CCSD13370437-A	N/A	N/A	A			$ 31,137.36	$ 32,071.48	$ 33,033.63	$ 34,024.64	$ 35,045.38	$ 36,096.74	$ 37,179.64	$ 38,295.03	$ 39,443.88	$ 40,627.20
Security Services	Security Configuration Review (3 standard database instances)	Per Request		CCSD13370438-A	N/A	N/A	A			$ 31,137.36	$ 32,071.48	$ 33,033.63	$ 34,024.64	$ 35,045.38	$ 36,096.74	$ 37,179.64	$ 38,295.03	$ 39,443.88	$ 40,627.20
Security Services	Security Configuration Review (3 web server instances)	Per Request		CCSD13370439-A	N/A	N/A	A			$ 31,137.36	$ 32,071.48	$ 33,033.63	$ 34,024.64	$ 35,045.38	$ 36,096.74	$ 37,179.64	$ 38,295.03	$ 39,443.88	$ 40,627.20

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	Product Name	Unit	Qty per config	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Security Services	Security Configuration Review (2 boundary defense devices)	Per Request		CCSD13370440-A	N/A	N/A	A			$ 40,824.54	$ 42,049.28	$ 43,310.76	$ 44,610.08	$ 45,948.38	$ 47,326.83	$ 48,746.64	$ 50,209.04	$ 51,715.31	$ 53,266.77
Security Services	Security Configuration Review (One Mainframe OS Instance)	Per Request		CCSD13370441-A	N/A	N/A	A			$ 77,497.44	$ 79,822.36	$ 82,217.03	$ 84,683.54	$ 87,224.05	$ 89,840.77	$ 92,535.99	$ 95,312.07	$ 98,171.43	$ 101,116.58
Security Services	Security Configuration Review (up to 3 Virtual infrastructure instances)	Per Request		CCSD13370442-A	N/A	N/A	A			$ 33,905.13	$ 34,922.28	$ 35,969.95	$ 37,049.05	$ 38,160.52	$ 39,305.34	$ 40,484.50	$ 41,699.03	$ 42,950.00	$ 44,238.50
Security Services	Security Configuration Review (One standard ERP solution)	Per Request		CCSD13370443-A	N/A	N/A	A			$ 89,952.38	$ 92,650.95	$ 95,430.48	$ 98,293.40	$101,242.20	$104,279.46	$ 107,407.85	$ 110,630.08	$ 113,948.98	$ 117,367.45
Security Services	CTI Diagnostic - Small (1 of TB of audit logs and rogue device detection for up to 1,000 devices)	Per Assessment		CCSD13370444-A	N/A	N/A	A			$ 38,748.72	$ 39,911.18	$ 41,108.51	$ 42,341.77	$ 43,612.02	$ 44,920.38	$ 46,268.00	$ 47,656.04	$ 49,085.72	$ 50,558.29
Security Services	CTI Diagnostic - Medium (2 of TB of audit logs and rogue device detection for up to 2,000 devices)	Per Assessment		CCSD13370445-A	N/A	N/A	A			$ 68,502.20	$ 70,557.26	$ 72,673.98	$ 74,854.20	$ 77,099.83	$ 79,412.82	$ 81,795.21	$ 84,249.06	$ 86,776.53	$ 89,379.83
Security Services	CTI Diagnostic - Large (3 of TB of audit logs and rogue device detection for up to 3,500 devices)	Per Assessment		CCSD13370446-A	N/A	N/A	A			$ 109,326.74	$ 112,606.54	$ 115,984.74	$ 119,464.28	$ 123,048.21	$ 126,739.65	$ 130,541.84	$ 134,458.10	$ 138,491.84	$ 142,646.60
Security Services	CTI Diagnostic - Very Large (4 of TB of audit logs and rogue device detection for up to 5,000 devices)	Per Assessment		CCSD13370447-A	N/A	N/A	A			$ 154,994.87	$ 159,644.72	$ 164,434.06	$ 169,367.08	$ 174,448.09	$ 179,681.54	$ 185,071.98	$ 190,624.14	$ 196,342.87	$ 202,233.15
Security Services	Suspicious Program Diagnostic - Small (up to 25 standard configuration for Servers)	Per Assessment		CCSD13370448-A	N/A	N/A	A			$ 37,364.84	$ 38,485.78	$ 39,640.35	$ 40,829.56	$ 42,054.45	$ 43,316.08	$ 44,615.57	$ 45,954.03	$ 47,332.66	$ 48,752.63
Security Services	Suspicious Program Diagnostic - Medium (up to 100 standard configuration for Servers)	Per Assessment		CCSD13370449-A	N/A	N/A	A			$ 80,265.20	$ 82,673.16	$ 85,153.35	$ 87,707.95	$ 90,339.19	$ 93,049.37	$ 95,840.85	$ 98,716.07	$ 101,677.56	$ 104,727.88
Security Services	Suspicious Program Diagnostic - Large (up to 250 standard configuration for Servers)	Per Assessment		CCSD13370450-A	N/A	N/A	A			$ 130,084.98	$ 133,987.53	$ 138,007.16	$ 142,147.37	$ 146,411.79	$ 150,804.15	$ 155,328.27	$ 159,988.12	$ 164,787.76	$ 169,731.40
Security Services	Suspicious Program Diagnostic - Very Large (1,000 standard configuration for Servers)	Per Assessment		CCSD13370451-A	N/A	N/A	A			$ 192,359.71	$ 198,130.50	$ 204,074.41	$ 210,196.64	$ 216,502.54	$ 222,997.62	$ 229,687.55	$ 236,578.18	$ 243,675.52	$ 250,985.79
Security Services	Remote Access Compromise Analysis - Small (1 TB of Remote Access Audit Logs)	Per Assessment		CCSD13370452-A	N/A	N/A	A			$ 3,944.07	$ 4,062.39	$ 4,184.26	$ 4,309.79	$ 4,439.08	$ 4,572.25	$ 4,709.42	$ 4,850.70	$ 4,996.22	$ 5,146.11
Security Services	Remote Access Compromise Analysis - Medium (2 of TB of Remote Access Audit Logs)	Per Assessment		CCSD13370453-A	N/A	N/A	A			$ 6,919.41	$ 7,127.00	$ 7,340.81	$ 7,561.03	$ 7,787.86	$ 8,021.50	$ 8,262.14	$ 8,510.01	$ 8,765.31	$ 9,028.27
Security Services	Remote Access Compromise Analysis - Large (3 of TB of Remote Access Audit Logs)	Per Assessment		CCSD13370454-A	N/A	N/A	A			$ 9,272.01	$ 9,550.18	$ 9,836.68	$ 10,131.78	$ 10,435.73	$ 10,748.81	$ 11,071.27	$ 11,403.41	$ 11,745.51	$ 12,097.88
Security Services	Remote Access Compromise Analysis - Very Large (4 of TB of Remote Access Audit Logs)	Per Assessment		CCSD13370455-A	N/A	N/A	A			$ 11,417.03	$ 11,759.54	$ 12,112.33	$ 12,475.70	$ 12,849.97	$ 13,235.47	$ 13,632.53	$ 14,041.51	$ 14,462.76	$ 14,896.64
Security Services	Insider Threat Detection Diagnostic - Small (Agency or Office with up to 99 employees, up to 250 GB of Audit Logs, and up to 3 Interviews)	Per Assessment		CCSD13370456-A	N/A	N/A	A			$ 34,597.07	$ 35,634.98	$ 36,704.03	$ 37,805.15	$ 38,939.31	$ 40,107.49	$ 41,310.71	$ 42,550.03	$ 43,826.53	$ 45,141.33
Security Services	Insider Threat Detection Diagnostic - Medium (Agency or Office with up to 999 employees, up to 500 GB of Audit Logs, and up to 5 Interviews)	Per Assessment		CCSD13370457-A	N/A	N/A	A			$ 62,274.73	$ 64,142.97	$ 66,067.26	$ 68,049.27	$ 70,090.75	$ 72,193.47	$ 74,359.28	$ 76,590.06	$ 78,887.76	$ 81,254.39
Security Services	Insider Threat Detection Diagnostic - Large (Agency or Office with up to 9,999 employees, up to 1 tT of Audit Logs, and up to 10 Interviews)	Per Assessment		CCSD13370458-A	N/A	N/A	A			$ 98,947.62	$ 101,916.05	$ 104,973.53	$ 108,122.73	$ 111,366.42	$ 114,707.41	$ 118,148.63	$ 121,693.09	$ 125,343.88	$ 129,104.20
Security Services	Insider Threat Detection Diagnostic - Very Large (Agency or Office with up to 10,000 employees, up to 2 TB of Audit Logs, and up to 3 Interviews)	Per Assessment		CCSD13370459-A	N/A	N/A	A			$ 139,772.16	$ 143,965.33	$ 148,284.29	$ 152,732.81	$ 157,314.80	$ 162,034.24	$ 166,895.27	$ 171,902.13	$ 177,059.19	$ 182,370.97
Security Services	Enterprise Fraud Program Assessment - Small - (Agency or Office with up 99 employees, 250 GB of Audit Logs, and up to 3 Fraud Detection Rule Sets)	Per Assessment		CCSD13370460-A	N/A	N/A	A			$ 68,502.20	$ 70,557.26	$ 72,673.98	$ 74,854.20	$ 77,099.83	$ 79,412.82	$ 81,795.21	$ 84,249.06	$ 86,776.53	$ 89,379.83
Security Services	Enterprise Fraud Program Assessment - Medium - (Agency or Office with up 999 employees, 500 GB of Audit Logs, and up to 5 Fraud Detection Rule Sets)	Per Assessment		CCSD13370461-A	N/A	N/A	A			$ 113,478.39	$ 116,882.74	$ 120,389.22	$ 124,000.90	$ 127,720.93	$ 131,552.55	$ 135,499.13	$ 139,564.10	$ 143,751.03	$ 148,063.56
Security Services	Enterprise Fraud Program Assessment - Large - (Agency or Office with up 9,999 employees, 1 TB of Audit Logs, and up to 5 Fraud Detection Rule Sets)	Per Assessment		CCSD13370462-A	N/A	N/A	A			$ 163,298.17	$ 168,197.11	$ 173,243.03	$ 178,440.32	$ 183,793.53	$ 189,307.33	$ 194,986.55	$ 200,836.15	$ 206,861.23	$ 213,067.07
Security Services	Enterprise Fraud Program Assessment - Very Large - (Agency or Office with up 10,000 employees, 2 TB of Audit Logs, and up to 5 Fraud Detection Rule Sets)	Per Assessment		CCSD13370463-A	N/A	N/A	A			$ 235,260.07	$ 242,317.87	$ 249,587.41	$ 257,075.03	$ 264,787.28	$ 272,730.90	$ 280,912.83	$ 289,340.21	$ 298,020.42	$ 306,961.03
Security Services	Data Loss Prevention - Network Monitoring - Small (1 Exgress Point, and 5 Simple, and 1 Complex DLP Policies)	Per Request		CCSD13370464-A	N/A	N/A	A			$ 130,084.98	$ 133,987.53	$ 138,007.16	$ 142,147.37	$ 146,411.79	$ 150,804.15	$ 155,328.27	$ 159,988.12	$ 164,787.76	$ 169,731.40
Security Services	Data Loss Prevention - Network Monitoring - Medium (2 Exgress Points, 7 Simple, and 2 Complex DLP Policies)	Per Request		CCSD13370465-A	N/A	N/A	A			$ 208,966.30	$ 215,235.29	$ 221,692.35	$ 228,343.12	$ 235,193.41	$ 242,249.21	$ 249,516.69	$ 257,002.19	$ 264,712.26	$ 272,653.62
Security Services	Data Loss Prevention - Network Monitoring - Large (3 Exgress Points, 9 Simple, and 3 Complex DLP Policies)	Per Request		CCSD13370466-A	N/A	N/A	A			$ 339,743.22	$ 349,935.52	$ 360,433.58	$ 371,246.59	$ 382,383.99	$ 393,855.51	$ 405,671.17	$ 417,841.31	$ 430,376.55	$ 443,287.85
Security Services	Data Loss Prevention - Network Monitoring - Very Large (4 Exgress Points, 12 Simple, and 5 Complex DLP Policies)	Per Request		CCSD13370467-A	N/A	N/A	A			$ 419,316.48	$ 431,895.98	$ 444,852.86	$ 458,198.44	$ 471,944.39	$ 486,102.73	$ 500,685.81	$ 515,706.38	$ 531,177.57	$ 547,112.90

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	Product Name	Unit	Qty per config	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Security Services	Data Loss Prevention - Endpoint protection - Small - (up to 150 IT infrastructure endpoints, 5 Simple, and 1 Complex DLP Policies)	Per Request		CCSD13370468-A	N/A	N/A	A			$ 123,165.57	$126,860.53	$130,666.35	$134,586.34	$138,623.93	$142,782.65	$ 147,066.13	$ 151,478.11	$ 156,022.46	$ 160,703.13
Security Services	Data Loss Prevention - Endpoint protection - Medium - (up to 1,250 IT infrastructure endpoints, 7 Simple, and 3 Complex DLP Policies)	Per Request		CCSD13370469-A	N/A	N/A	A			$ 204,814.65	$210,959.09	$217,287.86	$223,806.50	$230,520.69	$237,436.32	$ 244,559.40	$ 251,896.19	$ 259,453.07	$ 267,236.66
Security Services	Data Loss Prevention - Endpoint protection - Large - (up to 11,000 IT infrastructure endpoints, 9 Simple, and 3 Complex DLP Policies)	Per Request		CCSD13370470-A	N/A	N/A	A			$ 470,520.15	$484,635.75	$499,174.82	$514,150.07	$529,574.57	$545,461.81	$ 561,825.66	$ 578,680.43	$ 596,040.84	$ 613,922.07
Security Services	Data Loss Prevention - Endpoint protection - Very Large - (25,000 IT infrastructure endpoints, and 12 Simple, and 5 Complex DLP Policies)	Per Request		CCSD13370471-A	N/A	N/A	A			$ 705,780.22	$726,953.62	$748,762.23	$771,225.10	$794,361.85	$818,192.71	$ 842,738.49	$ 868,020.64	$ 894,061.26	$ 920,883.10
Security Services	Data Breach Diagnostics - Small (Up to 3 Systems, 120 GB of File Storage, and 100 GB of uncompressed text Audit Logs)	Per Assessment		CCSD13370472-A	N/A	N/A	A			$ 79,573.26	$ 81,960.46	$ 84,419.27	$ 86,951.85	$ 89,560.40	$ 92,247.22	$ 95,014.63	$ 97,865.07	$ 100,801.02	$ 103,825.06
Security Services	Data Breach Diagnostics - Medium (Up to 10 Systems, 120 GB of File Storage, and 500 GB of uncompressed text Audit Logs)	Per Assessment		CCSD13370473-A	N/A	N/A	A			$ 152,227.11	$156,793.92	$161,497.74	$166,342.67	$171,332.95	$176,472.94	$ 181,767.13	$ 187,220.14	$ 192,836.74	$ 198,621.85
Security Services	Data Breach Diagnostics - Large (Up to 50 Systems, 120 GB of File Storage, and 2 TB of uncompressed text Audit Logs)	Per Assessment		CCSD13370474-A	N/A	N/A	A			$ 242,179.49	$249,444.87	$256,928.22	$264,636.06	$272,575.15	$280,752.40	$ 289,174.97	$ 297,850.22	$ 306,785.73	$ 315,989.30
Security Services	Mobile Device Management (MDM) - Design and implement - Small	Per Request		CCSD13370475-A	N/A	N/A	A			$ 113,478.39	$116,882.74	$120,389.22	$124,000.90	$127,720.93	$131,552.55	$ 135,499.13	$ 139,564.10	$ 143,751.03	$ 148,063.56
Security Services	Mobile Device Management (MDM) - Design and implement - Medium	Per Request		CCSD13370476-A	N/A	N/A	A			$ 235,952.01	$243,030.57	$250,321.49	$257,831.14	$265,566.07	$273,533.05	$ 281,739.04	$ 290,191.22	$ 298,896.95	$ 307,863.86
Security Services	Mobile Device Management (MDM) - Design and implement - Large	Per Request		CCSD13370477-A	N/A	N/A	A			$ 339,051.28	$349,222.82	$359,699.50	$370,490.49	$381,605.20	$393,053.36	$ 404,844.96	$ 416,990.31	$ 429,500.02	$ 442,385.02
Security Services	Mobile Device Management (MDM) - Design and implement - Very Large	Per Request		CCSD13370478-A	N/A	N/A	A			$ 553,553.11	$570,159.71	$587,264.50	$604,882.43	$623,028.90	$641,719.77	$ 660,971.36	$ 680,800.51	$ 701,224.52	$ 722,261.26
Security Services	Mobile Security Strategy and Roadmap - Small	Per Request		CCSD13370479-A	N/A	N/A	A			$ 82,341.03	$ 84,811.26	$ 87,355.59	$ 89,976.26	$ 92,675.55	$ 95,455.82	$ 98,319.49	$ 101,269.08	$ 104,307.15	$ 107,436.36
Security Services	Mobile Security Strategy and Roadmap – Medium	Per Request		CCSD13370480-A	N/A	N/A	A			$ 145,307.69	$149,666.92	$154,156.93	$158,781.64	$163,545.09	$168,451.44	$ 173,504.98	$ 178,710.13	$ 184,071.44	$ 189,593.58
Security Services	Mobile Security Strategy and Roadmap – Large	Per Request		CCSD13370481-A	N/A	N/A	A			$ 238 719,78	$ 245 881.37	$253 257.81	$260 855.55	$268 681.21	$276 741.65	$ 285 043.90	$ 293 595.22	$ 302 403.07	$ 311 475.17
Security Services	Mobile Security Strategy and Roadmap – Very Large	Per Request		CCSD13370482-A	N/A	N/A	A			$ 601,989.01	$620,048.68	$638,650.14	$657,809.64	$677,543.93	$697,870.25	$ 718,806.36	$ 740,370.55	$ 762,581.67	$ 785,459.12
Security Services	Security Training Assessment - Small (Agency or Office with up to 999 employees)	Per Assessment		CCSD13370483-A	N/A	N/A	A			$ 61,721.17	$ 63,572.81	$ 65,479.99	$ 67,444.39	$ 69,467.72	$ 71,551.75	$ 73,698.31	$ 75,909.26	$ 78,186.53	$ 80,532.13
Security Services	Security Training Assessment - Medium (Agency or Office with up to 9,999 employees)	Per Assessment		CCSD13370484-A	N/A	N/A	A			$ 86,354.29	$ 88,944.91	$ 91,613.26	$ 94,361.66	$ 97,192.51	$100,108.28	$ 103,111.53	$ 106,204.88	$ 109,391.03	$ 112,672.76
Security Services	Security Training Assessment - Large (Agency or Office with up to 10,000 employees)	Per Assessment		CCSD13370485-A	N/A	N/A	A			$ 110,987.40	$114,317.02	$117,746.53	$121,278.93	$124,917.30	$128,664.81	$ 132,524.76	$ 136,500.50	$ 140,595.52	$ 144,813.38
Security Services	Security Training - Design and Delivery - (Training Presentation Deliverable and one training session (Up to 4 Hours))	Per Request		CCSD13370486-A	N/A	N/A	A			$ 121,089.74	$124,722.44	$128,464.11	$132,318.03	$136,287.57	$140,376.20	$ 144,587.49	$ 148,925.11	$ 153,392.86	$ 157,994.65
Security Services	Identity Access Management - Design and Implement - Small	Per Request		CCSD13370487-A	N/A	N/A	A			$ 411,013.19	$423,343.58	$436,043.89	$449,125.21	$462,598.96	$476,476.93	$ 490,771.24	$ 505,494.38	$ 520,659.21	$ 536,278.98
Security Services	Identity Access Management - Design and Implement - Medium	Per Request		CCSD13370488-A	N/A	N/A	A			$ 568,775.82	$585,839.10	$603,414.27	$621,516.70	$640,162.20	$659,367.06	$ 679,148.08	$ 699,522.52	$ 720,508.19	$ 742,123.44
Security Services	Access Management - Design and Implement - Large	Per Request		CCSD13370489-A	N/A	N/A	A			$ 853,855.67	$879,471.35	$905,855.49	$933,031.15	$961,022.08	$989,852.75	$1,019,548.33	$1,050,134.78	$1,081,638.82	$1,114,087.99
Security Services	Identity Provisioning and Management - Design and Implement - Small	Per Request		CCSD13370490-A	N/A	N/A	A			$ 411,013.19	$423,343.58	$436,043.89	$449,125.21	$462,598.96	$476,476.93	$ 490,771.24	$ 505,494.38	$ 520,659.21	$ 536,278.98
Security Services	Identity Provisioning and Management - Design and Implement - Medium	Per Request		CCSD13370491-A	N/A	N/A	A			$ 568,775.82	$585,839.10	$603,414.27	$621,516.70	$640,162.20	$659,367.06	$ 679,148.08	$ 699,522.52	$ 720,508.19	$ 742,123.44
Security Services	Identity Provisioning and Management - Design and Implement - Large	Per Request		CCSD13370492-A	N/A	N/A	A			$ 853,855.67	$879,471.35	$905,855.49	$933,031.15	$961,022.08	$989,852.75	$1,019,548.33	$1,050,134.78	$1,081,638.82	$1,114,087.99
Security Services	Identity Governance and Management - Design and Implement - Small	Per Request		CCSD13370493-A	N/A	N/A	A			$ 411,013.19	$423,343.58	$436,043.89	$449,125.21	$462,598.96	$476,476.93	$ 490,771.24	$ 505,494.38	$ 520,659.21	$ 536,278.98
Security Services	Identity Governance and Management - Design and Implement - Medium	Per Request		CCSD13370494-A	N/A	N/A	A			$ 568,775.82	$585,839.10	$603,414.27	$621,516.70	$640,162.20	$659,367.06	$ 679,148.08	$ 699,522.52	$ 720,508.19	$ 742,123.44
Security Services	Identity Governance and Management - Design and Implement - Large	Per Request		CCSD13370495-A	N/A	N/A	A			$ 853,855.67	$879,471.35	$905,855.49	$933,031.15	$961,022.08	$989,852.75	$1,019,548.33	$1,050,134.78	$1,081,638.82	$1,114,087.99
Third Party Software	Unisys Mainframe - Software License Transfer - KMSYS	Per Mainframe Upgrade		CCSU13370496-A	N/A	N/A	A			$ 26,467.21	$ -	$ -	$ -	$ 26,467.21	$ -	$ -	$ -	$ -	$ -
Third Party Software	Unisys Mainframe - Software License Transfer - SMA OpCon	Per Mainframe Upgrade		CCSU13370497-A	N/A	N/A	A			$ 17,178.44	$ -	$ -	$ -	$ 17,178.44	$ -	$ -	$ -	$ -	$ -
Third Party Software	Unisys Mainframe - Software License Transfer - Sightline	Per Mainframe Upgrade		CCSU13370498-A	N/A	N/A	A			$ 351,280.92	$ -	$ -	$ -	$403,973.05	$ -	$ -	$ -	$ -	$ -
Strategy Workshop Services	Cloud Transformation Workshop for Single Tower	Per Workshop		CCSI13370499-A	N/A	N/A	A			$ 80,000.00	$ 82,400.00	$ 84,872.00	$ 87,418.16	$ 90,040.70	$ 92,741.93	$ 95,524.18	$ 98,389.91	$ 101,341.61	$ 104,381.85
Strategy Workshop Services	Cloud Transformation Workshop	Per Workshop		CCSI13370500-A	N/A	N/A	A			$ 118,200.00	$121,746.00	$125,398.38	$129,160.33	$133,035.14	$137,026.20	$ 141,136.98	$ 145,371.09	$ 149,732.22	$ 154,224.19
Orderable (Combined) Fully Managed Configurations																			

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	Product Name	Unit	Qty per config	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Windows pConfig - 1	Windows pConfig - 1; 2-way Quad-Core 2.0 GHz; GB RAM; Mirrored 146 15K Hard Drives; Windows Server 2008 R2	Per Server		CCSU13310219-A	N/A	N/A	A			$ 255.87	$ 258.94	$ 258.35	$ 257.76	$ 257.06	$ 256.25	$ 256.38	$ 256.38	$ 256.38	$ 256.38
Windows pConfig - 2	Windows pConfig - 2; 2-way Six-Core 2.4 GHz; GB RAM; Mirrored 146 15K Hard Drives; Windows Server 2008 R2	Per Server		CCSU13310220-A	N/A	N/A	A			$ 285.65	$ 287.97	$ 285.99	$ 284.35	$ 282.57	$ 280.63	$ 283.78	$ 283.78	$ 283.78	$ 283.78
Windows pConfig - 3	Windows pConfig - 3; 4-way Six-Core 2.0 GHz; GB RAM; SAN Attached Storage; Windows Server 2008 R2	Per Server		CCSU13310221-A	N/A	N/A	A			$ 308.34	$ 306.21	$ 298.79	$ 293.14	$ 287.24	$ 281.10	$ 295.92	$ 295.92	$ 295.92	$ 295.92
Windows pConfig - 4	Windows pConfig - 4; 2-way Six-Core 2.4 GHz; GB RAM; Mirrored 146 15K Hard Drives; Windows Server 2008 R2; Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization Site's Local SAN Storage from hourly data synchronization	Per Server		CCSU13310222-A	N/A	N/A	A			$ 290.11	$ 292.56	$ 290.72	$ 289.23	$ 287.59	$ 285.80	$ 288.38	$ 288.38	$ 288.38	$ 288.38
Windows pConfig - 5	Windows pConfig - 5; 2-way Six-Core 2.4 GHz; GB RAM; Mirrored 146 15K Hard Drives; Windows Server 2008 R2; Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from Backup off-site tape Backups	Per Server		CCSU13310223-A	N/A	N/A	A			$ 285.65	$ 287.97	$ 285.99	$ 284.35	$ 282.57	$ 280.63	$ 283.78	$ 283.78	$ 283.78	$ 283.78
Linux pConfig - 1	Linux pConfig - 1 ; 2-way Quad-Core 2.0 GHz; 4 GB RAM; Mirrored 146 15K Hard Drives; RedHat or SUSE	Per Server		CCSU13310224-A	N/A	N/A	A			$ 230.31	$ 232.70	$ 231.46	$ 230.06	$ 228.53	$ 226.86	$ 230.27	$ 230.27	$ 230.27	$ 230.27
Linux pConfig - 2	Linux pConfig - 2 ; 2-way Six-Core 2.4 GHz; 16 GB RAM; Mirrored 146 15K Hard Drives; RedHat or SUSE	Per Server		CCSU13310225-A	N/A	N/A	A			$ 259.45	$ 261.35	$ 259.09	$ 256.65	$ 254.03	$ 251.24	$ 257.67	$ 257.67	$ 257.67	$ 257.67
Linux pConfig - 3	Linux pConfig - 3 ; 4-way Six-Core 2.0 GHz; 64 GB RAM; SAN Attached Storage; RedHat or SUSE	Per Server		CCSU13310226-A	N/A	N/A	A			$ 279.62	$ 278.08	$ 271.90	$ 265.44	$ 258.71	$ 251.71	$ 269.81	$ 269.81	$ 269.81	$ 269.81
Linux pConfig - 4	Linux pConfig - 4; 2-way Six-Core 2.4 GHz; 16 GB RAM; Mirrored 146 15K Hard Drives; RedHat or SUSE; Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Server		CCSU13310227-A	N/A	N/A	A			$ 263.91	$ 265.95	$ 263.83	$ 261.53	$ 259.05	$ 256.42	$ 262.27	$ 262.27	$ 262.27	$ 262.27
Linux pConfig - 5	Linux pConfig - 5; 2-way Six-Core 2.4 GHz; 16 GB RAM; Mirrored 146 15K Hard Drives; RedHat or SUSE; Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Server		CCSU13310228-A	N/A	N/A	A			$ 259.45	$ 261.35	$ 259.09	$ 256.65	$ 254.03	$ 251.24	$ 257.67	$ 257.67	$ 257.67	$ 257.67
Windows vConfig - 1	Windows vConfig - 1; 2vCPU; GB Ram; Windows Server 2008 R2; Firewall/IDS; Site-Site VPN; VPN Client; VLAN	Per Server		CCSU13310229-A	N/A	N/A	A			$ 23.89	$ 23.29	$ 23.08	$ 22.81	$ 22.67	$ 22.06	$ 21.31	$ 21.31	$ 21.31	$ 21.31
Windows vConfig - 2	Windows vConfig - 2; 4vCPU; GB Ram; Windows Server 2008 R2; Firewall/IDS; Site-Site VPN; VPN Client; VLAN	Per Server		CCSU13310230-A	N/A	N/A	A			$ 51.90	$ 51.23	$ 50.90	$ 50.52	$ 50.24	$ 48.50	$ 47.68	$ 47.68	$ 47.68	$ 47.68
Windows vConfig - 3	Linux vConfig - 3; 8vCPU; GB Ram; RedHat or SUSE; Firewall/IDS; Site-Site VPN; VPN Client; VLAN	Per Server		CCSU13310231-A	N/A	N/A	A			$ 160.11	$ 159.23	$ 158.52	$ 157.72	$ 156.95	$ 151.28	$ 150.26	$ 150.26	$ 150.26	$ 150.26
Windows vConfig - 4	Windows vConfig - 4; 4vCPU; GB Ram; Windows Server 2008 R2; Firewall/IDS; Site-Site VPN; VPN Client; VLAN; Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Server		CCSU13310232-A	N/A	N/A	A			$ 51.90	$ 51.23	$ 50.90	$ 50.52	$ 50.24	$ 48.50	$ 47.68	$ 47.68	$ 47.68	$ 47.68
Windows vConfig - 5	Windows vConfig - 5; 4vCPU; GB Ram; Windows Server 2008 R2; Firewall/IDS; Site-Site VPN; VPN Client; VLAN; Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Server		CCSU13310233-A	N/A	N/A	A			$ 51.90	$ 51.23	$ 50.90	$ 50.52	$ 50.24	$ 48.50	$ 47.68	$ 47.68	$ 47.68	$ 47.68
Linux vConfig - 1	Linux vConfig - 1; 2vCPU; GB Ram; RedHat or SUSE; Firewall/IDS; Site-Site VPN; VPN Client; VLAN	Per Server		CCSU13310234-A	N/A	N/A	A			$ 23.75	$ 23.16	$ 22.94	$ 22.67	$ 22.54	$ 21.93	$ 21.17	$ 21.17	$ 21.17	$ 21.17
Linux vConfig - 2	Linux vConfig - 2; 4vCPU; GB Ram; RedHat or SUSE; Firewall/IDS; Site-Site VPN; VPN Client; VLAN	Per Server		CCSU13310235-A	N/A	N/A	A			$ 51.76	$ 51.09	$ 50.76	$ 50.38	$ 50.10	$ 48.36	$ 47.54	$ 47.54	$ 47.54	$ 47.54
Linux vConfig - 3	Linux vConfig - 3; 8vCPU; GB Ram; RedHat or SUSE; Firewall/IDS; Site-Site VPN; VPN Client; VLAN	Per Server		CCSU13310236-A	N/A	N/A	A			$ 159.97	$ 159.09	$ 158.38	$ 157.58	$ 156.81	$ 151.15	$ 150.12	$ 150.12	$ 150.12	$ 150.12

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	Product Name	Unit	Qty per config	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Linux vConfig - 4	Linux vConfig - 4; 4vCPU; GB Ram; RedHat or SUSE; Firewall/IDS; Site-Site VPN; VPN Client; VLAN; Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Server		CCSU13310237-A	N/A	N/A	A			$ 51.76	$ 51.09	$ 50.76	$ 50.38	$ 50.10	$ 48.36	$ 47.54	$ 47.54	$ 47.54	$ 47.54
Linux vConfig - 5	Linux vConfig - 5; 4vCPU; GB Ram; RedHat or SUSE; Firewall/IDS; Site-Site VPN; VPN Client; VLAN; Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Server		CCSU13310238-A	N/A	N/A	A			$ 51.76	$ 51.09	$ 50.76	$ 50.38	$ 50.10	$ 48.36	$ 47.54	$ 47.54	$ 47.54	$ 47.54
AIX Config - 1	AIX Config - 1; 3.0GHz POWER7; 0.5 Cores; 6 GB RAM; AIX	Per Server		CCSI13310239-A	N/A	N/A	A			$ 171.51	$ 172.87	$ 173.38	$ 175.63	$ 177.09	$ 178.50	$ 180.78	$ 183.94	$ 182.85	$ 181.73
AIX Config - 2	AIX Config - 2; 3.0GHz POWER7; 1.0 Cores; 12 GB RAM; AIX	Per Server		CCSI13310240-A	N/A	N/A	A			$ 194.80	$ 195.94	$ 196.23	$ 198.25	$ 199.56	$ 200.76	$ 202.82	$ 205.76	$ 204.53	$ 203.19
AIX Config - 3	AIX Config - 3; 3.0GHz POWER7; 1.5 Cores; 18 GB RAM; AIX	Per Server		CCSI13310241-A	N/A	N/A	A			$ 218.10	$ 219.00	$ 219.07	$ 220.88	$ 222.04	$ 223.01	$ 224.85	$ 227.58	$ 226.21	$ 224.65
AIX Config - 4	AIX Config - 4; 3.0GHz POWER7; 1.0 Cores; 12 GB RAM; AIX; Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Server		CCSI13310242-A	N/A	N/A	A			$ 194.80	$ 195.94	$ 196.23	$ 198.25	$ 199.56	$ 200.76	$ 202.82	$ 205.76	$ 204.53	$ 203.19
AIX Config - 5	AIX Config - 5; 3.0GHz POWER7; 1.0 Cores; 12 GB RAM; AIX; Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Server		CCSI13310243-A	N/A	N/A	A			$ 194.80	$ 195.94	$ 196.23	$ 198.25	$ 199.56	$ 200.76	$ 202.82	$ 205.76	$ 204.53	$ 203.19
Co-Lo Config - 1	Co-Lo Config - 1; 1/4 Rack Configuration includes: 10U Cabinet Space; GB Network Bandwidth; 100Mb/s Uplink; IP Addresses; 110V AC Circuits	Per Rack		CCSU13330008-A	N/A	N/A	A			$ 49.85	$ 50.23	$ 50.63	$ 51.04	$ 53.10	$ 53.53	$ 53.98	$ 53.98	$ 53.98	$ 53.98
Co-Lo Config - 2	Co-Lo Config - 2; 1/2 Rack Configuration includes: 21U Cabinet Space; 10,000 GB Network Bandwidth; 100Mb/s Uplink; IP Addresses; 110V AC Circuits	Per Rack		CCSU13330009-A	N/A	N/A	A			$ 75.65	$ 76.42	$ 77.21	$ 78.03	$ 80.51	$ 81.38	$ 82.27	$ 82.27	$ 82.27	$ 82.27
Co-Lo Config - 3	Co-Lo Config - 3 ; Full Rack Configuration includes: 42U Cabinet Space; GB Network Bandwidth; 100Mb/s Uplink; IP Addresses; 110V AC Circuits	Per Rack		CCSU13330010-A	N/A	N/A	A			$ 135.48	$ 137.01	$ 138.59	$ 140.22	$ 144.55	$ 146.09	$ 147.67	$ 147.67	$ 147.67	$ 147.67
IBM Mainframe Config - 1	IBM Mainframe Config - 1;IBM System zEnterprise Processor z/OS	Per MIP		CCSI13310244-A	N/A	N/A	A			$ 75.03	$ 71.28	$ 67.72	$ 64.33	$ 61.11	$ 58.06	$ 55.16	$ 55.16	$ 55.16	$ 55.16
IBM Mainframe Config - 2	IBM Mainframe Config - 2; IBM System zEnterprise Processor Virtual Linux Prod IFL	Per MIP		CCSI13310245-A	N/A	N/A	A			$ 65.93	$ 62.63	$ 59.50	$ 56.52	$ 53.70	$ 51.01	$ 48.46	$ 48.46	$ 48.46	$ 48.46
IBM Mainframe Config - 3	IBM Mainframe Config - 3; IBM System zEnterprise Processor Virtual Linux Prod IFL; Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per MIP		CCSI13310246-A	N/A	N/A	A			$ 65.93	$ 62.63	$ 59.50	$ 56.52	$ 53.70	$ 51.01	$ 48.46	$ 48.46	$ 48.46	$ 48.46
IBM AS400 Config 1	IBM AS400 Config 1; IBM i Series / AS400	Per CPW		CCSI13310247-A	N/A	N/A	A			$ 8.19	$ 7.78	$ 7.39	$ 7.02	$ 6.67	$ 6.33	$ 6.02	$ 6.02	$ 6.02	$ 6.02
IBM AS400 Config 2	IBM AS400 Config 2; IBM i Series / AS400; Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per CPW		CCSI13310248-A	N/A	N/A	A			$ 8.19	$ 7.78	$ 7.39	$ 7.02	$ 6.67	$ 6.33	$ 6.02	$ 6.02	$ 6.02	$ 6.02
Unisys Mainframe Config - 1	Unisys Mainframe Config - 1; Unisys (Clearpath / Dorado)	Per MIP		CCSU13310249-A	N/A	N/A	A			$ 761.89	$ 751.54	$ 748.05	$ 744.76	$ 739.62	$ 738.04	$ 727.07	$ 727.07	$ 727.07	$ 727.07
Unisys Mainframe Config - 2	Unisys Mainframe Config - 2; Unisys (Clearpath / Libra) ;	Per MIP		CCSU13310250-A	N/A	N/A	A			$ 746.21	$ 739.37	$ 734.46	$ 733.45	$ 732.19	$ 732.01	$ 727.08	$ 727.08	$ 727.08	$ 727.08
Unisys Mainframe Config - 3	Unisys Mainframe Config - 3; Unisys (Clearpath / Dorado); Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per MIP		CCSU13310251-A	N/A	N/A	A			$ 7.43	$ 7.38	$ 7.34	$ 7.33	$ 7.33	$ 7.01	$ 6.98	$ 6.98	$ 6.98	$ 6.98
Unisys Mainframe Config - 4	Unisys Mainframe Config - 4; Unisys (Clearpath / Libra) ; Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per MIP		CCSU13310252-A	N/A	N/A	A			$ 10.83	$ 10.81	$ 10.81	$ 10.76	$ 10.74	$ 10.57	$ 10.39	$ 10.39	$ 10.39	$ 10.39
IaaS Windows vConfig - 1	IaaS Windows vConfig - 1; 2vCPU; GB Ram; Windows Server 2008 R2; Firewall/IDS; Site-Site VPN; VPN Client; VLAN	Per Server		CCSU13340029-A	N/A	N/A	A			$ 34.01	$ 32.62	$ 31.63	$ 31.55	$ 30.35	$ 30.29	$ 29.24	$ 29.24	$ 29.24	$ 29.24
IaaS Windows vConfig - 2	IaaS Windows vConfig - 2; 4vCPU; GB Ram; Windows Server 2008 R2; Firewall/IDS; Site-Site VPN; VPN Client; VLAN	Per Server		CCSU13340030-A	N/A	N/A	A			$ 71.32	$ 67.67	$ 64.74	$ 63.03	$ 59.99	$ 57.82	$ 55.46	$ 55.46	$ 55.46	$ 55.46

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	**Product Name**	**Unit**	**Qty per config**	**Provider Part Number**	**Version Major**	**Version Minor**	**Version Build**	**Manufacturer ID**	**Equipment Code**	**Price per unit \ Per Month**									
Description / Use *>*	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
IaaS Windows vConfig - 3	IaaS Windows vConfig - 3; 8vCPU; GB Ram; Windows Server 2008 R2; Firewall/IDS; Site-Site VPN; VPN Client; VLAN	Per Server		CCSU13340031-A	N/A	N/A	A			$ 215.51	$ 203.31	$ 192.95	$ 184.96	$ 174.88	$ 164.81	$ 157.31	$ 157.31	$ 157.31	$ 157.31
IaaS Windows vConfig - 4	IaaS Windows vConfig - 4; 4vCPU; GB Ram; Windows Server 2008 R2; Firewall/IDS; Site-Site VPN; VPN Client; VLAN; Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Server		CCSU13340032-A	N/A	N/A	A			$ 71.32	$ 67.67	$ 64.74	$ 63.03	$ 59.99	$ 57.82	$ 55.46	$ 55.46	$ 55.46	$ 55.46
IaaS Windows vConfig - 5	IaaS Windows vConfig - 5; 4vCPU; GB Ram; Windows Server 2008 R2; Firewall/IDS; Site-Site VPN; VPN Client; VLAN; Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Server		CCSU13340033-A	N/A	N/A	A			$ 71.32	$ 67.67	$ 64.74	$ 63.03	$ 59.99	$ 57.82	$ 55.46	$ 55.46	$ 55.46	$ 55.46
IaaS Linux vConfig - 1	IaaS Linux vConfig - 1; 2vCPU; 4 GB Ram; RedHat or SUSE; Firewall/IDS; Site-Site VPN; VPN Client; VLAN	Per Server		CCSU13340034-A	N/A	N/A	A			$ 33.87	$ 32.48	$ 31.49	$ 31.41	$ 30.22	$ 30.16	$ 29.11	$ 29.11	$ 29.11	$ 34.42
IaaS Linux vConfig - 2	IaaS Linux vConfig - 2; 4vCPU; 16 GB Ram; RedHat or SUSE; Firewall/IDS; Site-Site VPN; VPN Client; VLAN	Per Server		CCSU13340035-A	N/A	N/A	A			$ 71.18	$ 67.53	$ 64.60	$ 62.90	$ 59.86	$ 57.69	$ 55.32	$ 55.32	$ 50.10	$ 71.34
IaaS Linux vConfig - 3	IaaS Linux vConfig - 3; 8vCPU; 64 GB Ram; RedHat or SUSE; Firewall/IDS; Site-Site VPN; VPN Client; VLAN	Per Server		CCSU13340036-A	N/A	N/A	A			$ 215.37	$ 203.17	$ 192.81	$ 184.82	$ 174.74	$ 164.68	$ 157.17	$ 157.17	$ 134.08	$ 219.02
IaaS Linux vConfig - 4	IaaS Linux vConfig - 4; 4vCPU; 16 GB Ram; RedHat or SUSE; Firewall/IDS; Site-Site VPN; VPN Client; VLAN; Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Server		CCSU13340037-A	N/A	N/A	A			$ 71.18	$ 67.53	$ 64.60	$ 62.90	$ 59.86	$ 57.69	$ 55.32	$ 55.32	$ 50.10	$ 71.34
IaaS Linux vConfig - 5	IaaS Linux vConfig - 5; 4vCPU; 16 GB Ram; RedHat or SUSE; Firewall/IDS; Site-Site VPN; VPN Client; 741; Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Server		CCSU13340038-A	N/A	N/A	A			$ 71.18	$ 67.53	$ 64.60	$ 62.90	$ 59.86	$ 57.69	$ 55.32	$ 55.32	$ 50.10	$ 71.34
IaaS Storage Config - 1	IaaS Storage Config - 1; SAN attached storage; Raid 5; 10K - 15K RPM discs	Per GB		CCSU13340039-A	N/A	N/A	A			$ 0.06	$ 0.05	$ 0.05	$ 0.05	$ 0.05	$ 0.04	$ 0.04	$ 0.04	$ 0.03	$ 0.03
IaaS Storage Config - 2	IaaS Storage Config - 2; SAN attached storage; Raid 10; 10K - 15K RPM discs	Per GB		CCSU13340040-A	N/A	N/A	A			$ 0.24	$ 0.24	$ 0.24	$ 0.23	$ 0.23	$ 0.23	$ 0.23	$ 0.21	$ 0.19	$ 0.17
IaaS Storage Config - 3	IaaS Storage Config - 3; Network Attached Storage	Per GB		CCSU13340041-A	N/A	N/A	A			$ 0.07	$ 0.06	$ 0.06	$ 0.05	$ 0.05	$ 0.03	$ 0.03	$ 0.03	$ 0.03	$ 0.02
Other (insert description)										$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Other (insert description)										$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
										$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
										$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
										$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
										$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -

Within Schedule I, Description and Instructions tab under the Additional Notes (item c) section, the Commonwealth specifically requires that the Offeror must verify that all calculations, subtotal costs and grand total costs are accurate. In order to comply with this Commonwealth's requirement within the Offeror Pricing Forms (Schedule I), Unisys would like to bring to the Commonwealth's attention specific actions that were performed within the Offeror Pricing Forms (Schedule I). Unisys was required to make the following adjustments within Schedule I to allow the calculations, subtotal costs and grand total costs to be accurate. It is important to note that the adjustments were made with the sole purpose for allowing the Commonwealth to receive accurate costs from Unisys.

Adjustments required in order for all the calculations, subtotal costs and grand total costs to be accurate:

1) Catalog of Services, cells K627 through T627 had the value zeroed out to eliminate the double counting of the production machines
2) Catalog of Services, cells K619 through T621, K624 through T626, K630 through T632, K636 through T638 were modified by removing the "multiplication" (*) in the formula and replaced with "addition" (+) so the formula added infrastructure to Labor rather multiplying these figures.

Please note that the above adjustments are the specific areas within Schedule I that were modified to allow the calculations, subtotal cost and grand total costs to be accurate. Other calculations within Schedule I may have been impacted where these specific areas were included as part of the calculation in other sections of Schedule I.

As a result of these changes, the accurate Unisys grand total costs for the 10 year view to the Commonwealth totals $ 1,307,723,598. If the calculations were not modified within Schedule I, then the grand total costs for the 10 year view would have totaled $ 18,761,284,558 resulting in a material overstatement of the costs to the Commonwealth.

APPENDIX B - PROPOSAL COVER SHEET
COMMONWEALTH OF PENNSYLVANIA
OFFICE OF ADMINISTRATION – OFFICE FOR INFORMATION TECHNOLOGY
RFP# 6100022698

Enclosed in three separately sealed submittals is the proposal of the Offeror identified below for the above-referenced RFP:

Offeror Information:	
Offeror Name	Unisys Corporation
Offeror Mailing Address	4750 Lindle Road Harrisburg, Pennsylvania 17111
Offeror Website	www.unisys.com
Offeror Contact Person	Dean Shaner
Contact Person's Phone Number	(717) 526-1267
Contact Person's Facsimile Number	(717) 526-1175
Contact Person's E-Mail Address	dean.shaner@unisys.com
Offeror Federal ID Number	[redacted]
Offeror SAP/SRM Vendor Number	163299

Submittals Enclosed and Separately Sealed:	
	Technical Submittal
X	Disadvantaged Business Submittal
	Cost Submittal

Signature	
Signature of an official authorized to bind the Offeror to the provisions contained in the Offeror's proposal:	[redacted]
Printed Name	Ron Frankenfield
Title	Senior Vice President/President Global Managed Services

FAILURE TO COMPLETE, SIGN AND RETURN THIS FORM WITH THE OFFEROR'S PROPOSAL MAY RESULT IN THE REJECTION OF THE OFFEROR'S PROPOSAL

Unisys Response to

Commonwealth of Pennsylvania
Office of Administration
Office for Information Technology

Data Center Computing Services

Request for Proposal (RFP)
RFP 6100022698

Small Diverse Business Participation Submittal

June 19, 2013

This proposal has been reproduced on recycled paper

Contents

SMALL DIVERSE BUSINESS (SDB) PARTICIPATION SUBMITTAL (RFP REQUIREMENT II-9)..... 2

1.1 INTRODUCTION..... 2
1.2 A – PROOF OF SDB QUALIFYING DATA..... 3
1.2.1 Small Diverse Business Bureau of Small Business Opportunities (BSBO) Verifications..... 4
1.2.1.1 Acclaim Systems, Inc. – BSBO Verification Letter..... 4
1.2.1.2 American Personnel Managers and Consultants, Inc.—BSBO Verification Letter..... 5
1.2.1.3 Credo Technology Solutions, Inc. – BSBO Verification Letter..... 6
1.2.1.4 Domino Technologies, Inc.—BSBO Verification Letter..... 7
1.2.1.5 e & e IT Consulting Services, Inc.—BSBO Verification Letter..... 8
1.2.1.6 Info-Matrix Corporation—BSBO Verification Letter..... 9
1.2.1.7 Innovative Business Concepts, Inc.—BSBO Verification Letter..... 10
1.2.1.8 Latus Commercial Reality—BSBO Verification Letter..... 11
1.2.1.9 The Metropolitan Technology Services Group LLC—BSBO Verification Letter..... 12
1.2.1.10 PC Network, Inc.—BSBO Verification Letter..... 13
1.2.1.11 Pierson Computing Connection, Inc.—BSBO Verification Letter..... 14
1.3 B – SMALL DIVERSE BUSINESS PARTICIPATION..... 15
1.3.1 Numerical Percentage of Work Performed by the Small Diverse Businesses..... 15
1.3.1.1 (a) Percentage of Dollar Amount – Each Subcontract Commitment to Small Diverse Business..... 16
1.3.1.2 (b) Identified Small Diverse Business Entity..... 16
1.3.1.3 (c) Services or Supplies and Timeframe Provided By Each Small Diverse Business..... 17
1.3.1.4 (d) Location Where Each Small Diverse Business Will Provide Services or Supplies..... 17
1.3.1.5 (e) Timeframe for Each Small Diverse Business to Provide or Deliver Goods or Services..... 18
1.3.1.6 (f) Letters of Intent..... 19
1.3.1.7 (g) Small Diverse Businesses – Primary Person Contact Information..... 31
1.3.1.8 Total Percentages and SDB Subcontractor Commitment Contractual Obligation..... 32
1.3.1.9 Offeror's Project Person for Small Diverse Business information - Contact Information..... 32

Small Diverse Business (SDB) Participation Submittal (RFP Requirement II-9)

1.1 Introduction

Unisys carefully considered all available certified Small Diverse Businesses (SDB) in the Commonwealth of Pennsylvania that both complimented and extended Unisys' capabilities and operations providing CoPA with a strong and qualified team (Figure 1). These selected SDBs have these requirements in addition to their experience in the required area of support and their dedication to quality.

In addition to managing and coordinating SDB support requirements, Unisys is committed to mentoring SDB leadership and fostering their growth. The intention is to provide opportunities for them to excel and to provide feedback and dialog that improves and strengthens the SDBs' performance. This philosophy strengthens CoPA's SDBs workforce for this current CoPA project and future projects as well.

Figure 1. Unisys and Small Diverse Businesses (SDB) Provide a Synchronized Team. *Unisys and the SDBs combined functionality provide CoPA with a fully coordinated team.*

1.2 A – Proof of SDB Qualifying Data

RFP	*Requirement*
II-9 A	*To receive credit for being a Small Diverse Business or for subcontracting with a Small Diverse Business (including purchasing supplies and/or services through a purchase agreement), an Offeror must include proof of Small Diverse Business qualification in the Small Diverse Business participation submittal of the proposal, as indicated below:* • *A Small Diverse Business verified by BSBO as a Small Diverse Business must provide a photocopy of their verification letter.*

Unisys has partnered with 11 subcontractors and suppliers that qualify as Pennsylvania Small Diverse Businesses (SDB). Each is currently verified by the Pennsylvania Department of General Services Bureau of Small Business Opportunities (BSBO). Table 1 summarizes proof of the qualifying data. Copies of BSBO verification letters follow this table.

Table 1. Proof of Small Diverse Business Qualification

Subcontractor (SDB) Name	**Vendor Type**	**Certification**
Acclaim Systems, Inc.	MBE	BSBO Verification Letter
American Personnel Managers & Consultants, Inc.	WBE	BSBO Verification Letter
Credo Technology Solutions, Inc.	MBE	BSBO Verification Letter
Domino Technologies, Inc.	MBE	BSBO Verification Letter
E & E IT Consulting Services, Inc.	WBE	BSBO Verification Letter
Info-Matrix Corp	WBE	BSBO Verification Letter
Innovative Business Concepts, Inc.	WBE	BSBO Verification Letter
Latus Capital Advisors Inc.	WBE	BSBO Verification Letter
Metropolitan Services Technology Group LLC	WBE	BSBO Verification Letter
PC Network, Inc.	WBE	BSBO Verification Letter
Pierson Computing Connection, Inc.	WBE	BSBO Verification Letter

1.2.1 Small Diverse Business Bureau of Small Business Opportunities (BSBO) Verifications

1.2.1.1 Acclaim Systems, Inc. – BSBO Verification Letter

pennsylvania
DEPARTMENT OF GENERAL SERVICES

September 6, 2012

Kailash Kalantri
Acclaim Systems Inc
203 E Pennsylvania Boulevard
Feasterville, PA 19053

CERTIFICATIO NO: **163086-2012-07-S**
EXPIRATION DATE: **July 31, 2013**

The Bureau of Small Business Opportunities has reviewed your Recertification Application together with supporting documents. I am pleased to inform you that your company has been approved based on your certification application and your small business self-certification registration through the Small Business Procurement Initiative (SBPI). The Commonwealth now recognizes your company as a Small Business and a Small Diverse Business.

Through the application process, you have presented documentation that your company is engaged in providing certain products and/or services. Information regarding these products and/or services for which you have been certified has been electronically listed in the DGS database for use by all Commonwealth agencies. Please understand that your certification is a tool that you can use to market your goods or services to Commonwealth agencies.

Your certification is valid until the expiration date noted above. For additional information or assistance, please contact Bureau staff at (717) 783-3119 or by email at gs-bsbo@pa.gov. Best wishes in your business endeavors.

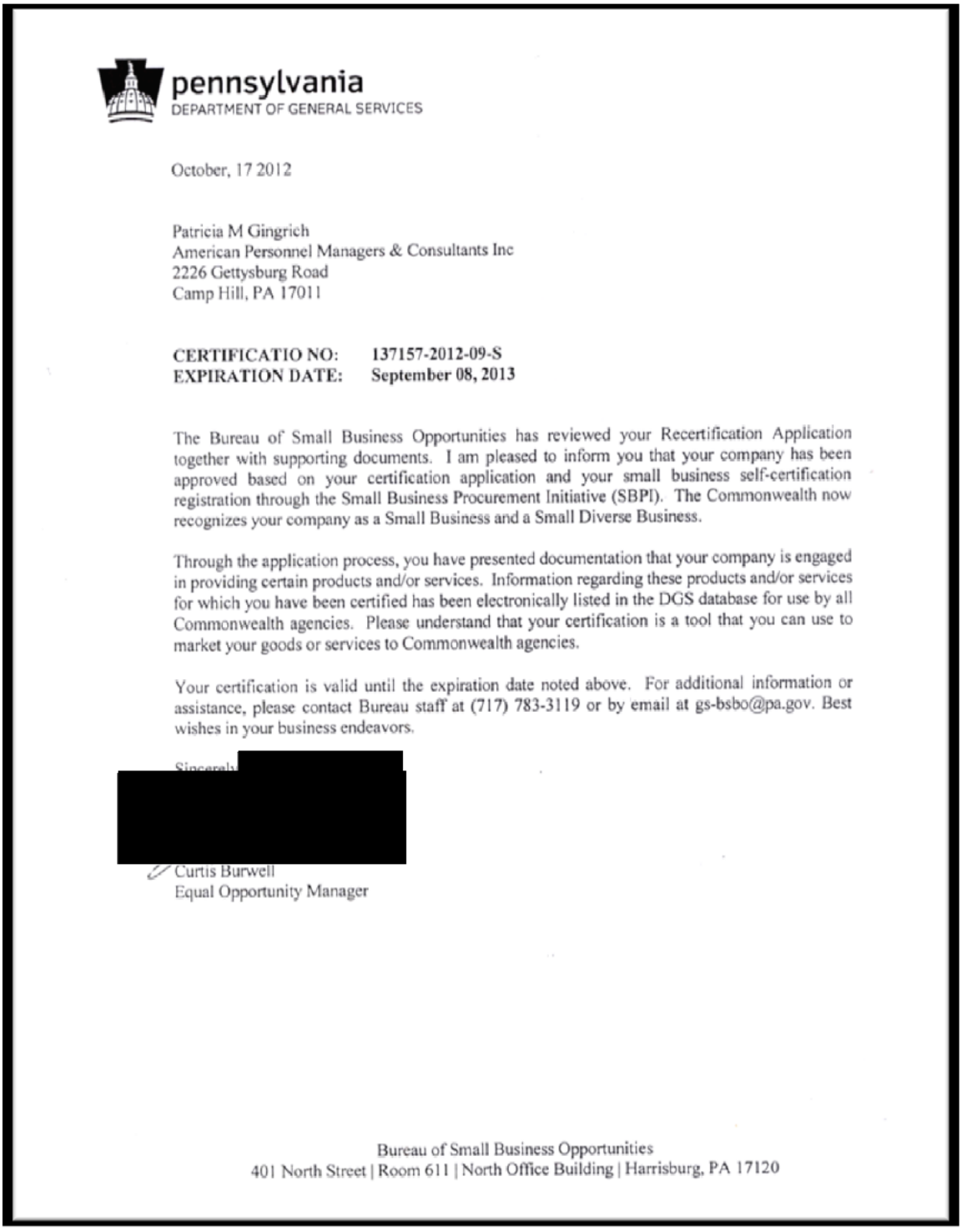
Sincerely,

[redacted]

Curtis Burwell
Equal Opportunity Manager

Bureau of Small Business Opportunities
401 North Street | Room 611 | North Office Building | Harrisburg, PA 17120

1.2.1.2 American Personnel Managers and Consultants, Inc.—BSBO Verification Letter



pennsylvania
DEPARTMENT OF GENERAL SERVICES

October, 17 2012

Patricia M Gingrich
American Personnel Managers & Consultants Inc
2226 Gettysburg Road
Camp Hill, PA 17011

CERTIFICATIO NO: **137157-2012-09-S**
EXPIRATION DATE: **September 08, 2013**

The Bureau of Small Business Opportunities has reviewed your Recertification Application together with supporting documents. I am pleased to inform you that your company has been approved based on your certification application and your small business self-certification registration through the Small Business Procurement Initiative (SBPI). The Commonwealth now recognizes your company as a Small Business and a Small Diverse Business.

Through the application process, you have presented documentation that your company is engaged in providing certain products and/or services. Information regarding these products and/or services for which you have been certified has been electronically listed in the DGS database for use by all Commonwealth agencies. Please understand that your certification is a tool that you can use to market your goods or services to Commonwealth agencies.

Your certification is valid until the expiration date noted above. For additional information or assistance, please contact Bureau staff at (717) 783-3119 or by email at gs-bsbo@pa.gov. Best wishes in your business endeavors.

Sincerely,

[redacted]

Curtis Burwell
Equal Opportunity Manager

Bureau of Small Business Opportunities
401 North Street | Room 611 | North Office Building | Harrisburg, PA 17120

1.2.1.3 Credo Technology Solutions, Inc. – BSBO Verification Letter

pennsylvania
DEPARTMENT OF GENERAL SERVICES

October, 19 2012

Jogendra Daita
Credo Technology Solutions Inc
110 Sunset Avenue
Suite 101
Harrisburg, PA 17112

CERTIFICATIO NO: 378902-2012-09-S
EXPIRATION DATE: September 14, 2013

The Bureau of Small Business Opportunities has reviewed your Certification Application together with supporting documents. I am pleased to inform you that your company has been approved based on your certification application and your small business self-certification registration through the Small Business Procurement Initiative (SBPI). The Commonwealth now recognizes your company as a Small Business and a Small Diverse Business.

Through the application process, you have presented documentation that your company is engaged in providing certain products and/or services. Information regarding these products and/or services for which you have been certified has been electronically listed in the DGS database for use by all Commonwealth agencies. Please understand that your certification is a tool that you can use to market your goods or services to Commonwealth agencies.

Your certification is valid until the expiration date noted above. For additional information or assistance, please contact Bureau staff at (717) 783-3119 or by email at gs-bsbo@pa.gov. Best wishes in your business endeavors.

Sincerely,

[redacted]

Curtis Burwell
Equal Opportunity Manager

Bureau of Small Business Opportunities
401 North Street | Room 611 | North Office Building | Harrisburg, PA 17120

1.2.1.4 Domino Technologies, Inc.—BSBO Verification Letter

pennsylvania
DEPARTMENT OF GENERAL SERVICES

October, 19 2012

Swami Nathan Balagopal
Domino Technologies Inc
6211 Lookout Drive
Mechanicsburg, PA 17050

CERTIFICATIO NO: **176163-2012-10-S**
EXPIRATION DATE: **October 3, 2013**

The Bureau of Small Business Opportunities has reviewed your Recertification Application together with supporting documents. I am pleased to inform you that your company has been approved based on your certification application and your small business self-certification registration through the Small Business Procurement Initiative (SBPI). The Commonwealth now recognizes your company as a Small Business and a Small Diverse Business.

Through the application process, you have presented documentation that your company is engaged in providing certain products and/or services. Information regarding these products and/or services for which you have been certified has been electronically listed in the DGS database for use by all Commonwealth agencies. Please understand that your certification is a tool that you can use to market your goods or services to Commonwealth agencies.

Your certification is valid until the expiration date noted above. For additional information or assistance, please contact Bureau staff at (717) 783-3119 or by email at gs-bsbo@pa.gov. Best wishes in your business endeavors.

Sincerely,

[redacted]

Equal Opportunity Manager

Bureau of Small Business Opportunities
401 North Street | Room 611 | North Office Building | Harrisburg, PA 17120

1.2.1.5 e & e IT Consulting Services, Inc.—BSBO Verification Letter

pennsylvania
DEPARTMENT OF GENERAL SERVICES

September 7, 2012

Linda K Etter
E & E IT Consulting Services Inc
2010 State Road
Suite 100
Camp Hill, PA 17011

CERTIFICATIO NO: **202218-2012-08-S**
EXPIRATION DATE: **August 16, 2013**

The Bureau of Small Business Opportunities has reviewed your Recertification Application together with supporting documents. I am pleased to inform you that your company has been approved based on your certification application and your small business self-certification registration through the Small Business Procurement Initiative (SBPI). The Commonwealth now recognizes your company as a Small Business and a Small Diverse Business.

Through the application process, you have presented documentation that your company is engaged in providing certain products and/or services. Information regarding these products and/or services for which you have been certified has been electronically listed in the DGS database for use by all Commonwealth agencies. Please understand that your certification is a tool that you can use to market your goods or services to Commonwealth agencies.

Your certification is valid until the expiration date noted above. For additional information or assistance, please contact Bureau staff at (717) 783-3119 or by email at gs-bsbo@pa.gov. Best wishes in your business endeavors.

Sincerely,

[redacted]

Curtis Burwell
Equal Opportunity Manager

Bureau of Small Business Opportunities
401 North Street | Room 611 | North Office Building | Harrisburg, PA 17120

1.2.1.6 Info-Matrix Corporation—BSBO Verification Letter

pennsylvania
DEPARTMENT OF GENERAL SERVICES

September 7, 2012

Brenda Ritter Orth
Info Matrix Corporation
1335 North Front Street
Harrisburg, PA 17102

CERTIFICATIO NO: **156374-2012-07-S**
EXPIRATION DATE: **July 26, 2013**

The Bureau of Small Business Opportunities has reviewed your Recertification Application together with supporting documents. I am pleased to inform you that your company has been approved based on your certification application and your small business self-certification registration through the Small Business Procurement Initiative (SBPI). The Commonwealth now recognizes your company as a Small Business and a Small Diverse Business.

Through the application process, you have presented documentation that your company is engaged in providing certain products and/or services. Information regarding these products and/or services for which you have been certified has been electronically listed in the DGS database for use by all Commonwealth agencies. Please understand that your certification is a tool that you can use to market your goods or services to Commonwealth agencies.

Your certification is valid until the expiration date noted above. For additional information or assistance, please contact Bureau staff at (717) 783-3119 or by email at gs-bsbo@pa.gov. Best wishes in your business endeavors.

Sincerely,

[redacted]

Curtis Burwell
Equal Opportunity Manager

Bureau of Small Business Opportunities
401 North Street | Room 611 | North Office Building | Harrisburg, PA 17120

1.2.1.7 Innovative Business Concepts, Inc.—BSBO Verification Letter

pennsylvania
DEPARTMENT OF GENERAL SERVICES

September 7, 2012

Jennifer P Briggs
Innovative Business Concepts
349 Oak Drive
Cumberland, PA 17070

CERTIFICATIO NO: 129749-2012-07-S
EXPIRATION DATE: July 27, 2013

The Bureau of Small Business Opportunities has reviewed your Recertification Application together with supporting documents. I am pleased to inform you that your company has been approved based on your certification application and your small business self-certification registration through the Small Business Procurement Initiative (SBPI). The Commonwealth now recognizes your company as a Small Business and a Small Diverse Business.

Through the application process, you have presented documentation that your company is engaged in providing certain products and/or services. Information regarding these products and/or services for which you have been certified has been electronically listed in the DGS database for use by all Commonwealth agencies. Please understand that your certification is a tool that you can use to market your goods or services to Commonwealth agencies.

Your certification is valid until the expiration date noted above. For additional information or assistance, please contact Bureau staff at (717) 783-3119 or by email at gs-bsbo@pa.gov. Best wishes in your business endeavors.

Sincerely,

[redacted]

Curtis Burwell
Equal Opportunity Manager

Bureau of Small Business Opportunities
401 North Street | Room 611 | North Office Building | Harrisburg, PA 17120

1.2.1.8 Latus Commercial Reality—BSBO Verification Letter

pennsylvania
DEPARTMENT OF GENERAL SERVICES

November, 20 2012

Laura J Martin
Latus Capital Advisors Inc
1100 Bent Creek Boulevard
Mechanicsburg, PA 17050

CERTIFICATIO NO: **368740-2012-10-S**
EXPIRATION DATE: **October 02, 2013**

Dear Laura J Martin:

The Bureau of Small Business Opportunities has reviewed your Certification Application together with supporting documents. I am pleased to inform you that your company has been approved based on your certification application and your small business self-certification registration through the Small Business Procurement Initiative (SBPI). The Commonwealth now recognizes your company as a Small Business and a Small Diverse Business.

Through the application process, you have presented documentation that your company is engaged in providing certain products and/or services. Information regarding these products and/or services for which you have been certified has been electronically listed in the DGS database for use by all Commonwealth agencies. Please understand that your certification is a tool that you can use to market your goods or services to Commonwealth agencies.

Your certification is valid until the expiration date noted above. For additional information or assistance, please contact Bureau staff at (717) 783-3119 or by email at gs-bsbo@pa.gov. Best wishes in your business endeavors.

Sincerely,

[redacted]

Curtis Burwell
Equal Opportunity Manager

Bureau of Small Business Opportunities
401 North Street | Room 611 | North Office Building | Harrisburg, PA 17120

1.2.1.9 The Metropolitan Technology Services Group LLC—BSBO Verification Letter

pennsylvania
DEPARTMENT OF GENERAL SERVICES

June 4, 2013

Jennifer Connolly
President
The Metropolitan Technology Services Group LLC
22 Wagner Farm Lane
Millstone, NJ 08535

Certification Number: **370936-2013-05-S**
Expiration Date: **May 10, 2014**
Business Types: **Information Technology**

Dear Jennifer Connolly:

The Bureau of Small Business Opportunities has reviewed your request for verification along with your supporting documents. I am pleased to inform you that your company has been verified as a Woman Business Enterprise (WBE) based on your certification with the Women's Business Enterprise National Council (WBENC) and your small business self-certification registration through the Small Business Procurement Initiative (SBPI). The Commonwealth now recognizes your company as a Small Diverse Business (WBE).

Please understand that the information that you provided for verification was represented as being true and correct. Please know that the Commonwealth shall treat any misstatement as fraudulent concealment of the true facts punishable as a crime under Section 4904 of the Pennsylvania Crime Code, Title 18, of Pa. Consolidation Statutes relating to unsworn falsification to authorities

Your verification is valid until the expiration date noted above. For additional information or assistance, please contact Bureau staff at (717) 783-3119 or by email at ra-bsboverification@pa.gov. Best wishes in your business endeavors.

Sincerely,

[redacted]

DeShawn A. Lewis, Director
Bureau of Small Business Opportunities (BSBO)

Bureau of Small Business Opportunities
401 North Street | Room 611 | North Office Building | Harrisburg, PA 17120

1.2.1.10 PC Network, Inc.—BSBO Verification Letter

pennsylvania
DEPARTMENT OF GENERAL SERVICES

October, 31 2012

Katrin Hillner Antram
PC Network Inc
1315 Walnut Street
Suite 1402
Philadelphia, PA 19107

CERTIFICATIO NO: **116258-2012-10-S**
EXPIRATION DATE: **October 24, 2013**

The Bureau of Small Business Opportunities has reviewed your Recertification Application together with supporting documents. I am pleased to inform you that your company has been approved based on your certification application and your small business self-certification registration through the Small Business Procurement Initiative (SBPI). The Commonwealth now recognizes your company as a Small Business and a Small Diverse Business.

Through the application process, you have presented documentation that your company is engaged in providing certain products and/or services. Information regarding these products and/or services for which you have been certified has been electronically listed in the DGS database for use by all Commonwealth agencies. Please understand that your certification is a tool that you can use to market your goods or services to Commonwealth agencies.

Your certification is valid until the expiration date noted above. For additional information or assistance, please contact Bureau staff at (717) 783-3119 or by email at gs-bsbo@pa.gov. Best wishes in your business endeavors.

Sincerely,

[redacted]

Curtis Burwell
Equal Opportunity Manager

Bureau of Small Business Opportunities
401 North Street | Room 611 | North Office Building | Harrisburg, PA 17120

1.2.1.11 Pierson Computing Connection, Inc.—BSBO Verification Letter

pennsylvania
DEPARTMENT OF GENERAL SERVICES

September 25, 2012

Debra A Pierson
Pierson Computing Connection Inc
6 North Frederick Street
Mechanicsburg, PA 17055

CERTIFICATIO NO: **154433-2012-07-S**
EXPIRATION DATE: **July 23, 2013**

The Bureau of Small Business Opportunities has reviewed your Recertification Application together with supporting documents. I am pleased to inform you that your company has been approved based on your certification application and your small business self-certification registration through the Small Business Procurement Initiative (SBPI). The Commonwealth now recognizes your company as a Small Business and a Small Diverse Business.

Through the application process, you have presented documentation that your company is engaged in providing certain products and/or services. Information regarding these products and/or services for which you have been certified has been electronically listed in the DGS database for use by all Commonwealth agencies. Please understand that your certification is a tool that you can use to market your goods or services to Commonwealth agencies.

Your certification is valid until the expiration date noted above. For additional information or assistance, please contact Bureau staff at (717) 783-3119 or by email at gs-bsbo@pa.gov. Best wishes in your business endeavors.

Sincerely,

[redacted]

Curtis Burwell
Equal Opportunity Manager

Bureau of Small Business Opportunities
401 North Street | Room 611 | North Office Building | Harrisburg, PA 17120

1.3 B – Small Diverse Business Participation

RFP	Requirement
II-9 B	*In addition to the above verification letter, the Offeror must include in the Small Diverse Business participation submittal of the proposal the following information:* 1. *Offerors must include a numerical percentage which represents the total percentage of the work (as a percentage of the total amount paid to the Offeror under the contract) that the Offeror commits to paying to Small Diverse Businesses (SDBs) as subcontractors. To support its total percentage SDB subcontractor commitment, Offeror must also include:* a) *The percentage of each subcontract commitment to a Small Diverse Business.* b) *The name of each Small Diverse Business. The Offeror will not receive credit for stating that after the contract is awarded it will find a Small Diverse Business.* c) *The services or supplies each Small Diverse Business will provide, including the timeframe for providing the services or supplies.* d) *The location where each Small Diverse Business will perform services.* e) *The timeframe for each Small Diverse Business to provide or deliver the goods or services.* f) *A completed and signed letter of intent, in the format set forth in Appendix J - SDB Letter of Intent, for each Small Diverse Business.* g) *The name, address and telephone number of the primary contact person for each Small Diverse Business.* 2. *The total percentages and each SDB subcontractor commitment will become contractual obligations once the contract is fully executed.* 3. *The name and telephone number of the Offeror's project (contact) person for the Small Diverse Business information.*

Our partners were selected based on their experience in providing quality goods and services to Unisys and the Commonwealth. Each firm selected participated in a bidding process with the Unisys Procurement organization to ensure requirements were clearly communicated and the best value for the Commonwealth was obtained through a competitive RFP with our suppliers. The firms listed below were allocated a specific percentage of the Total Contract Value based upon Unisys' evaluation of their capabilities to supply quality IT resources, hardware products, and office facility leasing/administration.

1.3.1 Numerical Percentage of Work Performed by the Small Diverse Businesses

RFP	Requirement
II-9 B 1	*In addition to the above verification letter, the Offeror must include in the Small Diverse Business participation submittal of the proposal the following information:* *1. Offerors must include a numerical percentage which represents the total percentage of the work (as a percentage of the total amount paid to the Offeror under the contract) that the Offeror commits to paying to Small Diverse Businesses (SDBs) as subcontractors.*

Unisys commits to paying the selected Small Diverse Businesses (SDBs), as subcontractors and/or suppliers, a numerical total percentage of 10.60% based on the percentage of the Total

Contract Value that represents the total percentage of the total cost submitted in the Cost Volume.

1.3.1.1 (a) Percentage of Dollar Amount – Each Subcontract Commitment to Small Diverse Business

RFP	*Requirement*
II-9 B 1a	*To support its total percentage SDB subcontractor commitment, Offeror must also include:* *a) The percentage of each subcontract commitment to a Small Diverse Business.*

Small Diverse Business	Percentage Each SDB Subcontractor
Acclaim Systems, Inc.	0.24%
American Personnel Managers & Consultants, Inc.	0.43%
Credo Technology Solutions, Inc.	0.67%
Domino Technologies, Inc.	0.69%
E & E IT Consulting Services, Inc.	0.73%
Info-Matrix Corporation	0.78%
Innovative Business Concepts, Inc.	0.81%
Latus Capital Advisors Inc.	0.59%
Metropolitan Technology Services Group LLC	0.70%
PC Network, Inc.	0.54%
Pierson Computing Connection, Inc.	4.42%

1.3.1.2 (b) Identified Small Diverse Business Entity

RFP	*Requirement*
II-9 B 1b	*To support its total percentage SDB subcontractor commitment, Offeror must also include:* *b) The name of each Small Diverse Business. The Offeror will not receive credit for stating that after the contract is awarded it will find a Small Diverse Business.*

1. Acclaim Systems, Inc.
2. American Personnel Managers & Consultant, Inc. (APMC)
3. Credo Technology Solutions, Inc.
4. Domino Technologies, Inc.
5. E & E IT Consulting Services, Inc.

6. Info-Matrix Corporation
7. Innovative Business Concepts, Inc.
8. Latus Capital Advisors Inc.
9. Metropolitan Technology Services Group LLC
10. PC Network, Inc.
11. Pierson Computing Connection, Inc.

1.3.1.3 (c) Services or Supplies and Timeframe Provided By Each Small Diverse Business

RFP	*Requirement*
II-9 B 1c	*To support its total percentage SDB subcontractor commitment, Offeror must also include:* *c) The services or supplies each Small Diverse Business will provide, including the timeframe for providing the services or supplies.*

Small Diverse Business	Service or Supply	Timeframe
Acclaim Systems, Inc.	Technical services labor	Full contract term
American Personnel Managers & Consultants, Inc.	Technical services labor	Full contract term
Credo Technology Solutions, Inc.	Technical services labor	Full contract term
Domino Technologies, Inc.	Technical services labor	Full contract term
E & E IT Consulting Services, Inc.	Technical services labor	Full contract term
Info-Matrix Corporation	Technical services labor	Full contract term
Innovative Business Concepts, Inc.	Technical services labor Computer hardware and maintenance services	Full contract term
Latus Capital Advisors Inc.	Real estate and facility management services	Full contract term
Metropolitan Technology Services Group LLC	Computer hardware and maintenance services	Full contract term
PC Network, Inc.	Technical services labor	Full contract term
Pierson Computing Connection, Inc.	Computer hardware and maintenance services	Full contract term

1.3.1.4 (d) Location Where Each Small Diverse Business Will Provide Services or Supplies

RFP	*Requirement*
II-9 B 1d	*To support its total percentage SDB subcontractor commitment, Offeror must also include:* *d) The location where each Small Diverse Business will perform services.*

Small Diverse Business	Services Location - Address
Acclaim Systems, Inc.	Harrisburg, PA
American Personnel Managers & Consultants, Inc.	Ashburn, VA, Eagan, MN, Harrisburg, PA
Credo Technology Solutions, Inc.	Harrisburg, PA
Domino Technologies, Inc.	Harrisburg, PA
E & E IT Consulting Services, Inc.	Harrisburg, PA
Info-Matrix Corporation	Harrisburg, PA
Innovative Business Concepts, Inc.	Harrisburg, PA
Latus Capital Advisors Inc.	Harrisburg, PA
Metropolitan Technology Services Group LLC	Harrisburg, PA
PC Network, Inc.	Harrisburg, PA
Pierson Computing Connection, Inc.	Harrisburg, PA

1.3.1.5 (e) Timeframe for Each Small Diverse Business to Provide or Deliver Goods or Services

RFP	*Requirement*
II-9 B 1e	*To support its total percentage SDB subcontractor commitment, Offeror must also include:* *e) The timeframe for each Small Diverse Business to provide or deliver the goods or services..*

Small Diverse Business	Timeframe to Provide or Deliver
Acclaim Systems, Inc.	Full contract term
American Personnel Managers & Consultants, Inc.	Full contract term
Credo Technology Solutions, Inc.	Full contract term
Domino Technologies, Inc.	Full contract term
E & E IT Consulting Services, Inc.	Full contract term
Info-Matrix Corporation	Full contract term
Innovative Business Concepts, Inc.	Full contract term
Latus Capital Advisors Inc.	Full contract term
Metropolitan Technology Services Group LLC	Full contract term
PC Network, Inc.	Full contract term
Pierson Computing Connection, Inc.	Full contract term

1.3.1.6 (f) Letters of Intent

RFP	*Requirement*
II-9 B 1f	*To support its total percentage SDB subcontractor commitment, Offeror must also include:* *f) A completed and signed letter of intent, in the format set forth in Appendix J - SDB Letter of Intent, for each Small Diverse Business.*

Unisys has included Letters of Intent for each Small Diverse Business that identifies the specific work, goods or services to be performed and how this effort relates to the project.

Small Diverse Business Letters of Intent are included in the following pages for these partner firms:

a. Acclaim Systems, Inc.
b. American Personnel Managers & Consultants, Inc. (APMC)
c. Credo Technology Solutions, Inc.
d. Domino Technologies, Inc.
e. E & E IT Consulting Services, Inc.
f. Info-Matrix Corporation
g. Innovative Business Concepts, Inc.
h. Latus Capital Advisors, Inc.
i. Metropolitan Technology Services Group LLC
j. PC Network, Inc.
k. Pierson Computing Connection, Inc.

UNISYS

June 17, 2013

Rakesh Khetawat
Director
Acclaim Systems Inc.
110 E Pennsylvania Blvd.
Feasterville, PA 19053

Dear Mr. Khetawat:

This letter serves as confirmation of the intent of Unisys Corporation to utilize Acclaim Systems Inc. on RFP 6100022698 (Data Center Computing Services) issued by the Commonwealth of Pennsylvania Office of Administration/Office for Technology.

If Unisys Corporation is the successful vendor, Acclaim Systems shall provide Technical services labor for the duration of the contract term and renewal periods.

These services represent 0.24% of the total amount Unisys Corporation will be paid under the initial term of the contract. The dollar value that the fixed percentage commitment represents will depend on the final negotiated contract pricing and actual contract usage or volume.

Acclaim Systems represents that it meets the small diverse business requirements set forth in the RFP and all required documentation has been provided to Unisys Corporation for its SDB submission.

We look forward to the opportunity to serve the Office of Administration/Office for Technology on this project. If you have any questions concerning our small diverse business commitment, please feel free to contact me at the number below.

Sincerely,

[redacted]

Beth Derr
Procurement Manager
Unisys Corporation
215-986-6552

Acknowledged,

[redacted]

Rakesh Khetawat
Director
Acclaim Systems Inc.
215-354-1422

June 17, 2013

Patricia M. Gingrich
President/CEO
American Personnel Managers & Consultants, Inc. (APMC)
2226 Gettysburg Road
Camp Hill, PA 17011

Dear Ms. Gingrich:

This letter serves as confirmation of the intent of Unisys Corporation to utilize American Personnel Managers & Consultants, Inc. (APMC) on RFP 6100022698 (Data Center Computing Services) issued by the Commonwealth of Pennsylvania Office of Administration/Office for Technology.

If Unisys Corporation is the successful vendor, APMC shall provide Technical Services Labor for the duration of the contract term and the renewal periods.

These services represent 0.43% of the total amount Unisys Corporation will be paid under the initial term of the contract. The dollar value that the fixed percentage commitment represents will depend on the final negotiated contract pricing and actual contract usage or volume.

APMC represents that it meets the small diverse business requirements set forth in the RFP and all required documentation has been provided to Unisys Corporation for its SDB submission.

We look forward to the opportunity to serve the Office of Administration/Office for Technology on this project. If you have any questions concerning our small diverse business commitment, please feel free to contact me at the number below.

Sincerely,

[redacted]

Beth Derr
Procurement Manager
Unisys Corporation
215-986-6552

Acknowledged,

[redacted]

Patricia M. Gingrich
President/CEO
American Personnel Managers and Consultants, Inc.
717-303-0229

UNISYS

June 17, 2013

Jogendra Daita
President & CEO
Credo Technology Solutions, Inc.
110 Sunset Ave.
Harrisburg, PA 17112

Dear Mr. Daita:

This letter serves as confirmation of the intent of Unisys Corporation to utilize Credo Technology Solutions, Inc. on RFP 6100022698 (Data Center Computing Services) issued by the Commonwea of Pennsylvania Office of Administration/Office for Technology.

If Unisys Corporation is the successful vendor, Credo Technology Solutions shall provide Technical Services Labor for the duration of the contract term and the renewal periods.

These services represent 0.67% of the total amount Unisys Corporation will be paid under the initial term of the contract. The dollar value that the fixed percentage commitment represents will depend on the final negotiated contract pricing and actual contract usage or volume.

Credo Technology Solutions represents that it meets the small diverse business requirements set forth in the RFP and all required documentation has been provided to Unisys Corporation for its SDB submission.

We look forward to the opportunity to serve the Office of Administration/Office for Technology on this project. If you have any questions concerning our small diverse business commitment, please feel free to contact me at the number below.

Sincerely,

[redacted]

Beth Derr
Procurement Manager
Unisys Corporation
215-986-6552

Acknowledged,

[redacted]

Jogendra Daita
President & CEO
Credo Technology Solutions, Inc.
717-540-9730

UNISYS

June 17, 2013

Nathan Balagopal
President
Domino Technologies, Inc.
Governor's Plaza South
2001 N. Front Street, Suite 334
Harrisburg, PA 17102

Dear Mr. Balagopal:

This letter serves as confirmation of the intent of Unisys Corporation to utilize Domino Technologies, Inc. on RFP 6100022698 (Data Center Computing Services) issued by the Commonwealth of Pennsylvania Office of Administration/Office for Technology.

If Unisys Corporation is the successful vendor, Domino Technologies shall provide Technical Services Labor for the duration of the contract term and the renewal periods.

These services represent 0.69% of the total amount Unisys Corporation will be paid under the initial term of the contract. The dollar value that the fixed percentage commitment represents will depend on the final negotiated contract pricing and actual contract usage or volume.

Domino Technologies represents that it meets the small diverse business requirements set forth in the RFP and all required documentation has been provided to Unisys Corporation for its SDB submission.

We look forward to the opportunity to serve the Office of Administration/Office for Technology on this project. If you have any questions concerning our small diverse business commitment, please feel free to contact me at the number below.

Sincerely,

[redacted]

Beth Derr
Procurement Manager
Unisys Corporation
215-986-6552

Acknowledged,

[redacted]

Nathan Balagopal
President
Domino Technologies, Inc.
717-579-1601

UNISYS

June 17, 2013

Linda K. Etter
President
E & E IT Consulting Services, Inc.
5026 Arthur Avenue
Mechanicsburg, PA 17050

Dear Ms. Etter:

This letter serves as confirmation of the intent of Unisys Corporation to utilize E & E IT Consulting Services, Inc. on RFP 6100022698 (Data Center Computing Services) issued by the Commonwealth of Pennsylvania Office of Administration/Office for Technology.

If Unisys Corporation is the successful vendor, E & E IT Consulting Services shall provide Technical services labor for the duration of the contract term and renewal periods.

These services represent 0.73% of the total amount Unisys Corporation will be paid under the initial term of the contract. The dollar value that the fixed percentage commitment represents will depend on the final negotiated contract pricing and actual contract usage or volume.

E & E IT Consulting Services represents that it meets the small diverse business requirements set forth in the RFP and all required documentation has been provided to Unisys Corporation for its SDB submission.

We look forward to the opportunity to serve the Office of Administration/Office for Technology on this project. If you have any questions concerning our small diverse business commitment, please feel free to contact me at the number below.

Sincerely,

[redacted]

Beth Derr
Procurement Manager
Unisys Corporation
215-986-6552

Acknowledged,

[redacted]

Linda K. Etter
President
E & E IT Consulting Services, Inc.
717-975-1664

UNISYS

June 17, 2013

Brenda S. Orth
President/CEO
Info-Matrix Corp.
650 North 12th Street
Lemoyne, PA 17043

Dear Ms. Orth:

This letter serves as confirmation of the intent of Unisys Corporation to utilize Info-Matrix Corp. on RFP 6100022698 (Data Center Computing Services) issued by the Commonwealth of Pennsylvania Office of Administration/Office for Technology.

If Unisys Corporation is the successful vendor, Info-Matrix shall provide Technical services labor for the duration of the contract term and renewal periods.

These services represent 0.78% of the total amount Unisys Corporation will be paid under the initial term of the contract. The dollar value that the fixed percentage commitment represents will depend on the final negotiated contract pricing and actual contract usage or volume.

Info-Matrix represents that it meets the small diverse business requirements set forth in the RFP and all required documentation has been provided to Unisys Corporation for its SDB submission.

We look forward to the opportunity to serve the Office of Administration/Office for Technology on this project. If you have any questions concerning our small diverse business commitment, please feel free to contact me at the number below.

Sincerely,

[redacted]

Beth Derr
Procurement Manager
Unisys Corporation
215-986-6552

Acknowledged,

[redacted]

Brenda S. Orth
President/CEO
Info-Matrix Corp.
717-260-9850

UNISYS

June 17, 2013

Jennifer Briggs
President
Innovative Business Concepts, Inc.
209 Hamilton Street
Harrisburg, PA 17102

Dear Ms. Briggs:

This letter serves as confirmation of the intent of Unisys Corporation to utilize Innovative Business Concepts, Inc. on RFP 6100022698 (Data Center Computing Services) issued by the Commonwealth of Pennsylvania Office of Administration/Office for Technology.

If Unisys Corporation is the successful vendor, Innovative Business Concepts shall provide Technical services labor for the duration of the contract term and renewal periods.

These services represent 0.81% of the total amount Unisys Corporation will be paid under the initial term of the contract. The dollar value that the fixed percentage commitment represents will depend on the final negotiated contract pricing and actual contract usage or volume.

Innovative Business Concepts represents that it meets the small diverse business requirements set forth in the RFP and all required documentation has been provided to Unisys Corporation for its SDE submission.

We look forward to the opportunity to serve the Office of Administration/Office for Technology on this project. If you have any questions concerning our small diverse business commitment, please feel free to contact me at the number below.

Sincerely,

[redacted]

Beth Derr
Procurement Manager
Unisys Corporation
215-986-6552

Acknowledged,

[redacted]

Jennifer Briggs
President
Innovative Business Concepts, Inc.
717-221-1125

UNISYS

June 17, 2013

Laura Martin
CPM/Broker/Owner
Latus Capital Advisors Inc.
1100 Bent Creek Blvd., 2nd Floor
Mechanicsburg, PA 17050

Dear Ms. Martin:

This letter serves as confirmation of the intent of Unisys Corporation to utilize Latus Capital Advisors Inc. on RFP 6100022698 (Data Center Computing Services) issued by the Commonwealth of Pennsylvania Office of Administration/Office for Technology.

If Unisys Corporation is the successful vendor, Latus Capital Advisors Inc. shall provide Real estate and facility management services for the duration of the contract term and the renewal periods.

These services represent 0.59% of the total amount Unisys Corporation will be paid under the initial term of the contract. The dollar value that the fixed percentage commitment represents will depend on the final negotiated contract pricing and actual contract usage or volume.

Latus Capital Advisors Inc. represents that it meets the small diverse business requirements set forth in the RFP and all required documentation has been provided to Unisys Corporation for its SDB submission.

We look forward to the opportunity to serve the Office of Administration/Office for Technology on this project. If you have any questions concerning our small diverse business commitment, please feel free to contact me at the number below.

Sincerely,

[redacted]

Beth Derr
Procurement Manager
Unisys Corporation
215-986-6552

Acknowledged,

[redacted]

Laura Martin
CPM/Broker/Owner
Latus Capital Advisors Inc.
717-795-6102 - x101

UNISYS

June 17, 2013

Jim Cafferky
Account Executive
Metropolitan Technology Services Group LLC
4400 Route 9 South, Suite 1000
Freehold, NJ 07728

Dear Mr. Cafferky:

This letter serves as confirmation of the intent of Unisys Corporation to utilize Metropolitan Technology Services Group LLC on RFP 6100022698 (Data Center Computing Services) issued by the Commonwealth of Pennsylvania Office of Administration/Office for Technology.

If Unisys Corporation is the successful vendor, Metropolitan Technology Services Group LLC shall provide Computer Hardware and maintenance services for the duration of the contract term and the renewal periods.

These services represent 0.70% of the total amount Unisys Corporation will be paid under the initial term of the contract. The dollar value that the fixed percentage commitment represents will depend on the final negotiated contract pricing and actual contract usage or volume.

Metropolitan Technology Services Group LLC represents that it meets the small diverse business requirements set forth in the RFP and all required documentation has been provided to Unisys Corporation for its SDB submission.

We look forward to the opportunity to serve the Office of Administration/Office for Technology on this project. If you have any questions concerning our small diverse business commitment, please feel free to contact me at the number below.

Sincerely,

[redacted]

Beth Derr
Procurement Manager
Unisys Corporation
215-986-6552

Acknowledged,

[redacted]

Jim Cafferky
Account Executive
Metropolitan Technology Services Group
732-786-1705

UNISYS

June 17, 2013

Katrin Hillner
President & CEO
PC Network Inc.
1315 Walnut Street, Suite 1402
Philadelphia, PA 19107

Dear Ms. Hillner:

This letter serves as confirmation of the intent of Unisys Corporation to utilize PC Network Inc. on RFP 6100022698 (Data Center Computing Services) issued by the Commonwealth of Pennsylvania Office of Administration/Office for Technology.

If Unisys Corporation is the successful vendor, PC Network shall provide Technical services labor for the duration of the contract term and renewal periods.

These services represent 0.54% of the total amount Unisys Corporation will be paid under the initial term of the contract. The dollar value that the fixed percentage commitment represents will depend on the final negotiated contract pricing and actual contract usage or volume.

PC Network represents that it meets the small diverse business requirements set forth in the RFP and all required documentation has been provided to Unisys Corporation for its SDB submission.

We look forward to the opportunity to serve the Office of Administration/Office for Technology on this project. If you have any questions concerning our small diverse business commitment, please feel free to contact me at the number below.

Sincerely,

[redacted]

Beth Derr
Procurement Manager
Unisys Corporation
215-986-6552

Acknowledged,

[redacted]

Katrin Hillner
President & CEO
PC Network Inc.
267-236-0152

UNISYS

June 13, 2013

Rick Loffredo
Director of Business Operations
Pierson Computing Connection, Inc.
10 Long Lane, Suite 103
Mechanicsburg, PA 17050

Dear Ms. Pierson:

This letter serves as confirmation of the intent of Unisys Corporation to utilize Pierson Computing Connection, Inc. on RFP 6100022698 (Data Center Computing Services) issued by the Commonwealth of Pennsylvania Office of Administration/Office for Technology.

If Unisys Corporation is the successful vendor, Pierson Computing Connection shall provide Computer Hardware and maintenance services for the duration of the contract term and the renewal periods.

These services represent 4.42% of the total amount Unisys Corporation will be paid under the initial term of the contract. The dollar value that the fixed percentage commitment represents will depend on the final negotiated contract pricing and actual contract usage or volume.

Pierson Computing Connection represents that it meets the small diverse business requirements set forth in the RFP and all required documentation has been provided to Unisys Corporation for its SDB submission.

We look forward to the opportunity to serve the Office of Administration/Office for Technology on this project. If you have any questions concerning our small diverse business commitment, please feel free to contact me at the number below.

Sincerely,

[redacted]

Beth Derr
Procurement Manager
Unisys Corporation
215-986-6552

Acknowledged,

[redacted]

Rick Loffredo
Director of Business Operations
Pierson Computing Connection, Inc.
717-796-0493

1.3.1.7 (g) Small Diverse Businesses – Primary Person Contact Information

RFP	*Requirement*
II-9 B 1g	*To support its total percentage SDB subcontractor commitment, Offeror must also include:* *g) The name, address and telephone number of the primary contact person for each Small Diverse Business.*

Small Diverse Business	Primary SDB Contacts - Contact Information
Acclaim Systems, Inc.	**Rakesh Khetawat,** 110 E. Pennsylvania Blvd, Feasterville, PA 19053 **Phone:** 215-354-1422, **Fx:** 215-354-0488, **Email:** rakeshk@acclaimsystems.com
American Personnel Managers & Consultants, Inc.	**Patricia M. Gingrich,** 2226, Gettysburg Road, Camp Hill, PA 17011 **Phone:** 717-303-0229, **Fx**: 717-737-4934, **Email:** amerijob13@aol.com
Credo Technology Solutions, Inc.	**Jogendra Daita**, , 110 Sunset Ave,Harrisburg,PA17112 **Phone:** 717.540.9730, **Email:** jdaita@credotsinc.com
Domino Technologies, Inc.	**Nathan Balagopal**, Governor's Plaza South, 2001 N. Front Street, Suite 334, Harrisburg, PA 17102 **Phone:** 717-579-1601, **Email:** nathanb@dominotech.net
E & E IT Consulting Services, Inc.	**Tracy K. Etter,** 5026 Arthur Avenue, Mechanicsburg, PA 17050 **Phone:** 717-975-1664, **Fx:** 717-975-1665, **Email:** letter@ene-it-consulting.com
Info-Matrix Corporation	**Brenda S. Orth,** 650 North 12th Street, Lemoyne, PA 17043 **Phone:** 717-260-9850, **Fx:** 717-260-9863, **Email:** britterorth@info-matrix.com
Innovative Business Concepts, Inc.	**Jennifer Briggs,** 209 Hamilton Street, Harrisburg, PA 17102 **Phone:** 717-221-1125, **Fx:** 717-774-3380, **Email:** jbriggs@innovative-bc.com
Latus Capital Advisors Inc.	**Laura Martin,** 1100 Bent Creek Blvd., 2nd Floor, Mechanicsburg, PA 17050 **Phone: (O)** 717-795-6102 - x101, **(M)** 717-919-7888, **Email:** lmartin@latusrealty.com
Metropolitan Technology Services Group LLC	**Jennifer Connolly,** 22 Wagner Farm Lane, Millstone, NJ 08535 **Phone: (O)** 732-786-1705, **(M)** 732-616-4950, **Email:** jconnolly@metrotsg.com
PC Network, Inc.	**Katrin Hillner,** 1315 Walnut Street, Suite 1402, Philadelphia, PA 19107 **Phone: (O)** 267-236-0152, **Email:** :katrin.hillner@pcn-inc.com
Pierson Computing Connection, Inc.	**Debra A. Pierson,** 10 Long Lane, Suite 100, Mechanicsburg, PA 17050 PO Box 206, New Kingstown, PA 17072 **Phone:** 717-796-0493, **Email:** dpierson@piersoncci.com

1.3.1.8 Total Percentages and SDB Subcontractor Commitment Contractual Obligation

RFP	*Requirement*
II-9 B 2	*The total percentages and each SDB subcontractor commitment will become contractual obligations once the contract is fully executed.*

Unisys understands and agrees that the total percentage and each SDB subcontractor commitment as indicated in this submittal will become contractual obligations once the contract is fully executed.

1.3.1.9 Offeror's Project Person for Small Diverse Business information - Contact Information

RFP	*Requirement*
II-9 B 3	*The name and telephone number of the Offeror's project (contact) person for the Small Diverse Business information.*

Offeror's Project Person for SDB Information	Contact Information
Brian Maydick	**Brian Maydick,** 4750 Lindle Road, Harrisburg, PA 17111 **Phone: (O)** 717-526-1214, **(M)** 717-982-3098, **Email:** brian.maydick@unisys.com

APPENDIX B - PROPOSAL COVER SHEET
COMMONWEALTH OF PENNSYLVANIA
OFFICE OF ADMINISTRATION – OFFICE FOR INFORMATION TECHNOLOGY
RFP# 6100022698

Enclosed in three separately sealed submittals is the proposal of the Offeror identified below for the above-referenced RFP:

Offeror Information:	
Offeror Name	Unisys Corporation
Offeror Mailing Address	4750 Lindle Road Harrisburg, Pennsylvania 17111
Offeror Website	www.unisys.com
Offeror Contact Person	Dean Shaner
Contact Person's Phone Number	(717) 526-1267
Contact Person's Facsimile Number	(717) 526-1175
Contact Person's E-Mail Address	[redacted]@unisys.com
Offeror Federal ID Number	[redacted]
Offeror SAP/SRM Vendor Number	163299

	Submittals Enclosed and Separately Sealed:
X	Technical Submittal
	Disadvantaged Business Submittal
	Cost Submittal

Signature	
Signature of an official authorized to bind the Offeror to the provisions contained in the Offeror's proposal:	[redacted]
Printed Name	Ron Frankenfield
Title	Senior Vice President/President Global Managed Services

FAILURE TO COMPLETE, SIGN AND RETURN THIS FORM WITH THE OFFEROR'S PROPOSAL MAY RESULT IN THE REJECTION OF THE OFFEROR'S PROPOSAL

Unisys Response to

Commonwealth of Pennsylvania

Office of Administration

Office for Information Technology

[redacted]

Request for Proposal (RFP)
RFP 6100022698

Technical Submittal

June 19, 2013

This proposal has been reproduced on recycled paper

J. Edward Coleman
Chairman & Chief Executive Officer

Unisys Corporation
801 Lakeview Drive
Blue Bell, PA 19422

Telephone
(215) 986-6100 (Office)

UNISYS

June 18, 2013

Bureau of IT Procurement
c/o Commonwealth Mail Processing Center
2 Technology Park (rear)
Attn: IT Procurement 506 Finance
Harrisburg, PA 17110
Attn: Janis Brown

RE: **Request for Proposal (RFP Number 6100022698) for the Commonwealth of Pennsylvania Data Center Computing Services**

Dear Ms. Brown:

Unisys Corporation is pleased to submit this proposal in response to Request for Proposals (RFP Number 6100022698) for the Commonwealth of Pennsylvania Data Center Computing Services. We reviewed the detailed requirements of the RFP and developed our proposal to meet them. We are confident that our proposal presents a sound approach, a proven team, technology, services, Commonwealth-specific knowledge experts, and a mature methodology for meeting the Commonwealth's main objective to implement a cost-effective, flexible, new data center service model based on usage.

Unisys offers world-class infrastructure standards and practices. Our company holds the coveted ISO 20000 certification for Service Provider Organizations. The Unisys ITSM practice was assessed by Underwriters Laboratories, Inc., which found Unisys to be in compliance with the ISO/IEC 20000-1:2005 standard, resulting in a 3-year certification. Unisys was the eighth company to be certified in the United States: the unique distinction of being the first service provider organization to receive the certification for its global operations.

Through this proposal and subsequent delivery of services, Unisys will align all participating agencies with ITIL and introduce operational efficiencies to improve the mean-time-to-resolve times and reduce service incidents overall. We employ state-of-the-art monitoring and knowledge-based escalation procedures to dramatically improve uptime and overall system performance. This gives our approach significantly improved reliability, consistency, responsiveness, and reduced mean time to repair while simultaneously reducing the total cost of ownership by reducing labor costs for routine or predefined tasks.

For this opportunity, we supplemented our extensive managed services experience at both the Data PowerHouse (DPH) and the Enterprise Server Farm (ESF) with key and proven partners like IBM and Deloitte Consulting because they bring to this engagement an extensive knowledge of the Commonwealth's current infrastructure and business systems environments. Currently performing as your primary services provider, we could think of no one better than these key partners—we are very pleased to have them on our team.

Should you have any questions about this proposal or need additional information, please contact:

Dean R. Shaner
4750 Lindle Road
Suite 301
Harrisburg, PA 17111
Telephone: (717) 526-1267
E-mail: dean.shaner@unisys.com

We appreciate this opportunity to provide IT Infrastructure support services to support your mission.

Sincerely,

[redacted]

[redacted]. Edward Coleman
Chairman and CEO

UNISYS

Statement of Understanding

The information contained herein has been prepared by Unisys Corporation ("Unisys") for evaluation and consideration by the Commonwealth of Pennsylvania ("Commonwealth") to buy the deliverables and services in this proposal in response to the Commonwealth Request for Proposal #6100022698 for Data Center Computing Services. By receipt of this proposal, the Commonwealth is not obligated to buy any products or services. Only a written contract that is signed by authorized representatives of Unisys and the Commonwealth will create any obligations for either party arising from, or related to, the services described in this proposal.

This proposal, including the fixed and Resource Unit (RU) price charges outlined in Unisys submission have been prepared in accordance with, and is submitted on the basis of Unisys understanding of the State's requirements based on the information provided in the RFP and as further described in its proposal. For greater certainty all references to "costs" refer to the proposed cost to the Commonwealth based on Unisys proposed charges and not to Unisys costs.

As allowed by the RFP, there are terms and conditions in the RFP (Appendix A and related Exhibits and Schedules) that Unisys would like to negotiate with the Commonwealth, and there are additional terms and conditions that Unisys would like to add to the contract. As per the RFP instructions, these areas of concern are included in our RFP response. Unisys requests that the Commonwealth and Unisys enter into a period of negotiation prior to the execution of a formal contract.

This proposal contains trade secrets and confidential proprietary information, as well as other information that is not subject to public disclosure under the Pennsylvania Right-to-Know-Law, 65 P.S. § 67.101, et seq., as follows:

- Data center addresses
- SSAE-16 reports
- Availability reports
- The personal contact information provided for Unisys customer references
- Organization charts and names (if included) as well as named resources in the response should be excluded to protect employee privacy and company proprietary information (delivery structure).

In consideration of the receipt of this document, Unisys requests that the Commonwealth not reproduce or make this information available in any manner to persons outside the group directly responsible for evaluation of its contents, except as

may be required by applicable public access law and/or regulation. Unisys is a registered trademark of Unisys Corporation. All other trade names, brands, and products referenced in this proposal are the service marks, trademarks, or registered trademark of the respective manufacturer of supplier.

Copyright © 2013 Unisys Corporation
All Rights Reserved
Unisys Corporation Confidential

UNISYS

Table of Contents

TRANSMITTAL LETTER

STATEMENT OF UNDERSTANDING

TABLE OF CONTENTS

1. STATEMENT OF THE PROBLEM 1-3

2. MANAGEMENT SUMMARY 2-3

2.1 THE PATH FORWARD 2-3
2.2 THE UNISYS TEAM 2-4
2.3 OUR EXECUTIVE LEADERSHIP TEAM 2-7
2.4 UNISYS SOLUTION 2-14
2.4.1 Unisys Tenets 2-14
2.5 THE PROPOSED SOLUTION 2-14

3. WORK PLAN (RFP REQUIREMENT II-3) 3-3

3.1 WORK PLAN OVERVIEW 3-4
3.1.1 Unisys Team Qualifications 3-4
3.1.2 Work Plan Description 3-6
3.2 DETAILED TASK PLAN 3-12
3.2.1 Transition Services 3-14
3.2.1.1 Account Organization 3-14
3.2.1.2 Enterprise Data Center (EDC) to Managed Services Model 3-15
3.2.1.3 Tools Implementation 3-16
3.2.2 Application Workload Migrations 3-17
3.2.2.1 Operational Readiness 3-17
3.2.2.2 Agency Application Workload Migrations 3-18
3.2.3 Transition Program Management 3-19
3.2.4 Steady State 3-19
3.3 PROJECT CONTROL AND REPORTING 3-25
3.3.1 Governance 3-25
3.3.2 Status Reports 3-26
3.4 ADDITIONAL SERVICE REQUIREMENTS 3-31
3.4.1 Emergency Preparedness 3-31
3.4.1.1 COOP Strategy 3-31
3.4.1.2 Essential Business Services addressed by COOP 3-32
3.4.1.3 Types of Events that Trigger the COOP 3-32
3.4.1.4 COOP Approach 3-33
3.4.2 Service Level Agreements 3-34
3.4.3 Service Catalog 3-35

3.4.4 Locations 3-37
3.4.5 Business and Technical Requirements 3-37
3.4.5.1 Program Management (A.1) 3-39
3.4.5.2 Data Center Architecture (A.2) 3-39
3.4.5.3 Technical Services (A.3) 3-40
3.4.5.4 Facility Management 3-40
3.4.5.5 Managed Hosting Services (A.5) 3-41
3.4.5.6 Capacity on Demand Services (A.6) 3-41
3.4.5.7 Transition Services (A.7) 3-42
3.4.6 Contract Requirements - Small Diverse Business Participation (RFP IV-6 3-43
3.4.7 Proposed Services 3-45
3.4.8 Payment for Services 3-45
ATTACHMENT 3–1 — SCHEDULE B: GOVERNANCE 3-47
ATTACHMENT 3–2 — SCHEDULE C: SERVICE CATALOG 3-49
ATTACHMENT 3–3 — SCHEDULE D: TRANSITION MILESTONES 3-51
ATTACHMENT 3–4 – SCHEDULE E: DATA CENTER LOCATIONS 3-53
ATTACHMENT 3–5 — SCHEDULE F: STATEMENT OF WORK 3-55
ATTACHMENT 3–6 — SCHEDULE H: CCPM 3-57
ATTACHMENT 3–7 — SCHEDULE M: DETAILED TRANSITION PLAN 3-59
ATTACHMENT 3–8 — SCHEDULE K: KEY PROGRAM DELIVERABLES 3-61
ATTACHMENT 3–9 — SCHEDULE J.3: SERVICE LEVEL AGREEMENTS 3-63

4. PRIOR EXPERIENCE 4-3

4.1 OVERALL 4-3
4.1.1 Team Introduction and Prior Experience 4-4
4.1.2 IBM, Key Partner 4-5
4.1.3 Deloitte, Key Partner 4-5
4.1.4 Teaming Approach 4-5
4.1.5 Small Diverse Business Partners 4-6
4.1.6 Why this Team 4-7
4.1.7 Experience and Services Relative to this RFP 4-10
4.1.8 Team Qualifications 4-11
4.1.9 Service Levels 4-16
4.1.10 Quality of Comparable Services 4-16
4.1.11 References and Length of Service 4-17
4.2 UNISYS CORPORATE INFORMATION 4-19
4.2.1 History and Background 4-19
4.2.2 Current Services 4-19
4.2.3 Client Focus 4-20
4.2.4 Services, Global Outsourcing is a Unisys Key Strategy 4-20
4.2.5 Global Footprint 4-22
4.2.6 Technology Agnostic and Committed to Strategic Partnerships 4-23
4.2.7 Corporate Organization 4-24
4.3 UNISYS STRATEGIC DIRECTION 4-27
4.3.1 Unisys Corporate Mission 4-27
4.3.2 Corporate Strategy 4-28
4.3.3 Innovation 4-31

4.3.4 Hybrid Enterprise – Building the Data Center of the Future 4-36
4.3.5 Platform Strategy 4-41
4.3.6 Service Management Strategy 4-43
4.3.7 Impact on the Commonwealth 4-45
4.3.8 Summary Unisys Strategic Direction 4-48
4.4 UNISYS DEDICATION TO QUALITY 4-51
4.4.1 Approach to Measuring & Maintaining High Quality Services 5-52
4.4.2 Industry-recognized Quality Standards and Awards 4-58
4.4.3 External Quality Certification 4-60
4.4.4 Detailed Approach and Quality Plan 4-64
4.4.5 Summary of the Unisys Dedication to Quality 4-73
4.5 CLIENT REFERENCES 4-75
4.5.1 Project References (RFP Appendix C) 4-75
4.5.2 Unisys Project References 4-79
4.5.2 IBM Project References 4-106
4.5.3 Deloitte LLP Project References 4-115
4.5.4 Acclaim Systems, Inc. Project References 4-126
4.5.5 American Personnel Managers and Consultants, Inc. Project References 4-132
4.5.6 Credo Technology Solutions, Inc. Project References 4-144
4.5.7 Domino Technologies, Inc. Project References 4-150
4.5.8 e&e IT Consulting Services, Inc. Project References 4-157
4.5.9 Info-Matrix Corporation Project References 4-163
4.5.10 Innovative Business Concepts, Inc. Project References 4-169
4.5.11 PC Network, Inc. Project References 4-176
4.5.12 Pierson Computing Connection, Inc. Project References 4-181
4.6 SUBCONTRACTORS AND SUPPLIERS 4-189
4.6.1 Unisys Subcontractors and Suppliers Capabilities Table 4-189
Schedule L – Unisys List of Subcontractors 4-190

5. PERSONNEL 5-3

5.1 CURRENT ORGANIZATIONAL STRUCTURE 5-7
5.2 NEW ORGANIZATIONAL STRUCTURE 5-8
5.3 KEY PERSONNEL OVERVIEW 5-12
5.4 DETAILS OF THE NEW ORGANIZATION 5-13
5.5 ROLES AND RESPONSIBILITY – HIGH LEVEL STEADY STATE 5-15
5.6 ROLES AND RESPONSIBILITY – HIGH LEVEL TRANSITION (INCLUDES ARCHITECT, BUILD) 5-17
5.7 AGENCY CENTRIC STAFFING APPROACH 5-19
5.8 INTERACTION WITH THE COMMONWEALTH 5-20
5.9 TRANSITION STAFFING APPROACH 5-23
5.10 KEY PERSONNEL TABLE 5-25
5.11 SUBCONTRACTOR KEY PERSONNEL TABLE 5-33
5.12 ORGANIZATIONAL FUNCTION DISCUSSION 6-36
5.13 HR DISCUSSION 6-66
5.13.1 Staff Contingency Plan 5-66
5.13.2 Staff Management 5-67
5.13.3 Training Policies and Procedures 5-69

5.13.4 Staff Retention 5-72
Key Resumes
Right to Represent Acknowledgement Forms
Respresentative Resumes

6. TRAINING 6-3

TRAINING DESCRIPTIONS 6-9

7. FINANCIAL CAPABILITY 7-3

7.1 FINANCIAL STABILITY AND ECONOMIC CAPABILITY 7-3
7.2 FINANCIAL STATEMENTS 7-13
7.3 CERTIFICATES OF INSURANCE 7-15
7.4 DUN & BRADSTREET COMPREHENSIVE REPORT 7-21

8. OBJECTIONS AND ADDITIONS TO CONTRACT TERMS AND CONDITIONS 8-3

9. REQUIRED FORMS 9-3

9.1 DOMESTIC WORKFORCE UTILIZATION CERTIFICATION (RFP APPENDIX D) 9-5
9.2 COSTARS PROGRAM ELECTION TO PARTICIPATE (RFP APPENDIX E) 9-7
9.3 TRADE SECRET FORM (RFP APPENDIX G) 9-9
9.4 LOBBYING CERTIFICATION AND DISCLOSURE OF LOBBYING ACTIVITIES (RFP APPENDIX H) 9-11

10. APPENDICES (MANDATORY REQUIREMENTS) 10-3

10.1 APPENDIX A - MANDATORY REQUIREMENTS (EVAL CRITERIA III-1) 10-3
10.1.1 ISO 27001Certification 10-4
10.1.2 ISO 9001 Certification 10-5
10.1.3 ISO/IEC 20000 Certifications 10-6
10.1.4 SSAE 16 Audit Findings Report 10-7
10.1.5 Six Sigma Certifications / Assessments / Evaluations 10-9
10.1.6 ITIL Certifications / Assessments / Evaluations 10-10

1.0 Statement of the Problem

1. STATEMENT OF THE PROBLEM 1-3

This page intentionally left blank.

1. Statement of the Problem

RFP	Requirement
II-1	Statement of the Problem. State in succinct terms your understanding of the problem presented or the service required by this RFP.

Governor Corbett and the Commonwealth's IT Leadership seek greater efficiencies from state government's IT compute function. In part, this is driven by the need to cut costs through consolidation, shift to a financial model where the Commonwealth no longer owns the IT infrastructure, and pays only for the amount of IT compute resources actually used through the use of an agile, flexible, and fully transparent pricing model. Of equal importance, the Commonwealth's Request for Proposal (RFP) outlines a completely new model to further improve service quality and delivery. This model includes enhanced IT service management leveraging ITIL V3 framework for process, adoption of best practices, a comprehensive service catalog tailored to meet individual agency needs, and many other improvements. Our proposal will demonstrate how the Unisys Team will help the Commonwealth achieve its vision to implement a new "compute" service model to modernize its computing environments, reduce costs, and strive for ever higher levels of accountability, efficiency, flexibility, security, and transparency for all agencies.

As Governor Corbett's 2013–2014 budget submission stated, "Fiscal discipline and continued self-refinement remain guiding principles for this budget as Pennsylvania looks to the future." Unisys understanding of this RFP stresses alignment with and support for the Governor's vision of "self-refinement" and "fiscal discipline" by seeking a highly qualified service provider to deliver compute services on a consumptive basis. This model will serve as a means to achieve better fiscal discipline and predictability for the Commonwealth.

As your current service provider, we understand your need for a single, accountable, reliable partner as this is the relationship we have defined with you over the last 13 years. We also recognize that today's operating model needs to change. The new operating model will be much different from today's. It will feature variable pricing, greater flexibility through a capacity on-demand approach, more transparency and allow the Commonwealth to scale according to changing business needs. The new operating model will provide the opportunity to lower costs of service while providing the means to tailor services to specific needs. As your current service provider, we welcome and embrace these changes.

The Commonwealth will enter into a single agreement with a company or consortium of companies (with a single prime contractor) for compute services that support the Commonwealth's transformation to an information-focused enterprise. These services will replace the existing Data PowerHouse (DPH) contract and consolidate at least five other compute facilities. We understand the Commonwealth requires vendor-provided facilities in addition to the use of the Commonwealth's Enterprise Data Center (EDC).

This procurement continues the evolution of the successful data center-centric model that began in 1999. In 2008, the next iteration occurred when the Commonwealth and Unisys achieved significant savings by adopting an enterprise shared infrastructure model. The Commonwealth has now defined a new innovative model.

To achieve additional efficiencies, the current model needs to change by adopting innovations such as the implementation of a flexible, agile, and transparent pricing model; a descriptive service catalog; secure capacity-on-demand capability; greater resiliency of your compute resources; disaster recovery services; and high-quality IT service management processes. Unisys applauds the Commonwealth's direction in these areas. Unisys experiences with other public sector agencies that have adopted similar innovations, such as the Defense Information System Agency (DISA), the Internal Revenue Service (IRS) and The California State University System (CSU) have yielded significant efficiencies similar to those anticipated by the Commonwealth.

Finally, training, knowledge transfer, and a well-defined organizational structure with effective communication, governance, management, and support resources are critical to deliver the required compute services and to meet service level agreements. A more definitive list of requested services is presented later in this section.

Vision — Achieving Greater Government Efficiency

During the latter half of the 1990s and into the early 2000s, the Commonwealth became one of the most technologically advanced and innovative state governments in the nation. During that time, the Commonwealth was consistently recognized as a leader in prestigious studies such as the Digital State Surveys and was repeatedly identified as a national best practice leader for IT in state governments. Much of this recognition was due to the Commonwealth's early vision in adopting several innovative enterprise IT initiatives. Few states, even after years of effort, have achieved the same level of success as Pennsylvania. Specifically, the Commonwealth achieved national leadership on the following initiatives:

- **Consolidation of Telecommunications Services –** In its time, the largest transition to competitive telecommunication services in the nation. More recently, a unified communications model including VoIP was implemented.
- **Consolidated Messaging –** The establishment of a statewide e-mail system that today remains one of the largest single public sector instances of Microsoft Exchange.
- **Cyber Security –** The Commonwealth was one of the first states to implement a comprehensive cyber security program that today is recognized as one of the best in the nation.
- **Data PowerHouse** and **Enterprise Data Center –** Recognized as national best practices: the DPH and the EDC were the first successful statewide consolidations and outsourcing (in the case of the DPH) of mission-critical systems in the nation.
- **Imagine PA –** The first statewide ERP implementation in the nation.

These widely recognized innovations fueled performance improvements and enhanced citizen and employee access to services throughout the Commonwealth. They also reduced cost by eliminating many duplicate services, which saved well over $500 million for the citizens of the Commonwealth.

The model outlined in this RFP will yield similar large-scale benefits. The Commonwealth's approach is visionary for state government, creating a totally new environment where services—and only those services you need—are purchased and where the Commonwealth sheds the heavy burden of owning and operating data centers and focuses on its core business of serving citizens.

Challenging Times — Drivers of Change for the Commonwealth

Budget Challenges. Beginning in 2002, significant budget constraints, driven largely by the poor macroeconomic environment, negatively affected the Commonwealth and other states nationwide. These budget constraints led to re-allocation of funds—traditionally targeted for IT investments—to basic Commonwealth services. This made it extremely difficult for the Commonwealth to continue maintenance and reinvestment in an efficient and robust IT infrastructure.

Impact on Commonwealth IT. Because of this economic downturn, the success of the Commonwealth's enterprise approach to IT was hampered, and agencies sought individual solutions to meet their immediate business needs. This led to the emergence of a loosely coupled network of separate IT solutions, redundant agency IT infrastructures and data centers, resulting in varying levels of performance, unused capacity, and inefficient use of resources. This model drove up costs and created a sub-optimized enterprise solution that at times, despite the excess capacity, could not efficiently support the Commonwealth's needs. Recognizing this reality, Executive Order 2004-8 was amended in 2007 to address the need for coordinated IT planning and resource utilization by directing the consolidation of some agency information technology organizations under the Office for Information Technology.

In 2008, economic conditions deteriorated even further, driven by the worst recession since the Great Depression. Tax revenue declined dramatically, and citizen filings for unemployment compensation and human services assistance skyrocketed, creating major budget and IT challenges.

In response, the Commonwealth collaborated with Unisys to adopt an enterprise shared infrastructure model, driving IT costs lower and improving the agility of agencies. For example, during peak tax processing season, Pennsylvania Department of Revenue has leveraged unused capacity shared with other agencies in the Data PowerHouse. In addition to providing greater agility to Commonwealth agencies, this shared model allowed Unisys and the Commonwealth to renegotiate the DPH agreement and generate $240 million in savings to the Commonwealth. Even though significant benefits were achieved in 2008, the Corbett administration recognized early that more could be done through further consolidation and sharing of resources, including IT.

Driving Greater Efficiencies. Shortly after his election in 2011, Governor Tom Corbett recognized the need to renew and reinvigorate the focus on greater government efficiency. Driven by challenging budget conditions, one of Governor Corbett's very first initiatives on his 2011 swearing-in was IT consolidation. Governor Corbett directed the Office of Administration and Department of General Services to work with all Commonwealth agencies to consolidate services, especially information technology. Improving efficiency in government through consolidation of services, including IT, was once again back in focus for the Commonwealth, further reinforcing the tenets of Executive Order 2004-8 as amended in 2007.

The Vision. Given the Governor's mandate for greater efficiency, the Commonwealth CIO and agency IT leadership developed a completely new and innovative model for providing IT compute services. Its focus is to eliminate inefficiencies, improve performance, and safeguard these critical services through enhanced security and service recovery in case of an emergency. The net result will be better services at a reduced cost.

Major Issues addressed by the RFP:

- *Need to consolidate IT resources to achieve economies of scale*
- *Need to eliminate duplication*
- *Need to finance future IT resources based on usage, not a fixed price*
- *Need for greater resiliency and DR for critical IT systems to maintain COG*
- *Need for a flexible service catalog to meet the unique needs of individual agencies*
- *Need to adopt industry performance standards like ITIL for service and operations*
- *Need for high-quality staff training and timely knowledge transfer*
- *Need for additional security enhancements*
- *Need for faster provisioning of services*
- *Need for a greater pricing transparency, predictability, and consistency*
- *Need to establish a new compute services contract*
- *Need for a multi-data center architecture*
- *Need for multitier service environments*
- *Need for primary support for the EDC*
- *Need to comply with Commonwealth contractual, regulatory, and policy requirements for security, architecture, and SDLC standards*
- *Need for SLAs*

And, of critical importantance…

Need for a service provider that can successfully deliver on its promises

Commonwealth IT leaders identified a number of specific needs:

As previously mentioned, the agency infrastructure and data center facilities that emerged during the economic challenges adds to the cost of maintaining numerous data center facilities and creates duplication with unused capacity. The Commonwealth operates at least five individual agency data centers, the DPH and the Enterprise Data Center. This does not include numerous other individual agencies' disaster recovery data center facilities. This decentralized model impedes the ability to achieve savings by limiting the capability to implement a "true" enterprise on-demand compute environment that optimizes the use of server, storage, and network capacity encapsulated by a common enterprise service management model and strong security framework.

The lack of a common provisioning platform is increasing the time required to provision compute resources and is another detriment of an inefficient decentralized model. A common provisioning platform used with an enterprise compute model can eliminate redundant administrative resources that repeat the same tasks multiple times in multiple centers. Automation of these functions will optimize resources, lead to significant savings, and improve response time for agencies that need to provision services quickly.

Another challenge to the Commonwealth is refreshing the technology to limit the risk of infrastructure failures and thereby realize savings from improved reliability and performance. In difficult budget times, gaining approval for large capital outlays is difficult at best.

A better approach (and one the Commonwealth is pursuing) is a consumptive model in which services—not hardware and software—are purchased as needed. This eliminates the challenge of large capital outlays at times when the Commonwealth does not have sufficient funds. This model also affords optimization of technology processing resources by significantly reducing the existence of excess IT compute capacity.

In addition to financial incentives, the Commonwealth seeks an enterprise compute services model to drive improvements to service management, a goal that will yield significant benefits in accountability and service quality. Decentralization raised barriers to establishing true interoperability and implementing enterprise service management best practices and processes such as the Information Technology Infrastructure Library (ITIL V3). The new enterprise model includes adopting a stronger set of enterprise governance policies for effective oversight and improved enterprise architecture implemented in a secure, low-risk transition model. It is clear that any new model must provide enhanced controls for security and data integrity to achieve compliance with applicable policies, laws, regulations, and controls. This new model is extremely important to the efficient and effective management of a major state government compute operation like what exists at the Commonwealth.

As your service provider for many years, we thoroughly understand that the criticality of Commonwealth services supported by the technology infrastructure demands a robust,

comprehensive, and effective disaster recovery capability. Maintaining numerous data centers that host dependent yet separated applications make planning and recovery significantly more complex. An example of this is the interdependencies among the Commonwealth Law Enforcement Assist Network (CLEAN) system at Pennsylvania State Police, JNET, and the Commonwealth Automated Registration and Titling System (CARATS) and Driver License and Commercial(DL&C) systems at PennDOT. Engineering a solution that provides resiliency and a robust recovery strategy at the enterprise level makes sound business sense and is a critical technical component of this procurement. To that end the Commonwealth has specified a geographically dispersed 2+ data center architecture as depicted in **Figure 1-1,** which will be overlaid with a key service framework consisting of:

- Program Management Services
- Technical Services
- Facilities Management Services
- Managed Hosting Services
- Capacity of Demand and Additional Services.

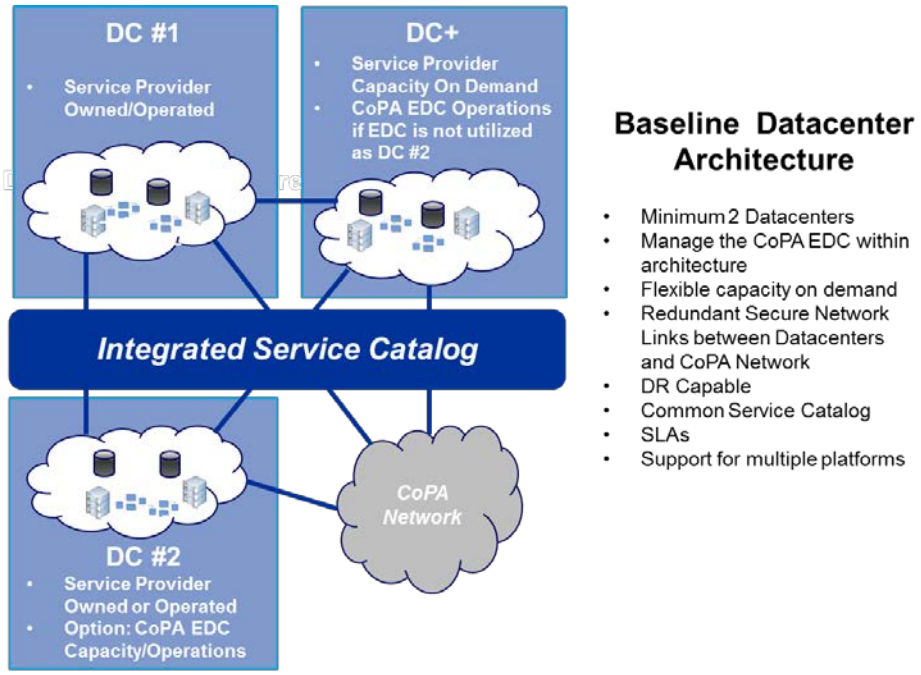


Figure 1-1. Baseline Data Center Architecture (as shown in the RFP)

Services Requested

The Commonwealth-specific needs were then detailed as services and requested in the RFP as follows:

- Minimize risk and disruption of critical services during the transition of existing systems and related computer resources to the new compute model
- Implement a comprehensive enterprise service catalog enabling agencies to select only those services they need
- Provide self-provisioning of selected resources for server and storage capacity in a well-documented, comprehensive enterprise service catalog that recognizes individual needs of the various agencies
- Implement an enterprisewide ITIL V3 IT Service Management platform to support the requirements in this RFP that will assist in continuous improvement and allow further cost savings over time
- Apply a transparent, consistent, and predictable pricing structure to facilitate accurate and timely budget projections
- Assist the Commonwealth with the transition, transformation, and then continual improvement of compute services through innovation and adoption of industry best practices
- Adhere to the Commonwealth's contractual, regulatory, and policy compliance requirements for security, architecture, and Systems Development Life Cycle (SDLC) standards articulated in this procurement
- Establish a tiered managed service capability to support high-availability hosting, backup, and disaster recovery services to maintain continuity of operations
- Properly train Commonwealth staff on new processes such as service ordering, tools, and security; transfer knowledge where appropriate for Commonwealth staff to achieve self-sufficiency
- Offer a variety of optional services such as an assessment of converting the Commonwealth from IPv4 to IPv6.

To successfully deliver the services above, a number of major challenges will need to be addressed, including:

- Migrating the data center services in the DPH that expire in December 2014, as well as additional services outlined in the RFP, with no unplanned service interruptions—all on an aggressive timeline
- Implementing an entirely new process and methodology for acquiring compute services based on a service catalog and consumptive pricing
- Maintaining security of the Commonwealth's sensitive data at all times during transition and then during steady state operations

- Providing proper infrastructure needed to mitigate possible latency and other application integration problems when moving applications that have dependencies on other applications.

To help mitigate the risk of these major challenges, the Data Center Computing Services RFP seeks to place the accountability on a single experienced service provider and the benefits of a consortium's shared experience and knowledge. We agree with this approach. The single service provider and the consortium must have detailed knowledge for both the Commonwealth agencies and their applications and a technical staff with the experience and knowledge and commitment to provide security solutions that safeguard Commonwealth data and resources throughout the contract's period. This "one leading many" strategy will dramatically improve the probability of success.

The real question is how do we achieve the new vision for a service-based consumptive model of compute services, user support, and consolidated data centers? The new model will emerge first through transition and then through transformation and result in an innovative compute model enabling the future of IT in the Commonwealth.

Transition and Transformation — Critical Success Factors

The future compute services model outlined in this procurement will provide the Commonwealth with substantial benefits. However, the path to the new model is complex, challenging, and if not managed appropriately, high risk. Agencies depend on compute services to meet the basic needs of the citizens of Pennsylvania. For example, systems in this RFP process Commonwealth driver license records, motor vehicle records, and state police records; provide critical services that keep our citizens safe; collect taxes and deliver benefits to the Commonwealth's most vulnerable and unemployed citizens; and support elections. These are just a few of the critical services dependent on a successful transition.

We respect the individual needs of each agency with strong consideration for their current business cycles and future business objectives in our planning activities for transition and transformation.

The Unisys Advantage: Incorporate the unique understanding of the Commonwealth business cycle requirements when developing transition and transformation plans.

Impact: Institutional knowledge and relationships gained over the past 13 years dramatically reduce the risk of failure because of our realistic approach to planning and our business process understanding.

Experience Matters. Meeting such a challenge is not new to Unisys. The Unisys Team successfully completed the Commonwealth's first transition to a consolidated data center model in 1999 and a transition to a shared technology model in 2008. Both happened on time, within budget, and with minimal disruption to the critical services provided to Pennsylvania's citizens. The experienced Unisys Team has successfully managed much of the Commonwealth's compute infrastructure for the past 14 years. In fact, Unisys and our team members

currently manage nearly 75 percent of the infrastructure within scope of this RFP.

Commonwealth Experience is CRITICAL. The valuable lessons learned from our team's collective one-of-a-kind experience confirms that the transition and successful operation of the Commonwealth's compute infrastructure is less about the hardware and more about a thorough understanding of the hundreds of agency applications that support critical services for citizens. Any successful transition must also respect each individual agency's business needs and business cycles. Our team has the needed level of knowledge, expertise, and experience specific to Commonwealth agencies that is critical to transition success. **In its absence, the risk of failure increases exponentially.**

Transition is Hard Work but Necessary. Only after a successful transition to the new model can the transformation to a consumptive approach and a program of continual improvement commence. Such a program will help the Commonwealth maximize the investment in compute services technologies and achieve even greater performance for the many critical services delivered by Commonwealth agencies.

Transformation Drives Additional Efficiencies. As systems and applications are transitioned to Unisys, they immediately will be operating on the new compute services model, thereby transformed and meeting all RFP requirements. Then, an active program of continual improvement will begin to enable the Commonwealth to adopt whatever new technologies or best practices emerge during the entire contract period. We are committed to making the Commonwealth the gold standard for government compute services.

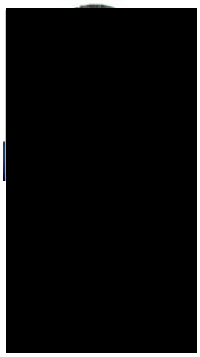
Success is Achievable. The Commonwealth seeks a service provider that can successfully deliver a new compute services model. This new model builds on the Commonwealth's IT success to date and will continue to enhance delivery of government services, improve efficiency and security of operations, and reduce the cost of government. That model needs to provide efficiencies for the Commonwealth going forward and achieve or exceed the performance standards mandated by this procurement. Unisys can successfully deliver and achieve the Commonwealth's vision and objectives.

In Summary

This RFP maps a new direction and offers a real vision for a new compute model to deliver critical services that benefit Pennsylvania's citizens. Unisys and our team of premier technology companies are confident we can assist the Commonwealth to achieve this new model while offering the lowest risk and best outcome to providing compute services efficiently for the contract's entire term.

In 1999, we accepted the challenge of consolidating the Commonwealth's 17 data centers and succeeded. In 2008, we accepted the challenge of reinventing Commonwealth operations to shared services, saved $240 million and succeeded. Now in 2013 and beyond, we are totally committed to accept this new challenge and successfully deliver the results expected in this RFP.

"For the past 12 years I have had the privilege to personally lead the Unisys Team that supports all of our business partnerships with the Commonwealth, and specifically the current DPH and EDC data center services engagements. My philosophy has been simple.....I am the person accountable to our Commonwealth clients...either Commonwealth agencies are completely satisfied with our services or we must make it right. Over these many years I have spent considerable time talking with IT leaders in the various agencies, personally listening to their ideas and concerns and when necessary dealing directly with any concerns. As a Unisys Vice President, my position provides considerable autonomy such that many concerns and issues can be resolved locally and without delay. In rare cases where concerns or issues must be elevated to our corporate leadership I have a direct line to the Unisys senior leadership team, including our CEO, and they have been extremely responsive to me and to matters affecting the Commonwealth. If given the privilege of continuing to deliver services under a new contract, I pledge my commitment to quality service will be stronger than ever."



Vice President, Unisys

2.0 Management Summary

2. MANAGEMENT SUMMARY 2-3

2.1 THE PATH FORWARD 2-3
2.2 THE UNISYS TEAM 2-4
2.3 OUR EXECUTIVE LEADERSHIP TEAM 2-7
2.4 UNISYS SOLUTION 2-14
2.4.1 Unisys Tenets 2-14
2.5 THE PROPOSED SOLUTION 2-14

"As a Pennsylvania-based corporation, Unisys and many of our employees depend on the critical services the Commonwealth will provide through this initiative. That is added incentive for our team to succeed and meet your expectations. As a demonstration of our commitment to the Commonwealth I will personally serve as the executive sponsor to ensure the highest levels of service and satisfaction."

Commonwealth Executive Sponsor
Chairman and CEO
Unisys

This page intentionally left blank.

2. Management Summary

RFP	*Requirement*
II-2	*Management Summary. Include a narrative description of the proposed effort and a list of the items to be delivered or services to be provided.*

This RFP is much broader and far more significant than consolidating infrastructure. The essence of this opportunity is optimized "compute services," supporting the Commonwealth's applications by providing the right service in the right capacity when it is needed and in a way that is cost effective, transparent, and secure. When the transition is complete and the benefits are realized, the industry will recognize this initiative for what it is—a paradigm shift in service delivery for state government.

2.1 The Path Forward

This engagement is an innovation effort to transform information technology (IT) at the Commonwealth to a robust yet flexible offering that supports current and future capacity and service levels that evolve, expand, and contract with the flow of changes in the Commonwealth's business and operating environment. No longer is it acceptable to carry fixed costs that burden the Commonwealth financially when changes in the economy, government funding, or government needs occur. IT at the Commonwealth must be an enabler of these changes to optimize your operating environment going forward.

The Commonwealth is seeking a fundamental shift in the way it acquires and operates IT by implementing a fully consumptive, secure private cloud services utility model. The model is based on an IT Service Management platform that leverages ITIL V3 best practices and Lean Six Sigma methods to create an "optimization framework" for an enterprise-centric IT infrastructure.

Ultimately, the Commonwealth and its chosen service provider will move the current Commonwealth applications to an Infrastructure as a Service (IaaS) operating model in which agencies can scale transactions and compute capacity based on need, therefore optimizing the cost of supporting these applications. **That is much different from today's contract which features fixed pricing for most services, limited transparency, and little flexibility to scale according to changing needs. The new model will provide the opportunity to lower costs of service and the means to tailor services to specific needs. As your current service provider, we welcome these changes.**

2.2 The Unisys Team

To be successful and to mitigate risk to the greatest degree possible, this innovative effort must start with a world-class team delivering specific and proven experience with the Commonwealth of Pennsylvania. Unisys, as the prime contractor, will be totally responsible for successfully delivering the compute services in this RFP's scope. As a Pennsylvania-based company with approximately 23,000 employees worldwide, Unisys has a long and successful record of accomplishment of working with you and other prestigious organizations on similar innovative efforts.

Innovation - Flexible Pricing Models

Unisys Experience with:

- *Defense Information Systems Agency (DISA)*
- *Internal Revenue Service (IRS)*
- *City of Minneapolis*
- *American Red Cross*
- *California State University System(CSU)*

For this engagement, we will bring forward many local IT experts—currently more than 150—who support the Commonwealth today and we build on that core group with new staff and skills to actively pursue robust new programs for continuous innovation and improvement. We again have partnered with **IBM** and others you know but also have engaged several new partners, including **Deloitte Consulting** (Deloitte). All have been carefully selected for their unique skills, knowledge or resources to enable success of this engagement, to deliver on time and on budget, and to meet the Commonwealth's high expectations for flexibility, service quality, and client satisfaction. We are blending resources most experienced with your applications and systems with new skills and new ideas to drive ongoing innovation and efficiencies.

Stability and reliability of your compute services environment will be our top priority. We estimate that our team – The Unisys Team – currently manages approximately 75 percent of your in-scope compute capacity. That level of knowledge and experience is a key differentiator between the Unisys Team and others that claim they have the credentials necessary to transition the Commonwealth's most important systems.

IBM and Deloitte are exclusive partners to the Unisys Team. Both are premier companies and experienced providers of services and technology to the Commonwealth. As illustrated in **Figure 2-1,** we considered many factors when we selected IBM and Deloitte for our core, "best of breed" team to deliver compute services to the Commonwealth.

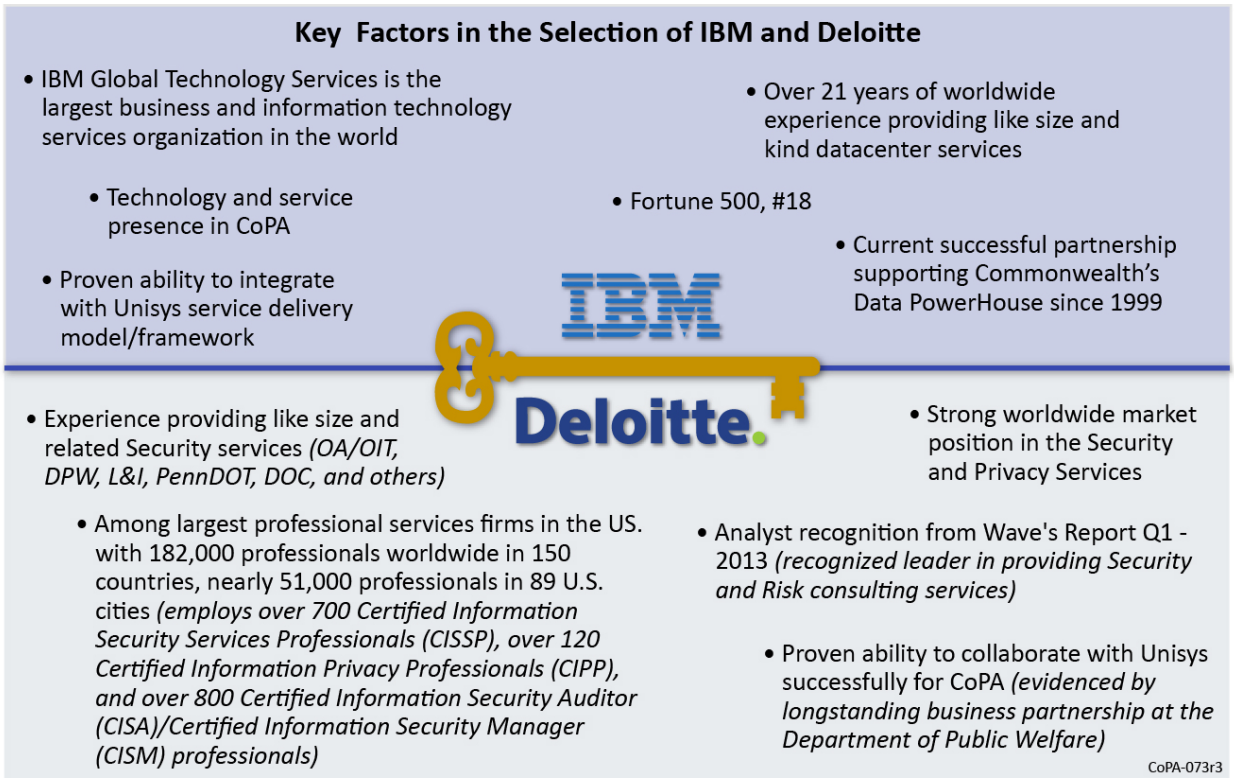


Figure 2-1. Key Factors

Figure 2-2 highlights the entire Unisys Team and each team member's role. Recognizing the value of the Commonwealth's approach with its own staff augmentation contract, Unisys assembled a large pool of Small Diverse Businesses (SDBs) to improve our ability to source the best technical resources at the best value while helping the local, small and diverse business community. Those SDB firms include **American Personnel Managers, Acclaim Systems, Credo Technology Solutions, Domino Technologies, e & e IT Consulting Systems, Info-Matrix Corporation, Innovative Business Concepts,** and **PCN.** We also selected **Pierson Computing Connection Incorporated** to provide certain technology components of our solution, and **Latus Commercial Realty** to provide commercial real estate services. In addition, we have added **Harrisburg University of Science and Technology** to provide educational and training support.

With added focus on innovation and emerging technologies, our team also includes BMC, Cisco, EMC, Microsoft, PMG, PureShare, Juniper, and VMware. These companies are on the leading edge of new technologies that can transform the way we operate and in turn deliver significant efficiencies. Section 4 of our proposal provides a detailed perspective of Unisys qualifications and additional details on the members of our team.

Figure 2-2. The Unisys Team

This consortium is world class. It includes the two primary inventors and suppliers—Unisys and IBM—of the technology infrastructure and system software running nearly all of the Commonwealth's business application systems. Therefore, the Unisys Team will have a direct line to software developers and technical support experts worldwide for issues that require around-the-clock problem solving.

We know success revolves around the Commonwealth's business application systems and keeping them fully operational. Unisys and IBM together offer more than 100 years of working knowledge of the Commonwealth's business application systems. Further, we augmented our team with Deloitte, the largest, most experienced applications integrator, developer, and application maintenance provider in support of the Commonwealth's business application systems. Deloitte also provides a variety of mission-critical IT

Committed to the Commonwealth

Local Knowledgeable Resources

In Pennsylvania, Unisys, IBM, and Deloitte Consulting employ 6,962 people with more than 900 people in the metropolitan Harrisburg area.

security services to the Commonwealth. Our team will leverage Deloitte's application knowledge and security capabilities extensively, further promoting success overall.

The Unisys Team has unsurpassed collective knowledge of your applications, business, history, nuances, people, policies, processes and systems. The Unisys Team has an unmatched – unrivaled record of accomplishment in the managed infrastructure services, security, and application services space for the Commonwealth. For example:

- We have consistently met high levels of availability and met or exceeded service level requirements
  - Specifically:
    - **Achieved overall 99.9915 percent availability** in the DPH since 2008
    - **Achieved greater than 99 percent of all SLAs** since 2008
- We have had no security breaches in the DPH
- We successfully completed a number of innovative initiatives, including:
  - Implementation of the enterprise shared infrastructure
  - Inclusion of tiered service levels and rate card
  - Piloting of self-provisioning
  - Near 100 percent ITIL V3 Foundation certification of all Unisys DPH and EDC delivery staff

Bottom line—we have assembled a team with by far the most experience and knowledge specific to the Commonwealth supplemented by a global network of experts to assist, as necessary. This team comprises experienced staff—many of whom you already know—starting with our executive leadership.

2.3 Our Executive Leadership Team

Because of this engagement's importance and our commitment to the Commonwealth of Pennsylvania, Ed Coleman, Unisys Chairman and CEO, has chosen to serve as Executive Sponsor and will personally ensure our company's complete commitment to its success.

In addition to Ed Coleman's role as Executive Sponsor, Unisys established an Executive Leadership Committee to support the efforts of our Harrisburg-based service delivery leadership team. This committee, which consists of senior business and service delivery executives from Unisys, IBM and Deloitte, was established to provide direct visibility into our respective organizations to

"We have an excellent service delivery team assigned to this initiative. [redacted] and [redacted] are some of the very best in service delivery. I trust their judgment and have empowered them to make the necessary decisions locally to keep the project on schedule and meet your expectations. Their team is complemented by a Unisys Executive Leadership Committee focused on providing whatever additional corporate resources and support are necessary to succeed."

—Ed Coleman
Commonwealth Executive Sponsor
Chairman & CEO

enable us to meet our commitments to the Commonwealth during transition and steady state operations. This committee also will be tasked to resolve issues that may arise but cannot be resolved locally. The committee will provide executive leadership, support, and direction throughout the engagement's entire life and will be a vital component of the transition and steady state governance model. **Figure 2-3** identifies the members of our Executive Leadership Committee.

Figure 2-3. Unisys Executive Leadership Committee

Our Service Delivery Team

The Harrisburg-based Unisys leadership team, depicted in **Figure 2-4,** will be led by [redacted] As Engagement Executive, Ann has worked closely with key Commonwealth executives to manage many aspects of the current Data PowerHouse (DPH) Program over the past five years. On joining Unisys, Ann oversaw the successful transition to shared services in 2008. This transformed service delivery and saved the Commonwealth $240 million.

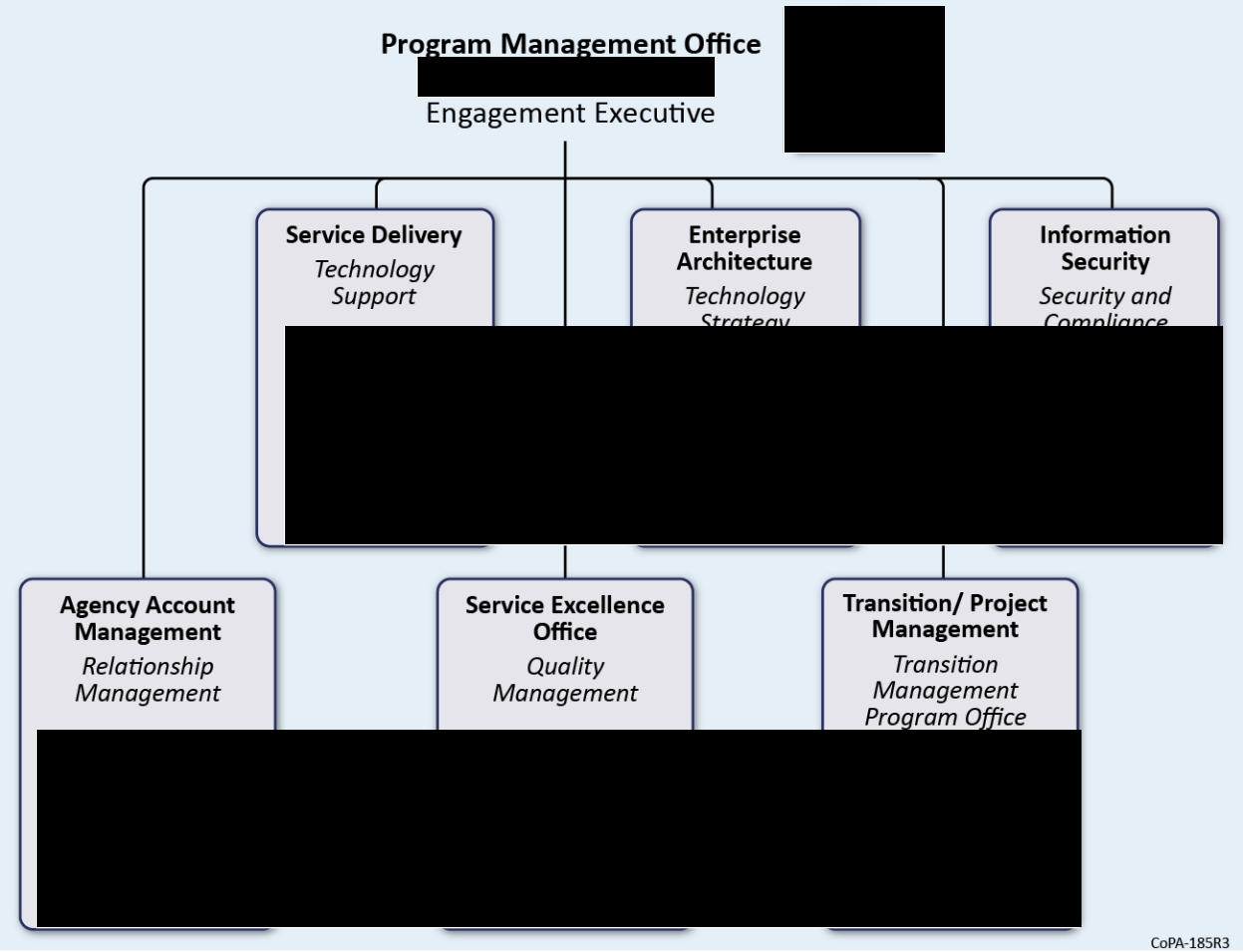


Figure 2-4. Unisys Harrisburg Service Delivery Team

During her tenure with Unisys, Ann spearheaded a number of innovative technology solutions, including server virtualization that reduced costs for the Commonwealth. She also fostered the evolution of the DPH architecture to new technology concepts, including disk-based backup solutions and flexible service offerings. Ann has demonstrated great sensitivity when it comes to customer satisfaction by implementing a number of in-depth survey processes designed to take the customer's pulse at many different levels on all aspects of service. She has held her team accountable to document issues and follow-up actions in collaboration with the agencies. These activities improved customer satisfaction significantly. Ann's Certifications – ITIL V3 Foundation.

[redacted] was presented with the 2012 Outstanding Leadership and Innovation ("Ollie") award from former Commonwealth CIO George White for his efforts at OA-Information Technology (OIT) to support the Pennsylvania State Police. The "Ollie" award is sponsored by the Office of Administration's Office for Information Technology and Government Technology magazine.

[redacted] will serve the Commonwealth as lead Agency Account Manager. Pete is a 23-year Unisys employee who has worked at the Commonwealth of Pennsylvania since 2002 in a variety of Project Management and Client Services Management roles supporting numerous Commonwealth organizations. Since 2005, he has worked on site at the Commonwealth Technology Center in very close collaboration with the Commonwealth CTO, CISO, Client Management, Enterprise Data Center, Enterprise Networking and Security, Enterprise Services, GIS, PMO, and many agencies. Certifications—ITIL V3 Foundation and PMP.

[redacted] will serve the Commonwealth as the Service Delivery Executive (Program Manager). Ricky brings 14 years of experience leading large Service Delivery organizations, most recently supporting outsourced engagements for Computer Sciences Corporation (CSC). Ricky will leverage his experience with leading large-scale data center delivery teams, including a team at Textron, where he directed the consolidation of 10 sites with multiple mainframes and more than 800 open systems servers and then managed an ongoing Service Delivery team of 500 employees. Certification—ITIL V3 Foundation.

[redacted] will serve the Commonwealth as PMO Transition Manager. Scott brings 27 years of IT delivery experience working for large IT outsourcing firms before joining Unisys at the beginning of this year. As a Transition Management leader working for Dell Services (formerly Perot Systems), Scott led multiple large-scale data center transitions, migrations, and system upgrades during his 5-year tenure. Scott managed Perot Systems' Healthcare Business Unit portfolio of transitions and data center migrations. Certifications—ITIL V3 Foundation and PMP.

[redacted] will serve the Commonwealth as the Senior Enterprise Architect under the new contract. He has 16 years of IT industry experience working for IBM in several architect roles before joining Unisys in 2011 as the Lead Client Architect managing the Unisys North American Client Architect team, which includes oversight of the Client Architects supporting the Commonwealth. While working for IBM, Bryan served as Transformation Integration Architect, leading a large team of architects to develop technical components to build a multitenant data center to support the State of Georgia's strategic consolidation plans. Certifications—ITIL V3 Foundation, Open Group Master IT Architect, and IBM IT Architect Certifications.

[redacted] will serve the Commonwealth as the Chief Security Manager. Mike brings more than 38 years of technical and management experience, working with a number of federal and state government agencies, including the Pennsylvania State Police (PSP), for which he managed security for the new Commonwealth Law Enforcement Assistance Network (CLEAN). He also collaborated with JNET to provide access to CLEAN by JNET users without requiring additional authentication and assisted Office of Administration/Office for Information Technology (OA/OIT) leadership with creating Security ITBs. Mike's efforts enabled deployment of the new Megan's Law application to its full user base much faster than would have been achievable otherwise, enabling PSP to meet its legislatively mandated deadline. Certifications—CISSP (Certified Information Systems Professional) and SANS GSEC (Global Information Assurance Certification Security Essentials Certification).

[redacted] will serve the Commonwealth as the Service Excellence Officer. Michael is currently the Operations Director for Unisys in North America responsible for all Unisys customers; Michael will be 100 percent dedicated to the Commonwealth. A 32-year employee with Unisys, Michael brings considerable successful experience across our client base. In his current role, he led a number of key initiatives under our ITIL V3 and Lean Six Sigma-based Continual Service Improvement Program. Michael led several service improvement initiatives for the Commonwealth, including multiple Kaizen Process Optimization workshops with the Unisys Team supporting the Commonwealth of Pennsylvania. One of these workshops laid the groundwork to transition the DPH contract from an antiquated Remedy system to the current ITSM 7.6 Remedy system. Certifications—Six Sigma Lean Black Belt and ITIL V3 Foundation.

Section 5 of our proposal provides a detailed description of the entire Unisys staffing plan, including other key personnel on the Unisys Team.

Our team is organized around your needs and largely based in Harrisburg -- close to you. That will help facilitate more effective coordination and communications. **Figure 2-5** is a high-level description of the functions of each of our seven core teams.

Figure 2-5. Seven Functional Teams

To illustrate the interaction between our team and the Commonwealth team, we present **Figure 2-6.** It is a high-level graphical depiction of the coordination and flow of communications between our respective organizations. Having significant experience with the Commonwealth, Unisys understands that it is not as simple as one Unisys point of contact to a single Commonwealth counterpart. The Commonwealth organization is multidimensional; each agency has its own management structure and IT support team, and the OA manages the contract on behalf of the agencies.

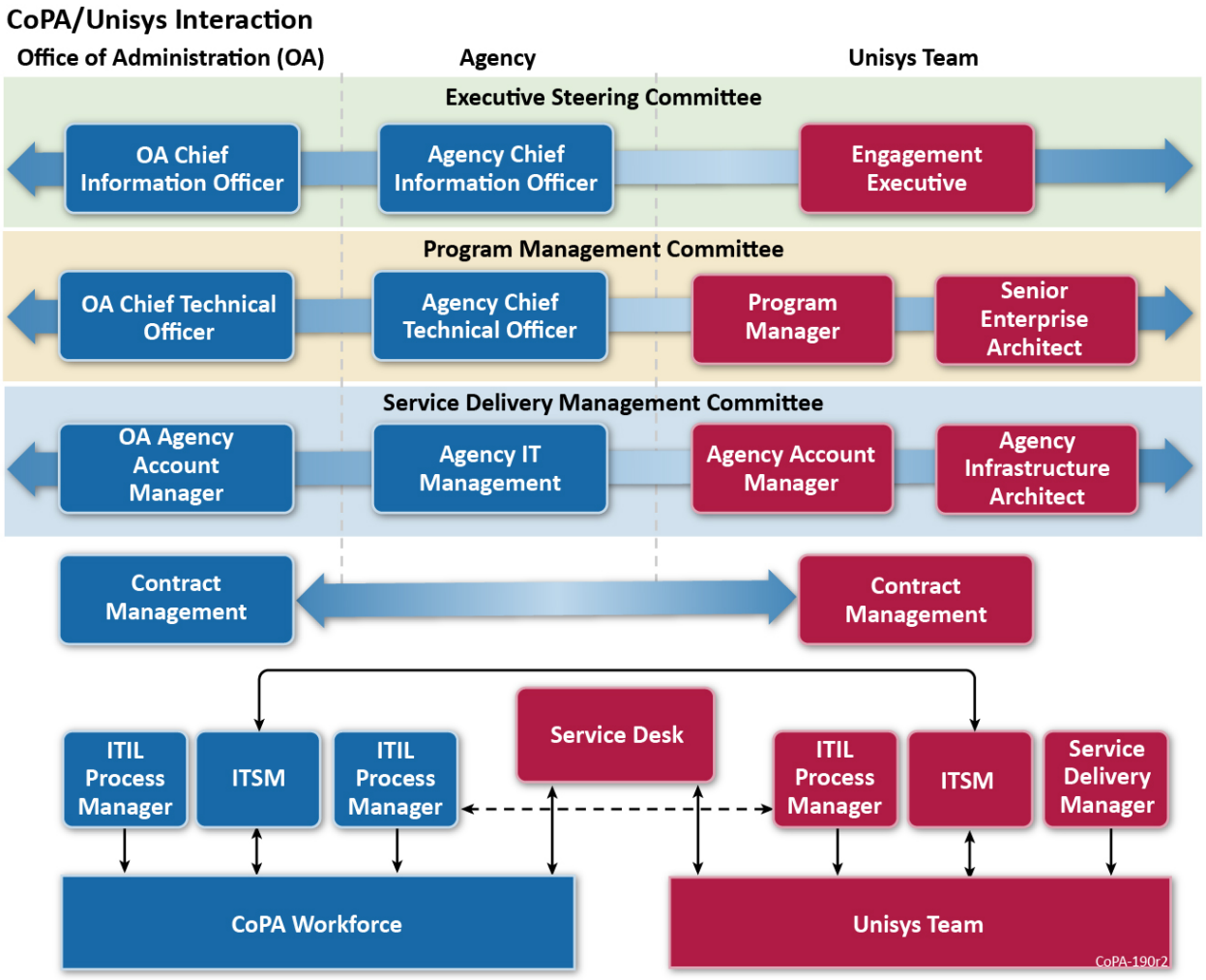


Figure 2-6. Commonwealth and Unisys Communication and Interaction Flow

As part of our deliverables, Unisys will develop, with you, a comprehensive stakeholder communications plan involving our leadership team in addition to our project and service delivery staff. That will enable those affected but not included above to have the necessary information on each stage of the transition.

Now that you have been introduced to the Unisys Team and our key leadership staff, the sections that follow highlight the solution strategy we followed to meet the Commonwealth's requirements as well as an overview of our proposed solution.

2.4 Unisys Solution

2.4.1 Unisys Tenets

Given our knowledge of the Commonwealth, and a detailed review of the RFP's requirements, we carefully selected our consortium partners, and designed a solution based on the following tenets:

- **"Do no harm" –** Every aspect of the engagement must be performed without any unplanned interruption of services
- **"Align compute services with the business" –** Our proposed solution must provide a transparent and flexible compute services environment aligned with the business needs of the agencies
- **"Achieve success together" –** Work closely with Commonwealth staff, understand and address their individual issues, and provide needed training to facilitate knowledge transfer and adoption of best practices
- **"Focus on moving software applications rather than moving hardware" –** This is about moving software applications that support the most important functions of Pennsylvania state government
- **"Managing change is key to success" –** We must implement strong change management practices, a solid training plan, and effective communications when transforming the Commonwealth to its future model
- **"Recognize and respect differences among individual agencies" –** We must recognize that agencies will have their autonomy to execute their business goals while assisting the Office of Administration with achieving its enterprise objectives
- **"Innovation is a must" –** In all aspects of our solution, we must look ahead…not back
- **"Security is paramount" –** We must encapsulate everything we do with a strong security framework that protects all Commonwealth data and IT resources.

2.5 The Proposed Solution

Our proposed solution is designed to eliminate any application latency risks to the Commonwealth's applications while providing an ongoing cost-effective solution to meet the Commonwealth's security, operational, and financial objectives. To deliver the required services and meet the RFP's requirements, we carefully architected two key components: the **Data Center Infrastructures** that will underpin the services delivered through a **Component-based Operating Model,** both of which are described below.

Data Center Infrastructures

As depicted in **Figure 2-7,** Unisys will provide a network of Tier 3 data centers interconnected to provide the optimum data center environment. This network improves resiliency and largely mitigates any application latency issues with the move of the DPH

and other agency data centers to the new compute environment. In addition to the EDC, our data center approach will be to leverage two additional compute facilities in [redacted] and [redacted] A contributing reason we chose the [redacted] facility as a primary production site is its location, which is within a 120-mile radius of Harrisburg—an important metric relative to the reduction of any potential latency issues with moving the Commonwealth's applications to a new location. Also, there is a robust telecommunications infrastructure in the [redacted] area to locate the workloads that currently exist in the DPH. Remaining agency data centers will be located in either the [redacted] or [redacted] facilities. During data gathering, we will study network latency and other factors with the productions applications in the agency data centers to determine the best location for the workloads based on potential latency issues that need to be mitigated. An important consideration in the selection of [redacted] as a data center is to provide geographical separation for disaster recovery workloads to better protect the Commonwealth in the event of a natural disaster occurring on the East Coast. Today, Commonwealth disaster recovery workloads are greater than 50 miles apart, but they are in the same geographical zone which poses a risk to the Commonwealth. [redacted] provides the ability to locate disaster workloads in the EDC or vice versa if geological separation is desired.

We plan to leave the EDC "as is" during migration to mitigate risk and to focus on other transition activities. Unisys will establish the IT Service Management (ITSM) infrastructure for the Commonwealth in the EDC initially and then a redundant copy in [redacted] to provide the compute services outlined in this proposal and to accommodate existing applications.

Unisys will deploy a network-operating environment that is fully fault tolerant and provides the scalability and flexibility needed going forward while reducing network-operating costs. Furthermore, this network will be integrated into COPANET to interconnect the compute facilities in **Figure 2-7**.

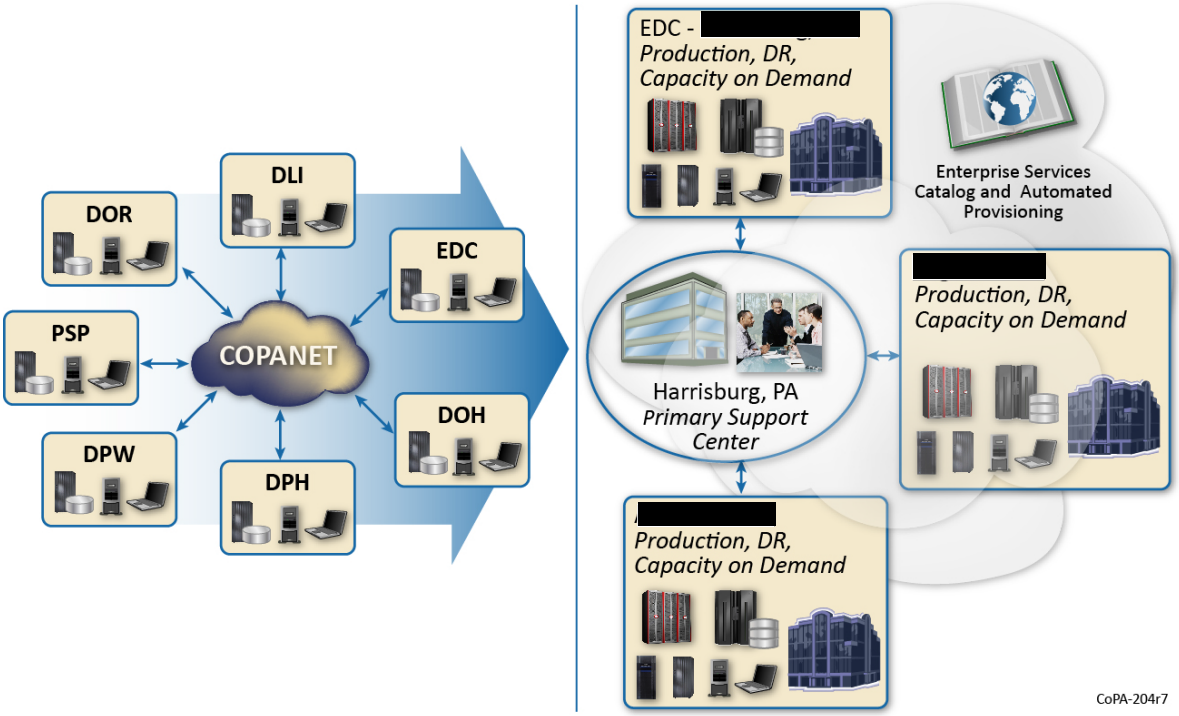


Figure 2-7. Proposed Data Center Architecture

Unisys also will deliver a modern disaster recovery plan and framework that leverages the use of Capacity-on-Demand computing to have the right amount of compute resources when needed eliminating the expense of having dedicated systems sitting idle. The Unisys approach to disaster recovery is based on systems as workloads that can be located in any facility that in turn can leverage capacity-on-demand models to make disaster recovery cost-effective moving forward.

While our compute centers are geographically dispersed to provide the maximum protection (risk reduction) flexibility and cost efficiencies, their operations will be integrated through the Component Based Operating Model depicted in **Figure 2-9**. The primary support center that will operate this model will be in the Harrisburg area, thereby providing not only convenient access by Commonwealth staff but also the opportunity to base the vast majority of our delivery and support team in Harrisburg avoiding the typical phone support only model provided by others

Common Infrastructure Architecture

Within each of the data centers is a common infrastructure architecture to support the Managed Hosting and Capacity-on-Demand Services. It is important to note there is no difference in the infrastructure platform to support Managed Hosting or Capacity-on-Demand thereby simplifying the management and provisioning efforts which enables the

ability to optimize and scale of workloads, which leads to cost efficiencies. The components that make up the infrastructure architecture are depicted in **Figure 2-8** below.

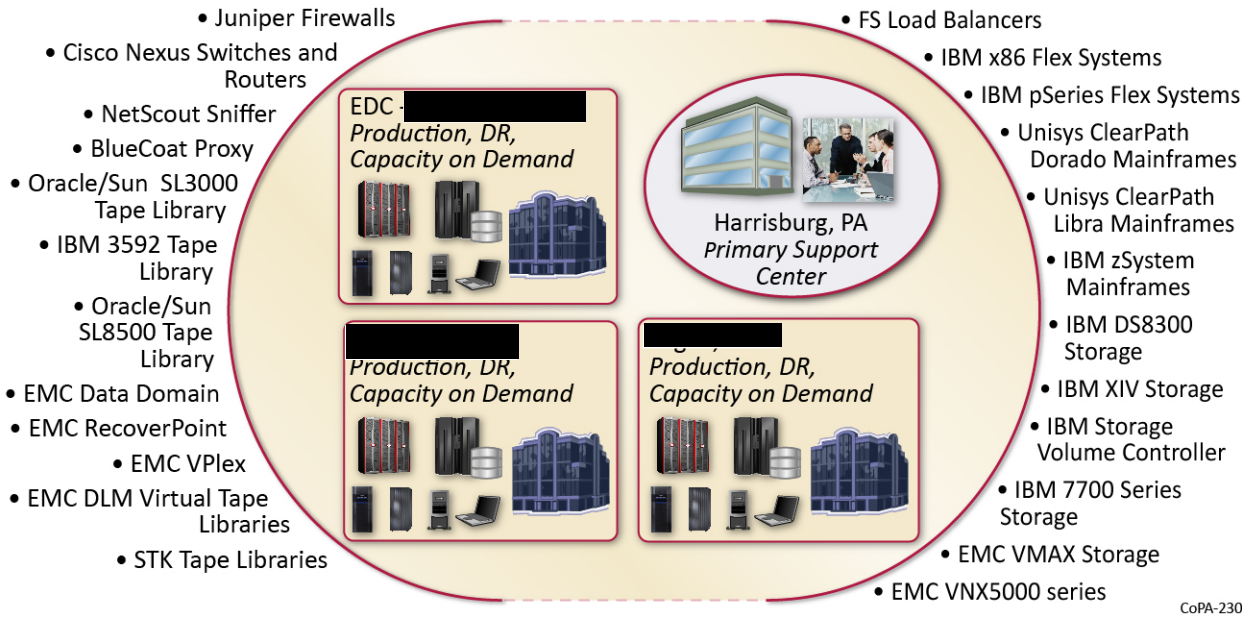


Figure 2-8. Common Infrastructure Architecture

Component Based Operating Model

To achieve the RFP's requirements, Unisys developed a component-based operating model as depicted in **Figure 2-9.** This model encompasses the requirements in the RFP and reflects a logical view that the Commonwealth can easily visualize. This compute services model illustrates the main deliverables and services and will sit on top of all compute data center facilities in **Figure 2-7** that Unisys provides for Commonwealth workloads, whether production or disaster recovery based.

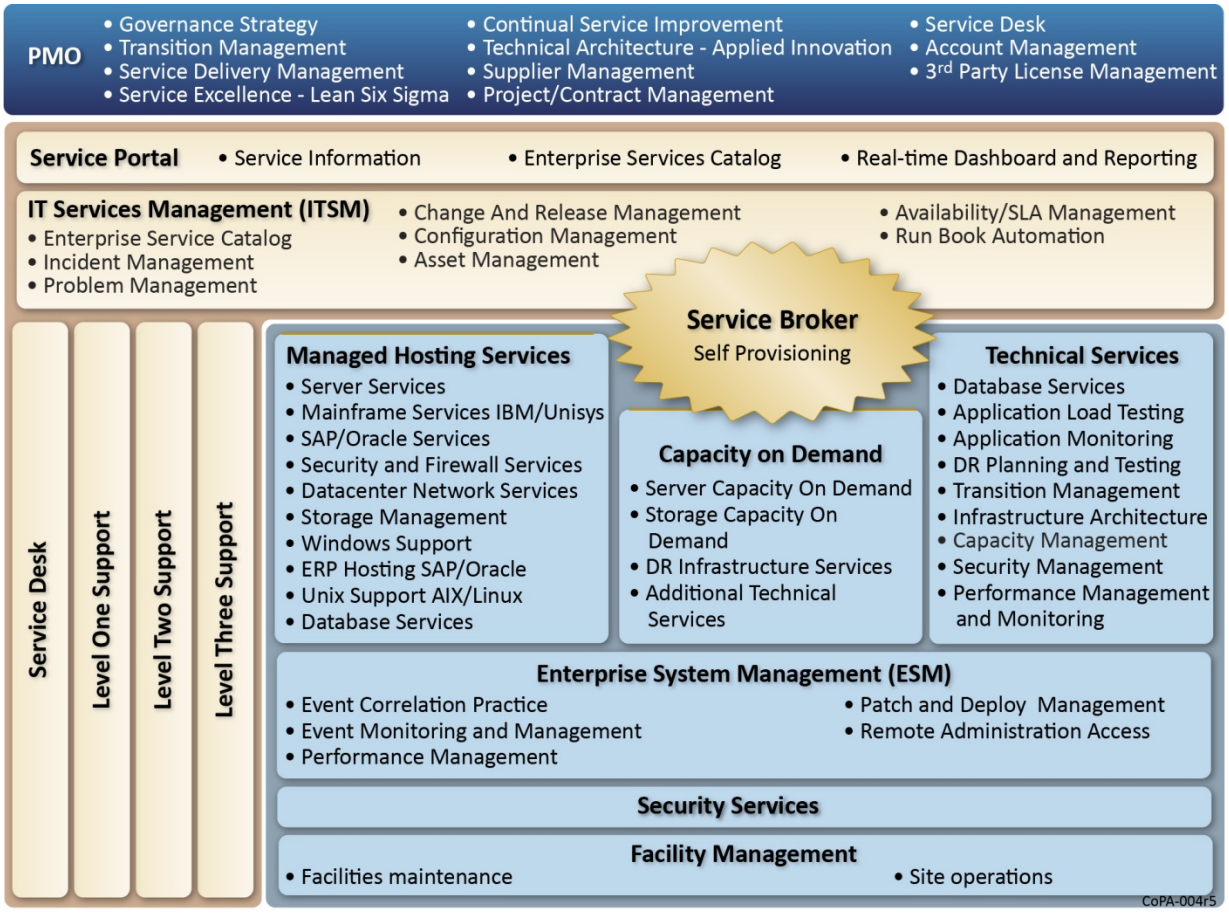


Figure 2-9. Component Based Operating Model

The Component Based Operating Model is broken down into the following components to support the requirements within the RFP:

1. **Program Management Office –** Establish a local and dedicated Program Management and Service Excellence Office that provides a focus on governance, a drive toward continued value, and cost savings by deploying Lean Six Sigma practices based on studies of cycle time and defect analysis from events that are extracted from the IT Service Management platform. By removing cycle time waste and defects of the operating environment, Unisys will provide the Commonwealth with continued cost savings and a higher quality IT compute environment. This same office is responsible for the ongoing governance of driving continuous service improvement and innovation.

2. **Service Portal –** Create an enterprise services portal, enterprise services catalog, and real-time dashboard to provide a single interface to all agencies to interact, provision, and be able to determine the performance of the IT operating environment in near real time. Each agency will have the ability to develop its own

personality with its service portal. Agencies will be able to configure their portals to develop their own "look and feel," determine the services they want to publish or offer, provision, and report on, in near real time, while still having access to the overall view of the enterprise as appropriate.

3. **IT Service Management –** Deliver an enterprise IT Service Management platform based on ITIL V3 best practices and Lean Six Sigma methods that drive the maturity of the IT operating model with a goal of achieving an efficiency gain of 5 percent year over year. Of significant importance is the development of an enterprise wide Configuration Management Database (CMDB) that defines the service that IT delivers to the Commonwealth. The creation of services in the CMDB will allow the Commonwealth to proactively determine business impact by determining a fault before it occurs and allowing maximum use of IT resources to reduce ongoing cost. Each agency will have its own instance in the service management environment to provide operating autonomy. Unisys will provide a federated service management environment to the OA so it has the overall view of the total IT operating environment at the Commonwealth. The Commonwealth can be comfortable knowing that Unisys supports a multitude of IT Service Management Systems, including BMC Remedy and ServiceNow. Our Component-based Operating model can be enabled with any one of the named IT Service Management Platforms.

4. **Managed Hosting Services and Capacity on Demand –** Enable an adaptive, flexible, and secure hardware compute environment that is based on a consumptive utility model with a "no volume commit" attribute that provides the agencies with the autonomy to perform their IT functions and meet their business requirements. In the Unisys compute model, there is fundamentally no difference between Managed Hosting Services and Capacity on Demand because they are served from the same hardware platforms and managed by the same ITSM management platform. As an innovation effort and to make sure the Commonwealth is aligned with market trends, the Unisys Team includes optional Virtual Private Cloud offerings from Microsoft and VMware in the Catalog of Services. From Microsoft, we included Azure, Office 365, and Dynamics as optional services. From VMware, we included its new offering in the marketplace for virtual private cloud capacity for Windows as an optional service.

5. **Service Broker –** Unisys will provide the Commonwealth with a consolidated, optimized, and centralized multitenant compute environment in which the agencies will not have to compromise their control by being able to self-provision workloads through the use of an enterprise service portal and catalog. Once ordered from the service catalog, the request will be processed through ITSM for change approval. When the request is approved, the Service Broker will invoke an automated runbook to execute the provisioning effort. Once the provisioning effort is complete, the runbook will update the Configuration Management Database. Agencies will be able to maintain a very real level of control over their compute environment required to meet the business need. As an innovation effort, the Service Catalog and

Service Broker will be an integrated pair to provision not only capacity from the private cloud environment we are providing the Commonwealth, but also all services from partners such as IBM, Microsoft, and VMware. Our vision for the Service Catalog and Service Broker is you can provision any service from any provider at any time with "no commit" that is then managed by the Component Based Compute Model provided in this RFP. One provisioning model and one management model will unify the compute model for the Commonwealth and provide the business flexibility and optimized compute environment the Commonwealth is looking for.

6. **Technical Services –** Unisys will provide a set of selectable services that can be procured from the services catalog to manage given applications in the Commonwealth agencies. These technical services can be people- or management-based services and can be procured in a consumption-based approach.

7. **Security Services –** Achieve and maintain a robust and comprehensive security environment that meets the IT Security policies set forth by the Commonwealth. This security environment will be managed by Deloitte, which has years of experience working with the Commonwealth to create, implement, and manage security policies.

8. **Facility Management –** Provide the ongoing management for all data centers whether Unisys or Commonwealth owned facilities.

9. **Service Desk –** The Service Desk will take calls from IT support staff to log incidents that were not automatically generated from the event monitoring system. The Service Desk will use knowledge management to try to resolve an event within an agreed time. If the event cannot be resolved in the agreed time, it will be escalated to Level One Support.

10. **Level One Support –** Level One Support manages all events that are automatically generated from the hardware and application environments as well as resolving incidents that are received from the Service Desk. Level One will use various tools, runbooks, and knowledge management to resolve incidents. If the incident is not resolved within a given time, it will be escalated to Level Two Support.

11. **Level Two Support –** Level Two Support is a team of very knowledgeable resources who can solve a wide array of Commonwealth compute issues. This team largely knows the individuals in the agencies and has an ongoing relationship with them. When Level Two Support believes it cannot resolve the incident in a timely way, it will pull in Level Three Support resources.

12. **Level Three Support –** Level Three Support is a team of architecture experts that deeply understands the compute architecture that supports the Commonwealth applications. This team is also an integral part of driving continuous improvement plan by identifying inefficiencies in the compute architecture.

Because of the Component Based Operating Model already described and the innovative approach to provisioning compute services, Commonwealth IT professionals may ask questions about how to provision workloads, how to manage and report on the workloads, and how to drive continuous improvement. To answer those expected questions, we provide brief summaries below.

"How do I provision workloads?"

The process will begin with logging onto the services portal that will be configured with a look and feel for each agency. In accordance with the agency and personal login credentials, users will be presented with the services they may provision. Provisioning a service will be an "Amazon-like" experience in which a user will select services from the catalog and provide quantity and key information to order the service. Once the "shopping cart" is filled, the order will be submitted and provisioned using the Service Broker. Each order processed by the ITSM system will have to be preapproved or approved when submitted. No runbook will be generated until a change is approved. Once a change is approved, the runbook will be executed to provision the desired service. Equally important, the CMDB will be automatically updated with the configuration information and the up- and downstream relationships as part of the runbook's execution.

"How do I manage and report in near real time the performance of those workloads?"

With the move to "IT as a business," it is imperative to be able to report in near real time the active performance, health, and quality of the IT services being provided to the Commonwealth. Unisys will provide real-time dashboards that are configurable by user preferences, meaning there are base profiles created for views for a CIO, CTO, Program Manager, and IT professional that enable these users to select the items they want to view on the dashboard. **Figure 2-10** is a representative example of a real-time dashboard.

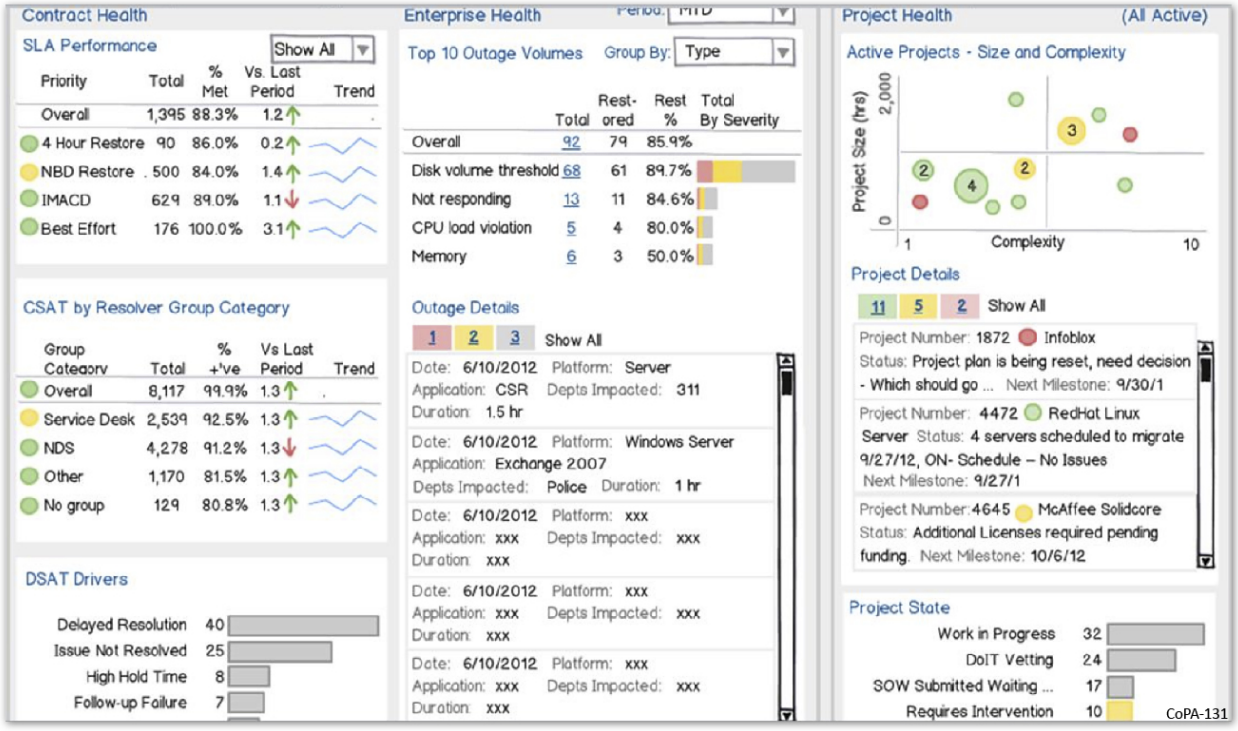


Figure 2-10. Real-time Dashboard

"How do I drive continuous improvement to drive greater value and cost containment?"

The Unisys team will provide a fulltime, dedicated Service Excellence Office. The office is responsible for driving Continuous Service Improvement to the Commonwealth throughout the entire ITIL V3 life cycle, across all Commonwealth Agencies, IT domains, and applications infrastructures. Unisys will apply Lean Six Sigma methodologies to analyze current and trending cycle times and defects collected from industry leading measurement tools. The Service Excellence Office will proactively eliminate anomalies to improve the operating environment from the time services are automatically provisioned through transition, implementation, and the ongoing IT Service Management. This will provide the Commonwealth with reduced costs, drive greater value, and increases quality while providing the Commonwealth with the highest client satisfaction experience.

To deliver and fully realize these solution's benefits, Unisys will develop and execute a comprehensive and reasonable work plan that focuses on the work effort to:

1. **Transition –** implement the component based operating model depicted in **Figure 2-9** across all future state data centers

2. **Migrate applications –** migrate the Commonwealth's applications to the new secure compute environment and immediately adopt the service reference architecture

3. **Implement Continual Service Improvement and Innovation Program (CSIIP) –** implement a continuous improvement program that drives out costs, generates additional value, and improves ongoing quality and client satisfaction.

Work Plan Overview – Simplified, Low Risk, and Based on Experience

Because of the critical nature of the Commonwealth's business systems, you cannot afford to have a service provider that needs to learn on the job. Unisys and our partners fully understand that the Commonwealth's critical business systems cannot be put at risk and that no unexpected downtime is acceptable. In building our proposed work plan, Unisys leveraged our knowledge and experience with the Commonwealth's infrastructure and business systems.

Work Plan – Low Risk and Based on Experience

Our competition may know the outsourcing business, but they do not know the Commonwealth to the degree of the Unisys Team. That is a critical distinction.

Our plan is realistic and achievable. During the first 28 months, the Commonwealth and our team will drive significant change. The realism of the Transition Work Plan is key to minimizing risk to the Commonwealth while we transform your current delivery processes and organization, implement new processes and organizations, and migrate applications from existing data centers to new locations.

On contract approval, Unisys will immediately initiate several actions. For example, the Unisys Team will mobilize in Harrisburg to begin the process of planning and initiating the transition. We will do this quickly because many of the identified resources are already on site and available to assist. Another action will be to formally stand up various governance teams and begin the flow of information. Some of our technical staff will prepare the various data center sites for migration and begin to install the network connections to COPANET. Concurrently, discussions will begin immediately to plan the EDC transition and DPH migration.

During this period and continuing through transition, our main responsibility will be confirming the current production systems are fully operable. Some of our current experts on these systems will actively engage with key members of the project teams; while others will maintain their focus on providing the high levels of service the Commonwealth has come to expect from our team. These experts will come together in the steady state to continue to provide and improve services that will meet or exceed all contractual commitments. **Figure 2-11** depicts the timeline for the various activities in the program.

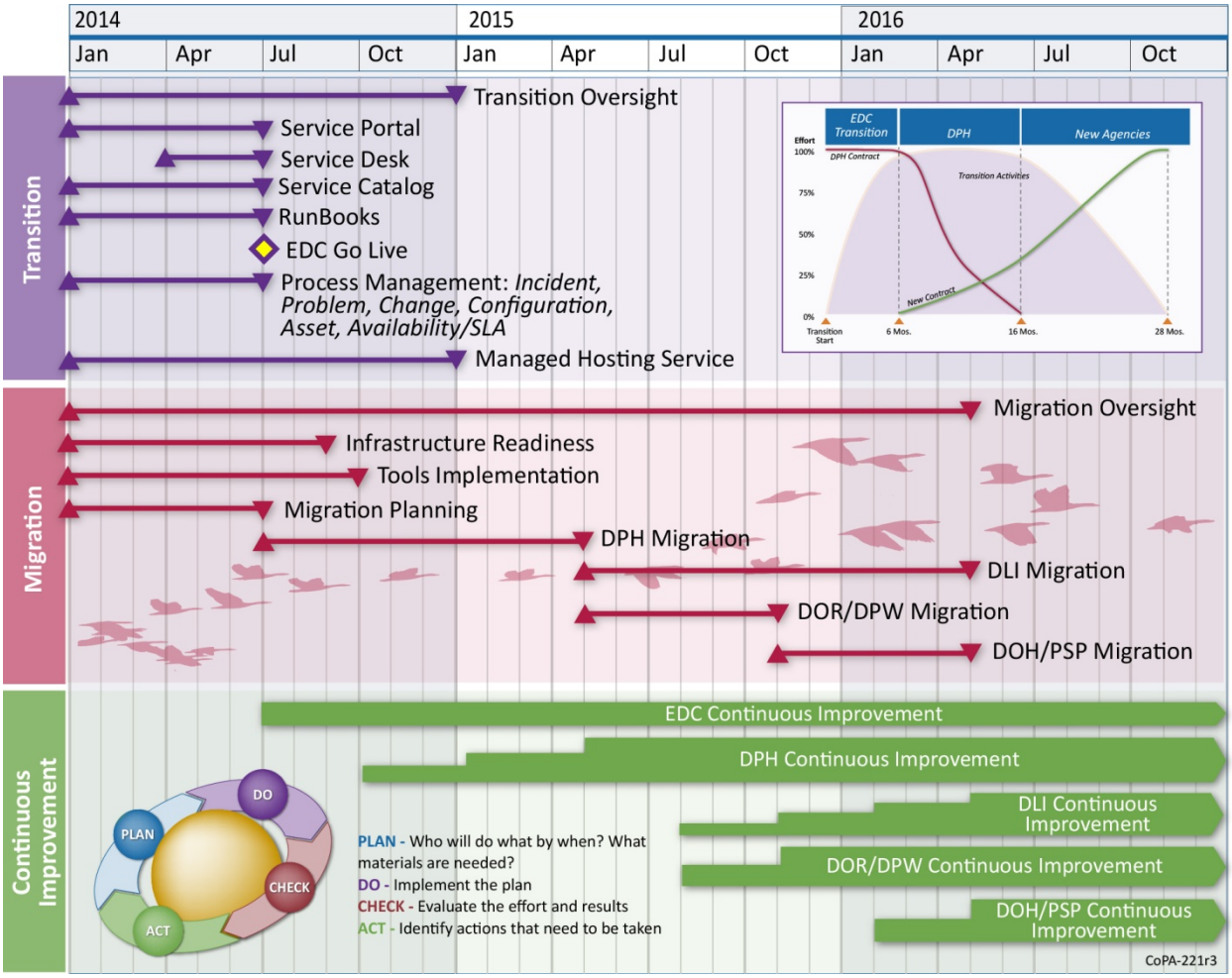


Figure 2-11. Work Plan Timeline

Transition

A major transition from the current operating model is required to achieve the objectives outlined in this RFP. Our approach to transition embodies our tenet of "Do No Harm." Therefore, we will use our detailed knowledge of the Commonwealth systems and lessons learned from prior transitions to mitigate risk. These include finalizing an aggressive but realistic transition plan with significant input from and approval of OA/OIT and the affected agencies.

Transition activities center on People (our team and your team), Process (policies, methodologies and procedures), and Technology (tools)—all required to successfully deliver the new component based operating model. One of the first tasks will be standing up our Program Management Office because it will play a key role throughout transition, transformation, and beyond.

At the core of our service delivery model is an IT Service Management Platform that supports the new processes and tools being implemented. This platform facilitates high-quality service delivery as well as improved sharing of information among all the new data centers, including the EDC. However, achieving the new model differs, depending on where current applications are hosted. The major difference is that the EDC will not be moving; therefore, all the tasks for a physical move of IT infrastructure and applications will be unnecessary for the EDC. An advantage for the Unisys Team is that we currently have significant technical resources helping to manage the EDC. Also, one of our partners, Domino, manages the PennDOT systems in the EDC. Together, we have knowledge of nearly all the technology. Therefore, we are very confident that we can methodically transfer total responsibility to our team in 6 months and very quickly the EDC will begin realizing the new model's benefits.

Transition and transformation of the DPH and the other agency data centers will require a complete relocation of applications and adoption of the new component based operating model. To accelerate the benefits of the new model to the Commonwealth, we architected the transition so that as applications are transferred to the new facility, they are operating in the transformed environment. That means you will receive value more quickly, and at the end of the transition, all systems will be transformed, in the steady state, and ready for a program of continuous improvement.

Application Migration

To migrate applications to the new data centers, the Unisys Team will be required to prepare the new data centers. These activities include establishing connectivity between COPANET and the data centers; establishing Commonwealth-specific infrastructure such as core LAN services; and implementing the infrastructure to support tools and shared infrastructure devices such as firewalls, backup, and monitoring. This project, Infrastructure Readiness, combined with the transition activities described above together will achieve the Operational Readiness milestone defined by the Commonwealth.

Because several migrations are required (DPH and five agency data centers), we will start with the DPH and then generally repeat the process (transition, infrastructure readiness, and so forth) above, incorporating additional lessons learned as we proceed. Again, a "Do no harm" strategy will be used to mitigate the risk of unplanned outages for all transitions and migrations.

In the Application Migration activities, there are three major focus areas:

- The first is **Operational Readiness,** which will provide the infrastructure and processes required to host applications. In these tasks, our team will create detailed designs and implement the Wide Area Network (WAN), Local Area Network (LAN), Storage and Backup infrastructure, Monitoring, Tools, Server Management, Dashboard, and Information Technology Service (ITSM) infrastructures.

- The second major focus area is the **Application Migration (AP) Planning,** which runs in parallel with Operational Readiness. In the planning framework, the AP team will analyze application affinity information gathered electronically as well as in meetings with the agencies and their application owners to determine application move groups. Draft application move group packages based on the information gathered will be created, results of the analysis will show which applications are related to share infrastructure with potential latency dependencies, schedule restrictions, size, complexity, or relate to and depend on other applications. A typical move package will not exceed 125 servers, instances, or images, including Wintel, Linux, or AIX instances and mainframe images. Applications will be targeted to the facility that provides the most benefits, but the Commonwealth will be the final approving authority of any plan.

- The last is the **execution of the migration plan** that overall will move thousands of agency applications in manageable phases. This by far will be the most intensive and most important of all the activities. Even though our team has significant knowledge of the various applications, this must be a collaborative effort with agencies to prevent unexpected interruption of the business of government. The Unisys Team will work closely with the OA/OIT and the agencies to develop detailed plans for each application to be migrated. These plans will include an Hour-by-Hour (HxH) plan, which will detail the step-by-step plans for the test, re-IP, and move events, which will include all precautions required to provide the appropriate level of security needed, fallback plans, testing and acceptance criteria, which will be used to determine the event's success.

As illustrated in **Figure 2-11**, the EDC's transition and transformation are planned to occur within 6 months, DPH within 16 months, and all agency data centers within 28 months. This schedule exceeds the requirements of the RFP and we believe is reasonable.

To oversee all these transition and migration activities is Unisys Transition and Program/Project Management. The Transition Executive, [redacted] will provide a collaborative, transparent, and candid process for the development and management of the plans, adherence to the plans through verified accomplishments, risk management, issue management, quality deliverables, and process improvement. The emphasis of our approach is to provide clear analysis of progress, identify opportunities for improvements, review lessons learned, and implement best practices for each project.

The Unisys Program Management Office (PMO) will have overall responsibility for meeting the contract requirements. Also, guiding and overseeing the Transition Program will be a Program Steering Committee comprising members from OA, agencies, Unisys, and our partner IBM. Also, Project Steering Committees will be used to guide and oversee each of the agency-focused projects.

Continuous Improvement

Unisys will establish a dedicated Service Excellence Office that proactively manages continuous service improvement, ITIL V3 process management, quality, and customer satisfaction through a comprehensive Quality Plan. This quality plan will focus on continuous service improvement, reducing risk, improving service quality, client satisfaction, and transparency, while reducing overall IT costs. We believe this is a key differentiator in our partnership with the Commonwealth. Unisys will develop, implement, manage and govern two detailed Quality Plans. The initial Quality Plan will be a Transition Quality Plan to make sure that quality is a primary focus in the critical Transition of the Commonwealth agencies to the new IT Services contract. Unisys will then develop and manage the IT Services Management Quality Plan, for steady state ongoing operations.

As applications are migrated to the new data centers, they will operate using the new tools and processes, thereby realizing the benefits of the new compute services model. Once applications and systems are transformed, they will reach the steady state. The future steady state model will leverage disciplined processes aligned with ITIL V3 best practices and accountability to deliver against stringent SLAs across more than 30 categories. This evolution from the current state to the future state will leverage state-of-the-art technology and tools coupled with the component based operating model as defined in **Figure 2-9**, and up-to-the-minute statistical reporting across the enterprise displayed on high-tech dashboards at the fingertips of Commonwealth agencies.

To keep these systems optimized, we propose an active and ongoing program to continually find new technologies or new processes that improve performance or lower the cost of operations. We call this our Continual Service Improvement and Innovation Program (CSIIP).

To optimize performance for the Commonwealth during steady state operations, Unisys will implement an ongoing program of Continual Improvement, as depicted in **Figure 2-12**. We developed and use a methodology that has worked well for our clients worldwide, and we will implement it at the Commonwealth. Collaboration is the main premise, and we know from experience that the Commonwealth wants to actively participate in bringing positive change to its compute operations. This program will be led and sponsored by the Service Excellence Office on the Unisys Team.

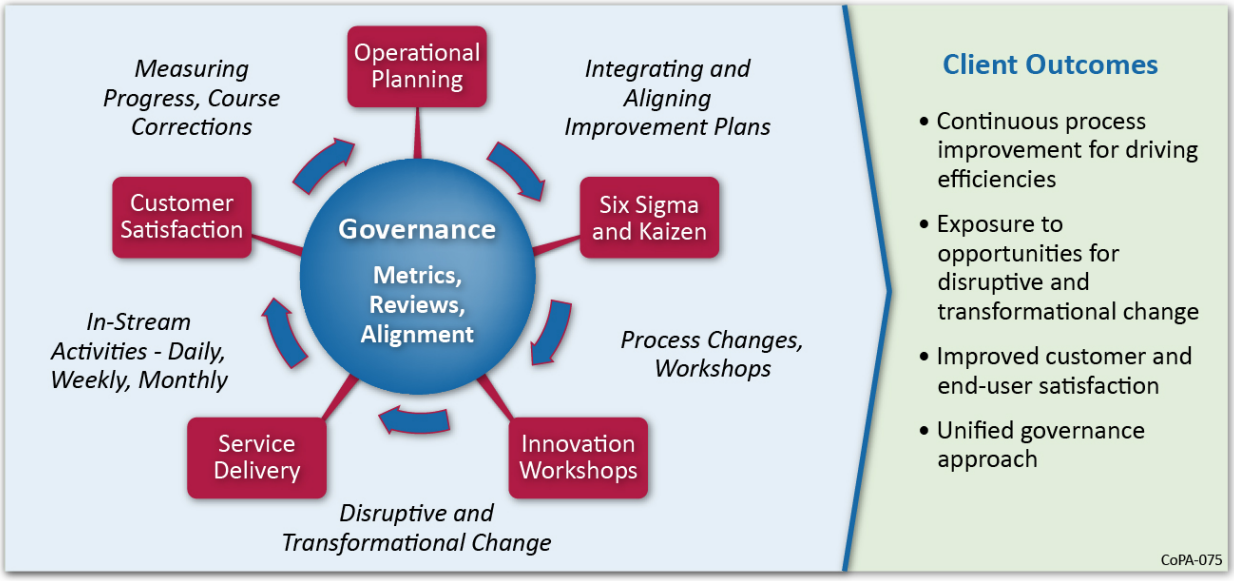


Figure 2-12. Continual Service Improvement and Innovation Program (CSIIP)

Rather than an ad hoc compilation of capabilities, tools, and methods, the CSIIP provides Unisys with a continuous and systematic way to deliver improvement and innovative outcomes for the Commonwealth by leveraging a highly structured yet flexible approach depicted in **Figure 2-12**. Two key elements include our CSIIP and Innovation Workshops.

The CSIIP process includes two types of workshops, Improvement/Kaizen or Innovation Workshops. We will use a global pool of trained facilitators who have conducted workshops across a wide range of industries worldwide.

Improvement/Kaizen workshops are joint sessions between the Commonwealth and Unisys, which focus on identifying opportunities for improvements and categorizing, prioritizing, and developing high-level business cases and implementation roadmaps for the most promising opportunities. Opportunities are governed on a SharePoint portal to provide agencies with visibility and transparency to the continual improvement process.

One of the CSIIP's major features is the ability to consolidate and analyze the many inputs required to effectively develop an innovation and improvement plan. This will provide the Commonwealth with the necessary information to make informed decisions based on relative cost/benefit, alignment with strategy, and ROI for various actions of varying scale from incremental through to truly "breakthrough" initiatives.

Unisys will also collaborate with the Commonwealth by hosting innovation workshops to drive continuous innovation. These workshops will focus on opportunity identification, categorization, prioritization of innovation opportunities, and then on the development of high-level business cases and implementation roadmaps for the most promising opportunities identified.

Innovation is what drives businesses and organizations to excel and is required to meet the ever increasing need for 'faster-better-cheaper.' Unisys' approach looks at all aspects of innovation (strategy, people, process and technology). All are required to be aligned for a program to be successful and impactful. Unisys will work with the Commonwealth and its agencies to clearly understand their strategic IT vision and then work with the each to provide a programmatic approach to innovation. Unisys will work with the Commonwealth to implement a "high-yield innovation pipeline" process to identify and incorporate new innovations into the Commonwealth Agency's IT and infrastructure for the Pennsylvania citizens receiving services.

"The Commonwealth has been a valued Unisys customer for many years. Together, we successfully completed major projects that have provided significant innovations and value like the DPH. I am confident that, if entrusted with this most important engagement, our team will raise the bar even higher for the Commonwealth and its citizens."

—Ed Coleman
Commonwealth Executive Sponsor
Chairman & CEO

The work plan we identified will provide a thoughtful, realistic, and achievable roadmap to meet the RFP's requirements, and just as important your high expectations for delivering a solution that will make the Commonwealth a leader in enterprise compute services.

Innovation Workshops

Unisys Innovation Workshops are collaborative workshops with the Commonwealth designed to explore opportunities for disruptive and transformational change. We will expose the Commonwealth to the latest disruptive technologies and trends and collaboratively examine opportunities for strategic business benefit.

Why the Commonwealth Should Choose the Unisys Team?

All critical services delivered by Commonwealth agencies will depend on this engagement's success. Therefore, it is vital to identify and mitigate all risks so the transition to a new operating model can happen without unplanned outages or reduction in service levels. The consequences of failure are immense and frankly unthinkable.

The Unisys Team of premier technology and service companies has the most experience and knowledge specific to the Commonwealth. As the Unisys Team has been the sole provider of managed DPH services to the Commonwealth, no other offerer can claim this level of expertise. Our experience includes a 13-year track record—measured and reported monthly—that no other team can claim. We have vast knowledge of the existing infrastructure, thousands of agency applications, and Commonwealth processes and business environment. This experience and knowledge will be essential to mitigate risk associated with this innovative endeavor and ultimately meet your high expectations.

And because we are your current service provider, we have greater flexibility and offer more opportunities to customize the work plan to further mitigate risk and meet individual needs of the many agencies that depend on these services. The challenge of the DPH contract's termination on December 31, 2014 will become much less of an issue.

In 1999, we accepted the challenge of consolidating the Commonwealth's 17 data centers and succeeded. In 2008, we accepted the challenge of reinventing Commonwealth operations to shared services, saved $240 million and succeeded. Now in 2013 and beyond, we are totally committed to accept this new challenge and successfully deliver the results expected by this RFP.

3.0 Work Plan

3. WORK PLAN (RFP REQUIREMENT II-3) 3-3

3.1 WORK PLAN OVERVIEW 3-4
3.1.1 Unisys Team Qualifications 3-4
3.1.2 Work Plan Description 3-6
3.2 DETAILED TASK PLAN 3-12
3.2.1 Transition Services 3-14
3.2.1.1 Account Organization 3-14
3.2.1.2 Enterprise Data Center (EDC) to Managed Services Model 3-15
3.2.1.3 Tools Implementation 3-16
3.2.2 Application Workload Migrations 3-17
3.2.2.1 Operational Readiness 3-17
3.2.2.2 Agency Application Workload Migrations 3-18
3.2.3 Transition Program Management 3-19
3.2.4 Steady State 3-19
3.3 PROJECT CONTROL AND REPORTING 3-25
3.3.1 Governance 3-25
3.3.2 Status Reports 3-26
3.4 ADDITIONAL SERVICE REQUIREMENTS 3-31
3.4.1 Emergency Preparedness 3-31
3.4.1.1 COOP Strategy 3-31
3.4.1.2 Essential Business Services addressed by COOP 3-32
3.4.1.3 Types of Events that Trigger the COOP 3-32
3.4.1.4 COOP Approach 3-33
3.4.2 Service Level Agreements 3-34
3.4.3 Service Catalog 3-35
3.4.4 Locations 3-37
3.4.5 Business and Technical Requirements 3-37
3.4.5.1 Program Management (A.1) 3-39
3.4.5.2 Data Center Architecture (A.2) 3-39
3.4.5.3 Technical Services (A.3) 3-40
3.4.5.4 Facility Management 3-40
3.4.5.5 Managed Hosting Services (A.5) 3-41
3.4.5.6 Capacity on Demand Services (A.6) 3-41
3.4.5.7 Transition Services (A.7) 3-42
3.4.6 Contract Requirements - Small Diverse Business Participation (RFP IV-6 3-43
3.4.7 Proposed Services 3-45
3.4.8 Payment for Services 3-45
ATTACHMENT 3–1 — SCHEDULE B: GOVERNANCE 3-47
ATTACHMENT 3–2 — SCHEDULE C: SERVICE CATALOG 3-49
ATTACHMENT 3–3 — SCHEDULE D: TRANSITION MILESTONES 3-51
ATTACHMENT 3–4 – SCHEDULE E: DATA CENTER LOCATIONS 3-53
ATTACHMENT 3–5 — SCHEDULE F: STATEMENT OF WORK 3-55
ATTACHMENT 3–6 — SCHEDULE H: CCPM 3-57

ATTACHMENT 3–7 — SCHEDULE M: DETAILED TRANSITION PLAN 3-59
ATTACHMENT 3–8 — SCHEDULE K: KEY PROGRAM DELIVERABLES 3-61
ATTACHMENT 3–9 — SCHEDULE J.3: SERVICE LEVEL AGREEMENTS 3-63

"Over the past few years, I have seen a rapid change in focus from individual technology and component management to integrated services and management. Using integrated service management, along with of ITIL V3 based processes and hybrid cloud services, IT organizations have improved capabilities to align IT usage and design with business requirements and strategic direction. By taking the integrated service management approach and selecting the technologies which meet the current requirements while providing the flexibility to adjust to future needs while maintaining the expected level of service delivery."

North America Lead Solution Architect
Global Managed Services

3. Work Plan (RFP Requirement II-3)

RFP	*Requirement*
II-3	*Work Plan. Describe in narrative form your technical plan for accomplishing the work. Use the task descriptions in Part IV of this RFP and Schedule F as your reference point. Modifications of the task descriptions are permitted; however, reasons for changes should be fully explained. Indicate the number of person hours allocated to each task. Include a Program Evaluation and Review Technique (PERT) or similar type display, time related, showing each event. If more than one approach is apparent, comment on why you chose this approach.*

This work plan presents the key steps we will take to transform the delivery of information technology to the Commonwealth. Our work plan implements a forward-looking vision of the Commonwealth requirements that shape how we will conduct ourselves and carry out our mission within the Commonwealth. This vision provides a roadmap for addressing the Commonwealth's enterprise-level technology transition, migration, and operations for the next decade. Many of the projects in this plan are not easy; they will test the resolve of our team and the Commonwealth as we move towards completion. However, we are extremely confident our plan is strong, our people are stronger, and the on-demand service delivery model will be successful.

What follows in this section is a detailed explanation of how we will accomplish transition of services, migration of infrastructure, operations and program management over the life of the project. As we have been guided by the RFP, this section responds to Part II, **Part IV,** and **Schedule F** task descriptions in our narrative, followed by related information contained in **Schedules C, E, F, H, J.3, K**, and **M**. Where appropriate, we will make references from the narrative text to information in these schedules.

We begin with a brief overview of the personnel responsible for the accomplishment of the work plan, their qualifications, and a discussion of the high-level summary timeline for the activities in the program. Then a narrative describing the specific tasks at a more detailed level follows this overview. We include a discussion of the program management we will employ on this program, followed by a narrative about the project's first phase—transition of services, which sets the stage for ongoing operations and management of the program in the steady state.

Following the transition services section, we discuss the migration for the hardware infrastructure, including achieving operational readiness and the actual data center moves.

We then discuss project governance, a key element for the program's success, followed by a discussion of the reporting we will provide to enable ongoing communications of the overall and individual areas of performance, issues, and risks.

Additional service requirements from the RFP, Part IV are then covered, including Emergency Preparedness, Service Level Agreements, the Enterprise Services Catalog, the locations for various program activities, and business and technical requirements. This section also includes additional acknowledgement of your conditions for using Small Diverse Businesses, authorization of any changes to the services provided, and conditions for payment.

3.1 Work Plan Overview

3.1.1 Unisys Team Qualifications

The team of Unisys, IBM, Deloitte, and our small business partners deliver more than 150 years of combined corporate experience working with the Commonwealth to deliver hardware infrastructure, system software, applications, and related services. No other team can deliver our depth, experience, and level of knowledge of agency applications and the supporting infrastructure.

Our People Are Our Strength

With experience gained in providing successful services under the existing Data PowerHouse (DPH) and Enterprise Data Center (EDC) contracts over the past 13 years, our team understands agency and multi-agency application interdependencies. For example, PSP's Criminal Law Enforcement Assist Network (CLEAN) system and that application system's interdependency on the availability of both JNET's gateway services and PennDOT's vehicle registration system. To properly support the Commonwealth's critical business ongoing and especially during a transition, the Commonwealth needs an experienced service provider and can ill afford a vendor that will be learning on the job.

Our people have Significant Transition Experience with the Commonwealth—this fact will facilitate success during the transition and significantly mitigates risk;

- *Our team is expert in the technology required to support your applications.*
- *Our experience delivers a solution design optimized to drive the performance, stability, and security of your applications.*

Since our team either invented or supplied most of the current infrastructure within the scope of this RFP, we are experts in the technology required to support your applications. Both our unique infrastructure experience and knowledge of the Commonwealth's business applications were leveraged to provide a solution design that is optimized to drive the performance, stability, and security of your business applications.

While other service providers will struggle to understand how to perform a successful migration of this size, we will use our combined experience and unique knowledge of Commonwealth applications to mitigate risk in all areas and successfully execute as we have in the past:

- Our transition strategy focuses intently on risk mitigation
- We clearly understand that transition requires moving your applications and data, not simply replacing hardware and shuffling people.

[redacted] Engagement Executive, will be leading the PMO and supporting [redacted] Transition Executive and [redacted] Sr. Enterprise Architect in the development and execution of the Work Plan. These three executives have extensive experience in defining, directing, and executing successful transitions, migrations, and steady state operations for large clients with complex outsourced infrastructure environments.

Ann thoroughly understands the Commonwealth's goals for the new Data Center Services contract. She has achieved success managing similar consolidation and Data Center compute services migration initiatives as Vice President of Technical Services at Cegedigm-Dendrite. Under her direction, the team had many successes, including designing and building a world-class data center from the ground up, then migrating dozens of customers to the center without disruption. The initiative's scope included consolidation of 3 data centers and 45 customer migrations. In 2008 and 2009, she oversaw the Commonwealth's major transformation and infrastructure consolidation initiative with the existing Unisys DPH contract extension. Ann has a deep and detailed knowledge of the DPH's current operations. She will leverage that knowledge in the planning and execution of the transition and migration to the new data center model we propose.

[redacted] comes to Unisys from Dell Services after serving as the Transition Manager for many and directly leading of its largest transitions and migrations. In January, Scott joined the Unisys Team locally and has worked closely with many on the DPH contract to understand the current relationship as well as chart the course for the Commonwealth's Data Center Consolidation effort. Understanding the importance of a successful transition, Unisys was willing to make this investment early. To properly migrate a project of this size, Unisys recognized the need for a dedicated and local Transition Manager and unlike our competition, Unisys did not want to wait to see if we would be awarded this business. He brings a strong background in Transition, Transformation, and Data Center Migration programs, including large hospital corporations as well as the hospitality industry. Scott also brings the unique understanding of how accounts need to execute and adjust to the

client's needs from his time as a client delivery executive serving clients in industries as diverse as steel, retail, publishing, telecommunications, and gaming. This experience, along with his skills in program and project management, provides a strong blend that will help the Unisys Team to succeed.

[redacted] joined Unisys in 2011, working primarily in Harrisburg and gaining an understanding of the current DPH environment, after working as a transition and transformation architect at IBM for 8 years. Bryan, who will also be based in Harrisburg, developed the initial rate card for our proposed Self-Provisioning Project for the Commonwealth and provided architecture support for the successful pilot conducted in 2012. He was instrumental in developing of the overall technical solution of our proposed compute services in response to this RFP. While at IBM, Bryan led the Transition and Transformation architectural team for the State of Georgia's data center migration plan, which included many of the computer services requested by the Commonwealth, including a centralized data center, common compute services architecture for the state, and well-planned application migrations to the central data center. Bryan also led the Transition and Transformation team in the migration and consolidation of a medium-sized telecommunications corporation from multiple data centers and service models to a single managed data center. Bryan's understanding of developing multitenant data center architectures and the impact of federal and state regulations will enable the Commonwealth to migrate to the Compute Services model while also maintaining the flexibility to meet individual agency requirements.

This is a brief introduction of our core team that developed the overall strategy for the program's Transition and Migration phases. They have worked closely with the architectural team to plan these critical phases of the project leading to steady state operations. They hold key management positions in the new ongoing organizational structure. Details on the Unisys key staff and our complete organization can be found in Section 5 Personnel.

3.1.2 Work Plan Description

The program activities have been designed in three primary parts or phases: (1) Transition, (2) Migration, and (3) Steady State Operations, which is expected to be achieved by Month 28 of the program schedule. The overall program is supported by a program management framework which includes detailed planning, effective communication, and status tracking. This section includes a high level narrative of our proposed work plan along with selected pictures of the detailed work plan which is included in Attachment 9 to Section 3.0 – Schedule M. This section also includes details on the Unisys methodology that was used to design our proposed program plan and will be used to refine it based on Commonwealth feedback.

Transition activities build the foundation that the steady state organization needs to function including development of the final organizational plan, the communications plan, the financial management plan, and the development of policies and procedures, which will govern and guide the program's steady state operation. This activity sets plans and executes the transition from the current steady state operations model to the new operating model.

Transition consists of projects and tasks that will be executed to support the implementation of the resources, processes, procedures, and tools required to effectively deliver steady state data center compute services to the Commonwealth. In other words, we will create the IT service management infrastructure to support the new environment's hardware and software infrastructure. Transition will be broken further into smaller projects such as Tools Implementation, Transition of Services, and Service Desk Implementation. Examples of these types of activities include the implementation of BMC's Remedy system, implementation of revisions to Service Management processes like change management, hiring and training of transition PMO staff, and knowledge transfer for implementation of Managed Services. In this phase, we will leverage our significant knowledge and broad experience with the Commonwealth to speed this process.

Migration activities focus on the relocation and provisioning of both the physical infrastructure and planned movement of applications to the target platforms. The re-envisioning of the current DPH, EDC, and incorporation of agencies currently outside the managed services contract will be planned, focused teams will be established to address each migration, and they will execute the individual actions required to accomplish the migration.

Migration will be comprised of activities that prepare the receiving data centers for the migration of applications, often called Infrastructure Readiness, as well as projects that will migrate applications and their data from Commonwealth Data Centers to Unisys facilities. The projects will be organized around migrating applications from each data center and be broken into manageable sizes. For example, the DPH Data Center will be broken into approximately nine smaller projects with scope based on inter-application dependencies, number of servers, and applications.

Transition Program Management activities consist of tasks that the Transition Program Office will execute to improve each project's performance in quality and performance to schedule. This will include tasks such as quality reviews; gathering and distribution of lessons learned, status meetings, and reports; and oversight of the project schedule rollup. Key attributes of these tasks are consistency, sharing, adjustments, and oversight.

As the incumbent vendor, Unisys will continue to provide outstanding service to the Commonwealth's mission-critical application infrastructure hosted in the DPH and staff augmentation services to the operations in the EDC until each location is fully transitioned to the new model. Our incumbency provides us with the uncommon ability to seed the transition and migration teams with knowledgeable resources who understand the

Commonwealth infrastructure, considerably reducing ramp-up time training staff on basic infrastructure support and each agency's priorities and nuances. It is during this time that we will accelerate our focus on reforming our organizational structure and work processes to meet the new model's changing requirements.

Once the transition activities conclude, **Steady State Operations** begins using the new operating model, which is developed during the Transition and Migration phases. Continuous Service Improvement activity commences during this phase providing opportunities to assess, design, and implement changes to the program processes to increase the value of the services to Commonwealth.

Table 3-1 below shows a projection of the work effort required to complete the transition by major activity.

Table 3-1. Transition Work Effort by Major Activity

Task Activity	Total Person Hours Allocated
Transition Project Management	42,705
Transition of Services	157,186
Tools Implementation Project	18,784
Infrastructure Readiness Project	45,869
Application Workload Migrations	56,998

The following Gantt chart shown in **Figure 3-2** provides a very high-level view of the timelines for the overall activities of this program.

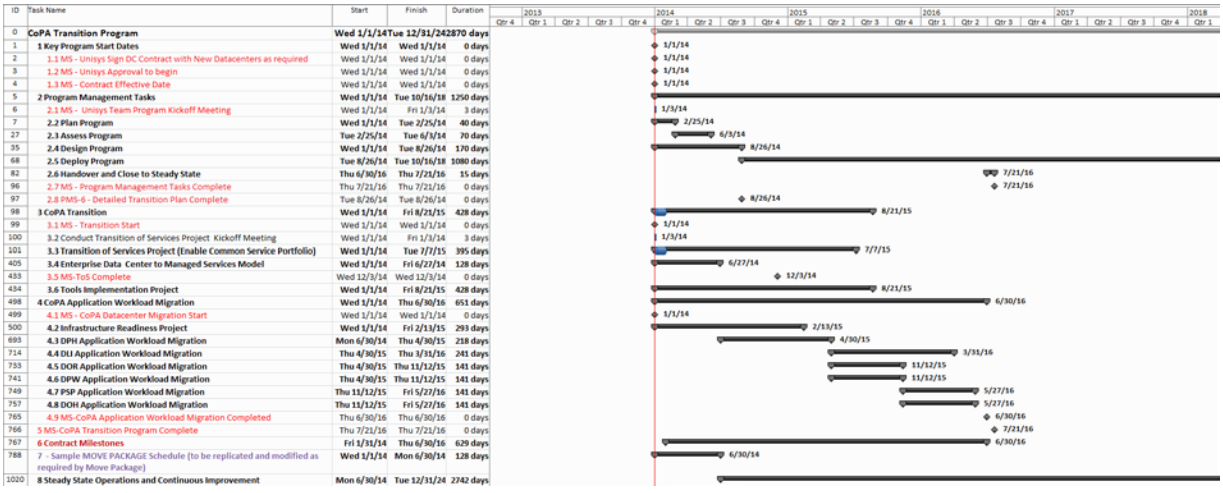


Figure 3-2. High-level Schedule of the Commonwealth's Transition Program

Transition Program Management Office – Project Start up

During **Month 1** of the program, much focus will be placed on program startup and long lead-time activities such as placing orders for the establishment of the telecommunications infrastructure. Executive planning sessions will be held to confirm a common understanding of scope, priorities, and timing. The Unisys Team will work with the Commonwealth to begin reviews and joint planning sessions for the Transition of Services, Tools Implementation, and Operational Readiness, which are critical to the EDC's transition to a Managed Services model. Unisys, IBM, and Deloitte are in the exceptional position to be able to leverage existing knowledge to expedite the turnover to the Unisys Team. Also, our account architecture team will create the architecture deliverables and review them with the Commonwealth to allow for long lead-time items such as circuits, core network equipment and storage, x86, AIX, and mainframe 'seed' equipment to be ordered.

During **Month 1** we bring key personnel on board to support the new contract starting with our Engagement Executive, [redacted] our Transition Executive, [redacted] our second Transition Manager, [redacted] and our Senior Enterprise Infrastructure Architect, [redacted] We will backfill positions currently held by Ann and Dave on the DPH contract. This team will lead all aspects of the transition efforts. We will also bring on our Service Excellence Officer, [redacted] to build our Service Excellence Office that will initially reform workflows of existing ITIL V3-aligned processes to meet the new services model requirements.

Transition Assessment and Data Gathering

Months 2 and 3 will contain many design and data gathering activities. We will begin the Tools Implementation tasks. The data center migration teams will begin analyzing the data collected from the BMC Atrium Discovery and Dependency Mapping (ADDM) tool to create move packages. Move Packages are defined as a group of dependent applications and data across several infrastructure components. We will conduct initial planning sessions with the Commonwealth stakeholders to solidify the order and timing of data center migrations. During this period, our key personnel will acclimate, and our Transition Program Management Office (TPMO) will be taking shape. As we move into Month 2, a team will begin detailed planning on the EDC's transition to quickly facilitate the transition to the Managed Services model.

It is also during **Months 2 and 3** that our executive leadership will work with Commonwealth executive leadership to solidify our approach to governance, communication, and reporting for steady state ongoing services, which will begin from the day an application is migrated to a Unisys Data Center, or workload in the EDC transitions to the managed services model. As dates are assigned to move packages, we will finalize the specific staff transition timeline for moving existing staff with Commonwealth knowledge to the new contract and we will start infusing our teams on both sides with new resources from IBM, Deloitte, and our SDB partners. We will on-board our Agency Account

Managers to acclimate the agencies to the changes in procedure and the support organization between the existing contract and the new model.

Transition Program Development – Process/Tool Refinement and Implementation

Many contract milestones will be completed in **Months 4 through 8.** To accomplish these milestones, we will complete the implementation and integration of the ITSM System with the Commonwealth ITSM system along with drafting of the CCPM. The ITIL V3 processes will be finalized and rolled out to the team. The Unisys Data Center core infrastructures will be installed, tested, and connected to COPANET, which will result in operational readiness. Toward the end of this period, the Data Center Migration Teams will begin detailed planning on the DPH migration to facilitate complete migration within 16 months. The Unisys Team will initiate training of the Commonwealth stakeholders that will cover many aspects of the contract, operational procedures, and review of strategy and plans aligned with program key deliverables.

At this time, the Unisys Team will complete the transition of the Enterprise Data Center from the current staff augmentation model to the new managed services model. Existing Unisys Team members augmented with additional staff will completely assume the site's management responsibilities. After the Enterprise Data Center is operating in the steady state, agencies with applications hosted in the EDC can order additional services through the Enterprise Services Catalog and change order processes, and the Unisys Team will be accountable for EDC Service Level Agreements (SLAs) under the new contract.

DPH Application Workload Migration

Months 9 through 16 will focus almost exclusively on planning and executing the DPH migration. To achieve this, Unisys, IBM, and the Commonwealth will work closely to plan the migration projects. The Unisys Team will be augmented with additional project management and technical resources that will perform migration tasks directly, or backfilling DPH team members who will be reassigned to provide a strong foundation of knowledge and experience to the DPH migration effort. The Commonwealth will verify the move packages that were identified by the Migration Team, develop and refine test plans for each application, and participate alongside the Unisys Team throughout the project to deliver a successful move. During this period, the Migration Team will put a strong communications strategy in place and plan to enable all stakeholders to have access to schedules and project plans. Unisys will develop a communications cadence of notifying affected users 30, 7, and again 2 days before any significant events such as re-IP events (if necessary) and move events.

Because the DPH will be migrated in at least nine separate move packages, an agency could have application infrastructure managed at the Willow Oak Data Center and the Unisys Data Center concurrently. As the migration move packages are relocated to the Unisys Data Center and the application infrastructure for each application is operating in the steady state, agencies with applications hosted in the Unisys Data Center can order

additional services through the Enterprise Services Catalog and Change Order processes, and the Unisys Team will be accountable for SLAs under the new contract. For all application infrastructures that remain at the Willow Oak Data Center, the Unisys Team will be accountable for SLAs under the current DPH contract until the infrastructure is relocated to the Unisys Data Center. By Month 16, the Unisys Team will complete the migration of the Data PowerHouse agency application infrastructure from the Willow Oak Data Center to the Unisys Data Centers.

At the end of **Month 16**, the DPH contract will officially expire, and all relevant staff supporting the existing DPH and EDC workloads will have transitioned to the new contract.

Unisys recognizes the importance of maintaining uninterrupted focus on the DPH migration due to its size, application interdependency complexity, and importance to the Commonwealth. With this in mind, no other migrations are planned during that time.

Agency Application Workload Migration – DLI, DPW, and DOR

As the DPH migrations are wrapping up in **Month 16,** the migration teams will turn their effort to the DLI, DPW, and DOR Data Centers in **Months 17 through 22.** DLI was chosen for the second wave of moves because of its size and complexity. The migration team is allowing up to 12 months for this move. IBM will take the lead on this migration because of its knowledge and experience with the Department of Labor & Industry (DLI). The Department of Revenue (DOR) is also included in this wave to avoid over allocation of DOR resources during its busy tax season. This wave also includes the Department of Public Welfare (DPW) Data Center.

Agency Application Workload Migration – PSP, DOH

In **Months 23 through 28,** the migration team will plan and relocate the applications within the Pennsylvania State Police (PSP) and Department of Health (DOH) Data Centers. Again, we took the time of year into account for the PSP Data Center migration. This wave is planned to begin in January 2016 and complete in June 2016, which will avoid busy summer and year-end holiday months.

As each agency application migration completes, the Unisys Team will officially assume responsibility for providing managed services to the agency from the Unisys Data Center, and when operational in steady state, the Unisys Team will be accountable for the achievement of service level commitments.

As Unisys and the Commonwealth conduct detailed Migration Planning beginning in Month 4, the order and combinations of data centers by wave may change as we continue to refine the planning and movement of the various agencies' infrastructure.

After transition and migration are complete, our fully populated steady state organization, processes and tools will be fully deployed and operating in the new environment. New

capabilities of capacity on demand, self provisioning, an expanded Service Desk capability, and ITIL V3 processes will be available and in use at this time. Further details of the transition from the current state to the new state of the Commonwealth's compute environment can be found in the following sections; a thorough discussion of the topic is provided in **Schedule M.**

3.2 Detailed Task Plan

The Unisys Work Plan is focused on the accomplishment of transition, migration, and steady state. Transition begins with a series of projects, tasks, and activities. Transition includes the required steps to implement a managed services model. Our Team will work closely to design and implement the processes, tools, and organizational structures required to deliver continuous services to the Commonwealth and stakeholders. The work products from these services will support the PMO and the rest of the team during execution of ongoing operations. A key element of the transition is transfer and implementation of the Unisys standard management toolset. This includes BMC Remedy ITSM, (Nagios) for monitoring, and BMC's Atrium Discovery and Dependence Mapping (ADDM) tool.

Our team will work with the Commonwealth to identify a technology refresh plan for existing hardware in the EDC during the EDC transition. Unisys will work with the Commonwealth to address a continuance of hardware maintenance until the infrastructure is replaced.

The daily TPMO operations will be tightly aligned with the PMO operations. [redacted] and her executive leadership team will drive effective handoffs of transition projects to the steady state. For transition architecture strategy and support, the TPMO will interface directly with the Senior Enterprise Infrastructure Architect, [redacted] and his team of Agency Infrastructure Architects.

Figure 3-3 shows the proposed Level 2 schedule for the Commonwealth's Transition Program.

ID	Task Name	Start	Finish	Duration
0	**CoPA Transition Program**	**1/1/14**	**12/31/24**	**2870 days**
1	**1 Key Program Start Dates**	**1/1/14**	**1/1/14**	**0 days**
2	1.1 MS - Unisys Sign DC Contract with New Datacenters as required	1/1/14	1/1/14	0 days
3	1.2 MS - Unisys Approval to begin	1/1/14	1/1/14	0 days
4	1.3 MS - Contract Effective Date	1/1/14	1/1/14	0 days
5	**2 Program Management Tasks**	**1/1/14**	**10/16/18**	**1250 days**
6	2.1 MS - Unisys Team Program Kickoff Meeting	1/1/14	1/3/14	3 days
7	**2.2 Plan Program**	**1/1/14**	**2/25/14**	**40 days**
27	**2.3 Assess Program**	**2/25/14**	**6/3/14**	**70 days**
35	**2.4 Design Program**	**1/1/14**	**8/26/14**	**170 days**
68	**2.5 Deploy Program**	**8/26/14**	**10/16/18**	**1080 days**
82	**2.6 Handover and Close to Steady State**	**6/30/16**	**7/21/16**	**15 days**
96	2.7 MS - Program Management Tasks Complete	7/21/16	7/21/16	0 days
97	2.8 PMS-6 - Detailed Transition Plan Complete	8/26/14	8/26/14	0 days
98	**3 CoPA Transition**	**1/1/14**	**7/17/15**	**403 days**
99	3.1 MS - Transition Start	1/1/14	1/1/14	0 days
100	3.2 Conduct Transition of Services Project Kickoff Meeting	1/1/14	1/3/14	3 days
101	**3.3 Transition of Services Project (Enable Common Service Portfolio)**	**1/1/14**	**3/27/15**	**323 days**
405	**3.4 Enterprise Data Center to Managed Services Model**	**1/1/14**	**6/27/14**	**128 days**
433	3.5 MS-ToS Complete	12/30/14	12/30/14	0 days
434	**3.6 Tools Implementation Project**	**1/1/14**	**7/17/15**	**403 days**
498	**4 CoPA Application Workload Migration**	**1/1/14**	**6/30/16**	**651 days**
499	4.1 MS - CoPA Datacenter Migration Start	1/1/14	1/1/14	0 days
500	**4.2 Infrastructure Readiness Project**	**1/1/14**	**2/13/15**	**293 days**
693	**4.3 DPH Application Workload Migration**	**6/30/14**	**4/30/15**	**218 days**
714	**4.4 DLI Application Workload Migration**	**4/30/15**	**3/31/16**	**241 days**
733	**4.5 DOR Application Workload Migration**	**4/30/15**	**10/27/15**	**128 days**
741	**4.6 DPW Application Workload Migration**	**4/30/15**	**10/27/15**	**128 days**
749	**4.7 PSP Application Workload Migration**	**10/27/15**	**4/24/16**	**129 days**
757	**4.8 DOH Application Workload Migration**	**10/27/15**	**4/24/16**	**129 days**
765	4.9 MS-CoPA Application Workload Migration Completed	6/30/16	6/30/16	0 days
766	5 MS-CoPA Transition Program Complete	7/21/16	7/21/16	0 days
767	**6 Contract Milestones**	**1/31/14**	**6/30/16**	**629 days**
768	6.1 CM-1 - Key Staffing Completed	1/31/14	1/31/14	0 days
769	6.2 CM-2 - Contract Management Plan	4/1/14	4/1/14	0 days
770	6.3 CM-3 - Staffing Completed	9/9/14	9/9/14	0 days
771	6.4 CM-4 - Data Center Architecture Complete	9/9/14	9/9/14	0 days
772	6.5 CM-5 - Data Gathering Completed	9/9/14	9/9/14	0 days
773	6.6 CM-6 - Detailed Transition Plan Completed	8/26/14	8/26/14	0 days
774	6.7 CM-7 - Commonwealth Compute Procs Manual (CCPM) Completed	6/17/14	6/17/14	0 days
775	6.8 CM-8 - Network Connectivity Completed	6/17/14	6/17/14	0 days
776	6.9 CM-9 - Security Arch, Soln, Policies and Procedures Completed	9/9/14	9/9/14	0 days
777	6.10 CM-10 - ITSM Systems Integration Completed	9/9/14	9/9/14	0 days
778	6.11 CM-11 - Financial Management Complete	9/9/14	9/9/14	0 days
779	6.12 CM-12 - Operational Readiness	12/2/14	12/2/14	0 days
780	6.13 CM-13 - SSAE 16 Audit of EDC Complete	12/3/14	12/3/14	0 days
781	6.14 CM-14 - DPH DCM Completed	6/30/15	6/30/15	0 days
782	6.15 CM-15 - EDC Transition Completed	12/30/14	12/30/14	0 days
783	6.16 CM-16 - L&I DCM Completed	6/30/16	6/30/16	0 days
784	6.17 CM-17 - DOR DCM Completed	6/30/16	6/30/16	0 days
785	6.18 CM-18 - PSP DCM Completed	6/30/16	6/30/16	0 days
786	6.19 CM-19 - DPW DCM Completed	6/30/16	6/30/16	0 days
787	6.20 CM-20 - DOH DCM Completed	6/30/16	6/30/16	0 days
788	7 - Sample MOVE PACKAGE Schedule (to be replicated and modified as required by Move Package)	**1/1/14**	**6/30/14**	**128 days**
789	7.1 DCM_MP - PLAN MIGRATION	**1/1/14**	**6/30/14**	**128 days**
915	7.2 DCM_MP - MIGRATION TO DC1	**1/28/14**	**4/3/14**	**46.75 days**
1020	**8 Steady State Operations and Continuous Improvement**	**6/30/14**	**12/31/24**	**2742 days**
1021	8.1 Operations Monitoring	6/30/14	12/31/24	2742 days
1022	8.2 Service Request Management	6/30/14	12/31/24	2742 days
1023	8.3 Disaster Recovery Testing	6/30/14	12/31/24	2742 days
1024	8.4 Security Testing	6/30/14	12/31/24	2742 days

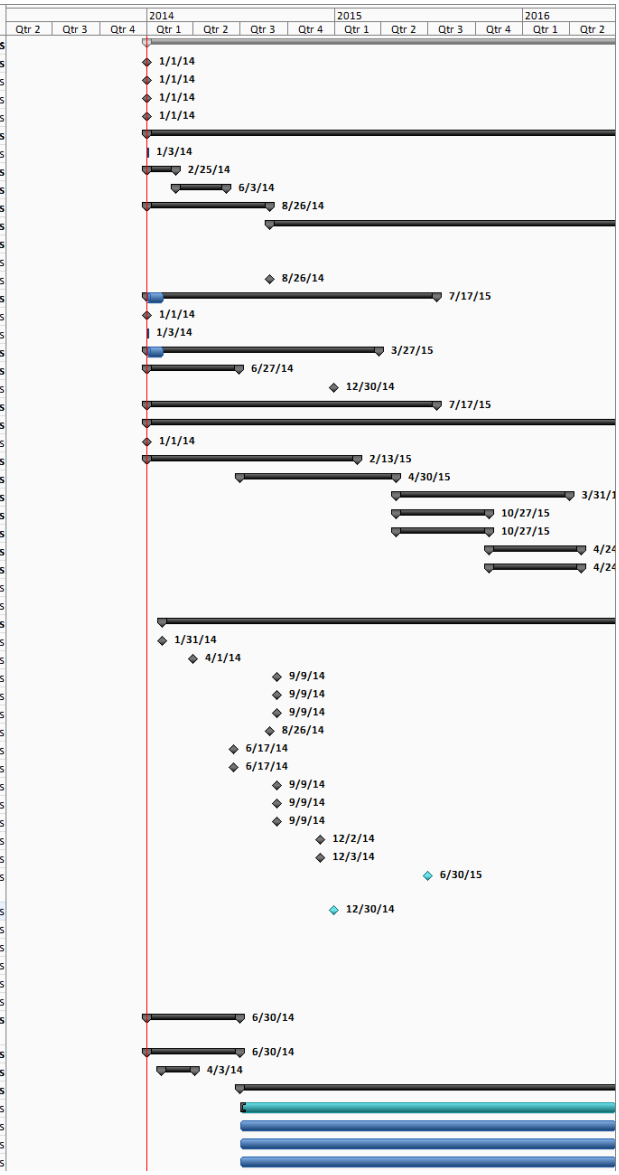


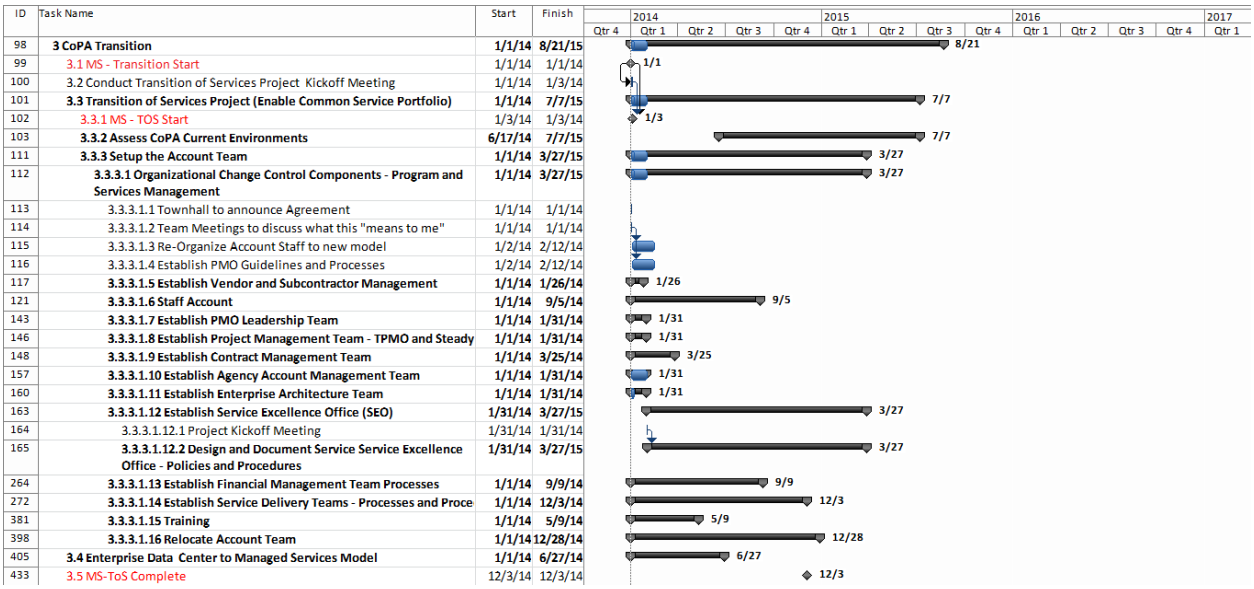
Figure 3-3. Level 2 Schedule of the Commonwealth's Transition Program

Our approach on transition timing was developed with the Commonwealth's goals in mind. Our initial focus is on transition of the EDC to a managed services model followed by data center migrations to move agency applications from the Willow Oak Data Center to a Unisys Data Center. These priorities will enable the Commonwealth to transition all obligations under the current DPH contract to the new data center compute services contract. In parallel, we are focusing on the accomplishment of key program deliverables within specified time frames. Remaining agency migrations will then take place between Months 17 and 28 with fewer constraints and priority than those for the DPH and EDC migrations.

3.2.1 Transition Services

Transition Services are the cornerstone of a successful relationship between the Commonwealth and the Unisys Team. In the Transition Services projects, tasks, and activities, the Commonwealth and the Unisys Team will work closely to design and implement the processes, tools, and organizations that are necessary to provide excellent services continuously to the Commonwealth and your stakeholders. The outputs from these services will assist the PMO and the rest of the entire team in executing the program's ongoing operations.

Among the important outcomes from the Transition Services projects will be deliverables such as the Commonwealth Computing Procedures Manual (CCPM), which will provide both the Commonwealth and the Unisys Team with a defined set of expectations. Along with the CCPM, these projects will establish the Program Management Office and the tools and processes they need to successfully deliver services to the Commonwealth. These tools and processes will include those that are needed to effectively support the ITIL V3 framework, provide the Commonwealth transparency into the billing, and establish the Service Desk. **Figure 3-4** below shows the Transition phase of the project.



ID	Task Name	Start	Finish
98	**3 CoPA Transition**	**1/1/14**	**8/21/15**
99	3.1 MS - Transition Start	1/1/14	1/1/14
100	3.2 Conduct Transition of Services Project Kickoff Meeting	1/1/14	1/3/14
101	**3.3 Transition of Services Project (Enable Common Service Portfolio)**	**1/1/14**	**7/7/15**
102	3.3.1 MS - TOS Start	1/3/14	1/3/14
103	**3.3.2 Assess CoPA Current Environments**	**6/17/14**	**7/7/15**
111	**3.3.3 Setup the Account Team**	**1/1/14**	**3/27/15**
112	**3.3.3.1 Organizational Change Control Components - Program and Services Management**	**1/1/14**	**3/27/15**
113	3.3.3.1.1 Townhall to announce Agreement	1/1/14	1/1/14
114	3.3.3.1.2 Team Meetings to discuss what this "means to me"	1/1/14	1/1/14
115	3.3.3.1.3 Re-Organize Account Staff to new model	1/2/14	2/12/14
116	3.3.3.1.4 Establish PMO Guidelines and Processes	1/2/14	2/12/14
117	**3.3.3.1.5 Establish Vendor and Subcontractor Management**	**1/1/14**	**1/26/14**
121	**3.3.3.1.6 Staff Account**	**1/1/14**	**9/5/14**
143	**3.3.3.1.7 Establish PMO Leadership Team**	**1/1/14**	**1/31/14**
146	**3.3.3.1.8 Establish Project Management Team - TPMO and Steady**	**1/1/14**	**1/31/14**
148	**3.3.3.1.9 Establish Contract Management Team**	**1/1/14**	**3/25/14**
157	**3.3.3.1.10 Establish Agency Account Management Team**	**1/1/14**	**1/31/14**
160	**3.3.3.1.11 Establish Enterprise Architecture Team**	**1/1/14**	**1/31/14**
163	**3.3.3.1.12 Establish Service Excellence Office (SEO)**	**1/31/14**	**3/27/15**
164	3.3.3.1.12.1 Project Kickoff Meeting	1/31/14	1/31/14
165	**3.3.3.1.12.2 Design and Document Service Service Excellence Office - Policies and Procedures**	**1/31/14**	**3/27/15**
264	**3.3.3.1.13 Establish Financial Management Team Processes**	**1/1/14**	**9/9/14**
272	**3.3.3.1.14 Establish Service Delivery Teams - Processes and Proce**	**1/1/14**	**12/3/14**
381	**3.3.3.1.15 Training**	**1/1/14**	**5/9/14**
398	**3.3.3.1.16 Relocate Account Team**	**1/1/14**	**12/28/14**
405	**3.4 Enterprise Data Center to Managed Services Model**	**1/1/14**	**6/27/14**
433	3.5 MS-ToS Complete	12/3/14	12/3/14

Figure 3-4. Initial Organization Set Up and EDC Transition

3.2.1.1 Account Organization

Unisys understands we are only as strong as our team. Early in the transition process, we will focus on training existing staff on changes brought on by the new contract; acquiring outstanding supplemental resources to deliver services; and providing the tools, processes, and work environment to enable them to be successful.

The activities for Account Organization will provide the framework to establish an effective Program Management Office.

3.2.1.1.1 Establish PMO Guidelines and Processes

Establishing the PMO guidelines and processes will include developing the interim Contract Management procedures as necessary, developing the vendor and Subcontractor Management policies and procedures, and modifying the existing Billing processes.

3.2.1.1.2 Organize Account Personnel

Organize Account Personnel will include tasks supporting talent acquisition and staff training, providing work space, and implementing standard work processes.

The Unisys Team identified individuals who will fill key positions as required by the Commonwealth. During these activities, Unisys will move individuals to these key roles by identifying and training them to assume the new roles. We will also identify other roles that are required early to lead organizations through the transition period.

Staffing plans for the technical and support teams will be reviewed and revised during the PMO's formation, including the PMO leadership team and the Project Management team, including the Transition Project Management team, the Enterprise Architecture team, and the Service Excellence team. Unisys will develop this plan to assign resources to the appropriate roles during the transition. We will engage Small Diverse Business partners to supply services and staffing requiring the establishment of processes for interaction among partners.

Contract, role, and industry-specific training will be planned and provided as appropriate to the staff as they move to their roles. This training includes CCPM, billing, Advanced ITIL V3, PMP, ITIL Foundation, and others as necessary. Unisys will partner with Harrisburg University to coordinate and deliver training.

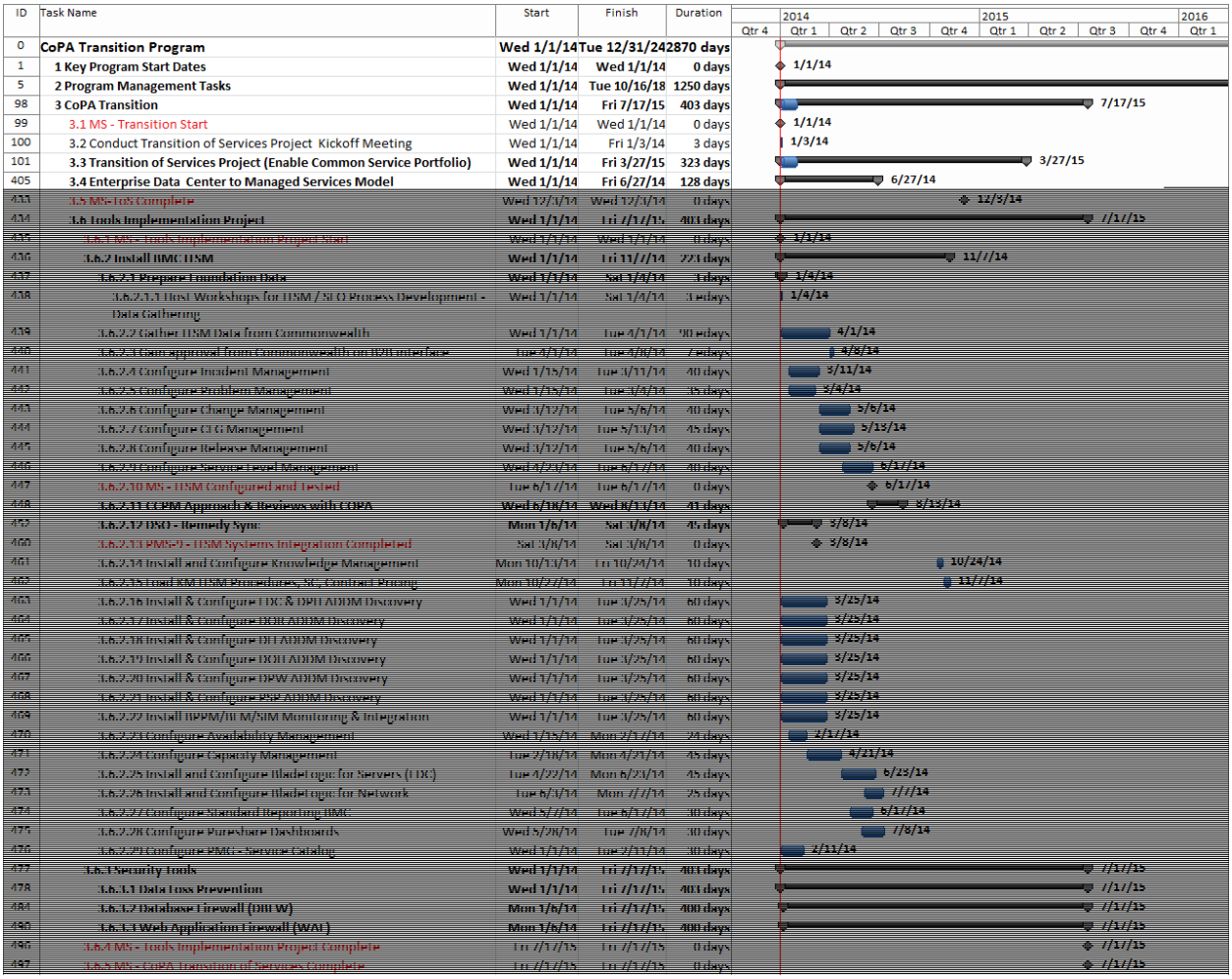
Establishment of the Service Excellence Office will enable and drive the reformation of existing ITIL V3 processes, the drafting of the Commonwealth Compute Procedures Manual, and the implementation of quality processes and policies.

3.2.1.2 Enterprise Data Center (EDC) to Managed Services Model

The EDC will transition to a Managed Services model. Key to this project is knowledge transfer and implementation of the Unisys standard management toolset. Unisys is uncommonly positioned to enable this transition quickly, using our current team that supports the EDC. This team is very knowledgeable of the Commonwealth's current environment, which will enable an expeditious knowledge transfer process. This project will depend on the implementation and customization of the BMC Remedy ITSM Toolset, Nagios for monitoring, and BMC's Atrium Discovery and Dependence Mapping (ADDM)

tool. During the EDC's transition, Unisys will work with the Commonwealth to identify a technology refresh plan for existing hardware in the EDC. Until the infrastructure is replaced, Unisys will work with the Commonwealth to include continuance of hardware maintenance.

3.2.1.3 Tools Implementation



ID	Task Name	Start	Finish	Duration
0	CoPA Transition Program	Wed 1/1/14	Tue 12/31/24	2870 days
1	1 Key Program Start Dates	Wed 1/1/14	Wed 1/1/14	0 days
5	2 Program Management Tasks	Wed 1/1/14	Tue 10/16/18	1250 days
98	3 CoPA Transition	Wed 1/1/14	Fri 7/17/15	403 days
99	3.1 MS - Transition Start	Wed 1/1/14	Wed 1/1/14	0 days
100	3.2 Conduct Transition of Services Project Kickoff Meeting	Wed 1/1/14	Fri 1/3/14	3 days
101	3.3 Transition of Services Project (Enable Common Service Portfolio)	Wed 1/1/14	Fri 3/27/15	323 days
405	3.4 Enterprise Data Center to Managed Services Model	Wed 1/1/14	Fri 6/27/14	128 days
433	3.5 MS - ITSM Complete	Wed 12/1/14	Wed 12/1/14	0 days
434	3.6 Tools Implementation Project	Wed 1/1/14	Fri 7/17/15	403 days
435	3.6.1 MS - Tools Implementation Project Start	Wed 1/1/14	Wed 1/1/14	0 days
436	3.6.2 Install BMC ITSM	Wed 1/1/14	Fri 11/7/14	221 days
437	3.6.2.1 Prepare Foundation Data	Wed 1/1/14	Sat 1/4/14	4 days
438	3.6.2.1.1 Host Workshops for ITSM / SLO Process Development - Data Gathering	Wed 1/1/14	Sat 1/4/14	4 days
439	3.6.2.2 Gather ITSM Data from Commonwealth	Wed 1/1/14	Tue 4/1/14	90 days
440	3.6.2.3 Gain approval from Commonwealth on ITSM interface	Tue 4/1/14	Tue 4/8/14	7 days
441	3.6.2.4 Configure Incident Management	Wed 1/15/14	Tue 3/11/14	40 days
442	3.6.2.5 Configure Problem Management	Wed 1/15/14	Tue 3/4/14	35 days
443	3.6.2.6 Configure Change Management	Wed 3/12/14	Tue 5/6/14	40 days
444	3.6.2.7 Configure CCB Management	Wed 3/12/14	Tue 5/13/14	45 days
445	3.6.2.8 Configure Release Management	Wed 3/12/14	Tue 5/6/14	40 days
446	3.6.2.9 Configure Service Level Management	Wed 4/23/14	Tue 6/17/14	40 days
447	3.6.2.10 MS - ITSM Configured and Tested	Tue 6/17/14	Tue 6/17/14	0 days
448	3.6.2.11 CCBM Approach & Reviews with COPA	Wed 6/18/14	Wed 8/13/14	41 days
452	3.6.2.12 DSO - Remedy Sync	Mon 1/6/14	Sat 3/8/14	45 days
460	3.6.2.13 MS - ITSM Systems Integration Completed	Sat 3/8/14	Sat 3/8/14	0 days
461	3.6.2.14 Install and Configure Knowledge Management	Mon 10/13/14	Fri 10/24/14	10 days
462	3.6.2.15 Load KM ITSM Procedures, SC, Context Proces	Mon 10/27/14	Fri 11/7/14	10 days
463	3.6.2.16 Install & Configure TDC & DPH ADDM Discovery	Wed 1/1/14	Tue 3/25/14	60 days
464	3.6.2.17 Install & Configure DOH ADDM Discovery	Wed 1/1/14	Tue 3/25/14	60 days
465	3.6.2.18 Install & Configure DT ADDM Discovery	Wed 1/1/14	Tue 3/25/14	60 days
466	3.6.2.19 Install & Configure DOH ADDM Discovery	Wed 1/1/14	Tue 3/25/14	60 days
467	3.6.2.20 Install & Configure DPW ADDM Discovery	Wed 1/1/14	Tue 3/25/14	60 days
468	3.6.2.21 Install & Configure PSP ADDM Discovery	Wed 1/1/14	Tue 3/25/14	60 days
469	3.6.2.22 Install BPPM/BI M/SIM Monitoring & Integration	Wed 1/1/14	Tue 3/25/14	60 days
470	3.6.2.23 Configure Availability Management	Wed 1/15/14	Mon 2/17/14	24 days
471	3.6.2.24 Configure Capacity Management	Tue 2/18/14	Mon 4/21/14	45 days
472	3.6.2.25 Install and Configure BladeLogic for Servers (DC)	Tue 4/22/14	Mon 6/23/14	45 days
473	3.6.2.26 Install and Configure BladeLogic for Network	Tue 6/3/14	Mon 7/7/14	25 days
474	3.6.2.27 Configure Standard Reporting BMC	Wed 5/7/14	Tue 6/17/14	30 days
475	3.6.2.28 Configure PureShare Dashboards	Wed 5/28/14	Tue 7/8/14	30 days
476	3.6.2.29 Configure PMG - Service Catalog	Wed 1/1/14	Tue 2/11/14	30 days
477	3.6.3 Security Tools	Wed 1/1/14	Fri 7/17/15	403 days
478	3.6.3.1 Data Loss Prevention	Wed 1/1/14	Fri 7/17/15	403 days
484	3.6.3.2 Database Firewall (DBFW)	Mon 1/6/14	Fri 7/17/15	400 days
490	3.6.3.3 Web Application Firewall (WAF)	Mon 1/6/14	Fri 7/17/15	400 days
496	3.6.4 MS - Tools Implementation Project Complete	Fri 7/17/15	Fri 7/17/15	0 days
497	3.6.5 MS - CoPA Transition of Services Complete	Fri 7/17/15	Fri 7/17/15	0 days

Figure 3-5. Tools Implementation Project Activities and Timeline

Unisys developed a technical architecture to support a multi-data center environment, network and security, and data center support architecture. The tools implementation project (**Figure 3–5**) is the precursor and basis for many other activities in the transition of services. Unisys will implement tools such as BMC's Remedy Suite for ITSM, PMG for Services Catalog and billing data, SolarWinds and Nagios for monitoring, BladeLogic for provisioning, and PureShare for dashboards along with other tools to form the architecture, which will be wrapped by processes and performed by Unisys, IBM, and

Deloitte. The PMG Services Catalog is unique in the industry because it provides an active service catalog and workflow that can begin at the customer's request. Much of the industry focuses the service catalog on self-provisioning and other IT tasks. The Real-time Dashboard is also unique because it provides an active CIO dashboard that can be set up with much of the report data while also sharing the data at the right level of detail for a variety of management levels and uses.

3.2.2 Application Workload Migrations

At Unisys, we believe the term Data Center Migration is a misnomer. The focus is and should be on the applications. The processes the team will follow require much input and participation from the Commonwealth application owners. Automated tools such as ADDM alongside traditional tools are used to minimize the dependency on customer input and maximize accuracy. Each migration project will last about 3 months. On the project, technical teams and applications teams will work closely to define the exact scope, plan tasks, identify risks, develop solutions, and identify optimum times for outages that will minimize the impact on the end users. In the 3-month project, much of the effort is spent on planning, verifying, and re-planning, all with the goal of a successful migration.

But before any applications can be moved, the receiving data center must be made operationally ready. This includes implementing the infrastructure components required to meet or exceed the service levels required.

3.2.2.1 Operational Readiness

ID	Task Name	Start	Finish	Duration
607	**4.2.3 Data Center Buildout**	**1/1/14**	**2/13/15**	**293 days**
608	**4.2.3.1 DC1 - Buildout - MP0**	**1/1/14**	**2/13/15**	**293 days**
609	4.2.3.1.1 MS - Begin DC1 - Buildout	1/1/14	1/1/14	0 days
610	**4.2.3.1.2 DC1 - Network Buildout**	**1/1/14**	**10/10/14**	**203 days**
625	**4.2.3.1.3 DC1 - Storage Buildout**	**10/10/14**	**1/30/15**	**80 days**
632	**4.2.3.1.4 DC1 - x86 Buildout**	**10/10/14**	**2/13/15**	**90 days**
640	4.2.3.1.5 DC1 - Backup Buildout	10/10/14	11/24/14	45 edays
641	4.2.3.1.6 DC1 - IBM MF Buildout	10/10/14	11/24/14	45 edays
642	4.2.3.1.7 DC1 - AIX Buildout	10/10/14	11/24/14	45 edays
643	4.2.3.1.8 DC1 - Monitoring Buildout	10/10/14	11/24/14	45 edays
644	4.2.3.1.9 Initiate SSAE 16 Audit for DC1	8/12/14	8/12/14	0 days
645	4.2.3.1.10 Execute SSAE 16 Audit for DC1	8/13/14	12/2/14	4 mons
646	4.2.3.1.11 MS - DC1 - Buildout - MP0 - COMPLETED	2/13/15	2/13/15	0 days
647	**4.2.3.2 DC2 - Buildout - MP0**	**1/1/14**	**5/16/14**	**97 days**
648	4.2.3.2.1 MS - Begin DC2 - Buildout	1/1/14	1/1/14	0 days
649	**4.2.3.2.2 DC2 - Network Buildout**	**1/1/14**	**5/16/14**	**97 days**
664	**4.2.3.2.3 DC2 - Storage Buildout**	**1/1/14**	**4/23/14**	**80 days**
671	**4.2.3.2.4 DC2 - x86 Buildout**	**1/1/14**	**5/7/14**	**90 days**
679	4.2.3.2.5 DC2 - Backup Buildout	1/1/14	2/15/14	45 edays
680	4.2.3.2.6 DC2 - IBM MF Buildout	1/1/14	2/15/14	45 edays
681	4.2.3.2.7 DC2 - AIX Buildout	1/1/14	2/15/14	45 edays
682	4.2.3.2.8 DC2 - Monitoring Buildout	1/1/14	2/15/14	45 edays
683	4.2.3.2.9 Initiate SSAE 16 Audit for DC2	1/1/14	1/1/14	0 days
684	4.2.3.2.10 Execute SSAE 16 Audit for DC2	1/1/14	4/22/14	4 mons
685	4.2.3.2.11 MS - DC2 - Buildout - MP0 - COMPLETED	5/16/14	5/16/14	0 days

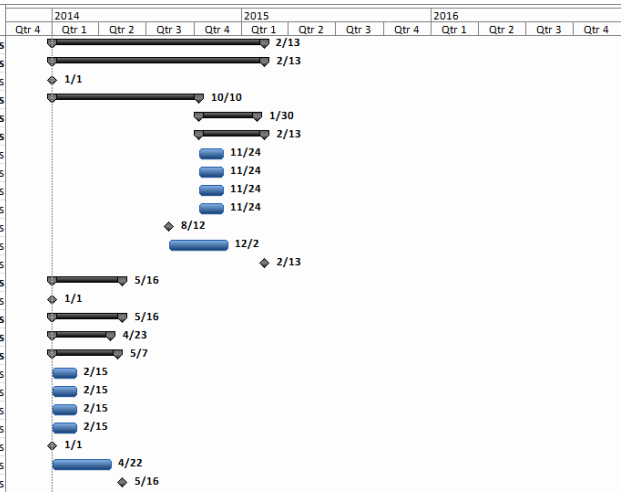
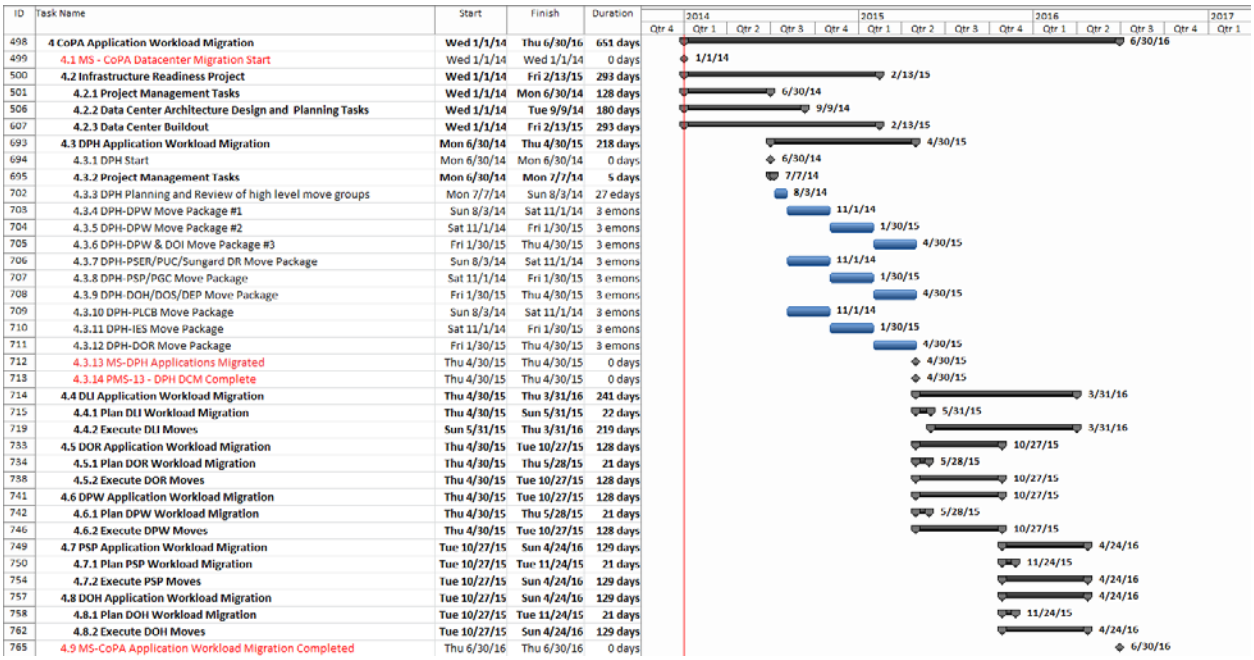


Figure 3-6. Operational Readiness Timeline

To achieve operational readiness, the data center must be prepared by connecting the data center to COPANET and have a local area network designed, built, tested and operational, including data security devices such as firewalls and intrusion detection and prevention.

Tools such as Remedy by BMC must be installed and operational to support ITIL V3 processes for incident, problem, change, release, asset, configuration, and service level management. Supporting tools such as PMG for billing and service catalog, ADDM for automated discovery, BladeLogic for provisioning and automated patching, PureShare for dashboards, and Nagios for monitoring must also be operational. Infrastructure such as storage, virtual servers, physical servers, monitoring, and backup must be in place. Operational Readiness activities and timeline are shown in **Figure 3–6.**

3.2.2.2 Agency Application Workload Migrations



ID	Task Name	Start	Finish	Duration
498	**4 CoPA Application Workload Migration**	**Wed 1/1/14**	**Thu 6/30/16**	**651 days**
499	4.1 MS - CoPA Datacenter Migration Start	Wed 1/1/14	Wed 1/1/14	0 days
500	**4.2 Infrastructure Readiness Project**	**Wed 1/1/14**	**Fri 2/13/15**	**293 days**
501	**4.2.1 Project Management Tasks**	**Wed 1/1/14**	**Mon 6/30/14**	**128 days**
506	**4.2.2 Data Center Architecture Design and Planning Tasks**	**Wed 1/1/14**	**Tue 9/9/14**	**180 days**
607	**4.2.3 Data Center Buildout**	**Wed 1/1/14**	**Fri 2/13/15**	**293 days**
693	**4.3 DPH Application Workload Migration**	**Mon 6/30/14**	**Thu 4/30/15**	**218 days**
694	4.3.1 DPH Start	Mon 6/30/14	Mon 6/30/14	0 days
695	**4.3.2 Project Management Tasks**	**Mon 6/30/14**	**Mon 7/7/14**	**5 days**
702	4.3.3 DPH Planning and Review of high level move groups	Mon 7/7/14	Sun 8/3/14	27 edays
703	4.3.4 DPH-DPW Move Package #1	Sun 8/3/14	Sat 11/1/14	3 emons
704	4.3.5 DPH-DPW Move Package #2	Sat 11/1/14	Fri 1/30/15	3 emons
705	4.3.6 DPH-DPW & DOI Move Package #3	Fri 1/30/15	Thu 4/30/15	3 emons
706	4.3.7 DPH-PSER/PUC/Sungard DR Move Package	Sun 8/3/14	Sat 11/1/14	3 emons
707	4.3.8 DPH-PSP/PGC Move Package	Sat 11/1/14	Fri 1/30/15	3 emons
708	4.3.9 DPH-DOH/DOS/DEP Move Package	Fri 1/30/15	Thu 4/30/15	3 emons
709	4.3.10 DPH-PLCB Move Package	Sun 8/3/14	Sat 11/1/14	3 emons
710	4.3.11 DPH-IES Move Package	Sat 11/1/14	Fri 1/30/15	3 emons
711	4.3.12 DPH-DOR Move Package	Fri 1/30/15	Thu 4/30/15	3 emons
712	4.3.13 MS-DPH Applications Migrated	Thu 4/30/15	Thu 4/30/15	0 days
713	4.3.14 PMS-13 - DPH DCM Complete	Thu 4/30/15	Thu 4/30/15	0 days
714	**4.4 DLI Application Workload Migration**	**Thu 4/30/15**	**Thu 3/31/16**	**241 days**
715	**4.4.1 Plan DLI Workload Migration**	**Thu 4/30/15**	**Sun 5/31/15**	**22 days**
719	**4.4.2 Execute DLI Moves**	**Sun 5/31/15**	**Thu 3/31/16**	**219 days**
733	**4.5 DOR Application Workload Migration**	**Thu 4/30/15**	**Tue 10/27/15**	**128 days**
734	**4.5.1 Plan DOR Workload Migration**	**Thu 4/30/15**	**Thu 5/28/15**	**21 days**
738	**4.5.2 Execute DOR Moves**	**Thu 4/30/15**	**Tue 10/27/15**	**128 days**
741	**4.6 DPW Application Workload Migration**	**Thu 4/30/15**	**Tue 10/27/15**	**128 days**
742	**4.6.1 Plan DPW Workload Migration**	**Thu 4/30/15**	**Thu 5/28/15**	**21 days**
746	**4.6.2 Execute DPW Moves**	**Thu 4/30/15**	**Tue 10/27/15**	**128 days**
749	**4.7 PSP Application Workload Migration**	**Tue 10/27/15**	**Sun 4/24/16**	**129 days**
750	**4.7.1 Plan PSP Workload Migration**	**Tue 10/27/15**	**Tue 11/24/15**	**21 days**
754	**4.7.2 Execute PSP Moves**	**Tue 10/27/15**	**Sun 4/24/16**	**129 days**
757	**4.8 DOH Application Workload Migration**	**Tue 10/27/15**	**Sun 4/24/16**	**129 days**
758	**4.8.1 Plan DOH Workload Migration**	**Tue 10/27/15**	**Tue 11/24/15**	**21 days**
762	**4.8.2 Execute DOH Moves**	**Tue 10/27/15**	**Sun 4/24/16**	**129 days**
765	4.9 MS-CoPA Application Workload Migration Completed	Thu 6/30/16	Thu 6/30/16	0 days

Figure 3-7. Agency Application Workload Phased Migrations

The application workloads supported in the agency data centers are planned to be moved in three phases, as shown in **Figure 3–7.** The first phase is focused on the Data PowerHouse Data Center; the second will be the Department of Labor & Industry, Department of Public Welfare, and Department of Revenue. Application workloads supported in the Pennsylvania State Police and Department of Health data centers will move last in the third and final phase. Unisys determined the order of agency migrations based on lower periods of activities, but also recognize that due to in-flight projects and other activities, these priorities may change. Each of these agency data centers will be divided into multiple projects based on size, complexity, and number of applications. Each project includes a similar set of tasks including documenting the application scope and supporting infrastructure, determining the move strategy for each component, such as "over the wire" or "lift-n-shift", and order of application migrations. This activity is

followed by detailed planning; identification of hardware in the receiving data center; remediation of hardcoded IP addresses in the application; test plan creation; data transfer, which will be planned to avoid peak work periods, and finally testing.

The Unisys plan includes over-the-wire transfer of data and when appropriate, operating systems and applications. This approach will minimize risk that may occur during reinstallation activities by using the current operating system and application setting and minimize outages by synchronizing periodically throughout the weeks leading to the migrating events, and can be more easily scheduled around peak work times for the agencies.

Each plan will include notifications to Commonwealth stakeholders 30, 7, and 2 days before events. Application owners will be expected to verify each application successfully migrated through appropriate testing activity.

3.2.3 Transition Program Management

The activities in the Transition Program Management section of the program schedule will predominantly be executed and overseen by the Transition Executive or one of the Deputy Transition Executives. This section includes tasks such as Program Executive Kickoff, Executive Planning Sessions, and other activities aimed at developing and strengthening agreement and like-mindedness among the Commonwealth and the Unisys Team. Items such as goals and objectives for each project will be shared and discussed, development/refinement of guiding principles, setting priorities between time, resources and quality. A consistent program cadence for status communications, risk and issues reviews and mitigation strategies will be developed. The Transition Program Management Office (TPMO) and governance structure will enable individuals filling important roles in the program such as the Commonwealth's Transition Executive and staff to quickly collaborate from the start with an organized and standardized approach.

The TPMO will be tightly aligned with the PMO executives; [redacted] and her executive leadership team promote effective handoffs of transition projects to the steady state. For transition architecture strategy and support, the TPMO will interface directly with the Senior Enterprise Infrastructure Architect, [redacted] and his team of Agency Infrastructure Architects.

3.2.4 Steady State

The steady state organization is the culmination of many months of hard work on behalf of the Unisys Team and the Commonwealth in joint collaboration to reach a common goal. It is the endgame, and it does not look at all like it does today. How does it look to you as a Commonwealth leader? How will you navigate the new processes and procedures to meet your business IT needs? How will you know that your IT infrastructure is in good hands and supporting the business the way it should be?

The year is 2016, the date is April 15th, and you have the typical anxiety that tax day brings on to the average American, but it is a little worse for you because you are the CIO of the Department of Revenue, and this is your heaviest processing day of the year. First thing that morning, you log on to your secure workstation and click on the link to your Real-time Dashboard. The tax systems running on the mainframe and the Integrated Tax System hosted on the SAP environment are showing heavy activity but performing optimally with enough headroom to make it through the rest of this important day.

You recall the meeting you and your team had last quarter with your Unisys Agency Account Manager, Agency Infrastructure Architect, and Capacity Planning Manager. That quarterly Capacity Planning Meeting provided the forum to walk through the performance of the systems and capacity averages and peaks over the previous year. It was clear during the meeting that based on Unisys projections, last quarter's capacity would never carry you through the processing peak expected in April. The Unisys Team recommended taking advantage of the Capacity on Demand service to get through this processing peak.

At a user friendly interface, the Agency IT Manager signed into the Enterprise Services Catalog and requested the additional server capacity in March to allow time for your application team to prepare the additional servers for peak processing. It was as simple as selecting several servers with standardized processing and memory capacity to support the expected load generated by last-minute taxpayers. Through self-provisioning, the capacity was made available within a few days, after you approved the request in the Enterprise Services Catalog, and turned over to your application team. This capacity can be leveraged for the time needed, and you plan to remove it from service at the end of May. Pennsylvania agencies can save thousands of dollars by judiciously using IT resources in a model in which they pay only for resources used.

The new steady state operations are collaborative, proactive, efficient, and cost-effective. The narrative that follows outlines several of the new operating model's benefits.

Contract Management

In the steady state, ordering services will be a lot different than it is in the DPH today. Agencies have multiple options on how to proceed with acquisition of resources needed to support their application infrastructure. The Unisys Enterprise Services Catalog contains thousands of items that an agency can select at an online interface with preconfigured approval workflows. Selection of additional capacity from the Enterprise Services Catalog is as simple as purchasing items on the Amazon Web site. Through the automation built into the Enterprise Services Catalog contract services schedule and exhibit information will be updated automatically.

For more custom solutions, agencies can still use the Enterprise Services Catalog to place an order for a custom solution to be architected by their Agency Infrastructure Architect, and ultimately purchased through the Enterprise Services Catalog. Through automated

billing and chargeback systems, Unisys Contract Management can easily track projects against federal funding streams for the agencies as needed.

Innovative Service Offerings

Unlike the fixed-price DPH contract, the new service model offers Capacity on Demand capabilities with consumption-based pricing models. Often, a Commonwealth agency user has the capability to log on to the Enterprise Services Catalog, request resources, and provision the servers from his or her own desktop. When the servers are no longer needed, the user can return to the same portal to request decommission of the servers. Under this service offering, the agency is charged only for resources available during the period, at least 1 month.

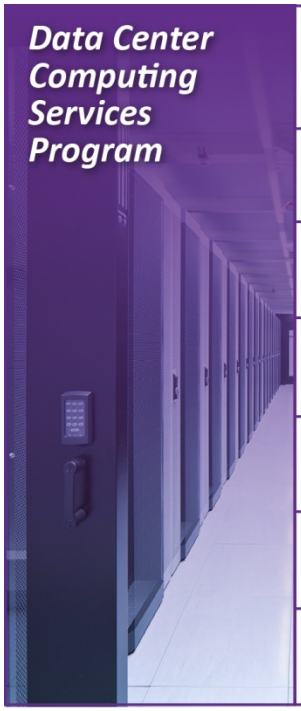
Operational Transparency

In the new world, Commonwealth leaders at all levels have access to a Real-time Dashboard that provides a view into the performance of services and applications being monitored by the Unisys Team at that time, outstanding service requests and incident tickets, upcoming changes to the environment, SLA status, and current customer satisfaction levels. The dashboard is a one-stop shop for agency status information.

How We Organize the Team

Details on the organization structure and functions can be found in **Section 5.0, Personnel.** At a high level, our team is organized into seven core functions, including the overall Program Management Office that includes the organization's executive layer and supporting personnel; the Agency Account Management team that provides liaison services to every agency using the Data Center Compute Services; the Service Delivery organization that is the core team providing infrastructure management services; the Transition Program Management Office that oversees transition and migration initiatives as well as steady state project management; the Service Excellence Office that oversees all ITIL V3-aligned processes, innovation, and customer satisfaction; the Enterprise Architecture team that develops and manages the technology management program for the services delivered; and the Security Office that oversees all aspects of the project to confirm compliance with security standards and requirements.

Figure 3-8 provides a high-level description of the functions of each of our seven core teams.



Program Management Office: Oversees all facets of the engagement. Provides oversight and management of the contract, financial functions, third-party software administration, and subcontract management. Responsible for detailed management of service level agreements and credits.
Account Management: Facilitates understanding of leveraging the contract to meet agency needs. Acts as the liaison and develops strategic relationships with agency leaders. Keeps agencies abreast of new technology. Handles pricing discussions.
Service Delivery: Provides all technology and service support functions, including data center operations, service desk, system administration, mainframe services, database administration, and network and security management.
Service Excellence Office: Includes all ITILV3 process management functions, customer satisfaction program management, reporting, and capacity planning. Confirms smooth execution of compliant processes. Analyzes and reports trends and corrective actions.
Enterprise Architecture: Provides overall development and management of technology strategy. Responsible for engineering of detailed data center services design at the agency level. Verifies currency of the service catalog offerings.
Transition/Project Management Office: Provides technical expertise and leadership during the transition from current state data center services through to steady state data center management services.
Chief Security Office: Oversees all aspects of the project to maintain compliance with security standards and requirements. Develops policies and performs periodic audits of processes and data to confirm compliance.

CoPA-187r4

Figure 3-8. Data Center Compute Services Program

Agency-Centric Staffing Approach

We understand that each agency is a unique and distinct customer of our services; therefore, a key to success is putting the agency at the center of our staffing model. Our model will enable the Commonwealth to realize savings from economy of scale without losing the personalized focus on the agencies that could be lost if a model aligned with technology domains was implemented. We give you the best of both worlds.

From the agency's perspective, a server is more than a box, and storage is more than just disks inside a frame. Outages to these devices can have a major impact on the functioning of an agency's application, and ultimately a negative effect on Commonwealth citizens. The alignment of our agency-centric model facilitates accountability at the agency and application level, in contrast with many outsourcing providers that structure their people and services around technology components without regard for the customer and applications supported. In those models, you are just a number.

There are six of these teams in the overall program, each providing personalized services to a subset of agencies participating in the program. Our model in **Figure 3-12** includes a three person leadership team for every Agency-Centric Team: an Agency Account Manager who manages the relationship with each agency supported and all aspects of the contract; an Agency Infrastructure Architect who manages the Technology Strategy for assigned agencies; and the Service Delivery Manager who is responsible for end-to-end delivery performance and direct oversees the management of all technicians aligned with the

agencies supported by the team. Most important, all our team members are aligned with the agency at the center of the model.

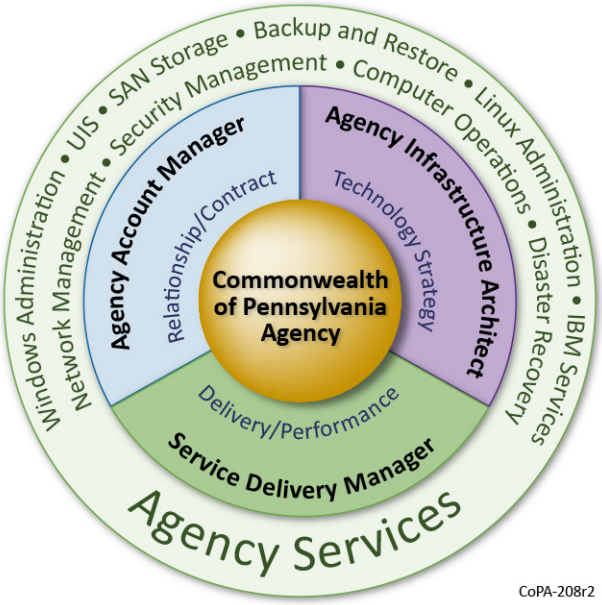


Figure 3-9. Agency-centric Service Delivery Team Structure

Governance

Strong governance and effective communication are cornerstones to an effective program. The established model promotes communications at all levels of the organization across every agency and the Office of Administration. Details on the governance program can be found in **Attachment 1 to Section 3.0 - Schedule B**.

The governance structure will be developed early in collaboration with the Commonwealth. Unisys recommends three levels of governing steering committees that convene regularly to address various aspects of the program. This structure will facilitate accountability for service levels; meeting the contract's requirements; and enable key stakeholders from the Commonwealth and the Unisys Team to jointly set the program's overall direction.

Communication

Details on how we interact with the Commonwealth staff can be found in Section 5.8, Interface with the Commonwealth. Organized, centralized, and targeted communication is essential to the success of a program of this magnitude. Our team will be located mainly in Harrisburg, close to the locations of Commonwealth agencies that will be using the services to facilitate effective communication and collaboration.

After working with the Commonwealth for many years, we understand that it is not as simple as one Unisys point of contact to a single Commonwealth counterpart. The Commonwealth organization is multidimensional; each agency has its own management structure and IT support team, and the Office of Administration manages the contract on behalf of the agencies. Our model effectively supports this organization.

In today's DPH organization, communication can flow to and from many directions, depending on the topic and the urgency. Formalization and centralization of the flow of communication from the Commonwealth workforce to the Unisys Team through the Unisys Service Desk will greatly simplify interactions and documentation of requests and issues in our connected ITSM systems that will provide ITIL V3 process compliance with every request.

The Commonwealth workforce has multiple options for communicating requests and reporting issues to the Unisys Team. They can call the Service Desk, which will receive requests from Commonwealth agencies, document them in the ITSM system, and assign requests to the Unisys Team. Alternatively, the Commonwealth workforce can enter a request directly into the Commonwealth's ITSM system, and the request will be replicated in the Unisys ITSM system. The Service Desk monitors the queues and will confirm that these requests are assigned to the Unisys Team, thus providing end-to-end support.

The Knowledge Management Portal is a new addition to our service offering. This portal will provide the Commonwealth and the Unisys Team with access to documentation and procedures used to provide services. It will serve as a repository for many aspects of the program, including the CCPM, Frequently Asked Questions, and Runbooks.

Quality

In the steady state, the Unisys Team will operate following disciplined processes that are tailored to promote an optimized workflow and ITIL V3 conformance. The Service Excellence Office (SEO) process management team consists of key leaders and executives with advanced ITIL V3 certification and education on Six Sigma methodologies who will work directly with Commonwealth Process Managers to provide compliance, proper documentation, timely approvals, and participation on joint Advisory Boards.

The quality of our services will be measured by performance metrics, and equally important in our rigorous Customer Satisfaction Management Program that takes your pulse from many perspectives, including Service Desk interactions, Agency Satisfaction Surveys, Executive OA leadership interactions, and more intensive satisfaction improvement initiatives as needed.

Continual Service Improvement and Innovation Program (CSIIP)

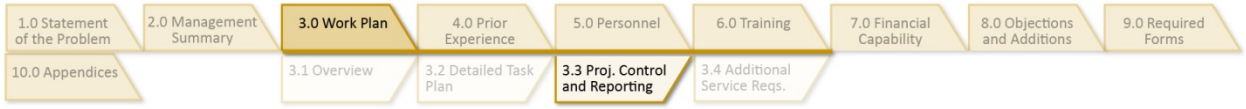
Through our Continual Service Improvement and Innovation Program (CSIIP), Unisys will provide a standard framework for aligning our improvement focus with your strategic

priorities. At the agency level, you will participate in CSIIP workshops to create an ongoing, formal program that encourages the proactive identification and introduction of measurable improvements in a specific work area or work process and to introduce "innovation in context" to those areas. One of this program's major features is the ability to consolidate and analyze the many inputs required to effectively develop an innovation and improvement plan.

The CSIIP process uses a structured approach to gathering and analyzing important factors to build a comprehensive roadmap to cover remediation, improvement, and innovation opportunities. This will provide the Commonwealth with the necessary information to make informed decisions based on relative cost/benefit, alignment with strategy, and return on investment for various actions, of varying scale from incremental through to truly breakthrough.

Our Enterprise Architect Team will host Innovation Workshops regularly to facilitate open communication and brainstorming the use of technology solutions to solve today's business challenges facing agency CIOs.

3.3 Project Control and Reporting



Successful management and control of a large project or program relies heavily on project controls and effective reporting. This section addresses two main components of governance and status reporting during transition and through the steady state of operations.

3.3.1 Governance

The Governance Strategy defined in Attachment 1 to Section 3.0 **Schedule B**, **Governance** presents a review of the overall approach to governance throughout transition and steady state phases of the project.

3.3.2 Status Reports

RFP Req	Requirement
IV-5.B	*Status Reports. Monthly progress reports covering activities, problems, risks and recommendations. This report should be keyed to the work plan the Offeror developed in its proposal, as amended or approved by the Issuing Office. During the Transition period of this project additional progress reports are required.* *Monthly Service Level, Change Management, Incident/Problem, Operational, and Billing Reports are to be provided. These reports will be developed in cooperation with the Commonwealth during the early stages of the engagement.*

Unisys has standard status and problem identification reports for managing transition activities and projects, ongoing requested projects, and operational ITSM processes. We recommend the reports below and will work with the Commonwealth during transition to review each report and make any adjustments or additions required to manage the contract's status reporting.

Unisys will provide the Commonwealth with two types of status reports:

- Monthly progress reports for transition activities and projects based on project management disciplines:
  - Risk Management
  - Scope Management
  - Quality Management
  - Time Management
  - Cost Management
  - Procurement Management
  - Integration Management
- IT Service Management (ITSM) status reports for critical processes, including:
  - Service Level Management
  - Change Management
  - Incident Management
  - Problem Management
  - Operations Management
  - Financial Billing Management.

Project Management Status Reporting

The Unisys SDF project management method employs a comprehensive set of reporting procedures as a crucial activity on every project. This approach to reporting requires early, frequent, and regular face-to-face and written reports with the Commonwealth agency Project Manager or PMO and as-needed reporting to project stakeholders and Commonwealth project team members.

The basis of these reporting procedures is factored on the following reporting principles:

- Reporting is essential to communicate accurate and timely project information
- Reporting mitigates project risk through early discovery of potential problems or issues
- Reporting is essential to managing expectations for the solution and its impact on stakeholders
- Reporting increases awareness of the project's overall status among all stakeholders
- Reporting improves the timing of the delivery of information between project phases so that interested parties all have the same understanding of the project's deliverables, tasks, and business rules
- Reporting creates goodwill and cooperation among the interested parties, thereby improving trust
- Reporting builds an internal commitment to realizing the business benefits of the operational and technological improvement opportunities for Commonwealth agencies and all the key stakeholders.

Reporting may be provided in a variety of formats from formal written reports to informal e-mail and voicemail. **Table 3-10** provides a standard set of **Status and Problem Identification Reporting** methods that Unisys recommends. We will review them with Commonwealth agencies and tailor or amend them to provide the Commonwealth with the desired reporting types and formats. Standard reports in the table below that indicate availability in an online repository will be available on the reports portal.

Table 3-10. Unisys Recommended Project Reporting

Method	Type of Information	Vehicle	Frequency	Responsible	Comments
Weekly Project Status Report	Executive summary; status of priority items, including activities delays, and disruptions; status of the action items in the project repository; identification of meeting cancellations and impacts; status of the project schedule	Report posted in an online Project Repository	Weekly	Unisys Project Manager	Priority items will change over time and be determined by the Commonwealth and Unisys Project Managers.
Issues and Action Items Report	Open issues and action items, responsible parties, scheduled dates, and impacts	Report posted in an online Project Repository	Weekly	Unisys Team	Final format to be determined by the Commonwealth and Unisys
Risk Register Report	Risk-related items identified, rated, and tracked with probabilities, mitigation strategies, and expected outcomes and recommendations Excel spreadsheet	Report posted in an online Project Repository	Weekly	Unisys Team	Unisys standard register format; final format to be determined by the Commonwealth and Unisys
Project Schedule	Current project schedule	Schedule posted in an online Project Repository	Weekly	Unisys Team	In Microsoft Project
Problem Identification Reports	Identifies problem areas describing each problem and its impact on the overall project and affected tasks and remediation options,	Report posted in an online Project Repository	As needed	Unisys Team	

IT Service Management Reporting

Unisys delivers operational ITSM reports to analyze and summarize service-affecting defect drivers and that provide data to help manage process improvement plans. Inputs are collected reactively from closed Incident, Problem, Change, Asset, and Configuration Management and Service Level Management data, as well as the Unisys Service Desk and Commonwealth management survey data, and proactively from performance and monitoring tools that scan and monitor the in-scope infrastructure and applications.

Weekly and monthly reports provide visibility to defect percentages and trends as well as an overall baseline of quality. These reports enable precise action for targeted defects and provide an overall, highly measurable perspective on quality.

Unisys will configure the reporting system for the Commonwealth to deliver the detailed and summary reports required for day-to-day operations and measuring overall performance. The reporting system is based on Remedy Analytics, PureShare Dashboard, and the standard reporting solution for our implementation of ITSM. Our implementation of analytics and dashboards provides standard best practice reports, ad hoc reporting capabilities, drill-down capabilities, and a consolidated dashboard view for overall service management. We will leverage this standard Unisys solution in creating our proposed solution.

Unisys will use Nagios, SolarWinds BMC ProactiveNet, and Performance Management (BPPM) to provide performance reporting. We will provide standard and ad hoc reporting for the in-scope infrastructure and application monitoring, which will be provided as views to the Commonwealth personnel for informational purposes. Unisys will provide the Commonwealth with monthly summary-level reports on the reports portal. The Commonwealth standard ITSM reports are included in **Table 3-11.**

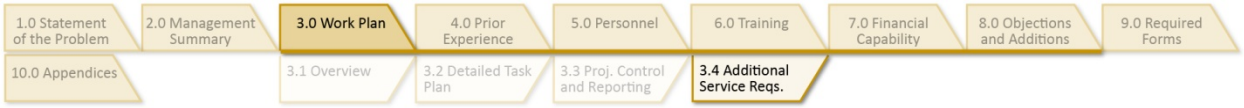
Table 3-11. Standard ITSM Reports

Report Category	Standard Reports
Asset/Configuration Standard Reporting	Software License Compliance Compliance Summary for Software Products Configuration Item Costs Lease Payments and Expiration Ongoing Payments to vendors Asset Aging Inventory Profile CI Relationship Profile Scorecard Analysis Business Service Supported by a CI CMDB reconciliation analysis Discovered data staleness report Services profile
Change Management Standard Reporting	Forward Schedule of Change Emergency Changes Report Change Backlog Report Open Changes by Status Changes that Spawned Incidents Changes that Spawned other Changes Changes Requests Backed Out Change Lifecycle and Process Efficiency Open Changes by Phase Change Rejected by CAB Planned Unavailability by Change

Report Category	Standard Reports
	Change Lead Time Report Change Backlog Report Change Bypass Process Report Change Trend Report Change Reason Report
Incident Management Standard Reporting	Number of Incidents by Status Incident Volume Trend Report Open Incidents Aging Report Incident Resolution Time Analysis Number of Incidents by Impact Number of Incidents opened by Operations Percentage of Incidents reopened Backlog of Unresolved Incidents Top Requestor Departments Top Requestor Sites Number of Incidents by Reported Source Number of Incidents by Product Category Number of Incidents with Status of Pending SLA Performance Summary Response Time Metric Report Metrics Scorecard Incident Trend Report Top 10 Resolvers Group Report
Problem Management Standard Reporting	Number of Problems by Status Percent of Re-occurring Problems by Impact MTTR for a Problem Average Time lag for Problem Resolution and closure Percent of Problems with a RCA Number of Opened Problem by Investigation Drivers Aging of Open Problems Number of Problems by CI Ratio of Problems to Incidents Number of Problems with High Priority Incidents
Service Request Management	Top 10 requested services Most requested services by location Historical demand analysis All Services Requests by category Open Service Request by category Top 10 Service Request Assignee Groups Top 10 Services that met SLAs Top 10 Services that missed SLAs SLA Report Summary Service Request Charges to Departments
Service Level Management Reports	Monthly SLA Reports by SLA Service Levels for Critical Measurement and Key Measurement items Recurring Deliverables Transition Milestones

Report Category	Standard Reports
Operational Reports	Backup/recovery, availability, and performance reports for: • Facility • Server Processing • Storage Subsystems • Network • Security • Services
Billing Reports	IBM SmartCloud Cost Management Reporting: • Monthly Crosstab Charges Report • Summary Crosstab Charges Report • Summary Crosstab Usage Report • Account Total Usage Report • Percentage Report • Invoice by Account Level Report • Top Usage Reports • Top 10 Pie Chart Report • Trend Reports

3.4 Additional Service Requirements



The Commonwealth noted a number of ancillary requirements for inclusion in the Work Plan that were not addressed in the Work Plan narrative, including topics such as Emergency Preparedness, Office Location, and Business and Technical Requirements. These are addressed in the following sub sections.

3.4.1 Emergency Preparedness

3.4.1.1 COOP Strategy

RFP	*Requirement*
	F. Emergency Preparedness. *To support continuity of operations during an emergency, including a pandemic, the Commonwealth needs a strategy for maintaining operations for an extended period of time. One part of this strategy is to ensure that essential contracts that provide critical business services to the Commonwealth have planned for such an emergency and put contingencies in place to provide needed goods and services.* *1. Describe Offeror anticipates such a crisis will impact its operations.* *2. Describe Offeror's emergency response continuity of operations plan. Please attach a copy of the plan, or at a minimum, summarize how the plan addresses the following aspects of pandemic preparedness:*

a) *Employee training (describe Offeror's training plan, and how frequently it plan will be shared with employees)*
b) *Identified essential business functions and key employees (within Offeror's organization) necessary to carry them out*
c) *Contingency plans for:*
   i.) *How Offeror will handle staffing issues when a portion of key employees are incapacitated due to illness.*
   ii.) *How Offeror employees will carry out the essential functions if contagion control measures prevent them from coming to the primary workplace.*
d) *How Offeror will communicate with staff and suppliers when primary communications systems are overloaded or otherwise fail, including key contacts, chain of communications (including suppliers), etc.*
e) *How and when Offeror's emergency plan will be tested, and if the plan will be tested by a third-party.*

The Commonwealth benefits from a Continuity of Operations (COOP) strategy, which is guided by an umbrella policy based on the ISO 22301-2003 business continuity standard. This strategy, combined with a multiple data center technical design to accommodate rapid recovery of systems and applications, addresses platform redundancy, continuity of shared infrastructure, disaster recovery for business application platforms, plans to address non-technical events such as inclement weather and pandemic threats, and staffing models in the event that human resources are unavailable.

3.4.1.2 Essential Business Services addressed by COOP

For this proposal, essential business services are identified as any service dependent on vendor-managed technology whose interruption would be detrimental to the Commonwealth's citizens or the goods and services they rely on from state government. Examples would include any technology platform that supports human health and welfare (DPW), safety and law enforcement (PSP), or transportation services (DOT).

3.4.1.3 Types of Events that Trigger the COOP

The Commonwealth will benefit from Unisys active management of potential continuity events, including:

- Pandemics
- Inclement weather and other natural disasters
- Data center power outages
- Emergency changes
- Security breaches
- Shared platform outages (host, network, or storage)
- Individual system failures
- Staff shortages.

Technical and logistical planning will alleviate outages to the managed service, and there is no anticipation these events will disrupt essential business functions. The COOP plan will call for regular exercises to address existing and emerging threats.

3.4.1.4 COOP Approach

Unisys will take great care in planning and implementing preventive measures to maintain the safety and security of our people, equipment, and the data that is maintained in the service center. With all these preventive measures, the service center must still plan for the "worst case" disaster. Planning for the worst case enables lesser disruptions to be adequately covered. Good planning as well as training and testing are the keys to a successful plan.

Recovery Concepts

A disaster is defined as any unplanned continuity event that renders a site or critical part of the managed service inoperable or inaccessible. The disaster's source may be:

- **Natural:** Such as flood, tornado, hurricane, or lightning
- **Human:** Such as sabotage accidental damage
- **Technical:** Such as mechanical failure hardware malfunctions

Regardless of the disaster's source, the recovery process is composed of the following major phases:

- Vital Record Protection
- Emergency Call Escalation
- Initial Damage Assessment
- Disaster Declaration
- Contingency Processing Procedures
- Primary Site Restoration.

3.4.1.4.1 Employee COOP training

Arrangements can be made for annual COOP desktop exercises together with the Commonwealth's Continuity of Government (CoG) Office, and agency DR tests will publish on the shared Services Portal. The COOP for Commonwealth Data Center services will be addressed in annual security training and each time a platform or application recovery test is conducted.

3.4.1.4.2 COOP for Illness

During a pandemic or an illness affecting many staff, Unisys will arrange for our global human resource function to backfill positions as needed with like-for-like personnel and cross-train staff members in primary and backup functions to provide staff continuity. Other options for staff continuity will be the use of trusted partners such as IBM, Deloitte, and a variety of Small Diverse Businesses familiar with outsourced data operations. Secure remote access will also comprise a major part of our planning for staff shortages to hinder the spread of disease or illness.

3.4.1.4.3 COOP for Contagion Control Measures

During a contagion event that prevents staff from working from their primary workplace, we will provide secure, two-factor remote connectivity for full-time and contractor personnel and test it periodically. Also, we will engineer redundant data center connectivity if staff cannot work in the primary facility. When necessary, we will provide hands-on personnel with respirators and other contagion prevention methods to allow staff to perform duties requiring physical access to the data center.

3.4.1.4.4 COOP for Communication Systems Anomalies

During a failure of normal communication of the COOP plan by shared portal or e-mail, we will use a combination of global Internet infrastructure, data center redundancy, mobile phone network, remote access capabilities, unified communications, and COOP training to address command and control center contingencies with its staff, contractors, and suppliers.

3.4.1.4.5 COOP Testing

Unisys will perform periodic COOP exercises audited by a third-party at a set interval and design them to test facility infrastructure between exercises to identify and avoid single points of failure in our managed services platform. Normal monthly maintenance of key infrastructure components such as water, power, cooling, and ventilation will test the continuity plan's physical aspects. We will address the plan's human components through awareness training, platform recovery tests, evacuation drills, and the use of planned failover to redundant infrastructure as appropriate.

3.4.2 Service Level Agreements

Unisys understands and supports the need for multiple SLA tiers to provide a flexible compute environment that optimizes the cost of computing. Furthermore, we understand the importance of measuring application availability.

Equally important, we understand the need to implement a quality office to drive continuous improvement efforts; we will establish a Service Excellence Office that drives

continued value and cost savings by deploying Six Sigma Lean practices based on studying cycle time and defect analysis from events that are extracted from the IT Service Management platform.

The Unisys proposed solution provides a common collection point and presentation for SLA data at our Services Portal described throughout our responses to **Schedule F,** Section 3.2.1 subsections.

Within **Attachment 7 to Section 3 - Schedule J.3: Service Level Agreements,** Unisys describes how the detailed input for the SLA measurements is collected, calculated, and presented. Many of the collection or calculation methods will require collaboration with the Commonwealth during transition.

3.4.3 Service Catalog

RFP	*Requirement*
IV-3.D	*Service Catalog* *The Offeror must complete Schedule C - Services Catalog as part of its technical submittal.* *a. DO NOT INCUDE ANY PRICING INFORMATION WITHIN THIS SCHEDULE*

Unisys provides an Enterprise Services Catalog, which will enable the Commonwealth to maintain services and have the flexibility to request additional services as needed to support changing business needs, business cycles, and new technologies.

The services in the Enterprise Services Catalog can be ordered within the tool. Each of these services will be processed as a Service Request and a solution developed. Some of these services are available to be automatically provisioned by the Enterprise Services Catalog tool. Our Enterprise Services Catalog is made up of the following sections:

1. **Catalog of Services**: The catalog is a copy of **Schedule I, Catalog of Services** but without the pricing.
2. **Description of Services**: This section describes each of the services listed in the Catalog of Services, including the service name; description of the service; units available to be ordered; specific customers if there are limitations, prerequisites, or co-requisites to support the service; activity to request the service; and the terms of use, which can include available services levels for the service.
3. The description of services is set up with the following sections:
   a. Fully Managed Services
   b. Managed Only Services
   c. Co-Location Services

d. Additional Technical Services (Per Hour)

e. Additional Technical Services (Technology Services).

The Unisys Enterprise Services Catalog in **Attachment 2 to Section 3 - Schedule C: Services Catalog** represents entries that are explicitly called out by the Commonwealth's RFP **Schedule I,** and many suggested by the RFP's other documents include **Schedule F** and the exhibits. Unisys experience with the Commonwealth for the past 13 years has been called on to augment these entries to enrich the choices to the Enterprise Services Catalog suggested by the RFP.

The Enterprise Services Catalog describes the specific entries shown, including related Enterprise Services Catalog items that will be needed to put a selection into its proper context. For example, the selection of a Gold Windows physical server will require the inclusion of an additional, identical server to provide the infrastructure capable of meeting the SLA. Similar instances exist throughout the Enterprise Services Catalog and are described. These dependencies are noted in each item's definition.

The Commonwealth's Enterprise Services Catalog will be accessible from the Unisys Services Portal and support user-based authentication and privileges along with support for associating agency and project-level accounting for each requested item. If the Commonwealth advises Unisys that a request may move directly to ordering or provisioning, the Enterprise Services Catalog tool may trigger automated ordering and deployment of the request. If change management must include approvals and scheduling, the Enterprise Services Catalog tool interfaces with the ITSM environment to participate in the process and gain the approvals and privilege necessary to trigger automated or staff processes to put the requests into motion.

The Enterprise Services Catalog in **Attachment 2 to Section 3 - Schedule C: Services Catalog** includes a rich selection of logical IT resources from servers and storage to networking. There is also a set of physical components such as racks, cages, and technical staff services available from the Enterprise Services Catalog. Ultimately, this wide selection is expandable. Unisys anticipates that transition will point out other IT services and resources that may be needed or helpful to the Commonwealth. Unisys is ready to enlarge and augment the Enterprise Services Catalog as quickly and responsively as the Commonwealth shows need.

The Enterprise Services Catalog is further defined and described in **Attachment 2 to Section 3 - Schedule C: Services Catalog.**

3.4.4 Locations

RFP	Requirement
IV-3.B	*Office Location.* *The selected Offeror must maintain an office in the Harrisburg, PA area during the term of the contract. If the selected Offeror does not currently have an office in the Harrisburg, PA area, it must establish an office within two (2) months of award of the contract.*

Unisys maintains an office in the Harrisburg area to support our current Commonwealth contracts. Since most of our resources are already local to Harrisburg, Unisys will continue to maintain a major presence within the Harrisburg area to support the services and relationship with the Commonwealth. The Commonwealth will benefit from local access to the Unisys account management and transition project management teams as well as space for combined Unisys and Commonwealth meetings. The Unisys Team's Service Desk, Operations, and local services support will also use this office.

Unisys will also maintain an office at each data center to provide local support functions. These functions will include hardware checkout support and tape management operations.

3.4.5 Business and Technical Requirements

RFP	Requirement
IV-3.A	*Business and Technical Requirements.* *The business and technical requirements are detailed in Schedule F of this RFP.*

As shown in **Figure 3-12** the Commonwealth's infrastructure environment has a diverse set of service management and technical requirements supporting the Commonwealth's applications and their related business activities and needs. By applying an integrated approach of people, processes, and technologies, Unisys will provide data center infrastructure management services that cover the requirements the Commonwealth describes in **Schedule F** and enables the Commonwealth to benefit from the delivery of consistent and transparent technical services, a detailed data center migration program, and the flexibility to adjust to changing business needs.

The work plan described in **Schedule F** covers the program and service management functions, technical services, and transition planning services to support the Commonwealth's needs with transparency, flexibility, and quality.

By establishing an integrated service management architecture for IT Services Management (ITSM) and Enterprise System Management (ESM) based on ITIL V3 and other industry best practices, the Commonwealth will gain visibility into the overall

management of the infrastructure services from initial requesting of the service through project implementation and into ongoing operations. The Unisys integrated service management platform is based on three technology areas operating in a common set of processes. The Services Portal provides access to the online service management portal, Enterprise Services Catalog, and online operational dashboard and other reporting information. The ITSM platform supports tracking for changes, incidents, problems and assets, the configuration management database, SLA management, and workflow-based automation. The ESM platform provides the event monitoring and correlation as well as the infrastructure management for the managed services.

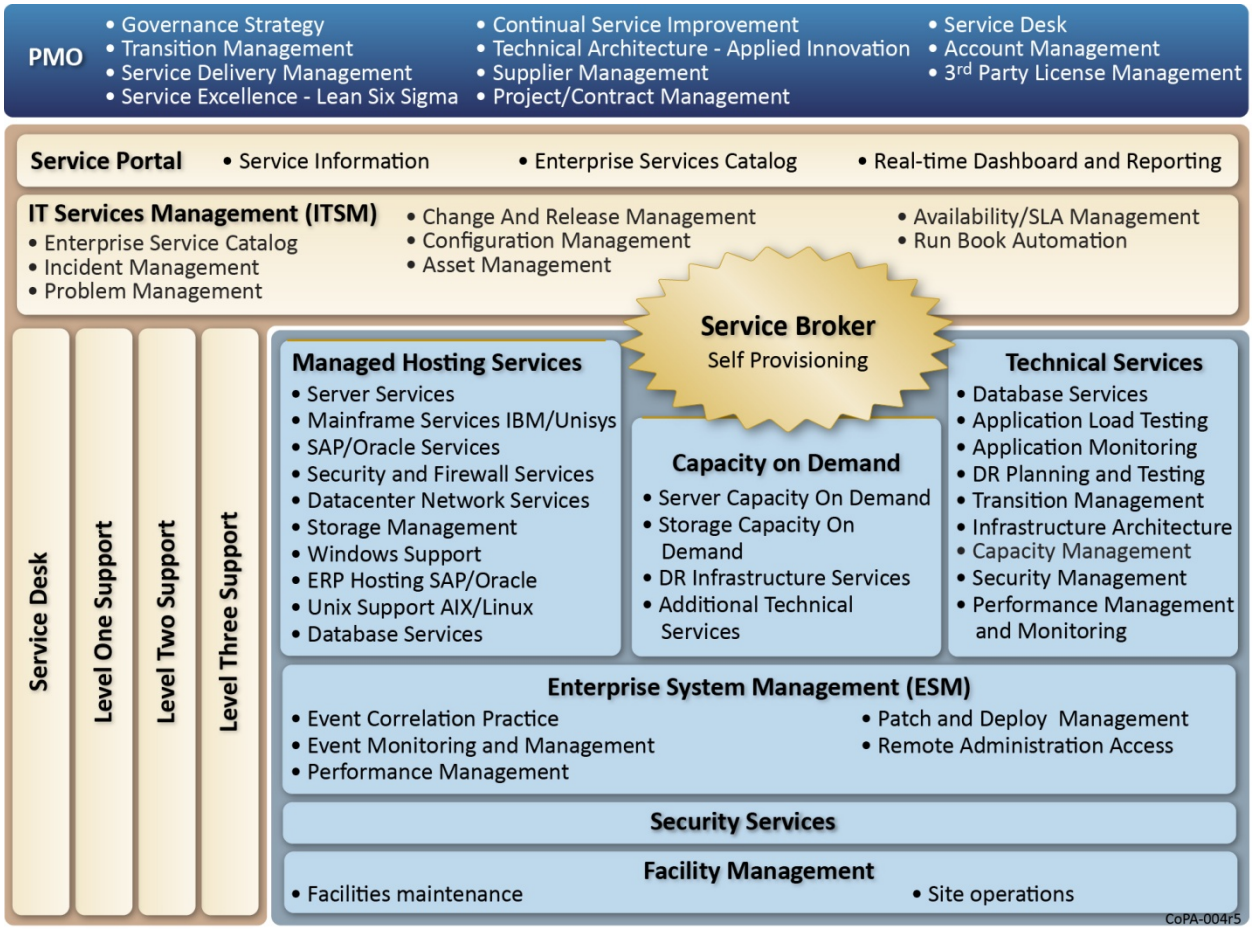


Figure 3-12. Unisys Service Management Model. *Using an integrated service management model as the foundation to provide the Commonwealth's managed infrastructure services.*

3.4.5.1 Program Management (A.1)

The Unisys Program Management Office (PMO) is the management team and primary interface for service delivery, projects, escalation, reporting, and billing. Our PMO supports and oversees account governance, transition management, continual improvement through service excellence, applied innovation through service and technology architecture, and management of the contract and suppliers.

The functional responsibilities for this team will be outlined in the technical solutions document in Schedule F, Section 3.2.1. By providing the following service management functions, the PMO will enable the Commonwealth to receive cost-effective, transparent, and flexible consumption-based services.

- Program and Service Management
- Availability and SLA Management
- Change and Release Management
- Service Desk
- Technical Architecture
- Account Management
- Configuration Management
- Third-party License Management.

The PMO will implement the service management, governance, and CSIIP functions during transition. As part of the service management implementation, Unisys will implement ITIL V3-based and ISO 20000-certified processes and integrated service management tools to monitor, manage, track, and report on the services and projects supporting the Commonwealth infrastructure. Through the implementation of the governance and CSIIP processes during transition, the Commonwealth will benefit from open communications, transparency, and continuous improvement for all services and activities supporting the common service portfolio.

3.4.5.2 Data Center Architecture (A.2)

With multiple data centers in the United States, the Commonwealth will benefit from the capability to migrate to fewer facilities, which can provide the managed infrastructure services and enable access to optional cloud hosting services. To support each agency's needs while also providing cost-effective services for the Commonwealth, the data centers are designed to support multi-tenant hosting services and infrastructure. The multi-tenant support includes network and security architectures that can enable separation between the agencies while sharing infrastructure components when possible to cost-effective services that can scale and adjust to specific requirements.

These facilities have the capability to provide several business continuity options to support the requirements of each agency's applications.

Unisys selected these data centers to limit the impact of network latency due to distance from Harrisburg and support the functionality for Tier 3 uptime compliance.

Our Data Center Architecture encompasses the following design functions and is located in Schedule F, Section 3.1:

- Multi-Data Center Environment (2+ Architecture)
- Network and Security Architecture
- Data Center Architecture and Technology.

3.4.5.3 Technical Services (A.3)

To support the Commonwealth's business and application environment changes, the infrastructure services will need to have the flexibility to change and adjust to the Commonwealth's needs as well as industry and technology advancements. Through the Technology Services, the Commonwealth will receive the ability to make changes in the services as well as implement new options to support the change in requirements.

The Technology Services support enables the introduction of new customers to the managed services and new or modified services to the Commonwealth. As part of the integrated service management processes, the Technology Services will also enable the Commonwealth to use new and updated technologies in the managed services as well as plan for changes in business needs due to usage, regulations, or legislation.

Our Technology Services encompass the following design functions and are located in Schedule F, Section 3.2.2.

- Transition Management (New Customer and/or Services)
- Infrastructure Architecture
- Capacity Management
- DR Planning and Testing
- Security Management
- Performance Monitoring and Management

3.4.5.4 Facility Management

Our approach to Facilities Management addresses all facets of managing the physical data center environment. Unisys selected geographically dispersed facilities to provide security and processing capability for the Commonwealth. When selecting the facilities, we searched for sites that simplified the monitoring activities displayed low risk for service

interruptions from unauthorized access, weather incidents, power incidents, damage to hardware, or injury to staff. We looked carefully at details such as power distribution, cooling, heating, ventilation, fire detection, fire suppression, access controls, and environmental controls.

We also selected facilities that supported our site operations objectives enabling data center staff and management to deliver world-class services to the Commonwealth; interface with the Commonwealth; and successfully implement our best practices for operational elements such as compute platforms, storage, networking, security, firewall, tape backup, and off-site tape rotation systems.

Our Facility Management section encompasses the following design functions and is located in Schedule F, Section 3.2.3:

- Facility Architecture and Maintenance
- Site Operations.

3.4.5.5 Managed Hosting Services (A.5)

Managed Hosting Services provide the people, process, and technologies to support each independent service while also being connected with the rest of the services by the integrated service management processes and platforms. For each of our services, we selected the technologies and people to provide a reliable, cost-effective solution for the Commonwealth to host and operate its applications.

Our Managed Hosting Services encompass the following design functions and are located in Schedule F, Section 3.2.4:

- Windows Support
- Storage Management
- ERP Hosting for SAP and Oracle
- UNIX Support for AIX and Linux
- Mainframe Services
- Security and Firewall
- Database Management Services
- Limited-Use Colocation Services.

3.4.5.6 Capacity on Demand Services (A.6)

Building capacity on demand that is realistic and relevant to the Commonwealth's business and technical requirements necessitates requires extensive experience and an extremely clear understanding of the underlying driver that the service demands. Only Unisys can

deliver this depth of understanding. Our server and storage capacity-on-demand model takes into account the business cycles experienced by the Commonwealth from a seasonal and longer legislative decision process that generates ebbs and flow in server demand. Our Disaster Recovery infrastructure on demand service model considers the need for servers, storage, and networks to support recovery of business applications and data when trouble strikes. Through Unisys use of similar technology platforms between the managed and capacity-on-demand services, the Commonwealth will have a flexible and manageable path of migration to the capacity-on-demand services.

By applying the integrated service management tools and processes for capacity and performance management and automation services, our capacity-on-demand services are designed to provide the necessary resources to address surges or long-term increases in processing requirements while providing reliable and cost-effective services.

Our Capacity on Demand Services encompasses the following design functions and are located in Schedule F, Section 3.2.5:

- Server Capacity on Demand
- Storage Capacity on Demand
- DR Infrastructure on Demand
- Additional Technical Services

3.4.5.7 Transition Services (A.7)

The Unisys Transition model is a critical mass for this contract. We alone have the background and skill to properly transition the Commonwealth from the current state to the proposed state specifically given our business knowledge.

We looked at the shared enterprise facilities and the individually owned agency data centers. We have a solid plan to transition the operations, applications, and data to our data centers with no impact on the user community.

We will pay careful attention to software licenses, protect Commonwealth interests, and add and subtract licenses to provide continued operations. We will maintain the integrity of data center configurations with regard to mainframes, servers, SAP, Oracle, and the other systems necessary to support business operations. Our strong governance model will oversee, control, and accomplish our transition plan.

Our Transition Services encompass the following design functions and are located in Schedule F, Section 3.3:

- Transition Plan
- Transition Program Management
- Security Transition Activities.

3.4.6 Contract Requirements - Small Diverse Business Participation (RFP IV-6

RFP	Requirement
IV-6	*Contract Requirements—Small Diverse Business Participation.* *All contracts containing Small Diverse Business participation must also include a provision requiring the selected contractor to meet and maintain those commitments made to Small Diverse Businesses at the time of proposal submittal or contract negotiation, unless a change in the commitment is approved by the BSBO. All contracts containing Small Diverse Business participation must include a provision requiring Small Diverse Business subcontractors to perform at least 50% of the subcontracted work.* *The selected contractor's commitments to Small Diverse Businesses made at the time of proposal submittal or contract negotiation shall, to the extent so provided in the commitment, be maintained throughout the term of the contract and through any renewal or extension of the contract. Any proposed change must be submitted to BSBO, which will make a recommendation to the Contracting Officer regarding a course of action.* *If a contract is assigned to another contractor, the new contractor must maintain the Small Diverse Business participation of the original contract.* *The selected contractor shall complete the Prime Contractor's Quarterly Utilization Report (or similar type document containing the same information) and submit it to the contracting officer of the Issuing Office and BSBO within ten (10) workdays at the end of each quarter the contract is in force. This information will be used to determine the actual dollar amount paid to Small Diverse Business subcontractors and suppliers. Also, this information will serve as a record of fulfillment of the commitment the selected contractor made and for which it received Small Diverse Business participation points. If there was no activity during the quarter then the form must be completed by stating "No activity in this quarter."* *NOTE: EQUAL EMPLOYMENT OPPORTUNITY AND CONTRACT COMPLIANCE STATEMENTS REFERRING TO COMPANY EQUAL EMPLOYMENT OPPORTUNITY POLICIES OR PAST CONTRACT COMPLIANCE PRACTICES DO NOT CONSTITUTE PROOF OF SMALL DIVERSE BUSINESS STATUS OR ENTITLE AN OFFEROR TO RECEIVE CREDIT FOR SMALL DIVERSE BUSINESS UTILIZATION.*

The Commonwealth of Pennsylvania recognizes the role that small businesses play in growing the economy. The Small Business Procurement Initiative announced by Governor Tom Corbett in July 2012 is another example of the Commonwealth's efforts to provide more business opportunities for small business in Pennsylvania.

As a Pennsylvania-based company, Unisys is committed to supporting the economic growth of small diverse businesses in Pennsylvania. Our proposal reflects this commitment through the use of several DGS-verified Small Diverse Businesses as subcontractor partners and suppliers in our proposed solution.

The Commonwealth of Pennsylvania is focused on economic growth by providing more business opportunities for small businesses and Unisys Corporation has a plan to support the Commonwealth's growth objectives. Our proposed solution for Data Center Computing Services includes the utilization of 11 Pennsylvania DGS-verified small diverse businesses to assist us in providing quality services to the Commonwealth. The Small Diverse Business Participation Submittal of this proposal provides information about our partners, the services and supplies that they will provide, and the economic value of their contribution. Procurement contract agreements have been established with each of our

partners to confirm that program scope, service level agreements, service responsibilities and compensation are clearly communicated. Letters of intent describing our commitment to each partner are included in Volume II of our proposal for Commonwealth review. Unisys will keep commitments made to Small Diverse Businesses as documented in our SDB submittal throughout the term of the contract and through any renewal of extension of the contract.

All Unisys subcontracts with our DGS-certified Small Diverse Business partners will include provisions (terms) requiring that the firm retain performance of at least 50% of the subcontracted work. In addition, Unisys agrees that if a contract is assigned to another contractor that the new contract will maintain the Small Diverse Business participation of the original contract if this can be achieved without adversely affecting service to the Commonwealth.

Providing the economic growth opportunities envisioned by the Small Business Procurement Initiative is important to the Commonwealth of Pennsylvania and to Unisys Corporation. In developing our solution, we carefully evaluated several DGS verified small diverse business firms for inclusion on the Unisys Team and selected those with the appropriate skills and company culture to support the delivery of high quality services and supplies to the Commonwealth. The Small Diverse Business Participation Submittal of our proposal provides details on each of these firms and the planned role for each in our managed services solution. The SDB Participation Submittal also includes the planned financial commitment for each of these firms which Unisys expects to maintain through the duration of the contract.

Unisys understands that all proposed changes to the Small Diverse Business participation included in our proposed solution need to be submitted to the Commonwealth of Pennsylvania's Bureau of Small Business Opportunities (BSBO) for review. In all cases, Unisys will offer our recommended plan to the Bureau of Small Business Opportunities for addressing changes to the scope of Small Diverse Business content while meeting or exceeding economic commitments to these partners.

The Commonwealth has indicated a need for accurate and timely information regarding the participation of Small Diverse Business (SDB) firms within the Data Center Compute Services project to be reported on a quarterly basis. Unisys Corporation will prepare and submit a Prime Contractor's Quarterly Utilization Report to the DGS contracting officer and the Bureau of Small Business Opportunities within ten (10) workdays at the end of each quarter that the contract is in force.

3.4.7 Proposed Services

RFP	Requirement
IV-3.C	*Proposed Services.* *The selected Offeror shall not significantly alter or discontinue any service defined in this RFP or proposed by the Offeror without prior written authorization from the Commonwealth.*

Unisys recognizes that services should not be significantly altered or discontinued without notification and written approval from the Commonwealth. The Commonwealth benefits from our open communications on significant changes to any proposed or defined services. As these changes, including discontinuation, are identified, Unisys will work with the Commonwealth to review the changes and request approval for any services or contract changes.

3.4.8 Payment for Services

RFP	Requirement
IV-3.E	*Payment for Services* *The selected Offeror may bill for a Service once the Commonwealth accepts the Service via ITSM.*

Unisys recognizes the Commonwealth should receive a completed work product or implementation before billing for the service. We will use the acceptance of a service request in the ITSM system as the Commonwealth's approval to begin the billing process.

This page intentionally left blank.

Attachment 3–1 — Schedule B: Governance

This page intentionally left blank.

Attachment 3–2 — Schedule C: Service Catalog

This page intentionally left blank.

Attachment 3–3 — Schedule D: Transition Milestones

This page intentionally left blank.

Attachment 3–4 – Schedule E: Data Center Locations

This page intentionally left blank.

Attachment 3–5 — Schedule F: Statement of Work

This page intentionally left blank.

Attachment 3–6 — Schedule H: CCPM

This page intentionally left blank.

Attachment 3–7 — Schedule M: Detailed Transition Plan

This page intentionally left blank.

Attachment 3–8 — Schedule K: Key Program Deliverables

This page intentionally left blank.

Attachment 3–9 — Schedule J.3: Service Level Agreements

This page intentionally left blank.

Request for Proposal

RFP # 6100022698

Commonwealth of Pennsylvania

Office of Administration

Office for Information Technology

Data Center Computing Services

SCHEDULE B

GOVERNANCE

1. **Management Meetings**. There shall be weekly meetings of the Management Committee during the Transition Period and monthly meetings thereafter. The purpose of such meetings shall be to (1) track the progress of the Transition and Transformation Plan, (2) review Contractor's performance of the Services Levels, (3) resolve disputes, (4) track the progress of the Services and other projects, (5) coordinate and plan for any new hardware or software acquisitions and service deployments, and (6) address any other matters properly brought before the Management Committee.

2. **Management Committee**. "Management Committee" shall be a committee comprised of ten members, five of whom shall be appointed by Commonwealth and five of whom shall be appointed by Contractor from Contractor's executive management staff. Commonwealth and Contractor shall each have one (1) vote with respect to matters that are brought before the Management Committee for resolution. Commonwealth shall designate one of its members on the Management Committee to act as the chairperson of the Management Committee. Both Commonwealth and Contractor can change the individuals on the Management Committee on an as-needed basis. The Management Committee shall be authorized and responsible for (1) generally overseeing the performance of this Contract, (2) providing input and advise to the Governor's Office of Administration regarding Commonwealth's strategic and tactical decisions in respect of the Services, the Systems and any other aspect of the business relationship between Commonwealth and Contractor under this Contract, and (3) monitoring and attempting to resolve disputes regarding the provision of the Services and the Services Levels.

3. **Commonwealth Computing Procedures Manual**. For each Commonwealth Agency and as part of the Services, Contractor shall establish procedures pursuant to which Contractor proposes that policies of Commonwealth and Contractor will be adhered to during the Term for the Commonwealth, and shall deliver to Commonwealth, not later than thirty (30) days prior to the commencement of the activities contemplated under the Transition Plan for the Commonwealth's approval or comment, a draft Commonwealth Computing Procedures Manual generally summarizing (1) the Services, (2) the computer hardware and software environments in which, and the various Services Locations at which, the Services will be performed, (3) the documentation, if any, which provides further details regarding the Services, (4) the procedures Contractor intends to use, and the activities Contractor proposes to undertake, in order to manage the Services, and (5) the procedures of a management reporting system that Contractor will use to manage this Contract and communicate to and with Commonwealth. Commonwealth may, at its request, participate to whatever degree it desires in the preparation of the draft Commonwealth Computing Procedures Manual. Contractor may periodically propose and, at the request of Commonwealth, shall promptly propose updates of the Commonwealth Computing Procedures Manual to reflect any changes in the operations or procedures described therein, all of which proposed changes shall be subject to Commonwealth's approval or comment. Reference Schedule H - Commonwealth Computing Procedures Manual for additional details.

UNISYS RESPONSE:

Management Meetings

There shall be weekly meetings of the Management Committee during the Transition Period and monthly meetings thereafter. The purpose of such meetings shall be to (1) track the progress of the Transition and Transformation Plan, (2) review Contractor's performance of the Services Levels, (3) resolve disputes, (4) track the progress of the Services and other projects, (5) coordinate and plan for any new hardware or software acquisitions and service deployments, and (6) address any other matters properly brought before the Management Committee.

Unisys understands the need for meetings to effectively and efficiently communicate important information to program stakeholders as part of a good governance model. Management meetings, however, are but one component of that communication and governance model.

A three-tier meeting structure will provide visibility at all levels in our respective organizations.

- **Tier 1 – Executive Governance and Steering Committees —** The objective of these meetings is to focus on the engagement's strategy and goals. This will serve to better align the IT initiatives with the Commonwealth's business goals. These meetings will develop and review strategy for the engagement. They will provide a forum for sharing insights on the application of industry best practices. These meetings are held monthly early on the contract and quarterly as steady state operations are achieved.
- **Tier 2 – Program Management —** Program management meetings focus on operational performance. The objectives of these meetings are to manage performance and effectiveness, manage SLAs and communications, and provide a platform for continuous improvement. These meetings occur weekly in the Transition Phase and monthly as operations reach the steady state.
- **Tier 3 – Service Delivery Management Teams —** These meetings are meant to handle day-to-day issues. They will focus on daily operations, escalation management, third-party management and handoffs, and end-to-end incident management. These meetings occur daily during the transition and weekly after the steady state is achieved.

All meetings require controlled agendas to enable them to be held according to their mutually agreed frequency and to make the meetings productive for all parties. All points for improvement can be added to the CSIIP library to be jointly addressed by Unisys and the Commonwealth.

Examples of subject matter addressed by the governance teams and processes include the following:

- **Transition and Transformation Plan Tracking —** Gather status and metrics from transition and transformation activities, assess status and risk, identify issues and

risks, design and implement mitigation for risks and corrective actions for issues, and track issues to closure at subsequent meetings

- **Contractor Performance Reviews —** Gather status and metrics from service level activities, gather status and metrics from the transition, assess status and risk, identify issues and risks, design and implement mitigation for risks and corrective actions for issues, and track issues to closure at subsequent meetings
- **Dispute Management —** Gather the facts, distill them to relevant information, develop possible solutions, negotiate potential solutions with the disputing organizations, find common ground or acceptable compromise, implement solutions, and track disputes for recurring problems until the situation is closed
- **Issues/Risk Database —** Track the progress and usefulness of the deployed services, track the availability of unused services, track the status and risk for services, and track the status and risk for projects. Produce reports for review and comment at meetings, gather information and assignments from meetings, confirm the staff responsible for the issue or risk is aware of guidance from leadership, and record the status from staff working the issue or risk.
- **Acquisition Planning —** Coordinate and conduct planning sessions to address the enterprise impacts on new hardware of software acquisitions, service deployments, and projects. Document findings in the issues and risks database, confirm the staff responsible for the issue or risk is aware of guidance from leadership, and record the status from staff working the issue or risk.
- **Agenda Development —** For each meeting, appoint a moderator who will write and maintain the agenda for the meeting and confirm that all matters are presented to the correct level of management to evaluate and render decisions.

The objective of the Executive Steering Committee (ESC) is to provide strategic direction and oversight to the engagement, maintaining alignment with business objectives for each organization and monitoring the delivery of services to maintain continued business value. The ESC's roles and responsibilities include:

- Provide direction to the engagement and alignment with strategic initiatives
- Review account planning documents
- Provide final resolution of escalated issues
- Review business and technical proposals submitted by business sponsors
- Advise and guide the Program Management Committee as appropriate
- Review performance (reports and recommendations provided by the Program Management Committee)
- Review continuous improvement initiatives, achievement of milestones, and deliverables
- Review service levels annually and reset them as necessary
- Review key performance metrics (SLAs, and so forth) as needed
- Review decisions by key personnel
- Discuss overall satisfaction with the engagement.

The Program Management Committee (PMC) provides overall management of the relationship and delivery of the program, enabling the program to be aligned with the objectives set forth by the ESC and confirming the achievement of those objectives. The PMC's roles and responsibilities include:

- Assist with the alignment of service delivery with the Commonwealth's business strategy
- Assist in the development of a technology roadmap enabling efficient and effective management of IT resources
- Report the status and progress to the ESC each quarter
- Review change proposals
- Review performance
- Discuss overall satisfaction
- Create and review plans for continuous improvement
- Implement continuous improvement initiatives
- Resolve disputes
- Review personnel decisions
- Oversee day-to-day delivery of services.

The Service Delivery Management Committee (SDMC) provides overall management for day-to-day delivery streams, attains service delivery objectives set by the ESC, and makes recommendations to support program strategy. The SDMC's roles and responsibilities include

- Manage day-to-day operations
- Report progress to the Program Managers
- Review change proposals
- Review delivery performance
- Resolve delivery issues
- Review personnel decisions
- Make recommendations to support program objectives
- Implement continuous improvement initiatives
- Resolve disputes.

Management Committee

"Management Committee" shall be a committee comprised of ten members, five of whom shall be appointed by Commonwealth and five of whom shall be appointed by Contractor from Contractor's executive management staff. Commonwealth and Contractor shall each have one (1) vote with respect to matters that are brought before the Management Committee for resolution. Commonwealth shall designate one of its members on the Management Committee to act as the chairperson of the Management Committee. Both Commonwealth and Contractor can change the individuals on the Management Committee on an as-needed basis.

The Management Committee shall be authorized and responsible for (1) generally overseeing the performance of this Contract, (2) providing input and advise to the Governor's Office of Administration regarding Commonwealth's strategic and tactical decisions in respect of the Services, the Systems and any other aspect of the business relationship between Commonwealth and Contractor under this Contract, and (3) monitoring and attempting to resolve disputes regarding the provision of the Services and the Services Levels.

The Management Committee forms the heart of the project's governance.

"Governance is the set of processes that ensure the effective and efficient use of IT in enabling and organization to achieve its goals."

Source: Gartner, IT Governance Key Initiative Overview, July 22, 2011

The Management Committee includes governance at the strategic and tactical levels and maintains clarity of purpose, responsibility, and direction to allow proper focus on collaboration between the Commonwealth and the Unisys Team to achieve the Commonwealth's IT governance objectives.

Unisys developed a three-tier management committee structure. The Executive Governance Committee provides a clear description of this committee. The committee's membership will include five Commonwealth members and five Contractor members. Within the first 3 days of the contract, Unisys will collaborate with the Commonwealth Contracting Officer to identify the five Commonwealth members for this committee. The first meeting of the Executive Governance Committee will occur within 5 business days of the contract's start.

During the meetings, when voting is required to make decisions, each member of the Executive Governance Committee will have an equal vote on the decision, without regard to his or her respective employer (the Commonwealth or Unisys).

The chairperson of the Executive Governance Committee will be a Commonwealth employee. The committee's moderator and scribe will be a Unisys employee.

Membership of the Executive Governance Committee will be fluid, and as needed. Membership will be adjusted to address changes in employment or other needs (skills or experience) in the committee's structure.

The moderator will establish meeting agendas that include contract performance, strategic and tactical service decisions, system decisions, Commonwealth and Unisys business relationship issues, contract risks, and service level provision issues.

A recent TPI research study indicates that 5 percent to 30 percent of a transaction's expected value is lost through ineffective governance.

There are significant benefits to the Commonwealth when good governance is practiced, including:

- Improved business value
- Stronger relationships between the Commonwealth and the Unisys Team
- Enabled strategic partnering
- Improved communications
- Increased focus and proper prioritization
- Increased understanding of the Commonwealth's expectations and what is needed to accomplish them
- Clarification of accountability across Commonwealth and Unisys teams.

The Unisys approach to governance is focused on

- **Meeting objectives and honoring commitments —** By thoroughly evaluating the planned IT environment and analyzing the scope identified in the RFP, we plan on meeting our objectives and honoring our commitments. We will make thorough use of the Unisys JRM Builder tool to clarify responsibilities across the environment. We will employ the CSIIP program to manage and monitor focal points for collaboration.
- **Teaming for efficiency and removing barriers to excellence —** We will establish partnership principles that recognize we are vested in each other's success. We will build a Governance Program Plan that will fully operationalize governance and continually drive governance maturity.
- **IT goals focused on business outcomes and people computing —** Applying good process and technology is important to the success of any outsourcing project, but by focusing on people, the greatest potential is achieved. By applying People Computing concepts, we will increase collaboration at all levels—including the executive level—and maintain alignment and participation. We will seek to develop direct relationships with end user communities. We will understand and respond to changing business needs. We will do this by putting people first, before technology and process.

  We will also build a focus on the future by understanding our impact on future business outcomes. We will perform strategic and tactical planning. We will perform with continual innovation and improvement embedded in our activities, and we will regularly recalibrate our services and delivery to keep things fresh and current.

The Unisys approach strives to provide optimized IT with a mature governance model. The Unisys governance strategy involves two primary areas:

1. The definition of a well-documented Strategic Program Plan

2. A definition of the processes, organization, and relationships that will be used to govern the program.

The Strategic Program Plan

The Strategic Program Plan will involve the following:

- Developing a clear understanding of the Commonwealth's "business" and why Unisys services are vital to your constituents to help the account team put their work into proper context.
- Developing a framework for exactly what outcomes you are expect from this engagement.

The partnership's guiding principles should include mutual understanding of the key goals, values, and contributions required from each member of the team (including the Commonwealth). This will lead to faster decision-making and communications that are more direct.

A Governance Maturity Assessment is a first step to proper governance. In this phase of the project, the combined team, along with a draft framework plan, will complete a Governance Maturity Assessment Matrix. The five-stage maturity model will measure key attributes of good collaborative governance against five levels of maturity from nonexistent to optimized. The outcome will be an understanding of our organization's current governance maturity level, and it will identify the areas for greatest improvement that are linked to business issues being experienced.

A Governance Management System should be established and based on the Commonwealth's values for what is key to be communicated or alerted and should include early warning signals to warn of any potential failures to allow redress instead of remediation. The proposed communications and governance metric should be a simple visual control—red or green stickers in a common area to rate the week's communications success, for example.

One of the objectives for the PMO communication plan should be to assess communications events for the Unisys Team and the Commonwealth with an aim to prevent any individual or communication event from becoming a single point of failure in the relationship. A clear set of management escalation processes, escalation levels, and criteria should be developed to resolve business issues in a timely way. This process should also include a de-escalation process.

Instead of being "rear-view mirror" controls (telling you what happened after it takes place), focus should be made on alerting the team to unwelcome conditions that allow it to take immediate and predefined actions to proactively address the situation.

Communication Management is an important component of the Strategic Program Plan. In this discipline, a cadence for communications is established—and daily, weekly, or monthly communications are implemented to communicate information such as improvements, innovations, pro-activity, and changes using various forms of communication. Each agency leader will have an assigned Agency Account Manager serving as the primary point of contact from the Unisys Team who will promote effective two-way communication.

Defining the Processes, Organization, and Relationships

Defining roles and responsibilities is the first step of this portion of the strategy. A roles and responsibilities matrix will be developed to define the various actives. Defining roles and responsibilities will enable each critical activity to be covered by individuals who are either responsible or accountable for it, and all key people to be informed or consulted.

Then, a Joint Responsibility Matrix (JRM) will be developed. This will assign the Unisys Enterprise Services Catalog—based on ITIL V3—to the Commonwealth's environment. This activity will foster alignment and attempt to eliminate potential gaps. It will make use of a Unisys proprietary tool—JRM Builder—to facilitate and generate output that is color coded for easy reference.

Understanding the Commonwealth and Unisys organizational counterparts for each role on the project team is important in understanding the need to share ownership and work together to collaboratively manage the services that are provided. A simple template will facilitate the clear communication of the relationships for each role.

Effective governance is a critical success factor for this complicated transformation. The Unisys Team fully understands the Commonwealth's management structure and the independence of agency leadership. We have the relationships and experience to work with the Commonwealth to quickly establish a governance structure that facilitates rapid transition to the new model in a way that leverages optimizations from the new infrastructure model while respecting the individuality of agencies.

Commonwealth of Pennsylvania

Office of Administration

Office for Information Technology

Data Center Computing Services

SCHEDULE C

SERVICES CATALOG

Table of Contents

Introduction 7

Catalog of Services (Schedule I Tab 6) 9

Enterprise Services Catalog Template 89

Compute Services - Fully Managed Services 90

Fully Managed - X86 (Windows and Linux) 91

X86 (Windows or Linux) Physical Configuration - Configuration Components 91

X86 (Windows or Linux) Physical Configuration - Orderable Configurations 103

X86 (Windows or Linux) Virtual Configuration - Configuration Components 113

X86 (Windows or Linux) Virtual Configuration – Orderable Configurations 127

X86 (Windows or Linux) Tiers of Service 137

Fully Managed - P-Series Server (AIX) 149

P-Series (AIX) Server Configuration - Configuration Components 149

P-Series (AIX) Server Configuration – Orderable Configurations 155

P-Series (AIX) Tiers of Service 160

Compute Services - Managed Only Services 163

Managed Only Services – X86 (Windows and Linux) 163

Managed Only Services – P-Series (AIX) 165

Fully Managed - Storage and Backup 166

Storage Services 167

Tape and Backup Services 170

Compute Services - Co-Location Services 173

Co-Location Services - Configuration Components 173

Co-Location Services – Combined Configurations 178

Compute Services - Mainframe Services 181

IBM Mainframe Storage and Backup 181
IBM Mainframe Storage Services 181
IBM Mainframe Backup and Tape Services 182
IBM Mainframe Service 184
IBM Mainframe Configuration - Configuration Components 184
IBM Mainframe Configuration – Orderable Configurations 189
IBM Mainframe Tiers of Service 194
Unisys Mainframe Storage and Backup 197
Unisys Mainframe Storage Services 197
Unisys Mainframe Backup and Tape Services 198
Unisys Mainframe Service 200
Unisys Mainframe Configuration - Configuration Components 200
Unisys Mainframe Configuration – Orderable Configurations 206
Unisys Mainframe Tiers of Service 210
Compute Services - Infrastructure as a Service 213
Infrastructure as a Service (IaaS) – Windows and Linux 213
IaaS Windows/Linux Configuration - Configuration Components 213
IaaS Windows Configuration – Orderable Configurations 226
IaaS Linux Configuration – Orderable Configurations 231
Infrastructure as a Service (IaaS) – Storage 236
IaaS Storage Configuration - Configuration Components 236
Infrastructure as a Service – Storage – Orderable Configurations 241
Infrastructure as a Service - Backup 244
Third Party Software Management Service 245
Third Party Software – Unisys Supplied License and Management 245

Third Party Software – Commonwealth Supplied License, Unisys Supplied Maintenance 264
Additional Technical Resources 269
Additional Technical Services 279
Database Management Services 279
Database Management Services 279
Database Software 294
Database Management Deployment and Support Services - AIX 323
Database Management Deployment and Support Services – z-Series 348
Batch and Job Scheduling 373
Service Management 381
Custom Reports 381
ITSM Additional Licensing 382
Application Definition Mapping 383
Compute Services – Infrastructure Monitoring 385
Fully Managed Service 386
Windows / Linux 386
P-Series (AIX) Services 390
Storage and Backup Services 393
Managed Only Service 405
Windows / Linux 405
Mainframe Services 407
IBM Mainframe 407
Unisys Mainframe – Storage and Backup 413
Unisys Mainframe Configuration – Add On Software Run Pack 415
Unisys Mainframe Exhibit Based Replacements 419

Infrastructure as a Service 425
Microsoft Cloud Compute Services 425
VMWare vCloud Hybrid Cloud Compute Services 443
Identity and Access Management Services 461
Business Continuity and Disaster Recovery 465
Business Continuity - Planning Services 465
Disaster Recovery - Testing 468
Disaster Recovery – Storage and Backup 470
Application Services 483
Application Performance Monitoring Services 483
Application Capacity Management Services 487
Application Architecture Review 493
Application Assessment Services 495
Application Testing Services 503
Load/Availability Testing 513
Application Migration Services 518
Middleware Application Services 522
User Experience (UX) Design 551
Data Quality Management (DQM) Analysis & Strategy 557
Information Management Services 559
Enterprise Resource Planning (ERP) Management Services 563
Enterprise Resource Planning (ERP) Application Security Services 565
Communication Strategy 569
Infrastructure Virtualization and Migration Services 573
Data Center Facility Services 576

Data Center Relocation Services 593
Network and Security Services 596
IPV6 Services 596
LAN Network Services 597
Virtual Private Network Services 598
Network Load Balancing Services 606
Reverse Proxy Services 612
Stealth Security Services 615
Security Services 640
Security Vulnerability Assessment 640
Security Risk Management 650
Security Configuration Review 655
Cyber Threat Intelligence (CTI) Analysis 657
Data Prevention 666
Mobile Security 672
Security Awareness Training 675
Identity & Access Management (IAM) Service 677
Third Party Software 684
Strategy Workshop Services 685

Introduction

The Unisys Enterprise Services Catalog represents entries that have been explicitly called out by the Commonwealth's Compute Services Request for Proposal (RFP) Schedule I Many additional suggestion came from other RFP's documents including Schedule F and the associated Exhibits. Unisys' experience with the Commonwealth augmented these entries enriching the choices contained in the Unisys Enterprise Services Catalog as suggested by the RFP.

The Enterprise Services Catalog provides descriptions for the specific entries shown including descriptions of related Enterprise Services Catalog items that will be needed to place a selection into its proper context. For example, the selection of a Gold Windows physical server will require the inclusion of an additional, identical server to provide the infrastructure capable of meeting the SLA. Similar instances exist, and are described, throughout the Enterprise Services Catalog. These dependencies are noted within the definition of each item.

The Commonwealth's Enterprise Services Catalog will be accessible from Unisys' Service Portal and support user-based authentication and privilege along with support for agency and project level accounting association with each requested item. Where the Commonwealth has advised Unisys that a request may move directly to ordering or provisioning, the Enterprise Services Catalog tool may trigger automated ordering and deployment of the request. Where change management must include approvals and scheduling, the Enterprise Services Catalog tool interfaces with the ITSM environment to participate in the process and gain the approvals and privilege necessary to trigger automated or staff processes to put the requests into motion.

The Enterprise Services Catalog that follows includes a rich selection of logical IT resources from servers and storage to networking. There is also a set of physical components such as racks, cages, and technical staff services available from the Enterprise Services Catalog. Ultimately, the Enterprise Services Catalog is a dynamic tool that is expandable to the Commonwealth's requirements. Unisys anticipates that transition will uncover other Information Technology (IT) services and resources that may be needed by the Commonwealth. The Enterprise Services Catalog is laid out with the following sections.

1) Catalog of Services

2) Enterprise Services Catalog Template

3) Compute Services - Fully Managed Services

4) Compute Services - Managed Only Services

5) Compute Services - Co-location Services

6) Compute Services - Mainframe Services

7) Compute Services – Infrastructure as a Service

8) Third-Party Software

9) Additional Technical Resources

10) Additional Technical Services

.

Catalog of Services (Schedule I Tab 6)

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Description / Use ==>	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevant Manufacture Part Number if needed*	*Provider's Equipment Code if needed*
* Note: This data is sample data provided as an example. The data contained do not contain actual prices or product information.									
* Sample Data ==>	Mainframe Dorado MIPS	Per MIP		ABC51323698	45687	1245	rv:5.0.1	FDCFG12599	XYZ123
* Sample Data ==>	VirtualServer Windows2008 vCPU	Per VCPU		ABC51323699	45688	1246	rv:5.0.2	FDCFG12600	XYZ124
* Sample Data ==>	VirtualServer Windows2008 vRAM	Per Gig		ABC51323700	45689	1247	rv:5.0.3	FDCFG12601	XYZ125
* Sample Data ==>	VirtualServer Windows2008 Gig Diskspace Tier1	Per Gig		ABC51323701	45690	1248	rv:5.0.4	FDCFG12602	XYZ126
* Sample Data ==>	VirtualServer Windows2008 Gig Diskspace Tier2	Per Gig		ABC51323702	45691	1249	rv:5.0.5	FDCFG12603	XYZ127
* Sample Data ==>	VirtualServer Windows2008 IIS Feature	Per Instance		ABC51323703	45692	1250	rv:5.0.6	FDCFG12604	XYZ128
* Sample Data ==>	VirtualServer Windows2008 WebServer Feature	Per Instance		ABC51323704	45693	1251	rv:5.0.7	FDCFG12605	XYZ129
* Sample Data ==>	Backup Service Disk	Per Server		ABC51323705	45694	1252	rv:5.0.8	FDCFG12606	XYZ130
* Sample Data ==>	SSL Certificate	Per Cert		ABC51323706	45695	1253	rv:5.0.9	FDCFG12607	XYZ131
Server - Fully Managed (1)									
x86 Server Configurations (Windows)									
Windows pConfig - 1	2-way Quad-Core 2.0 GHz	Per Server		CCSU13310001-A	N/A	N/A	A		
Windows pConfig - 2, 4, 5	2-way Six-Core 2.4 GHz	Per Server		CCSU13310002-A	N/A	N/A	A		
Windows pConfig - 3	4-way Six-Core 2.0 GHz	Per Server		CCSU13310003-A	N/A	N/A	A		
Windows pConfig - 1, 2, 3, 4, 5	GB RAM	Per GB		CCSU13310004-A	N/A	N/A	A		
Windows pConfig - 1, 2, 4, 5	Mirrored 146 15K Hard Drives	Per Primary + Mirror drive		CCSU13310005-A	N/A	N/A	A		
Windows pConfig - 3	SAN Attached Storage	Per GB		CCSU13310006-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Windows pConfig - 1, 2, 3, 4, 5	Windows Server 2008 R2	Per License		CCSU13310007-A	2008	R2	A		
Windows pConfig - 4	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization Site's Local SAN Storage from hourly data synchronization	Per Service		CCSU13310008-A	N/A	N/A	A		
Windows pConfig - 5	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Service		CCSU13310009-A	N/A	N/A	A		
Windows pConfig - 1	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310010-A	N/A	N/A	A		
Windows pConfig - 1	Fully Managed (1) - Gold Tier	Per Config		CCSU13310011-A	N/A	N/A	A		
Windows pConfig - 1	Fully Managed (1) - Silver Tier	Per Config		CCSU13310012-A	N/A	N/A	A		
Windows pConfig - 1	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310013-A	N/A	N/A	A		
Windows pConfig - 1	Fully Managed (1) - Basic Tier	Per Config		CCSU13310014-A	N/A	N/A	A		
Windows pConfig - 2	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310015-A	N/A	N/A	A		
Windows pConfig - 2	Fully Managed (1) - Gold Tier	Per Config		CCSU13310016-A	N/A	N/A	A		
Windows pConfig - 2	Fully Managed (1) - Silver Tier	Per Config		CCSU13310017-A	N/A	N/A	A		
Windows pConfig - 2	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310018-A	N/A	N/A	A		
Windows pConfig - 2	Fully Managed (1) - Basic Tier	Per Config		CCSU13310019-A	N/A	N/A	A		
Windows pConfig - 3	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310020-A	N/A	N/A	A		
Windows pConfig - 3	Fully Managed (1) - Gold Tier	Per Config		CCSU13310021-A	N/A	N/A	A		
Windows pConfig - 3	Fully Managed (1) - Silver Tier	Per Config		CCSU13310022-A	N/A	N/A	A		
Windows pConfig - 3	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310023-A	N/A	N/A	A		
Windows pConfig - 3	Fully Managed (1) - Basic Tier	Per Config		CCSU13310024-A	N/A	N/A	A		
Windows pConfig - 4	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310025-A	N/A	N/A	A		
Windows pConfig - 4	Fully Managed (1) - Gold Tier	Per Config		CCSU13310026-A	N/A	N/A	A		
Windows pConfig - 4	Fully Managed (1) - Silver Tier	Per Config		CCSU13310027-A	N/A	N/A	A		
Windows pConfig - 4	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310028-A	N/A	N/A	A		
Windows pConfig - 4	Fully Managed (1) - Basic Tier	Per Config		CCSU13310029-A	N/A	N/A	A		
Windows pConfig - 5	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310030-A	N/A	N/A	A		
Windows pConfig - 5	Fully Managed (1) - Gold Tier	Per Config		CCSU13310031-A	N/A	N/A	A		
Windows pConfig - 5	Fully Managed (1) - Silver Tier	Per Config		CCSU13310032-A	N/A	N/A	A		
Windows pConfig - 5	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310033-A	N/A	N/A	A		
Windows pConfig - 5	Fully Managed (1) - Basic Tier	Per Config		CCSU13310034-A	N/A	N/A	A		
Windows pConfig - 1	2-way Quad-Core 2.0 GHz		1						

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
	GB RAM		4						
	Mirrored 146 15K Hard Drives		1						
	Windows Server 2008 R2		1						
	Sub-Total								
Windows pConfig - 1	Fully Managed (1) - Platinum Tier		1						
Windows pConfig - 1	Fully Managed (1) - Gold Tier		1						
Windows pConfig - 1	Fully Managed (1) - Silver Tier		1						
Windows pConfig - 1	Fully Managed (1) - Bronze Tier		1						
Windows pConfig - 1	Fully Managed (1) - Basic Tier		1						
Windows pConfig - 2	2-way Six-Core 2.4 GHz		1						
	GB RAM		16						
	Mirrored 146 15K Hard Drives		1						
	Windows Server 2008 R2		1						
	Sub-Total								
Windows pConfig - 2	Fully Managed (1) - Platinum Tier		1						
Windows pConfig - 2	Fully Managed (1) - Gold Tier		1						
Windows pConfig - 2	Fully Managed (1) - Silver Tier		1						
Windows pConfig - 2	Fully Managed (1) - Bronze Tier		1						
Windows pConfig - 2	Fully Managed (1) - Basic Tier		1						
Windows pConfig - 3	4-way Six-Core 2.0 GHz		1						
	GB RAM		64						
	SAN Attached Storage		500						
	Windows Server 2008 R2		1						
	Sub-Total								
Windows pConfig - 3	Fully Managed (1) - Platinum Tier		1						
Windows pConfig - 3	Fully Managed (1) - Gold Tier		1						
Windows pConfig - 3	Fully Managed (1) - Silver Tier		1						
Windows pConfig - 3	Fully Managed (1) - Bronze Tier		1						
Windows pConfig - 3	Fully Managed (1) - Basic Tier		1						
Windows pConfig - 4	2-way Six-Core 2.4 GHz		1						
	GB RAM		16						
	Mirrored 146 15K Hard Drives		1						
	Windows Server 2008 R2		1						

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization Site's Local SAN Storage from hourly data synchronization		1						
	Sub-Total								
Windows pConfig - 4	Fully Managed (1) - Platinum Tier		1						
Windows pConfig - 4	Fully Managed (1) - Gold Tier		1						
Windows pConfig - 4	Fully Managed (1) - Silver Tier		1						
Windows pConfig - 4	Fully Managed (1) - Bronze Tier		1						
Windows pConfig - 4	Fully Managed (1) - Basic Tier		1						
Windows pConfig - 5	2-way Six-Core 2.4 GHz		1						
	GB RAM		16						
	Mirrored 146 15K Hard Drives		1						
	Windows Server 2008 R2		1						
	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from Backup off-site tape Backups		1						
	Sub-Total								
Windows pConfig - 5	Fully Managed (1) - Platinum Tier		1						
Windows pConfig - 5	Fully Managed (1) - Gold Tier		1						
Windows pConfig - 5	Fully Managed (1) - Silver Tier		1						
Windows pConfig - 5	Fully Managed (1) - Bronze Tier		1						
Windows pConfig - 5	Fully Managed (1) - Basic Tier		1						
x86 Server Configurations (Linux)									
Linux pConfig - 1	2-way Quad-Core 2.0 GHz	Per Server		CCSU13310035-A	N/A	N/A	A		
Linux pConfig - 2, 4, 5	2-way Six-Core 2.4 GHz	Per Server		CCSU13310036-A	N/A	N/A	A		
Linux pConfig - 3	4-way Six-Core 2.0 GHz	Per Server		CCSU13310037-A	N/A	N/A	A		
Linux pConfig - 1	GB RAM	Per GB		CCSU13310038-A	N/A	N/A	A		
Linux pConfig - 1, 2, 4, 5	Mirrored 146 15K Hard Drives	Per Primary + Mirror drive		CCSU13310039-A	N/A	N/A	A		
Linux pConfig - 3	SAN Attached Storage	Per GB		CCSU13310040-A	N/A	N/A	A		
Linux pConfig - 1, 2, 3, 4 , 5	RedHat or SUSE	Per License		CCSU13310041-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Linux pConfig - 4	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Service		CCSU13310042-A	N/A	N/A	A		
Linux pConfig - 5	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Service		CCSU13310043-A	N/A	N/A	A		
Linux pConfig - 1	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310044-A	N/A	N/A	A		
Linux pConfig - 1	Fully Managed (1) - Gold Tier	Per Config		CCSU13310045-A	N/A	N/A	A		
Linux pConfig - 1	Fully Managed (1) - Silver Tier	Per Config		CCSU13310046-A	N/A	N/A	A		
Linux pConfig - 1	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310047-A	N/A	N/A	A		
Linux pConfig - 1	Fully Managed (1) - Basic Tier	Per Config		CCSU13310048-A	N/A	N/A	A		
Linux pConfig - 2	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310049-A	N/A	N/A	A		
Linux pConfig - 2	Fully Managed (1) - Gold Tier	Per Config		CCSU13310050-A	N/A	N/A	A		
Linux pConfig - 2	Fully Managed (1) - Silver Tier	Per Config		CCSU13310051-A	N/A	N/A	A		
Linux pConfig - 2	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310052-A	N/A	N/A	A		
Linux pConfig - 2	Fully Managed (1) - Basic Tier	Per Config		CCSU13310053-A	N/A	N/A	A		
Linux pConfig - 3	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310054-A	N/A	N/A	A		
Linux pConfig - 3	Fully Managed (1) - Gold Tier	Per Config		CCSU13310055-A	N/A	N/A	A		
Linux pConfig - 3	Fully Managed (1) - Silver Tier	Per Config		CCSU13310056-A	N/A	N/A	A		
Linux pConfig - 3	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310057-A	N/A	N/A	A		
Linux pConfig - 3	Fully Managed (1) - Basic Tier	Per Config		CCSU13310058-A	N/A	N/A	A		
Linux pConfig - 4	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310059-A	N/A	N/A	A		
Linux pConfig - 4	Fully Managed (1) - Gold Tier	Per Config		CCSU13310060-A	N/A	N/A	A		
Linux pConfig - 4	Fully Managed (1) - Silver Tier	Per Config		CCSU13310061-A	N/A	N/A	A		
Linux pConfig - 4	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310062-A	N/A	N/A	A		
Linux pConfig - 4	Fully Managed (1) - Basic Tier	Per Config		CCSU13310063-A	N/A	N/A	A		
Linux pConfig - 5	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310064-A	N/A	N/A	A		
Linux pConfig - 5	Fully Managed (1) - Gold Tier	Per Config		CCSU13310065-A	N/A	N/A	A		
Linux pConfig - 5	Fully Managed (1) - Silver Tier	Per Config		CCSU13310066-A	N/A	N/A	A		
Linux pConfig - 5	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310067-A	N/A	N/A	A		
Linux pConfig - 5	Fully Managed (1) - Basic Tier	Per Config		CCSU13310068-A	N/A	N/A	A		
Linux pConfig - 1	2-way Quad-Core 2.0 GHz		1						
	4 GB RAM		4						
	Mirrored 146 15K Hard Drives		1						
	RedHat or SUSE		1						

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
	Sub-Total								
Linux pConfig - 1	Fully Managed (1) - Platinum Tier		1						
Linux pConfig - 1	Fully Managed (1) - Gold Tier		1						
Linux pConfig - 1	Fully Managed (1) - Silver Tier		1						
Linux pConfig - 1	Fully Managed (1) - Bronze Tier		1						
Linux pConfig - 1	Fully Managed (1) - Basic Tier		1						
Linux pConfig - 2	2-way Six-Core 2.4 GHz		1						
	16 GB RAM		16						
	Mirrored 146 15K Hard Drives		1						
	RedHat or SUSE		1						
	Sub-Total								
Linux pConfig - 2	Fully Managed (1) - Platinum Tier		1						
Linux pConfig - 2	Fully Managed (1) - Gold Tier		1						
Linux pConfig - 2	Fully Managed (1) - Silver Tier		1						
Linux pConfig - 2	Fully Managed (1) - Bronze Tier		1						
Linux pConfig - 2	Fully Managed (1) - Basic Tier		1						
Linux pConfig - 3	4-way Six-Core 2.0 GHz		1						
	64 GB RAM		64						
	SAN Attached Storage		500						
	RedHat or SUSE		1						
	Sub-Total								
Linux pConfig - 3	Fully Managed (1) - Platinum Tier		1						
Linux pConfig - 3	Fully Managed (1) - Gold Tier		1						
Linux pConfig - 3	Fully Managed (1) - Silver Tier		1						
Linux pConfig - 3	Fully Managed (1) - Bronze Tier		1						
Linux pConfig - 3	Fully Managed (1) - Basic Tier		1						
Linux pConfig - 4	2-way Six-Core 2.4 GHz		1						
	16 GB RAM		16						
	Mirrored 146 15K Hard Drives		1						
	RedHat or SUSE		1						
	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization		1						
	Sub-Total								
Linux pConfig - 4	Fully Managed (1) - Platinum Tier		1						

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Linux pConfig - 4	Fully Managed (1) - Gold Tier		1						
Linux pConfig - 4	Fully Managed (1) - Silver Tier		1						
Linux pConfig - 4	Fully Managed (1) - Bronze Tier		1						
Linux pConfig - 4	Fully Managed (1) - Basic Tier		1						
Linux pConfig - 5	2-way Six-Core 2.4 GHz		1						
	16 GB RAM		16						
	Mirrored 146 15K Hard Drives		1						
	RedHat or SUSE		1						
	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups		1						
	Sub-Total								
Linux pConfig - 5	Fully Managed (1) - Platinum Tier		1						
Linux pConfig - 5	Fully Managed (1) - Gold Tier		1						
Linux pConfig - 5	Fully Managed (1) - Silver Tier		1						
Linux pConfig - 5	Fully Managed (1) - Bronze Tier		1						
Linux pConfig - 5	Fully Managed (1) - Basic Tier		1						
x86 (Windows) - Virtual Servers									
Windows vConfig - 1	2vCPU	Per Instance		CCSU13310069-A	N/A	N/A	A		
Windows vConfig - 2, 4, 5	4vCPU	Per Instance		CCSU13310070-A	N/A	N/A	A		
Windows vConfig - 3	8vCPU	Per Instance		CCSU13310071-A	N/A	N/A	A		
Windows vConfig - 1, 2, 3, 4, 5	GB Ram	Per GB		CCSU13310072-A	N/A	N/A	A		
Windows vConfig - 1, 2, 3, 4, 5	Windows Server 2008 R2	Per License		CCSU13310073-A	2008	R2	A		
Windows vConfig - 1, 2, 3, 4, 5	Firewall/IDS	Per Config		CCSU13310074-A	N/A	N/A	A		
Windows vConfig - 1, 2, 3, 4, 5	Site-Site VPN	Per Config		CCSU13310075-A	N/A	N/A	A		
Windows vConfig - 1, 2, 3, 4, 5	VPN Client	Per Config		CCSU13310076-A	N/A	N/A	A		
Windows vConfig - 1, 2, 3, 4, 5	VLAN	Per Config		CCSU13310077-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Windows vConfig - 4	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Config		CCSU13310078-A	N/A	N/A	A		
Windows vConfig - 5	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Config		CCSU13310079-A	N/A	N/A	A		
Windows vConfig - 1	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310080-A	N/A	N/A	A		
Windows vConfig - 1	Fully Managed (1) - Gold Tier	Per Config		CCSU13310081-A	N/A	N/A	A		
Windows vConfig - 1	Fully Managed (1) - Silver Tier	Per Config		CCSU13310082-A	N/A	N/A	A		
Windows vConfig - 1	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310083-A	N/A	N/A	A		
Windows vConfig - 1	Fully Managed (1) - Basic Tier	Per Config		CCSU13310084-A	N/A	N/A	A		
Windows vConfig - 2	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310085-A	N/A	N/A	A		
Windows vConfig - 2	Fully Managed (1) - Gold Tier	Per Config		CCSU13310086-A	N/A	N/A	A		
Windows vConfig - 2	Fully Managed (1) - Silver Tier	Per Config		CCSU13310087-A	N/A	N/A	A		
Windows vConfig - 2	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310088-A	N/A	N/A	A		
Windows vConfig - 2	Fully Managed (1) - Basic Tier	Per Config		CCSU13310089-A	N/A	N/A	A		
Windows vConfig - 3	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310090-A	N/A	N/A	A		
Windows vConfig - 3	Fully Managed (1) - Gold Tier	Per Config		CCSU13310091-A	N/A	N/A	A		
Windows vConfig - 3	Fully Managed (1) - Silver Tier	Per Config		CCSU13310092-A	N/A	N/A	A		
Windows vConfig - 3	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310093-A	N/A	N/A	A		
Windows vConfig - 3	Fully Managed (1) - Basic Tier	Per Config		CCSU13310094-A	N/A	N/A	A		
Windows vConfig - 4	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310095-A	N/A	N/A	A		
Windows vConfig - 4	Fully Managed (1) - Gold Tier	Per Config		CCSU13310096-A	N/A	N/A	A		
Windows vConfig - 4	Fully Managed (1) - Silver Tier	Per Config		CCSU13310097-A	N/A	N/A	A		
Windows vConfig - 4	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310098-A	N/A	N/A	A		
Windows vConfig - 4	Fully Managed (1) - Basic Tier	Per Config		CCSU13310099-A	N/A	N/A	A		
Windows vConfig - 5	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310100-A	N/A	N/A	A		
Windows vConfig - 5	Fully Managed (1) - Gold Tier	Per Config		CCSU13310101-A	N/A	N/A	A		
Windows vConfig - 5	Fully Managed (1) - Silver Tier	Per Config		CCSU13310102-A	N/A	N/A	A		
Windows vConfig - 5	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310103-A	N/A	N/A	A		
Windows vConfig - 5	Fully Managed (1) - Basic Tier	Per Config		CCSU13310104-A	N/A	N/A	A		
Windows vConfig - 1	2vCPU		1						
	GB Ram		4						
	Windows Server 2008 R2		1						
	Firewall/IDS		1						

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
	Site-Site VPN		1						
	VPN Client		1						
	VLAN		1						
	Sub-Total								
Windows vConfig - 1	Fully Managed (1) - Platinum Tier		1						
Windows vConfig - 1	Fully Managed (1) - Gold Tier		1						
Windows vConfig - 1	Fully Managed (1) - Silver Tier		1						
Windows vConfig - 1	Fully Managed (1) - Bronze Tier		1						
Windows vConfig - 1	Fully Managed (1) - Basic Tier		1						
Windows vConfig - 2	4vCPU		1						
	GB Ram		16						
	Windows Server 2008 R2		1						
	Firewall/IDS		1						
	Site-Site VPN		1						
	VPN Client		1						
	VLAN		1						
	Sub-Total								
Windows vConfig - 2	Fully Managed (1) - Platinum Tier		1						
Windows vConfig - 2	Fully Managed (1) - Gold Tier		1						
Windows vConfig - 2	Fully Managed (1) - Silver Tier		1						
Windows vConfig - 2	Fully Managed (1) - Bronze Tier		1						
Windows vConfig - 2	Fully Managed (1) - Basic Tier		1						
Windows vConfig - 3	8vCPU		1						
	GB Ram		64						
	Windows Server 2008 R2		1						
	Firewall/IDS		1						
	Site-Site VPN		1						
	VPN Client		1						
	VLAN		1						
	Sub-Total								
Windows vConfig - 3	Fully Managed (1) - Platinum Tier		1						
Windows vConfig - 3	Fully Managed (1) - Gold Tier		1						
Windows vConfig - 3	Fully Managed (1) - Silver Tier		1						
Windows vConfig - 3	Fully Managed (1) - Bronze Tier		1						
Windows vConfig - 3	Fully Managed (1) - Basic Tier		1						

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Windows vConfig - 4	4vCPU		1						
	GB Ram		16						
	Windows Server 2008 R2		1						
	Firewall/IDS		1						
	Site-Site VPN		1						
	VPN Client		1						
	VLAN		1						
	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization		1						
	Sub-Total								
Windows vConfig - 4	Fully Managed (1) - Platinum Tier		1						
Windows vConfig - 4	Fully Managed (1) - Gold Tier		1						
Windows vConfig - 4	Fully Managed (1) - Silver Tier		1						
Windows vConfig - 4	Fully Managed (1) - Bronze Tier		1						
Windows vConfig - 4	Fully Managed (1) - Basic Tier		1						
Windows vConfig - 5	4vCPU		1						
	GB Ram		16						
	Windows Server 2008 R2		1						
	Firewall/IDS		1						
	Site-Site VPN		1						
	VPN Client		1						
	VLAN		1						
	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups		1						
	Sub-Total								
Windows vConfig - 5	Fully Managed (1) - Platinum Tier		1						
Windows vConfig - 5	Fully Managed (1) - Gold Tier		1						
Windows vConfig - 5	Fully Managed (1) - Silver Tier		1						
Windows vConfig - 5	Fully Managed (1) - Bronze Tier		1						
Windows vConfig - 5	Fully Managed (1) - Basic Tier		1						
x86 (Linux) - Virtual Servers									
Linux vConfig - 1	2vCPU	Per Instance		CCSU13310105-A	N/A	N/A	A		
Linux vConfig - 2, 4, 5	4vCPU	Per Instance		CCSU13310106-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Linux vConfig - 3	8vCPU	Per Instance		CCSU13310107-A	N/A	N/A	A		
Linux vConfig - 1, 2, 3, 4, 5	GB Ram	Per GB		CCSU13310108-A	N/A	N/A	A		
Linux vConfig - 1, 2, 3, 4, 5	RedHat or SUSE	Per License		CCSU13310109-A	N/A	N/A	A		
Linux vConfig - 1, 2, 3, 4, 5	Firewall/IDS	Per Config		CCSU13310110-A	N/A	N/A	A		
Linux vConfig - 1, 2, 3, 4, 5	Site-Site VPN	Per Config		CCSU13310111-A	N/A	N/A	A		
Linux vConfig - 1, 2, 3, 4, 5	VPN Client	Per Config		CCSU13310112-A	N/A	N/A	A		
Linux vConfig - 1, 2, 3, 4, 5	VLAN	Per Config		CCSU13310113-A	N/A	N/A	A		
Linux vConfig - 4	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Config		CCSU13310114-A	N/A	N/A	A		
Linux vConfig - 5	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Config		CCSU13310115-A	N/A	N/A	A		
Linux vConfig - 1	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310116-A	N/A	N/A	A		
Linux vConfig - 1	Fully Managed (1) - Gold Tier	Per Config		CCSU13310117-A	N/A	N/A	A		
Linux vConfig - 1	Fully Managed (1) - Silver Tier	Per Config		CCSU13310118-A	N/A	N/A	A		
Linux vConfig - 1	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310119-A	N/A	N/A	A		
Linux vConfig - 1	Fully Managed (1) - Basic Tier	Per Config		CCSU13310120-A	N/A	N/A	A		
Linux vConfig - 2	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310121-A	N/A	N/A	A		
Linux vConfig - 2	Fully Managed (1) - Gold Tier	Per Config		CCSU13310122-A	N/A	N/A	A		
Linux vConfig - 2	Fully Managed (1) - Silver Tier	Per Config		CCSU13310123-A	N/A	N/A	A		
Linux vConfig - 2	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310124-A	N/A	N/A	A		
Linux vConfig - 2	Fully Managed (1) - Basic Tier	Per Config		CCSU13310125-A	N/A	N/A	A		
Linux vConfig - 3	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310126-A	N/A	N/A	A		
Linux vConfig - 3	Fully Managed (1) - Gold Tier	Per Config		CCSU13310127-A	N/A	N/A	A		
Linux vConfig - 3	Fully Managed (1) - Silver Tier	Per Config		CCSU13310128-A	N/A	N/A	A		
Linux vConfig - 3	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310129-A	N/A	N/A	A		
Linux vConfig - 3	Fully Managed (1) - Basic Tier	Per Config		CCSU13310130-A	N/A	N/A	A		
Linux vConfig - 4	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310131-A	N/A	N/A	A		
Linux vConfig - 4	Fully Managed (1) - Gold Tier	Per Config		CCSU13310132-A	N/A	N/A	A		
Linux vConfig - 4	Fully Managed (1) - Silver Tier	Per Config		CCSU13310133-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Linux vConfig - 4	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310134-A	N/A	N/A	A		
Linux vConfig - 4	Fully Managed (1) - Basic Tier	Per Config		CCSU13310135-A	N/A	N/A	A		
Linux vConfig - 5	Fully Managed (1) - Platinum Tier	Per Config		CCSU13310136-A	N/A	N/A	A		
Linux vConfig - 5	Fully Managed (1) - Gold Tier	Per Config		CCSU13310137-A	N/A	N/A	A		
Linux vConfig - 5	Fully Managed (1) - Silver Tier	Per Config		CCSU13310138-A	N/A	N/A	A		
Linux vConfig - 5	Fully Managed (1) - Bronze Tier	Per Config		CCSU13310139-A	N/A	N/A	A		
Linux vConfig - 5	Fully Managed (1) - Basic Tier	Per Config		CCSU13310140-A	N/A	N/A	A		
Linux vConfig - 1	2vCPU		1						
	GB Ram		4						
	RedHat or SUSE		1						
	Firewall/IDS		1						
	Site-Site VPN		1						
	VPN Client		1						
	VLAN		1						
	Sub-Total								
Linux vConfig - 1	Fully Managed (1) - Platinum Tier		1						
Linux vConfig - 1	Fully Managed (1) - Gold Tier		1						
Linux vConfig - 1	Fully Managed (1) - Silver Tier		1						
Linux vConfig - 1	Fully Managed (1) - Bronze Tier		1						
Linux vConfig - 1	Fully Managed (1) - Basic Tier		1						
Linux vConfig - 2	4vCPU		1						
	GB Ram		16						
	RedHat or SUSE		1						
	Firewall/IDS		1						
	Site-Site VPN		1						
	VPN Client		1						
	VLAN		1						
	Sub-Total								
Linux vConfig - 2	Fully Managed (1) - Platinum Tier		1						
Linux vConfig - 2	Fully Managed (1) - Gold Tier		1						
Linux vConfig - 2	Fully Managed (1) - Silver Tier		1						
Linux vConfig - 2	Fully Managed (1) - Bronze Tier		1						
Linux vConfig - 2	Fully Managed (1) - Basic Tier		1						
Linux vConfig - 3	8vCPU		1						

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
	GB Ram		64						
	RedHat or SUSE		1						
	Firewall/IDS		1						
	Site-Site VPN		1						
	VPN Client		1						
	VLAN		1						
	Sub-Total								
Linux vConfig - 3	Fully Managed (1) - Platinum Tier		1						
Linux vConfig - 3	Fully Managed (1) - Gold Tier		1						
Linux vConfig - 3	Fully Managed (1) - Silver Tier		1						
Linux vConfig - 3	Fully Managed (1) - Bronze Tier		1						
Linux vConfig - 3	Fully Managed (1) - Basic Tier		1						
Linux vConfig - 4	4vCPU		1						
	GB Ram		16						
	RedHat or SUSE		1						
	Firewall/IDS		1						
	Site-Site VPN		1						
	VPN Client		1						
	VLAN		1						
	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization		1						
	Sub-Total								
Linux vConfig - 4	Fully Managed (1) - Platinum Tier		1						
Linux vConfig - 4	Fully Managed (1) - Gold Tier		1						
Linux vConfig - 4	Fully Managed (1) - Silver Tier		1						
Linux vConfig - 4	Fully Managed (1) - Bronze Tier		1						
Linux vConfig - 4	Fully Managed (1) - Basic Tier		1						
Linux vConfig - 5	4vCPU		1						
	GB Ram		16						
	RedHat or SUSE		1						
	Firewall/IDS		1						
	Site-Site VPN		1						
	VPN Client		1						
	VLAN		1						

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups		1						
	Sub-Total								
Linux vConfig - 5	Fully Managed (1) - Platinum Tier		1						
Linux vConfig - 5	Fully Managed (1) - Gold Tier		1						
Linux vConfig - 5	Fully Managed (1) - Silver Tier		1						
Linux vConfig - 5	Fully Managed (1) - Bronze Tier		1						
Linux vConfig - 5	Fully Managed (1) - Basic Tier		1						
P-Series Server Configurations									
AIX Config - 1, 2, 3, 4, 5	3.0GHz POWER7	Per Server		CCSI13310141-A	N/A	N/A	A		
AIX Config - 1	Cores	Per .5 Core		CCSI13310142-A	N/A	N/A	A		
AIX Config - 1, 2, 3, 4, 5	GB RAM	Per GB		CCSI13310143-A	N/A	N/A	A		
AIX Config - 1, 2, 3, 4, 5	AIX	Per License		CCSI13310144-A	N/A	N/A	A		
AIX Config - 4	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Config		CCSI13310145-A	N/A	N/A	A		
AIX Config - 5	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Config		CCSI13310146-A	N/A	N/A	A		
AIX Config - 1	Fully Managed (1) - Platinum Tier	Per Config		CCSI13310147-A	N/A	N/A	A		
AIX Config - 1	Fully Managed (1) - Gold Tier	Per Config		CCSI13310148-A	N/A	N/A	A		
AIX Config - 1	Fully Managed (1) - Silver Tier	Per Config		CCSI13310149-A	N/A	N/A	A		
AIX Config - 1	Fully Managed (1) - Bronze Tier	Per Config		CCSI13310150-A	N/A	N/A	A		
AIX Config - 1	Fully Managed (1) - Basic Tier	Per Config		CCSI13310151-A	N/A	N/A	A		
AIX Config - 2	Fully Managed (1) - Platinum Tier	Per Config		CCSI13310152-A	N/A	N/A	A		
AIX Config - 2	Fully Managed (1) - Gold Tier	Per Config		CCSI13310153-A	N/A	N/A	A		
AIX Config - 2	Fully Managed (1) - Silver Tier	Per Config		CCSI13310154-A	N/A	N/A	A		
AIX Config - 2	Fully Managed (1) - Bronze Tier	Per Config		CCSI13310155-A	N/A	N/A	A		
AIX Config - 2	Fully Managed (1) - Basic Tier	Per Config		CCSI13310156-A	N/A	N/A	A		
AIX Config - 3	Fully Managed (1) - Platinum Tier	Per Config		CCSI13310157-A	N/A	N/A	A		
AIX Config - 3	Fully Managed (1) - Gold Tier	Per Config		CCSI13310158-A	N/A	N/A	A		
AIX Config - 3	Fully Managed (1) - Silver Tier	Per Config		CCSI13310159-A	N/A	N/A	A		
AIX Config - 3	Fully Managed (1) - Bronze Tier	Per Config		CCSI13310160-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
AIX Config - 3	Fully Managed (1) - Basic Tier	Per Config		CCSI13310161-A	N/A	N/A	A		
AIX Config - 4	Fully Managed (1) - Platinum Tier	Per Config		CCSI13310162-A	N/A	N/A	A		
AIX Config - 4	Fully Managed (1) - Gold Tier	Per Config		CCSI13310163-A	N/A	N/A	A		
AIX Config - 4	Fully Managed (1) - Silver Tier	Per Config		CCSI13310164-A	N/A	N/A	A		
AIX Config - 4	Fully Managed (1) - Bronze Tier	Per Config		CCSI13310165-A	N/A	N/A	A		
AIX Config - 4	Fully Managed (1) - Basic Tier	Per Config		CCSI13310166-A	N/A	N/A	A		
AIX Config - 5	Fully Managed (1) - Platinum Tier	Per Config		CCSI13310167-A	N/A	N/A	A		
AIX Config - 5	Fully Managed (1) - Gold Tier	Per Config		CCSI13310168-A	N/A	N/A	A		
AIX Config - 5	Fully Managed (1) - Silver Tier	Per Config		CCSI13310169-A	N/A	N/A	A		
AIX Config - 5	Fully Managed (1) - Bronze Tier	Per Config		CCSI13310170-A	N/A	N/A	A		
AIX Config - 5	Fully Managed (1) - Basic Tier	Per Config		CCSI13310171-A	N/A	N/A	A		
AIX Config - 1	3.0GHz POWER7		1						
	0.5 Cores		0.5						
	6 GB RAM		6						
	AIX		1						
	Sub-Total								
AIX Config - 1	Fully Managed (1) - Platinum Tier		1						
AIX Config - 1	Fully Managed (1) - Gold Tier		1						
AIX Config - 1	Fully Managed (1) - Silver Tier		1						
AIX Config - 1	Fully Managed (1) - Bronze Tier		1						
AIX Config - 1	Fully Managed (1) - Basic Tier		1						
AIX Config - 2	3.0GHz POWER7		1						
	1.0 Cores		1						
	12 GB RAM		12						
	AIX		1						
	Sub-Total								
AIX Config - 2	Fully Managed (1) - Platinum Tier		1						
AIX Config - 2	Fully Managed (1) - Gold Tier		1						
AIX Config - 2	Fully Managed (1) - Silver Tier		1						
AIX Config - 2	Fully Managed (1) - Bronze Tier		1						
AIX Config - 2	Fully Managed (1) - Basic Tier		1						
AIX Config - 3	3.0GHz POWER7		1						
	1.5 Cores		1.5						
	18 GB RAM		18						

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
	AIX		1						
	Sub-Total								
AIX Config - 3	Fully Managed (1) - Platinum Tier		1						
AIX Config - 3	Fully Managed (1) - Gold Tier		1						
AIX Config - 3	Fully Managed (1) - Silver Tier		1						
AIX Config - 3	Fully Managed (1) - Bronze Tier		1						
AIX Config - 3	Fully Managed (1) - Basic Tier		1						
AIX Config - 4	3.0GHz POWER7		1						
	1.0 Cores		1						
	12 GB RAM		12						
	AIX		1						
	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization		1						
	Sub-Total								
AIX Config - 4	Fully Managed (1) - Platinum Tier		1						
AIX Config - 4	Fully Managed (1) - Gold Tier		1						
AIX Config - 4	Fully Managed (1) - Silver Tier		1						
AIX Config - 4	Fully Managed (1) - Bronze Tier		1						
AIX Config - 4	Fully Managed (1) - Basic Tier		1						
AIX Config - 5	3.0GHz POWER7		1						
	1.0 Cores		1						
	12 GB RAM		12						
	AIX		1						
	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups		1						
	Sub-Total								
AIX Config - 5	Fully Managed (1) - Platinum Tier		1						
AIX Config - 5	Fully Managed (1) - Gold Tier		1						
AIX Config - 5	Fully Managed (1) - Silver Tier		1						
AIX Config - 5	Fully Managed (1) - Bronze Tier		1						
AIX Config - 5	Fully Managed (1) - Basic Tier		1						
AIX Config - 5	**Total**								
Server - Managed Only (2)									

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Server - Managed Only x86 (Windows, Linux)									
	Platinum Tier	Server/Instance		CCSU13320001-A	N/A	N/A	A		
	Gold Tier	Server/Instance		CCSU13320002-A	N/A	N/A	A		
	Silver Tier	Server/Instance		CCSU13320003-A	N/A	N/A	A		
	Bronze Tier	Server/Instance		CCSU13320004-A	N/A	N/A	A		
	Basic Tier	Server/Instance		CCSU13320005-A	N/A	N/A	A		
Server - Managed Only UNIX (IBM P-Series, AIX)									
	Platinum	LPAR		CCSI13320006-A	N/A	N/A	A		
	Gold Tier	LPAR		CCSI13320007-A	N/A	N/A	A		
	Silver Tier	LPAR		CCSI13320008-A	N/A	N/A	A		
	Bronze Tier	LPAR		CCSI13320009-A	N/A	N/A	A		
	Basic Tier	LPAR		CCSI13320010-A	N/A	N/A	A		
Storage and Backup - Fully Managed (1)									
Enterprise Storage									
	* Dedicated - Config 1 - SAN Raid 5	GB		CCSZ13310172-A	N/A	N/A	A		
	* Dedicated - Config 2 - SAN Raid 10	GB		CCSZ13310173-A	N/A	N/A	A		
	Dedicated - Config 3 - Net Attached	GB		CCSZ13310174-A	N/A	N/A	A		
Tape and Backup									
	** Server Tape Stored	GB Stored		CCSU13310175-A	N/A	N/A	A		
	** Offsite Tape Storage	Tapes		CCSU13310176-A	N/A	N/A	A		
Limited Co-Lo (Data Center Only Charge) (3)									
Limited Co-Lo Configurations									
Co-Lo Config - 1	1/4 Rack Configuration includes: 10U Cabinet Space	Per Config		CCSU13330001-A	N/A	N/A	A		
Co-Lo Config - 2	1/2 Rack Configuration includes: 21U Cabinet Space	Per Config		CCSU13330002-A	N/A	N/A	A		
Co-Lo Config - 3	Full Rack Configuration includes: 42U Cabinet Space	Per Config		CCSU13330003-A	N/A	N/A	A		
Co-Lo Config - 1, 2, 3	Network Bandwidth	Per GB		CCSU13330004-A	N/A	N/A	A		
Co-Lo Config - 1, 2, 3	100Mb/s Uplink	Each		CCSU13330005-A	N/A	N/A	A		
Co-Lo Config - 1, 2, 3	IP Addresses	Each		CCSU13330006-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Co-Lo Config - 1	110V AC Circuits	Per Circuit		CCSU13330007-A	N/A	N/A	A		
Co-Lo Config - 1	1/4 Rack Configuration includes: 10U Cabinet Space		1						
	GB Network Bandwidth		5000						
	100Mb/s Uplink		1						
	IP Addresses		6						
	110V AC Circuits		5						
Co-Lo Config - 1	**Total**								
Co-Lo Config - 2	1/2 Rack Configuration includes: 21U Cabinet Space		1						
	10,000 GB Network Bandwidth		10000						
	100Mb/s Uplink		1						
	IP Addresses		14						
	110V AC Circuits		10						
Co-Lo Config - 2	**Total**								
Co-Lo Config - 3	Full Rack Configuration includes: 42U Cabinet Space		1						
	GB Network Bandwidth		20000						
	100Mb/s Uplink		1						
	IP Addresses		30						
	110V AC Circuits		20						
Co-Lo Config - 3	**Total**								
Mainframe Services (4)									
IBM Mainframe									
	*** IBM Mainframe Allocated DASD	GB		CCSI13310177-A	N/A	N/A	A		
	IBM Tapes in Storage - VTS	GB		CCSI13310178-A	N/A	N/A	A		
	IBM Offsite Tape Storage	Tape/Reel		CCSI13310179-A	N/A	N/A	A		
IBM Mainframe Configurations									
IBM Mainframe Config - 1	IBM System zEnterprise Processor z/OS	Per MIP		CCSI13310180-A	N/A	N/A	A		
IBM Mainframe Config - 2, 3	IBM System zEnterprise Processor Virtual Linux Prod IFL	Per MIP		CCSI13310181-A	N/A	N/A	A		
IBM AS400 Config 1, 2	IBM i Series / AS400	Per CPW		CCSI13310182-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
IBM Mainframe Config - 3	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Config		CCSI13310183-A	N/A	N/A	A		
IBM AS400 Config 2	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Config		CCSI13310184-A	N/A	N/A	A		
IBM Mainframe Config - 1	Mainframe Services (4) - Platinum Tier	Per Config		CCSI13310185-A	N/A	N/A	A		
IBM Mainframe Config - 1	Mainframe Services (4) - Gold Tier	Per Config		CCSI13310186-A	N/A	N/A	A		
IBM Mainframe Config - 1	Mainframe Services (4) - Basic Tier	Per Config		CCSI13310187-A	N/A	N/A	A		
IBM Mainframe Config - 2	Mainframe Services (4) - Platinum Tier	Per Config		CCSI13310188-A	N/A	N/A	A		
IBM Mainframe Config - 2	Mainframe Services (4) - Gold Tier	Per Config		CCSI13310189-A	N/A	N/A	A		
IBM Mainframe Config - 2	Mainframe Services (4) - Basic Tier	Per Config		CCSI13310190-A	N/A	N/A	A		
IBM Mainframe Config - 3	Mainframe Services (4) - Platinum Tier	Per Config		CCSI13310191-A	N/A	N/A	A		
IBM Mainframe Config - 3	Mainframe Services (4) - Gold Tier	Per Config		CCSI13310192-A	N/A	N/A	A		
IBM Mainframe Config - 3	Mainframe Services (4) - Basic Tier	Per Config		CCSI13310193-A	N/A	N/A	A		
IBM AS400 Config 1	Mainframe Services (4) - Platinum Tier	Per Config		CCSI13310194-A	N/A	N/A	A		
IBM AS400 Config 1	Mainframe Services (4) - Gold Tier	Per Config		CCSI13310195-A	N/A	N/A	A		
IBM AS400 Config 1	Mainframe Services (4) - Basic Tier	Per Config		CCSI13310196-A	N/A	N/A	A		
IBM AS400 Config 2	Mainframe Services (4) - Platinum Tier	Per Config		CCSI13310197-A	N/A	N/A	A		
IBM AS400 Config 2	Mainframe Services (4) - Gold Tier	Per Config		CCSI13310198-A	N/A	N/A	A		
IBM AS400 Config 2	Mainframe Services (4) - Basic Tier	Per Config		CCSI13310199-A	N/A	N/A	A		
IBM Mainframe Config - 1	IBM System zEnterprise Processor z/OS		1						
	Sub-Total								
IBM Mainframe Config - 1	Mainframe Services (4) - Platinum Tier		1						

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
IBM Mainframe Config - 1	Mainframe Services (4) - Gold Tier		1						
IBM Mainframe Config - 1	Mainframe Services (4) - Basic Tier		1						
IBM Mainframe Config - 2	IBM System zEnterprise Processor Virtual Linux Prod IFL		1						
	Sub-Total								
IBM Mainframe Config - 2	Mainframe Services (4) - Platinum Tier		1						
IBM Mainframe Config - 2	Mainframe Services (4) - Gold Tier		1						
IBM Mainframe Config - 2	Mainframe Services (4) - Basic Tier		1						
IBM Mainframe Config - 3	IBM System zEnterprise Processor Virtual Linux Prod IFL		1						
	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization		1						
	Sub-Total								
IBM Mainframe Config - 3	Mainframe Services (4) - Platinum Tier		1						
IBM Mainframe Config - 3	Mainframe Services (4) - Gold Tier		1						
IBM Mainframe Config - 3	Mainframe Services (4) - Basic Tier		1						
IBM AS400 Config 1	IBM i Series / AS400		1						
	Sub-Total								
IBM AS400 Config 1	Mainframe Services (4) - Platinum Tier		1						
IBM AS400 Config 1	Mainframe Services (4) - Gold Tier		1						
IBM AS400 Config 1	Mainframe Services (4) - Basic Tier		1						
IBM AS400 Config 2	IBM i Series / AS400		1						
	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization		1						
	Sub-Total								
IBM AS400 Config 2	Mainframe Services (4) - Platinum Tier		1						

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
IBM AS400 Config 2	Mainframe Services (4) - Gold Tier		1						
IBM AS400 Config 2	Mainframe Services (4) - Basic Tier		1						
Unisys Mainframe									
	*** Unisys DASD	GB		CCSU13310200-A	N/A	N/A	A		
	Unisys Tapes in Storage - VTS	GB		CCSU13310201-A	N/A	N/A	A		
	Unisys Offsite Tape Storage	Tape/Reel		CCSU13310202-A	N/A	N/A	A		
Unisys Mainframe Configurations									
Unisys Mainframe Config - 1, 3	Unisys (ClearPath / Dorado)	Per MIP		CCSU13310203-A	N/A	N/A	A		
Unisys Mainframe Config - 2, 4	Unisys (ClearPath / Libra)	Per Mip		CCSU13310204-A	N/A	N/A	A		
Unisys Mainframe Config - 3	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Config		CCSU13310205-A	N/A	N/A	A		
Unisys Mainframe Config - 4	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Config		CCSU13310206-A	N/A	N/A	A		
Unisys Mainframe Config - 1	Mainframe Services (4) - Platinum Tier	Per Config		CCSU13310207-A	N/A	N/A	A		
Unisys Mainframe Config - 1	Mainframe Services (4) - Gold Tier	Per Config		CCSU13310208-A	N/A	N/A	A		
Unisys Mainframe Config - 1	Mainframe Services (4) - Basic Tier	Per Config		CCSU13310209-A	N/A	N/A	A		
Unisys Mainframe Config - 2	Mainframe Services (4) - Platinum Tier	Per Config		CCSU13310210-A	N/A	N/A	A		
Unisys Mainframe Config - 2	Mainframe Services (4) - Gold Tier	Per Config		CCSU13310211-A	N/A	N/A	A		
Unisys Mainframe Config - 2	Mainframe Services (4) - Basic Tier	Per Config		CCSU13310212-A	N/A	N/A	A		
Unisys Mainframe Config - 3	Mainframe Services (4) - Platinum Tier	Per Config		CCSU13310213-A	N/A	N/A	A		
Unisys Mainframe Config - 3	Mainframe Services (4) - Gold Tier	Per Config		CCSU13310214-A	N/A	N/A	A		
Unisys Mainframe Config - 3	Mainframe Services (4) - Basic Tier	Per Config		CCSU13310215-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Unisys Mainframe Config - 4	Mainframe Services (4) - Platinum Tier	Per Config		CCSU13310216-A	N/A	N/A	A		
Unisys Mainframe Config - 4	Mainframe Services (4) - Gold Tier	Per Config		CCSU13310217-A	N/A	N/A	A		
Unisys Mainframe Config - 4	Mainframe Services (4) - Basic Tier	Per Config		CCSU13310218-A	N/A	N/A	A		
Unisys Mainframe Config - 1	Unisys (ClearPath / Dorado)		1						
	Sub-Total								
Unisys Mainframe Config - 1	Mainframe Services (4) - Platinum Tier		1						
Unisys Mainframe Config - 1	Mainframe Services (4) - Gold Tier		1						
Unisys Mainframe Config - 1	Mainframe Services (4) - Basic Tier		1						
Unisys Mainframe Config - 2	Unisys (ClearPath / Libra)		1						
	Sub-Total								
Unisys Mainframe Config - 2	Mainframe Services (4) - Platinum Tier		1						
Unisys Mainframe Config - 2	Mainframe Services (4) - Gold Tier		1						
Unisys Mainframe Config - 2	Mainframe Services (4) - Basic Tier		1						
Unisys Mainframe Config - 3	Unisys (ClearPath / Dorado)		1						
	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization		1						
	Sub-Total								
Unisys Mainframe Config - 3	Mainframe Services (4) - Platinum Tier		1						
Unisys Mainframe Config - 3	Mainframe Services (4) - Gold Tier		1						

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Unisys Mainframe Config - 3	Mainframe Services (4) - Basic Tier		1						
Unisys Mainframe Config - 4	Unisys (ClearPath / Libra)		1						
	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization		1						
	Sub-Total								
Unisys Mainframe Config - 4	Mainframe Services (4) - Platinum Tier		1						
Unisys Mainframe Config - 4	Mainframe Services (4) - Gold Tier		1						
Unisys Mainframe Config - 4	Mainframe Services (4) - Basic Tier		1						
IaaS x86 Server Configurations (Windows)									
IaaS Windows vConfig - 1	2vCPU	Per Server		CCSU13340001-A	N/A	N/A	A		
IaaS Windows vConfig - 2, 4, 5	4vCPU	Per Server		CCSU13340002-A	N/A	N/A	A		
IaaS Windows vConfig - 3	8vCPU	Per Server		CCSU13340003-A	N/A	N/A	A		
IaaS Windows vConfig - 1, 2, 3, 4, 5	GB Ram	Per GB		CCSU13340004-A	N/A	N/A	A		
IaaS Windows vConfig - 1, 2, 3, 4, 5	Windows Server 2008 R2	Per License		CCSU13340005-A	2008	R2	A		
IaaS Windows vConfig - 1, 2, 3, 4, 5	Firewall/IDS	Per Config		CCSU13340006-A	N/A	N/A	A		
IaaS Windows vConfig - 1, 2, 3, 4, 5	Site-Site VPN	Per Config		CCSU13340007-A	N/A	N/A	A		
IaaS Windows vConfig - 1, 2, 3, 4, 5	VPN Client	Per Config		CCSU13340008-A	N/A	N/A	A		
IaaS Windows vConfig - 1, 2, 3, 4, 5	VLAN	Per Config		CCSU13340009-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
IaaS Windows vConfig - 4	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Config		CCSU13340010-A	N/A	N/A	A		
IaaS Windows vConfig - 5	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Config		CCSU13340011-A	N/A	N/A	A		
IaaS Windows vConfig - 1	2vCPU		1						
	GB Ram		4						
	Windows Server 2008 R2		1						
	Firewall/IDS		1						
	Site-Site VPN		1						
	VPN Client		1						
	VLAN		1						
IaaS Windows vConfig - 1	Total								
IaaS Windows vConfig - 2	4vCPU		1						
	GB Ram		16						
	Windows Server 2008 R2		1						
	Firewall/IDS		1						
	Site-Site VPN		1						
	VPN Client		1						
	VLAN		1						
IaaS Windows vConfig - 2	Total								
IaaS Windows vConfig - 3	8vCPU		1						
	GB Ram		64						
	Windows Server 2008 R2		1						
	Firewall/IDS		1						
	Site-Site VPN		1						
	VPN Client		1						
	VLAN		1						
IaaS Windows vConfig - 3	Total								

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
IaaS Windows vConfig - 4	4vCPU		1						
	GB Ram		16						
	Windows Server 2008 R2		1						
	Firewall/IDS		1						
	Site-Site VPN		1						
	VPN Client		1						
	VLAN		1						
	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization		1						
IaaS Windows vConfig - 4	Total								
IaaS Windows vConfig - 5	4vCPU		1						
	GB Ram		16						
	Windows Server 2008 R2		1						
	Firewall/IDS		1						
	Site-Site VPN		1						
	VPN Client		1						
	VLAN		1						
	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups		1						
IaaS Windows vConfig - 5	Total								
IaaS x86 Server Configurations (Linux)									
IaaS Linux vConfig - 1	2vCPU	Per Server		CCSU13340012-A	N/A	N/A	A		
IaaS Linux vConfig - 2, 4, 5	4vCPU	Per Server		CCSU13340013-A	N/A	N/A	A		
IaaS Linux vConfig - 3	8vCPU	Per Server		CCSU13340014-A	N/A	N/A	A		
IaaS Linux vConfig - 1, 2, 3, 4, 5	GB Ram	Per GB		CCSU13340015-A	N/A	N/A	A		
IaaS Linux vConfig - 1, 2, 3, 4, 5	RedHat or SUSE	Per License		CCSU13340016-A			A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
IaaS Linux vConfig - 1, 2, 3, 4, 5	Firewall/IDS	Per Config		CCSU13340017-A			A		
IaaS Linux vConfig - 1, 2, 3, 4, 5	Site-Site VPN	Per Config		CCSU13340018-A			A		
IaaS Linux vConfig - 1, 2, 3, 4, 5	VPN Client	Per Config		CCSU13340019-A			A		
IaaS Linux vConfig - 1, 2, 3, 4, 5	VLAN	Per Config		CCSU13340020-A	N/A	N/A	A		
IaaS Linux vConfig - 4	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Config		CCSU13340021-A			A		
IaaS Linux vConfig - 5	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Config		CCSU13340022-A			A		
IaaS Linux vConfig - 1	2vCPU		1						
	4 GB Ram		4						
	RedHat or SUSE		1						
	Firewall/IDS		1						
	Site-Site VPN		1						
	VPN Client		1						
	VLAN		1						
IaaS Linux vConfig - 1	Total								
IaaS Linux vConfig - 2	4vCPU		1						
	16 GB Ram		16						
	RedHat or SUSE		1						
	Firewall/IDS		1						
	Site-Site VPN		1						
	VPN Client		1						
	VLAN		1						
IaaS Linux vConfig - 2	Total								
IaaS Linux vConfig - 3	8vCPU		1						
	64 GB Ram		64						
	RedHat or SUSE		1						
	Firewall/IDS		1						
	Site-Site VPN		1						
	VPN Client		1						

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
	VLAN		1						
IaaS Linux vConfig - 3	Total								
IaaS Linux vConfig - 4	4vCPU		1						
	16 GB Ram		16						
	RedHat or SUSE		1						
	Firewall/IDS		1						
	Site-Site VPN		1						
	VPN Client		1						
	VLAN		1						
	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization		1						
IaaS Linux vConfig - 4	Total								
IaaS Linux vConfig - 5	4vCPU		1						
	16 GB Ram		16						
	RedHat or SUSE		1						
	Firewall/IDS		1						
	Site-Site VPN		1						
	VPN Client		1						
	VLAN		1						
	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups		1						
IaaS Linux vConfig - 5	Total								
IaaS Storage Configurations									
IaaS Storage Config - 1, 2	SAN attached storage	Per GB		CCSU13340023-A	N/A	N/A	A		
IaaS Storage Config - 3	Network Attached Storage	Per GB		CCSU13340024-A	N/A	N/A	A		
IaaS Storage Config - 1	Raid 5	Per GB		CCSU13340025-A	N/A	N/A	A		
IaaS Storage Config - 2	Raid 10	Per GB		CCSU13340026-A	N/A	N/A	A		
IaaS Storage Config - 1, 2	10K - 15K RPM discs	Per GB		CCSU13340027-A	N/A	N/A	A		
IaaS Storage Config - 1	SAN attached storage		1						
	Raid 5		1						
	10K - 15K RPM discs		1						

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
IaaS Storage Config - 1	Total								
IaaS Storage Config - 2	SAN attached storage		1						
	Raid 10		1						
	10K - 15K RPM discs		1						
IaaS Storage Config - 2	Total								
IaaS Storage Config - 3	Network Attached Storage		1						
IaaS Storage Config - 3	Total								
IaaS Backup Configurations									
IaaS Backup Config - 1	Remote Offsite backup per GB	Per GB		CCSU13340028-A	N/A	N/A	A		
Reserve Account									
	Reserve Account - Enterprise Datacenter								
Third Party Software									
Third Party Software									
Vendor	**Product**								
B & L	BL/LIB Tape Library Management System	License		CCSU13350001-A			A		
B & L	BL/SCHED Scheduling & Monitoring System	License		CCSU13350002-A			A		
BMC Software	BMC AppSight for Windows/.NET - Division Edition	License		CCSU13350003-A			A		
BMC Software	BMC AppSight Named Users	License		CCSU13350004-A			A		
BMC Software	BMC AppSight QA Users	License		CCSU13350005-A			A		
BMC Software	CONTROL-M Enterprise Manager	License		CCSU13350006-A			A		
BMC Software	CONTROL-M Full Admin User	License		CCSU13350007-A			A		
BMC Software	CONTROL-M Tasks (100 Tasks per Unit)	License		CCSU13350008-A			A		
BMC Software	Database Director (D2)	License		CCSI13350009-A			A		
BMC Software	Eclipse iBuild	License		CCSI13350010-A			A		
BMC Software	Eclipse iChange	License		CCSI13350011-A			A		
BMC Software	Eclipse iCheck	License		CCSI13350012-A			A		
BMC Software	Eclipse iCopy	License		CCSI13350013-A			A		
BMC Software	Eclipse iExtract	License		CCSI13350014-A			A		
BMC Software	Eclipse iLM	License		CCSI13350015-A			A		
BMC Software	Eclipse iLoad	License		CCSI13350016-A			A		
BMC Software	Eclipse iRecover	License		CCSI13350017-A			A		
BMC Software	Eclipse iSurvey	License		CCSI13350018-A			A		
BMC Software	Eclipse iUnload	License		CCSI13350019-A			A		
BMC Software	Mission Control	License		CCSI13350020-A			A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Business Objects	Crystal Reports	License		CCSU13350021-A			A		
Bytware Inc.	StandGuard Anti-Virus	License		CCSU13350022-A			A		
Citrix	XenApp Advanced (User Counts)	License		CCSU13350023-A			A		
Citrix	XenApp Enterprise (User Counts)	License		CCSU13350024-A			A		
Computer Associates International, Inc.	CA-Explore for CICS	License		CCSI13350025-A			A		
Computer Associates International, Inc.	SOA Security Manager	License		CCSU13350026-A			A		
Computer Associates International, Inc.	SOA Security Manager Additional Secured Web Services	License		CCSU13350027-A			A		
Computer Associates International, Inc.	SOA Security Manager Additional Users	License		CCSU13350028-A			A		
Corticon Technologies	Corticon Business Rules Server – Unlimited CPUs	License		CCSU13350029-A			A		
Corticon Technologies	Corticon Server – per Non-Production Server	License		CCSU13350030-A			A		
Corticon Technologies	Corticon Business Rules Modeling Studio – per Named User	License		CCSU13350031-A			A		
CSI International	EPIC	License		CCSI13350032-A			A		
CSI International	FAQS/PCS	License		CCSI13350033-A			A		
CSI International	FAQS/ASO	License		CCSI13350034-A			A		
EMC Corporation	PowerPath	License		CCSU13350035-A			A		
EMC Corporation	PowerPath (per CPU)	License		CCSU13350036-A			A		
EMC Corporation	Symmetrix® VMAX Fully Automated Storage Tiering for Virtual Pools (FAST VP)	License		CCSU13350037-A			A		
EMC Corporation	Vsphere Enterprise Plus	License		CCSU13350038-A			A		
Experian QAS	NameSearch - Production (Licensed per Server up to 8 CPU)	License		CCSU13350039-A			A		
Experian QAS	NameSearch - Non-Production (Licensed per Server)	License		CCSU13350040-A			A		
Formula Consultants, Inc.	Star 1100	License		CCSU13350041-A			A		
GlobalScape	CuteFTP Pro 2.0	License		CCSU13350042-A			A		
HELPSYS	Robot/Schedule	License		CCSI13350043-A			A		
Idea Integration	XGEN	License		CCSU13350044-A			A		
Informatica Corporation	SSA-Name 3	License		CCSU13350045-A			A		
Infragistics	NetAdvantage for .NET	License		CCSU13350046-A			A		
KMSYS Worldwide, Inc.	IQU Plus-1	License		CCSU13350047-A			A		
Levi, Ray and Shoup	VPS/PCL	License		CCSI13350048-A			A		
Levi, Ray and Shoup	VPS/TCP/IP	License		CCSI13350049-A			A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Levi, Ray and Shoup	VPS/DRS	License		CCSI13350050-A			A		
Levi, Ray and Shoup	VPS	License		CCSI13350051-A			A		
MacKinney Systems, Inc.	CICS Response Time Monitor	License		CCSI13350052-A			A		
Marble Computer, Inc.	OS DCD III Data Correlation and Documentation System	License		CCSU13350053-A			A		
Microsoft	BizTalk Adaptor for MQSeries	License		CCSU13350054-A			A		
Microsoft	BizTalk Server Enterprise (Single Processor)	License		CCSU13350055-A			A		
Microsoft	BizTalk Server Standard (Single Processor)	License		CCSU13350056-A			A		
Microsoft	SQL Server CAL	License		CCSU13350057-A			A		
Microsoft	SQL Server Enterprise (Single Processor)	License		CCSU13350058-A			A		
Microsoft	SQL Server Enterprise	License		CCSU13350059-A			A		
Microsoft	SQL Server Standard (Single Processor)	License		CCSU13350060-A			A		
Microsoft	SQL Server Standard	License		CCSU13350061-A			A		
Microsoft	SQL Server Standard per 2-Core	License		CCSU13350062-A			A		
Microsoft	Visual Studio Foundation Server	License		CCSU13350063-A			A		
Microsoft	Visual Studio Foundation Server CAL	License		CCSU13350064-A			A		
Microsoft	Visual Studio Professional with MSDN	License		CCSU13350065-A			A		
Microsoft	Windows Server Datacenter Edition (Single Processor)	License		CCSU13350066-A			A		
Microsoft	Windows Server Enterprise Edition	License		CCSU13350067-A			A		
Microsoft	Windows Server Standard Edition	License		CCSU13350068-A			A		
Microsoft	Windows Terminal Service Client Access Licenses	License		CCSU13350069-A			A		
Network Associates	McAfee Anti-Virus	License		CCSU13350070-A			A		
Novell	Platespin Migrator	License		CCSU13350071-A			A		
Novell	SUSE Linux	License		CCSI13350072-A			A		
OpenText	Metastorm Integration Manager for CICS (MIM for CICS)	License		CCSI13350073-A			A		
Oracle	Oracle Change Management Pack	License		CCSU13350074-A			A		
Oracle	Oracle Database 10g Enterprise	License		CCSU13350075-A			A		
Oracle	Oracle Database Enterprise Edition	License		CCSU13350076-A			A		
Oracle	Oracle Diagnostic Pack	License		CCSU13350077-A			A		
Oracle	Oracle Enterprise Linux	License		CCSU13350078-A			A		
Oracle	Oracle Exadata Storage Software	License		CCSU13350079-A			A		
Oracle	Oracle Partitioning	License		CCSU13350080-A			A		
Oracle	Oracle Tuning Pack	License		CCSU13350081-A			A		
Oracle	Real Application Cluster - Processor Perpetual	License		CCSU13350082-A			A		
Oracle	Spatial and Graph - Processor Perpetual	License		CCSU13350083-A			A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Pitney Bowes	Finalist (Doc Sense)	License		CCSI13350084-A			A		
Pitney Bowes	CODE-1 Plus	License		CCSU13350085-A			A		
Pitney Bowes	CODE-1 Plus (Test / Development)	License		CCSU13350086-A			A		
Pitney Bowes	Online Window for Finalist	License		CCSI13350087-A			A		
Quest	Central Performance Suite for SQL Server, Tier A	License		CCSU13350088-A			A		
Quest	Central Performance Suite for SQL Server, Tier B	License		CCSU13350089-A			A		
Quest	Foglight Database Management Suite for SQL Server	License		CCSU13350090-A			A		
Quest	Foglight for SQL Server per CPU Socket	License		CCSU13350091-A			A		
Quest	Foglight OS Management per CPU Socket	License		CCSU13350092-A			A		
Quest	Foglight Server for FSM	License		CCSU13350093-A			A		
RealVNC	VNC Enterprise Edition for Windows	License		CCSU13350094-A			A		
Red Hat	Red Hat Enterprise Linux	License		CCSU13350095-A			A		
Schema Systems Limited	Q Editor Plus One	License		CCSU13350096-A			A		
Segus Inc.	OPC/Graph	License		CCSI13350097-A			A		
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG20	License		CCSU13350098-A			A		
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG40	License		CCSU13350099-A			A		
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG60	License		CCSU13350100-A			A		
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG80	License		CCSU13350101-A			A		
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG130	License		CCSU13350102-A			A		
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG20	License		CCSU13350103-A			A		
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG40	License		CCSU13350104-A			A		
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG60	License		CCSU13350105-A			A		
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG80	License		CCSU13350106-A			A		
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG130	License		CCSU13350107-A			A		
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG140	License		CCSU13350108-A			A		
Sightline	OS 2200 Interface Agent - MAPPER, SWG20	License		CCSU13350109-A			A		
Sightline	OS 2200 Interface Agent - MAPPER, SWG40	License		CCSU13350110-A			A		
Sightline	OS 2200 Interface Agent - MAPPER, SWG60	License		CCSU13350111-A			A		
Sightline	OS 2200 Interface Agent - MAPPER, SWG80	License		CCSU13350112-A			A		
Sightline	OS 2200 Interface Agent - MAPPER, SWG130	License		CCSU13350113-A			A		
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG20	License		CCSU13350114-A			A		
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG40	License		CCSU13350115-A			A		
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG60	License		CCSU13350116-A			A		
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG80	License		CCSU13350117-A			A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG130	License		CCSU13350118-A			A		
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG140	License		CCSU13350119-A			A		
Sightline	OS 2200 Interface Agent - System Log, SWG20	License		CCSU13350120-A			A		
Sightline	OS 2200 Interface Agent - System Log, SWG40	License		CCSU13350121-A			A		
Sightline	OS 2200 Interface Agent - System Log, SWG60	License		CCSU13350122-A			A		
Sightline	OS 2200 Interface Agent - System Log, SWG80	License		CCSU13350123-A			A		
Sightline	OS 2200 Interface Agent - System Log, SWG130	License		CCSU13350124-A			A		
Sightline	OS 2200 Interface Agent - System Log, SWG140	License		CCSU13350125-A			A		
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG20	License		CCSU13350126-A			A		
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG40	License		CCSU13350127-A			A		
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG60	License		CCSU13350128-A			A		
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG80	License		CCSU13350129-A			A		
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG130	License		CCSU13350130-A			A		
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG140	License		CCSU13350131-A			A		
Sightline	OS 2200 Power Agent, SWG20	License		CCSU13350132-A			A		
Sightline	OS 2200 Power Agent, SWG40	License		CCSU13350133-A			A		
Sightline	OS 2200 Power Agent, SWG60	License		CCSU13350134-A			A		
Sightline	OS 2200 Power Agent, SWG80	License		CCSU13350135-A			A		
Sightline	OS 2200 Power Agent, SWG130	License		CCSU13350136-A			A		
Sightline	OS 2200 Power Agent, SWG140	License		CCSU13350137-A			A		
Sightline	OS 2200 Torch Capacity Manager Power Agent, SWG40	License		CCSU13350138-A			A		
Sightline	OS 2200 Torch Capacity Manager Power Agent, SWG60	License		CCSU13350139-A			A		
Sightline	OS 2200 Torch Capacity Manager Power Agent, SWG130	License		CCSU13350140-A			A		
Sightline	OS 2200 Torch Capacity Manager Power Agent, SWG140	License		CCSU13350141-A			A		
Sightline	OS 2200 Torch Interface Agent - I/O TRACE, SWG40	License		CCSU13350142-A			A		
Sightline	OS 2200 Torch Interface Agent - I/O TRACE, SWG60	License		CCSU13350143-A			A		
Sightline	OS 2200 Torch Interface Agent - I/O TRACE, SWG130	License		CCSU13350144-A			A		
Sightline	OS 2200 Torch Interface Agent - LOG, SWG40	License		CCSU13350145-A			A		
Sightline	OS 2200 Torch Interface Agent - LOG, SWG60	License		CCSU13350146-A			A		
Sightline	OS 2200 Torch Interface Agent - LOG, SWG130	License		CCSU13350147-A			A		
Sightline	OS 2200 Torch Interface Agent - LOG, SWG140	License		CCSU13350148-A			A		
Sightline	OS 2200 Torch Interface Agent - MAPPER, SWG40	License		CCSU13350149-A			A		
Sightline	OS 2200 Torch Interface Agent - MAPPER, SWG60	License		CCSU13350150-A			A		
Sightline	OS 2200 Torch Interface Agent - MAPPER, SWG130	License		CCSU13350151-A			A		
Sightline	Windows 2000 Interface Agent - Internet Information Server	License		CCSU13350152-A			A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Sightline	Windows 2000 Interface Agent - .NET	License		CCSU13350153-A			A		
Sightline	Windows 2000 Interface Agent - SQL Server	License		CCSU13350154-A			A		
Sightline	Windows 2000 Power Agent Upto 32 CPU's	License		CCSU13350155-A			A		
SMA	OpCon/xps EXEC LSAM, Group 3	License		CCSU13350156-A			A		
SMA	OpCon/xps EXEC LSAM, Group 12	License		CCSU13350157-A			A		
SMA	OpCon/xps EXEC LSAM Development, Group 2	License		CCSU13350158-A			A		
SMA	OpCon/xps EXEC LSAM Development, Group 12	License		CCSU13350159-A			A		
SMA	OpCon/xps Production SAM	License		CCSU13350160-A			A		
SMA	OpCon/xps Starter Kit	License		CCSU13350161-A			A		
SMA	OpCon/xps User Interface	License		CCSU13350162-A			A		
Sybase	EAServer Deploy Advanced - Active	License		CCSU13350163-A			A		
Sybase	EAServer Deploy Advanced - Passive	License		CCSU13350164-A			A		
Symantec	Backup Exec System Recovery Server	License		CCSU13350165-A			A		
Symantec	EndPoint Protection	License		CCSU13350166-A			A		
Symantec	Ghost Solution Suite	License		CCSU13350167-A			A		
Symantec	NetBackup Client Application and Database Pack, UNX, Tier 3	License		CCSU13350168-A			A		
Symantec	NetBackup Client Application and Database Pack, UNX, Tier 4	License		CCSU13350169-A			A		
Symantec	NetBackup Client Application and Database Pack, WIN, Tier 2	License		CCSU13350170-A			A		
Symantec	NetBackup Client Application and Database Pack, WIN, Tier 3	License		CCSU13350171-A			A		
Symantec	NetBackup Client Application and Database Pack, WIN, Tier 4	License		CCSU13350172-A			A		
Symantec	NetBackup Enterprise Client, UNX, Tier 4	License		CCSU13350173-A			A		
Symantec	NetBackup Enterprise Client, WIN, Tier 1	License		CCSU13350174-A			A		
Symantec	NetBackup Enterprise Client, WIN, Tier 2	License		CCSU13350175-A			A		
Symantec	NetBackup Enterprise Client, WIN, Tier 3	License		CCSU13350176-A			A		
Symantec	NetBackup Enterprise Server, WIN, Tier 2	License		CCSU13350177-A			A		
Symantec	NetBackup Enterprise Server, WIN, Tier 3	License		CCSU13350178-A			A		
Symantec	NetBackup Library Based Tape Drive Option, XPLAT	License		CCSU13350179-A			A		
Symantec	NetBackup Media Server Encryption Option (MSEO) WIN, Tier 2	License		CCSU13350180-A			A		
Symantec	NetBackup Platform Base, XPLAT (per Terabyte)	License		CCSU13350181-A			A		
Symantec	NetBackup Shared Storage Option, XPLAT	License		CCSU13350182-A			A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Symantec	NetBackup Standard Client, XPLAT	License		CCSU13350183-A			A		
Symantec	NetBackup Vault Additional Drive Option, XPLAT	License		CCSU13350184-A			A		
Symantec	NetBackup Vault Base Option, XPLAT (4 tape drives per license)	License		CCSU13350185-A			A		
Symantec	Veritas NetBackup Enterprise Server License, Tier 3	License		CCSU13350186-A			A		
Symantec	Veritas NetBackup Windows Client, Tier 4	License		CCSU13350187-A			A		
Tone Software Corp.	Dynastep	License		CCSU13350188-A			A		
Unicon Group Ltd.	LOUIS II LCOM Host Module	License		CCSU13350189-A			A		
Unicon Group Ltd.	LOUIS II Extract & Reporting Module	License		CCSU13350190-A			A		
Unicon Group Ltd.	LOUIS II DERIVE Option	License		CCSU13350191-A			A		
Unicon Group Ltd.	LOUIS II DMS Interface	License		CCSU13350192-A			A		
Unicon Group Ltd.	LOUIS II RDMS Interface	License		CCSU13350193-A			A		
Unicon Group Ltd.	LOUIS II RELATE Option	License		CCSU13350194-A			A		
VanDyke Technologies	VShell Workgroup Server	License		CCSU13350195-A			A		
Veeam	nWorks ESX Monitoring for SCOM	License		CCSU13350196-A			A		
Veeam	nWorks Management Pack for VMWare	License		CCSU13350197-A			A		
VMware, Inc.	VMware vSphere 4 Enterprise Plus for 1 Processor	License		CCSU13350198-A			A		
VMware, Inc.	VMware vSphere 5 Enterprise Plus for 1 Processor	License		CCSU13350199-A			A		
Western American Data	Rlist	License		CCSU13350200-A			A		
Winternals	Winternals Administrator's Pak	License		CCSU13350201-A			A		
WinZip Computing	Winzip	License		CCSU13350202-A			A		
XtremeSoft	AppMetrics	License		CCSU13350203-A			A		
USPS	Correct Address	License		CCSU13350204-A			A		
IBM	FileNet	License		CCSU13350205-A			A		
Microsoft	SharePoint (with SA)	License		CCSU13350206-A			A		
IBM	WebSphere MQ (Procesor Value Unit)	License		CCSU13350207-A			A		
Xerox	XeroxDocuShare	License		CCSU13350208-A			A		
Hybrid Third Party Software									
Vendor	**Product**								
Computer Associates International, Inc.	CA 90's Services (freeware)	License		CCSI13350209-A			A		
Computer Associates International, Inc.	Vision Builder	License		CCSI13350210-A			A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Computer Associates International, Inc.	Easytrieve Plus	License		CCSI13350211-A			A		
Computer Associates International, Inc.	Easytrieve Plus MVS	License		CCSI13350212-A			A		
Computer Associates International, Inc.	Easytrieve Plus IMS	License		CCSI13350213-A			A		
Computer Associates International, Inc.	Easytrieve Plus IMS Option MVS	License		CCSI13350214-A			A		
Computer Associates International, Inc.	Easytrieve Plus DB2 OPT	License		CCSI13350215-A			A		
Computer Associates International, Inc.	Easytrieve Plus DB2 Option MVS	License		CCSI13350216-A			A		
Computer Associates International, Inc.	Endevor/MVS Automated Configuration Mgr MVS	License		CCSI13350217-A			A		
Computer Associates International, Inc.	Endevor/MVS External Security Int. MVS	License		CCSI13350218-A			A		
Computer Associates International, Inc.	Endevor/MVS MVS	License		CCSI13350219-A			A		
Computer Associates International, Inc.	Endevor/MVS Extended Processor	License		CCSI13350220-A			A		
Computer Associates International, Inc.	CA-Librarian	License		CCSI13350221-A			A		
Computer Associates International, Inc.	CA-META COBOL	License		CCSI13350222-A			A		
Computer Associates International, Inc.	Panvalet	License		CCSI13350223-A			A		
Computer Associates International, Inc.	Panvalet ISPF	License		CCSI13350224-A			A		
Computer Associates International, Inc.	SORT (INCL DART)	License		CCSI13350225-A			A		
Computer Associates International, Inc.	SRAM	License		CCSI13350226-A			A		
dotJ Software Inc.	dotJ Custom Tag Library	License		CCSU13350227-A			A		
Formula Consultants, Inc.	Star 1100	License		CCSU13350228-A			A		
Idea Integration	XGEN	License		CCSU13350229-A			A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Informatica Corporation	Change DataMove for DB2 Source	License		CCSI13350230-A			A		
Informatica Corporation	DataMove for DB2 Source	License		CCSI13350231-A			A		
Informatica Corporation	Change DataMove	License		CCSI13350232-A			A		
Informatica Corporation	DataMove for IMS Source	License		CCSI13350233-A			A		
Informatica Corporation	Change DataMove for IMS Source	License		CCSI13350234-A			A		
Informatica Corporation	DataMove	License		CCSI13350235-A			A		
Informatica Corporation	Change DataMove DB2 Target	License		CCSI13350236-A			A		
Informatica Corporation	DataMove DB2 Target	License		CCSI13350237-A			A		
Informatica Corporation	Change DataMove/DataMove Target for UDB	License		CCSI13350238-A			A		
Informatica Corporation	SSA - Name 3	License		CCSU13350239-A			A		
KMSYS Worldwide, Inc.	IQU Plus-1	License		CCSU13350240-A			A		
KMSYS Worldwide, Inc.	IQU Reorg Composer	License		CCSU13350241-A			A		
KMSYS Worldwide, Inc.	QPLXSS	License		CCSU13350242-A			A		
KMSYS Worldwide, Inc.	QPLXSV	License		CCSU13350243-A			A		
KMSYS Worldwide, Inc.	QPLXV	License		CCSU13350244-A			A		
Marble Computer Inc.	OS DCD III Data Correlation and Documentation System	License		CCSU13350245-A			A		
Microsoft	SQL Server Enterprise	License		CCSU13350246-A			A		
SAS Institute, Inc.	Base SAS	License		CCSI13350247-A			A		
SAS Institute, Inc.	SAS/ACCESS Interface for IMS	License		CCSI13350248-A			A		
SAS Institute, Inc.	SAS/ACCESS DB2	License		CCSI13350249-A			A		
SAS Institute, Inc.	SAS/AF	License		CCSI13350250-A			A		
SAS Institute, Inc.	SAS/FSP	License		CCSI13350251-A			A		
SAS Institute, Inc.	SAS/GRAPH	License		CCSI13350252-A			A		
SAS Institute, Inc.	SAS/SHARE	License		CCSI13350253-A			A		
SAS Institute, Inc.	SAS/STAT	License		CCSI13350254-A			A		
Schema Systems Limited	Q Editor Plus One	License		CCSU13350255-A			A		
SMA	OpCon/xps EXEC LSAM, Group 3	License		CCSU13350256-A			A		
SMA	OpCon/xps EXEC LSAM, Group 8	License		CCSU13350257-A			A		
SMA	OpCon/xps EXEC LSAM, Group 14	License		CCSU13350258-A			A		
SMA	OpCon/xps Microsoft LSAM	License		CCSU13350259-A			A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
SMA	OpCon/xps User Interface	License		CCSU13350260-A			A		
Sybase	EAServer Deploy Advanced - Active	License		CCSU13350261-A			A		
Sybase	EAServer Deploy Advanced - Passive	License		CCSU13350262-A			A		
TRILOGexport, Inc.	TriTune Automation Component (APC)	License		CCSI13350263-A			A		
Unicon Group Ltd.	LOUIS II Database Gateway	License		CCSU13350264-A			A		
Unicon Group Ltd.	LOUIS II DMS Interface	License		CCSU13350265-A			A		
Unicon Group Ltd.	LOUIS II Extract & Reporting Module	License		CCSU13350266-A			A		
Unicon Group Ltd.	LOUIS II LCOM Host Module	License		CCSU13350267-A			A		
Unicon Group Ltd.	LOUIS II MAPPER Interface	License		CCSU13350268-A			A		
Unicon Group Ltd.	LOUIS II RDMS Interface	License		CCSU13350269-A			A		
Verisign	Secure Site Pro SSL	License		CCSU13350270-A			A		
Western American Data	Rlist	License		CCSU13350271-A			A		
WinZip	Self-Extractor 10-user license	License		CCSU13350272-A			A		
Additional Services									
Other (insert description)				-			0		
Other (insert description)				-			0		
Orderable (Combined) Fully Managed Configurations									
Windows pConfig - 1	Windows pConfig - 1; 2-way Quad-Core 2.0 GHz; GB RAM; Mirrored 146 15K Hard Drives; Windows Server 2008 R2	Per Server		CCSU13310219-A	N/A	N/A	A		
Windows pConfig - 2	Windows pConfig - 2; 2-way Six-Core 2.4 GHz; GB RAM; Mirrored 146 15K Hard Drives; Windows Server 2008 R2	Per Server		CCSU13310220-A	N/A	N/A	A		
Windows pConfig - 3	Windows pConfig - 3; 4-way Six-Core 2.0 GHz; GB RAM; SAN Attached Storage; Windows Server 2008 R2	Per Server		CCSU13310221-A	N/A	N/A	A		
Windows pConfig - 4	Windows pConfig - 4; 2-way Six-Core 2.4 GHz; GB RAM; Mirrored 146 15K Hard Drives; Windows Server 2008 R2; Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization Site's Local SAN Storage from hourly data synchronization	Per Server		CCSU13310222-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Windows pConfig - 5	Windows pConfig - 5; 2-way Six-Core 2.4 GHz; GB RAM; Mirrored 146 15K Hard Drives; Windows Server 2008 R2; Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from Backup off-site tape Backups	Per Server		CCSU13310223-A	N/A	N/A	A		
Linux pConfig - 1	Linux pConfig - 1 ; 2-way Quad-Core 2.0 GHz; 4 GB RAM; Mirrored 146 15K Hard Drives; RedHat or SUSE	Per Server		CCSU13310224-A	N/A	N/A	A		
Linux pConfig - 2	Linux pConfig - 2 ; 2-way Six-Core 2.4 GHz; 16 GB RAM; Mirrored 146 15K Hard Drives; RedHat or SUSE	Per Server		CCSU13310225-A	N/A	N/A	A		
Linux pConfig - 3	Linux pConfig - 3 ; 4-way Six-Core 2.0 GHz; 64 GB RAM; SAN Attached Storage; RedHat or SUSE	Per Server		CCSU13310226-A	N/A	N/A	A		
Linux pConfig - 4	Linux pConfig - 4; 2-way Six-Core 2.4 GHz; 16 GB RAM; Mirrored 146 15K Hard Drives; RedHat or SUSE; Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Server		CCSU13310227-A	N/A	N/A	A		
Linux pConfig - 5	Linux pConfig - 5; 2-way Six-Core 2.4 GHz; 16 GB RAM; Mirrored 146 15K Hard Drives; RedHat or SUSE; Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Server		CCSU13310228-A	N/A	N/A	A		
Windows vConfig - 1	Windows vConfig - 1; 2vCPU; GB Ram; Windows Server 2008 R2; Firewall/IDS; Site-Site VPN; VPN Client; VLAN	Per Server		CCSU13310229-A	N/A	N/A	A		
Windows vConfig - 2	Windows vConfig - 2; 4vCPU; GB Ram; Windows Server 2008 R2; Firewall/IDS; Site-Site VPN; VPN Client; VLAN	Per Server		CCSU13310230-A	N/A	N/A	A		
Windows vConfig - 3	Linux vConfig - 3; 8vCPU; GB Ram; RedHat or SUSE; Firewall/IDS; Site-Site VPN; VPN Client; VLAN	Per Server		CCSU13310231-A	N/A	N/A	A		
Windows vConfig - 4	Windows vConfig - 4; 4vCPU; GB Ram; Windows Server 2008 R2; Firewall/IDS; Site-Site VPN; VPN Client; VLAN; Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Server		CCSU13310232-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Windows vConfig - 5	Windows vConfig - 5; 4vCPU; GB Ram; Windows Server 2008 R2; Firewall/IDS; Site-Site VPN; VPN Client; VLAN; Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Server		CCSU13310233-A	N/A	N/A	A		
Linux vConfig - 1	Linux vConfig - 1; 2vCPU; GB Ram; RedHat or SUSE; Firewall/IDS; Site-Site VPN; VPN Client; VLAN	Per Server		CCSU13310234-A	N/A	N/A	A		
Linux vConfig - 2	Linux vConfig - 2; 4vCPU; GB Ram; RedHat or SUSE; Firewall/IDS; Site-Site VPN; VPN Client; VLAN	Per Server		CCSU13310235-A	N/A	N/A	A		
Linux vConfig - 3	Linux vConfig - 3; 8vCPU; GB Ram; RedHat or SUSE; Firewall/IDS; Site-Site VPN; VPN Client; VLAN	Per Server		CCSU13310236-A	N/A	N/A	A		
Linux vConfig - 4	Linux vConfig - 4; 4vCPU; GB Ram; RedHat or SUSE; Firewall/IDS; Site-Site VPN; VPN Client; VLAN; Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Server		CCSU13310237-A	N/A	N/A	A		
Linux vConfig - 5	Linux vConfig - 5; 4vCPU; GB Ram; RedHat or SUSE; Firewall/IDS; Site-Site VPN; VPN Client; VLAN; Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Server		CCSU13310238-A	N/A	N/A	A		
AIX Config - 1	AIX Config - 1; 3.0GHz POWER7; 0.5 Cores; 6 GB RAM; AIX	Per Server		CCSI13310239-A	N/A	N/A	A		
AIX Config - 2	AIX Config - 2; 3.0GHz POWER7; 1.0 Cores; 12 GB RAM; AIX	Per Server		CCSI13310240-A	N/A	N/A	A		
AIX Config - 3	AIX Config - 3; 3.0GHz POWER7; 1.5 Cores; 18 GB RAM; AIX	Per Server		CCSI13310241-A	N/A	N/A	A		
AIX Config - 4	AIX Config - 4; 3.0GHz POWER7; 1.0 Cores; 12 GB RAM; AIX; Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Server		CCSI13310242-A	N/A	N/A	A		
AIX Config - 5	AIX Config - 5; 3.0GHz POWER7; 1.0 Cores; 12 GB RAM; AIX; Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Server		CCSI13310243-A	N/A	N/A	A		
Co-Lo Config - 1	Co-Lo Config - 1; 1/4 Rack Configuration includes: 10U Cabinet Space; GB Network Bandwidth; 100Mb/s Uplink; IP Addresses; 110V AC Circuits	Per Rack		CCSU13330008-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Co-Lo Config - 2	Co-Lo Config - 2; 1/2 Rack Configuration includes: 21U Cabinet Space; 10,000 GB Network Bandwidth; 100Mb/s Uplink; IP Addresses; 110V AC Circuits	Per Rack		CCSU13330009-A	N/A	N/A	A		
Co-Lo Config - 3	Co-Lo Config - 3 ; Full Rack Configuration includes: 42U Cabinet Space; GB Network Bandwidth; 100Mb/s Uplink; IP Addresses; 110V AC Circuits	Per Rack		CCSU13330010-A	N/A	N/A	A		
IBM Mainframe Config - 1	IBM Mainframe Config - 1;IBM System zEnterprise Processor z/OS	Per MIP		CCSI13310244-A	N/A	N/A	A		
IBM Mainframe Config - 2	IBM Mainframe Config - 2; IBM System zEnterprise Processor Virtual Linux Prod IFL	Per MIP		CCSI13310245-A	N/A	N/A	A		
IBM Mainframe Config - 3	IBM Mainframe Config - 3; IBM System zEnterprise Processor Virtual Linux Prod IFL; Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per MIP		CCSI13310246-A	N/A	N/A	A		
IBM AS400 Config 1	IBM AS400 Config 1; IBM i Series / AS400	Per CPW		CCSI13310247-A	N/A	N/A	A		
IBM AS400 Config 2	IBM AS400 Config 2; IBM i Series / AS400; Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per CPW		CCSI13310248-A	N/A	N/A	A		
Unisys Mainframe Config - 1	Unisys Mainframe Config - 1; Unisys (ClearPath / Dorado)	Per MIP		CCSU13310249-A	N/A	N/A	A		
Unisys Mainframe Config - 2	Unisys Mainframe Config - 2; Unisys (ClearPath / Libra) ;	Per MIP		CCSU13310250-A	N/A	N/A	A		
Unisys Mainframe Config - 3	Unisys Mainframe Config - 3; Unisys (ClearPath / Dorado); Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per MIP		CCSU13310251-A	N/A	N/A	A		
Unisys Mainframe Config - 4	Unisys Mainframe Config - 4; Unisys (ClearPath / Libra) ; Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per MIP		CCSU13310252-A	N/A	N/A	A		
IaaS Windows vConfig - 1	IaaS Windows vConfig - 1; 2vCPU; GB Ram; Windows Server 2008 R2; Firewall/IDS; Site-Site VPN; VPN Client; VLAN	Per Server		CCSU13340029-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
IaaS Windows vConfig - 2	IaaS Windows vConfig - 2; 4vCPU; GB Ram; Windows Server 2008 R2; Firewall/IDS; Site-Site VPN; VPN Client; VLAN	Per Server		CCSU13340030-A	N/A	N/A	A		
IaaS Windows vConfig - 3	IaaS Windows vConfig - 3; 8vCPU; GB Ram; Windows Server 2008 R2; Firewall/IDS; Site-Site VPN; VPN Client; VLAN	Per Server		CCSU13340031-A	N/A	N/A	A		
IaaS Windows vConfig - 4	IaaS Windows vConfig - 4; 4vCPU; GB Ram; Windows Server 2008 R2; Firewall/IDS; Site-Site VPN; VPN Client; VLAN; Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Server		CCSU13340032-A	N/A	N/A	A		
IaaS Windows vConfig - 5	IaaS Windows vConfig - 5; 4vCPU; GB Ram; Windows Server 2008 R2; Firewall/IDS; Site-Site VPN; VPN Client; VLAN; Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Server		CCSU13340033-A	N/A	N/A	A		
IaaS Linux vConfig - 1	IaaS Linux vConfig - 1; 2vCPU; 4 GB Ram; RedHat or SUSE; Firewall/IDS; Site-Site VPN; VPN Client; VLAN	Per Server		CCSU13340034-A	N/A	N/A	A		
IaaS Linux vConfig - 2	IaaS Linux vConfig - 2; 4vCPU; 16 GB Ram; RedHat or SUSE; Firewall/IDS; Site-Site VPN; VPN Client; VLAN	Per Server		CCSU13340035-A	N/A	N/A	A		
IaaS Linux vConfig - 3	IaaS Linux vConfig - 3; 8vCPU; 64 GB Ram; RedHat or SUSE; Firewall/IDS; Site-Site VPN; VPN Client; VLAN	Per Server		CCSU13340036-A	N/A	N/A	A		
IaaS Linux vConfig - 4	IaaS Linux vConfig - 4; 4vCPU; 16 GB Ram; RedHat or SUSE; Firewall/IDS; Site-Site VPN; VPN Client; VLAN; Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Server		CCSU13340037-A	N/A	N/A	A		
IaaS Linux vConfig - 5	IaaS Linux vConfig - 5; 4vCPU; 16 GB Ram; RedHat or SUSE; Firewall/IDS; Site-Site VPN; VPN Client; 741; Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Server		CCSU13340038-A	N/A	N/A	A		
IaaS Storage Config - 1	IaaS Storage Config - 1; SAN attached storage; Raid 5; 10K - 15K RPM discs	Per GB		CCSU13340039-A	N/A	N/A	A		
IaaS Storage Config - 2	IaaS Storage Config - 2; SAN attached storage; Raid 10; 10K - 15K RPM discs	Per GB		CCSU13340040-A	N/A	N/A	A		
IaaS Storage Config - 3	IaaS Storage Config - 3; Network Attached Storage	Per GB		CCSU13340041-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Additional Technical Resources									
Infrastructure (mainframe, mid-range and x86) Architects/Engineers		Per Hour		CCSZ13360001-A	N/A	N/A	A		
Microsoft Product Specialists (e.g. Exchange, SharePoint)		Per Hour		CCSZ13360002-A	N/A	N/A	A		
Basis and SAP Oracle support		Per Hour		CCSD13360003-A	N/A	N/A	A		
Performance Specialists		Per Hour		CCSZ13360004-A	N/A	N/A	A		
Mainframe Systems Programmers		Per Hour		CCSZ13360005-A	N/A	N/A	A		
Batch Administrators		Per Hour		CCSZ13360006-A	N/A	N/A	A		
3rd Party Software Product Specialists		Per Hour		CCSZ13360007-A	N/A	N/A	A		
System Administrator (Windows, AIX, Linux)		Per Hour		CCSZ13360008-A	N/A	N/A	A		
System Administrator (Middleware support)		Per Hour		CCSZ13360009-A	N/A	N/A	A		
Storage Administrator		Per Hour		CCSZ13360010-A	N/A	N/A	A		
Data Backup Administrator		Per Hour		CCSZ13360011-A	N/A	N/A	A		
Database Administrator		Per Hour		CCSZ13360012-A	N/A	N/A	A		
Database Architects		Per Hour		CCSZ13360013-A	N/A	N/A	A		
Database Analysts		Per Hour		CCSZ13360014-A	N/A	N/A	A		
Project Management Support		Per Hour		CCSZ13360015-A	N/A	N/A	A		
Network Administrator		Per Hour		CCSZ13360016-A	N/A	N/A	A		
Facilities Administrator		Per Hour		CCSZ13360017-A	N/A	N/A	A		
Security Administrator		Per Hour		CCSZ13360018-A	N/A	N/A	A		
Security Architects		Per Hour		CCSZ13360019-A	N/A	N/A	A		
Security Analysts		Per Hour		CCSZ13360020-A	N/A	N/A	A		
Asset Management Administrator		Per Hour		CCSZ13360021-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Quality Assurance Support		Per Hour		CCSZ13360022-A	N/A	N/A	A		
Remedy Support Specialist		Per Hour		CCSZ13360023-A	N/A	N/A	A		
IT Service Continuity Specialist		Per Hour		CCSZ13360024-A	N/A	N/A	A		
Infrastructure (mainframe, mid-range and x86) Architects/Engineers - Junior		Per Hour		CCSZ13360025-A	N/A	N/A	A		
Microsoft Product Specialists (e.g. Exchange, SharePoint) - Junior		Per Hour		CCSZ13360026-A	N/A	N/A	A		
Basis and SAP Oracle support - Junior		Per Hour		CCSD13360027-A	N/A	N/A	A		
Performance Specialists - Junior		Per Hour		CCSZ13360028-A	N/A	N/A	A		
Unisys Mainframe Systems Programmers - Junior		Per Hour		CCSU13360029-A	N/A	N/A	A		
Batch Administrators - Junior		Per Hour		CCSZ13360030-A	N/A	N/A	A		
Unisys Mainframe Batch Administrator - Senior		Per Hour		CCSU13360031-A	N/A	N/A	A		
Unisys Mainframe Batch Administrator - Junior		Per Hour		CCSU13360032-A	N/A	N/A	A		
3rd Party Software Product Specialists - Junior		Per Hour		CCSZ13360033-A	N/A	N/A	A		
System Administrator (Windows, AIX, Linux) - Junior		Per Hour		CCSZ13360034-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
System Administrator (Middleware support) - Junior		Per Hour		CCSZ13360035-A	N/A	N/A	A		
Data Backup Administrator - Junior		Per Hour		CCSZ13360036-A	N/A	N/A	A		
Database Administrator - Junior		Per Hour		CCSZ13360037-A	N/A	N/A	A		
Database Architects - Junior		Per Hour		CCSZ13360038-A	N/A	N/A	A		
Database Analysts - Junior		Per Hour		CCSZ13360039-A	N/A	N/A	A		
Project Management Support - Junior		Per Hour		CCSZ13360040-A	N/A	N/A	A		
Facilities Administrator - Junior		Per Hour		CCSZ13360041-A	N/A	N/A	A		
Network Administrator - Junior		Per Hour		CCSZ13360042-A	N/A	N/A	A		
Security Administrator - Junior		Per Hour		CCSZ13360043-A	N/A	N/A	A		
Security Architects - Junior		Per Hour		CCSZ13360044-A	N/A	N/A	A		
Security Analysts - Junior		Per Hour		CCSZ13360045-A	N/A	N/A	A		
Smart Hands and Feet Support		Per Hour		CCSU13360046-A	N/A	N/A	A		
Unisys Mainframe User Account Administrator		Per Hour		CCSU13360047-A	N/A	N/A	A		
Messaging Architect		Per Hour		CCSU13360048-A	N/A	N/A	A		
Senior Messaging Consultant		Per Hour		CCSU13360049-A	N/A	N/A	A		
Messaging Consultant		Per Hour		CCSU13360050-A	N/A	N/A	A		
Senior Active Directory Consultant		Per Hour		CCSU13360051-A	N/A	N/A	A		
Active Directory Consultant		Per Hour		CCSU13360052-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Application Support Consultant		Per Hour		CCSU13360053-A	N/A	N/A	A		
Technical Writer		Per Hour		CCSU13360054-A	N/A	N/A	A		
Automation Engineer - Senior		Per Hour		CCSU13360055-A	N/A	N/A	A		
Automation Engineer - Junior		Per Hour		CCSU13360056-A	N/A	N/A	A		
Senior Technology Consultant 1 - 2200 Database Support		Per Hour		CCSU13360057-A	N/A	N/A	A		
Senior Technology Consultant 2 - Windows 2000 and Middleware		Per Hour		CCSU13360058-A	N/A	N/A	A		
Senior Technology Consultant 3 - 2200 Mainframe Applications, Performance, and Security		Per Hour		CCSU13360059-A	N/A	N/A	A		
Senior Technology Consultant 4 - Middleware Products and Applications		Per Hour		CCSU13360060-A	N/A	N/A	A		
Senior Technology Consultant 5 - 2200 Database Design and Maintenance		Per Hour		CCSU13360061-A	N/A	N/A	A		
Senior Technology Consultant 6 – Data Warehouse Systems and Oracle Database Servers		Per Hour		CCSU13360062-A	N/A	N/A	A		
SPC Principal Engineer		Per Hour		CCSU13360063-A	N/A	N/A	A		
SPC Consulting Engineer		Per Hour		CCSU13360064-A	N/A	N/A	A		
Consultant 1		Per Hour		CCSU13360065-A	N/A	N/A	A		
Consultant 2		Per Hour		CCSU13360066-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Consultant 3		Per Hour		CCSU13360067-A	N/A	N/A	A		
Consultant 4		Per Hour		CCSU13360068-A	N/A	N/A	A		
Integration Architect		Per Hour		CCSU13360069-A	N/A	N/A	A		
Program Analyst		Per Hour		CCSU13360070-A	N/A	N/A	A		
Programmer		Per Hour		CCSU13360071-A	N/A	N/A	A		
Senior Programmer		Per Hour		CCSU13360072-A	N/A	N/A	A		
Senior Systems Analyst		Per Hour		CCSU13360073-A	N/A	N/A	A		
Senior Systems Architect		Per Hour		CCSU13360074-A	N/A	N/A	A		
Sr. Engagement Manager		Per Hour		CCSU13360075-A	N/A	N/A	A		
Systems Analyst		Per Hour		CCSU13360076-A	N/A	N/A	A		
Systems Architect		Per Hour		CCSU13360077-A	N/A	N/A	A		
Technology Architect		Per Hour		CCSU13360078-A	N/A	N/A	A		
Solutions Architect		Per Hour		CCSI13360079-A	N/A	N/A	A		
System Administrator (AIX, Linux) - Junior		Per Hour		CCSI13360080-A	N/A	N/A	A		
Storage Administrator - Junior		Per Hour		CCSI13360081-A	N/A	N/A	A		
Solutions Architect - Junior		Per Hour		CCSI13360082-A	N/A	N/A	A		
Asset Management Administrator - Junior		Per Hour		CCSI13360083-A	N/A	N/A	A		
Quality Assurance Support - Junior		Per Hour		CCSI13360084-A	N/A	N/A	A		
Remedy Support Specialist - Junior		Per Hour		CCSI13360085-A	N/A	N/A	A		
IT Service Continuity Specialist - Junior		Per Hour		CCSI13360086-A	N/A	N/A	A		
Mainframe System Programmer (IBM) - Junior		Per Hour		CCSI13360087-A	N/A	N/A	A		
Project Manager - ERP		Per Hour		CCSD13360088-A	N/A	N/A	A		
Functional Team Lead - ERP		Per Hour		CCSD13360089-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Senior Functional Specialist ERP		Per Hour		CCSD13360090-A	N/A	N/A	A		
Junior Functional Specialist - ERP		Per Hour		CCSD13360091-A	N/A	N/A	A		
Testing / Documentation Specialist - ERP		Per Hour		CCSD13360092-A	N/A	N/A	A		
Trainer		Per Hour		CCSD13360093-A	N/A	N/A	A		
Technical Team Lead		Per Hour		CCSD13360094-A	N/A	N/A	A		
Senior Developer		Per Hour		CCSD13360095-A	N/A	N/A	A		
Junior Developer		Per Hour		CCSD13360096-A	N/A	N/A	A		
Database Administrator Team Lead		Per Hour		CCSD13360097-A	N/A	N/A	A		
Senior System Administration Specialist		Per Hour		CCSD13360098-A	N/A	N/A	A		
Junior System Administration Specialist		Per Hour		CCSD13360099-A	N/A	N/A	A		
Senior Security Specialist		Per Hour		CCSD13360100-A	N/A	N/A	A		
Junior Security Specialist		Per Hour		CCSD13360101-A	N/A	N/A	A		
Program Manager - Onsite		Per Hour		CCSD13360102-A	N/A	N/A	A		
Senior Functional Analyst - Onsite		Per Hour		CCSD13360103-A	N/A	N/A	A		
Junior Functional Analyst - Onsite		Per Hour		CCSD13360104-A	N/A	N/A	A		
Testing / Documentation Specialist - Onsite		Per Hour		CCSD13360105-A	N/A	N/A	A		
Architect - Onsite		Per Hour		CCSD13360106-A	N/A	N/A	A		
Senior Developer - Onsite		Per Hour		CCSD13360107-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Junior Developer - Onsite		Per Hour		CCSD13360108-A	N/A	N/A	A		
Automated Tester - Onsite		Per Hour		CCSD13360109-A	N/A	N/A	A		
Database Administrator Team Lead - Onsite		Per Hour		CCSD13360110-A	N/A	N/A	A		
Senior Database Adminstrator Specialist - Onsite		Per Hour		CCSD13360111-A	N/A	N/A	A		
Junior Database Administrator Specialist - Onsite		Per Hour		CCSD13360112-A	N/A	N/A	A		
Security Specialist - Onsite		Per Hour		CCSD13360113-A	N/A	N/A	A		
Configuration Analyst - Onsite		Per Hour		CCSD13360114-A	N/A	N/A	A		
Additional Technical Services									
Database Management Service	Database Management Service - Database Support Resources - Platinum (Up to 500 hours per month)	Per Request		CCSD13370001-A	N/A	N/A	A		
Database Management Service	Database Management Service - Database Support Resources - Gold (Up to 375 hours per month)	Per Request		CCSD13370002-A	N/A	N/A	A		
Database Management Service	Database Management Service - Database Support Resources - Silver (Up to 250 hours per month)	Per Request		CCSD13370003-A	N/A	N/A	A		
Database Management Service	Database Management Service - Database Support Resources - Bronze (Up to 160 hours per month)	Per Request		CCSD13370004-A	N/A	N/A	A		
Database Management Service	Database Management Service - Database Support Resources - Basic (Up to 80 hours per month)	Per Request		CCSD13370005-A	N/A	N/A	A		
Database Management Service	Database Software - Microsoft SQL 2012 Enterprise - Physical Server using Windows pConfig-3	Per Server Instance		CCSU13370006-A	N/A	N/A	A		
Database Management Service	Database Software - Microsoft SQL 2012 Standad - Physical Server using Windows pConfig-3	Per Server Instance		CCSU13370007-A	N/A	N/A	A		
Database Management Service	Database Software - Microsoft SQL 2012 Enterprise - Virtual Server using Windows vConfig-3	Per Server Instance		CCSU13370008-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Database Management Service	Database Software - Microsoft SQL 2012 Standard - Virtual Server using Windows vConfig-3	Per Server Instance		CCSU13370009-A	N/A	N/A	A		
Database Management Service	Database Software - Oracle 11g Enterprise - Physical Server using Windows pConfig-3	Per Server Instance		CCSU13370010-A	N/A	N/A	A		
Database Management Service	Database Software - Oracle 11g Real Application Server - Physical Server using Windows pConfig-3	Per Server Instance		CCSU13370011-A	N/A	N/A	A		
Database Management Service	Database Software - Oracle 11g Standard - Physical Server using Windows pConfig-3	Per Server Instance		CCSU13370012-A	N/A	N/A	A		
Database Management Service	Database Software - Oracle 11g Enterprise - Physical Server using Windows pConfig-3 - Annual Maintenance	Per Server Instance		CCSU13370505-A	N/A	N/A	A		
Database Management Service	Database Software - Oracle 11g Real Application Server - Physical Server using Windows pConfig-3 - Annual Maintenance	Per Server Instance		CCSU13370506-A	N/A	N/A	A		
Database Management Service	Database Software - Oracle 11g Standard - Physical Server using Windows pConfig-3 - Annual Maintenance	Per Server Instance		CCSU13370507-A	N/A	N/A	A		
Database Management Service	Database Software - Sybase ASE Enterprise - Physical Server using Windows pConfig-3	Per Server Instance		CCSU13370013-A	N/A	N/A	A		
Database Management Service	Database Software - Sybase Replication Server using Windows pConfig-3	Per Server Instance		CCSU13370014-A	N/A	N/A	A		
Database Management Service	Database Software - Sybase ASE Standard - Physical Server using Windows pConfig-3	Per Server Instance		CCSU13370015-A	N/A	N/A			
Database Management Service	Database Software - Sybase ASE Enterprise - Physical Server using Windows pConfig-3 - Annual Maintenance	Per Server Instance		CCSU13370508-A	N/A	N/A	A		
Database Management Service	Database Software - Sybase Replication Server using Windows pConfig-3 - Annual Maintenance	Per Server Instance		CCSU13370509-A	N/A	N/A	A		
Database Management Service	Database Software - Sybase ASE Standard - Physical Server using Windows pConfig-3 - Annual Maintenance	Per Server Instance		CCSU13370510-A	N/A	N/A			
Database Management Service	Oracle Build p-Series Standard (1 server)	Per Request		CCSI13370016-A	N/A	N/A	A		
Database Management Service	Oracle Build p-Series Complex (2 servers in clustered pair)	Per Request		CCSI13370017-A	N/A	N/A	A		
Database Management Service	Oracle Upgrade p-Series Standard (1 server)	Per Request		CCSI13370018-A	N/A	N/A	A		
Database Management Service	Oracle Upgrade p-Series Complex (2 servers in clustered pair)	Per Request		CCSI13370019-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Database Management Service	DB2 Build p-Series Standard (1 server)	Per Request		CCSI13370020-A	N/A	N/A	A		
Database Management Service	DB2 Build p-Series Complex (2 servers)	Per Request		CCSI13370021-A	N/A	N/A	A		
Database Management Service	DB2 Upgrade p-Series Standard (1 server)	Per Request		CCSI13370022-A	N/A	N/A	A		
Database Management Service	DB2 Upgrade p-Series Complex (2 servers)	Per Request		CCSI13370023-A	N/A	N/A	A		
Database Management Service	p-Series Database Administrator for Oracle (3TB)	Per Database		CCSI13370024-A	N/A	N/A	A		
Database Management Service	p-Series Database Administrator for Oracle (7TB)	Per Database		CCSI13370025-A	N/A	N/A	A		
Database Management Service	p-Series Database Administrator for Oracle (12TB)	Per Database		CCSI13370026-A	N/A	N/A	A		
Database Management Service	p-Series Database Administrator for DB2 (3TB)	Per Database		CCSI13370027-A	N/A	N/A	A		
Database Management Service	p-Series Database Administrator for DB2 (7TB)	Per Database		CCSI13370028-A	N/A	N/A	A		
Database Management Service	p-Series Database Administrator for DB2 (12TB)	Per Database		CCSI13370029-A	N/A	N/A	A		
Database Management Service	p-Series Database Administrator for High Availability Databases: Oracle RAC or DB2 Clusters (20 databases)	Per Database		CCSI13370030-A	N/A	N/A	A		
Database Management Service	p-Series Database Administrator for High Availability Databases: Oracle RAC or DB2 Clusters (40 databases)	Per Database		CCSI13370031-A	N/A	N/A	A		
Database Management Service	p-Series Database Administrator for High Availability Databases: Oracle RAC or DB2 Clusters (60 databases)	Per Database		CCSI13370032-A	N/A	N/A	A		
Database Management Service	IMS Upgrade z-Series Standard (1 subsystem without data sharing or clustering)	Per Request		CCSI13370033-A	N/A	N/A	A		
Database Management Service	IMS Upgrade z-Series Complex (2 subsystems with data sharing and clustering across multiple CECs)	Per Request		CCSI13370034-A	N/A	N/A	A		
Database Management Service	IMS Maintenance z-Series Standard (1 subsystem without data sharing or clustering)	Per Request		CCSI13370035-A	N/A	N/A	A		
Database Management Service	IMS Maintenance z-Series Complex (2 subsystems with data sharing and clustering across multiple CECs)	Per Request		CCSI13370036-A	N/A	N/A	A		
Database Management Service	DB2 Upgrade z Series Standard (1 subsystem without data sharing or clustering)	Per Request		CCSI13370037-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Database Management Service	DB2 Upgrade z-Series Complex (2 subsystems with data sharing and clustering across multiple CECs)	Per Request		CCSI13370038-A	N/A	N/A	A		
Database Management Service	DB2 Maintenance z-Series Standard (1 subsystem without data sharing or clustering)	Per Request		CCSI13370039-A	N/A	N/A	A		
Database Management Service	DB2 Maintenance z-Series Complex (2 subsystems with data sharing and clustering across multiple CECs)	Per Request		CCSI13370040-A	N/A	N/A	A		
Database Management Service	z-Series Database Administrator for DB2 (5TB)	Per Database		CCSI13370041-A	N/A	N/A	A		
Database Management Service	z-Series Database Administrator for DB2 (10TB)	Per Database		CCSI13370042-A	N/A	N/A	A		
Database Management Service	z-Series Database Administrator for DB2 (15TB)	Per Database		CCSI13370043-A	N/A	N/A	A		
Database Management Service	z-Series Database Administrator for IMS (5TB)	Per Database		CCSI13370044-A	N/A	N/A	A		
Database Management Service	z-Series Database Administrator for IMS (10TB)	Per Database		CCSI13370045-A	N/A	N/A	A		
Database Management Service	z-Series Database Administrator for IMS (15TB)	Per Database		CCSI13370046-A	N/A	N/A	A		
Database Management Service	z-Series High Availability Databases: IMS or DB2 DataSharing (25 databases)	Per Database		CCSI13370047-A	N/A	N/A	A		
Database Management Service	z-Series High Availability Databases: IMS or DB2 DataSharing (50 databases)	Per Database		CCSI13370048-A	N/A	N/A	A		
Database Management Service	z-Series High Availability Databases: IMS or DB2 DataSharing (75 databases)	Per Database		CCSI13370049-A	N/A	N/A	A		
Batch and Job Scheduling	Batch and Job Scheduling- Job Creation or Modification - Small (Up to 25 Steps in Job Script)	Per Job Script		CCSU13370050-A	N/A	N/A	A		
Batch and Job Scheduling	Batch and Job Scheduling- Job Creation or Modification - Medium (Up to 50 Steps in Job Script)	Per Job Script		CCSU13370051-A	N/A	N/A	A		
Batch and Job Scheduling	Batch and Job Scheduling- Job Creation or Modification - Large (Up to 100 Steps in Job Script)	Per Job Script		CCSU13370052-A	N/A	N/A	A		
Batch and Job Scheduling	Batch and Job Scheduling- Scheduling and Monitoring - Small (Up to 25 Steps in Job Script)	Per Job Script		CCSU13370053-A	N/A	N/A	A		
Batch and Job Scheduling	Batch and Job Scheduling- Scheduling and Monitoring - Medium (Up to 50 Steps in Job Script)	Per Job Script		CCSU13370054-A	N/A	N/A	A		
Batch and Job Scheduling	Batch and Job Scheduling- Scheduling and Monitoring - Large (Up to 100 Steps in Job Script)	Per Job Script		CCSU13370055-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Batch and Job Scheduling	Batch and Job Scheduling- Scheduling and Monitoring - Small (Up to 25 Steps in Job Script) - Control M Software	Per Job Script		CCSU13370511-A	N/A	N/A	A		
Batch and Job Scheduling	Batch and Job Scheduling- Scheduling and Monitoring - Medium (Up to 50 Steps in Job Script) - Control M Software	Per Job Script		CCSU13370512-A	N/A	N/A	A		
Batch and Job Scheduling	Batch and Job Scheduling- Scheduling and Monitoring - Large (Up to 100 Steps in Job Script) - Control M Software	Per Job Script		CCSU13370513-A	N/A	N/A	A		
Batch and Job Scheduling	AIX Production Batch Operations Support (50,000 jobs per year)	Per Month		CCSI13370056-A	N/A	N/A	A		
Batch and Job Scheduling	IBM Mainframe Production Batch Operations Support (50,000 jobs per year)	Per Month		CCSI13370057-A	N/A	N/A	A		
Service Management	Service Management Custom Report - Small (4 hours to create report)	Per Report		CCSU13370058-A	N/A	N/A	A		
Service Management	Service Management Custom Report - Medium (8 hours to create report)	Per Report		CCSU13370059-A	N/A	N/A	A		
Service Management	Service Management Custom Report - Large (20 hours to create report)	Per Report		CCSU13370060-A	N/A	N/A	A		
Service Management	ITSM Named Licenses - Agency Access to ITSM, license supports 1 user	Per License		CCSU13370061-A	N/A	N/A	A		
Service Management	ITSM Floating Licenses - Agency Access to ITSM, license supports 10 users	Per License		CCSU13370062-A	N/A	N/A	A		
Service Management	Application Mapping (ADDM) Discovery Script Setup - Small	Per Application Discovery Script		CCSU13370063-A	N/A	N/A	A		
Service Management	Application Mapping (ADDM) Discovery Script Setup - Medium	Per Application Discovery Script		CCSU13370064-A	N/A	N/A	A		
Service Management	Application Mapping (ADDM) Discovery Script Setup - Large	Per Application Discovery Script		CCSU13370065-A	N/A	N/A	A		
Service Management	Application Mapping (ADDM) Discovery Script Maintenance - Small	Per Application Discovery Script		CCSU13370066-A	N/A	N/A	A		
Service Management	Application Mapping (ADDM) Discovery Script Maintenance - Medium	Per Application Discovery Script		CCSU13370067-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Service Management	Application Mapping (ADDM) Discovery Script Maintenance - Large	Per Application Discovery Script		CCSU13370068-A	N/A	N/A	A		
Compute Services - Infrastructure Monitoring	Microsoft System Center 2012 (SCOM) - Standard	Per Server		CCSU13370069-A	N/A	N/A	A		
Fully Managed	Fully Managed – Physical – Platinum – Comm/Decomm	Per Server		CCSU13370070-A	N/A	N/A	A		
Fully Managed	Fully Managed – Physical – Gold – Comm/Decomm	Per Server		CCSU13370071-A	N/A	N/A	A		
Fully Managed	Fully Managed – Physical – Silver – Comm/Decomm	Per Server		CCSU13370072-A	N/A	N/A	A		
Fully Managed	Fully Managed – Physical – Bronze – Comm/Decomm	Per Server		CCSU13370073-A	N/A	N/A	A		
Fully Managed	Fully Managed – Physical – Basic – Comm/Decomm	Per Server		CCSU13370074-A	N/A	N/A	A		
Fully Managed	Fully Managed – Virtual – Platinum – Comm/Decomm	Per Server		CCSU13370075-A	N/A	N/A	A		
Fully Managed	Fully Managed – Virtual – Gold – Comm/Decomm	Per Server		CCSU13370076-A	N/A	N/A	A		
Fully Managed	Fully Managed – Virtual – Silver – Comm/Decomm	Per Server		CCSU13370077-A	N/A	N/A	A		
Fully Managed	Fully Managed – Virtual – Bronze – Comm/Decomm	Per Server		CCSU13370078-A	N/A	N/A	A		
Fully Managed	Fully Managed – Virtual – Basic – Comm/Decomm	Per Server		CCSU13370079-A	N/A	N/A	A		
Fully Managed	Platinum AIX Service Level Package	Per Package		CCSI13370080-A	N/A	N/A	A		
Fully Managed	Gold AIX Service Level Package	Per Package		CCSI13370081-A	N/A	N/A	A		
Fully Managed	Disaster Recovery - AIX (271 images)	Per Server		CCSI13370082-A	N/A	N/A	A		
Storage and Backup Service	Archive Services: Archive storage that provides record-level content management and replication to DR	Per GB of Protected Data		CCSU13370083-A	N/A	N/A	A		
Storage and Backup Service	EMC PowerPath Storage Load Balancing S/W for Physical Servers.	Per CPU per Server		CCSU13370085-A	N/A	N/A	A		
Storage and Backup Service	EMC PowerPath Storage Load Balancing S/W forVirtual Server Hosts UNITS : 322 CPUs ESX Virtual Servers	Per Server		CCSU13370086-A	N/A	N/A	A		
Storage and Backup Service	Archive Services: Cost Effective Archive storage with replication to DR.	Per GB of Protected Data		CCSU13370088-A	N/A	N/A	A		
Storage and Backup Service	IBM Storwize V7000 High Performance Tier	Per System	1	CCSI13370558-A	N/A	N/A	A		
Storage and Backup Service	IBM Storwize V7000 Standard Performance Tier	Per System	1	CCSI13370559-A	N/A	N/A	A		
Storage and Backup Service	IBM XIV Standard Performance Tier	Per System	1	CCSI13370560-A	N/A	N/A	A		
Storage and Backup Service	IBM XIV High Performance Tier	Per System	1	CCSI13370561-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Storage and Backup Service	IBM Storwize V7000 Unified NAS Tier	Per System	1	CCSI13370562-A	N/A	N/A	A		
Storage and Backup Service	IBM Standard Rack	Per System	1	CCSI13370563-A	N/A	N/A	A		
Managed Only	Managed Only – Platinum – Comm/Decomm	Per Server		CCSI13370091-A	N/A	N/A	A		
Managed Only	Managed Only – Gold – Comm/Decomm	Per Server		CCSU13370092-A	N/A	N/A	A		
Managed Only	Managed Only – Silver – Comm/Decomm	Per Server		CCSU13370093-A	N/A	N/A	A		
Managed Only	Managed Only – Bronze – Comm/Decomm	Per Server		CCSU13370094-A	N/A	N/A	A		
Managed Only	Managed Only – Basic – Comm/Decomm	Per Server		CCSU13370095-A	N/A	N/A	A		
IBM Mainframe Services	Platinum IBM Mainframe Service Level Package	Per Package		CCSI13370096-A	N/A	N/A	A		
IBM Mainframe Services	Gold IBM Mainframe and i-Series Service Level Package	Per Package		CCSI13370097-A	N/A	N/A	A		
IBM Mainframe Services	DPH IBM Mainframe Services	Per Package		CCSI13370098-A	N/A	N/A	A		
IBM Mainframe Services	Disaster Recovery - Mainframe / i-series (134 images)	Per Package		CCSI13370099-A	N/A	N/A	A		
Unisys Mainframe - Storage and Backup Service	Mainframe Services: EMC RecoverPoint Replication	Per 50 TB of replicated storage		CCSU13370100-A	N/A	N/A	A		
Unisys Mainframe - Storage and Backup Service	Mainframe Services: EMC SRDF Replication	Per 50 TB of replicated storage		CCSU13370101-A	N/A	N/A	A		
Unisys Mainframe Configuration - Add-On Software Run Pack	Unisys Mainframe (ClearPath Dorado) – Config-1 – Run Pack(Add-on software run pack for Config - 1)	Per Config		CCSU13370102-A	N/A	N/A	A		
Unisys Mainframe Configuration - Add-On Software Run Pack	Unisys Mainframe (ClearPath Libra) – Config-2 – Run Pack(Add-on software run pack for Config - 2)	Per Config		CCSU13370103-A	N/A	N/A	A		
Unisys Mainframe Configuration - Add-On Software Run Pack	Unisys Mainframe (ClearPath Dorado) – Config-3 – Run Pack(Add-on software run pack for Config - 3)	Per Config		CCSU13370104-A	N/A	N/A	A		
Unisys Mainframe Configuration - Add-On Software Run Pack	Unisys Mainframe (ClearPath Libra) – Config-4 – Run Pack(Add-on software run pack for Config - 4)	Per Config		CCSU13370105-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Unisys Mainframe Configuration - Exhibit Based Replacement	Unisys Mainframe (ClearPath Dorado) – DPW Production System(Provides technology replacement of DPW mainframe as described in the Exhibits)	Per Config		CCSU13370106-A	N/A	N/A	A		
Unisys Mainframe Configuration - Exhibit Based Replacement	Unisys Mainframe (ClearPath Dorado) – PSP Production System(Provides technology replacement of PSP mainframe as described in the Exhibits)	Per Config		CCSU13370107-A	N/A	N/A	A		
Unisys Mainframe Configuration - Exhibit Based Replacement	Unisys Mainframe (ClearPath Dorado) – DPW/PSP DR(Provides technology replacement of DPW/PSP DR mainframe as described in the Exhibits)	Per Config		CCSU13370108-A	N/A	N/A	A		
Unisys Mainframe Configuration - Exhibit Based Replacement	Unisys Mainframe (ClearPath Libra) – PA Game Production(Provides technology replacement of PA Game Production mainframe as described in the Exhibits)	Per Config		CCSU13370109-A	N/A	N/A	A		
Unisys Mainframe Configuration - Exhibit Based Replacement	Unisys Mainframe (ClearPath Libra) – PA Game Development(Provides technology replacement of PA Game Development mainframe as described in the Exhibits)	Per Config		CCSU13370110-A	N/A	N/A	A		
Unisys Mainframe Configuration - Exhibit Based Replacement	Unisys Mainframe (ClearPath Libra) – PA Game DR(Provides technology replacement of PA Game DR mainframe as described in the Exhibits)	Per Config		CCSU13370111-A	N/A	N/A	A		
Microsoft Cloud Compute Services	Microsoft SharePoint Online Plan 1 (Govt Cloud) - per user monthly subscription	Per User		CCSM13370113-A	N/A	N/A	A		
Microsoft Cloud Compute Services	Microsoft SharePoint Online Plan 2 (Govt Cloud) - per user monthly subscription	Per User		CCSM13370114-A	N/A	N/A	A		
Microsoft Cloud Compute Services	Microsoft Office 365 Plan 1 (Govt Cloud) - per user monthly subscription	Per User		CCSM13370115-A	N/A	N/A	A		
Microsoft Cloud Compute Services	Microsoft Office 365 Plan 3 (Govt Cloud) - per user monthly subscription	Per User		CCSM13370116-A	N/A	N/A	A		
Microsoft Cloud Compute Services	Microsoft Project Server Online (Govt Cloud) - per user monthly subscription	Per User		CCSM13370117-A	N/A	N/A	A		
Microsoft Cloud Compute Services	Microsoft Project Server Online w/ Project Pro (Govt Cloud) - per user monthly subscription	Per User		CCSM13370118-A	N/A	N/A	A		
Microsoft Cloud Compute Services	Microsoft Dynamics CRM Online - per user monthly subscription	Per User		CCSM13370119-A	N/A	N/A	A		
Microsoft Cloud Compute Services	Microsoft Compute Svr VM - 1 Core-1.75GB RAM-2x1TB Disk Storage Non-Windows OS 1	Per Server for 100 Hours		CCSM13370120-A	N/A	N/A	A		
Microsoft Cloud Compute Services	Microsoft Compute Svr VM - 1 Core-1.75GB RAM-2x1TB Disk Storage Windows OS 1	Per Server for 100 Hours		CCSM13370121-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Microsoft Cloud Compute Services	Microsoft Hi Mem Compute Svr VM- 4 Core-28GB RAM-8x1TB Disk Storage Non-Windows OS	Per Server for 100 Hours		CCSM13370122-A	N/A	N/A	A		
Microsoft Cloud Compute Services	Microsoft Hi Mem Compute Svr VM - 4 Core-28GB RAM-8x1TB Disk Storage Windows OS	Per Server for 100 Hours		CCSM13370123-A	N/A	N/A	A		
Microsoft Cloud Compute Services	Microsoft Hi Mem Compute Svr VM - 8 Core-56GB RAM-16x1TB Disk Storage Non-Windows OS	Per Server for 100 Hours		CCSM13370124-A	N/A	N/A	A		
Microsoft Cloud Compute Services	Microsoft Hi Mem Compute Svr VM - 8 Core-56GB RAM-16x1TB Disk Storage Windows OS	Per Server for 100 Hours		CCSM13370125-A	N/A	N/A	A		
Microsoft Cloud Compute Services	Microsoft Hi Mem Compute Svr - 4 Core-28GB RAM-Cloud Services	Per Server for 100 Hours		CCSM13370126-A	N/A	N/A	A		
Microsoft Cloud Compute Services	Microsoft Hi Mem Compute Svr - 8 Core-56GB RAM-Cloud Services	Per Server for 100 Hours		CCSM13370127-A	N/A	N/A	A		
Microsoft Cloud Compute Services	Microsoft Azure Storage Geo Redundancy 100 GB	Per Month		CCSM13370128-A	N/A	N/A	A		
Microsoft Cloud Compute Services	Microsoft Azure Storage Local Redundancy 100 GB	Per Month		CCSM13370129-A	N/A	N/A	A		
Microsoft Cloud Compute Services	Microsoft Azure Backup Service 10 GB	Per Month		CCSM13370130-A	N/A	N/A	A		
Microsoft Cloud Compute Services	Office 365 Migration Service	Per Month		CCSM13370131-A	N/A	N/A	A		
Microsoft Cloud Compute Services	Office 365 Migration Tool	Per User		CCSM13370132-A	N/A	N/A	A		
Microsoft Cloud Compute Services	Office 365 Management Service	Per Month		CCSM13370133-A	N/A	N/A	A		
Microsoft Cloud Compute Services	Microsoft Sharepoint Online Migration	Per Month		CCSM13370134-A	N/A	N/A	A		
Microsoft Cloud Compute Services	Microsoft Sharepoint Management Service	Per Month		CCSM13370135-A	N/A	N/A	A		
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Dedicated Cloud - Base Service	Per Month		CCSV13370136-A	N/A	N/A	A		
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Dedicated Cloud - Compute add-on (1 additional)	Per Month		CCSV13370137-A	N/A	N/A	A		
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Dedicated Cloud - Compute add-on (2-3 additional)	Per Month		CCSV13370138-A	N/A	N/A	A		
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Dedicated Cloud - Compute add-on (4-5 additional)	Per Month		CCSV13370139-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Dedicated Cloud - Compute add-on (6-7 additional)	Per Month		CCSV13370140-A	N/A	N/A	A		
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Dedicated Cloud - Compute add-on (8+ additional)	Per Month		CCSV13370141-A	N/A	N/A	A		
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Dedicated Cloud - Support add-on (1 additional)	Per Month		CCSV13370142-A	N/A	N/A	A		
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Dedicated Cloud - Support add-on (2-3 additional)	Per Month		CCSV13370143-A	N/A	N/A	A		
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Dedicated Cloud - Support add-on (4-5 additional)	Per Month		CCSV13370144-A	N/A	N/A	A		
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Dedicated Cloud - Support add-on (6-7 additional)	Per Month		CCSV13370145-A	N/A	N/A	A		
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Dedicated Cloud - Support add-on (8+ additional)	Per Month		CCSV13370146-A	N/A	N/A	A		
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Dedicated Cloud - Storage add-on (1 additional)	Per Month		CCSV13370147-A	N/A	N/A	A		
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Dedicated Cloud - Storage add-on (2-3 additional)	Per Month		CCSV13370148-A	N/A	N/A	A		
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Dedicated Cloud - Storage add-on (4-5 additional)	Per Month		CCSV13370149-A	N/A	N/A	A		
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Dedicated Cloud - Storage add-on (6+ additional)	Per Month		CCSV13370150-A	N/A	N/A	A		
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Dedicated Cloud - Bandwidth add-on	Per Month		CCSV13370151-A	N/A	N/A	A		
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Dedicated Cloud - Public IP add-on	Per Month		CCSV13370152-A	N/A	N/A	A		
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Virtual Cloud - Base Service	Per Month		CCSV13370153-A	N/A	N/A	A		
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Virtual Cloud - Compute add-on (1-5 additional)	Per Month		CCSV13370154-A	N/A	N/A	A		
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Virtual Cloud - Compute add-on (6-11 additional)	Per Month		CCSV13370155-A	N/A	N/A	A		
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Virtual Cloud - Compute add-on (12-17 additional)	Per Month		CCSV13370156-A	N/A	N/A	A		
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Virtual Cloud - Compute add-on (18-23 additional)	Per Month		CCSV13370157-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Virtual Cloud - Compute add-on (24+ additional)	Per Month		CCSV13370158-A	N/A	N/A	A		
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Virtual Cloud - Support add-on (1-5 additional)	Per Month		CCSV13370159-A	N/A	N/A	A		
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Virtual Cloud - Support add-on (6-11 additional)	Per Month		CCSV13370160-A	N/A	N/A	A		
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Virtual Cloud - Support add-on (12-17 additional)	Per Month		CCSV13370161-A	N/A	N/A	A		
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Virtual Cloud - Support add-on (18-23 additional)	Per Month		CCSV13370162-A	N/A	N/A	A		
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Virtual Cloud - Support add-on (24+ additional)	Per Month		CCSV13370163-A	N/A	N/A	A		
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Virtual Cloud - Storage add-on (1-5 additional)	Per Month		CCSV13370164-A	N/A	N/A	A		
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Virtual Cloud - Storage add-on (6-11 additional)	Per Month		CCSV13370165-A	N/A	N/A	A		
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Virtual Cloud - Storage add-on (12-17 additional)	Per Month		CCSV13370166-A	N/A	N/A	A		
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Virtual Cloud - Storage add-on (18+ additional)	Per Month		CCSV13370167-A	N/A	N/A	A		
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Virtual Cloud - Bandwidth add-on	Per Month		CCSV13370168-A	N/A	N/A	A		
VMWare Hybrid Cloud Compute Services	VMWare vCloud Hybrid Service - Virtual Cloud - Public IP add-on	Per Month		CCSV13370169-A	N/A	N/A	A		
Identity and Access Management Service	Active Directory Support - Small	Per Month		CCSU13370170-A	N/A	N/A	A		
Identity and Access Management Service	Active Directory Support - Medium	Per Month		CCSU13370171-A	N/A	N/A	A		
Identity and Access Management Service	Active Directory Support - Large	Per Month		CCSU13370172-A	N/A	N/A	A		
Identity and Access Management Service	Active Directory Support - Very Large	Per Month		CCSU13370173-A	N/A	N/A	A		
Identity and Access Management Service	PKI Support - Small	Per Month		CCSU13370174-A	N/A	N/A	A		
Identity and Access Management Service	PKI Support - Medium	Per Month		CCSU13370175-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Identity and Access Management Service	PKI Support - Large	Per Month		CCSU13370176-A	N/A	N/A	A		
Business Continuity and Disaster Recovery	Development of Data Center Disaster Recovery Plan	Per Plan		CCSI13370177-A	N/A	N/A	A		
Business Continuity and Disaster Recovery	Business Impact Assessment Workshop	Per Workshop		CCSI13370178-A	N/A	N/A	A		
Business Continuity and Disaster Recovery	Resilient Strategy Development Workshop	Per Workshop		CCSI13370179-A	N/A	N/A	A		
Business Continuity and Disaster Recovery	Labor for Tier 3 to Tier 6 DR Service Testing (Disk-based)	Per Server		CCSU13370180-A	N/A	N/A	A		
Business Continuity and Disaster Recovery	Labor for Tier 1 & Tier 2 DR Service Testing (Tape-based)	Per Server		CCSU13370181-A	N/A	N/A	A		
Business Continuity and Disaster Recovery	DR Config-1 Storage	Per GB		CCSU13370182-A	N/A	N/A	A		
Business Continuity and Disaster Recovery	DR Config-2 Storage	Per GB		CCSU13370183-A	N/A	N/A	A		
Business Continuity and Disaster Recovery	Tape Library Resources to 100,000 GB to Tier1 DR RTO	Per GB of Protected Data		CCSU13370184-A	N/A	N/A	A		
Business Continuity and Disaster Recovery	Tape Library Resources to 100,000 GB to Tier2 DR RTO	Per GB of Protected Data		CCSU13370185-A	N/A	N/A	A		
Business Continuity and Disaster Recovery	Backup to Disk for 255,000 GBs of deduplicated data	Per Gb of Protected Data		CCSU13370186-A	N/A	N/A	A		
Business Continuity and Disaster Recovery	Mainframe Services: EMC RecoverPoint Data Replication for 27,000 GBs of VMAX10K Storage	Per GB of Replicated Data		CCSU13370187-A	N/A	N/A	A		
Business Continuity and Disaster Recovery	EMC RecoverPoint SnapShot & Replication for 32,256 GBs of Config2 Storage	Per GB of Replicated Data		CCSU13370188-A	N/A	N/A	A		
Business Continuity and Disaster Recovery	EMC RecoverPoint SnapShot & Replication for 84,700 GBs of Config1 Storage	Per GB of Replicated Data		CCSU13370189-A	N/A	N/A	A		
Business Continuity and Disaster Recovery	Mainframe Services: EMC SRDF Data Replication for 50,000 GB of VMAX Storage	Per GB of Replicated Data		CCSU13370190-A	N/A	N/A	A		
Business Continuity and Disaster Recovery	Open Systems Services: EMC VPlex Metro Replication for 150,000 GBs	Per GB of Replicated Data		CCSU13370192-A	N/A	N/A	A		
Business Continuity and Disaster Recovery	SAN Switch Port, purchased in pairs, for SAN-attached Servers	Per SAN Port		CCSU13370193-A	N/A	N/A	A		
Business Continuity and Disaster Recovery	IBM Storwize V7000 Disaster Recovery System	Per System	1	CCSI13370564-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Business Continuity and Disaster Recovery	IBM XIV High Performance Disaster Recovery Tier	Per System	1	CCSI13370565-A	N/A	N/A	A		
Application Performance Monitoring Services	Application Performance Monitoring Service - Setup – Small	Per Application		CCSU13370194-A	N/A	N/A	A		
Application Performance Monitoring Services	Application Performance Monitoring Service - Setup – Medium	Per Application		CCSU13370195-A	N/A	N/A	A		
Application Performance Monitoring Services	Application Performance Monitoring Service - Setup - Large	Per Application		CCSU13370196-A	N/A	N/A	A		
Application Performance Monitoring Services	Application Performance Monitoring Service - Ongoing Support – Small	Per Application		CCSU13370197-A	N/A	N/A	A		
Application Performance Monitoring Services	Application Performance Monitoring Service - Ongoing Support – Medium	Per Application		CCSU13370198-A	N/A	N/A	A		
Application Performance Monitoring Services	Application Performance Monitoring Service - Ongoing Support - Large	Per Application		CCSU13370199-A	N/A	N/A	A		
Application Capacity Management Services	Application Capacity Management - Setup – Small	Per Application		CCSU13370200-A	N/A	N/A	A		
Application Capacity Management Services	Application Capacity Management - Setup – Medium	Per Application		CCSU13370201-A	N/A	N/A	A		
Application Capacity Management Services	Application Capacity Management – Setup - Large	Per Application		CCSU13370202-A	N/A	N/A	A		
Application Capacity Management Services	Application Capacity Management - Ongoing Support – Small	Per Application		CCSU13370203-A	N/A	N/A	A		
Application Capacity Management Services	Application Capacity Management - Ongoing Support – Medium	Per Application		CCSU13370204-A	N/A	N/A	A		
Application Capacity Management Services	Application Capacity Management – Ongoing Support - Large	Per Application		CCSU13370205-A	N/A	N/A	A		
Application Capacity Management Services	Application Capacity Management - Appdynamics Agent License – Small	Per Application		CCSU13370555-A	N/A	N/A	A		
Application Capacity Management Services	Application Capacity Management - Appdynamics Agent License – Medium	Per Application		CCSU13370556-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Application Capacity Management Services	Application Capacity Management – Appdynamics Agent License - Large	Per Application		CCSU13370557-A	N/A	N/A	A		
Application Architecture	Review Application Architecture - Small	Per Assessment		CCSD13370206-A	N/A	N/A	A		
Application Architecture	Review Application Architecture - Medium	Per Assessment		CCSD13370207-A	N/A	N/A	A		
Application Architecture	Review Application Architecture - Large	Per Assessment		CCSD13370208-A	N/A	N/A	A		
Application Assessment	Application Performance Impact Assessment (Follow-on for 5 applications)	Per Assessment		CCSI13370209-A	N/A	N/A	A		
Application Assessment	Open System Database Performance Assessment - Small (Up to 100 objects)	Per Assessment		CCSD13370210-A	N/A	N/A	A		
Application Assessment	Open System Database Performance Assessment - Medium (Up to 500 objects)	Per Assessment		CCSD13370211-A	N/A	N/A	A		
Application Assessment	Open System Database Performance Assessment - Large (Up to 1,000 objects)	Per Assessment		CCSD13370212-A	N/A	N/A	A		
Application Assessment	Open System Configuration Management Assessment - Small (Up to 10 Application Pages)	Per Assessment		CCSD13370213-A	N/A	N/A	A		
Application Assessment	Open System Configuration Management Assessment - Medium (Up to 25 Application Pages)	Per Assessment		CCSD13370214-A	N/A	N/A	A		
Application Assessment	Open System Configuration Management Assessment - Small (Up to 50 Application Pages)	Per Assessment		CCSD13370215-A	N/A	N/A	A		
Application Assessment	Mobile Wireframe Assessment - Small (Up to 10 Pages)	Per Assessment		CCSD13370216-A	N/A	N/A	A		
Application Assessment	Mobile Wireframe Assessment - Medium (Up to 25 Pages)	Per Assessment		CCSD13370217-A	N/A	N/A	A		
Application Assessment	Mobile Wireframe Assessment - Small (Up to 50 Pages)	Per Assessment		CCSD13370218-A	N/A	N/A	A		
Application Assessment	Application Management Innovation Workshop	Per Workshop		CCSU13370219-A	N/A	N/A	A		
Application Assessment	Application Modernization Assessment - 1 Week	Per Assessment		CCSU13370220-A	N/A	N/A	A		
Application Assessment	Application Modernization Assessment - 4 Week	Per Assessment		CCSU13370221-A	N/A	N/A	A		
Application Testing Services	Test Assessment	Per Assessment		CCSD13370222-A	N/A	N/A	A		
Application Testing Services	Test Estimation and Test Approach Planning	Per Assessment		CCSD13370223-A	N/A	N/A	A		
Application Testing Services	System Integration and Acceptance Testing, UAT Support - Small	Per Request		CCSD13370224-A	N/A	N/A	A		
Application Testing Services	System Integration and Acceptance Testing, UAT Support - Medium	Per Request		CCSD13370225-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Application Testing Services	System Integration and Acceptance Testing, UAT Support - Large	Per Request		CCSD13370226-A	N/A	N/A	A		
Application Testing Services	Automated Regression Testing - Small	Per Request		CCSD13370227-A	N/A	N/A	A		
Application Testing Services	Automated Regression Testing - Medium	Per Request		CCSD13370228-A	N/A	N/A	A		
Application Testing Services	Automated Regresion Testing - Large	Per Request		CCSD13370229-A	N/A	N/A	A		
Application Testing Services	Test Data Management - Small	Per Request		CCSD13370230-A	N/A	N/A	A		
Application Testing Services	Test Data Management - Medium	Per Request		CCSD13370231-A	N/A	N/A	A		
Application Testing Services	Test Data Management - Large	Per Request		CCSD13370232-A	N/A	N/A	A		
Application Testing Services	ADA Compliance Testing - Small	Per Request		CCSD13370233-A	N/A	N/A	A		
Application Testing Services	ADA Compliance Testing - Medium	Per Request		CCSD13370234-A	N/A	N/A	A		
Application Testing Services	ADA Compliance Testing - Large	Per Request		CCSD13370235-A	N/A	N/A	A		
Application Load/Availability Testing	Application Load Testing - Script Creation - Small (Up to 20 Application Pages)	Per Script		CCSD13370236-A	N/A	N/A	A		
Application Load/Availability Testing	Application Load Testing - Script Creation - Medium (Up to 50 Application Pages)	Per Script		CCSD13370237-A	N/A	N/A	A		
Application Load/Availability Testing	Application Load Testing - Script Creation - Large (Up to 100 Application Pages)	Per Script		CCSD13370238-A	N/A	N/A	A		
Application Load/Availability Testing	Application Load Testing - Script Maintenance - Small (Up to 10 of Application Pages)	Per Script		CCSD13370239-A	N/A	N/A	A		
Application Load/Availability Testing	Application Load Testing - Script Maintenance - Medium (Up To 25 of Application Pages)	Per Script		CCSD13370240-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Application Load/Availability Testing	Application Load Testing - Script Maintenance - Large (Up to 50 Application Pages)	Per Script		CCSD13370241-A	N/A	N/A	A		
Application Load/Availability Testing	Application Load Testing - Execution and Analysis - Small (Up to 25 Application Test Scripts)	Per Test		CCSD13370242-A	N/A	N/A	A		
Application Load/Availability Testing	Application Load Testing - Execution and Analysis - Medium (Up to 50 Application Test Scripts)	Per Test		CCSD13370243-A	N/A	N/A	A		
Application Load/Availability Testing	Application Load Testing - Execution and Analysis - Large (100 Application Test Scripts)	Per Test		CCSD13370244-A	N/A	N/A	A		
Application Load/Availability Testing	Synthetic Transaction Modeling - Small	Per Test		CCSD13370245-A	N/A	N/A	A		
Application Load/Availability Testing	Synthetic Transaction Modeling - Medium	Per Test		CCSD13370246-A	N/A	N/A	A		
Application Load/Availability Testing	Synthetic Transaction Modeling - Large	Per Test		CCSD13370247-A	N/A	N/A	A		
Application Migration Services	Enterprise Application Transition Strategy - Small	Per Assessment		CCSD13370248-A	N/A	N/A	A		
Application Migration Services	Enterprise Application Transition Strategy - Medium	Per Assessment		CCSD13370249-A	N/A	N/A	A		
Application Migration Services	Enterprise Application Transition Strategy - Large	Per Assessment		CCSD13370250-A	N/A	N/A	A		
Application Migration Services	Enterprise Application Transition Strategy - Very Large	Per Assessment		CCSD13370251-A	N/A	N/A	A		
Application Migration Services	Application Migration Plan - Small	Per Migration Plan		CCSD13370252-A	N/A	N/A	A		
Application Migration Services	Application Migration Plan - Medium	Per Migration Plan		CCSD13370253-A	N/A	N/A	A		
Application Migration Services	Application Migration Plan - Large	Per Migration Plan		CCSD13370254-A	N/A	N/A	A		
Middleware Service	WebSphere Build p-Series Standard (1 server)	Per Request		CCSI13370255-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Middleware Service	WebSphere Build p-Series Complex (2 servers)	Per Request		CCSI13370256-A	N/A	N/A	A		
Middleware Service	WebSphere Upgrade p-Series Standard (1 server)	Per Request		CCSI13370257-A	N/A	N/A	A		
Middleware Service	WebSphere Upgrade p-Series Complex (2 servers)	Per Request		CCSI13370258-A	N/A	N/A	A		
Middleware Service	DataPower Quickstart Services	Per Request		CCSI13370259-A	N/A	N/A	A		
Middleware Service	p-Series Support for WebSphere App Server (10 Instances)	Per Month		CCSI13370260-A	N/A	N/A	A		
Middleware Service	p-Series Support for WebSphere App Server (25 Instances)	Per Month		CCSI13370261-A	N/A	N/A	A		
Middleware Service	p-Series Support for WebSphere App Server (40 Instances)	Per Month		CCSI13370262-A	N/A	N/A	A		
Middleware Service	p-Series Support for WebSphere MQ Queue Managers (40 Instances)	Per Month		CCSI13370263-A	N/A	N/A	A		
Middleware Service	p-Series Support for WebSphere MQ Queue Managers (80 Instances)	Per Month		CCSI13370264-A	N/A	N/A	A		
Middleware Service	p-Series Support for WebSphere MQ Queue Managers (120 Instances)	Per Month		CCSI13370265-A	N/A	N/A	A		
Middleware Service	WebSphere Build z-Series Standard (1 subsystem without data sharing or clustering)	Per Month		CCSI13370266-A	N/A	N/A	A		
Middleware Service	WebSphere Build z-Series Complex (2 subsystems with data sharing and clustering across multiple CECs)	Per Month		CCSI13370267-A	N/A	N/A	A		
Middleware Service	WebSphere Upgrade z-Series Standard (1 subsystem without data sharing or clustering)	Per Request		CCSI13370268-A	N/A	N/A	A		
Middleware Service	WebSphere Upgrade z-Series Complex (2 subsystems with data sharing and clustering across multiple CECs)	Per Request		CCSI13370269-A	N/A	N/A	A		
Middleware Service	z-Series Support for WebSphere App Server (10 Instances)	Per Month		CCSI13370272-A	N/A	N/A	A		
Middleware Service	z-Series Support for WebSphere App Server (25 Instances)	Per Month		CCSI13370273-A	N/A	N/A	A		
Middleware Service	z-Series Support for WebSphere App Server (40 Instances)	Per Month		CCSI13370274-A	N/A	N/A	A		
Middleware Service	z-Series Support for WebSphere MQ Queue Managers (40 Queue Managers)	Per Month		CCSI13370275-A	N/A	N/A	A		
Middleware Service	z-Series Support for WebSphere MQ Queue Managers (80 Queue Managers)	Per Month		CCSI13370276-A	N/A	N/A	A		
Middleware Service	z-Series Support for WebSphere MQ Queue Managers (120 Queue Managers)	Per Month		CCSI13370277-A	N/A	N/A	A		
Application User Experience	User Experience Strategy - Small	Per Request		CCSD13370278-A	N/A	N/A	A		
Application User Experience	User Experience Strategy - Medium	Per Request		CCSD13370279-A	N/A	N/A	A		
Application User Experience	User Experience Strategy - Large	Per Request		CCSD13370280-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Application User Experience	User Experience Design - Small	Per Request		CCSD13370281-A	N/A	N/A	A		
Application User Experience	User Experience Design - Medium	Per Request		CCSD13370282-A	N/A	N/A	A		
Application User Experience	User Experience Design - Large	Per Request		CCSD13370283-A	N/A	N/A	A		
Application User Experience	User Experience Prototype Development - Small	Per Request		CCSD13370284-A	N/A	N/A	A		
Application User Experience	User Experience Prototype Development - Medium	Per Request		CCSD13370285-A	N/A	N/A	A		
Application User Experience	User Experience Prototype Development - Large	Per Request		CCSD13370286-A	N/A	N/A	A		
Data Quality Management	Data Quality Management Assessment - Small	Per Assessment		CCSD13370287-A	N/A	N/A	A		
Data Quality Management	Data Quality Management Assessment - Medium	Per Assessment		CCSD13370288-A	N/A	N/A	A		
Data Quality Management	Data Quality Management Assessment - Large	Per Assessment		CCSD13370289-A	N/A	N/A	A		
Data Quality Management	Data Quality Management Assessment - Very Large	Per Assessment		CCSD13370290-A	N/A	N/A	A		
Information Management Strategy	Information Management Strategy - Small	Per Assessment		CCSD13370291-A	N/A	N/A	A		
Information Management Strategy	Information Management Strategy - Medium	Per Assessment		CCSD13370292-A	N/A	N/A	A		
Information Management Strategy	Information Management Strategy - Large	Per Assessment		CCSD13370293-A	N/A	N/A	A		
Information Management Strategy	Information Management Strategy - Very Large	Per Assessment		CCSD13370294-A	N/A	N/A	A		
Information Management Strategy	Information Management Full Implementation Lifecycle - Small	Per Assessment		CCSD13370295-A	N/A	N/A	A		
Information Management Strategy	Information Management Full Implementation Lifecycle - Medium	Per Assessment		CCSD13370296-A	N/A	N/A	A		
Information Management Strategy	Information Management Full Implementation Lifecycle - Large	Per Assessment		CCSD13370297-A	N/A	N/A	A		
Information Management Strategy	Information Management Full Implementation Lifecycle - Very Large	Per Assessment		CCSD13370298-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
ERP Services	ERP Fit/Gap Analysis (4 week duration)	Per Assessment		CCSD13370299-A	N/A	N/A	A		
ERP Services	ERP Product Selection	Per Assessment		CCSD13370300-A	N/A	N/A	A		
ERP Services	ERP Security Review and Segregation of Duties Analysis - Small (Up to 25 users and roles)	Per Assessment		CCSD13370302-A	N/A	N/A	A		
ERP Services	ERP Security Review and Segregation of Duties Analysis - Small (Up to 100 users and roles)	Per Assessment		CCSD13370303-A	N/A	N/A	A		
ERP Services	ERP Security Review and Segregation of Duties Analysis - Small (Up to 500 users and roles)	Per Assessment		CCSD13370304-A	N/A	N/A	A		
ERP Services	ERP Governance Risk, and Compliance (GRC) Review - Small (Agency System Configuration and Parameters for 1 GRC Capability)	Per Assessment		CCSD13370305-A	N/A	N/A	A		
ERP Services	ERP Governance Risk, and Compliance (GRC) Review - Medium (Agency System Configuration and Parameters for 3 GRC Capability)	Per Assessment		CCSD13370306-A	N/A	N/A	A		
ERP Services	ERP Governance Risk, and Compliance (GRC) Review - Large (Agency System Configuration and Parameters for 5 GRC Capability)	Per Assessment		CCSD13370307-A	N/A	N/A	A		
Communications Strategy	Stakeholder Analysis	Per Assessment		CCSD13370308-A	N/A	N/A	A		
Communications Strategy	Communications Plan	Per Request		CCSD13370309-A	N/A	N/A	A		
Communications Strategy	Communications Delivery	Per Request		CCSD13370310-A	N/A	N/A	A		
Infrastructure Virtualization and Migration Services	Cirba Software for Application and Infrastructure Mapping	Per Server Instance		CCSU13370311-A	N/A	N/A	A		
Infrastructure Virtualization and Migration Services	Application and Infrastructure Mapping with CIRBA	Per Request		CCSU13370312-A	N/A	N/A	A		
Infrastructure Virtualization and Migration Services	Application and Infrastructure Mapping and Consolidation Planning with CIRBA	Per Day/Week		CCSU13370313-A	N/A	N/A	A		
Data Center Facility Services	Security Cage - EDC - Small	Per Cage		CCSU13370501-A	N/A	N/A	A		
Data Center Facility Services	Security Cage - EDC - Medium	Per Cage		CCSU13370502-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Data Center Facility Services	Security Cage - EDC - Large	Per Cage		CCSU13370503-A	N/A	N/A	A		
Data Center Facility Services	Security Cage - EDC - Very Large	Per Cage		CCSU13370504-A	N/A	N/A	A		
Data Center Facility Services	Security Cage - [redacted] - Small	Per Cage		CCSU13370314-A	N/A	N/A	A		
Data Center Facility Services	Security Cage - [redacted] - Medium	Per Cage		CCSU13370315-A	N/A	N/A	A		
Data Center Facility Services	Security Cage - [redacted] - Large	Per Cage		CCSU13370316-A	N/A	N/A	A		
Data Center Facility Services	Security Cage - [redacted] - Very Large	Per Cage		CCSU13370317-A	N/A	N/A	A		
Data Center Facility Services	Security Cage - [redacted] - Small	Per Cage		CCSU13370318-A	N/A	N/A	A		
Data Center Facility Services	Security Cage - [redacted] - Medium	Per Cage		CCSU13370319-A	N/A	N/A	A		
Data Center Facility Services	Security Cage - [redacted] - Large	Per Cage		CCSU13370320-A	N/A	N/A	A		
Data Center Facility Services	Security Cage - [redacted] - Very Large	Per Cage		CCSU13370321-A	N/A	N/A	A		
Data Center Facility Services	Security Cage - EDC - Small - Setup	Per Cage		CCSU13370514-A	N/A	N/A	A		
Data Center Facility Services	Security Cage - EDC - Medium - Setup	Per Cage		CCSU13370515-A	N/A	N/A	A		
Data Center Facility Services	Security Cage - EDC - Large - Setup	Per Cage		CCSU13370516-A	N/A	N/A	A		
Data Center Facility Services	Security Cage - EDC - Very Large - Setup	Per Cage		CCSU13370517-A	N/A	N/A	A		
Data Center Facility Services	Security Cage - [redacted] - Small - Setup	Per Cage		CCSU13370518-A	N/A	N/A	A		
Data Center Facility Services	Security Cage - [redacted] - Medium - Setup	Per Cage		CCSU13370519-A	N/A	N/A	A		
Data Center Facility Services	Security Cage - [redacted] - Large - Setup	Per Cage		CCSU13370520-A	N/A	N/A	A		
Data Center Facility Services	Security Cage - [redacted] - Very Large - Setup	Per Cage		CCSU13370521-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Data Center Facility Services	Security Cage - [redacted] - Small - Setup	Per Cage		CCSU13370522-A	N/A	N/A	A		
Data Center Facility Services	Security Cage - [redacted] - Medium - Setup	Per Cage		CCSU13370523-A	N/A	N/A	A		
Data Center Facility Services	Security Cage - [redacted] - Large - Setup	Per Cage		CCSU13370524-A	N/A	N/A	A		
Data Center Facility Services	Security Cage - [redacted] - Very Large - setup	Per Cage		CCSU13370525-A	N/A	N/A	A		
Data Center Facility Services	Enclosed Network Security Conduit	Per Foot		CCSU13370322-A	N/A	N/A	A		
Data Center Facility Services	Enclosed Security Cable Tray	Per Foot		CCSU13370323-A	N/A	N/A	A		
Data Center Facility Services	Security Camera	Per Camera		CCSU13370324-A	N/A	N/A	A		
Data Center Facility Services	Access Control Panel	Per Panel		CCSU13370325-A	N/A	N/A	A		
Data Center Facility Services	Security Cabinet	Per Cabinet		CCSU13370326-A	N/A	N/A	A		
Data Center Relocation Services	Lift and Ship of Server Hardware	Per Server		CCSU13370327-A	N/A	N/A	A		
Data Center Relocation Services	Data Center Relocation Services	Per Request		CCSI13370328-A	N/A	N/A	A		
Data Center Relocation Services	Transition Tools: EMC RecoverPoint Solution for migrations for 10,000 GB of SAN-attached Storage	Per GB		CCSU13370329-A	N/A	N/A	A		
Network and Security Service	IPV6 Strategy	Per Assessment		CCSP13370330-A	N/A	N/A	A		
Network and Security Service	LAN Switch install for new Managed Racks	Per Rack		CCSU13370331-A	N/A	N/A	A		
Network and Security Service	VPN Planning - Business Partner	Per VPN Request		CCSU13370332-A	N/A	N/A	A		
Network and Security Service	VPN Implementation - Business Partner	Per VPN Request		CCSU13370333-A	N/A	N/A	A		
Network and Security Service	VPN Modification - Business Partner	Per VPN Request		CCSU13370334-A	N/A	N/A	A		
Network and Security Service	VPN Decommission - Business Partner	Per VPN Request		CCSU13370335-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Network and Security Service	VPN Planning - Agency	Per VPN Request		CCSU13370336-A	N/A	N/A	A		
Network and Security Service	VPN Implementation - Agency	Per VPN Request		CCSU13370337-A	N/A	N/A	A		
Network and Security Service	VPN Modification - Agency	Per VPN Request		CCSU13370338-A	N/A	N/A	A		
Network and Security Service	VPN Decommission- Agency	Per VPN Request		CCSU13370339-A	N/A	N/A	A		
Network and Security Service	Hardware Network Load Balancer - Design and Implement - Small	Per Request		CCSU13370340-A	N/A	N/A	A		
Network and Security Service	Hardware Network Load Balancer - Design and Implement - Medium	Per Request		CCSU13370341-A	N/A	N/A	A		
Network and Security Service	Hardware Network Load Balancer - Design and Implement - Large	Per Request		CCSU13370342-A	N/A	N/A	A		
Network and Security Service	Hardware Network Load Balancer - Modify - Small	Per Request		CCSU13370343-A	N/A	N/A	A		
Network and Security Service	Hardware Network Load Balancer - Modify - Medium	Per Request		CCSU13370344-A	N/A	N/A	A		
Network and Security Service	Hardware Network Load Balancer - Modify - Large	Per Request		CCSU13370345-A	N/A	N/A	A		
Network and Security Service	SSL Offloading on Network Load Balancer - Design and Implement	Per Request		CCSU13370346-A	N/A	N/A	A		
Network and Security Service	SSL Offloading on Network Load Balancer - Modify	Per Request		CCSU13370349-A	N/A	N/A	A		
Network and Security Service	Multi-Site Global Network Load Balancer - Design and Implement - Small	Per Request		CCSU13370352-A	N/A	N/A	A		
Network and Security Service	Multi-Site Global Network Load Balancer - Design and Implement - Medium	Per Request		CCSU13370353-A	N/A	N/A	A		
Network and Security Service	Multi-Site Global Network Load Balancer - Design and Implement - Large	Per Request		CCSU13370354-A	N/A	N/A	A		
Network and Security Service	Multi-Site Global Network Load Balancer - Modify - Small	Per Request		CCSU13370355-A	N/A	N/A	A		
Network and Security Service	Multi-Site Global Network Load Balancer - Modify - Medium	Per Request		CCSU13370356-A	N/A	N/A	A		
Network and Security Service	Multi-Site Global Network Load Balancer - Modify - Large	Per Request		CCSU13370357-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Network and Security Service	Reverse Proxy - Design & Implement - Proxy Platform - Small	Per Proxy		CCSU13370358-A	N/A	N/A	A		
Network and Security Service	Reverse Proxy - Design & Implement - Proxy Platform - Medium	Per Proxy		CCSU13370359-A	N/A	N/A	A		
Network and Security Service	Reverse Proxy - Design & Implement - Proxy Platform - Large	Per Proxy		CCSU13370360-A	N/A	N/A	A		
Network and Security Service	Reverse Proxy - Design & Implement - Application Service - Small	Per Request		CCSU13370361-A	N/A	N/A	A		
Network and Security Service	Reverse Proxy - Design & Implement - Application Service - Medium	Per Request		CCSU13370362-A	N/A	N/A	A		
Network and Security Service	Reverse Proxy - Design & Implement - Application Service - Large	Per Request		CCSU13370363-A	N/A	N/A	A		
Network and Security Service	Reverse Proxy - Modify - Application Service - Small	Per Request		CCSU13370364-A	N/A	N/A	A		
Network and Security Service	Reverse Proxy - Modify - Application Service - Medium	Per Request		CCSU13370365-A	N/A	N/A	A		
Network and Security Service	Reverse Proxy - Modify - Application Service - Large	Per Request		CCSU13370366-A	N/A	N/A	A		
Network and Security Service	Stealth Starter Plan (2 week)	Per Request		CCSU13370367-A	N/A	N/A	A		
Network and Security Service	Stealth Secure Virtual Terminal (SSVT) Started Plan Add-On (2 week)	Per Request		CCSU13370368-A	N/A	N/A	A		
Network and Security Service	Stealth Service - Discovery	Per Engagement		CCSU13370369-A	N/A	N/A	A		
Network and Security Service	Stealth Service - Design	Per Engagement		CCSU13370370-A	N/A	N/A	A		
Network and Security Service	Stealth Service - Deployment	Per Engagement		CCSU13370371-A	N/A	N/A	A		
Network and Security Service	Stealth Network Appliance (1000 Licenses, 300 Mbps)	Per Appliance		CCSU13370372-A	N/A	N/A	A		
Network and Security Service	Stealth Network Appliance (1000 Licenses, 800 Mbps)	Per Appliance		CCSU13370373-A	N/A	N/A	A		
Network and Security Service	Stealth Network Appliance (RPS, 1 Gbps)	Per Appliance		CCSU13370374-A	N/A	N/A	A		
Network and Security Service	Stealth Network Appliance (1000 Licenses, 300 Mbps) - Annual Maintenance	Per Appliance		CCSU13370526-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Network and Security Service	Stealth Network Appliance (1000 Licenses, 800 Mbps) - Annual Maintenance	Per Appliance		CCSU13370527-A	N/A	N/A	A		
Network and Security Service	Stealth Network Appliance (RPS, 1 Gbps) - Annual Maintenance	Per Appliance		CCSU13370528-A	N/A	N/A	A		
Network and Security Service	Stealth Client License (1-24)	Per License		CCSU13370375-A	N/A	N/A	A		
Network and Security Service	Stealth Client License (25-49)	Per License		CCSU13370376-A	N/A	N/A	A		
Network and Security Service	Stealth Client License (50-99)	Per License		CCSU13370377-A	N/A	N/A	A		
Network and Security Service	Stealth Client License (100-249)	Per License		CCSU13370378-A	N/A	N/A	A		
Network and Security Service	Stealth Client License (250-499)	Per License		CCSU13370379-A	N/A	N/A	A		
Network and Security Service	Stealth Client License (500-999)	Per License		CCSU13370380-A	N/A	N/A	A		
Network and Security Service	Stealth Client License (1000+)	Per License		CCSU13370381-A	N/A	N/A	A		
Network and Security Service	Stealth Client License (1-24) - Annual Maintenance	Per License		CCSU13370529-A	N/A	N/A	A		
Network and Security Service	Stealth Client License (25-49) - Annual Maintenance	Per License		CCSU13370530-A	N/A	N/A	A		
Network and Security Service	Stealth Client License (50-99) - Annual Maintenance	Per License		CCSU13370531-A	N/A	N/A	A		
Network and Security Service	Stealth Client License (100-249) - Annual Maintenance	Per License		CCSU13370532-A	N/A	N/A	A		
Network and Security Service	Stealth Client License (250-499) - Annual Maintenance	Per License		CCSU13370533-A	N/A	N/A	A		
Network and Security Service	Stealth Client License (500-999) - Annual Maintenance	Per License		CCSU13370534-A	N/A	N/A	A		
Network and Security Service	Stealth Client License (1000+) - Annual Maintenance	Per License		CCSU13370535-A	N/A	N/A	A		
Network and Security Service	Stealth Client Expansion License (1-24)	Per License		CCSU13370382-A	N/A	N/A	A		
Network and Security Service	Stealth Client Expansion License (25-49)	Per License		CCSU13370383-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Network and Security Service	Stealth Client Expansion License (50-99)	Per License		CCSU13370384-A	N/A	N/A	A		
Network and Security Service	Stealth Client Expansion License (100-249)	Per License		CCSU13370385-A	N/A	N/A	A		
Network and Security Service	Stealth Client Expansion License (250-499)	Per License		CCSU13370386-A	N/A	N/A	A		
Network and Security Service	Stealth Client Expansion License (500-999)	Per License		CCSU13370387-A	N/A	N/A	A		
Network and Security Service	Stealth Client Expansion License (1000+)	Per License		CCSU13370388-A	N/A	N/A	A		
Network and Security Service	Stealth Client Expansion License (1-24) - Annual Maintenance	Per License		CCSU13370536-A	N/A	N/A	A		
Network and Security Service	Stealth Client Expansion License (25-49) - Annual Maintenance	Per License		CCSU13370537-A	N/A	N/A	A		
Network and Security Service	Stealth Client Expansion License (50-99) - Annual Maintenance	Per License		CCSU13370538-A	N/A	N/A	A		
Network and Security Service	Stealth Client Expansion License (100-249) - Annual Maintenance	Per License		CCSU13370539-A	N/A	N/A	A		
Network and Security Service	Stealth Client Expansion License (250-499) - Annual Maintenance	Per License		CCSU13370540-A	N/A	N/A	A		
Network and Security Service	Stealth Client Expansion License (500-999) - Annual Maintenance	Per License		CCSU13370541-A	N/A	N/A	A		
Network and Security Service	Stealth Client Expansion License (1000+) - Annual Maintenance	Per License		CCSU13370542-A	N/A	N/A	A		
Network and Security Service	Stealth Server License (1-4)	Per License		CCSU13370389-A	N/A	N/A	A		
Network and Security Service	Stealth Server License (5-9)	Per License		CCSU13370390-A	N/A	N/A	A		
Network and Security Service	Stealth Server License (10-24)	Per License		CCSU13370391-A	N/A	N/A	A		
Network and Security Service	Stealth Server License (25-49)	Per License		CCSU13370392-A	N/A	N/A	A		
Network and Security Service	Stealth Server License (50-99)	Per License		CCSU13370393-A	N/A	N/A	A		
Network and Security Service	Stealth Server License (100+)	Per License		CCSU13370394-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Network and Security Service	Stealth Server License (1-4) - Annual Maintenance	Per License		CCSU13370543-A	N/A	N/A	A		
Network and Security Service	Stealth Server License (5-9) - Annual Maintenance	Per License		CCSU13370544-A	N/A	N/A	A		
Network and Security Service	Stealth Server License (10-24) - Annual Maintenance	Per License		CCSU13370545-A	N/A	N/A	A		
Network and Security Service	Stealth Server License (25-49) - Annual Maintenance	Per License		CCSU13370546-A	N/A	N/A	A		
Network and Security Service	Stealth Server License (50-99) - Annual Maintenance	Per License		CCSU13370547-A	N/A	N/A	A		
Network and Security Service	Stealth Server License (100+) - Annual Maintenance	Per License		CCSU13370548-A	N/A	N/A	A		
Network and Security Service	Stealth Server Expansion License (1-4)	Per License		CCSU13370395-A	N/A	N/A	A		
Network and Security Service	Stealth Server Expansion License (5-9)	Per License		CCSU13370396-A	N/A	N/A	A		
Network and Security Service	Stealth Server Expansion License (10-24)	Per License		CCSU13370397-A	N/A	N/A	A		
Network and Security Service	Stealth Server Expansion License (25-49)	Per License		CCSU13370398-A	N/A	N/A	A		
Network and Security Service	Stealth Server Expansion License (50-99)	Per License		CCSU13370399-A	N/A	N/A	A		
Network and Security Service	Stealth Server Expansion License (100+)	Per License		CCSU13370400-A	N/A	N/A	A		
Network and Security Service	Stealth Server Expansion License (1-4) - Annual Maintenance	Per License		CCSU13370549-A	N/A	N/A	A		
Network and Security Service	Stealth Server Expansion License (5-9) - Annual Maintenance	Per License		CCSU13370550-A	N/A	N/A	A		
Network and Security Service	Stealth Server Expansion License (10-24) - Annual Maintenance	Per License		CCSU13370551-A	N/A	N/A	A		
Network and Security Service	Stealth Server Expansion License (25-49) - Annual Maintenance	Per License		CCSU13370552-A	N/A	N/A	A		
Network and Security Service	Stealth Server Expansion License (50-99) - Annual Maintenance	Per License		CCSU13370553-A	N/A	N/A	A		
Network and Security Service	Stealth Server Expansion License (100+) - Annual Maintenance	Per License		CCSU13370554-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Network and Security Service	Stealth Authorization Service Stand Alone License	Per License		CCSU13370401-A	N/A	N/A	A		
Network and Security Service	Stealth Authorization Service with AD/LDAP License	Per License		CCSU13370402-A	N/A	N/A	A		
Network and Security Service	Stealth Authorization Service with RADIUS License	Per License		CCSU13370403-A	N/A	N/A	A		
Network and Security Service	Stealth Secure Virtual Terminal 4GB Windows Boot Device	Per Device		CCSU13370404-A	N/A	N/A	A		
Security Services	Vulnerability Assessment - Infrastructure - Small	Per Assessment		CCSD13370405-A	N/A	N/A	A		
Security Services	Vulnerability Assessment - Infrastructure - Medium	Per Assessment		CCSD13370406-A	N/A	N/A	A		
Security Services	Vulnerability Assessment - Infrastructure - Large	Per Assessment		CCSD13370407-A	N/A	N/A	A		
Security Services	Vulnerability Assessment - Infrastructure - Very Large	Per Assessment		CCSD13370408-A	N/A	N/A	A		
Security Services	Vulnerability Assessment - Web / mobile Application - Small (Up to 35 Custom Web Application Pages)	Per Assessment		CCSD13370409-A	N/A	N/A	A		
Security Services	Vulnerability Assessment - Web / mobile Application - Medium (Up to 70 Custom Web Application Pages)	Per Assessment		CCSD13370410-A	N/A	N/A	A		
Security Services	Vulnerability Assessment - Web / mobile Application - Large (Up to 100 Custom Web Application Pages)	Per Assessment		CCSD13370411-A	N/A	N/A	A		
Security Services	Vulnerability Assessment - Web / mobile Application - Very Large (Up to 175 Custom Web Application Pages)	Per Assessment		CCSD13370412-A	N/A	N/A	A		
Security Services	Vulnerability Assessment - Database - Small (Up to 3 Database Server with up to 5 database instances or Oracle SIDs)	Per Assessment		CCSD13370413-A	N/A	N/A	A		
Security Services	Vulnerability Assessment - Database - Medium (Up to 5 database servers with up to ten database instances or Oracle SIDs)	Per Assessment		CCSD13370414-A	N/A	N/A	A		
Security Services	Vulnerability Assessment - Database - Large (Up to 10 Database Servers with up to 15 database instances or Oracle SIDs)	Per Assessment		CCSD13370415-A	N/A	N/A	A		
Security Services	Vulnerability Assessment - Database - Very Large (Up to 20 database servers with up to 30 database instances or Oracle SIDs)	Per Assessment		CCSD13370416-A	N/A	N/A	A		
Security Services	Vulnerability Assessment - Wireless - Small (Up to 2 locations with up to 25 wireless access points)	Per Assessment		CCSD13370417-A	N/A	N/A	A		
Security Services	Vulnerability Assessment - Wireless - Medium (Up to 3 locations with up to 50 wireless access points)	Per Assessment		CCSD13370418-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Security Services	Vulnerability Assessment - Wireless - Large (Up to 4 locations with up to 75 wireless access points)	Per Assessment		CCSD13370419-A	N/A	N/A	A		
Security Services	Security Code Review - Small (Up to 500,000 Lines of Code for one web application custom source code; includes manual verification on up to 15 vulnerabilities with up to 4 instances per vulnerability assimilated)	Per Assessment		CCSD13370420-A	N/A	N/A	A		
Security Services	Security Code Review - Medium (Up to 1,000,000 Lines of Code for one web application custom source code; includes manual verification on up to 20 vulnerabilities with up to 6 instances per vulnerability assimilated)	Per Assessment		CCSD13370421-A	N/A	N/A	A		
Security Services	Security Code Review - Large (Up to 2,000,000 Lines of Code for one web application custom source code; includes manual verification on up to 25 vulnerabilities with up to 8 instances per vulnerability assimilated)	Per Assessment		CCSD13370422-A	N/A	N/A	A		
Security Services	Security Code Review - Very Large (Up to 3,500,000 Lines of Code for one web application custom source code; includes manual verification on up to 35 vulnerabilities with up to 10 instances per vulnerability assimilated)	Per Assessment		CCSD13370423-A	N/A	N/A	A		
Security Services	Security Risk Assessment - Small (An Agency or Office with up to 99 employees & 1 Security Guidelines)	Per Assessment		CCSD13370424-A	N/A	N/A	A		
Security Services	Security Risk Assessment - Medium (An Agency or Office with up to 999 employees & 2 Security Guidelines)	Per Assessment		CCSD13370425-A	N/A	N/A	A		
Security Services	Security Risk Assessment - Large (An Agency or Office with up to 9,999 employees & 5 Security Guidelines)	Per Assessment		CCSD13370426-A	N/A	N/A	A		
Security Services	Security Risk Assessment - Very Large (An Agency or Office with 10,000+ employees & 10 Security Guidelines)	Per Assessment		CCSD13370427-A	N/A	N/A	A		
Security Services	eGRC Solution - Install and initial setup	Per Implementation		CCSD13370428-A	N/A	N/A	A		
Security Services	eGRC Solution - Design and Configure - Small	Per Request		CCSD13370429-A	N/A	N/A	A		
Security Services	eGRC Solution - Design and Configure - Medium	Per Request		CCSD13370430-A	N/A	N/A	A		
Security Services	eGRC Solution - Design and Configure - Large	Per Request		CCSD13370431-A	N/A	N/A	A		
Security Services	eGRC Solution - Design and Configure - Very Large	Per Request		CCSD13370432-A	N/A	N/A	A		
Security Services	eGRC Solution - Develop risk assessment templates - Small	Per Request		CCSD13370433-A	N/A	N/A	A		
Security Services	eGRC Solution - Develop risk assessment templates - Medium	Per Request		CCSD13370434-A	N/A	N/A	A		
Security Services	eGRC Solution - Develop risk assessment templates - Large	Per Request		CCSD13370435-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Security Services	eGRC Solution - Develop risk assessment templates - Very Large	Per Request		CCSD13370436-A	N/A	N/A	A		
Security Services	Security Configuration Review (Standard OS Platform - up to 3 information Systems	Per Request		CCSD13370437-A	N/A	N/A	A		
Security Services	Security Configuration Review (3 standard database instances)	Per Request		CCSD13370438-A	N/A	N/A	A		
Security Services	Security Configuration Review (3 web server instances)	Per Request		CCSD13370439-A	N/A	N/A	A		
Security Services	Security Configuration Review (2 boundary defense devices)	Per Request		CCSD13370440-A	N/A	N/A	A		
Security Services	Security Configuration Review (One Mainframe OS Instance)	Per Request		CCSD13370441-A	N/A	N/A	A		
Security Services	Security Configuration Review (up to 3 Virtual infrastructure instances)	Per Request		CCSD13370442-A	N/A	N/A	A		
Security Services	Security Configuration Review (One standard ERP solution)	Per Request		CCSD13370443-A	N/A	N/A	A		
Security Services	CTI Diagnostic - Small (1 of TB of audit logs and rogue device detection for up to 1,000 devices)	Per Assessment		CCSD13370444-A	N/A	N/A	A		
Security Services	CTI Diagnostic - Medium (2 of TB of audit logs and rogue device detection for up to 2,000 devices)	Per Assessment		CCSD13370445-A	N/A	N/A	A		
Security Services	CTI Diagnostic - Large (3 of TB of audit logs and rogue device detection for up to 3,500 devices)	Per Assessment		CCSD13370446-A	N/A	N/A	A		
Security Services	CTI Diagnostic - Very Large (4 of TB of audit logs and rogue device detection for up to 5,000 devices)	Per Assessment		CCSD13370447-A	N/A	N/A	A		
Security Services	Suspicious Program Diagnostic - Small (up to 25 standard configuration for Servers)	Per Assessment		CCSD13370448-A	N/A	N/A	A		
Security Services	Suspicious Program Diagnostic - Medium (up to 100 standard configuration for Servers)	Per Assessment		CCSD13370449-A	N/A	N/A	A		
Security Services	Suspicious Program Diagnostic - Large (up to 250 standard configuration for Servers)	Per Assessment		CCSD13370450-A	N/A	N/A	A		
Security Services	Suspicious Program Diagnostic - Very Large (1,000 standard configuration for Servers)	Per Assessment		CCSD13370451-A	N/A	N/A	A		
Security Services	Remote Access Compromise Analysis - Small (1 TB of Remote Access Audit Logs)	Per Assessment		CCSD13370452-A	N/A	N/A	A		
Security Services	Remote Access Compromise Analysis - Medium (2 of TB of Remote Access Audit Logs)	Per Assessment		CCSD13370453-A	N/A	N/A	A		
Security Services	Remote Access Compromise Analysis - Large (3 of TB of Remote Access Audit Logs)	Per Assessment		CCSD13370454-A	N/A	N/A	A		
Security Services	Remote Access Compromise Analysis - Very Large (4 of TB of Remote Access Audit Logs)	Per Assessment		CCSD13370455-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Security Services	Insider Threat Detection Diagnostic - Small (Agency or Office with up to 99 employees, up to 250 GB of Audit Logs, and up to 3 Interviews)	Per Assessment		CCSD13370456-A	N/A	N/A	A		
Security Services	Insider Threat Detection Diagnostic - Medium (Agency or Office with up to 999 employees, up to 500 GB of Audit Logs, and up to 5 Interviews)	Per Assessment		CCSD13370457-A	N/A	N/A	A		
Security Services	Insider Threat Detection Diagnostic - Large (Agency or Office with up to 9,999 employees, up to 1 tT of Audit Logs, and up to 10 Interviews)	Per Assessment		CCSD13370458-A	N/A	N/A	A		
Security Services	Insider Threat Detection Diagnostic - Very Large (Agency or Office with up to 10,000+ employees, up to 2 TB of Audit Logs, and up to 3 Interviews)	Per Assessment		CCSD13370459-A	N/A	N/A	A		
Security Services	Enterprise Fraud Program Assessment - Small - (Agency or Office with up 99 employees, 250 GB of Audit Logs, and up to 3 Fraud Detection Rule Sets)	Per Assessment		CCSD13370460-A	N/A	N/A	A		
Security Services	Enterprise Fraud Program Assessment - Medium - (Agency or Office with up 999 employees, 500 GB of Audit Logs, and up to 5 Fraud Detection Rule Sets)	Per Assessment		CCSD13370461-A	N/A	N/A	A		
Security Services	Enterprise Fraud Program Assessment - Large - (Agency or Office with up 9,999 employees, 1 TB of Audit Logs, and up to 5 Fraud Detection Rule Sets)	Per Assessment		CCSD13370462-A	N/A	N/A	A		
Security Services	Enterprise Fraud Program Assessment - Very Large - (Agency or Office with up 10,000+ employees, 2 TB of Audit Logs, and up to 5 Fraud Detection Rule Sets)	Per Assessment		CCSD13370463-A	N/A	N/A	A		
Security Services	Data Loss Prevention - Network Monitoring - Small (1 Exgress Point, and 5 Simple, and 1 Complex DLP Policies)	Per Request		CCSD13370464-A	N/A	N/A	A		
Security Services	Data Loss Prevention - Network Monitoring - Medium (2 Exgress Points, 7 Simple, and 2 Complex DLP Policies)	Per Request		CCSD13370465-A	N/A	N/A	A		
Security Services	Data Loss Prevention - Network Monitoring - Large (3 Exgress Points, 9 Simple, and 3 Complex DLP Policies)	Per Request		CCSD13370466-A	N/A	N/A	A		
Security Services	Data Loss Prevention - Network Monitoring - Very Large (4 Exgress Points, 12 Simple, and 5 Complex DLP Policies)	Per Request		CCSD13370467-A	N/A	N/A	A		
Security Services	Data Loss Prevention - Endpoint protection - Small - (up to 150 IT infrastructure endpoints, 5 Simple, and 1 Complex DLP Policies)	Per Request		CCSD13370468-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Security Services	Data Loss Prevention - Endpoint protection - Medium - (up to 1,250 IT infrastructure endpoints, 7 Simple, and 3 Complex DLP Policies)	Per Request		CCSD13370469-A	N/A	N/A	A		
Security Services	Data Loss Prevention - Endpoint protection - Large - (up to 11,000 IT infrastructure endpoints, 9 Simple, and 3 Complex DLP Policies)	Per Request		CCSD13370470-A	N/A	N/A	A		
Security Services	Data Loss Prevention - Endpoint protection - Very Large - (25,000 IT infrastructure endpoints, and 12 Simple, and 5 Complex DLP Policies)	Per Request		CCSD13370471-A	N/A	N/A	A		
Security Services	Data Breach Diagnostics - Small (Up to 3 Systems, 120 GB of File Storage, and 100 GB of uncompressed text Audit Logs)	Per Assessment		CCSD13370472-A	N/A	N/A	A		
Security Services	Data Breach Diagnostics - Medium (Up to 10 Systems, 120 GB of File Storage, and 500 GB of uncompressed text Audit Logs)	Per Assessment		CCSD13370473-A	N/A	N/A	A		
Security Services	Data Breach Diagnostics - Large (Up to 50 Systems, 120 GB of File Storage, and 2 TB of uncompressed text Audit Logs)	Per Assessment		CCSD13370474-A	N/A	N/A	A		
Security Services	Mobile Device Management (MDM) - Design and implement - Small	Per Request		CCSD13370475-A	N/A	N/A	A		
Security Services	Mobile Device Management (MDM) - Design and implement - Medium	Per Request		CCSD13370476-A	N/A	N/A	A		
Security Services	Mobile Device Management (MDM) - Design and implement - Large	Per Request		CCSD13370477-A	N/A	N/A	A		
Security Services	Mobile Device Management (MDM) - Design and implement - Very Large	Per Request		CCSD13370478-A	N/A	N/A	A		
Security Services	Mobile Security Strategy and Roadmap - Small	Per Request		CCSD13370479-A	N/A	N/A	A		
Security Services	Mobile Security Strategy and Roadmap – Medium	Per Request		CCSD13370480-A	N/A	N/A	A		
Security Services	Mobile Security Strategy and Roadmap – Large	Per Request		CCSD13370481-A	N/A	N/A	A		
Security Services	Mobile Security Strategy and Roadmap – Very Large	Per Request		CCSD13370482-A	N/A	N/A	A		
Security Services	Security Training Assessment - Small (Agency or Office with up to 999 employees)	Per Assessment		CCSD13370483-A	N/A	N/A	A		
Security Services	Security Training Assessment - Medium (Agency or Office with up to 9,999 employees)	Per Assessment		CCSD13370484-A	N/A	N/A	A		
Security Services	Security Training Assessment - Large (Agency or Office with up to 10,000+ employees)	Per Assessment		CCSD13370485-A	N/A	N/A	A		

Field Name ==>	Product Name	Unit	Qty per config	Prov0 ider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code
Security Services	Security Training - Design and Delivery - (Training Presentation Deliverable and one training session (Up to 4 Hours))	Per Request		CCSD13370486-A	N/A	N/A	A		
Security Services	Identity Access Management - Design and Implement - Small	Per Request		CCSD13370487-A	N/A	N/A	A		
Security Services	Identity Access Management - Design and Implement - Medium	Per Request		CCSD13370488-A	N/A	N/A	A		
Security Services	Access Management - Design and Implement - Large	Per Request		CCSD13370489-A	N/A	N/A	A		
Security Services	Identity Provisioning and Management - Design and Implement - Small	Per Request		CCSD13370490-A	N/A	N/A	A		
Security Services	Identity Provisioning and Management - Design and Implement - Medium	Per Request		CCSD13370491-A	N/A	N/A	A		
Security Services	Identity Provisioning and Management - Design and Implement - Large	Per Request		CCSD13370492-A	N/A	N/A	A		
Security Services	Identity Governance and Management - Design and Implement - Small	Per Request		CCSD13370493-A	N/A	N/A	A		
Security Services	Identity Governance and Management - Design and Implement - Medium	Per Request		CCSD13370494-A	N/A	N/A	A		
Security Services	Identity Governance and Management - Design and Implement - Large	Per Request		CCSD13370495-A	N/A	N/A	A		
Third Party Software	Unisys Mainframe - Software License Transfer - KMSYS	Per Mainframe Upgrade		CCSU13370496-A	N/A	N/A	A		
Third Party Software	Unisys Mainframe - Software License Transfer - SMA OpCon	Per Mainframe Upgrade		CCSU13370497-A	N/A	N/A	A		
Third Party Software	Unisys Mainframe - Software License Transfer - Sightline	Per Mainframe Upgrade		CCSU13370498-A	N/A	N/A	A		
Strategy Workshop Services	Cloud Transformation Workshop for Single Tower	Per Workshop		CCSI13370499-A	N/A	N/A	A		
Strategy Workshop Services	Cloud Transformation Workshop	Per Workshop		CCSI13370500-A	N/A	N/A	A		

This page intentionally left blank.

Enterprise Services Catalog Template

Service Attribute	*Service Attribute Description*	
Service Name	*Title of Service*	
Detailed Description	*Short description of the service*	
Service Customers / Users	*Any participating Commonwealth agency or office, unless otherwise noted*	
Service Prerequisites	*These are the minimum or identified perquisite or additional services or activities required when this service is ordered?*	
Request the Service	*To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.* *Or* *To request this service, submit a Solution Request in the online Enterprise Services Catalog*	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
Provider Part Number	*Product Name*	*Orderable Units and related restrictions (per set of hours, tasks, etc.)?*

This page intentionally left blank.

Compute Services - Fully Managed Services

Fully Managed - X86 (Windows and Linux)

X86 (Windows or Linux) Physical Configuration - Configuration Components

Service Attribute	*Service Attribute Description*	
Service Name	Windows / Linux Physical Server – Configuration 1 – 2 way Quad-Core 2.0 GHz	
Detailed Description	Two socket, 4 cores per socket CPU's running at 2.0 GHz	
Service Customers / Users	Cannot Be Ordered Separately	
Service Prerequisites	1) Cannot Be Ordered Separately	
Request the Service	Cannot Be Ordered Separately	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310001-A	Windows pConfig-1 - 2-way Quad-Core 2.0 GHz	Per Physical Server
CCSU13310035-A	Linux pConfig-1 - 2-way Quad-Core 2.0 GHz	Per Physical Server

Service Attribute	*Service Attribute Description*	
Service Name	Windows / Linux Physical Server – Configuration 2, 4, 5 – 2 way Six-Core 2.4 GHz	
Detailed Description	Two socket, 6 cores per socket CPU's running at 2.4 GHz	
Service Customers / Users	Cannot Be Ordered Separately	
Service Prerequisites	Cannot Be Ordered Separately	
Request the Service	Cannot Be Ordered Separately	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310002-A	Windows pConfig – 2,4,5 - 2 way Six-Core 2.4 GHz	Per Physical Server
CCSU13310036-A	Linux pConfig – 2,4,5 - 2 way Six-Core 2.4 GHz	Per Physical Server

Service Attribute	*Service Attribute Description*	
Service Name	Windows / Linux Physical Server – Configuration 3 – 2 way Six-Core 2.0 GHz	
Detailed Description	Two socket, 6 cores per socket CPU's running at 2.0 GHz	
Service Customers / Users	Cannot Be Ordered Separately	
Service Prerequisites	Cannot Be Ordered Separately	
Request the Service	Cannot Be Ordered Separately	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310003-A	Windows pConfig – 3 - 2 way Six-Core 2.0 GHz	Per Physical Server
CCSU13310037-A	Linux pConfig – 3 - 2 way Six-Core 2.0 GHz	Per Physical Server

Service Attribute	*Service Attribute Description*	
Service Name	Windows / Linux pConfig – 1, 2, 3, 4, 5 - GB RAM	
Detailed Description	1 GB of Physical Random Access Memory (RAM)	
Service Customers / Users	Cannot Be Ordered Separately	
Service Prerequisites	Cannot Be Ordered Separately	
Request the Service	Cannot Be Ordered Separately	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310004-A	Windows GB RAM	Per GB
CCSU13310038-A	Linux GB RAM	Per GB

Service Attribute	*Service Attribute Description*	
Service Name	Windows / Linux pConfig – 1,2,4,5 – Mirrored 146 GB 15K Hard Drives	
Detailed Description	Two internal 146 GB 15K Hard Drives, Mirrored	
Service Customers / Users	Cannot Be Ordered Separately	
Service Prerequisites	Cannot Be Ordered Separately	
Request the Service	Cannot Be Ordered Separately	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310005-A	Windows Mirrored 146 15K Hard Drives	Per Primary + Mirrored
CCSU13310039-A	Linux Mirrored 146 15K Hard Drives	Per Primary + Mirrored

Service Attribute	*Service Attribute Description*	
Service Name	Windows / Linux pConfig – 3 – SAN Attached Storage	
Detailed Description	Short write up on what the Catalog item will do	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	What is required before this service or service element be ordered? 1) Selection of another service (what service?) 2) Solution Request submittal 3) Etc.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310006-A	Windows SAN Attached Storage	Per GB
CCSU13310040-A	Linux SAN Attached Storage	Per GB

Service Attribute	*Service Attribute Description*	
Service Name	Windows – pConfig 1,2,3,4,5 – Windows Server 2008 R2	
Detailed Description	Windows Server 2008 R2 License for One (1) physical server.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1) One physical server configuration 1, 2, 3, 4, or 5 2) One Commissioning/Decommissioning Service	
Request the Service	Cannot Be Ordered Separately	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310007-A	Windows pConfig-1, 2, 3, 4, 5 – Windows Server 2008 R2	Per License

Service Attribute	*Service Attribute Description*	
Service Name	Linux – pConfig 1, 2, 3, 4, 5 – Red Hat or SUSE	
Detailed Description	Red Hat or SUSE License for One (1) physical server.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	3) One physical server configuration 1, 2, 3, 4, or 5 1) One Commissioning/Decommissioning Service	
Request the Service	Cannot Be Ordered Separately	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310041-A	Linux pConfig-1,2,3,4,5 – Red Hat or SUSE	Per License

Service Attribute	*Service Attribute Description*	
Service Name	Windows / Linux pConfig – 4 – Disaster Recovery Server with 24 hour Recovery Point Objective	
Detailed Description	Provides two physical configuration 4 servers, with one configured as a disaster recovery server. The disaster recovery server has a 24 hour Recovery Point Objective.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1. For Platinum, servers must be ordered in groups of three 2. For Gold, servers must be ordered at a minimum in a pair of two (2) 3. Must order a commissioning/decommissioning service, one for each server.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310008-A	Windows pConfig - 4 – Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization Site's Local SAN Storage from hourly	Per Service

	data synchronization	
CCSU13310042-A	Windows pConfig - 4 – Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization Site’s Local SAN Storage from hourly data synchronization	Per Service

Service Attribute	*Service Attribute Description*	
Service Name	Windows / Linux pConfig – 5 – Disaster Recovery Server with 72 hour Recovery Point Objective	
Detailed Description	Provides two physical configuration 5 servers, with one configured as a disaster recovery server. The disaster recovery server has a 24 hour Recovery Point Objective.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1. For Platinum, servers must be ordered in groups of three 2. For Gold, servers must be ordered at a minimum in a pair of two (2) 3. Must order a commissioning/decommissioning service, one for each server.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310009-A	Windows pConfig - 5 - Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Service

CCSU13310043-A	Linux pConfig - 5 - Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Service

X86 (Windows or Linux) Physical Configuration - Orderable Configurations

Service Attribute	*Service Attribute Description*	
Service Name	Windows Physical Server – Configuration 1	
Detailed Description	One physical Windows server with 2 physical CPU's, each with 4 cores operating at 2.4 GHz with 4 GB of RAM and 2 mirrored internal 146 GB Hard Drives operating at 15K RPM's.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1. For Platinum, servers must be ordered in groups of three 2. For Gold, servers must be ordered at a minimum in a pair of two (2) 3. Must order a commissioning/decommissioning service, one for each server. 4. Selection of appropriate tier (Platinum, Gold, Silver, Bronze, Basic) of server support	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310219-A	Windows pConfig-1	Per Physical Server

Service Attribute	*Service Attribute Description*	
Service Name	Windows Physical Server – Configuration 2	
Detailed Description	One physical Windows server with 2 physical CPU's, each with six (6) cores operating at 2.4 GHz with 16 GB of RAM and 2 mirrored internal 146 GB Hard Drives operating at 15K RPM's.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1. For Platinum, servers must be ordered in groups of three 2. For Gold, servers must be ordered at a minimum in a pair of two (2) 3. Must order a commissioning/decommissioning service, one for each server. 4. Selection of appropriate tier (Platinum, Gold, Silver, Bronze, Basic) of server support	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310220-A	Windows pConfig-2	Per Physical Server

Service Attribute	*Service Attribute Description*	
Service Name	Windows Physical Server – Configuration 3	
Detailed Description	One physical Windows server with two physical CPU's, each with six cores operating at 2.0 GHz with 128 GB of RAM.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1. For Platinum, servers must be ordered in groups of three 2. For Gold, servers must be ordered at a minimum in a pair of two (2) 3. Must order a commissioning/decommissioning service, one for each server. 4. Selection of appropriate tier (Platinum, Gold, Silver, Bronze, Basic) of server support	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310221-A	Windows pConfig-3	Per Physical Server

Service Attribute	*Service Attribute Description*	
Service Name	Windows Physical Server – Configuration 4	
Detailed Description	One physical Windows server with 2 physical CPU's, each with six (6) cores operating at 2.4 GHz with 16 GB of RAM and 2 mirrored internal 146 GB Hard Drives operating at 15K RPM's.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1. For Platinum, servers must be ordered in groups of three 2. For Gold, servers must be ordered at a minimum in a pair of two (2) 3. Must order a commissioning/decommissioning service, one for each server. 4. Selection of appropriate tier (Platinum, Gold, Silver, Bronze, Basic) of server support	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310222-A	Windows pConfig-4	Per Physical Server

Service Attribute	*Service Attribute Description*	
Service Name	Windows Physical Server – Configuration 5	
Detailed Description	One physical Windows server with 2 physical CPU's, each with six (6) cores operating at 2.4 GHz with 16 GB of RAM and 2 mirrored internal 146 GB Hard Drives operating at 15K RPM's.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1. For Platinum, servers must be ordered in groups of three 2. For Gold, servers must be ordered at a minimum in a pair of two (2) 3. Must order a commissioning/decommissioning service, one for each server. 4. Selection of appropriate tier (Platinum, Gold, Silver, Bronze, Basic) of server support	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310223-A	Windows pConfig-5	Per Physical Server

Service Attribute	*Service Attribute Description*	
Service Name	Linux Physical Server – Configuration 1	
Detailed Description	One physical Linux server with 2 physical CPU's, each with four cores operating at 2.4 GHz with 4 GB of RAM and 2 mirrored internal 146 GB Hard Drives operating at 15K RPM's.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1. For Platinum, servers must be ordered in groups of three 2. For Gold, servers must be ordered at a minimum in a pair of two (2) 3. Must order a commissioning/decommissioning service, one for each server. 4. Selection of appropriate tier (Platinum, Gold, Silver, Bronze, Basic) of server support	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310224-A	Linux pConfig-1	Per Physical Server

Service Attribute	*Service Attribute Description*	
Service Name	Linux Physical Server – Configuration 2	
Detailed Description	One physical Linux server with 2 physical CPU's, each with six (6) cores operating at 2.4 GHz with 16 GB of RAM and 2 mirrored internal 146 GB Hard Drives operating at 15K RPM's.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1. For Platinum, servers must be ordered in groups of three 2. For Gold, Silver, must be ordered at a minimum in a pair of two (2) 3. Must order a commissioning/decommissioning service, one for each server. 4. Selection of appropriate tier (Platinum, Gold, Silver, Bronze, Basic) of server support	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310225-A	Linux pConfig-2	Per Physical Server

Service Attribute	*Service Attribute Description*	
Service Name	Linux Physical Server – Configuration 3	
Detailed Description	One physical Linux server with 2 physical CPU's, each with six (6) cores operating at 2.0 GHz with 128 GB of RAM.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1. For Platinum, servers must be ordered in groups of three 2. For Gold, servers must be ordered at a minimum in a pair of two (2) 3. Must order a commissioning/decommissioning service, one for each server. 4. Selection of appropriate tier (Platinum, Gold, Silver, Bronze, Basic) of server support	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310226-A	Linux pConfig-3	Per Physical Server

Service Attribute	*Service Attribute Description*	
Service Name	Linux Physical Server – Configuration 4	
Detailed Description	One physical Linux server with 2 physical CPU's, each with six (6) cores operating at 2.4 GHz with 16 GB of RAM and 2 mirrored internal 146 GB Hard Drives operating at 15K RPM's.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1. For Platinum, servers must be ordered in groups of three 2. For Gold, servers must be ordered at a minimum in a pair of two (2) 3. Must order a commissioning/decommissioning service, one for each server. 4. Selection of appropriate tier (Platinum, Gold, Silver, Bronze, Basic) of server support	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310227-A	Linux pConfig-4	Per Physical Server

Service Attribute	*Service Attribute Description*	
Service Name	Linux Physical Server – Configuration 5	
Detailed Description	One physical Linux server with 2 physical CPU's, each with six (6) cores operating at 2.4 GHz with 16 GB of RAM and 2 mirrored internal 146 GB Hard Drives operating at 15K RPM's.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1. For Platinum, servers must be ordered in groups of three 2. For Gold, servers must be ordered at a minimum in a pair of two (2) 3. Must order a commissioning/decommissioning service, one for each server. 4. Selection of appropriate tier (Platinum, Gold, Silver, Bronze, Basic) of server support	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310228-A	Linux pConfig-5	Per Physical Server

X86 (Windows or Linux) Virtual Configuration - Configuration Components

Service Attribute	*Service Attribute Description*	
Service Name	Windows / Linux Virtual Configuration 1 – 2 vCPU	
Detailed Description	One virtual Windows or Linux server with 2 virtual CPU's, with 4 GB of RAM	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1. For Platinum, servers must be ordered in groups of three 2. For Gold, servers must be ordered at a minimum in a pair of two (2) 3. Must order a commissioning/decommissioning service, one for each server. 4. Selection of appropriate tier (Platinum, Gold, Silver, Bronze, Basic) of server support	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310069-A	Windows vConfig-1 – 2 vCPU	Per Virtual Server
CCSU13310105-A	Linux vConfig-1 – 2 vCPU	Per Virtual Server

Service Attribute	*Service Attribute Description*	
Service Name	Windows / Linux Virtual Configuration 2, 4, 5 – 4 vCPU	
Detailed Description	One virtual Windows or Linux server with 4 virtual CPU's, with 16 GB of RAM	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1. For Platinum, servers must be ordered in groups of three 2. For Gold, Silver, servers must be ordered at a minimum in a pair of two (2) 3. Must order a commissioning/decommissioning service, one for each server. 4. Selection of appropriate tier (Platinum, Gold, Silver, Bronze, Basic) of server support	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310070-A	Windows vConfig – 2,4,5 – 4 vCPU	Per Virtual Server
CCSU13310106-A	Linux vConfig – 2,4,5 – 4 vCPU	Per Virtual Server

Service Attribute	*Service Attribute Description*	
Service Name	Windows / Linux Virtual Configuration 3 – 8 vCPU	
Detailed Description	One virtual Windows or Linux server with 8 virtual CPU's, with 64 GB of RAM	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1. For Platinum, servers must be ordered in groups of three 2. For Gold, servers must be ordered at a minimum in a pair of two (2) 3. Must order a commissioning/decommissioning service, one for each server. 4. Selection of appropriate tier (Platinum, Gold, Silver, Bronze, Basic) of server support	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310071-A	Windows vConfig – 3 – 8 vCPU	Per Virtual Server
CCSU13310107-A	Linux vConfig – 3 – 8 vCPU	Per Virtual Server

Service Attribute	*Service Attribute Description*	
Service Name	Windows / Linux Virtual Configuration – 1, 2, 3, 4, 5 - GB RAM	
Detailed Description	1 GB of virtual Random Access Memory	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1) A previously ordered configuration 1, 2, 3 Windows or Linux virtual server. 2) For configuration 4 and 5, the same incremental memory must be ordered on both servers.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310072-A	Windows vConfig-1, 2, 3, 4, 5 - GB RAM	Per GB
CCSU13310108-A	Linux vConfig-1, 2, 3, 4, 5 - GB RAM	Per GB

Service Attribute	*Service Attribute Description*	
Service Name	Windows – Virtual Configuration 1, 2, 3, 4, 5 – Windows Server 2008 R2	
Detailed Description	A copy of Windows Server 2008 R2 for a virtual machine.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	Cannot Be Ordered Separately	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310073-A	Windows vConfig-1, 2, 3, 4, 5 – Windows Server 2008 R2	Per License

Service Attribute	*Service Attribute Description*	
Service Name	Linux – Virtual Configuration 1, 2, 3, 4, 5 – Red Hat or SUSE	
Detailed Description	A copy of Red Hat or SUSE Linux for a virtual machine.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	Cannot Be Ordered Separately	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310109-A	Linux vConfig-1, 2, 3, 4, 5 – Red Hat or SUSE	Per License

Service Attribute	*Service Attribute Description*	
Service Name	Windows / Linux Virtual Configuration-1,2,3,4,5 – Firewall/IDS	
Detailed Description	One Firewall/IDS for a Windows or Linux virtual machine	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	Cannot Be Ordered Separately	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310074-A	Windows vConfig-1, 2, 3, 4, 5 – Firewall/IDS	Per License
CCSU13310110-A	Linux vConfig-1, 2, 3, 4, 5 – Firewall/IDS	Per License

Service Attribute	*Service Attribute Description*	
Service Name	Windows / Linux Virtual Configuration-1, 2, 3, 4,5– Site to Site VPN	
Detailed Description	One Site to Site VPN for a Windows or Linux virtual machine.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	Cannot Be Ordered Separately	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310075-A	Windows vConfig-1, 2, 3, 4, 5 – Site to Site VPN	Per License
CCSU13310111-A	Linux vConfig-1, 2, 3, 4, 5 – Site to Site VPN	Per License

Service Attribute	*Service Attribute Description*	
Service Name	Windows / Linux VConfig-1, 2, 3, 4, 5 - VPN Client	
Detailed Description	One VPN Client for a Windows or Linux virtual machine.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	Cannot Be Ordered Separately	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310076-A	Windows vConfig-1, 2, 3, 4, 5 – VPN Client	Per License
CCSU13310112-A	Linux vConfig-1, 2, 3, 4, 5 – VPN Client	Per License

Service Attribute	*Service Attribute Description*	
Service Name	Windows / Linux VConfig-1, 2, 3, 4, 5 - VLAN	
Detailed Description	One VLAN assignment for a Windows or Linux virtual machine.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	Cannot Be Ordered Separately	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310077-A	Windows vConfig-1, 2, 3, 4, 5 – VLAN	Per Config
CCSU13310113-A	Linux vConfig-1, 2, 3, 4, 5 – VLAN	Per Config

Service Attribute	*Service Attribute Description*	
Service Name	Windows / Linux vConfig – 4 – Disaster Recovery Server with 24 hour Recovery Point Objective	
Detailed Description	Provides two physical configuration 4 servers, with one configured as a disaster recovery server. The disaster recovery server has a 24 hour Recovery Point Objective.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1. For Platinum, servers must be ordered in groups of three 2. For Gold, Silver, Bronze and Basic, servers must be ordered at a minimum in a pair of two (2) 3. Must order a commissioning/decommissioning service, one for each server.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310078-A	Windows vConfig-4 – Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization Site's	Per Service

	Local SAN Storage from hourly data synchronization	
CCSU13310114-A	Linux vConfig-4 – Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization Site’s Local SAN Storage from hourly data synchronization	Per Service

Service Attribute	*Service Attribute Description*	
Service Name	Windows / Linux vConfig – 5 – Disaster Recovery Server with 72 hour Recovery Point Objective	
Detailed Description	Provides two physical configuration 5 servers, with one configured as a disaster recovery server. The disaster recovery server has a 72 hour Recovery Point Objective.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1. For Platinum, servers must be ordered in groups of three 2. For Gold, Silver, Bronze and Basic, servers must be ordered at a minimum in a pair of two (2) 3. Must order a commissioning/decommissioning service, one for each server.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310079-A	Windows vConfig-5 - Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Service

CCSU13310115-A	Linux vConfig-5 - Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Service

X86 (Windows or Linux) Virtual Configuration – Orderable Configurations

Service Attribute	*Service Attribute Description*	
Service Name	Windows Virtual Server – Configuration 1	
Detailed Description	One virtual Windows server with 2 virtual CPU's, with 4 GB of RAM	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1. For Platinum, servers must be ordered in groups of three 2. For Gold, servers must be ordered at a minimum in a pair of two (2) 3. Must order a commissioning/decommissioning service, one for each server. 4. Selection of appropriate tier (Platinum, Gold, Silver, Bronze, Basic) of server support	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310229-A	Windows vConfig-1	Per Virtual Server

Service Attribute	*Service Attribute Description*	
Service Name	Windows Virtual Server – Configuration 2	
Detailed Description	One virtual Windows server with 4 virtual CPU's, with 16 GB of RAM	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1) For Platinum, servers must be ordered in groups of three 2) For Gold, servers must be ordered at a minimum in a pair of two (2) 3) Must order a commissioning/decommissioning service, one for each server. 4) Selection of appropriate tier (Platinum, Gold, Silver, Bronze, Basic) of server support	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310230-A	Windows vConfig-2	Per Virtual Server

Service Attribute	*Service Attribute Description*	
Service Name	Windows Virtual Server – Configuration 3	
Detailed Description	One virtual Windows server with 8 virtual CPU's, with 64 GB of RAM	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1) For Platinum, servers must be ordered in groups of three 2) For Gold, servers must be ordered at a minimum in a pair of two (2) 3) Must order a commissioning/decommissioning service, one for each server. 4) Selection of appropriate tier (Platinum, Gold, Silver, Bronze, Basic) of server support	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310231-A	Windows vConfig-3	Per Virtual Server

Service Attribute	*Service Attribute Description*	
Service Name	Windows Virtual Server – Configuration 4	
Detailed Description	One virtual Windows server with 4 virtual CPU's, with 16 GB of RAM	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	What is required before this service or service element be ordered? 1) For Platinum, servers must be ordered in groups of three 2) For Gold, Silver, Bronze and Basic, servers must be ordered at a minimum in a pair of two (2) 3) Must order a commissioning/decommissioning service, one for each server. 4) Selection of appropriate tier (Platinum, Gold, Silver, Bronze, Basic) of server support	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310232-A	Windows vConfig-4	Per Virtual Server

Service Attribute	*Service Attribute Description*	
Service Name	Windows Virtual Server – Configuration 5	
Detailed Description	One virtual Windows server with 4 virtual CPU's, with 16 GB of RAM	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1) For Platinum, servers must be ordered in groups of three 2) For Gold, Silver, Bronze and Basic, servers must be ordered at a minimum in a pair of two (2) 3) Must order a commissioning/decommissioning service, one for each server. 4) Selection of appropriate tier (Platinum, Gold, Silver, Bronze, Basic) of server support	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310233-A	Windows vConfig-5	Per Virtual Server

Service Attribute	*Service Attribute Description*	
Service Name	Linux Virtual Server – Configuration 1	
Detailed Description	One virtual Linux server with 2 virtual CPU's, with 4 GB of RAM	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	What is required before this service or service element be ordered? 1) For Platinum, servers must be ordered in groups of three 2) For Gold, servers must be ordered at a minimum in a pair of two (2) 3) Must order a commissioning/decommissioning service, one for each server. 4) Selection of appropriate tier (Platinum, Gold, Silver, Bronze, Basic) of server support	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310234-A	Linux vConfig-1	Per Virtual Server

Service Attribute	*Service Attribute Description*	
Service Name	Linux Virtual Server – Configuration 2	
Detailed Description	One virtual Linux server with 4 virtual CPU's, with 16 GB of RAM	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1) For Platinum, servers must be ordered in groups of three 2) For Gold, servers must be ordered at a minimum in a pair of two (2) 3) Must order a commissioning/decommissioning service, one for each server. 4) Selection of appropriate tier (Platinum, Gold, Silver, Bronze, Basic) of server support	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310235-A	Linux vConfig-2	Per Virtual Server

Service Attribute	*Service Attribute Description*	
Service Name	Linux Virtual Server – Configuration 3	
Detailed Description	One virtual Linux server with 8 virtual CPU's, with 64 GB of RAM	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1. For Platinum, servers must be ordered in groups of three 2. For Gold, servers must be ordered at a minimum in a pair of two (2) 3. Must order a commissioning/decommissioning service, one for each server. 4. Selection of appropriate tier (Platinum, Gold, Silver, Bronze, Basic) of server support	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310236-A	Windows vConfig-3	Per Virtual Server

Service Attribute	*Service Attribute Description*	
Service Name	Linux Virtual Server – Configuration 4	
Detailed Description	One virtual Linux server with 4 virtual CPU's, with 16 GB of RAM	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1) For Platinum, servers must be ordered in groups of three 2) For Gold, Silver, Bronze and Basic, servers must be ordered at a minimum in a pair of two (2) 3) Must order a commissioning/decommissioning service, one for each server. 4) Selection of appropriate tier (Platinum, Gold, Silver, Bronze, Basic) of server support	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310237-A	Linux vConfig-4	Per Virtual Server

Service Attribute	*Service Attribute Description*	
Service Name	Linux Virtual Server – Configuration 5	
Detailed Description	One virtual Linux server with 4 virtual CPU's, with 16 GB of RAM	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1) For Platinum, servers must be ordered in groups of three 2) For Gold, Silver, Bronze and Basic, servers must be ordered at a minimum in a pair of two (2) 3) Must order a commissioning/decommissioning service, one for each server. 4) Selection of appropriate tier (Platinum, Gold, Silver, Bronze, Basic) of server support	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310238-A	Linux vConfig-5	Per Virtual Server

X86 (Windows or Linux) Tiers of Service

Service Attribute	*Service Attribute Description*	
Service Name	Fully Managed Physical Windows Server Support	
Detailed Description	Management of Windows servers, in alignment to Schedule F, section 3.2.4.1	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1. For Platinum, servers must be ordered in groups of three. Servers must be geographically dispersed, and actively load balanced at the application layer. 2. For Gold, servers must be ordered at a minimum in a pair of two, and must be actively load balanced at the application layer. 3. For Configuration 4 and 5 servers, Disaster Recovery services must be selected.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310010-A	Windows pConfig-1 Fully Managed – Platinum Tier	Per Physical Server
CCSU13310011-A	Windows pConfig-1 Fully	Per Physical Server

	Managed – Gold Tier	
CCSU13310012-A	Windows pConfig-1 Fully Managed – Silver Tier	Per Physical Server
CCSU13310013-A	Windows pConfig-1 Fully Managed – Bronze Tier	Per Physical Server
CCSU13310014-A	Windows pConfig-1 Fully Managed – Basic Tier	Per Physical Server
CCSU13310015-A	Windows pConfig-2 Fully Managed – Platinum Tier	Per Physical Server
CCSU13310016-A	Windows pConfig-2 Fully Managed – Gold Tier	Per Physical Server
CCSU13310017-A	Windows pConfig-2 Fully Managed – Silver Tier	Per Physical Server
CCSU13310018-A	Windows pConfig-2 Fully Managed – Bronze Tier	Per Physical Server
CCSU13310019-A	Windows pConfig-2 Fully Managed – Basic Tier	Per Physical Server
CCSU13310020-A	Windows pConfig-3 Fully Managed – Platinum Tier	Per Physical Server
CCSU13310021-A	Windows pConfig-3 Fully Managed – Gold Tier	Per Physical Server
CCSU13310022-A	Windows pConfig-3 Fully Managed – Silver Tier	Per Physical Server
CCSU13310023-A	Windows pConfig-3 Fully Managed – Bronze Tier	Per Physical Server
CCSU13310024-A	Windows pConfig-3 Fully Managed – Basic Tier	Per Physical Server

CCSU13310025-A	Windows pConfig-4 Fully Managed – Platinum Tier	Per Physical Server
CCSU13310026-A	Windows pConfig-4 Fully Managed – Gold Tier	Per Physical Server
CCSU13310027-A	Windows pConfig-4 Fully Managed – Silver Tier	Per Physical Server
CCSU13310028-A	Windows pConfig-4 Fully Managed – Bronze Tier	Per Physical Server
CCSU13310029-A	Windows pConfig-4 Fully Managed – Basic Tier	Per Physical Server
CCSU13310030-A	Windows pConfig-5 Fully Managed – Platinum Tier	Per Physical Server
CCSU13310031-A	Windows pConfig-5 Fully Managed – Gold Tier	Per Physical Server
CCSU13310032-A	Windows pConfig-5 Fully Managed – Silver Tier	Per Physical Server
CCSU13310033-A	Windows pConfig-5 Fully Managed – Bronze Tier	Per Physical Server
CCSU13310034-A	Windows pConfig-5 Fully Managed – Basic Tier	Per Physical Server

Service Attribute	*Service Attribute Description*	
Service Name	Fully Managed Physical Linux Server Support	
Detailed Description	Management of physical Linux servers, in alignment to Schedule F, section 3.2.4.4	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1) For Platinum, servers must be ordered in groups of three. Servers must be geographically dispersed, and actively load balanced at the application layer. 2) For Gold, servers must be ordered at a minimum in a pair of two, and must be actively load balanced at the application layer. 3) For Configuration 4 and 5 servers, Disaster Recovery services must be selected.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310044-A	Linux pConfig-1 Fully Managed – Platinum Tier	Per Physical Server
CCSU13310045-A	Linux pConfig-1 Fully Managed – Gold Tier	Per Physical Server

CCSU13310046-A	Linux pConfig-1 Fully Managed – Silver Tier	Per Physical Server
CCSU13310047-A	Linux pConfig-1 Fully Managed – Bronze Tier	Per Physical Server
CCSU13310048-A	Linux pConfig-1 Fully Managed – Basic Tier	Per Physical Server
CCSU13310049-A	Linux pConfig-2 Fully Managed – Platinum Tier	Per Physical Server
CCSU13310050-A	Linux pConfig-2 Fully Managed – Gold Tier	Per Physical Server
CCSU13310051-A	Linux pConfig-2 Fully Managed – Silver Tier	Per Physical Server
CCSU13310052-A	Linux pConfig-2 Fully Managed – Bronze Tier	Per Physical Server
CCSU13310053-A	Linux pConfig-2 Fully Managed – Basic Tier	Per Physical Server
CCSU13310054-A	Linux pConfig-3 Fully Managed – Platinum Tier	Per Physical Server
CCSU13310055-A	Linux pConfig-3 Fully Managed – Gold Tier	Per Physical Server
CCSU13310056-A	Linux pConfig-3 Fully Managed – Silver Tier	Per Physical Server
CCSU13310057-A	Linux pConfig-3 Fully Managed – Bronze Tier	Per Physical Server
CCSU13310058-A	Linux pConfig-3 Fully Managed – Basic Tier	Per Physical Server
CCSU13310059-A	Linux pConfig-4 Fully Managed – Platinum Tier	Per Physical Server

CCSU13310060-A	Linux pConfig-4 Fully Managed – Gold Tier	Per Physical Server
CCSU13310061-A	Linux pConfig-4 Fully Managed – Silver Tier	Per Physical Server
CCSU13310062-A	Linux pConfig-4 Fully Managed – Bronze Tier	Per Physical Server
CCSU13310063-A	Linux pConfig-4 Fully Managed – Basic Tier	Per Physical Server
CCSU13310064-A	Linux pConfig-5 Fully Managed – Platinum Tier	Per Physical Server
CCSU13310065-A	Linux pConfig-5 Fully Managed – Gold Tier	Per Physical Server
CCSU13310066-A	Linux pConfig-5 Fully Managed – Silver Tier	Per Physical Server
CCSU13310067-A	Linux pConfig-5 Fully Managed – Bronze Tier	Per Physical Server
CCSU13310068-A	Linux pConfig-5 Fully Managed – Basic Tier	Per Physical Server

Service Attribute	*Service Attribute Description*	
Service Name	Fully Managed Virtual Windows Server Support	
Detailed Description	Management of virtual Windows servers, in alignment to Schedule F, section 3.2.4.1	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1) For Platinum, servers must be ordered in groups of three. Servers must be geographically dispersed, and actively load balanced at the application layer. 2) For Gold, servers must be ordered at a minimum in a pair of two, and must be actively load balanced at the application layer. 3) For Configuration 4 and 5 servers, Disaster Recovery services must be selected.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310080-A	Windows vConfig-1 Fully Managed – Platinum Tier	Per Virtual Server
CCSU13310081-A	Windows vConfig-1 Fully Managed – Gold Tier	Per Virtual Server

CCSU13310082-A	Windows vConfig-1 Fully Managed – Silver Tier	Per Virtual Server
CCSU13310083-A	Windows vConfig-1 Fully Managed – Bronze Tier	Per Virtual Server
CCSU13310084-A	Windows vConfig-1 Fully Managed – Basic Tier	Per Virtual Server
CCSU13310085-A	Windows vConfig-2 Fully Managed – Platinum Tier	Per Virtual Server
CCSU13310086-A	Windows vConfig-2 Fully Managed – Gold Tier	Per Virtual Server
CCSU13310087-A	Windows vConfig-2 Fully Managed – Silver Tier	Per Virtual Server
CCSU13310088-A	Windows vConfig-2 Fully Managed – Bronze Tier	Per Virtual Server
CCSU13310089-A	Windows vConfig-2 Fully Managed – Basic Tier	Per Virtual Server
CCSU13310090-A	Windows vConfig-3 Fully Managed – Platinum Tier	Per Virtual Server
CCSU13310091-A	Windows vConfig-3 Fully Managed – Gold Tier	Per Virtual Server
CCSU13310092-A	Windows vConfig-3 Fully Managed – Silver Tier	Per Virtual Server
CCSU13310093-A	Windows vConfig-3 Fully Managed – Bronze Tier	Per Virtual Server
CCSU13310094-A	Windows vConfig-3 Fully Managed – Basic Tier	Per Virtual Server
CCSU13310095-A	Windows vConfig-4 Fully Managed – Platinum Tier	Per Virtual Server

CCSU13310096-A	Windows vConfig-4 Fully Managed – Gold Tier	Per Virtual Server
CCSU13310097-A	Windows vConfig-4 Fully Managed – Silver Tier	Per Virtual Server
CCSU13310098-A	Windows vConfig-4 Fully Managed – Bronze Tier	Per Virtual Server
CCSU13310099-A	Windows vConfig-4 Fully Managed – Basic Tier	Per Virtual Server
CCSU13310100-A	Windows vConfig-5 Fully Managed – Platinum Tier	Per Virtual Server
CCSU13310101-A	Windows vConfig-5 Fully Managed – Gold Tier	Per Virtual Server
CCSU13310102-A	Windows vConfig-5 Fully Managed – Silver Tier	Per Virtual Server
CCSU13310103-A	Windows vConfig-5 Fully Managed – Bronze Tier	Per Virtual Server
CCSU13310104-A	Windows vConfig-5 Fully Managed – Basic Tier	Per Virtual Server

Service Attribute	*Service Attribute Description*	
Service Name	Fully Managed Virtual Linux Server Support	
Detailed Description	Management of virtual Linux servers, in alignment to Schedule F, section 3.2.4.4	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1) For Platinum, servers must be ordered in groups of three. Servers must be geographically dispersed, and actively load balanced at the application layer. 2) For Gold, servers must be ordered at a minimum in a pair of two, and must be actively load balanced at the application layer. 3) For Configuration 4 and 5 servers, Disaster Recovery services must be selected.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310116-A	Linux vConfig-1 Fully Managed – Platinum Tier	Per Virtual Server
CCSU13310117-A	Linux vConfig-1 Fully Managed – Gold Tier	Per Virtual Server

CCSU13310118-A	Linux vConfig-1 Fully Managed – Silver Tier	Per Virtual Server
CCSU13310119-A	Linux vConfig-1 Fully Managed – Bronze Tier	Per Virtual Server
CCSU13310120-A	Linux vConfig-1 Fully Managed – Basic Tier	Per Virtual Server
CCSU13310121-A	Linux vConfig-2 Fully Managed – Platinum Tier	Per Virtual Server
CCSU13310122-A	Linux vConfig-2 Fully Managed – Gold Tier	Per Virtual Server
CCSU13310123-A	Linux vConfig-2 Fully Managed – Silver Tier	Per Virtual Server
CCSU13310124-A	Linux vConfig-2 Fully Managed – Bronze Tier	Per Virtual Server
CCSU13310125-A	Linux vConfig-2 Fully Managed – Basic Tier	Per Virtual Server
CCSU13310126-A	Linux vConfig-3 Fully Managed – Platinum Tier	Per Virtual Server
CCSU13310127-A	Linux vConfig-3 Fully Managed – Gold Tier	Per Virtual Server
CCSU13310128-A	Linux vConfig-3 Fully Managed – Silver Tier	Per Virtual Server
CCSU13310129-A	Linux vConfig-3 Fully Managed – Bronze Tier	Per Virtual Server
CCSU13310130-A	Linux vConfig-3 Fully Managed – Basic Tier	Per Virtual Server
CCSU13310131-A	Linux vConfig-4 Fully Managed – Platinum Tier	Per Virtual Server

CCSU13310132-A	Linux vConfig-4 Fully Managed – Gold Tier	Per Virtual Server
CCSU13310133-A	Linux vConfig-4 Fully Managed – Silver Tier	Per Virtual Server
CCSU13310134-A	Linux vConfig-4 Fully Managed – Bronze Tier	Per Virtual Server
CCSU13310135-A	Linux vConfig-4 Fully Managed – Basic Tier	Per Virtual Server
CCSU13310136-A	Linux vConfig-5 Fully Managed – Platinum Tier	Per Virtual Server
CCSU13310137-A	Linux vConfig-5 Fully Managed – Gold Tier	Per Virtual Server
CCSU13310138-A	Linux vConfig-5 Fully Managed – Silver Tier	Per Virtual Server
CCSU13310139-A	Linux vConfig-5 Fully Managed – Bronze Tier	Per Virtual Server
CCSU13310140-A	Linux vConfig-5 Fully Managed – Basic Tier	Per Virtual Server

Fully Managed - P-Series Server (AIX)

P-Series (AIX) Server Configuration - Configuration Components

Service Attribute	*Service Attribute Description*	
Service Name	AIX Config – 1, 2, 3, 4, 5 – 3.0GHz POWER7 Server	
Detailed Description	AIX Config – 1, 2, 3, 4, 5 – 3.0GHz POWER7 Server	
Service Customers / Users	Any participating Commonwealth agency or office.	
Service Prerequisites	Not eligible for separate purchase; must be purchased in conjunction with a Fully Managed AIX Config and AIX Config – 1, 2, 3, 4, 5 – AIX License	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
Unisys assigned	AIX Config – 1, 2, 3, 4, 5 – 3.0GHz POWER7 Server	Per Server

Service Attribute	*Service Attribute Description*	
Service Name	AIX Config – 1,2 ,3 ,4 ,5 – Cores	
Detailed Description	AIX Config – 1, 2, 3, 4, 5 – Cores	
Service Customers / Users	Any participating Commonwealth agency or office.	
Service Prerequisites	May be optionally added to purchase of AIX Config – 1, 2, 3, 4, 5 – 3.0GHz POWER7 Server.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13310141-A	AIX Config – 1, 2, 3, 4, 5 – Cores	Per .5 Core

Service Attribute	*Service Attribute Description*	
Service Name	AIX Config – 1, 2, 3, 4, 5 – GB RAM	
Detailed Description	AIX Config – 1, 2, 3, 4, 5 – GB RAMs	
Service Customers / Users	Any participating Commonwealth agency or office.	
Service Prerequisites	May be optionally added to purchase of AIX Config – 1, 2, 3, 4, 5 – 3.0GHz POWER7 Server.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13310142-A	AIX Config – 1, 2, 3, 4, 5 – GB RAMs	Per 1.0 GB RAM

Service Attribute	*Service Attribute Description*	
Service Name	AIX Config – 1, 2, 3, 4, 5 – AIX License	
Detailed Description	AIX Config – 1, 2, 3, 4, 5 – AIX License	
Service Customers / Users	Any participating Commonwealth agency or office.	
Service Prerequisites	Not eligible for separate purchase; must be purchased in conjunction with a Fully Managed AIX Config and AIX Config – 1, 2, 3, 4, 5 – 3.0GHz POWER7 Server.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13310143-A	AIX Config – 1, 2, 3, 4, 5 – AIX License	Per AIX License

Service Attribute	*Service Attribute Description*	
Service Name	AIX Config-4 DR Server	
Detailed Description	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	
Service Customers / Users	Any participating Commonwealth agency or office.	
Service Prerequisites	Must be purchased in conjunction with a Fully Managed AIX Config and its prerequisites.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13310145-A	AIX Config-4 DR Server	Per Config

Service Attribute	*Service Attribute Description*	
Service Name	AIX Config-5 DR Server	
Detailed Description	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	
Service Customers / Users	Any participating Commonwealth agency or office.	
Service Prerequisites	Must be purchased in conjunction with a Fully Managed AIX Config and its prerequisites.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13310146-A	AIX Config-5 DR Server	Per Config

P-Series (AIX) Server Configuration – Orderable Configurations

Service Attribute	*Service Attribute Description*	
Service Name	P-Series (AIX) Physical Server – Configuration 1	
Detailed Description	One AIX Server with 3.0GHz POWER7, 0.5 Cores, 6 GB RAM, AIX	
Service Customers / Users	Any participating Commonwealth agency or office.	
Service Prerequisites	Selection of appropriate tier (Platinum, Gold, Silver, Bronze, Basic) of server support	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSI13310239-A	AIX Config-1	Per Server

Service Attribute	*Service Attribute Description*	
Service Name	pSeries (AIX) Server – Configuration 2	
Detailed Description	One AIX Server with 3.0GHz POWER7, 1.0 Cores, 12 GB RAM, AIX	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	Selection of appropriate tier (Platinum, Gold, Silver, Bronze, Basic) of server support	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSI13310240-A	AIX Config-2	Per Server

Service Attribute	*Service Attribute Description*	
Service Name	PSeries (AIX) Server – Configuration 3	
Detailed Description	One AIX Server with 3.0GHz POWER7, 1.5 Cores, 18 GB RAM, AIX	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	Selection of appropriate tier (Platinum, Gold, Silver, Bronze, Basic) of server support	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSI13310241-A	AIX Config-3	Per Server

Service Attribute	*Service Attribute Description*	
Service Name	PSeries (AIX) Server – Configuration 4	
Detailed Description	One AIX Server with 3.0GHz POWER7, 1.5 Cores, 18 GB RAM, AIX, Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	Selection of appropriate tier (Platinum, Gold, Silver, Bronze, Basic) of server support	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSI13310242-A	AIX Config-4	Per Server

Service Attribute	*Service Attribute Description*	
Service Name	PSeries (AIX) Server – Configuration 5	
Detailed Description	One AIX Server with 3.0GHz POWER7, 1.5 Cores, 18 GB RAM, AIX, Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	Selection of appropriate tier (Platinum, Gold, Silver, Bronze, Basic) of server support	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSI13310243-A	AIX Config-5	Per Server

P-Series (AIX) Tiers of Service

Service Attribute	*Service Attribute Description*	
Service Name	Fully Managed P-Series (AIX) Server Support	
Detailed Description	Management of AIX servers, in alignment to Schedule F, section 3.2.4.4	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites		
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSI13310147-A	P-Series (AIX) Config-1 Fully Managed – Platinum Tier	Per Physical Server
CCSI13310148-A	P-Series (AIX) Config-1 Fully Managed – Gold Tier	Per Physical Server
CCSI13310149-A	P-Series (AIX) Config-1 Fully Managed – Silver Tier	Per Physical Server
CCSI13310150-A	P-Series (AIX) Config-1 Fully Managed – Bronze Tier	Per Physical Server
CCSI13310151-A	P-Series (AIX) Config-1 Fully Managed – Basic Tier	Per Physical Server

CCSI13310152-A	P-Series (AIX) Config-2 Fully Managed – Platinum Tier	Per Physical Server
CCSI13310153-A	P-Series (AIX) Config-2 Fully Managed – Gold Tier	Per Physical Server
CCSI13310154-A	P-Series (AIX) Config-2 Fully Managed – Silver Tier	Per Physical Server
CCSI13310155-A	P-Series (AIX) Config-2 Fully Managed – Bronze Tier	Per Physical Server
CCSI13310156-A	P-Series (AIX) Config-2 Fully Managed – Basic Tier	Per Physical Server
CCSI13310157-A	P-Series (AIX) Config-3 Fully Managed – Platinum Tier	Per Physical Server
CCSI13310158-A	P-Series (AIX) Config-3 Fully Managed – Gold Tier	Per Physical Server
CCSI13310159-A	P-Series (AIX) Config-3 Fully Managed – Silver Tier	Per Physical Server
CCSI13310160-A	P-Series (AIX) Config-3 Fully Managed – Bronze Tier	Per Physical Server
CCSI13310161-A	P-Series (AIX) Config-3 Fully Managed – Basic Tier	Per Physical Server
CCSI13310162-A	P-Series (AIX) Config-4 Fully Managed – Platinum Tier	Per Physical Server
CCSI13310163-A	P-Series (AIX) Config-4 Fully Managed – Gold Tier	Per Physical Server
CCSI13310164-A	P-Series (AIX) Config-4 Fully Managed – Silver Tier	Per Physical Server
CCSI13310165-A	P-Series (AIX) Config-4 Fully Managed – Bronze Tier	Per Physical Server

CCSI13310166-A	P-Series (AIX) Config-4 Fully Managed – Basic Tier	Per Physical Server
CCSI13310167-A	P-Series (AIX) Config-5 Fully Managed – Platinum Tier	Per Physical Server
CCSI13310168-A	P-Series (AIX) Config-5 Fully Managed – Gold Tier	Per Physical Server
CCSI13310169-A	P-Series (AIX) Config-5 Fully Managed – Silver Tier	Per Physical Server
CCSI13310170-A	P-Series (AIX) Config-5 Fully Managed – Bronze Tier	Per Physical Server
CCSI13310171-A	P-Series (AIX) Config-5 Fully Managed – Basic Tier	Per Physical Server

Compute Services - Managed Only Services

Managed Only Services – X86 (Windows and Linux)

Service Attribute	*Service Attribute Description*	
Service Name	Managed Only Services for Agency Owned Windows or Linux Server Support	
Detailed Description	Windows management services or Commonwealth owned Windows service, in alignment to the requirements in Schedule F, Section 3.2.4.1	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1) For Platinum, three Commonwealth owned Windows servers must be shipped to the data centers. 2) For Gold, two Commonwealth owned servers must be shipped to the data center. 3) For Bronze and Basic, one Commonwealth server must be shipped to the data center. 4) Must order a commissioning/decommissioning service, one for each server.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**

CCSU13320001-A	Windows / Linux – Platinum Tier	Per Server Instance
CCSU13320002-A	Windows / Linux - Gold Tier	Per Virtual Server
CCSU13320003-A	Windows / Linux – Silver Tier	Per Virtual Server
CCSU13320004-A	Windows / Linux – Bronze Tier	Per Virtual Server
CCSU13320005-A	Windows / Linux– Basic Tier	Per Virtual Server

Managed Only Services – P-Series (AIX)

Service Attribute	*Service Attribute Description*	
Service Name	Managed Only Services for Agency Owned AIX Server Support	
Detailed Description	AIX management services for Commonwealth owned AIX service, in alignment to the requirements in Schedule F, Section 3.2.4.4	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites		
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSI13320006-A	AIX – Platinum Tier	Per Server Instance
CCSI13320007-A	AIX - Gold Tier	Per Virtual Server
CCSI13320008-A	AIX – Silver Tier	Per Virtual Server
CCSI13320009-A	AIX – Bronze Tier	Per Virtual Server
CCSI13320010-A	AIX– Basic Tier	Per Virtual Server

This Page Intentionally Left Blank

Fully Managed - Storage and Backup

Storage Services

Service Attribute	*Service Attribute Description*	
Service Name	Fully Managed – Storage Service – Dedicated – Config 1 – SAN RAID 5	
Detailed Description	Storage Service – Dedicated – Config 1 – SAN Raid 5	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites		
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSZ13310172-A	Dedicated – Config 1 – SAN RAID 5	Per GB

Service Attribute	*Service Attribute Description*	
Service Name	Fully Managed – Storage Service – Dedicated – Config 2 – SAN Raid 10	
Detailed Description	– Storage Service – Dedicated – Config 2 – SAN Raid 10	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites		
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSZ13310173-A	Dedicated – Config 10 – SAN RAID 10	Per GB

Service Attribute	*Service Attribute Description*	
Service Name	Fully Managed – Storage Service – Dedicated – Config 3 – Net Attached	
Detailed Description	Storage Service – Dedicated – Config 3 – Net Attached	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites		
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSZ13310174-A	Dedicated – Config 3 – Net Attached	Per GB

Tape and Backup Services

Service Attribute	*Service Attribute Description*	
Service Name	Fully Managed – Tape and Backup – Server Tape Stored	
Detailed Description	– Tape and Backup – Server Tape Stored	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites		
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310175-A	Server Tape Stored	Per GB Stored

Service Attribute	*Service Attribute Description*	
Service Name	Fully Managed – Storage Service – Tape and Backup – Offsite Tape Storage	
Detailed Description	Storage Service – Tape and Backup – Offsite Tape Storage	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites		
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310176-A	Offsite Tape Storage	Per Tape

This Page Intentionally Left Blank

Compute Services - Co-Location Services

Co-Location Services - Configuration Components

Service Attribute	*Service Attribute Description*	
Service Name	Co-Location Services - Cabinet	
Detailed Description	Co-Location Services - Cabinet	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites		
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13330001-A	Co-Lo Config-1	Per ¼ Rack (10U) Configuration
CCSU13330002-A	Co-Lo Config-2	Per ½ Rack (21U) Configuration
CCSU13330003-A	Co-Lo Config-3	Per Rack (42U) Configuration

Service Attribute	*Service Attribute Description*	
Service Name	Colocation Services – Network Bandwidth	
Detailed Description	Colocation Services – Network Bandwidth	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites		
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13330004-A	Network Bandwidth	Per GB

Service Attribute	*Service Attribute Description*	
Service Name	Colocation Service – 100 Mb/s Uplink	
Detailed Description	Colocation Service – 100 Mb/s Uplink	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites		
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13330005-A	100 Mb/s Uplink	Per Uplink

Service Attribute	*Service Attribute Description*	
Service Name	Colocation Service – IP Address	
Detailed Description	Colocation Service – IP Address	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites		
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13330006-A	IP Address	Per IP address

Service Attribute	*Service Attribute Description*	
Service Name	AC Circuit	
Detailed Description	AC Circuit	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites		
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13330007-A	110V AC Circuit	Per Circuit

Co-Location Services – Combined Configurations

Service Attribute	*Service Attribute Description*	
Service Name	Co-Location Services –Config-1 - ¼ Cabinet Configuration	
Detailed Description	Includes 10U bay – includes 6 IP addresses, 5,000 GB of network bandwidth, 100Mb/s uplink, 5 110VAC circuits	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites		
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13330008-A	Co-Lo Config-1	Per ¼ Rack (10U) Configuration

Service Attribute	*Service Attribute Description*	
Service Name	Co-Location Services –Config-2 - ½ Cabinet Configuration	
Detailed Description	Includes 21U bay – includes 14 IP addresses, 10,000GB of network bandwidth, 100Mb/s uplink, 10 110VAC circuits	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites		
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13330009-A	Co-Lo Config-2	Per ½ Rack (21U) Configuration

Service Attribute	*Service Attribute Description*	
Service Name	Co-Location Services –Config-3 - Full Cabinet Configuration	
Detailed Description	Includes 42U cabinet – includes 30 IP addresses, 20,000GB of network bandwidth, 100Mb/s uplink, 20 110VAC circuits	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites		
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13330010-A	Co-Lo Config-3	Per Rack (42U) Configuration

Compute Services - Mainframe Services

IBM Mainframe Storage and Backup

IBM Mainframe Storage Services

Service Attribute	*Service Attribute Description*	
Service Name	IBM Mainframe Allocated DASD	
Detailed Description	IBM Mainframe Allocated DASD	
Service Customers / Users	Any participating Commonwealth agency or department.	
Service Prerequisites	None	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13310177-A	IBM Mainframe Allocated DASDs	Per GB

IBM Mainframe Backup and Tape Services

Service Attribute	*Service Attribute Description*	
Service Name	IBM Tapes in Storage – Virtual Tape Storage (VTS)	
Detailed Description	IBM Tapes in Storage - VTS	
Service Customers / Users	Any participating Commonwealth agency or department.	
Service Prerequisites	None	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13310178-A	IBM Tapes in Storage - VTS	Per 1.0 GB

Service Attribute	*Service Attribute Description*	
Service Name	IBM Offsite Tape Storage	
Detailed Description	IBM Offsite Tape Storage	
Service Customers / Users	Any participating Commonwealth agency or department.	
Service Prerequisites	None	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13310179-A	IBM Offsite Tape Storage	Per Tape

IBM Mainframe Service

IBM Mainframe Configuration - Configuration Components

Service Attribute	*Service Attribute Description*	
Service Name	IBM System zEnterprise Processor z/OS	
Detailed Description	IBM System zEnterprise Processor z/OS	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites		
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13310180-A	IBM Mainframe – Config-1 - IBM System zEnterprise Processor z/OS	Per MIP

Service Attribute	*Service Attribute Description*	
Service Name	IBM System zEnterprise Processor Virtual Linux Production IFL	
Detailed Description	3 IBM System zEnterprise Processor Virtual Linux Prod IFLs	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites		
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13310181-A	IBM Mainframe Config 2,3 - IBM System zEnterprise Processor Virtual Linux Prod IFL	Per MIP

Service Attribute	*Service Attribute Description*	
Service Name	IBM iSeries (AS/400)	
Detailed Description	IBM iSeries (AS/400)	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites		
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13310182-A	IBM AS400 Config-1,2 - IBM iSeries (AS/400)	Per CPW

Service Attribute	*Service Attribute Description*	
Service Name	IBM Mainframe Config-3 – Disaster Recovery Server with 24 hour Recovery Point Objective	
Detailed Description	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1) A corresponding IBM Mainframe Config	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSI13310183-A	IBM Mainframe Config-3 – Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization Site's Local SAN Storage from hourly data synchronization	Per Config

Service Attribute	*Service Attribute Description*	
Service Name	IBM AS400 Config-2 – Disaster Recovery Server with 24 hour Recovery Point Objective	
Detailed Description	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1) A corresponding AS400 Config	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSI13310184-A	IBM AS400 Config-2 – Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization Site's Local SAN Storage from hourly data synchronization	Per Config

IBM Mainframe Configuration – Orderable Configurations

Service Attribute	*Service Attribute Description*	
Service Name	IBM System zEnterprise Processor z/OS – Config-1	
Detailed Description	IBM System zEnterprise Processor z/OS	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	Selection of appropriate tier (Platinum, Gold, Basic) of server support	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13310244-A	IBM Mainframe – Config-1 - IBM System zEnterprise Processor z/OS	Per MIP

Service Attribute	*Service Attribute Description*	
Service Name	IBM System zEnterprise Processor Virtual Linux Production IFL – Config-2	
Detailed Description	IBM System zEnterprise Processor Virtual Linux Production IFL	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	Selection of appropriate tier (Platinum, Gold, Basic) of server support	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13310245-A	IBM Mainframe Config 2 - IBM System zEnterprise Processor Virtual Linux Prod IFL	Per MIP

Service Attribute	*Service Attribute Description*	
Service Name	IBM System zEnterprise Processor Virtual Linux Production IFL – Config-3	
Detailed Description	IBM System zEnterprise Processor Virtual Linux Prod IFL Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	Selection of appropriate tier (Platinum, Gold, Basic) of server support	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13310246-A	IBM Mainframe Config 3 - IBM System zEnterprise Processor Virtual Linux Prod IFL	Per MIP

Service Attribute	*Service Attribute Description*	
Service Name	IBM iSeries (AS/400) – Config-1	
Detailed Description	IBM iSeries (AS/400)	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	Selection of appropriate tier (Platinum, Gold, Basic) of server support	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13310247-A	IBM AS400 Config-1 - IBM iSeries (AS/400)	Per CPW

Service Attribute	*Service Attribute Description*	
Service Name	IBM iSeries (AS/400) – Config-2	
Detailed Description	IBM iSeries / AS400 Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	Selection of appropriate tier (Platinum, Gold, Basic) of server support	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13310248-A	IBM AS400 Config-2 - IBM iSeries (AS/400)	Per CPW

BM Mainframe Tiers of Service

Service Attribute	*Service Attribute Description*	
Service Name	IBM Mainframe Fully Managed Server Support	
Detailed Description	Management of Mainframe servers, in alignment to Schedule F, section 3.2.4.5	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	IBM Mainframe Config – 1 IBM System zEnterprise Processor z/OS, or IBM Mainframe Config – 2, 3 IBM System zEnterprise Processor Virtual Linux Prod IFL.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSI13310185-A	IBM Mainframe Config-1 Fully Managed – Platinum Tier	Per Physical Server
CCSI13310186-A	IBM Mainframe Config-1 Fully Managed – Gold Tier	Per Physical Server
CCSI13310187-A	IBM Mainframe Config-1 Fully Managed – Basic Tier	Per Physical Server
CCSI13310188-A	IBM Mainframe Config-2 Fully	Per Physical Server

	Managed – Platinum Tier	
CCSI13310189-A	IBM Mainframe Config-2 Fully Managed – Gold Tier	Per Physical Server
CCSI13310190-A	IBM Mainframe Config-2 Fully Managed – Basic Tier	Per Physical Server
CCSI13310191-A	IBM Mainframe Config-3 Fully Managed – Platinum Tier	Per Physical Server
CCSI13310192-A	IBM Mainframe Config-3 Fully Managed – Gold Tier	Per Physical Server
CCSI13310193-A	IBM Mainframe Config-3 Fully Managed – Basic Tier	Per Physical Server

Service Attribute	*Service Attribute Description*	
Service Name	IBM iSeries (AS/400) Managed Server Support	
Detailed Description	Management of Mainframe servers, in alignment to Schedule F, section 3.2.4.5	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	Must be ordered with IBM AS400 Config 1, 2 IBM iSeries / AS400.	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSI13310194-A	IBM Mainframe Config-1 Fully Managed – Platinum Tier	Per Physical Server
CCSI13310195-A	IBM Mainframe Config-1 Fully Managed – Gold Tier	Per Physical Server
CCSI13310196-A	IBM Mainframe Config-1 Fully Managed – Basic Tier	Per Physical Server
CCSI13310197-A	IBM Mainframe Config-2 Fully Managed – Platinum Tier	Per Physical Server
CCSI13310198-A	IBM Mainframe Config-2 Fully Managed – Gold Tier	Per Physical Server
CCSI13310199-A	IBM Mainframe Config-2 Fully Managed – Basic Tier	Per Physical Server

Unisys Mainframe Storage and Backup

Unisys Mainframe Storage Services

Service Attribute	*Service Attribute Description*	
Service Name	UNISYS Mainframe – Allocated DASD	
Detailed Description	UNISYS Mainframe – Allocated DASD	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites		
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310200-A	UNISYS Mainframe Allocated DASD	Per GB

Unisys Mainframe Backup and Tape Services

Service Attribute	*Service Attribute Description*	
Service Name	UNISYS Mainframe – Tapes in Storage – Virtual Tape Storage (VTS)	
Detailed Description	UNISYS Mainframe – Tapes in Storage – Virtual Tape Storage (VTS)	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites		
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310201-A	UNISYS Tapes in Storage - VTS	Per GB Stored

Service Attribute	*Service Attribute Description*	
Service Name	UNISYS Mainframe – Offsite Tape Storage	
Detailed Description	UNISYS Mainframe – Offsite Tape Storage	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites		
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310202-A	UNISYS Offsite Tape Storage	Per Tape/Reel

Unisys Mainframe Service

Unisys Mainframe Configuration - Configuration Components

Service Attribute	*Service Attribute Description*	
Service Name	Unisys Mainframe (ClearPath Dorado) – Config-1,3	
Detailed Description	Provides Unisys Dorado (OS 2200) mainframe MIPS and operating system. Config -1 Production Only Config – 3 Production and DR	
Service Customers / Users	Department of Public Welfare Pennsylvania State Police	
Service Prerequisites	What is required before this service or service element be ordered? 1) Solution Request submittal to confirm requested system meets application processing requirements 2) For Config -3 Total of Production and DR MIPS identified	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13310203-A	Unisys Mainframe Config 1, 3 - Unisys (ClearPath / Dorado)	Per MIP

Service Attribute	*Service Attribute Description*	
Service Name	Unisys Mainframe (ClearPath Libra) – Config2,4	
Detailed Description	Provides Unisys Libra (MCP) mainframe MIPS and operating system. Config -2 Production Only Config -4 Production and DR	
Service Customers / Users	Pennsylvania Game Commission	
Service Prerequisites	What is required before this service or service element be ordered? 1) Solution Request submittal to confirm requested system meets application processing requirements 2) For Config -3 Total of Production and DR MIPS identified	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13310204-A	Unisys Mainframe Config- 2, 4 - Unisys (ClearPath / Libra)	Per MIP

Service Attribute	*Service Attribute Description*	
Service Name	Unisys Mainframe Config-3 – ClearPath / Dorado Disaster Recovery Server with 24 hour Recovery Point Objective	
Detailed Description	Provides Unisys Dorado (OS 2200) mainframe MIPS and operating system. Provides both Production and DR MIPS	
Service Customers / Users	Department of Public Welfare Pennsylvania State Police	
Service Prerequisites	What is required before this service or service element be ordered? 1) Solution Request submittal to confirm requested system meets application processing requirements 2) Total of Production and DR MIPS identified 3) Data replication services ordered	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310205-A	Unisys Mainframe Config-3 – Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from	Per Config

	hourly data synchronization Site's Local SAN Storage from hourly data synchronization	

Service Attribute	*Service Attribute Description*	
Service Name	Unisys Mainframe Config-4 – ClearPath / Libra Disaster Recovery Server with 24 hour Recovery Point Objective	
Detailed Description	Provides Unisys Libra (MCP) mainframe MIPS and operating system. Provides both Production and DR MIPS	
Service Customers / Users	Pennsylvania Game Commission	
Service Prerequisites	What is required before this service or service element be ordered? 1) Solution Request submittal to confirm requested system meets application processing requirements 2) Total of Production and DR MIPS identified 3) Data replication services ordered	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310206-A	Unisys Mainframe Config-4 – Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization Site's Local SAN Storage from	Per Config

	hourly data synchronization	

Unisys Mainframe Configuration – Orderable Configurations

Service Attribute	*Service Attribute Description*	
Service Name	Unisys Mainframe (ClearPath Dorado) – Config-1	
Detailed Description	Provides Unisys Dorado (OS 2200) mainframe MIPS and operating system. Provides Production MIPS	
Service Customers / Users	Department of Public Welfare Pennsylvania State Police	
Service Prerequisites	What is required before this service or service element be ordered? 1) Solution Request submittal to confirm requested system meets application processing requirements	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13310249-A	Unisys Mainframe Config 1 - Unisys (ClearPath / Dorado)	Per MIP

Service Attribute	*Service Attribute Description*	
Service Name	Unisys Mainframe (ClearPath Libra) – Config 2	
Detailed Description	Provides Unisys Libra (MCP) mainframe MIPS and operating system. Provides both Production and DR MIPS	
Service Customers / Users	Pennsylvania Game Commission	
Service Prerequisites	What is required before this service or service element be ordered? 1) Solution Request submittal to confirm requested system meets application processing requirements 2) Total of Production and DR MIPS identified 3) Data replication services ordered	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13310250-A	Unisys Mainframe Config- 2 - Unisys (ClearPath / Libra)	Per MIP

Service Attribute	*Service Attribute Description*	
Service Name	Unisys Mainframe (ClearPath Dorado) – Config-3	
Detailed Description	Provides Unisys Dorado (OS 2200) mainframe MIPS and operating system. Provides both Production and DR MIPS	
Service Customers / Users	Department of Public Welfare Pennsylvania State Police	
Service Prerequisites	What is required before this service or service element be ordered? 1) Solution Request submittal to confirm requested system meets application processing requirements 2) Total of Production and DR MIPS identified 3) Data replication services ordered	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13310251-A	Unisys Mainframe Config 3 - Unisys (ClearPath / Dorado)	Per MIP

Service Attribute	*Service Attribute Description*	
Service Name	Unisys Mainframe (ClearPath Libra) – Config-4	
Detailed Description	Provides Unisys Libra (MCP) mainframe MIPS and operating system. Provides both Production and DR MIPS	
Service Customers / Users	Pennsylvania Game Commission	
Service Prerequisites	What is required before this service or service element be ordered? 1) Solution Request submittal to confirm requested system meets application processing requirements 2) Total of Production and DR MIPS identified 3) Data replication services ordered	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13310252-A	Unisys Mainframe Config-4 - Unisys (ClearPath / Libra)	Per MIP

Unisys Mainframe Tiers of Service

Service Attribute	*Service Attribute Description*	
Service Name	UNISYS Mainframe Fully Managed Server Support	
Detailed Description	Provides hardware, operating system and operational support to meet required service level	
Service Customers / Users	Department of Public Welfare Pennsylvania State Police Pennsylvania Game Commission	
Service Prerequisites	What is required before this service or service element be ordered? 1) Solution Request submittal 2) Solution Request to confirm requested system and staff meets application processing requirements	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13310207-A	UNISYS Mainframe Config-1 Fully Managed – Platinum Tier	Per Physical Server
CCSU13310208-A	UNISYS Mainframe Config-1 Fully Managed – Gold Tier	Per Physical Server
CCSU13310209-A	UNISYS Mainframe Config-1 Fully Managed – Basic Tier	Per Physical Server
CCSU13310210-A	UNISYS Mainframe Config-2 Fully Managed – Platinum Tier	Per Physical Server

CCSU13310211-A	UNISYS Mainframe Config-2 Fully Managed – Gold Tier	Per Physical Server
CCSU13310212-A	UNISYS Mainframe Config-2 Fully Managed – Basic Tier	Per Physical Server
CCSU13310213-A	UNISYS Mainframe Config-3 Fully Managed – Platinum Tier	Per Physical Server
CCSU13310214-A	UNISYS Mainframe Config-3 Fully Managed – Gold Tier	Per Physical Server
CCSU13310215-A	UNISYS Mainframe Config-3 Fully Managed – Basic Tier	Per Physical Server
CCSU13310216-A	UNISYS Mainframe Config-4 Fully Managed – Platinum Tier	Per Physical Server
CCSU13310217-A	UNISYS Mainframe Config-4 Fully Managed – Gold Tier	Per Physical Server
CCSU13310218-A	UNISYS Mainframe Config-4 Fully Managed – Basic Tier	Per Physical Server

This Page Intentionally Left Blank

Compute Services - Infrastructure as a Service

Infrastructure as a Service (IaaS) – Windows and Linux

IaaS Windows/Linux Configuration - Configuration Components

Service Attribute	*Service Attribute Description*	
Service Name	Infrastructure as a Service - Windows / Linux Virtual Configuration 1 – 2 vCPU	
Detailed Description	Two virtual CPU's for a Virtual Windows or Linux Server	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	A previously ordered configuration 1 virtual Windows or Linux server	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13340001-A	IaaS Windows vConfig-1 – 2 vCPU	Per Virtual Server
CCSU13340012-A	IaaS Linux vConfig-1 – 2 vCPU	Per Virtual Server

Service Attribute	*Service Attribute Description*	
Service Name	Infrastructure as a Service - Windows / Linux Virtual Configuration 2, 4, 5 – 4 vCPU	
Detailed Description	Four virtual CPU's for Windows or Linux virtual machine.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1) A previously ordered configuration 2,4, or 5 virtual Windows or Linux server 2) For configuration 4 and 5, incremental CPU's must be ordered for both virtual servers. A previously ordered configuration 1 virtual Windows or Linux server 3) For configuration 4 and 5, incremental CPU's must be ordered for both virtual servers.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13340002-A	IaaS Windows vConfig – 2, 4, 5 – 4 vCPU	Per Virtual Server
CCSU13340013-A	IaaS Linux vConfig – 2, 4, 5 – 4 vCPU	Per Virtual Server

Service Attribute	*Service Attribute Description*	
Service Name	Infrastructure as a Service - Windows / Linux Virtual Configuration 3 – 8 vCPU	
Detailed Description	Eight virtual CPU's for configuration 3 Windows and Linux virtual Servers	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	A previously ordered configuration 3 virtual Windows or Linux server	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13340003-A	IaaS Windows vConfig – 3 – 8 vCPU	Per Virtual Server
CCSU13340014-A	IaaS Linux vConfig – 3 – 8 vCPU	Per Virtual Server

Service Attribute	*Service Attribute Description*	
Service Name	Infrastructure as a Service - Windows / Linux Virtual Configuration – 1, 2, 3, 4, 5 - GB RAM	
Detailed Description	One GB of Random Access Memory for a virtual Windows or Linux machine.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1) A previously ordered configuration virtual Windows or Linux server 2) For configuration 4 and 5, incremental memory must be ordered for both virtual servers.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13340004-A	IaaS Windows vConfig-1, 2, 3, 4, 5 - GB RAM	Per GB
CCSU13340015-A	IaaS Linux vConfig-1, 2, 3, 4, 5 - GB RAM	Per GB

Service Attribute	*Service Attribute Description*	
Service Name	Infrastructure as a Service - Windows – Virtual Configuration 1, 2, 3, 4, 5 – Windows Server 2008 R2	
Detailed Description	A Windows Server 2008 R2 License for a virtual windows server	
Service Customers / Users		
Service Prerequisites	Cannot Be Ordered Separately	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13340005-A	IaaS Windows vConfig-1, 2, 3, 4, 5 – Windows Server 2008 R2	Per License

Service Attribute	*Service Attribute Description*	
Service Name	Infrastructure as a Service - Linux – Virtual Configuration 1, 2, 3, 4, 5 – Red Hat or SUSE	
Detailed Description	A RedHat or SUSE Linux License for a virtual Linux server	
Service Customers / Users		
Service Prerequisites	Cannot Be Ordered Separately	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13340016-A	IaaS Linux vConfig-1, 2, 3, 4, 5 – Red Hat or SUSE	Per License

Service Attribute	*Service Attribute Description*	
Service Name	Infrastructure as a Service - Windows / Linux Virtual Configuration-1, 2, 3, 4, 5 – Firewall/IDS	
Detailed Description	One Firewall/IDS for a Windows or Linux virtual machine	
Service Customers / Users		
Service Prerequisites	Cannot Be Ordered Separately	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13340006-A	IaaS Windows vConfig-1, 2, 3, 4, 5 – Firewall/IDS	Per License
CCSU13340017-A	IaaS Linux vConfig-1, 2, 3, 4, 5 – Firewall/IDS	Per License

Service Attribute	*Service Attribute Description*	
Service Name	Infrastructure as a Service - Windows / Linux Virtual Configuration-1, 2, 3, 4, 5– Site to Site VPN	
Detailed Description	One Site to Site VPN for a Windows or Linux virtual machine.	
Service Customers / Users		
Service Prerequisites	Cannot Be Ordered Separately	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13340007-A	IaaS Windows vConfig-1, 2, 3, 4, 5 – Site to Site VPN	Per License
CCSU13340018-A	IaaS Linux vConfig-1, 2, 3, 4, 5 – Site to Site VPN	Per License

Service Attribute	*Service Attribute Description*	
Service Name	Infrastructure as a Service - Windows / Linux VConfig-1, 2, 3, 4, 5 - VPN Client	
Detailed Description	One VPN Client for a Windows or Linux virtual machine.	
Service Customers / Users		
Service Prerequisites	Cannot Be Ordered Separately	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13340008-A	IaaS Windows vConfig-1, 2, 3, 4, 5 – VPN Client	Per License
CCSU13340008-A	IaaS Linux vConfig-1, 2, 3, 4, 5 – VPN Client	Per License

Service Attribute	*Service Attribute Description*	
Service Name	Infrastructure as a Service - Windows / Linux vConfig – 4 – Disaster Recovery Server with 24 hour Recovery Point Objective	
Detailed Description	Provides two virtual configuration 4 servers, with one configured as a disaster recovery server. The disaster recovery server has a 24 hour Recovery Point Objective.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1) At least two servers must be ordered for this configuration. 2) Must order a commissioning/decommissioning service, one for each server.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13340010-A	IaaS Windows vConfig-4 – Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization Site's Local SAN Storage from hourly data synchronization	Per Service

CCSU13340021-A	IaaS Linux vConfig-4 – Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization Site’s Local SAN Storage from hourly data synchronization	Per Service

Service Attribute	*Service Attribute Description*	
Service Name	Infrastructure as a Service - Windows / Linux vConfig – 5 – Disaster Recovery Server with 72 hour Recovery Point Objective	
Detailed Description	Provides two physical configuration 5 servers, with one configured as a disaster recovery server. The disaster recovery server has a 72 hour Recovery Point Objective.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1) At least two servers must be ordered for this configuration. 2) Must order a commissioning/decommissioning service, one for each server.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13340011-A	IaaS Windows vConfig-5 - Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Service
CCSU13340022-A	IaaS Linux vConfig-5 - Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape	Per Service

	Backups	

IaaS Windows Configuration – Orderable Configurations

Service Attribute	*Service Attribute Description*	
Service Name	Infrastructure As a Service – Windows vConfig 1	
Detailed Description	One virtual Windows server with 2 virtual CPU's, with 4 GB of RAM	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	Must order a commissioning/decommissioning service, one for each server.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13340029-A	IaaS Windows vConfig-1	Per Server

Service Attribute	*Service Attribute Description*	
Service Name	Infrastructure as a Service – Windows vConfig-2	
Detailed Description	One virtual Windows server with 4 virtual CPU's, with 16 GB of RAM	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	Must order a commissioning/decommissioning service, one for each server.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13340030-A	IaaS Windows Config-2	Per Server

Service Attribute	*Service Attribute Description*	
Service Name	Infrastructure as a Service – Windows vConfig-3	
Detailed Description	One virtual Windows server with 8 virtual CPU's, with 64 GB of RAM	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	Must order a commissioning/decommissioning service, one for each server.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13340031-A	IaaS Windows vConfig-3	Per Server

Service Attribute	*Service Attribute Description*	
Service Name	Infrastructure as a Service – Windows vConfig-4	
Detailed Description	One virtual Windows server with 4 virtual CPU's, with 16 GB of RAM	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1) Must order a commissioning/decommissioning service, one for each server. 2) A minimum of two servers must be ordered 3) Disaster recovery services must be ordered	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13340032-A	IaaS Windows Config-4	Per Server

Service Attribute	*Service Attribute Description*	
Service Name	Infrastructure as a Service – Windows vConfig-5	
Detailed Description	One virtual Windows server with 4 virtual CPU's, with 16 GB of RAM	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1) Must order a commissioning/decommissioning service, one for each server. 2) A minimum of two servers must be ordered 3) Disaster recovery services must be ordered	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13340033-A	IaaS Windows Config-5	Per Server

IaaS Linux Configuration – Orderable Configurations

Service Attribute	*Service Attribute Description*	
Service Name	Infrastructure As a Service – Linux vConfig 1	
Detailed Description	One virtual Linux server with 2 virtual CPU's, with 4 GB of RAM	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	Must order a commissioning/decommissioning service, one for each server.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13340034-A	IaaS Linux vConfig-1	Per Server

Service Attribute	*Service Attribute Description*	
Service Name	Infrastructure as a Service – Linux vConfig-2	
Detailed Description	One virtual Linux server with 4 virtual CPU's, with 16 GB of RAM	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	Must order a commissioning/decommissioning service, one for each server.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13340035-A	IaaS Linux vConfig-2	Per Server

Service Attribute	*Service Attribute Description*	
Service Name	Infrastructure as a Service – Linux vConfig-3	
Detailed Description	One virtual Linux server with 8 virtual CPU's, with 64 GB of RAM	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	Must order a commissioning/decommissioning service, one for each server.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13340036-A	IaaS Linux vConfig-3	Per Server

Service Attribute	*Service Attribute Description*	
Service Name	Infrastructure as a Service – Linux vConfig-4	
Detailed Description	One virtual Linux server with 4 virtual CPU's, with 16 GB of RAM	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1) Must order a commissioning/decommissioning service, one for each server. 2) A minimum of two servers must be ordered 3) Disaster recovery services must be ordered	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13340037-A	IaaS Linux vConfig-4	Per Server

Service Attribute	*Service Attribute Description*	
Service Name	Infrastructure as a Service – Linux vConfig-5	
Detailed Description	One virtual Linux server with 4 virtual CPU's, with 16 GB of RAM	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1) Must order a commissioning/decommissioning service, one for each server. 2) A minimum of two servers must be ordered 3) Disaster recovery services must be ordered	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13340038-A	IaaS Linux vConfig-5	Per Server

Infrastructure as a Service (IaaS) – Storage

IaaS Storage Configuration - Configuration Components

Service Attribute	*Service Attribute Description*	
Service Name	Infrastructure as a Service – Storage – IaaS Storage Config-1, 2 - SAN Attached Storage	
Detailed Description	SAN Attached Storage	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites		
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	Service Option Name	Orderable Unit
CCSU13340023-A	IaaS Storage Config-1, 2 - SAN attached Storage	Per GB

Service Attribute	*Service Attribute Description*
Service Name	Infrastructure as a Service – Storage – IaaS Storage Config-3 - Network Attached Storage
Detailed Description	Network Attached Storage
Service Customers / Users	Any participating Commonwealth agency or office
Service Prerequisites	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog

Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13340024-A	IaaS Storage Config-3 - Network attached Storage	Per GB

Service Attribute	*Service Attribute Description*
Service Name	Infrastructure as a Service – Storage – IaaS Storage Config-1 - RAID 5
Detailed Description	RAID 5
Service Customers / Users	Any participating Commonwealth agency or office
Service Prerequisites	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog

Provider Part Number(s)	Service Option Name	Orderable Unit
CCSU13340025-A	IaaS Storage Config-1 - RAID 5	Per GB

Service Attribute	*Service Attribute Description*
Service Name	Infrastructure as a Service – Storage – IaaS Storage Config-2 - RAID 10
Detailed Description	RAID 10
Service Customers / Users	Any participating Commonwealth agency or office
Service Prerequisites	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog

Provider Part Number(s)	Service Option Name	Orderable Unit
CCSU13340026-A	IaaS Storage Config-2 - RAID 10	Per GB

Service Attribute	*Service Attribute Description*
Service Name	Infrastructure as a Service – Storage – IaaS Storage Config-1,2 - 10-15K RPM Discs
Detailed Description	10-15K RPM Discs
Service Customers / Users	Any participating Commonwealth agency or office
Service Prerequisites	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog

Provider Part Number(s)	Service Option Name	Orderable Unit
CCSU13340027-A	IaaS Storage Config-1,2 - 10K-15K RPM Discs	Per GB

Infrastructure as a Service – Storage – Orderable Configurations

Service Attribute	*Service Attribute Description*	
Service Name	Infrastructure as a Service – Storage – SAN Attached – RAID 5	
Detailed Description	Infrastructure as a Service – Storage – SAN Attached – RAID 5	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites		
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13340039-A	IaaS Storage Config-1	Per GB

Service Attribute	*Service Attribute Description*	
Service Name	Infrastructure as a Service – Storage – SAN Attached – RAID 10	
Detailed Description	Infrastructure as a Service – Storage – SAN Attached – RAID 10	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites		
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13340040-A	IaaS Storage Config-2	Per GB

Service Attribute	*Service Attribute Description*	
Service Name	Infrastructure as a Service – Storage – Network Attached Storage	
Detailed Description	Infrastructure as a Service – Storage – Network Attached Storage	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites		
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13340041-A	IaaS Storage Config-3	Per GB

Infrastructure as a Service - Backup

Service Attribute	*Service Attribute Description*	
Service Name	Infrastructure as a Service – Backup	
Detailed Description	Remote Offsite backup per GB	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites		
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13340028-A	IaaS Backup Config-1	Per GB

Third Party Software Management Service

Third Party Software – Unisys Supplied License and Management

Service Attribute	*Service Attribute Description*
Service Name	Third Party Software
Detailed Description	Each of the software items below are defined within Exhibit B.4. Unisys will provide the software license and ongoing maintenance.
Service Customers / Users	Any participating Commonwealth agency or office
Service Prerequisites	1) Fully Managed or Mainframe Servers for each installation The listed software-- • is a co-requisite for DPH IBM Mainframe Service Catalog Offering; • must be purchased together, i.e., all the respective Service Catalog entries must be purchased; • requires a one-year commitment; • will be invoiced monthly; and • is subject to the additional conditions shown below. <u>Limited to use by PennDOT for a capacity of 1000 MIPS of DPH IBM Mainframe total capacity of 2130 MIPS:</u> BMC Software Database Director (D2) BMC Software Eclipse iBuild BMC Software Eclipse iChange BMC Software Eclipse iCheck BMC Software Eclipse iCopy BMC Software Eclipse iExtract BMC Software Eclipse iLM BMC Software Eclipse iLoad

	BMC Software Eclipse iRecover BMC Software Eclipse iSurvey BMC Software Eclipse iUnload BMC Software Mission Control Levi, Ray and Shoup VPS/PCL Levi, Ray and Shoup VPS/TCP/IP Levi, Ray and Shoup VPS/DRS Levi, Ray and Shoup VPS Pitney Bowes Finalist (Doc Sense) Computer Associates International, Inc. CA 90's Services (freeware) Computer Associates International, Inc. Vision Builder Computer Associates International, Inc. CA-Librarian Computer Associates International, Inc. CA-META COBOL SAS Institute, Inc. Base SAS SAS Institute, Inc. SAS/ACCESS Interface for IMS SAS Institute, Inc. SAS/ACCESS DB2 SAS Institute, Inc. SAS/AF SAS Institute, Inc. SAS/FSP SAS Institute, Inc. SAS/GRAPH SAS Institute, Inc. SAS/SHARE SAS Institute, Inc. SAS/STAT <u>Limited to use by PennDOT:</u> Novell SUSE Linux Oracle Database 10g Enterprise

	Oracle Diagnostic Pack Oracle Partitioning Oracle Tuning Pack Oracle Real Application Cluster - Processor Perpetual Oracle Spatial and Graph - Processor Perpetual <u>Hard-capped at 181 MIPS of DPH IBM Mainframe processing capacity for the Department of Corrections:</u> Computer Associates International, Inc. CA-Explore for CICS CSI International EPIC CSI International FAQS/PCS CSI International FAQS/ASO MacKinney Systems, Inc. CICS Response Time <u>Limited to use by Department of Revenue for a capacity of 566 MIPS of DPH IBM Mainframe total capacity of 2130 MIPS</u> OpenText Metastorm Integration Manager for CICS (MIM for CICS) Segus Inc. OPC/Graph Computer Associates International, Inc. CA 90's Services (freeware) Computer Associates International, Inc. Easytrieve Plus Computer Associates International, Inc. Easytrieve Plus IMS Computer Associates International, Inc. Easytrieve Plus DB2 OPT Computer Associates International, Inc. Panvalet Computer Associates International, Inc. Panvalet ISPF Computer Associates International, Inc. SORT (INCL

	DART) Computer Associates International, Inc. SRAM Informatica Corporation Change DataMove for DB2 Source Informatica Corporation DataMove for DB2 Source Informatica Corporation Change DataMove Informatica Corporation DataMove for IMS Source Informatica Corporation Change DataMove for IMS Source Informatica Corporation DataMove Informatica Corporation Change DataMove DB2 Target Informatica Corporation DataMove DB2 Target Informatica Corporation Change DataMove/DataMove Target for UDB Informatica Corporation SSA - Name 3 <u>Limited to use by Department of Labor and Industry - Unemployment Compensation for a capacity of 280 MIPS of DPH IBM Mainframe total capacity of 2130 MIPS</u> Computer Associates International, Inc. CA 90's Services (freeware) Computer Associates International, Inc. Easytrieve Plus MVS Computer Associates International, Inc. Easytrieve Plus IMS Option MVS Computer Associates International, Inc. Easytrieve Plus DB2 Option MVS Computer Associates International, Inc. Endevor/MVS Automated Configuration Mgr MVS Computer Associates International, Inc. Endevor/MVS External Security Int. MVS Computer Associates International, Inc. Endevor/MVS

	MVS Computer Associates International, Inc. Endevor/MVS Extended Processor <u>Agencies using System i: Aging, CSC and Labor and Industry-BOIS</u> HELPSYS Robot/Schedule 2)□	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
CCSU13350001-A	BL/LIB Tape Library Management System	License
CCSU13350002-A	BL/SCHED Scheduling & Monitoring System	License
CCSU13350003-A	BMC AppSight for Windows/.NET - Division Edition	License
CCSU13350004-A	BMC AppSight Named Users	License
CCSU13350005-A	BMC AppSight QA Users	License
CCSU13350006-A	CONTROL-M Enterprise Manager	License
CCSU13350007-A	CONTROL-M Full Admin User	License
CCSU13350008-A	CONTROL-M Tasks (100 Tasks per Unit)	License
CCSI13350009-A	Database Director (D2)	License

CCSI13350010-A	Eclipse iBuild	License
CCSI13350011-A	Eclipse iChange	License
CCSI13350012-A	Eclipse iCheck	License
CCSI13350013-A	Eclipse iCopy	License
CCSI13350014-A	Eclipse iExtract	License
CCSI13350015-A	Eclipse iLM	License
CCSI13350016-A	Eclipse iLoad	License
CCSI13350017-A	Eclipse iRecover	License
CCSI13350018-A	Eclipse iSurvey	License
CCSI13350019-A	Eclipse iUnload	License
CCSI13350020-A	Mission Control	License
CCSU13350021-A	Crystal Reports	License
CCSU13350022-A	StandGuard Anti-Virus	License
CCSU13350023-A	XenApp Advanced (User Counts)	License
CCSU13350024-A	XenApp Enterprise (User Counts)	License
CCSI13350025-A	CA-Explore for CICS	License
CCSU13350026-A	SOA Security Manager	License
CCSU13350027-A	SOA Security Manager Additional Secured Web Services	License

CCSU13350028-A	SOA Security Manager Additional Users	License
CCSU13350029-A	Corticon Business Rules Server – Unlimited CPUs	License
CCSU13350030-A	Corticon Server – per Non-Production Server	License
CCSU13350031-A	Corticon Business Rules Modeling Studio – per Named User	License
CCSI13350032-A	EPIC	License
CCSI13350033-A	FAQS/PCS	License
CCSI13350034-A	FAQS/ASO	License
CCSU13350035-A	PowerPath	License
CCSU13350036-A	PowerPath (per CPU)	License
CCSU13350037-A	Symmetrix® VMAX Fully Automated Storage Tiering for Virtual Pools (FAST VP)	License
CCSU13350038-A	vSphere Enterprise Plus	License
CCSU13350039-A	NameSearch - Production (Licensed per Server up to 8 CPU)	License
CCSU13350040-A	NameSearch - Non-Production (Licensed per Server)	License
CCSU13350041-A	Star 1100	License
CCSU13350042-A	CuteFTP Pro 2.0	License

CCSI13350043-A	Robot/Schedule	License
CCSU13350044-A	XGEN	License
CCSU13350045-A	SSA-Name 3	License
CCSU13350046-A	NetAdvantage for .NET	License
CCSU13350047-A	IQU Plus-1	License
CCSI13350048-A	VPS/PCL	License
CCSI13350049-A	VPS/TCP/IP	License
CCSI13350050-A	VPS/DRS	License
CCSI13350051-A	VPS	License
CCSI13350052-A	CICS Response Time Monitor	License
CCSU13350053-A	OS DCD III Data Correlation and Documentation System	License
CCSU13350054-A	BizTalk Adaptor for MQSeries	License
CCSU13350055-A	BizTalk Server Enterprise (Single Processor)	License
CCSU13350056-A	BizTalk Server Standard (Single Processor)	License
CCSU13350057-A	SQL Server CAL	License
CCSU13350058-A	SQL Server Enterprise (Single Processor)	License
CCSU13350059-A	SQL Server Enterprise	License
CCSU13350060-A	SQL Server Standard (Single	License

	Processor)	
CCSU13350061-A	SQL Server Standard	License
CCSU13350062-A	SQL Server Standard per 2-Core	License
CCSU13350063-A	Visual Studio Foundation Server	License
CCSU13350064-A	Visual Studio Foundation Server CAL	License
CCSU13350065-A	Visual Studio Professional with MSDN	License
CCSU13350066-A	Windows Server Datacenter Edition (Single Processor)	License
CCSU13350067-A	Windows Server Enterprise Edition	License
CCSU13350068-A	Windows Server Standard Edition	License
CCSU13350069-A	Windows Terminal Service Client Access Licenses	License
CCSU13350070-A	McAfee Anti-Virus	License
CCSU13350071-A	PlateSpin Migrate	License
CCSI13350072-A	SUSE Linux	License
CCSI13350073-A	Metastorm Integration Manager for CICS (MIM for CICS)	License
CCSU13350074-A	Oracle Change Management Pack	License

CCSU13350075-A	Oracle Database 10g Enterprise	License
CCSU13350076-A	Oracle Database Enterprise Edition	License
CCSU13350077-A	Oracle Diagnostic Pack	License
CCSU13350078-A	Oracle Enterprise Linux	License
CCSU13350079-A	Oracle Exadata Storage Software	License
CCSU13350080-A	Oracle Partitioning	License
CCSU13350081-A	Oracle Tuning Pack	License
CCSU13350082-A	Real Application Cluster - Processor Perpetual	License
CCSU13350083-A	Spatial and Graph - Processor Perpetual	License
CCSI13350084-A	Finalist (Doc Sense)	License
CCSU13350085-A	CODE-1 Plus	License
CCSU13350086-A	CODE-1 Plus (Test / Development)	License
CCSI13350087-A	Online Window for Finalist	License
CCSU13350088-A	Central Performance Suite for SQL Server, Tier A	License
CCSU13350089-A	Central Performance Suite for SQL Server, Tier B	License
CCSU13350090-A	Foglight Database Management Suite for SQL Server	License

CCSU13350091-A	Foglight for SQL Server per CPU Socket	License
CCSU13350092-A	Foglight OS Management per CPU Socket	License
CCSU13350093-A	Foglight Server for FSM	License
CCSU13350094-A	VNC Enterprise Edition for Windows	License
CCSU13350095-A	Red Hat Enterprise Linux	License
CCSU13350096-A	Q Editor Plus One	License
CCSI13350097-A	OPC/Graph	License
CCSU13350098-A	OS 2200 Interface Agent - CMS/Telcon, SWG20	License
CCSU13350099-A	OS 2200 Interface Agent - CMS/Telcon, SWG40	License
CCSU13350100-A	OS 2200 Interface Agent - CMS/Telcon, SWG60	License
CCSU13350101-A	OS 2200 Interface Agent - CMS/Telcon, SWG80	License
CCSU13350102-A	OS 2200 Interface Agent - CMS/Telcon, SWG130	License
CCSU13350103-A	OS 2200 Interface Agent - KONS/TIP Memory, SWG20	License
CCSU13350104-A	OS 2200 Interface Agent - KONS/TIP Memory, SWG40	License
CCSU13350105-A	OS 2200 Interface Agent - KONS/TIP Memory, SWG60	License

CCSU13350106-A	OS 2200 Interface Agent - KONS/TIP Memory, SWG80	License
CCSU13350107-A	OS 2200 Interface Agent - KONS/TIP Memory, SWG130	License
CCSU13350108-A	OS 2200 Interface Agent - KONS/TIP Memory, SWG140	License
CCSU13350109-A	OS 2200 Interface Agent - MAPPER, SWG20	License
CCSU13350110-A	OS 2200 Interface Agent - MAPPER, SWG40	License
CCSU13350111-A	OS 2200 Interface Agent - MAPPER, SWG60	License
CCSU13350112-A	OS 2200 Interface Agent - MAPPER, SWG80	License
CCSU13350113-A	OS 2200 Interface Agent - MAPPER, SWG130	License
CCSU13350114-A	OS 2200 Interface Agent - MCB/Step Control, SWG20	License
CCSU13350115-A	OS 2200 Interface Agent - MCB/Step Control, SWG40	License
CCSU13350116-A	OS 2200 Interface Agent - MCB/Step Control, SWG60	License
CCSU13350117-A	OS 2200 Interface Agent - MCB/Step Control, SWG80	License
CCSU13350118-A	OS 2200 Interface Agent - MCB/Step Control, SWG130	License
CCSU13350119-A	OS 2200 Interface Agent -	License

	MCB/Step Control, SWG140	
CCSU13350120-A	OS 2200 Interface Agent - System Log, SWG20	License
CCSU13350121-A	OS 2200 Interface Agent - System Log, SWG40	License
CCSU13350122-A	OS 2200 Interface Agent - System Log, SWG60	License
CCSU13350123-A	OS 2200 Interface Agent - System Log, SWG80	License
CCSU13350124-A	OS 2200 Interface Agent - System Log, SWG130	License
CCSU13350125-A	OS 2200 Interface Agent - System Log, SWG140	License
CCSU13350126-A	OS 2200 Interface Agent - UDS/DMS, SWG20	License
CCSU13350127-A	OS 2200 Interface Agent - UDS/DMS, SWG40	License
CCSU13350128-A	OS 2200 Interface Agent - UDS/DMS, SWG60	License
CCSU13350129-A	OS 2200 Interface Agent - UDS/DMS, SWG80	License
CCSU13350130-A	OS 2200 Interface Agent - UDS/DMS, SWG130	License
CCSU13350131-A	OS 2200 Interface Agent - UDS/DMS, SWG140	License
CCSU13350132-A	OS 2200 Power Agent, SWG20	License

CCSU13350133-A	OS 2200 Power Agent, SWG40	License
CCSU13350134-A	OS 2200 Power Agent, SWG60	License
CCSU13350135-A	OS 2200 Power Agent, SWG80	License
CCSU13350136-A	OS 2200 Power Agent, SWG130	License
CCSU13350137-A	OS 2200 Power Agent, SWG140	License
CCSU13350138-A	OS 2200 Torch Capacity Manager Power Agent, SWG40	License
CCSU13350139-A	OS 2200 Torch Capacity Manager Power Agent, SWG60	License
CCSU13350140-A	OS 2200 Torch Capacity Manager Power Agent, SWG130	License
CCSU13350141-A	OS 2200 Torch Capacity Manager Power Agent, SWG140	License
CCSU13350142-A	OS 2200 Torch Interface Agent - I/O TRACE, SWG40	License
CCSU13350143-A	OS 2200 Torch Interface Agent - I/O TRACE, SWG60	License
CCSU13350144-A	OS 2200 Torch Interface Agent - I/O TRACE, SWG130	License
CCSU13350145-A	OS 2200 Torch Interface Agent - LOG, SWG40	License
CCSU13350146-A	OS 2200 Torch Interface Agent - LOG, SWG60	License

CCSU13350147-A	OS 2200 Torch Interface Agent - LOG, SWG130	License
CCSU13350148-A	OS 2200 Torch Interface Agent - LOG, SWG140	License
CCSU13350149-A	OS 2200 Torch Interface Agent - MAPPER, SWG40	License
CCSU13350150-A	OS 2200 Torch Interface Agent - MAPPER, SWG60	License
CCSU13350151-A	OS 2200 Torch Interface Agent - MAPPER, SWG130	License
CCSU13350152-A	Windows 2000 Interface Agent - Internet Information Server	License
CCSU13350153-A	Windows 2000 Interface Agent - .NET	License
CCSU13350154-A	Windows 2000 Interface Agent - SQL Server	License
CCSU13350155-A	Windows 2000 Power Agent Up to 32 CPU's	License
CCSU13350156-A	OpCon/xps EXEC LSAM, Group 3	License
CCSU13350157-A	OpCon/xps EXEC LSAM, Group 12	License
CCSU13350158-A	OpCon/xps EXEC LSAM Development, Group 2	License
CCSU13350159-A	OpCon/xps EXEC LSAM Development, Group 12	License
CCSU13350160-A	OpCon/xps Production SAM	License

CCSU13350161-A	OpCon/xps Starter Kit	License
CCSU13350162-A	OpCon/xps User Interface	License
CCSU13350163-A	EAServer Deploy Advanced - Active	License
CCSU13350164-A	EAServer Deploy Advanced - Passive	License
CCSU13350165-A	Backup Exec System Recovery Server	License
CCSU13350166-A	Endpoint Protection	License
CCSU13350167-A	Ghost Solution Suite	License
CCSU13350168-A	NetBackup Client Application and Database Pack, UNX, Tier 3	License
CCSU13350169-A	NetBackup Client Application and Database Pack, UNX, Tier 4	License
CCSU13350170-A	NetBackup Client Application and Database Pack, WIN, Tier 2	License
CCSU13350171-A	NetBackup Client Application and Database Pack, WIN, Tier 3	License
CCSU13350172-A	NetBackup Client Application and Database Pack, WIN, Tier 4	License
CCSU13350173-A	NetBackup Enterprise Client, UNX, Tier 4	License
CCSU13350174-A	NetBackup Enterprise Client, WIN, Tier 1	License

CCSU13350175-A	NetBackup Enterprise Client, WIN, Tier 2	License
CCSU13350176-A	NetBackup Enterprise Client, WIN, Tier 3	License
CCSU13350177-A	NetBackup Enterprise Server, WIN, Tier 2	License
CCSU13350178-A	NetBackup Enterprise Server, WIN, Tier 3	License
CCSU13350179-A	NetBackup Library Based Tape Drive Option, XPLAT	License
CCSU13350180-A	NetBackup Media Server Encryption Option (MSEO) WIN, Tier 2	License
CCSU13350181-A	NetBackup Platform Base, XPLAT (per Terabyte)	License
CCSU13350182-A	NetBackup Shared Storage Option, XPLAT	License
CCSU13350183-A	NetBackup Standard Client, XPLAT	License
CCSU13350184-A	NetBackup Vault Additional Drive Option, XPLAT	License
CCSU13350185-A	NetBackup Vault Base Option, XPLAT (4 tape drives per license)	License
CCSU13350186-A	Veritas NetBackup Enterprise Server License, Tier 3	License
CCSU13350187-A	Veritas NetBackup Windows Client, Tier 4	License

CCSU13350188-A	DYNA-STEP	License
CCSU13350189-A	LOUIS II LCOM Host Module	License
CCSU13350190-A	LOUIS II Extract & Reporting Module	License
CCSU13350191-A	LOUIS II DERIVE Option	License
CCSU13350192-A	LOUIS II DMS Interface	License
CCSU13350193-A	LOUIS II RDMS Interface	License
CCSU13350194-A	LOUIS II RELATE Option	License
CCSU13350195-A	VShell Workgroup Server	License
CCSU13350196-A	nWorks ESX Monitoring for SCOM	License
CCSU13350197-A	nWorks Management Pack for VMWare	License
CCSU13350198-A	VMware vSphere 4 Enterprise Plus for 1 Processor	License
CCSU13350199-A	VMware vSphere 5 Enterprise Plus for 1 Processor	License
CCSU13350200-A	Rlist	License
CCSU13350201-A	Winternals Administrator's Pak	License
CCSU13350202-A	WinZip	License
CCSU13350203-A	AppMetrics	License
CCSU13350204-A	Correct Address	License

CCSU13350205-A	FileNet	License
CCSU13350206-A	SharePoint (with SA)	License
CCSU13350207-A	WebSphere MQ (Processor Value Unit)	License
CCSU13350208-A	Xerox DocuShare	License

Third Party Software – Commonwealth Supplied License, Unisys Supplied Maintenance

Service Attribute	*Service Attribute Description*	
Service Name	Hybrid Third Party Software	
Detailed Description	Each of the software items below are defined within Exhibit B.10. The Commonwealth owns the license and Unisys will provide the ongoing maintenance.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	Fully Managed, Managed Only, or Mainframe servers supporting each software installation.	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13350209-A	CA 90's Services (freeware)	License
CCSI13350210-A	Vision Builder	License
CCSI13350211-A	Easytrieve Plus	License
CCSI13350212-A	Easytrieve Plus MVS	License
CCSI13350213-A	Easytrieve Plus IMS	License
CCSI13350214-A	Easytrieve Plus IMS Option MVS	License
CCSI13350215-A	Easytrieve Plus DB2 OPT	License

CCSI13350216-A	Easytrieve Plus DB2 Option MVS	License
CCSI13350217-A	Endevor/MVS Automated Configuration Mgr MVS	License
CCSI13350218-A	Endevor/MVS External Security Int. MVS	License
CCSI13350219-A	Endevor/MVS MVS	License
CCSI13350220-A	Endevor/MVS Extended Processor	License
CCSI13350221-A	CA-Librarian	License
CCSI13350222-A	CA-META COBOL	License
CCSI13350223-A	Panvalet	License
CCSI13350224-A	Panvalet ISPF	License
CCSI13350225-A	SORT (INCL DART)	License
CCSI13350226-A	SRAM	License
CCSU13350227-A	dotJ Custom Tag Library	License
CCSU13350228-A	Star 1100	License
CCSU13350229-A	XGEN	License
CCSI13350230-A	Change DataMove for DB2 Source	License
CCSI13350231-A	DataMove for DB2 Source	License
CCSI13350232-A	Change DataMove	License

CCSI13350233-A	DataMove for IMS Source	License
CCSI13350234-A	Change DataMove for IMS Source	License
CCSI13350235-A	DataMove	License
CCSI13350236-A	Change DataMove DB2 Target	License
CCSI13350237-A	DataMove DB2 Target	License
CCSI13350238-A	Change DataMove/DataMove Target for UDB	License
CCSU13350239-A	SSA - Name 3	License
CCSU13350240-A	IQU Plus-1	License
CCSU13350241-A	IQU Reorg Composer	License
CCSU13350242-A	QPLXSS	License
CCSU13350243-A	QPLXSV	License
CCSU13350244-A	QPLXV	License
CCSU13350245-A	OS DCD III Data Correlation and Documentation System	License
CCSU13350246-A	SQL Server Enterprise	License
CCSI13350247-A	Base SAS	License
CCSI13350248-A	SAS/ACCESS Interface for IMS	License
CCSI13350249-A	SAS/ACCESS DB2	License
CCSI13350250-A	SAS/AF	License

CCSI13350251-A	SAS/FSP	License
CCSI13350252-A	SAS/GRAPH	License
CCSI13350253-A	SAS/SHARE	License
CCSI13350254-A	SAS/STAT	License
CCSU13350255-A	Q Editor Plus One	License
CCSU13350256-A	OpCon/xps EXEC LSAM, Group 3	License
CCSU13350257-A	OpCon/xps EXEC LSAM, Group 8	License
CCSU13350258-A	OpCon/xps EXEC LSAM, Group 14	License
CCSU13350259-A	OpCon/xps Microsoft LSAM	License
CCSU13350260-A	OpCon/xps User Interface	License
CCSU13350261-A	EAServer Deploy Advanced - Active	License
CCSU13350262-A	EAServer Deploy Advanced - Passive	License
CCSI13350263-A	TriTune Automation Component (APC)	License
CCSU13350264-A	LOUIS II Database Gateway	License
CCSU13350265-A	LOUIS II DMS Interface	License
CCSU13350266-A	LOUIS II Extract & Reporting Module	License

CCSU13350267-A	LOUIS II LCOM Host Module	License
CCSU13350268-A	LOUIS II MAPPER Interface	License
CCSU13350269-A	LOUIS II RDMS Interface	License
CCSU13350270-A	Secure Site Pro SSL	License
CCSU13350271-A	Rlist	License
CCSU13350272-A	Self-Extractor 10-user license	License

Additional Technical Resources

Service Attribute	*Service Attribute Description*	
Service Name	Additional Technical Resources	
Detailed Description	In addition to the standard managed infrastructure services, the Commonwealth can request the use of additional technology resources and services to support activities which are not provided as part of a managed infrastructure service. The Commonwealth has the flexibility to use additional technical support personnel to support short and long term assignments for projects and ongoing support activities.	
Service Customers / Users	*Any participating Commonwealth agency or office*	
Service Prerequisites		
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSZ13360001-A	**Infrastructure (mainframe, mid-range and x86) Architects/Engineers**	**Per Hour**
CCSZ13360002-A	**Microsoft Product Specialists (e.g. Exchange, SharePoint)**	**Per Hour**
CCSD13360003-A	**Basis and SAP Oracle support**	**Per Hour**

CCSZ13360004-A	**Performance Specialists**	**Per Hour**
CCSZ13360005-A	**Mainframe Systems Programmers**	**Per Hour**
CCSZ13360006-A	**Batch Administrators**	**Per Hour**
CCSZ13360007-A	**3rd Party Software Product Specialists**	**Per Hour**
CCSZ13360008-A	**System Administrator (Windows, AIX, Linux)**	**Per Hour**
CCSZ13360009-A	**System Administrator (Middleware support)**	**Per Hour**
CCSZ13360010-A	**Storage Administrator**	**Per Hour**
CCSZ13360011-A	**Data Backup Administrator**	**Per Hour**
CCSZ13360012-A	**Database Administrator**	**Per Hour**
CCSZ13360013-A	**Database Architects**	**Per Hour**
CCSZ13360014-A	**Database Analysts**	**Per Hour**
CCSZ13360015-A	**Project Management Support**	**Per Hour**
CCSZ13360016-A	**Network Administrator**	**Per Hour**
CCSZ13360017-A	**Facilities Administrator**	**Per Hour**
CCSZ13360018-A	**Security Administrator**	**Per Hour**
CCSZ13360019-A	**Security Architects**	**Per Hour**
CCSZ13360020-A	**Security Analysts**	**Per Hour**
CCSZ13360021-A	**Asset Management**	**Per Hour**

	Administrator	
CCSZ13360022-A	**Quality Assurance Support**	**Per Hour**
CCSZ13360023-A	**Remedy Support Specialist**	**Per Hour**
CCSZ13360024-A	**IT Service Continuity Specialist**	**Per Hour**
CCSZ13360025-A	**Infrastructure (mainframe, mid-range and x86) Architects/Engineers - Junior**	**Per Hour**
CCSZ13360026-A	**Microsoft Product Specialists (e.g. Exchange, SharePoint) - Junior**	**Per Hour**
CCSD13360027-A	**Basis and SAP Oracle support - Junior**	**Per Hour**
CCSZ13360028-A	**Performance Specialists - Junior**	**Per Hour**
CCSU13360029-A	**Unisys Mainframe Systems Programmers - Junior**	**Per Hour**
CCSZ13360030-A	**Batch Administrators - Junior**	**Per Hour**
CCSU13360031-A	**Unisys Mainframe Batch Administrator - Senior**	**Per Hour**
CCSU13360032-A	**Unisys Mainframe Batch Administrator - Junior**	**Per Hour**
CCSZ13360033-A	**3rd Party Software Product Specialists - Junior**	**Per Hour**
CCSZ13360034-A	**System Administrator (Windows, AIX, Linux) - Junior**	**Per Hour**

CCSZ13360035-A	**System Administrator (Middleware support) - Junior**	**Per Hour**
CCSZ13360036-A	**Data Backup Administrator - Junior**	**Per Hour**
CCSZ13360037-A	**Database Administrator - Junior**	**Per Hour**
CCSZ13360038-A	**Database Architects - Junior**	**Per Hour**
CCSZ13360039-A	**Database Analysts - Junior**	**Per Hour**
CCSZ13360040-A	**Project Management Support - Junior**	**Per Hour**
CCSZ13360041-A	**Facilities Administrator - Junior**	**Per Hour**
CCSZ13360042-A	**Network Administrator - Junior**	**Per Hour**
CCSZ13360043-A	**Security Administrator - Junior**	**Per Hour**
CCSZ13360044-A	**Security Architects - Junior**	**Per Hour**
CCSZ13360045-A	**Security Analysts - Junior**	**Per Hour**
CCSU13360046-A	**Smart Hands and Feet Support**	**Per Hour**
CCSU13360047-A	**Unisys Mainframe User Account Administrator**	**Per Hour**
CCSU13360048-A	**Messaging Architect**	**Per Hour**
CCSU13360049-A	**Senior Messaging Consultant**	**Per Hour**

CCSU13360050-A	**Messaging Consultant**	**Per Hour**
CCSU13360051-A	**Senior Active Directory Consultant**	**Per Hour**
CCSU13360052-A	**Active Directory Consultant**	**Per Hour**
CCSU13360053-A	**Application Support Consultant**	**Per Hour**
CCSU13360054-A	**Technical Writer**	**Per Hour**
CCSU13360055-A	**Automation Engineer - Senior**	**Per Hour**
CCSU13360056-A	**Automation Engineer - Junior**	**Per Hour**
CCSU13360057-A	**Senior Technology Consultant 1 - 2200 Database Support**	**Per Hour**
CCSU13360058-A	**Senior Technology Consultant 2 - Windows 2000 and Middleware**	**Per Hour**
CCSU13360059-A	**Senior Technology Consultant 3 - 2200 Mainframe Applications, Performance, and Security**	**Per Hour**
CCSU13360060-A	**Senior Technology Consultant 4 - Middleware Products and Applications**	**Per Hour**
CCSU13360061-A	**Senior Technology Consultant 5 - 2200 Database Design and Maintenance**	**Per Hour**
CCSU13360062-A	**Senior Technology Consultant 6 – Data Warehouse Systems and Oracle Database Servers**	**Per Hour**

CCSU13360063-A	**SPC Principal Engineer**	**Per Hour**
CCSU13360064-A	**SPC Consulting Engineer**	**Per Hour**
CCSU13360065-A	**Consultant 1**	**Per Hour**
CCSU13360066-A	**Consultant 2**	**Per Hour**
CCSU13360067-A	**Consultant 3**	**Per Hour**
CCSU13360068-A	**Consultant 4**	**Per Hour**
CCSU13360069-A	**Integration Architect**	**Per Hour**
CCSU13360070-A	**Program Analyst**	**Per Hour**
CCSU13360071-A	**Programmer**	**Per Hour**
CCSU13360072-A	**Senior Programmer**	**Per Hour**
CCSU13360073-A	**Senior Systems Analyst**	**Per Hour**
CCSU13360074-A	**Senior Systems Architect**	**Per Hour**
CCSU13360075-A	**Sr. Engagement Manager**	**Per Hour**
CCSU13360076-A	**Systems Analyst**	**Per Hour**
CCSU13360077-A	**Systems Architect**	**Per Hour**
CCSU13360078-A	**Technology Architect**	**Per Hour**
CCSI13360079-A	**Solutions Architect**	**Per Hour**
CCSI13360080-A	**System Administrator (AIX, Linux) - Junior**	**Per Hour**
CCSI13360081-A	**Storage Administrator -**	**Per Hour**

	Junior	
CCSI13360082-A	**Solutions Architect - Junior**	**Per Hour**
CCSI13360083-A	**Asset Management Administrator - Junior**	**Per Hour**
CCSI13360084-A	**Quality Assurance Support - Junior**	**Per Hour**
CCSI13360085-A	**Remedy Support Specialist - Junior**	**Per Hour**
CCSI13360086-A	**IT Service Continuity Specialist - Junior**	**Per Hour**
CCSI13360087-A	**Mainframe System Programmer (IBM) - Junior**	**Per Hour**
CCSD13360088-A	**Project Manager - ERP**	**Per Hour**
CCSD13360089-A	**Functional Team Lead - ERP**	**Per Hour**
CCSD13360090-A	**Senior Functional Specialist ERP**	**Per Hour**
CCSD13360091-A	**Junior Functional Specialist - ERP**	**Per Hour**
CCSD13360092-A	**Testing / Documentation Specialist - ERP**	**Per Hour**
CCSD13360093-A	**Trainer**	**Per Hour**
CCSD13360094-A	**Technical Team Lead**	**Per Hour**
CCSD13360095-A	**Senior Developer**	**Per Hour**
CCSD13360096-A	**Junior Developer**	**Per Hour**

CCSD13360097-A	**Database Administrator Team Lead**	**Per Hour**
CCSD13360098-A	**Senior System Administration Specialist**	**Per Hour**
CCSD13360099-A	**Junior System Administration Specialist**	**Per Hour**
CCSD13360100-A	**Senior Security Specialist**	**Per Hour**
CCSD13360101-A	**Junior Security Specialist**	**Per Hour**
CCSD13360102-A	**Program Manager - Onsite**	**Per Hour**
CCSD13360103-A	**Senior Functional Analyst - Onsite**	**Per Hour**
CCSD13360104-A	**Junior Functional Analyst - Onsite**	**Per Hour**
CCSD13360105-A	**Testing / Documentation Specialist - Onsite**	**Per Hour**
CCSD13360106-A	**Architect - Onsite**	**Per Hour**
CCSD13360107-A	**Senior Developer - Onsite**	**Per Hour**
CCSD13360108-A	**Junior Developer - Onsite**	**Per Hour**
CCSD13360109-A	**Automated Tester - Onsite**	**Per Hour**
CCSD13360110-A	**Database Administrator Team Lead - Onsite**	**Per Hour**
CCSD13360111-A	**Senior Database Administrator Specialist - Onsite**	**Per Hour**

CCSD13360112-A	**Junior Database Administrator Specialist - Onsite**	**Per Hour**
CCSD13360113-A	**Security Specialist - Onsite**	**Per Hour**
CCSD13360114-A	**Configuration Analyst - Onsite**	**Per Hour**

This Page Intentionally Left Blank

Additional Technical Services

Database Management Services

Database Management Services

Service Attribute	*Service Attribute Description*
Service Name	Database Management Service - Platinum
Detailed Description	The Database Management Services service provides agencies with foundational Database Administration services to support the installation, configuration, backup/recovery and operational management of the Database. Services are provided through various tiers that provide basic to full service coverage and capabilities. Services Include: Database Creation / Management • Install and patch Database software • Create and maintain shell database instance sized appropriately based on supplied requirements Backup Management • Create and Establish Database backups integrated with the larger system backup strategy • Monitor and analyze successful execution, retention and storage of backups Database Recovery • Support database recovery from backup or archive log • Support Disaster Recovery planning, rehearsing and execution Application Release Management • Execute defined tasks to support deployment management through various test environments per defined work plans • Execute physical deployment of application objects within

	the database Data Management • Refresh data from Backup/Export periodically • Create and execute data alteration/extract solutions periodically via supplied requirements • Proactive Database Performance Analysis • Proactively monitor and report on database health and performance • Provide periodic reports highlighting performance trends and consumption patterns • Execute database system level tuning and maintenance to support performance goals • Proactive SQL Analysis / Tuning Recommendations • Proactively monitor and report on database SQL performance in the production environment • Provide monthly reports highlighting performance trends and a list of SQL tuning opportunities • Development of tuning options for identified performance opportunities Provide Level 2/3 Technical Help Desk Support • Support triage and resolution of calls from the Level 1 Help Desk • Collect and report metrics, solutions and outcomes of said support Tools used • Erwin, Oracle Enterprise Manager, Microsoft Management Studio, Sybase Central, IBM Data Studio, Toad, Oracle SQL Developer Platforms Supported • Oracle, DB2, SQL Server, Sybase 500 hour per month per request Full time resources proactively monitoring and recommending leading practices. Available 24x7x365 (on-site coverage averages

	96 hrs/week not to exceed 500 hrs/month) with responsiveness SLAs. Resources are vendor certified (where applicable) with over 10 years of experience
Service Customers / Users	Any participating Commonwealth agency or office
Service Prerequisites	1) Fully Managed Windows, Linux, AIX, Unisys Mainframe or IBM Mainframe server service for the number of servers or MIPS required to support the database. 2) Database Software Licensing and Maintenance a. Option 1: Unisys Database Management Service Supplied Software, or b. Option 2: Agency supplied Software
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog

Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSD13370001-A	Database Management Service – Platinum (up to 500 hours per month)	Per Request / Up to 500 hours per request

Service Attribute	*Service Attribute Description*
Service Name	Database Management Service – Gold
Detailed Description	The Database Management Services service provides agencies with foundational Database Administration services to support the installation, configuration, backup/recovery and operational management of the Database. Services are provided through various tiers that provide basic to full service coverage and capabilities. Services Include: • Database Creation / Management • Install and patch Database software • Create and maintain shell database instance sized appropriately based on supplied requirements Backup Management • Create and Establish Database backups integrated with the larger system backup strategy • Monitor and analyze successful execution, retention and storage of backups Database Recovery • Support database recovery from backup or archive log • Support Disaster Recovery planning, rehearsing and execution Application Release Management • Execute defined tasks to support deployment management through various test environments per defined work plans • Execute physical deployment of application objects within the database Data Management • Refresh data from Backup/Export periodically • Create and execute data alteration/extract solutions periodically via supplied requirements

	• Proactive Database Performance Analysis • Proactively monitor and report on database health and performance • Provide periodic reports highlighting performance trends and consumption patterns • Execute database system level tuning and maintenance to support performance goals • Proactive SQL Analysis / Tuning Recommendations • Proactively monitor and report on database SQL performance in the production environment • Provide monthly reports highlighting performance trends and a list of SQL tuning opportunities • Development of tuning options for identified performance opportunities Provide Level 2/3 Technical Help Desk Support • Support triage and resolution of calls from the Level 1 Help Desk • Collect and report metrics, solutions and outcomes of said support Tools used • Erwin, Oracle Enterprise Manager, Microsoft Management Studio, Sybase Central, IBM Data Studio, Toad, Oracle SQL Developer Platforms Supported • Oracle, DB2, SQL Server, Sybase 375 hour per month per request Full time resources proactively monitoring and recommending leading practices. Available 24x7x365 (on-site coverage averages 80 hrs/week not to exceed 375 hrs/month) with responsiveness SLA's. Resources are vendor certified (where applicable) with over 8 years of experience

Service Customers / Users	Any participating Commonwealth agency or office
Service Prerequisites	1) Fully Managed Windows, Linux, AIX, Unisys Mainframe or IBM Mainframe server service for the number of servers or MIPS required to support the database. 2) Database Software Licensing and Maintenance a. Option 1: Unisys Database Management Service Supplied Software, or b. Option 2: Agency supplied Software
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog

Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSD13370002-A	Database Management Service – Gold (up to 375 hours per month)	Per Request / Up to 375 hours per request

Service Attribute	*Service Attribute Description*
Service Name	Database Management Service - Silver
Detailed Description	The Database Management Services service provides agencies with foundational Database Administration services to support the installation, configuration, backup/recovery and operational management of the Database. Services are provided through various tiers that provide basic to full service coverage and capabilities. Services Include: Database Creation / Management • Install and patch Database software • Create and maintain shell database instance sized appropriately based on supplied requirements Backup Management • Create and Establish Database backups integrated with the larger system backup strategy • Monitor and analyze successful execution, retention and storage of backups Database Recovery • Support database recovery from backup or archive log • Support Disaster Recovery planning, rehearsing and execution • Application Release Management • Execute defined tasks to support deployment management through various test environments per defined work plans • Execute physical deployment of application objects within the database Data Management • Refresh data from Backup/Export periodically • Create and execute data alteration/extract solutions periodically via supplied requirements

	• Proactive Database Performance Analysis • Proactively monitor and report on database health and performance • Provide periodic reports highlighting performance trends and consumption patterns • Execute database system level tuning and maintenance to support performance goals • Proactive SQL Analysis / Tuning Recommendations • Proactively monitor and report on database SQL performance in the production environment • Provide monthly reports highlighting performance trends and a list of SQL tuning opportunities • Development of tuning options for identified performance opportunities Provide Level 2/3 Technical Help Desk Support • Support triage and resolution of calls from the Level 1 Help Desk • Collect and report metrics, solutions and outcomes of said support Tools used • Erwin, Oracle Enterprise Manager, Microsoft Management Studio, Sybase Central, IBM Data Studio, Toad, Oracle SQL Developer Platforms Supported • Oracle, DB2, SQL Server, Sybase 250 hour per month per request Full time resources proactively monitoring providing operational status. Available 24x7x365 (on-site coverage averages 60 hrs/week not to exceed 250 hrs/month) with responsiveness SLA's. Resources have over 6 years of qualified experience

Service Customers / Users	Any participating Commonwealth agency or office
Service Prerequisites	1) Fully Managed Windows, Linux, AIX, Unisys Mainframe or IBM Mainframe server service for the number of servers or MIPS required to support the database. 2) Database Software Licensing and Maintenance a. Option 1: Unisys Database Management Service Supplied Software, or b. Option 2: Agency supplied Software
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog

Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSD13370003-A	Database Management Service – Silver (up to 250 hours per month)	Per Request / Up to 250 hours per request

Service Attribute	*Service Attribute Description*
Service Name	Database Management Service - Bronze
Detailed Description	The Database Management Services service provides agencies with foundational Database Administration services to support the installation, configuration, backup/recovery and operational management of the Database. Services are provided through various tiers that provide basic to full service coverage and capabilities. Services Include: Database Creation / Management • Install and patch Database software • Create and maintain shell database instance sized appropriately based on supplied requirements Backup Management • Create and Establish Database backups integrated with the larger system backup strategy • Monitor and analyze successful execution, retention and storage of backups Database Recovery • Support database recovery from backup or archive log • Support Disaster Recovery planning, rehearsing and execution • Application Release Management • Execute defined tasks to support deployment management through various test environments per defined work plans • Execute physical deployment of application objects within the database Data Management • Refresh data from Backup/Export periodically • Create and execute data alteration/extract solutions periodically via supplied requirements

- Proactive Database Performance Analysis
- Proactively monitor and report on database health and performance
- Provide periodic reports highlighting performance trends and consumption patterns
- Execute database system level tuning and maintenance to support performance goals
- Proactive SQL Analysis / Tuning Recommendations
- Proactively monitor and report on database SQL performance in the production environment
- Provide monthly reports highlighting performance trends and a list of SQL tuning opportunities
- Development of tuning options for identified performance opportunities

Provide Level 2/3 Technical Help Desk Support

- Support triage and resolution of calls from the Level 1 Help Desk
- Collect and report metrics, solutions and outcomes of said support

Tools used

- Erwin, Oracle Enterprise Manager, Microsoft Management Studio, Sybase Central, IBM Data Studio, Toad, Oracle SQL Developer

Platforms Supported

- Oracle, DB2, SQL Server, Sybase

160 hour per month per request

Shared resources proactively monitoring providing operational status. Available 24x7x365 on-site coverage averages 40 hrs/week not to exceed 160 hrs/month) with responsiveness SLA's.

Resources are available from a pool of qualified DBA's with over 4 years of experience

Service Customers / Users	Any participating Commonwealth agency or office
Service Prerequisites	1) Fully Managed Windows, Linux, or AIX server service for the number of servers required to support the database. 2) Database Software Licensing and Maintenance a. Option 1: Unisys Database Management Service Supplied Software, or b. Option 2: Agency supplied Software
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog

Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSD13370004-A	Database Management Service – Bronze (up to 160 hours per month)	Per Request / Up to 160 hours per request

Service Attribute	*Service Attribute Description*
Service Name	Database Management Service - Basic
Detailed Description	The Database Management Services service provides agencies with foundational Database Administration services to support the installation, configuration, backup/recovery and operational management of the Database. Services are provided through various tiers that provide basic to full service coverage and capabilities. Services Include: Database Creation / Management • Install and patch Database software • Create and maintain shell database instance sized appropriately based on supplied requirements Backup Management • Create and Establish Database backups integrated with the larger system backup strategy • Monitor and analyze successful execution, retention and storage of backups Database Recovery • Support database recovery from backup or archive log • Support Disaster Recovery planning, rehearsing and execution • Application Release Management • Execute defined tasks to support deployment management through various test environments per defined work plans • Execute physical deployment of application objects within the database Data Management • Refresh data from Backup/Export periodically • Create and execute data alteration/extract solutions periodically via supplied requirements

	• Proactive Database Performance Analysis • Proactively monitor and report on database health and performance • Provide periodic reports highlighting performance trends and consumption patterns • Execute database system level tuning and maintenance to support performance goals • Proactive SQL Analysis / Tuning Recommendations • Proactively monitor and report on database SQL performance in the production environment • Provide monthly reports highlighting performance trends and a list of SQL tuning opportunities • Development of tuning options for identified performance opportunities Provide Level 2/3 Technical Help Desk Support • Support triage and resolution of calls from the Level 1 Help Desk • Collect and report metrics, solutions and outcomes of said support Tools used • Erwin, Oracle Enterprise Manager, Microsoft Management Studio, Sybase Central, IBM Data Studio, Toad, Oracle SQL Developer Platforms Supported • Oracle, DB2, SQL Server, Sybase 80 hour per month per request Shared resources available to support requested execution of listed services. Available 8x5x365 and not to exceed 80 hrs/month with responsiveness SLA's. Resources are available from a pool of qualified DBA's with over 2 years of experience

Service Customers / Users	Any participating Commonwealth agency or office
Service Prerequisites	1) Fully Managed Windows, Linux, or AIX server service for the number of servers required to support the database. 2) Database Software Licensing and Maintenance a. Option 1: Unisys Database Management Service Supplied Software, or b. Option 2: Agency supplied Software
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog

Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSD13370005-A	Database Management Service – Basic (up to 80 hours per month)	Per Request / Up to 80 hours per request

Database Software

Service Attributes	*Service Attribute Description*	
Service Name	Database Software - MS SQL Enterprise 2012 SPLA License - Based Upon Physical Configuration 3 (4 CPU / 6 Core)	
Detailed Description	As part of the Database Management service, the MS SQL Enterprise 2012 SPLA License provides the database functionality to support applications requiring MS SQL. MS SQL Enterprise includes additional capabilities over MS SQL Standard to support database high availability. This service is based upon licensing to Windows pConfig-3. If the database server uses another physical configuration, a quote will be necessary. The number of units to be ordered is based on the number of servers requested.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1) Fully Managed Windows Server Physical Configuration 3 for each database server. 2) Database Management Service – Database Management Support (Platinum, Gold, Silver, Bronze, or Basic)	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370006-A	Database –Software - MS SQL Enterprise 2012 SPLA License - Based Upon Physical Configuration 3 (4 CPU / 6	Per Server Instance

	Core)	

Service Attribute	*Service Attribute Description*	
Service Name	Database Software - MS SQL Standard 2012 SPLA License - Based Upon Physical Configuration 3 (4 CPU / 6 Core)	
Detailed Description	As part of the Database Management service, the MS SQL Standard 2012 SPLA License provides the database functionality to support applications requiring MS SQL. This service is based upon licensing to Windows pConfig-3. If the database server uses another physical configuration, a quote will be necessary. The number of units to be ordered is based on the number of servers requested.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1) Fully Managed Windows Server Physical Configuration 3 for each database server 2) Database Management Service – Database Management Support (Bronze, Gold, Silver, Bronze, or Basic)	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370007-A	Database –Software - MS SQL Standard 2012 SPLA License - Based Upon Physical Configuration 3 (4 CPU / 6 Core)	Per Server Instance

Service Attribute	*Service Attribute Description*	
Service Name	Database Software - MS SQL Enterprise 2012 SPLA License - Based Upon Virtual Configuration 3 (8vCPU) - Must have number of vCPUs to match vCPUs used and number of VMWare servers in cluster	
Detailed Description	As part of the Database Management service, the MS SQL Enterprise 2012 SPLA License provides the database functionality to support applications requiring MS SQL. MS SQL Enterprise includes additional capabilities over MS SQL Standard to support database high availability. This service is based upon licensing to Windows vConfig-3. If the database server uses another physical configuration, a quote will be necessary. This license service is based upon the Platinum Application Availability SLA. The number of units to be ordered is based on the number of servers requested and number of VMWare ESX cluster physical servers supporting the database servers.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1) Fully Managed Windows Server Virtual Configuration 3 for each database server 2) Database Management Service – Database Management Support (Platinum, Gold, Silver, Bronze, or Basic)	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**

CCSU13370008-A	Database –Software - MS SQL Enterprise 2012 SPLA License - Based Upon Virtual Configuration 3 (8 vCPU)	Per Server

Service Attribute	*Service Attribute Description*	
Service Name	Database Software - MS SQL Standard 2012 SPLA License - Based Upon Virtual Configuration 3 (8vCPU) - Must have number of vCPUs to match vCPUs used and number of VMWare servers in cluster	
Detailed Description	As part of the Database Management service, the MS SQL Standard 2012 SPLA License provides the database functionality to support applications requiring MS SQL. This service is based upon licensing to Windows vConfig-3. If the database server uses another physical configuration, a quote will be necessary. The number of units to be ordered is based on the number of servers requested and number of VMWare ESX cluster physical servers supporting the database servers.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1) Fully Managed Windows Server Virtual Configuration 3 for each database server 2) Database Management Service – Database Management Support (Platinum, Gold, Silver, Bronze, or Basic)	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370009-A	Database –Software - MS SQL Standard 2012 SPLA License - Based Upon Virtual Configuration 3 (8 vCPU)	Per Server

Service Attribute	*Service Attribute Description*	
Service Name	Database Management Service - Platinum - Oracle 11g Enterprise - Based Upon Physical Configuration 3 (4 CPU / 6 Core) - Perpetual License	
Detailed Description	As part of the Database Management service, the Oracle 11g Enterprise Perpetual License provides the database functionality to support applications requiring Oracle databases. Oracle 11g Enterprise includes additional capabilities over Oracle 11g Standard to support database high availability and larger databases. The number of units to be ordered is based on the number of servers requested	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1) Fully Managed Windows Server Physical Configuration 3 for each database server 2) Database Management Service – Database Management Support (Platinum, Gold, Silver, Bronze, or Basic) 3) Database Software – Oracle 11g Enterprise – Annual Maintenance 4) Requires a 12 month commitment during first year of purchase.	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370010-A	Database –Software - Oracle Enterprise 11g License - Based Upon Physical Configuration 3	Per Server Instance

	(4 CPU / 6 Core)	

Service Attribute	*Service Attribute Description*
Service Name	Database Software - Oracle 11g Real Application Cluster (RAC) - Based Upon Physical Configuration 3 (4 CPU / 6 Core) - Perpetual License
Detailed Description	As part of the Database Management service, the Oracle 11g Enterprise Perpetual License provides the database functionality to support applications requiring Oracle databases. Oracle 11g Enterprise includes additional capabilities over Oracle 11g Standard to support database high availability and larger databases. With the addition of Oracle Real Application Clustering, these functions are enhanced. This service is based upon licensing to Windows pConfig-3. If the database server uses another physical configuration, a quote will be necessary. The number of units to be ordered is based on the number of servers requested running Oracle 11g and require clustering.
Service Customers / Users	Any participating Commonwealth agency or office
Service Prerequisites	1) Fully Managed Windows Server Physical Configuration 3 for each database server 2) Database Management Service – Database Management Support (Platinum, Gold, Silver, Bronze, or Basic) 3) Database Software – Oracle Real Application Cluster Software – Annual Maintenance 4) Requires a 12 month commitment during first year of purchase.
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog

Provider Part Number(s)	Service Option Name	Orderable Unit / Restrictions per Unit
CCSU13370011-A	Database –Software – Oracle Real Application Cluster License - Based Upon Physical Configuration 3 (4 CPU / 6 Core)	Per Server Instance

Service Attribute	*Service Attribute Description*	
Service Name	Database Software - Oracle 11g Standard - Based Upon Physical Configuration 3 (4 CPU / 6 Core) - Perpetual License	
Detailed Description	As part of the Database Management service, the Oracle 11g Standard Perpetual License provides the database functionality to support applications requiring Oracle databases. This service is based upon licensing to Windows pConfig-3. If the database server uses another physical configuration, a quote will be necessary. The number of units to be ordered is based on the number of servers requested running Oracle 11g and require clustering.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1) Fully Managed Windows Server Physical Configuration 3 for each database server 2) Database Management Service – Database Management Support (Platinum, Gold, Bronze, Bronze, or Basic) 3) Database Software – Oracle 11g Standard – Annual Maintenance 4) Requires a 12 month commitment during first year of purchase.	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370012-A	Database –Software - Oracle 11g Standard - Based Upon	Per Server Instance

	Physical Configuration 3 (4 CPU / 6 Core)	

Service Attribute	*Service Attribute Description*	
Service Name	Database Management Service - Platinum - Oracle 11g Enterprise - Based Upon Physical Configuration 3 (4 CPU / 6 Core) – Annual Maintenance	
Detailed Description	As part of the Database Management service, the Oracle 11g Enterprise Perpetual License provides the database functionality to support applications requiring Oracle databases. Oracle 11g Enterprise includes additional capabilities over Oracle 11g Standard to support database high availability and larger databases. The number of units to be ordered is based on the number of servers requested The Annual Maintenance service provides the manufacturers ongoing software support contract.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	5) Fully Managed Windows Server Physical Configuration 3 for each database server 6) Database Management Service – Database Management Support (Platinum, Gold, Silver, Bronze, or Basic) 7) Database Software – Oracle Enterprise Database - License	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370505-A	Database –Software - Oracle Enterprise 11g - Based Upon Physical Configuration 3 (4 CPU / 6 Core) – Annual	Per Server Instance

	Maintenance	

Service Attribute	*Service Attribute Description*
Service Name	Database Software - Oracle 11g Real Application Cluster (RAC) - Based Upon Physical Configuration 3 (4 CPU / 6 Core) – Annual Maintenance
Detailed Description	As part of the Database Management service, the Oracle 11g Enterprise Perpetual License provides the database functionality to support applications requiring Oracle databases. Oracle 11g Enterprise includes additional capabilities over Oracle 11g Standard to support database high availability and larger databases. With the addition of Oracle Real Application Clustering, these functions are enhanced. This service is based upon licensing to Windows pConfig-3. If the database server uses another physical configuration, a quote will be necessary. The number of units to be ordered is based on the number of servers requested running Oracle 11g and require clustering. The Annual Maintenance service provides the manufacturers ongoing software support contract.
Service Customers / Users	Any participating Commonwealth agency or office
Service Prerequisites	5) Fully Managed Windows Server Physical Configuration 3 for each database server 6) Database Management Service – Database Management Support (Platinum, Gold, Silver, Bronze, or Basic) Database Software – Oracle Real Application Cluster Software –License
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog

Provider Part Number(s)	Service Option Name	Orderable Unit / Restrictions per Unit
CCSU13370506-A	Database –Software – Oracle Real Application Cluster License - Based Upon Physical Configuration 3 (4 CPU / 6 Core) – Annual Maintenance	Per Server Instance

Service Attribute	*Service Attribute Description*	
Service Name	Database Software - Oracle 11g Standard - Based Upon Physical Configuration 3 (4 CPU / 6 Core) – Annual Maintenance	
Detailed Description	As part of the Database Management service, the Oracle 11g Standard Perpetual License provides the database functionality to support applications requiring Oracle databases. This service is based upon licensing to Windows pConfig-3. If the database server uses another physical configuration, a quote will be necessary. The number of units to be ordered is based on the number of servers requested running Oracle 11g and require clustering. The Annual Maintenance service provides the manufacturers ongoing software support contract.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	5) Fully Managed Windows Server Physical Configuration 3 for each database server 6) Database Management Service – Database Management Support (Platinum, Gold, Bronze, Bronze, or Basic) 7) Database Software – Oracle 11g Standard - License	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370507-A	Database –Software - Oracle 11g Standard - Based Upon Physical Configuration 3 (4	Per Server Instance

	CPU / 6 Core) – Annual Maintenance	

Service Attribute	*Service Attribute Description*
Service Name	Database Software - Sybase ASE Enterprise - Based Upon Physical Configuration 3 (4 CPU / 6 Core) - Perpetual License
Detailed Description	As part of the Database Management service, the Sybase ASE Enterprise Perpetual License provides the database functionality to support applications requiring Sybase databases. Sybase ASE Enterprise includes additional capabilities over Sybase ASE Standard to support database high availability and larger databases. With the addition of Sybase Real Application Clustering, these functions are enhanced. This service is based upon licensing to Windows pConfig-3. If the database server uses another physical configuration, a quote will be necessary. The number of units to be ordered is based on the number of servers requested for Sybase databases.
Service Customers / Users	Any participating Commonwealth agency or office
Service Prerequisites	1) Fully Managed Windows Server Physical Configuration 3 for each database server 2) Database Management Service – Database Management Support (Platinum, Gold, Silver, Bronze, or Basic) 3) Database Software – Sybase ASE Enterprise – Annual Maintenance 4) Requires a 12 month commitment during first year of purchase.
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog

Provider Part Number(s)	Service Option Name	Orderable Unit / Restrictions per Unit
CCSU13370013-A	Database –Software - Sybase ASE Enterprise License - Based Upon Physical Configuration 3 (4 CPU / 6 Core)	Per Server Instance

Service Attribute	*Service Attribute Description*	
Service Name	Database Software - Sybase Replication Server - Based Upon Physical Configuration 3 (4 CPU / 6 Core) - Perpetual License	
Detailed Description	As part of the Database Management service, the Sybase Replication Perpetual License provides database replication functionality to support applications requiring Sybase databases. This service is based upon licensing to Windows pConfig-3. If the database server uses another physical configuration, a quote will be necessary. The number of units to be ordered is based on the number of servers requested to run Sybase replication.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1) Fully Managed Windows Server Physical Configuration 3 for each replication server 2) Database Management Service – Database Management Support (Platinum, Gold, Silver, Bronze, or Basic) 3) Database Software – Sybase Replication Server – Annual Maintenance 4) Requires a 12 month commitment during first year of purchase.	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**

CCSI13370014-A	Database –Software - Sybase Replication Server License - Based Upon Physical Configuration 3 (4 CPU / 6 Core)	Per Server Instance

Service Attribute	*Service Attribute Description*	
Service Name	Database Software - Sybase ASE Standard - Based Upon Physical Configuration 3 (4 CPU / 6 Core) - Perpetual License	
Detailed Description	As part of the Database Management service, the Sybase ASE Enterprise Perpetual License provides the database functionality to support applications requiring Sybase databases. The number of units to be ordered is based on the number of servers requested for Sybase databases.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1) Fully Managed Windows Server Physical Configuration 3 for each database server 2) Database Management Service – Database Management Support (Platinum, Gold, Bronze, Bronze, or Basic) 3) Database Software – Sybase ASE Standard – Annual Maintenance 4) Requires a 12 month commitment during first year of purchase.	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370015-A	Database –Software - Sybase ASE Standard License - Based Upon Physical Configuration 3	Per Server Instance

	(4 CPU / 6 Core)	

Service Attribute	*Service Attribute Description*
Service Name	Database Software - Sybase ASE Enterprise - Based Upon Physical Configuration 3 (4 CPU / 6 Core) – Annual Maintenance
Detailed Description	As part of the Database Management service, the Sybase ASE Enterprise Perpetual License provides the database functionality to support applications requiring Sybase databases. Sybase ASE Enterprise includes additional capabilities over Sybase ASE Standard to support database high availability and larger databases. With the addition of Sybase Real Application Clustering, these functions are enhanced. This service is based upon licensing to Windows pConfig-3. If the database server uses another physical configuration, a quote will be necessary. The number of units to be ordered is based on the number of servers requested for Sybase databases. The Annual Maintenance service provides the manufacturers ongoing software support contract.
Service Customers / Users	Any participating Commonwealth agency or office
Service Prerequisites	5) Fully Managed Windows Server Physical Configuration 3 for each database server 6) Database Management Service – Database Management Support (Platinum, Gold, Silver, Bronze, or Basic) 7) Database Software – Sybase ASE Enterprise - License
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog

Provider Part Number(s)	Service Option Name	Orderable Unit / Restrictions per Unit
CCSU13370508-A	Database –Software - Sybase ASE Enterprise - Based Upon Physical Configuration 3 (4 CPU / 6 Core) – Annual Maintenance	Per Server Instance

Service Attribute	*Service Attribute Description*	
Service Name	Database Software - Sybase Replication Server - Based Upon Physical Configuration 3 (4 CPU / 6 Core) – Annual Maintenance	
Detailed Description	As part of the Database Management service, the Sybase Replication Perpetual License provides database replication functionality to support applications requiring Sybase databases. This service is based upon licensing to Windows pConfig-3. If the database server uses another physical configuration, a quote will be necessary. The number of units to be ordered is based on the number of servers requested to run Sybase replication. The Annual Maintenance service provides the manufacturers ongoing software support contract.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	5) Fully Managed Windows Server Physical Configuration 3 for each replication server 6) Database Management Service – Database Management Support (Platinum, Gold, Silver, Bronze, or Basic) 7) Database Software – Sybase Replication Server – Annual Maintenance	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370509-A	Database –Software - Sybase Replication Server - Based	Per Server Instance

	Upon Physical Configuration 3 (4 CPU / 6 Core) – Annual Maintenance	

Service Attribute	*Service Attribute Description*	
Service Name	Database Software - Sybase ASE Standard - Based Upon Physical Configuration 3 (4 CPU / 6 Core) - Perpetual License	
Detailed Description	As part of the Database Management service, the Sybase ASE Enterprise Perpetual License provides the database functionality to support applications requiring Sybase databases. The number of units to be ordered is based on the number of servers requested for Sybase databases. The Annual Maintenance service provides the manufacturers ongoing software support contract.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	5) Fully Managed Windows Server Physical Configuration 3 for each database server 6) Database Management Service – Database Management Support (Platinum, Gold, Bronze, Bronze, or Basic) 7) Database Software – Sybase ASE Standard - License	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370510-A	Database –Software - Sybase ASE Standard - Based Upon Physical Configuration 3 (4 CPU / 6 Core) – Annual Maintenance	Per Server Instance

Database Management Deployment and Support Services - AIX

Service Attribute	*Service Attribute Description*
Service Name	Oracle Build p-Series Standard (1 server)
Detailed Description	Identify performance and availability requirements Perform hardware selection; solicit physical build from client Baseline current environment and utilization (e.g., CPU, memory) Create high-level design using requirements in Assess phase and baseline build documentation Develop a project plan with milestones, dependencies and resource allocations Plan, track, document, and coordinate activities for the project Create data base or WAS-specific test plans and develop acceptance criteria Request Storage allocations per defined standards Install and configure AIX v6.x on 1 LPAR per server Install and configure Bundle Middleware Package Configure AIX and Bundle Middleware per customer build requirements Test hardware and software according to documented test plan Turn-over system to customer and obtain sign-off Build from base level hardware with no OS pre-installed, physical servers are pre-installed in racks with all hardware installed, base OS, I/O, and HA configuration only (no applications), with base images and configuration standards supplied by customer.
Service Customers / Users	Any participating Commonwealth agency or office.
Service Prerequisites	Software and/or hardware to complete service

	Access to affected systems and/or facilities.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370016-A	Oracle Build p-Series Standard	Per Request

Service Attribute	*Service Attribute Description*
Service Name	Oracle Build p-Series Complex (2 servers in clustered pair)
Detailed Description	Identify performance and availability requirements Perform hardware selection; solicit physical build from client Baseline current environment and utilization (e.g., CPU, memory) Create high-level design using requirements in Assess phase and baseline build documentation Develop a project plan with milestones, dependencies and resource allocations Plan, track, document, and coordinate activities for the project Create data base or WAS-specific test plans and develop acceptance criteria Request Storage allocations per client defined requirements Work with SO to confirm power up and burn-in of Server Install and configure AIX v6.x on 1 LPAR per server Install and configure Bundle Middleware Package Configure AIX and Bundle Middleware per customer build requirements Test hardware and software according to documented test plan Validate acceptance criteria have been met Turn-over system to customer and obtain sign-off Build from base level hardware with no OS pre-installed, physical servers are pre-installed in racks with all hardware installed, base OS, I/O, and HA configuration only (no applications), with base images and configuration standards supplied by customer.
Service Customers / Users	Any participating Commonwealth agency or office.

Service Prerequisites	Software and/or hardware to complete service Access to affected systems and/or facilities.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370017-A	Oracle Build p-Series Complex	Per Request

Service Attribute	*Service Attribute Description*
Service Name	Oracle Upgrade p-Series Standard (1 server)
Detailed Description	Identify performance and availability profile Collect Performance Baseline Create high-level design using requirements in Assess phase and baseline build documentation Develop a project plan with milestones, dependencies and resource allocations Plan, track, document, and coordinate activities for the project Create application-specific test plans and develop acceptance criteria Request new hardware requirements based upon performance requirements Install and configure current version of target Bundle on 1 LPAR per server Test software according to document test plan Validate acceptance criteria have been met Turn-over system to customer and obtain sign-off This is Upgrade of DB only - 1 version level upgrade only, OS will be at a version(s) which support the upgraded DB, base images and configuration standards to be supplied by client. Storage and SAN Fabric are client or other Bundle responsibility, with remote delivery for services is primary alternative, with on-site when necessary.
Service Customers / Users	Any participating Commonwealth agency or office.
Service Prerequisites	Software and/or hardware to complete service Access to affected systems and/or facilities.

Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370018-A	Oracle Upgrade p-Series Standard	Per Request

Service Attribute	*Service Attribute Description*
Service Name	Oracle Upgrade p-Series Complex (2 servers in clustered pair)
Detailed Description	Identify performance and availability profile Collect Performance Baseline Create high-level design using requirements in Assess phase and baseline build documentation Develop a project plan with milestones, dependencies and resource allocations Plan, track, document, and coordinate activities for the project Create application-specific test plans and develop acceptance criteria Request new hardware requirements based upon performance requirements Install and configure current version of target Bundle on 1 LPAR per server Test software according to document test plan Validate acceptance criteria have been met Turn-over system to customer and obtain sign-off This is Upgrade of DB only - 1 version level upgrade only, OS will be at a version(s) which support the upgraded DB, base images and configuration standards to be supplied by client. Storage and SAN Fabric are client or other Bundle responsibility, with remote delivery for services is primary alternative, with on-site when necessary.
Service Customers / Users	Any participating Commonwealth agency or office.
Service Prerequisites	Software and/or hardware to complete service Access to affected systems and/or facilities.

Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370019-A	Oracle Upgrade p-Series Complex	Per Request

Service Attribute	*Service Attribute Description*
Service Name	DB2 Build p-Series Standard (1 server)
Detailed Description	Identify performance and availability requirements Perform hardware selection; solicit physical build from SO Baseline current environment and utilization (e.g., CPU, memory) Create high-level design using requirements in Assess phase and baseline build documentation Develop a project plan with milestones, dependencies and resource allocations Plan, track, document, and coordinate activities for the project Create data base or WAS-specific test plans and develop acceptance criteria Request Storage allocations per client defined requirements Work with SO to confirm power up and burn-in of Server Install and configure AIX v6.x on 1 LPAR per server Install and configure Bundle Middleware Package Configure AIX and Bundle Middleware per customer build requirements Test hardware and software according to documented test plan Validate acceptance criteria have been met Turn-over system to customer and obtain sign-off Build from base level hardware with no OS pre-installed, physical servers are pre-installed in racks with all hardware installed, base OS, I/O, and HA configuration only (no applications), with base images and configuration standards supplied by customer.
Service Customers / Users	Any participating Commonwealth agency or office.

Service Prerequisites	Software and/or hardware to complete service Access to affected systems and/or facilities.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370020-A	DB2 Build p-Series Standard	Per Request

Service Attribute	*Service Attribute Description*
Service Name	DB2 Build p-Series Complex (2 servers)
Detailed Description	Identify performance and availability requirements Perform hardware selection; solicit physical build from client Baseline current environment and utilization (e.g., CPU, memory) Create high-level design using requirements in Assess phase and baseline build documentation Develop a project plan with milestones, dependencies and resource allocations Plan, track, document, and coordinate activities for the project Create data base or WAS-specific test plans and develop acceptance criteria Request Storage allocations per client defined requirements Work with client to confirm power up and burn-in of Server Install and configure AIX v6.x on 1 LPAR per server Install and configure Bundle Middleware Package Configure AIX and Bundle Middleware per customer build requirements Test hardware and software according to documented test plan Validate acceptance criteria have been met Turn-over system to customer and obtain sign-off Build from base level hardware with no OS pre-installed, physical servers are pre-installed in racks with all hardware installed, base OS, I/O, and HA configuration only (no applications), with base images and configuration standards supplied by customer.
Service Customers / Users	Any participating Commonwealth agency or office.

Service Prerequisites	Software and/or hardware to complete service Access to affected systems and/or facilities.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370021-A	DB2 Build p-Series Complex	Per Request

Service Attribute	*Service Attribute Description*
Service Name	DB2 Upgrade p-Series Standard (1 server)
Detailed Description	Identify performance and availability profile Collect Performance Baseline Create high-level design using requirements in Assess phase and baseline build documentation Develop a project plan with milestones, dependencies and resource allocations Plan, track, document, and coordinate activities for the project Create application-specific test plans and develop acceptance criteria Request new hardware requirements based upon performance requirements Install and configure current version of target Bundle on 1 LPAR per server Test software according to document test plan Validate acceptance criteria have been met Turn-over system to customer and obtain sign-off This is Upgrade of DB only - 1 version level upgrade only, OS will be at a version which support the upgraded DB, base images and configuration standards to be supplied by client. Storage and SAN Fabric are client or other Bundle responsibility, with remote delivery for services is primary alternative, with on-site when necessary.
Service Customers / Users	Any participating Commonwealth agency or office.
Service Prerequisites	Software and/or hardware to complete service Access to affected systems and/or facilities.

Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.

Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370022-A	DB2 Upgrade p-Series Standard	Per Request

Service Attribute	*Service Attribute Description*
Service Name	DB2 Upgrade p-Series Complex (2 servers)
Detailed Description	Identify performance and availability profile Collect Performance Baseline Create high-level design using requirements in Assess phase and baseline build documentation Develop a project plan with milestones, dependencies and resource allocations Plan, track, document, and coordinate activities for the project Create application-specific test plans and develop acceptance criteria Request new hardware requirements based upon performance requirements Install and configure current version of target Bundle on 1 LPAR per server Test software according to document test plan Validate acceptance criteria have been met Turn-over system to customer and obtain sign-off This is Upgrade of DB only - 1 version level upgrade only, OS will be at a version which supports the upgraded DB, base images and configuration standards to be supplied by client. Storage and SAN Fabric are client or other Bundle responsibility, with remote delivery for services is primary alternative, with on-site when necessary.
Service Customers / Users	Any participating Commonwealth agency or office.
Service Prerequisites	Software and/or hardware to complete service Access to affected systems and/or facilities.

Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.

Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370023-A	DB2 Upgrade p-Series Complex	Per Request

Service Attribute	*Service Attribute Description*	
Service Name	p-Series Database Administrator for Oracle (3TB)	
Detailed Description	This services bundle is to provide database administration for Oracle databases on System p. 1 to 35 databases totaling up to maximum of 3TB.	
Service Customers / Users	Any participating Commonwealth agency or office.	
Service Prerequisites	12- month commitment	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370024-A	p-Series Database Administrator for Oracle (3TB Cap)	Per Request / Up to 35 Databases totaling 3 TB stored data

Service Attribute	*Service Attribute Description*	
Service Name	p-Series Database Administrator for Oracle (7TB)	
Detailed Description	This services bundle is to provide database administration for Oracle databases on System p. 36 to 75 databases totaling up to maximum of 7TB.	
Service Customers / Users	Any participating Commonwealth agency or office.	
Service Prerequisites	12- month commitment	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370025-A	p-Series Database Administrator for Oracle (7 TB)	Per Request / Up to 75 Databases totaling 7 TB stored data

Service Attribute	*Service Attribute Description*	
Service Name	p-Series Database Administrator for Oracle (12TB)	
Detailed Description	This services bundle is to provide database administration for Oracle databases on System p. 76 to 120 databases totaling up to maximum of 12TB.	
Service Customers / Users	Any participating Commonwealth agency or office.	
Service Prerequisites	12- month commitment	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370026-A	p-Series Database Administrator for Oracle (12GB)	Per Request / Up to 120 Databases totaling 12 TB stored data

Service Attribute	*Service Attribute Description*	
Service Name	p-Series Database Administrator for DB2 (3TB)	
Detailed Description	This services bundle is to provide database administration for DB2 databases on System p. 1 to 35 databases totaling up to maximum of 3TB.	
Service Customers / Users	Any participating Commonwealth agency or office.	
Service Prerequisites	12- month commitment	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370027-A	p-Series Database Administrator for DB2 (3TB)	Per Request / Up to 35Databases totaling 3 TB stored data

Service Attribute	*Service Attribute Description*	
Service Name	p-Series Database Administrator for DB2 (7TB)	
Detailed Description	This services bundle is to provide database administration for DB2 databases on System p. 36 to 75 databases totaling up to maximum of 7TB.	
Service Customers / Users	Any participating Commonwealth agency or office.	
Service Prerequisites	12- month commitment	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370028-A	p-Series Database Administrator for DB2 (7TB)	Per Request / Up to 75 Databases totaling 7 TB stored data

Service Attribute	*Service Attribute Description*	
Service Name	p-Series Database Administrator for DB2 (12TB)	
Detailed Description	This services bundle is to provide database administration for DB2 databases on System p. 76 to 120 databases totaling up to maximum of 12 TB.	
Service Customers / Users	Any participating Commonwealth agency or office.	
Service Prerequisites	12- month commitment	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370029-A	p-Series Database Administrator for DB2 (12TB)	Per Request / Up to 120 Databases totaling 12 TB stored data

Service Attribute	*Service Attribute Description*	
Service Name	p-Series Database Administrator for High Availability Databases: Oracle RAC or DB2 Clusters (20 databases)	
Detailed Description	This services bundle is to provide database administration for Oracle RAC or DB2 clusters. This is support for 1 to 20 clustered databases.	
Service Customers / Users	Any participating Commonwealth agency or office.	
Service Prerequisites	Standard Database Administrator Enterprise Services Catalog offering for each individual server in RAC or cluster. 12- month commitment	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370030-A	p-Series Database Administrator for High Availability Databases: Oracle RAC or DB2 Clusters (20 databases)	Per Request / Up to 20 clustered databases

Service Attribute	*Service Attribute Description*	
Service Name	p-Series Database Administrator for High Availability Databases: Oracle RAC or DB2 Clusters (40 databases)	
Detailed Description	This services bundle is to provide database administration for Oracle RAC or DB2 clusters. This is support for 21 to 40 clustered databases.	
Service Customers / Users	Any participating Commonwealth agency or office.	
Service Prerequisites	Standard Database Administrator Enterprise Services Catalog offering for each individual server in RAC or cluster. 12- month commitment	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370031-A	p-Series Database Administrator for Database High Availability Oracle RAC/DB2 Clusters Number of databases (40)	Per Request / Up to 40 clustered databases

Service Attribute	*Service Attribute Description*	
Service Name	p-Series Database Administrator for High Availability Databases: Oracle RAC or DB2 Clusters (60 databases)	
Detailed Description	This services bundle is to provide database administration for DBA HA for Oracle RAC/DB2 clusters. This is support for 41 to 60 clustered databases.	
Service Customers / Users	Any participating Commonwealth agency or office.	
Service Prerequisites	Standard Database Administrator Enterprise Services Catalog offering for each individual server in RAC or cluster. 12- month commitment	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370032-A	p-Series Database Administrator for High Availability Databases: Oracle RAC or DB2 Clusters (60 databases)	Per Request / Up to 60 clustered databases

Database Management Deployment and Support Services – z-Series

Service Attribute	*Service Attribute Description*
Service Name	IMS Upgrade z-Series Standard (1 subsystem without data sharing or clustering)
Detailed Description	Identify performance and availability profile Collect Performance Baseline Create high-level design using requirements in Assess phase and baseline build documentation Develop a project plan with milestones, dependencies and resource allocations Plan, track, document, and coordinate activities for the project Create application-specific test plans and develop acceptance criteria Request new hardware requirements based upon performance requirements Install and configure current version of target Bundle on 1 LPAR per server Test software according to document test plan Validate acceptance criteria have been met Turn-over system to customer and obtain sign-off This is Upgrade of IMS only - 1 version level upgrade only, OS will be at a version which support the upgraded DB, base images and configuration standards to be supplied by client. Remote delivery for services is primary alternative, with on-site when necessary.
Service Customers / Users	Any participating Commonwealth agency or office.
Service Prerequisites	Software and/or hardware to complete service Access to affected systems and/or facilities.

Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370033-A	IMS Upgrade z-Series Standard	Per Request

Service Attribute	*Service Attribute Description*
Service Name	IMS Upgrade z-Series Complex (2 subsystems with data sharing and clustering across multiple CECs)
Detailed Description	Identify performance and availability profile Collect Performance Baseline Create high-level design using requirements in Assess phase and baseline build documentation Develop a project plan with milestones, dependencies and resource allocations Plan, track, document, and coordinate activities for the project Create application-specific test plans and develop acceptance criteria Request new hardware requirements based upon performance requirements Install and configure current version of target Bundle on 1 LPAR per server Test software according to document test plan Validate acceptance criteria have been met Turn-over system to customer and obtain sign-off This is Upgrade of IMS only - 1 version level upgrade only, OS will be at a version which support the upgraded DB, base images and configuration standards to be supplied by client. Remote delivery for services is primary alternative, with on-site when necessary.
Service Customers / Users	Any participating Commonwealth agency or office.
Service Prerequisites	Software and/or hardware to complete service Access to affected systems and/or facilities.
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services

	Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370034-A	IMS Upgrade z-Series Complex	Per Request

Service Attribute	*Service Attribute Description*
Service Name	IMS Maintenance z-Series Standard (1 subsystem without data sharing or clustering)
Detailed Description	Identify performance and availability profile Collect Performance Baseline Create high-level design using requirements in Assess phase and baseline build documentation Develop a project plan with milestones, dependencies and resource allocations Plan, track, document, and coordinate activities for the project Create application-specific test plans and develop acceptance criteria Request new hardware requirements based upon performance requirements Install and configure current version of target Bundle on 1 LPAR per server Test software according to document test plan Validate acceptance criteria have been met Turn-over system to customer and obtain sign-off This is Maintenance of IMS only - 1 version level upgrade only, OS will be at a version which support the upgraded DB, base images and configuration standards to be supplied by client. Remote delivery for services is primary alternative, with on-site when necessary.
Service Customers / Users	Any participating Commonwealth agency or office.
Service Prerequisites	Software and/or hardware to complete service Access to affected systems and/or facilities.

Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370035-A	IMS Maintenance z-Series Standard	Per Request

Service Attribute	*Service Attribute Description*
Service Name	IMS Maintenance z-Series Complex (2 subsystems with data sharing and clustering across multiple CECs)
Detailed Description	Identify performance and availability profile Collect Performance Baseline Create high-level design using requirements in Assess phase and baseline build documentation Develop a project plan with milestones, dependencies and resource allocations Plan, track, document, and coordinate activities for the project Create application-specific test plans and develop acceptance criteria Request new hardware requirements based upon performance requirements Install and configure current version of target Bundle on 1 LPAR per server Test software according to document test plan Validate acceptance criteria have been met Turn-over system to customer and obtain sign-off This is Maintenance of IMS only - 1 version level upgrade only, OS will be at a version which support the upgraded DB, base images and configuration standards to be supplied by client. Remote delivery for services is primary alternative, with on-site when necessary.
Service Customers / Users	Any participating Commonwealth agency or office.
Service Prerequisites	Software and/or hardware to complete service Access to affected systems and/or facilities.

Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370036-A	IMS Maintenance z-Series Complex	Per Request

Service Attribute	*Service Attribute Description*
Service Name	DB2 Upgrade z Series Standard (1 subsystem without data sharing or clustering)
Detailed Description	Identify performance and availability profile Collect Performance Baseline Create high-level design using requirements in Assess phase and baseline build documentation Develop a project plan with milestones, dependencies and resource allocations Plan, track, document, and coordinate activities for the project Create application-specific test plans and develop acceptance criteria Request new hardware requirements based upon performance requirements Install and configure current version of target Bundle on 1 LPAR per server Test software according to document test plan Validate acceptance criteria have been met Turn-over system to customer and obtain sign-off This is Upgrade of DB only - 1 version level upgrade only, OS will be at a version which supports the upgraded DB, base images and configuration standards to be supplied by client. Remote delivery for services is primary alternative, with on-site when necessary.
Service Customers / Users	Any participating Commonwealth agency or office.
Service Prerequisites	Software and/or hardware to complete service Access to affected systems and/or facilities.
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services

	Catalog item using the above Service Name.	
Provider Part Number(s)	Service Option Name	Orderable Unit / Restrictions per Unit
CCSI13370037-A	DB2 Upgrade z-Series Standard	Per Request

Service Attribute	*Service Attribute Description*
Service Name	DB2 Upgrade z-Series Complex (2 subsystems with data sharing and clustering across multiple CECs)
Detailed Description	Identify performance and availability profile Collect Performance Baseline Create high-level design using requirements in Assess phase and baseline build documentation Develop a project plan with milestones, dependencies and resource allocations Plan, track, document, and coordinate activities for the project Create application-specific test plans and develop acceptance criteria Request new hardware requirements based upon performance requirements Install and configure current version of target Bundle on 1 LPAR per server Test software according to document test plan Validate acceptance criteria have been met Turn-over system to customer and obtain sign-off This is Upgrade of DB only - 1 version level upgrade only, OS will be at a version which supports the upgraded DB, base images and configuration standards to be supplied by client. Remote delivery for services is primary alternative, with on-site when necessary.
Service Customers / Users	Any participating Commonwealth agency or office.
Service Prerequisites	Software and/or hardware to complete service Access to affected systems and/or facilities.
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services

	Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370038-A	DB2 Upgrade z-Series Complex	Per Request

Service Attribute	*Service Attribute Description*
Service Name	DB2 Maintenance z-Series Standard (1 subsystem without data sharing or clustering)
Detailed Description	Identify performance and availability profile Collect Performance Baseline Create high-level design using requirements in Assess phase and baseline build documentation Develop a project plan with milestones, dependencies and resource allocations Plan, track, document, and coordinate activities for the project Create application-specific test plans and develop acceptance criteria Request new hardware requirements based upon performance requirements Install and configure current version of target Bundle on 1 LPAR per server Test software according to document test plan Validate acceptance criteria have been met Turn-over system to customer and obtain sign-off This is Upgrade of DB only - 1 version level upgrade only, OS will be at a version which supports the upgraded DB, base images and configuration standards to be supplied by client. Remote delivery for services is primary alternative, with on-site when necessary.
Service Customers / Users	Any participating Commonwealth agency or office.
Service Prerequisites	Software and/or hardware to complete service Access to affected systems and/or facilities.
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services

	Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370039-A	DB2 Maintenance z-Series Standard	Per Request

Service Attribute	*Service Attribute Description*
Service Name	DB2 Maintenance z-Series Complex (2 subsystems with data sharing and clustering across multiple CECs)
Detailed Description	Identify performance and availability profile Collect Performance Baseline Create high-level design using requirements in Assess phase and baseline build documentation Develop a project plan with milestones, dependencies and resource allocations Plan, track, document, and coordinate activities for the project Create application-specific test plans and develop acceptance criteria Request new hardware requirements based upon performance requirements Install and configure current version of target Bundle on 1 LPAR per server Test software according to document test plan Validate acceptance criteria have been met Turn-over system to customer and obtain sign-off This is Upgrade of DB only - 1 version level upgrade only, OS will be at a version which supports the upgraded DB, base images and configuration standards to be supplied by client. Remote delivery for services is primary alternative, with on-site when necessary.
Service Customers / Users	Any participating Commonwealth agency or office.
Service Prerequisites	Software and/or hardware to complete service Access to affected systems and/or facilities.
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services

	Catalog item using the above Service Name.	
Provider Part Number(s)	Service Option Name	Orderable Unit / Restrictions per Unit
CCSI13370040-A	DB2 Maintenance z-Series Complex	Per Request

Service Attribute	*Service Attribute Description*	
Service Name	z-Series Database Administrator for DB2 (5TB)	
Detailed Description	This services bundle is to provide database administration for DB2 databases on System z. 1 to 40 databases totaling up to maximum of 5TB. 1 FTE in the bundle for one month.	
Service Customers / Users	Any participating Commonwealth agency or office.	
Service Prerequisites	12- month commitment	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370041-A	z-Series Database Administrator for DB2 (5TB)	Per Request / up to 40 databases with a total of 5 TB stored data

Service Attribute	*Service Attribute Description*	
Service Name	z-Series Database Administrator for DB2 (10TB)	
Detailed Description	This services bundle is to provide database administration for DB2 databases on System z. 41 to 80 databases totaling up to maximum of 10TB. 2 FTEs in the bundle for one month.	
Service Customers / Users	Any participating Commonwealth agency or office.	
Service Prerequisites	12- month commitment	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370042-A	z-Series Database Administrator for DB2 (10TB)	Per Request / Up to 80 databases with a total of 10 TB stored data

Service Attribute	*Service Attribute Description*	
Service Name	z-Series Database Administrator for DB2 (15TB)	
Detailed Description	This services bundle is to provide database administration for DB2 databases on System z. 81 to 120 databases totaling up to maximum of 15TB. 3 FTEs in the bundle for one month.	
Service Customers / Users	Any participating Commonwealth agency or office.	
Service Prerequisites	12- month commitment	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370043-A	z-Series Database Administrator for DB2 (15TB)	Per Request / Up to 120 databases with a total of 15 TB data stored

Service Attribute	*Service Attribute Description*	
Service Name	z-Series Database Administrator for IMS (5TB)	
Detailed Description	This services bundle is to provide database administration for IMS databases on System z. 1 to 40 databases totaling up to maximum of 5TB. 1 FTE in the bundle for one month.	
Service Customers / Users	Any participating Commonwealth agency or office.	
Service Prerequisites	12- month commitment	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370044-A	z-Series Database Administrator for IMS (5TB)	Per Request / Up to 40 databases with a total of 5 TB data stored

Service Attribute	*Service Attribute Description*	
Service Name	z-Series Database Administrator for IMS (10TB)	
Detailed Description	This services bundle is to provide database administration for IMS databases on System z. 41 to 80 databases totaling up to maximum of 10TB. 2 FTE in the bundle for one month.	
Service Customers / Users	Any participating Commonwealth agency or office.	
Service Prerequisites	12- month commitment	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370045-A	z-Series Database Administrator for IMS (10TB)	Per Request / Up to 80 databases with a total of 10 TB data stored

Service Attribute	*Service Attribute Description*	
Service Name	z-Series Database Administrator for IMS (15TB)	
Detailed Description	This services bundle is to provide database administration for IMS databases on System z. 81 to 120 databases totaling up to maximum of 15TB. 3 FTE in the bundle for one month.	
Service Customers / Users	Any participating Commonwealth agency or office.	
Service Prerequisites	12- month commitment	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370046-A	z-Series Database Administrator for IMS (15TB)	Per Request / Up to 120 databases with a total of 15 TB data stored

Service Attribute	*Service Attribute Description*	
Service Name	z-Series High Availability Databases: IMS or DB2 DataSharing (25 databases)	
Detailed Description	This services bundle is to provide database administration for DBA HA for IMS or DB2 DataSharing. This is support for 1 to 25 clustered databases. 1 FTE in the bundle for one month.	
Service Customers / Users	Any participating Commonwealth agency or office.	
Service Prerequisites	Standard Database Administrator Enterprise Services Catalog offering. 12- month commitment	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370047-A	z-Series High Availability Databases: IMS or DB2 DataSharing (25 databases)	Per Request / Up to 25 clustered databases

Service Attribute	*Service Attribute Description*	
Service Name	z-Series High Availability Databases: IMS or DB2 DataSharing (50 databases)	
Detailed Description	This services bundle is to provide database administration for DBA HA for IMS or DB2 Data Sharing. This is support for 26 to 50 clustered databases. 2 FTE in the bundle for one month.	
Service Customers / Users	Any participating Commonwealth agency or office.	
Service Prerequisites	Standard Database Administrator Enterprise Services Catalog offering. 12- month commitment	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370048-A	z-Series High Availability Databases: IMS or DB2 DataSharing (50 databases)	Per Request / Up to 50 clustered databases

Service Attribute	*Service Attribute Description*	
Service Name	z-Series High Availability Databases: IMS or DB2 DataSharing (75 databases)	
Detailed Description	This services bundle is to provide database administration for DBA HA for IMS or DB2 DataSharing. This is support for 51 to 75 clustered databases. 3 FTE in the bundle for one month.	
Service Customers / Users	Any participating Commonwealth agency or office.	
Service Prerequisites	Standard Database Administrator Enterprise Services Catalog offering. 12- month commitment	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370049-A	z-Series High Availability Databases: IMS or DB2 DataSharing (75 databases)	Per Request / Up to 75 clustered databases

Batch and Job Scheduling

Service Attribute	*Service Attribute Description*	
Service Name	Batch and Job Scheduling –Job Creation or Modification	
Detailed Description	This service is for creating or modifying batch jobs and for scheduling and monitoring batch jobs in production.	
Service Customers / Users	Any participating Commonwealth agency or office Application Owners	
Service Prerequisites	Batch jobs must be run on the Unisys managed infrastructure that is in-scope	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370050-A	Batch and Job Scheduling – Job Creation or Modification – Small	Per Script / up to 25 Steps
CCSU13370051-A	Batch and Job Scheduling – Job Creation or Modification – Medium	Per Script / up to 50 Steps
CCSU13370052-A	Batch and Job Scheduling – Job Creation or Modification – Large	Per Script / up to 100 Steps

Service Attribute	*Service Attribute Description*	
Service Name	Batch and Job Scheduling –Scheduling and Monitoring	
Detailed Description	This Service will setup a batch job in the production scheduling tool and provide monitoring for the batch job to help confirm successful completion.	
Service Customers / Users	Any participating Commonwealth agency or office Application Owners	
Service Prerequisites	What is required before this service or service element be ordered? 1) Batch job has been created and tested successfully as part of the Change Management and Release and Deployment processes	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370053-A	Batch and Job Scheduling – Scheduling and Monitoring - Small	Per Script / up to 25 Steps
CCSU13370054-A	Batch and Job Scheduling – Scheduling and Monitoring - Medium	Per Script / up to 50 Steps
CCSU13370055-A	Batch and Job Scheduling – Scheduling and Monitoring - Large	Per Script / up to 100 Steps

Service Attribute	*Service Attribute Description*	
Service Name	Batch and Job Scheduling –Scheduling and Monitoring – Control M License	
Detailed Description	This Service will setup a batch job in the production scheduling tool and provide monitoring for the batch job to help confirm successful completion.	
Service Customers / Users	Any participating Commonwealth agency or office Application Owners	
Service Prerequisites	What is required before this service or service element be ordered? 1) Batch job has been created and tested successfully as part of the Change Management and Release and Deployment processes 2) Batch Job is monitored by Batch and Job Scheduling – Scheduling and Monitoring service.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370511-A	Batch and Job Scheduling – Scheduling and Monitoring – Small –Control M License	Per Script / up to 25 Steps
CCSU13370512-A	Batch and Job Scheduling – Scheduling and Monitoring – Medium – Control M License	Per Script / up to 50 Steps

CCSU13370513-A	Batch and Job Scheduling – Scheduling and Monitoring – Large – Control M License	Per Script / up to 100 Steps

Service Attribute	*Service Attribute Description*	
Service Name	AIX Production Batch Operations Support (50,000 jobs per year)	
Detailed Description	AIX Production Batch Operations Support will be performed by remote US and on-site batch operators. AIX Production Batch Operations Support provides the following: 1. Schedule batch jobs; 2. Start and re-start batch jobs; 3. Monitor scheduled batch jobs; 4. Resolve non-application batch scheduling conflicts for root cause analysis and change management purposes; 5. Monitor scheduler-related incidents, and develop and recommend changes to the scheduler database; 6. Perform required batch setup activities, such as ad hoc requests; 7. Schedule batch jobs that require immediate execution upon request; 8. Invoke resolution and restart procedures in case of batch job failure; 9. Alert Commonwealth as set forth in CCPM; 10. Recover customer's batch environment; and 11. Log each batch job.	
Service Customers / Users	Any participating agency/department. Annual commitment, invoiced monthly.	
Service Prerequisites	AIX environment	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**

CCSI13370056-A	AIX Production Batch Operations	Per Package of 50,000 jobs per year

Service Attribute	*Service Attribute Description*
Service Name	IBM Mainframe Production Batch Operations Support (50,000 jobs per year)
Detailed Description	IBM Mainframe Production Batch Operations Support will be performed by remote US and on-site batch operators. IBM Mainframe Production Batch Operations Support provides the following: 1. Schedule batch jobs; 2. Start and re-start batch jobs; 3. Monitor scheduled batch jobs; 4. Resolve non-application batch scheduling conflicts for root cause analysis and change management purposes; 5. Monitor scheduler-related incidents, and develop and recommend changes to the scheduler database; 6. Perform required batch setup activities, such as ad hoc requests; 7. Schedule batch jobs that require immediate execution upon request; 8. Invoke resolution and restart procedures in case of batch job failure; 9. Alert Commonwealth as set forth in CCPM; 10. Recover customer's batch environment; and 11. Log each batch job.
Service Customers / Users	Any participating agency/department. Annual commitment, invoiced monthly.
Service Prerequisites	IBM Mainframe environment.
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.

Provider Part Number(s)	Service Option Name	Orderable Unit / Restrictions per Unit
CCSI13370057-A	IBM Mainframe Production Batch Operations	Per Package of 50,000 jobs per year

Service Management

Custom Reports

Service Attribute	*Service Attribute Description*	
Service Name	Service Management Custom Report	
Detailed Description	The Service Management Custom Report Service will allow Commonwealth personnel to request a custom report in support of the Governance of the Contract. The report request will be reviewed and approved, configured, tested and placed into production per agreed timeframe to complete an approved request.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	What is required before this service or service element can be ordered or completed? Approvals from the Commonwealth/Unisys PMO	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370058-A	Service Management Custom Report – Small	Per Report / 4 hours effort to complete
CCSU13370059-A	Service Management Custom Report – Medium	Per Report / 8 hours to complete
CCSU13370060-A	Service Management Custom Report - Large	Per Report / 20 hours to complete

ITSM Additional Licensing

Service Attribute	*Service Attribute Description*	
Service Name	Commonwealth ITSM User Licensing – Service Desk	
Detailed Description	Provide a named user or transfer of a user on a named license or a floating user license for use by the Commonwealth / Agency Service Desk users	
Service Customers / Users	Any participating Commonwealth agency or office Service Desk Management	
Service Prerequisites	What is required before this service or service element be ordered? 1) Training in Unisys Remedy ITSM Solution 2) Approval of the request by the Commonwealth / Unisys PMO	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370061-A	ITSM Licensing – End User Service Desk – Named User	Named License per month
CCSU13370062-A	ITSM Licensing – Floating User Service Desk – Floating users	Floating License per month for up to 10 users

Application Definition Mapping

Service Attribute	*Service Attribute Description*	
Service Name	Application Mapping Discovery Script - Setup	
Detailed Description	This Service will provide the necessary setup services to support calculating an availability infrastructure SLA that will support a new or modified Commonwealth / Agency application following transition. This service includes the mapping of CMDB items to the Application CI, configuring event monitoring, incident management and service level management applications to support an availability SLA for the specified Application.	
Orderable Unit	Per Number of Days to Complete the setup for small, medium and large application infrastructure environments.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites		
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370063-A	Application Definition Mapping – Initial Discovery Script - Small	Per Application Discovery Script / 4 hours
CCSU13370064-A	Application Definition Mapping – Initial Discovery Script - Medium	Per Application Discovery Script / 8 hours
CCSU13370065-A	Application Definition Mapping – Initial Discovery Script - Large	Per Application Discovery Script / 16 hours

Service Attribute	*Service Attribute Description*	
Service Name	Application Mapping Discovery Script Maintenance	
Detailed Description	This Service will provide the necessary support to maintain and monitor the Application Availability SLA monitoring environment including the mapping of CMDB items to the Application CI, configuration of event monitoring, incident management and service level management applications to support an availability SLA for the specified Application.	
Orderable Unit	Number of hours required to support the Application Availability SLA yearly depending upon whether the application infrastructure is small (8 hours), medium (16 hours) or large (32 hours). Charged monthly.	
Service Customers / Users	Any participating Commonwealth agency or office Application Owners	
Service Prerequisites		
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370066-A	Application Definition Mapping – Discovery Script – Maintenance - Small	8 hours per year support
CCSU13370067-A	Application Definition Mapping – Discovery Script - Maintenance - Medium	16 hours per year support
CCSU13370068-A	Application Definition Mapping – Discovery Script - Maintenance - Large	32 hours per year support

Compute Services – Infrastructure Monitoring

Service Attribute	*Service Attribute Description*	
Service Name	Microsoft System Center 2012 (SCOM)	
Detailed Description	This service will provide SCOM monitoring of infrastructure supporting an application on a per server basis. This service will substitute for the default Nagios monitoring service that Unisys provides as a standard if the Commonwealth / Agency Application Owner prefers to have SCOM monitoring for a Windows/Linux infrastructure environment.	
Service Customers / Users	Any participating Commonwealth agency or office Application Owners	
Service Prerequisites	What is required before this service or service element be ordered? 1) SCOM Monitoring Server Capacity	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370069-A	Microsoft System Center 2012 (SCOM) – Standard	Per Server (virtual or physical)

Fully Managed Service

Windows / Linux

Service Attribute	*Service Attribute Description*
Service Name	Fully Managed Windows / Linux – Physical Server - Commission/Decommission Service Fee
Detailed Description	This fee includes the following: 1) Physical installation of the server 2) Installation of the operating system 3) Initial patching and security remediation 4) Setup of monitoring and CMDB CI entries 5) At decommissioning, wipe of any data from local drives 6) Unracking of server 7) For Unisys owned assets, disposal of all server and server related parts.
Service Customers / Users	Any participating Commonwealth agency or office
Service Prerequisites	1) Ordering of a physical or virtual fully managed Windows or Linux server 2) Ordering of managed only services 3) Ordering of Infrastructure as a Service server.
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog

Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370070-A	Fully Managed – Physical – Platinum – Comm/Decomm	Per Server
CCSU13370071-A	Fully Managed – Physical – Gold – Comm/Decomm	Per Server
CCSU13370072-A	Fully Managed – Physical – Silver – Comm/Decomm	Per Server
CCSU13370073-A	Fully Managed – Physical – Bronze – Comm/Decomm	Per Server
CCSU13370074-A	Fully Managed – Physical – Basic – Comm/Decomm	Per Server

Service Attribute	*Service Attribute Description*	
Service Name	Fully Managed Windows / Linux – Virtual Server - Commission/Decommission Service Fee	
Detailed Description	This fee includes the following: 4) Physical installation of the server 5) Installation of the operating system 6) Initial patching and security remediation 7) Setup of monitoring and CMDB CI entries 8) At decommissioning, wipe of any data from local drives 9) Unracking of server 10) For Unisys owned assets, disposal of all server and server related parts.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1) Ordering of a physical or virtual fully managed Windows or Linux server	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**

CCSU13370075-A	Fully Managed – Virtual – Platinum – Comm/Decomm	Per Server
CCSU13370076-A	Fully Managed – Virtual – Gold – Comm/Decomm	Per Server
CCSU13370077-A	Fully Managed – Virtual – Silver – Comm/Decomm	Per Server
CCSU13370078-A	Fully Managed – Virtual – Bronze – Comm/Decomm	Per Server
CCSU13370079-A	Fully Managed – Virtual – Basic – Comm/Decomm	Per Server

P-Series (AIX) Services

Service Attribute	*Service Attribute Description*	
Service Name	Platinum AIX Service Level Package	
Detailed Description	This package provides the additional hardware, software and services needed beyond the Resource Units to attain an availability of 99.999%.	
Service Customers / Users	Any participating Commonwealth agency or department	
Service Prerequisites	This service is only available after the workload is migrated to the new data center from the DPH and requires use of a second data center. For Platinum Tier Service Levels, there must be a minimum of three instances of the application, geographically dispersed and clustered or load balanced in such a manner that if one instance is taken offline, the end user sees no disruption or degradation of service. Must purchase a quantity of three of one of the following items: • AIX Config – 1 Fully Managed (1) - Platinum Tier • AIX Config – 2 Fully Managed (1) - Platinum Tier • AIX Config – 3 Fully Managed (1) - Platinum Tier • AIX Config – 4 Fully Managed (1) - Platinum Tier • AIX Config – 5 Fully Managed (1) - Platinum Tier The above Configs also have prerequisites that can be found in their Enterprise Services Catalog entry. Four-year commitment, invoiced monthly.	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**

CCSI13370080-A	Platinum AIX Service Level Package	Per Package

Service Attribute	*Service Attribute Description*
Service Name	Gold AIX Service Level Package
Detailed Description	This package provides the additional hardware, software and services needed beyond the Resource Units to attain an availability of 99.99%.
Service Customers / Users	Any participating Commonwealth agency or department.
Service Prerequisites	This service is only available after the workload is migrated to the new data center from the DPH and requires use of a second data center. For Gold Tier Service Levels, there must be a minimum of two instances of the application, either clustered or load balanced in such a manner that if one instance is taken offline, the end user sees no disruption or degradation of service. Must purchase a quantity of two of one of the following items: • AIX Config – 1 Fully Managed (1) - Gold Tier • AIX Config – 2 Fully Managed (1) - Gold Tier • AIX Config – 3 Fully Managed (1) - Gold Tier • AIX Config – 4 Fully Managed (1) - Gold Tier • AIX Config – 5 Fully Managed (1) - Gold Tier The above Configs also have prerequisites that can be found in their Enterprise Services Catalog entry. Four-year commitment, invoiced monthly.
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog.

Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per**

		Unit
CCSI13370081-A	Gold AIX Service Level Package	Per Package

Service Attribute	***Service Attribute Description***	
Service Name	Disaster Recovery - AIX (271 images)	
Detailed Description	This replaces the Disaster Recovery environment currently provided by Unisys as part of the DPH contract and set forth in Exhibit B5 and Exhibit B9.	
Service Customers / Users	Current users of the DPH Disaster Recovery service.	
Service Prerequisites	The Commonwealth and IBM will conduct knowledge transfer and establish a test process and schedule prior to service assumption. Annual commitment, invoiced monthly.	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370082-A	Disaster Recovery - AIX	Per Package

Storage and Backup Services

Service Attribute	*Service Attribute Description*	
Service Name	Archive Services: Archive storage that provides record-level content management and replication to DR	
Detailed Description	The service offers secure, reliable storage of data objects that satisfy the regulatory compliance requirements of SEC 17a-4, Sarbanes-Oxley, and HIPAA. The service provides long-term disk-based archive storage for data that is required to meet compliance requirements to provide content authentication, non-eraseability, and record-level content management. The service includes software costs for replication of content to an alternate Unisys-managed site and associated infrastructure at the alternate Unisys-managed site.	
Service Customers / Users	The Service is Available to Any participating Commonwealth agency or office.	
Service Prerequisites	What is required before this service or service element be ordered? 1) Selection of sufficient Network services to provide bandwidth for replication between sites. 2) Selection of sufficient Data Center resources to provide space and power for required infrastructure.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370083-A	Archive Services: Archive storage that provides record-level content management and replication to DR	Per GB of Protected Data

Service Attribute	*Service Attribute Description*
Service Name	EMC PowerPath Storage Load Balancing S/W for Physical Servers.
Detailed Description	For Fully-managed physical servers with a single O/S that are SAN-attached to EMC storage the service provides: **Automate failover and recovery** – Mitigates the threat of application disruptions from adapter and cable failures or user errors. Automates failover to alternate data paths in order to keep business processes online. Leverages intelligent, dynamic path testing to remove faulty paths and restore repaired paths to service without user intervention and without disrupting applications. **Optimize load balancing** – Helps eliminate I/O bottlenecks by intelligently optimizing data access across all available data paths. Manages I/O to goal that no path becomes overloaded while others have underutilized bandwidth. Leverages load-based path testing to confirm the viability of a data path for the workload assigned to it. **Standardize path management** – Provides standardization of storage path management for Linux, Microsoft Windows, and UNIX across evolving physical and virtual environments. Supports heterogeneous servers, operating systems, and storage including EMC and qualified non-EMC storage arrays.
Service Customers / Users	The Service is Available to Any participating Commonwealth agency or office.
Service Prerequisites	What is required before this service or service element be ordered? 1) Selection of sufficient server and SAN-attached storage to support server O/S and install of software.
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.

Provider Part Number(s)	Service Option Name	Orderable Unit / Restrictions per Unit
CCSU13370085-A	EMC PowerPath Storage Load Balancing S/W for Physical Servers.	Per CPU Per Server

Service Attribute	*Service Attribute Description*
Service Name	EMC PowerPath Storage Load Balancing S/W for Virtual Server hosts.
Detailed Description	For Fully-managed virtual host servers with multiple virtual servers that are SAN-attached to EMC storage the service provides: **Automate failover and recovery** – Mitigates the threat of application disruptions from adapter and cable failures or user errors. Automates failover to alternate data paths in order to keep business processes online. Leverages intelligent, dynamic path testing to remove faulty paths and restore repaired paths to service without user intervention and without disrupting applications. **Optimize load balancing** – Helps eliminate I/O bottlenecks by intelligently optimizing data access across all available data paths. Manages I/O to goal that no path becomes overloaded while others have underutilized bandwidth. Leverages load-based path testing to confirm the viability of a data path for the workload assigned to it. **Standardize path management** – Provides standardization of storage path management for Linux, Microsoft Windows, and UNIX across evolving physical and virtual environments. Supports heterogeneous servers, operating systems, and storage including EMC and qualified non-EMC storage arrays.
Service Customers / Users	The Service is Available to Any participating Commonwealth agency or office.
Service Prerequisites	What is required before this service or service element be ordered? 1) Selection of sufficient server and SAN-attached storage to support server O/S and install of software.
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.

Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370086-A	EMC PowerPath Storage Load Balancing S/W for Virtual Server hosts.	Per CPU per Virtual Host Server

Service Attribute	*Service Attribute Description*	
Service Name	Archive Services: Cost Effective Archive storage with replication to DR.	
Detailed Description	The service provides long-term disk-based archive storage for data but does not provide compliance requirements for content authentication, non-eraseability, and record-level content management. The service includes software costs for replication of content to an alternate Unisys-managed site and associated infrastructure at the alternate Unisys-managed site.	
Service Customers / Users	The Service is Available to Any participating Commonwealth agency or office.	
Service Prerequisites	What is required before this service or service element be ordered? 1) Selection of sufficient Network services to provide bandwidth for replication between sites. 2) Selection of sufficient Data Center resources to provide space and power for required infrastructure.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370088-A	Archive Services: Cost Effective Archive storage with replication to DR.	Per GB of Protected Data

Service Attribute	*Service Attribute Description*	
Service Name	IBM Storwize V7000 High Performance Tier	
Detailed Description	This solution includes one storage subsystem which provides 180.8 TB via Raid 5 of useable space. This includes • IBM Storwize V7000 (Model 2076-124) • 240 – 900 GB 10k SAS disk • 8 – Fiber Optic Cable LC-LC • Two PDU power cords • Remote Mirroring license for 8 disk shelves • Includes four year hardware and software maintenance	
Service Customers / Users	Any participating Commonwealth agency or office.	
Service Prerequisites	Access to affected systems and/or facilities. Does not include ongoing storage management support; hardware, software and maintenance services only.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370558-A	IBM Storwize V7000 High Performance Replication Tier	Per System

Service Attribute	*Service Attribute Description*	
Service Name	IBM Storwize V7000 Standard Performance Tier	
Detailed Description	This solution includes one storage subsystem which provides 34.4 TB via Raid 10 of useable space. This includes • IBM Storwize V7000 (Model 2076-124) • 240 – 300 GB 15k SAS disk • 8 – Fiber Optic Cable LC-LC • Two PDU power cords • Remote Mirroring license for 8 disk shelves • Includes four year hardware and software maintenance	
Service Customers / Users	Any participating Commonwealth agency or office.	
Service Prerequisites	Access to affected systems and/or facilities. Does not include ongoing storage management support; hardware, software and maintenance services only.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370559-A	IBM Storwize V7000 Standard Performance Replication Tier	Per System

Service Attribute	*Service Attribute Description*	
Service Name	IBM XIV Standard Performance Tier	
Detailed Description	This solution includes one storage subsystem which provides 243.3 TB of useable space. This includes: • IBM XIV Gen 3 (2812-214) • 15 Module System • Unix/Linux/VMWare/Windows Host Attachment • 24 – Fiber Channel Cables • Remote Mirroring license • Includes four year hardware and software maintenance	
Service Customers / Users	Any participating Commonwealth agency or office.	
Service Prerequisites	Access to affected systems and/or facilities. Does not include ongoing storage management support; hardware, software and maintenance services only.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370560-A	IBM XIV Standard Performance Tier	Per System

Service Attribute	*Service Attribute Description*	
Service Name	IBM XIV High Performance Tier	
Detailed Description	This solution includes one storage subsystem which provides 190 TB of useable space with SSD. This includes: • IBM XIV Gen 3 (2812-214) • 15 Module System with SSD • 24 – Fiber Channel Cables • Unix/Linux/VMWare/Windows Host Attachment • Remote Mirroring license • Includes four year hardware and software maintenance	
Service Customers / Users	Any participating Commonwealth agency or office.	
Service Prerequisites	Access to affected systems and/or facilities. Does not include ongoing storage management support; hardware, software and maintenance services only.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370561-A	IBM XIV High Performance Tier	Per System

Service Attribute	*Service Attribute Description*	
Service Name	IBM Storwize V7000 Unified NAS Tier	
Detailed Description	This solution includes one storage subsystem which provides 11.8 TB of useable space. This includes: • IBM Storwize V7000 Unified • CIFS/NFS/HTTP/FTP/iSCSI/FC Protocols • 9 – 2 TB 7.2k SATA • 4 – 5M Fiber Channel Cables (LC-LC) • Includes four year hardware and software maintenance	
Service Customers / Users	Any participating Commonwealth agency or office.	
Service Prerequisites	Access to affected systems and/or facilities. Does not include ongoing storage management support; hardware, software and maintenance services only.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370562-A	IBM Storwize V7000 Unified NAS Tier	Per System

Service Attribute	*Service Attribute Description*	
Service Name	IBM Standard Rack	
Detailed Description	This solution includes one standard IBM 7014-T42 rack: •□ IBM Rack (7014-T42) •□ Front Door For 2.0 Meter Rack (Flat Black) •□ Side Panel For 1.8 or 2.0 Meter Rack (Black) •□ 7188/9188 PDU To Wall,4.3M,48A,IEC 309,2P+G 60A Plug •□ Universal Side Mount PDU(1P 24/48A,3P 16/24A) •□ Universal PDU Base/Side Mount Specify (1P 24/48A,3P 16/24A) •□ Includes four year hardware and software maintenance	
Service Customers / Users	Any participating Commonwealth agency or office.	
Service Prerequisites	Access to affected systems and/or facilities. Does not include ongoing storage management support; hardware, software and maintenance services only.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370563-A	IBM Standard Rack	Per System

Managed Only Service

Windows / Linux

Service Attribute	*Service Attribute Description*	
Service Name	Managed Only Windows / Linux – Commission/Decommission Service Fee	
Detailed Description	Short write up on what the Catalog item will do	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	What is required before this service or service element be ordered? 1) Selection of another service (what service?) 2) Solution Request submittal 3) Etc.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370091-A	Managed Only – Platinum – Comm/Decomm	Per Server
CCSU13370092-A	Managed Only – Gold – Comm/Decomm	Per Server

CCSU13370093-A	Managed Only – Silver – Comm/Decomm	Per Server
CCSU13370094-A	Managed Only – Bronze – Comm/Decomm	Per Server
CCSU13370095-A	Managed Only – Basic – Comm/Decomm	Per Server

Mainframe Services

IBM Mainframe

Service Attribute	*Service Attribute Description*
Service Name	Platinum IBM Mainframe Service Level Package
Detailed Description	This package provides the additional hardware, software and services needed beyond the Resource Units to attain an availability of 99.999%.
Service Customers / Users	Any participating agency/department.
Service Prerequisites	This service is only available after the workload is migrated to the new data center from the DPH and requires use of a second data center. For Platinum Tier Service Levels, there must be a minimum of three instances of the application, geographically dispersed and clustered or load balanced in such a manner that if one instance is taken offline, the end user sees no disruption or degradation of service. Must purchase a quantity of three of one of the following items: • IBM Mainframe Config – 1 Mainframe Services (4) - Platinum Tier, • IBM Mainframe Config – 2 Mainframe Services (4) - Platinum Tier, or • IBM Mainframe Config – 3 Mainframe Services (4) - Platinum Tier. The necessary quantity of the following should must also be purchased: • IBM Mainframe Config – 1 IBM System zEnterprise Processor z/OS • IBM Mainframe Config – 2, 3 IBM System zEnterprise Processor Virtual Linux Prod IFL. • Four-year commitment, invoiced monthly.

Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370096-A	Platinum IBM Mainframe Service Level Package	Per Package

Service Attribute	Service Attribute Description
Service Name	Gold IBM Mainframe and i-Series Service Level Package
Detailed Description	This package provides the additional hardware, software and services needed beyond the Resource Units to attain an availability of 99.99%.
Service Customers / Users	Any participating agency/department.
Service Prerequisites	This service is only available after the workload is migrated to the new data center from the DPH and requires use of a second data center. For Gold Tier Service Levels, there must be a minimum of two instances of the application, either clustered or load balanced in such a manner that if one instance is taken offline, the end user sees no disruption or degradation of service. Must purchase a quantity of two of one of the following items: • IBM Mainframe Config – 1 Mainframe Services (4) - Gold Tier • IBM Mainframe Config – 2 Mainframe Services (4) - Gold Tier • IBM Mainframe Config – 3 Mainframe Services (4) - Gold Tier • IBM AS400 Config 1 Mainframe Services (4) - Gold Tier • IBM AS400 Config 2 Mainframe Services (4) - Gold Tier. The necessary quantity of the following should must also be purchased: • IBM Mainframe Config – 1 IBM System zEnterprise Processor z/OS • IBM Mainframe Config – 2, 3 IBM System zEnterprise Processor Virtual Linux Prod IFL • IBM AS400 Config 1, 2 IBM i Series / AS400. • Four-year commitment, invoiced monthly.
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog.

Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370097-A	Gold IBM Mainframe and i-Series Service Level Package	Per Package

Service Attribute	*Service Attribute Description*	
Service Name	DPH IBM Mainframe Services	
Detailed Description	Additional configuration items and services required to reproduce existing mainframe environment in the new data center.	
Service Customers / Users	Current users of the IBM Mainframe services.	
Service Prerequisites	Commitment for term of Agreement, invoiced monthly.	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog.	
Provider Part Number(s)	Service Option Name	Orderable Unit / Restrictions per Unit
CCSI13370098-A	IBM Mainframe Services – Exhibit based Configuration additions	Per Package

Service Attribute	*Service Attribute Description*	
Service Name	Disaster Recovery - Mainframe / iSeries (134 images)	
Detailed Description	This reproduces the Disaster Recovery environment currently provided as part of the DPH contract and set forth in Exhibit 19.01.	
Service Customers / Users	Current users of the DPH Disaster Recovery service.	
Service Prerequisites	Mainframe DPH Enterprise Services Catalog item and its prerequisites Annual commitment, invoiced monthly.	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370099-A	Disaster Recovery - Mainframe / iSeries	Per Package

Unisys Mainframe – Storage and Backup

Service Attribute	*Service Attribute Description*	
Service Name	Mainframe Services: EMC RecoverPoint Replication	
Detailed Description	Storage services provides 50TB of data replication for a Unisys-managed Production datacenter Mainframe.	
Orderable Unit	By 50TB quantities of SAN-attached Mainframe storage	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	Requested storage is Unisys-managed and Mainframe attached in Unisys-managed Production datacenter A matching quantity of data replication is requested in the Unisys-managed Disaster Recovery site. A sufficient amount of network bandwidth has been requisitioned between the Unisys-managed datacenters.	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370099-A	Mainframe Services: EMC RecoverPoint Replication	Per 50 TB

Service Attribute	*Service Attribute Description*	
Service Name	Mainframe Services: EMC SRDF Replication	
Detailed Description	Storage services provides 50TB of data replication for a Unisys-managed Production datacenter Mainframe.	
Orderable Unit	By 50TB quantities of SAN-attached Mainframe storage	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1) Requested storage is Unisys-managed and Mainframe attached in Unisys-managed Production datacenter 2) A matching quantity of data replication is requested in the Unisys-managed Disaster Recovery site. 3) A sufficient amount of network bandwidth has been requisitioned between the Unisys-managed datacenters.	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370100-A	Mainframe Services: EMC SRDF Replication	Per 50 TB

Unisys Mainframe Configuration – Add On Software Run Pack

Service Attribute	*Service Attribute Description*	
Service Name	Unisys Mainframe (ClearPath Dorado) – Config-1 – Run Pack	
Detailed Description	Provides Unisys supplied operating system utilities and Compilers to Config – 1.	
Service Customers / Users	Department of Public Welfare Pennsylvania State Police	
Service Prerequisites	What is required before this service or service element be ordered? 1) Solution Request submittal to confirm requested system meets application processing requirements 2) Order Config - 1	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370102-A	Unisys Mainframe Config 1 - Unisys (ClearPath / Dorado) Software Run Pack	Per Config

Service Attribute	*Service Attribute Description*	
Service Name	Unisys Mainframe (ClearPath Libra) – Config 2 – Run Pack	
Detailed Description	Provides Unisys supplied operating system utilities and Compilers to Config – 2.	
Service Customers / Users	Pennsylvania Game Commission	
Service Prerequisites	What is required before this service or service element be ordered? 1) Solution Request submittal to confirm requested system meets application processing requirements 2) Order Config - 2	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370103-A	Unisys Mainframe Config- 2 - Unisys (ClearPath / Libra) Software Run Pack	Per Config

Service Attribute	*Service Attribute Description*	
Service Name	Unisys Mainframe (ClearPath Dorado) – Config- 3 – Run Pack	
Detailed Description	Provides Unisys supplied operating system utilities and Compilers to Config – 3.	
Service Customers / Users	Department of Public Welfare Pennsylvania State Police	
Service Prerequisites	What is required before this service or service element be ordered? 1) Solution Request submittal to confirm requested system meets application processing requirements 2) Order Config - 3	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370104-A	Unisys Mainframe Config 3 - Unisys (ClearPath / Dorado) Software Run Pack	Per Config

Service Attribute	*Service Attribute Description*	
Service Name	Unisys Mainframe (ClearPath Libra) – Config 4 – Run Pack	
Detailed Description	Provides Unisys supplied operating system utilities and Compilers to Config – 4.	
Service Customers / Users	Pennsylvania Game Commission	
Service Prerequisites	What is required before this service or service element be ordered? 1) Solution Request submittal to confirm requested system meets application processing requirements 2) Order Config - 4	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370105-A	Unisys Mainframe Config-4 - Unisys (ClearPath / Libra) Software Run Pack	Per Config

Unisys Mainframe Exhibit Based Replacements

Service Attribute	*Service Attribute Description*	
Service Name	Unisys Mainframe (ClearPath Dorado) – DPW Production System	
Detailed Description	Provides technology replacement of DPW mainframe as described in the Exhibits	
Service Customers / Users	Department of Public Welfare	
Service Prerequisites	What is required before this service or service element be ordered? *1)* Solution Request submittal to confirm requested system and staff meets application processing requirements	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13370106-A	Unisys Mainframe (ClearPath Dorado) – DPW Production System	Per Config

Service Attribute	*Service Attribute Description*	
Service Name	Unisys Mainframe (ClearPath Dorado) – PSP Production System	
Detailed Description	Provides technology replacement of PSP mainframe as described in the Exhibits	
Service Customers / Users	Pennsylvania State Police	
Service Prerequisites	What is required before this service or service element be ordered? *1)* Solution Request submittal to confirm requested system and staff meets application processing requirements	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13370107-A	Unisys Mainframe (ClearPath Dorado) – PSP Production System	Per Config

Service Attribute	*Service Attribute Description*	
Service Name	Unisys Mainframe (ClearPath Dorado) – DPW/PSP DR system	
Detailed Description	Provides technology replacement of DPW/PSP DR mainframe as described in the Exhibits	
Service Customers / Users	Department of Public Welfare Pennsylvania State Police	
Service Prerequisites	What is required before this service or service element be ordered? 1) Solution Request submittal to confirm requested system and staff meets application processing requirements	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13370108-A	Unisys Mainframe (ClearPath Dorado) – DPW/PSP DR system	Per Config

Service Attribute	*Service Attribute Description*	
Service Name	Unisys Mainframe (ClearPath Libra) – PA Game Production system	
Detailed Description	Provides technology replacement of PA Game Production mainframe as described in the Exhibits	
Service Customers / Users	Pennsylvania Game Commission	
Service Prerequisites	What is required before this service or service element be ordered? 1) Solution Request submittal to confirm requested system and staff meets application processing requirements	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13370109-A	Unisys Mainframe (ClearPath Dorado) – PA Game Production System	Per Config

Service Attribute	*Service Attribute Description*	
Service Name	Unisys Mainframe (ClearPath Libra) – PA Game Development system	
Detailed Description	Provides technology replacement of PA Game Development mainframe as described in the Exhibits	
Service Customers / Users	Pennsylvania Game Commission	
Service Prerequisites	What is required before this service or service element be ordered? 1) Solution Request submittal to confirm requested system and staff meets application processing requirements	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13370110-A	Unisys Mainframe (ClearPath Dorado) – PA Game Development System	Per Config

Service Attribute	*Service Attribute Description*	
Service Name	Unisys Mainframe (ClearPath Libra) – PA Game DR system	
Detailed Description	Provides technology replacement of PA Game DR mainframe as described in the Exhibits	
Service Customers / Users	Pennsylvania Game Commission	
Service Prerequisites	What is required before this service or service element be ordered? 1) Solution Request submittal to confirm requested system and staff meets application processing requirements	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit**
CCSU13370111-A	Unisys Mainframe (ClearPath Dorado) – PA Game DR System	Per Config

Infrastructure as a Service

Microsoft Cloud Compute Services

Service Attribute	*Service Attribute Description*	
Service Name	Microsoft SharePoint Online – Government Cloud	
Detailed Description	SharePoint Online delivers the powerful features of SharePoint without the associated overhead of managing the infrastructure. Microsoft SharePoint Online enables an organization to easily create and manage custom team-focused and project-focused sites for collaboration. In addition, it's possible to deploy an organization-wide intranet portal used to disseminate information and news across the organization.	
Service Customers / Users	*Any participating Commonwealth agency or office*	
Service Prerequisites	1) The SharePoint Administrator service is required based on the total number of SharePoint users.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSM13370113-A	SharePoint Online Plan 1 (Govt Cloud)	Per User Monthly Subscription
CCSM13370114-A	SharePoint Online Plan 2 (Govt Cloud)	Per User Monthly Subscription

Service Attribute	*Service Attribute Description*	
Service Name	Microsoft Office 365 – Government Cloud	
Detailed Description	Microsoft Office 365 delivers the power of cloud productivity to businesses of all sizes, helping save time, money, and free up valued resources. Office 365 combines the familiar Microsoft Office desktop suite with cloud-based versions of Microsoft's next-generation communications and collaboration services—including Microsoft Exchange Online, Microsoft SharePoint Online, Microsoft Office Web Apps, and Microsoft Lync Online—to help users be productive from virtually anywhere through the Internet.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	The Office 365 Administrator service is required based on the total number of SharePoint users.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSM13370115-A	Microsoft Office 365 Plan 1 (Govt Cloud)	Per User Monthly Subscription
CCSM13370116-A	Microsoft Office 365 Plan 3 (Govt Cloud)	Per User Monthly Subscription

Service Attribute	*Service Attribute Description*	
Service Name	Microsoft Project Server Online – Government Cloud	
Detailed Description	Microsoft Project Online is a flexible online solution for project portfolio management (PPM) and everyday work. Delivered through Office 365, Project Online enables organizations to get started, prioritize project portfolio investments and deliver the intended business value—from virtually anywhere on nearly any device.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1) None	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSM13370117-A	Microsoft Project Server Online (Govt Cloud)	Per User Monthly Subscription
CCSM13370118-A	Microsoft Project Server Online with Project Pro (Govt Cloud)	Per User Monthly Subscription

Service Attribute	*Service Attribute Description*	
Service Name	Microsoft Dynamics CRM Online	
Detailed Description	Microsoft Dynamics is a flexible, powerful business solution for CRM and ERP that connects your business with its employees, partners, and suppliers and—most importantly—your customers.	
Service Customers / Users	Any participating Commonwealth agency or office.	
Service Prerequisites	1) None	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSM13370119-A	Microsoft Dynamics CRM Online	Per User monthly subscription

Service Attribute	*Service Attribute Description*	
Service Name	Microsoft Azure Compute Server VM – 1 Core, 1.75 GB RAM, 2x1TB Disk Storage	
Detailed Description	Microsoft Azure Compute Server VM – 1 Core, 1.75 GB RAM, 2x1TB Disk Storage	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	What is required before this service or service element be ordered? 1) Selection of another service (what service?) 2) Solution Request submittal 3) Etc.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSM13370120-A	Compute Server VM - 1 Core-1.75GB RAM-2x1TB Disk Storage Non-Windows OS 1	Per Server Instance / 100 Hours
CCSM13370121-A	Compute Server VM - 1 Core-1.75GB RAM-2x1TB Disk Storage Windows OS 1	Per Server Instance / 100 Hours

Service Attribute	*Service Attribute Description*	
Service Name	Microsoft Azure Compute Server VM – 4 Core, 28 GB RAM, 8x1TB Disk Storage	
Detailed Description	Microsoft Azure Compute Server VM – 4 Core, 28 GB RAM, 8x1TB Disk Storage	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1) None	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSM13370122-A	Hi Compute Server VM - 4 Core-28 GB RAM-8x1TB Disk Storage Non-Windows OS 1	Per Server Instance / 100 Hours
CCSM13370123-A	Hi Compute Server VM - 4 Core-28 GB RAM-8x1TB Disk Storage Windows OS 1	Per Server Instance / 100 Hours

Service Attribute	*Service Attribute Description*	
Service Name	Microsoft Azure Compute Server VM – 8 Core, 56 GB RAM, 16x1TB Disk Storage	
Detailed Description	Microsoft Azure Compute Server VM – 8 Core, 56 GB RAM, 16x1TB Disk Storage	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1) None	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSM13370124-A	Hi Mem Compute Server VM - 8 Core-56 GB RAM-16x1TB Disk Storage Non-Windows OS 1	Per Server Instance / 100 Hours
CCSM13370125-A	Hi Mem Compute Server VM - 8 Core-56 GB RAM-16x1TB Disk Storage Windows OS 1	Per Server Instance / 100 Hours

Service Attribute	*Service Attribute Description*	
Service Name	Microsoft Azure Compute Server VM – 4 Core, 28 GB RAM, - Cloud Services	
Detailed Description	Microsoft Azure Compute Server VM – 4 Core, 28 GB RAM, - Cloud Services	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	None	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSM13370126-A	Hi Mem Compute Server VM - 4 Core-28 GB RAM – Cloud Services	Per Server Instance

Service Attribute	*Service Attribute Description*	
Service Name	Microsoft Azure Compute Server VM – 8 Core, 56 GB RAM, - Cloud Services	
Detailed Description	Microsoft Azure Compute Server VM – 8 Core, 56 GB RAM, - Cloud Services	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites		
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSM13370127-A	Hi Mem Compute Server VM - 8 Core-56 GB RAM – Cloud Services	Per Server Instance

Service Attribute	*Service Attribute Description*	
Service Name	Microsoft Azure Storage Geo Redundancy	
Detailed Description		
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	Microsoft Azure Compute Servers	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSM13370128-A	Microsoft Azure Storage Geo Redundancy – 100GB	Per 100 GB

Service Attribute	*Service Attribute Description*	
Service Name	Microsoft Azure Storage Local Redundancy – 100GB	
Detailed Description		
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	Microsoft Azure Compute Servers	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSM13370129-A	Microsoft Azure Storage Local Redundancy – 100GB	Per 100 GB

Service Attribute	*Service Attribute Description*	
Service Name	Microsoft Azure Backup Service	
Detailed Description		
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	Microsoft Azure Compute Servers	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSM13370130-A	Microsoft Azure Backup Service – 10 GB	Per 10 GB

Microsoft Cloud Management Services

Service Attribute	*Service Attribute Description*	
Service Name	Office 365 Migration Service	
Detailed Description	This service provides On-Premise messaging systems to MS Office 365 online service migration support. The migration project team is consisted of project manager, Exchange Architect, Engineer, System Administrator and Technical Writer.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	What is required before this service or service element be ordered? 1) Microsoft Office 365 – Government Cloud services 2) Office 365 Migration Tool	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSM13370131-A	Office 365 migration service	Per Month per Migration

Service Attribute	*Service Attribute Description*	
Service Name	Office 365 Migration Tool	
Detailed Description	Dell Exchange Migration Wizard provides inter-org migration support from the existing on-premise Exchange servers to the MS Office 365 online email systems. With the tool, it allows migration task to be performed in efficiently and quickly manner. It helps to reduce end user impact, project risk and total migration cost.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	What is required before this service or service element be ordered? • Office 365 –Government Cloud service • Office 365 –Government Cloud Migration service • Office 365 –Government Cloud Management service	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**

CCSM13370132-A	Office 365 Migration Tool	Per User

Service Attribute	*Service Attribute Description*	
Service Name	Office 365 Management Service	
Detailed Description	Unisys Messaging and Collaboration System Administers provide level 2.5-3 administer support for MS Office 365 Online services. To provide service coordination and user related Office 365 service support.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	What is required before this service or service element be ordered? • Microsoft Office 365 – Government Cloud Management Services • Office 365 –Government Cloud Migration tool service • Office 365 –Government Cloud Migration service	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSM13370133-A	Office 365 Management Service	Per Month / Up to 20,000 users

Service Attribute	*Service Attribute Description*	
Service Name	Microsoft SharePoint Online Migration	
Detailed Description	This service provides On Premise SharePoint systems to MS Online service migration support. The migration project team is consisted of project manager, SharePoint Architect, Engineer, System Administrator and Technical Writer.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	What is required before this service or service element be ordered? 1) Microsoft SharePoint Online – Government services 2) Microsoft SharePoint Online – Government Management services	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSM13370134-A	Microsoft SharePoint Online Migration	Per Month per Migration

Service Attribute	*Service Attribute Description*	
Service Name	Microsoft SharePoint Online Management Service	
Detailed Description	Unisys SharePoint System Administers provides level 2.5-3 administer support for MS Online services. To provide service coordination, user related SharePoint support.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	What is required before this service or service element be ordered? 1) Microsoft SharePoint Online – Government Cloud migration services	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSM13370135-A	Microsoft SharePoint Online Management Service	Per Month / Up to 20,000 users

VMWare vCloud Hybrid Cloud Compute Services

Service Attribute	*Service Attribute Description*	
Service Name	VMWare vCloud Hybrid Service – Dedicated Cloud Base Service	
Detailed Description	VMware vCloud® Hybrid Service™ is a secure, dedicated or multi-tenant solution operated by VMware, built on the trusted foundation of vSphere®. vCloud Hybrid Service is packaged as pools of resources that can be allocated by a customer to discrete VMs as needed, rather than as individual instances. **Dedicated Cloud:** Base Compute unit of 120 GB VRAM and 30 GHz vCPU Base Storage unit of 6 TB of single-tier block storage Base Bandwidth unit of 50 Mbps Base Public IP allocation of 3 public IP addresses	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	Requires a minimum of 1 year commitment.	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSV13370136-A	VMWare vCloud Hybrid Service – Dedicated Cloud – Base Service	What are the Orderable Units and related restrictions (per set of hours, tasks, etc.)?

Service Attribute	*Service Attribute Description*	
Service Name	VMWare vCloud Hybrid Service – Dedicated Cloud – Add On Compute Service	
Detailed Description	VMware vCloud® Hybrid Service™ is a secure, dedicated or multi-tenant solution operated by VMware, built on the trusted foundation of vSphere®. vCloud Hybrid Service is packaged as pools of resources that can be allocated by a customer to discrete VMs as needed, rather than as individual instances. The add-on services for Dedicated Cloud for an additional capacity based upon the follow items Compute unit of 120 GB VRAM and 30 GHz vCPU	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1) Add-On Service requires an initial order of the Base Dedicated Cloud service 2) For each Compute Add-On, a Support Add-On is required 3) Requires a minimum of 1 year commitment	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSV13370136-A	VMWare vCloud Hybrid Service - Dedicated Cloud -	Per Month / 1 Additional Unit

	Compute add-on (1 additional)	
CCSV13370137-A	VMWare vCloud Hybrid Service - Dedicated Cloud - Compute add-on (2-3 additional)	Per Month / 2-3 Additional Units
CCSV13370138-A	VMWare vCloud Hybrid Service - Dedicated Cloud - Compute add-on (4-5 additional)	Per Month / 4-5 Additional Units
CCSV13370139-A	VMWare vCloud Hybrid Service - Dedicated Cloud - Compute add-on (6-7 additional)	Per Month / 6-7 Additional Units
CCSV13370140-A	VMWare vCloud Hybrid Service - Dedicated Cloud - Compute add-on (8+ additional)	Per Month / 8+ Additional Units

Service Attribute	Service Attribute Description
Service Name	VMWare vCloud Hybrid Service – Dedicated Cloud – Add On Support Service
Detailed Description	VMware vCloud® Hybrid Service™ is a secure, dedicated or multi-tenant solution operated by VMware, built on the trusted foundation of vSphere®. vCloud Hybrid Service is packaged as pools of resources that can be allocated by a customer to discrete VMs as needed, rather than as individual instances. The add-on services for Dedicated Cloud for an additional capacity based upon the follow items Support for Compute unit of 120 GB VRAM and 30 GHz vCPU
Service Customers / Users	Any participating Commonwealth agency or office
Service Prerequisites	1) Add-On Service requires an initial order of the Base Dedicated Cloud service 2) For each Support Add-On, a Compute Add-On is required 3) Requires a minimum of 1 year commitment for the Base Dedicated Cloud
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog

Provider Part Number(s)	Service Option Name	Orderable Unit / Restrictions per Unit
CCSV13370138-A	VMWare vCloud Hybrid Service - Dedicated Cloud -	Per Month / 1 Additional Unit

	Support add-on (1 additional)	
CCSV13370140-A	VMWare vCloud Hybrid Service - Dedicated Cloud - Support add-on (2-3 additional)	Per Month / 2-3 Additional Units
CCSV13370141-A	VMWare vCloud Hybrid Service - Dedicated Cloud - Support add-on (4-5 additional)	Per Month / 4-5 Additional Units
CCSV13370138-A	VMWare vCloud Hybrid Service - Dedicated Cloud - Support add-on (6-7 additional)	Per Month / 6-7 Additional Units
CCSV13370140-A	VMWare vCloud Hybrid Service - Dedicated Cloud - Support add-on (8+ additional)	Per Month / 8+ Additional Units

Service Attribute	Service Attribute Description
Service Name	VMWare vCloud Hybrid Service – Dedicated Cloud – Add On Storage Service
Detailed Description	VMware vCloud® Hybrid Service™ is a secure, dedicated or multi-tenant solution operated by VMware, built on the trusted foundation of vSphere®. vCloud Hybrid Service is packaged as pools of resources that can be allocated by a customer to discrete VMs as needed, rather than as individual instances. The add-on services for Dedicated Cloud for an additional capacity based upon the follow items Storage unit of 6 TB of single-tier block storage
Service Customers / Users	Any participating Commonwealth agency or office
Service Prerequisites	1) Add-On Service requires an initial order of the Base Dedicated Cloud service. 2) Requires a minimum of 1 year commitment for the Base Dedicated Cloud.
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog

Provider Part Number(s)	Service Option Name	Orderable Unit / Restrictions per Unit
CCSV13370147-A	VMWare vCloud Hybrid Service - Dedicated Cloud - Storage add-on (1 additional)	Per Month / 1 Additional Unit

CCSV13370148-A	VMWare vCloud Hybrid Service - Dedicated Cloud - Storage add-on (2-3 additional)	Per Month / 2-3 Additional Units
CCSV13370149-A	VMWare vCloud Hybrid Service - Dedicated Cloud - Storage add-on (4-5 additional)	Per Month / 4-5 Additional Units
CCSV13370150-A	VMWare vCloud Hybrid Service - Dedicated Cloud - Storage add-on (6+ additional)	Per Month / 6+ Additional Units

Service Attribute	Service Attribute Description
Service Name	VMWare vCloud Hybrid Service – Dedicated Cloud – Add On Bandwidth Service
Detailed Description	VMware vCloud® Hybrid Service™ is a secure, dedicated or multi-tenant solution operated by VMware, built on the trusted foundation of vSphere®. vCloud Hybrid Service is packaged as pools of resources that can be allocated by a customer to discrete VMs as needed, rather than as individual instances. The add-on services for Dedicated Cloud for an additional capacity based upon the follow items Bandwidth unit of 50 Mbps
Service Customers / Users	Any participating Commonwealth agency or office
Service Prerequisites	1) Add-On Service requires an initial order of the Base Dedicated Cloud service. 2) Requires a minimum of 1 year commitment for the Base Dedicated Cloud.
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog

Provider Part Number(s)	Service Option Name	Orderable Unit / Restrictions per Unit
CCSV13370151-A	VMWare vCloud Hybrid Service - Dedicated Cloud - Bandwidth add-on (1+ additional)	Per Month / 1+ Additional Unit

Service Attribute	Service Attribute Description
Service Name	VMWare vCloud Hybrid Service – Dedicated Cloud – Add On Public IP Service
Detailed Description	VMware vCloud® Hybrid Service™ is a secure, dedicated or multi-tenant solution operated by VMware, built on the trusted foundation of vSphere®. vCloud Hybrid Service is packaged as pools of resources that can be allocated by a customer to discrete VMs as needed, rather than as individual instances. The add-on services for Dedicated Cloud for an additional capacity based upon the follow items Public IP allocation of 3 public IP addresses
Service Customers / Users	Any participating Commonwealth agency or office
Service Prerequisites	1) Add-On Service requires an initial order of the Base Dedicated Cloud service. 2) Requires a minimum of 1 year commitment for the Base Dedicated Cloud.
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog

Provider Part Number(s)	Service Option Name	Orderable Unit / Restrictions per Unit
CCSV13370152-A	VMWare vCloud Hybrid Service - Dedicated Cloud - Public IP add-on (1+ additional)	Per Month / 1+ Additional Unit

Service Attribute	Service Attribute Description	
Service Name	VMWare vCloud Hybrid Service – Virtual Cloud Base Service	
Detailed Description	VMware vCloud® Hybrid Service™ is a secure, Virtual or multi-tenant solution operated by VMware, built on the trusted foundation of vSphere®. vCloud Hybrid Service is packaged as pools of resources that can be allocated by a customer to discrete VMs as needed, rather than as individual instances. **Virtual Cloud:** Base Compute unit of 20 GB VRAM and 5 GHz vCPU (burst up to 10 GHz) Base Storage unit of 2 TB of single-tier block storage Base Bandwidth unit of 10 Mbps Base Public IP allocation of 2 public IP addresses	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	Requires a minimum of a 3 month commitment.	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSV13370153-A	VMWare vCloud Hybrid Service – Virtual Cloud – Base Service	What are the Orderable Units and related restrictions (per set of hours, tasks, etc.)?

Service Attribute	Service Attribute Description	
Service Name	VMWare vCloud Hybrid Service – Virtual Cloud – Add On Compute Service	
Detailed Description	VMware vCloud® Hybrid Service™ is a secure, Virtual or multi-tenant solution operated by VMware, built on the trusted foundation of vSphere®. vCloud Hybrid Service is packaged as pools of resources that can be allocated by a customer to discrete VMs as needed, rather than as individual instances. The add-on services for Virtual Cloud for additional capacity based upon the follow items Compute unit of 20 GB VRAM and 5 GHz vCPU (burst up to 10 GHz)	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1) Add-On Service requires an initial order of the Base Virtual Cloud service 2) For each Compute Add-On, a Support Add-On is required 3) Requires a minimum of a 3 month commitment for	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSV13370154-A	VMWare vCloud Hybrid	Per Month / 1-5 Additional

	Service – Virtual Cloud - Compute add-on (1-5 additional)	Units
CCSV13370155-A	VMWare vCloud Hybrid Service – Virtual Cloud - Compute add-on (6-11 additional)	Per Month / 6-11 Additional Units
CCSV13370156-A	VMWare vCloud Hybrid Service – Virtual Cloud - Compute add-on (12-17 additional)	Per Month / 12-17 Additional Units
CCSV13370157-A	VMWare vCloud Hybrid Service – Virtual Cloud - Compute add-on (18-23 additional)	Per Month / 18-23 Additional Units
CCSV13370158-A	VMWare vCloud Hybrid Service – Virtual Cloud - Compute add-on (24+ additional)	Per Month / 24+ Additional Units

Service Attribute	Service Attribute Description
Service Name	VMWare vCloud Hybrid Service – Virtual Cloud – Add On Support Service
Detailed Description	VMware vCloud® Hybrid Service™ is a secure, Virtual or multi-tenant solution operated by VMware, built on the trusted foundation of vSphere®. vCloud Hybrid Service is packaged as pools of resources that can be allocated by a customer to discrete VMs as needed, rather than as individual instances. The add-on services for Virtual Cloud for an additional capacity based upon the follow items Support for Compute unit of 20 GB VRAM and 5 GHz vCPU (burst up to 10 GHz)
Service Customers / Users	Any participating Commonwealth agency or office
Service Prerequisites	1) Add-On Service requires an initial order of the Base Virtual Cloud service 2) For each Support Add-On, a Compute Add-On is required 3) Requires a minimum of 1 year commitment for the Base Virtual Cloud
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog

Provider Part Number(s)	Service Option Name	Orderable Unit / Restrictions per Unit
CCSV13370159-A	VMWare vCloud Hybrid Service – Virtual Cloud -	Per Month / 1-5 Additional

	Support add-on (1-5 additional)	Units
CCSV13370160-A	VMWare vCloud Hybrid Service – Virtual Cloud - Support add-on (6-11 additional)	Per Month / 6-11 Additional Units
CCSV13370161-A	VMWare vCloud Hybrid Service – Virtual Cloud - Support add-on (12-17 additional)	Per Month / 12-17 Additional Units
CCSV13370162-A	VMWare vCloud Hybrid Service – Virtual Cloud - Support add-on (18-23 additional)	Per Month / 18-23 Additional Units
CCSV13370163-A	VMWare vCloud Hybrid Service – Virtual Cloud - Support add-on (24+ additional)	Per Month / 24+ Additional Units

Service Attribute	Service Attribute Description
Service Name	VMWare vCloud Hybrid Service – Virtual Cloud – Add On Storage Service
Detailed Description	VMware vCloud® Hybrid Service™ is a secure, Virtual or multi-tenant solution operated by VMware, built on the trusted foundation of vSphere®. vCloud Hybrid Service is packaged as pools of resources that can be allocated by a customer to discrete VMs as needed, rather than as individual instances. The add-on services for Virtual Cloud for an additional capacity based upon the follow items Storage unit of 6 TB of single-tier block storage
Service Customers / Users	Any participating Commonwealth agency or office
Service Prerequisites	1) Add-On Service requires an initial order of the Base Virtual Cloud service. 2) Requires a minimum of 1 year commitment for the Base Virtual Cloud.
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog

Provider Part Number(s)	Service Option Name	Orderable Unit / Restrictions per Unit
CCSV13370164-A	VMWare vCloud Hybrid Service – Virtual Cloud - Storage add-on (1-5 additional)	Per Month / 1-5 Additional Unit

CCSV13370165-A	VMWare vCloud Hybrid Service – Virtual Cloud - Storage add-on (6-11 additional)	Per Month / 6-11 Additional Units
CCSV13370166-A	VMWare vCloud Hybrid Service – Virtual Cloud - Storage add-on (12-17 additional)	Per Month / 12-17 Additional Units
CCSV13370167-A	VMWare vCloud Hybrid Service – Virtual Cloud - Storage add-on (18+ additional)	Per Month / 18+ Additional Units

Service Attribute	Service Attribute Description
Service Name	VMWare vCloud Hybrid Service – Virtual Cloud – Add On Bandwidth Service
Detailed Description	VMware vCloud® Hybrid Service™ is a secure, Virtual or multi-tenant solution operated by VMware, built on the trusted foundation of vSphere®. vCloud Hybrid Service is packaged as pools of resources that can be allocated by a customer to discrete VMs as needed, rather than as individual instances. The add-on services for Virtual Cloud for an additional capacity based upon the follow items Bandwidth unit of 10 Mbps
Service Customers / Users	Any participating Commonwealth agency or office
Service Prerequisites	1) Add-On Service requires an initial order of the Base Virtual Cloud service. 2) Requires a minimum of 1 year commitment for the Base Virtual Cloud.
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog

Provider Part Number(s)	Service Option Name	Orderable Unit / Restrictions per Unit
CCSV13370168-A	VMWare vCloud Hybrid Service – Virtual Cloud - Bandwidth add-on (1+ additional)	Per Month / 1+ Additional Unit

Service Attribute	Service Attribute Description
Service Name	VMWare vCloud Hybrid Service – Virtual Cloud – Add On Public IP Service
Detailed Description	VMware vCloud® Hybrid Service™ is a secure, Virtual or multi-tenant solution operated by VMware, built on the trusted foundation of vSphere®. vCloud Hybrid Service is packaged as pools of resources that can be allocated by a customer to discrete VMs as needed, rather than as individual instances. The add-on services for Virtual Cloud for an additional capacity based upon the follow items Public IP allocation of 2 public IP addresses
Service Customers / Users	Any participating Commonwealth agency or office
Service Prerequisites	1) Add-On Service requires an initial order of the Base Virtual Cloud service. 2) Requires a minimum of 1 year commitment for the Base Virtual Cloud.
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog

Provider Part Number(s)	Service Option Name	Orderable Unit / Restrictions per Unit
CCSV13370169-A	VMWare vCloud Hybrid Service – Virtual Cloud - Public IP add-on (1+ additional)	Per Month / 1+ Additional Unit

Identity and Access Management Services

Service Attribute	*Service Attribute Description*	
Service Name	Active Directory Support	
Detailed Description	Provide support to administer Commonwealth Active Directory Forests and Domains. Support activities provided include: • Limited User, computer and group management. Where applicable these will be delegated for agency control and management. • Networked service management (print shares, DFS, application partition management) • Limited Group policy management. Where applicable these will be delegated for agency control and management. • DNS management • Topology and Replication management • Information management and security administration (password policies etc.) • AD Reporting • Level 2 for End user support	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites		
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part	**Service Option Name**	**Orderable Unit / Restrictions**

Number(s)		per Unit
CCSU13370170-A	Active Directory Support – Small	Per Forest / One Forest, Up to 2 Domains, up to 5 domain controllers, Up to 1,000 AD Objects, and Up to 2 sites
CCSU13370171-A	Active Directory Support – Medium	Per Forest / One Forest, Up to 3 Domains, up to 20 domain controllers, Up to 5,000 AD Objects, and Up to 3 sites
CCSU13370172-A	Active Directory Support – Large	Per Forest / One Forest, Up to 5 Domains, Up to 200 domain controllers, Up to 100,000 AD Objects, and Up to 5 sites
CCSU13370173-A	Active Directory Support – Very Large	Per Forest / One Forest, Up to 10 Domains, up to 500 domain controllers, up to 500,000 AD Objects, and Up to 10 sites

Service Attribute	*Service Attribute Description*	
Service Name	PKI Support	
Detailed Description	Provide support to administer Commonwealth PKI Certificate Authorities (CA). Support activities provided include: • Implementation and configuration • Certificate issuance and management • Template creation and Management • Level 2 for End user support	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites		
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370174-A	PKI Support – Small	Per PKI environment / 1 Issuing CA, up to 1000 certificates, and up to 2 templates
CCSU13370175-A	PKI Support – Medium	Per PKI environment / 2 Issuing CA, up to 10000 certificates, and up to 5 templates

CCSU13370176-A	PKI Support – Large	Per PKI environment / 3 Issuing CA, up to 10000 certificates, and up to 10 templates

Business Continuity and Disaster Recovery

Business Continuity - Planning Services

Service Attribute	*Service Attribute Description*	
Service Name	Development of a Data Center Disaster Recovery Plan	
Detailed Description	The objectives of this project are to begin the development the Data Center Disaster Recovery (DR) Plan. This Plan will document the steps needed to relocate to an alternate site and begin recovery the IT environment in the defined timeframe. A Plan Owner should be identified at the very start of this activity, who will then assume responsibility for the Plan as soon as it is completed enabling IBM to focus on skills transfer during the execution of this Statement of Work	
Service Customers / Users	Any participating Commonwealth agency or office.	
Service Prerequisites	None	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370177-A	Development of a Data Center Disaster Recovery Plan	Per Plan

Service Attribute	Service Attribute Description
Service Name	Business Impact Assessment Workshop
Detailed Description	IBM will provide Business Continuity and Resilience Services in the form of a Business Impact Analysis Workshop to assist Commonwealth of Pennsylvania in developing and documenting the Business requirements for disaster recovery. IBM working in conjunction with Commonwealth of Pennsylvania will define Recovery Time and Recovery Point objectives for critical business functions. The output of this Statement of Work provides the base business requirements for developing a Disaster Recovery Strategy and Disaster Recovery Plan.
Service Customers / Users	Any participating Commonwealth agency or office
Service Prerequisites	None
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.

Provider Part Number(s)	Service Option Name	Orderable Unit / Restrictions per Unit
CCSI13370178-A	Business Impact Assessment Workshop	Per Workshop

Service Attribute	*Service Attribute Description*	
Service Name	Resilient Strategy Development Workshop	
Detailed Description	The objectives of this project are to identify gaps, industry best practices and make recommendations for Commonwealth of Pennsylvania's Resilient Strategy Design for a disaster scenario resulting in the loss of physical data center and/or servers within the defined Recovery Time and Point Objectives for in-scope servers and data. IBM will develop up to one (1) Resilient Strategy Design based on a mutually agreed Data Center facility.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	None	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370179-A	Resilient Strategy Development Workshop	Per Workshop

Disaster Recovery - Testing

Service Attribute	*Service Attribute Description*	
Service Name	Labor for DR Tier 3 to Tier 6 DR Testing	
Detailed Description	The service provides the labor to complete an annual DR test for an application or portion of an application that has selected the disk-based restore provided as part of the Tier 3 through Tier 6 DR Services. The RFP stipulates 2 tests per year therefore 2 of these must be purchased for each application group.	
Service Customers / Users	The Service is Available to Any participating Commonwealth agency or office.	
Service Prerequisites	What is required before this service or service element be ordered? 1) The Unisys-managed data center has been provisioned with sufficient resources to complete a DR test at a site separate from Production. 2) The Unisys-managed Production Data Center holds the Fully –Managed assets that require the specified DR services. 3) The storage replication services have been provisioned and the Production and DR storage have been managed by Unisys for 30 days.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370180-A	Labor for DR Tier 3 to Tier 6 DR Testing	Per Server

Service Attribute	*Service Attribute Description*	
Service Name	Labor for Tier 1 & Tier 2 DR Service Testing (Tape-based)	
Detailed Description	The service provides the labor to complete an annual DR test for an application or portion of an application that has selected the disk-based restore provided as part of the Tier 1 and Tier 2 DR Services. The RFP stipulates 2 tests per year therefore 2 of these must be purchased for each application group.	
Service Customers / Users	The Service is Available to Any participating Commonwealth agency or office.	
Service Prerequisites	What is required before this service or service element be ordered? 1) The Unisys-managed data center has been provisioned with sufficient resources to complete a DR test at a site separate from Production. 2) The Unisys-managed Production Data Center holds the Fully –Managed assets that require the specified DR services. 3) The backup to tape services in the Production Data Center has been managed by Unisys for 30 days.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370181-A	Labor for Tier 1 & Tier 2 DR Service Testing (Tape-based)	Per Server

Disaster Recovery – Storage and Backup

Service Attribute	*Service Attribute Description*	
Service Name	DR Config-1 Storage	
Detailed Description	The Storage matches the Config-1 Storage described for Production in the Schedule I, Volumetrics	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	What is required before this service or service element be ordered? 1) Selection of sufficient Data Center Facilities Services 2) Solution Request submittal	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370182-A	DR Config-1 Storage	Per GB

Service Attribute	*Service Attribute Description*	
Service Name	DR Config-2 Storage	
Detailed Description	The Storage matches the Config-2 Storage described for Production in the Schedule I, Volumetrics	
Service Customers / Users	The service is available to Any participating Commonwealth agency or office	
Service Prerequisites	What is required before this service or service element be ordered? 1) Selection of sufficient Data Center Facilities Services 2) Solution Request submittal	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
DR Config-2 Storage	DR Config-2 Storage	Per GB

Service Attribute	*Service Attribute Description*	
Service Name	DR Tape Library Resources for Tier1 DR RTO based on 100,000 GB	
Detailed Description	The Tier1 DR Services delivers to an RTO of 72 hrs using restoral of data from tape. This service provides the DR Tape Library capacity to meet that requirement during DR tests and in the unlikely event of an actual DR.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	What is required before this service or service element be ordered? 1) The Unisys-managed data center has been provisioned with sufficient resources to complete a DR test at a site separate from Production. 2) The Unisys-managed Production Data Center holds the Fully –Managed assets that require the specified DR services. 3) The storage replication services have been provisioned and the Production and DR storage have been managed by Unisys for 30 days.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370184-A	DR Tape Library Resources for Tier1 DR RTO based on 100,000 GB	Per GB of Protected Data

Service Attribute	*Service Attribute Description*	
Service Name	DR Tape Library Resources for Tier2 DR RTO based on 100,000 GB	
Detailed Description	The Tier2 DR Services delivers to an RTO of 48 hrs using restoral of data from tape. This service provides the DR Tape Library capacity to meet that requirement during DR tests and in the unlikely event of an actual DR. A greater number of tape drives are needed to process data restores in a shorter period of time.	
Service Customers / Users	The Service is Available to Any participating Commonwealth agency or office.	
Service Prerequisites	What is required before this service or service element be ordered? 1) The Unisys-managed data center has been provisioned with sufficient resources to complete a DR test at a site separate from Production. 2) The Unisys-managed Production Data Center holds the Fully –Managed assets that require the specified DR services. 3) The storage replication services have been provisioned and the Production and DR storage have been managed by Unisys for 30 days.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370185-A	DR Tape Library Resources for Tier2 DR RTO based on 100,000 GB	Per GB of Protected Data

Service Attribute	*Service Attribute Description*	
Service Name	Backup to Disk for 255,000 GBs of de-duplicated data	
Detailed Description	The Service provides hardware to allow backups to be written to an EMC Data Domain storage device. The storage written to the device is de-duplicated in order to provide the maximum use of the physical drives in the platform.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	What is required before this service or service element be ordered? 1) The service is available as a component of backup and/or disaster recovery service to servers that are Fully-Managed by Unisys. 2) The Commonwealth servers that use the service must be managed by the Unisys-managed backup infrastructure. 3) The Service can provide a primary target in Production for backups as well as a complementing DR instance so that Production backups are replicated to DR but in this case the Commonwealth must order each instance as well as sufficient network bandwidth for the replication.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370186-A	Backup to Disk for 255,000 GBs of de-duplicated data	Per GB of Protected Data

Service Attribute	*Service Attribute Description*	
Service Name	Mainframe Services: EMC RecoverPoint Data Replication for 27,000 GBs of VMAX10K Storage.	
Detailed Description	If the Commonwealth elects to provision the Unisys Mainframe with VMAX10K storage then it can use this means of replicating data from the Production location to the DR location.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	What is required before this service or service element be ordered? 1) The Commonwealth must provision the Unisys Mainframe with EMC's VMAX10K storage. 2) The Commonwealth must provision sufficient VMAX10K storage at the DR location to receive the data replicated from the Production VMAX10K	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370187-A	Mainframe Services: EMC RecoverPoint Data Replication for 27,000 GBs of VMAX10K Storage.	Per GB of Replicated Data

Service Attribute	*Service Attribute Description*	
Service Name	EMC RecoverPoint SnapShot & Replication for 32,256 GBs of Config2 Storage	
Detailed Description	The storage service adds snapshot and replication services for Config2 storage.	
Service Customers / Users	The Service is Available to Any participating Commonwealth agency or office.	
Service Prerequisites	What is required before this service or service element be ordered? 1) In the case of Snapshots only, the selection of sufficient Production Config2 Production storage allocated to a server as well as the selection of sufficient set-aside space for the accumulation of snapshots. 2) In the case of Snapshots and replication, the selection of sufficient Production Config2 storage and sufficient storage at the target location as well as the selection of sufficient set-aside space for the accumulation of snapshots at Production and, if desired, at the target location	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370188-A	EMC RecoverPoint SnapShot & Replication for 32,256 GBs of Config2 Storage	Per GB of Protected Data

Service Attribute	*Service Attribute Description*	
Service Name	EMC RecoverPoint SnapShot & Replication for 84,700 GBs of Config1 Storage	
Detailed Description	The storage service adds snapshot and replication services for Config1 storage.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	What is required before this service or service element be ordered? 1) In the case of Snapshots only, the selection of sufficient Production Config1 Production storage allocated to a server as well as the selection of sufficient set-aside space for the accumulation of snapshots. 2) In the case of Snapshots and replication, the selection of sufficient Production Config1 storage and sufficient storage at the target location as well as the selection of sufficient set-aside space for the accumulation of snapshots at Production and, if desired, at the target location	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370189-A	EMC RecoverPoint SnapShot & Replication for 84,700 GBs of Config1 Storage	Per GB of Replicated Data

Service Attribute	*Service Attribute Description*	
Service Name	Mainframe Services: EMC SRDF Data Replication for 50,000 GB of VMAX Storage	
Detailed Description	If the Commonwealth elects to provision the Unisys Mainframe with VMAX10K storage then it can use this means of replicating data from the Production location to the DR location.	
Service Customers / Users	The Service is Available to Any participating Commonwealth agency or office.	
Service Prerequisites	What is required before this service or service element be ordered? 1) The Commonwealth must provision the Unisys Mainframe with EMC's VMAX10K storage. 2) The Commonwealth must provision sufficient VMAX10K storage at the DR location to receive the data replicated from the Production VMAX10K	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370190-A	Mainframe Services: EMC SRDF Data Replication for 50,000 GB of VMAX Storage	Per GB of Replicated Data

Service Attribute	*Service Attribute Description*	
Service Name	Open Systems Services: EMC VPLEX Metro Replication for 140,000 GBs	
Detailed Description	This service provides a means of replicating data over limited distances in support of DR Tier5 & Tier6 DR Services.	
Service Customers / Users	The Service is Available to Any participating Commonwealth agency or office.	
Service Prerequisites	What is required before this service or service element be ordered? 1) The service requires both source and target servers and storage to be provisioned. 2) The service requires an initial feasibility review to analyze expected response times. 3) The network bandwidth required to support the needed data replication is provisioned separately.	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370192-A	Open Systems Services: EMC VPLEX Metro Replication for 140,000 GBs	Per GB of Replicated Data

Service Attribute	*Service Attribute Description*	
Service Name	SAN Switch Port, purchased in pairs, for SAN-attached Servers	
Detailed Description	This service is used to provide servers with access to Unisys-managed SAN storage infrastructure	
Service Customers / Users	The Service is Available to Any participating Commonwealth agency or office.	
Service Prerequisites	What is required before this service or service element be ordered? 1) The service is available to Fully-managed servers only.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370193-A	SAN Switch Port, purchased in pairs, for SAN-attached Servers	Per Server

Service Attribute	*Service Attribute Description*	
Service Name	IBM Storwize V7000 Disaster Recovery System	
Detailed Description	This solution includes one storage subsystem which provides 118 TB via Raid 10/5 of useable space. This includes • IBM Storwize V7000 (Model 2076-124) • 177 – 900 GB 10k SAS disk • 15 – 300 GB 15k SAS disk • 8 – Fiber Optic Cable LC-LC • Two PDU power cords • Remote Mirroring license for 8 disk shelves • Includes four year hardware and software maintenance	
Service Customers / Users	Any participating Commonwealth agency or office.	
Service Prerequisites	Access to affected systems and/or facilities. Disaster Recovery service Does not include ongoing storage management support; hardware, software and maintenance services only.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370564-A	IBM Storwize V7000 Disaster Recovery System	Per System

Service Attribute	*Service Attribute Description*	
Service Name	IBM XIV High Performance Disaster Recovery Tier	
Detailed Description	This solution includes one storage subsystem which provides 190 TB of useable space. This includes: • IBM XIV Gen 3 (2812-214) • 12 Module System with SSD • Unix/Linux/VMWare/Windows Host Attachment • 24 – Fiber Channel Cables • Remote Mirroring license • Includes four year hardware and software maintenance	
Service Customers / Users	Any participating Commonwealth agency or office.	
Service Prerequisites	Access to affected systems and/or facilities. Disaster Recovery service Does not include ongoing storage management support; hardware, software and maintenance services only.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370565-A	IBM XIV High Performance Disaster Recovery Tier	Per System

Application Services

Application Performance Monitoring Services

Service Attribute	*Service Attribute Description*
Service Name	Application Performance Monitoring Setup Service
Detailed Description	This service will configure the following services for managing application performance and monitoring using the AppDynamics toolset in the production or test environment •□ Auto-discover and map application dependencies •□ Automatic code instrumentation •□ Self-learn application performance baselines •□ Auto-detect performance problems •□ Auto-detect and display transaction workflows •□ Auto-trigger diagnostic collection •□ Automation workflow for remediation •□ Custom executive dashboards “on the fly”
Orderable Unit	•□ Small Application (101- 250 IIS/JVM/PHP) •□ Medium Application (252 – 500 IIS/JVM/PHP) •□ Large Application (501- 1000 IIS/JVM/PHP)
Service Customers / Users	Any participating Commonwealth agency or office Application Owners
Service Prerequisites	What is required before this service or service element be ordered? 1)□Application must be supported on Unisys managed infrastructure
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services

	Catalog item using the above Service Name Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370194-A	Application Performance Monitoring Service - Setup – Small	Small Application (101- 250 IIS/JVM/PHP)
CCSU13370195-A	Application Performance Monitoring Service - Setup – Medium	Medium Application (251-500 IIS/JVM/PHP)
CCSU13370196-A	Application Performance Monitoring Service - Setup - Large	Large Application (501 – 1000 IIS/JVM/PHP)

Service Attribute	*Service Attribute Description*
Service Name	Application Performance Monitoring Ongoing Support Service
Detailed Description	This service will support the modification and ongoing execution of the following services for managing application performance and monitoring using the AppDynamics toolset •□ Auto-discover and map application dependencies •□ Automatic code instrumentation •□ Self-learn application performance baselines •□ Auto-detect performance problems •□ Auto-detect and display transaction workflows •□ Auto-trigger diagnostic collection •□ Automation workflow for remediation •□ Custom executive dashboards “on the fly”
Orderable Unit	•□ Small Application (101- 250 IIS/JVM/PHP) •□ Medium Application (252 – 500 IIS/JVM/PHP) •□ Large Application (501- 1000 IIS/JVM/PHP)
Service Customers / Users	*Any participating Commonwealth agency or office* Application Owners
Service Prerequisites	What is required before this service or service element be ordered? 1)□Application must be supported on Unisys managed infrastructure
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name Or To request this service, submit a Solution Request in the online

	Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370197-A	Application Performance Monitoring Service - Ongoing Support – Small	Small Application (101- 250 IIS/JVM/PHP)
CCSU13370198-A	Application Performance Monitoring Service - Ongoing Support – Medium	Medium Application (251-500 IIS/JVM/PHP)
CCSU13370199-A	Application Performance Monitoring Service - Ongoing Support - Large	Large Application (501 – 1000 IIS/JVM/PHP)

Application Capacity Management Services

Service Attribute	*Service Attribute Description*
Service Name	Application Capacity Management Setup Service
Detailed Description	This Service will provide capacity related analyses and recommendations using the capacity management, modeling and analytic capabilities of the BMC Capacity Optimization Toolset for a specific Commonwealth/Agency Application : • Forecast workload of each agency's application-based processor and memory usage using projected workload transaction and user volumes supplied by the Commonwealth. • Track application-based processor and memory usage and report the usage and trends to the Commonwealth. • Provide data storage capacity planning by estimating, measuring, and reporting on data storage used for supporting Commonwealth applications. • Utilize storage forecasts for each application provided by the Commonwealth to make periodic recommendations for upgrading or consolidating data storage capacity. • Support capacity planning for new application infrastructure focused on estimating, measuring, and reporting on network, server, and data storage usage over time for each application. • Capacity baselines will be established during testing of the application environment. Unisys will track application-based infrastructure usage. • Recommendations for upgrading existing infrastructure capacity.
Service Customers / Users	Any participating Commonwealth agency or office Application Owners
Service Prerequisites	What is required before this service or service element be ordered? Application must be supported on Unisys managed

	infrastructure	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370200-A	Application Capacity Management - Setup – Small	Per Application / up to 40 hours and up to 10 servers
CCSU13370201-A	Application Capacity Management - Setup – Medium	Per Application / up to 80 hours and up to 20 servers
CCSU13370202-A	Application Capacity Management – Setup - Large	Per Application / up to 120 hours and 21 – 30 servers

Service Attribute	*Service Attribute Description*
Service Name	Application Capacity Management Ongoing Maintenance Service
Detailed Description	This Service will provide ongoing support and capacity related analyses and recommendations using the capacity management, modeling and analytic capabilities of the BMC Capacity Optimization Toolset for a specific Commonwealth/Agency Application : • Forecast workload of each agency's application-based processor and memory usage using projected workload transaction and user volumes supplied by the Commonwealth. • Track application-based processor and memory usage and report the usage and trends to the Commonwealth. • Provide data storage capacity planning by estimating, measuring, and reporting on data storage used for supporting Commonwealth applications. • Utilize storage forecasts for each application provided by the Commonwealth to make periodic recommendations for upgrading or consolidating data storage capacity. • Support capacity planning for new application infrastructure focused on estimating, measuring, and reporting on network, server, and data storage usage over time for each application. • Capacity baselines will be established during testing of the application environment. Unisys will track application-based infrastructure usage. • Recommendations for upgrading existing infrastructure capacity. • Small Application (40 hours) (5 – 10 servers) • Medium Application (80 hours) (11- 20 servers) Large Application (120 hours) (21 – 30 servers)
Service Customers /	Any participating Commonwealth agency or office Application

Users	Owners	
Service Prerequisites	What is required before this service or service element be ordered? 1) Application must be supported on Unisys managed infrastructure 2) Application Capacity Management Setup Service for the specific Application is complete	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370203-A	Application Capacity Management - Ongoing Support – Small	Per Application / up to 40 hours and up to 10 servers
CCSU13370204-A	Application Capacity Management - Ongoing Support – Medium	Per Application / up to 80 hours and up to 20 servers
CCSU13370205-A	Application Capacity Management – Ongoing Support - Large	Per Application / up to 120 hours and 21 – 30 servers

Service Attribute	*Service Attribute Description*
Service Name	Application Capacity Management - Monitoring Tool License
Detailed Description	This Service will provide ongoing support and capacity related analyses and recommendations using the capacity management, modeling and analytic capabilities of the BMC Capacity Optimization Toolset for a specific Commonwealth/Agency Application : • Forecast workload of each agency's application-based processor and memory usage using projected workload transaction and user volumes supplied by the Commonwealth. • Track application-based processor and memory usage and report the usage and trends to the Commonwealth. • Provide data storage capacity planning by estimating, measuring, and reporting on data storage used for supporting Commonwealth applications. • Utilize storage forecasts for each application provided by the Commonwealth to make periodic recommendations for upgrading or consolidating data storage capacity. • Support capacity planning for new application infrastructure focused on estimating, measuring, and reporting on network, server, and data storage usage over time for each application. • Capacity baselines will be established during testing of the application environment. Unisys will track application-based infrastructure usage. • Recommendations for upgrading existing infrastructure capacity. • The tool license covers the server monitoring agent license. • Small Application (5 – 10 servers) • Medium Application (11- 20 servers) • Large Application (21 – 30 servers)

Service Customers / Users	Any participating Commonwealth agency or office Application Owners	
Service Prerequisites	What is required before this service or service element be ordered? 3) Application must be supported on Unisys managed infrastructure 4) Application Capacity Management Setup Service for the specific Application is complete	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370555-A	Application Capacity Management - Ongoing Support – Small	Per Application / Up to 10 servers
CCSU13370556-A	Application Capacity Management - Ongoing Support – Medium	Per Application / Up to 20 servers
CCSU13370557-A	Application Capacity Management – Ongoing Support - Large	Per Application / Up to 21 – 30 servers

Application Architecture Review

Service Attribute	*Service Attribute Description*	
Service Name	**Application Architecture Review**	
Detailed Description	Conduct in-depth review of application architecture, framework and design for robustness and extensibility that includes • Review Logical Architecture to gauge ability to fulfill application requirements. • Analyze Design and Coding Patterns for consistency, reusability and adaptability for desired business solution. • Review Component Design for explicit boundaries, loose coupling and standards conformance. • Analyze Application Integration and Cohesiveness to enable cross-module integration and reduce discrepancies	
Service Customers / Users	Business, technology or security managers of Any participating Commonwealth agency or office	
Service Prerequisites	• Approvals from the Commonwealth/Unisys PMO • Availability of supporting infrastructure and tools (software) solution to perform the assessment • Define assessment scope	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSD13370206-A	Application Architecture Review - Small	Per Assessment / Review 10 use cases, 5 class diagrams containing up to 10 classes each, 20 sequence diagrams, and architecture document not

		exceeding 100 pages
CCSD13370207-A	Application Architecture Review - Medium	Per Assessment /Review 30 use cases, 10 class diagrams containing up to 10 classes each, 40 sequence diagrams, and architecture document not exceeding 150 pages
CCSD13370208-A	Application Architecture Review – Large	Per Assessment / Review up to 50 use cases, 30 class diagrams containing up to 20 classes each, 60 sequence diagrams, and architecture document not exceeding 200 pages. Additionally, review complimentary product selection, integration pattern, scope of use (leveraging the investments), and product implementation architecture and design

Application Assessment Services

Service Attribute	*Service Attribute Description*	
Service Name	Application Performance Impact Assessment (follow-on for 5 applications)	
Detailed Description	Deep Dive Analysis is based on an average of five (5) individual user transactions or up to twenty five (25) total transactions; Application should be one of the applications work shopped or project change request would be followed to accommodate the additional application performance workshops.	
Service Customers / Users	Agencies who have participated in the APOC Assessment.	
Service Prerequisites	This is a follow-on effort to the APOC assessment. Can only be combined with this offering as a secondary output of that service.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370209-A	Application Performance Impact Assessment	Per Assessment

Service Attribute	*Service Attribute Description*	
Service Name	**Open System Database Performance Assessment**	
Detailed Description	The Open System Database Performance Assessment service provides agencies with a broad review and assessment of their current database operating solution. The assessment will include a broad spectrum of operational considerations such as: • Database Configuration Verification – An effort to analyze the database software was installed and configured in alignment with vendor leading practices • Infrastructure Topology Assessment – An effort to analyze the system topology configuration and capacity to identify performance tuning opportunities. • Historic Trending – An effort to review historic performance characteristics, business trends and usage patterns to help identify performance tuning opportunities. • SQL Query Analysis – Review of heavily exercised and/or complex queries that consume substantial system resources for performance tuning opportunities.	
Service Customers / Users	Business, technology or security managers of Any participating Commonwealth agency or office	
Service Prerequisites	• Approvals from the Commonwealth/Unisys PMO • Availability of supporting infrastructure and tools (software) solution to perform the assessment • Define assessment scope	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**

CCSD13370210-A	Open System Database Performance Assessment - Small	Per Assessment (up to 100 database object)
CCSD13370211-A	Open System Database Performance Assessment - Medium	Per Assessment (Up to 500 database objects)
CCSD13370212-A	Open System Database Performance Assessment - Large	Per Assessment (up to 1,000 database objects)

Service Attribute	*Service Attribute Description*
Service Name	**Open System Configuration Management Assessment**
Detailed Description	The Open System Configuration Management (CM) Assessment service provides agencies with a broad review and assessment of their current configuration management solution. The assessment will analyze a full spectrum of operational considerations such as: • CM Infrastructure Management Process Assessment – An effort to review processes and practices that support the instantiation of a new machine, alterations to existing machines and the deployment of new application code to the machine. • CM Tools / Operational Assessment – An effort to analyze the infrastructure, tools and processes used to perform configuration management, including source code management, build/deployment management, IT Service Request management. • CM Incident/Problem Management Assessment – An effort to review processes and practices to determine alignment with ITIL incidents/problems management leading practices. Once complete, the assessment results document will highlight potential improvement opportunities to streamline the configuration management process, reduce risk and increase efficiency and repeatability.
Service Customers / Users	Business, technology or security managers of any participating Commonwealth agency or office
Service Prerequisites	• Approvals from the Commonwealth/Unisys PMO • Availability of supporting infrastructure and tools (software) solution to perform the assessment • Define assessment scope
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.

Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSD13370213-A	Open System Configuration Management Assessment - Small	Per Assessment (single application)
CCSD13370214-A	Open System Configuration Management Assessment - Medium	Per Assessment (Multiple Application / Complex Architecture)
CCSD13370215-A	Open System Configuration Management Assessment - Large	Per Assessment (Enterprise Architecture)

Service Attribute	*Service Attribute Description*	
Service Name	**Mobile Wireframe Assessment**	
Detailed Description	The Mobile Wireframe Assessment service provides agencies with an assessment and review of mobile solution requirements to create a wireframe prototype. The assessment will analyze a full spectrum of operational considerations such as: Mobile Readiness Assessment – An assessment of current infrastructure, standards, policies, tools and software to determine readiness to support mobile development and production operations	
Service Customers / Users	Business, technology or security managers of Any participating Commonwealth agency or office	
Service Prerequisites	• Approvals from the Commonwealth/Unisys PMO • Availability of supporting infrastructure and tools (software) solution to perform the assessment • Define assessment scope	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSD13370216-A	Mobile Wireframe Assessment / - Small	Per Assessment (up to 10 pages)
CCSD13370217-A	Mobile Wireframe Assessment / - Medium	Per Assessment (up to 25 pages)
CCSD13370218-A	Mobile Wireframe Assessment / - Large	Per Assessment (up to 50 pages)

Service Attribute	*Service Attribute Description*	
Service Name	Application Management Innovation Workshop	
Detailed Description	Application Management Innovation Workshop helps the client identify opportunities on how social computing, cloud computing, big data, and mobile can be leveraged internally and externally within their environment and then prioritizes the opportunities based on key evaluation criteria.	
Service Customers / Users	Any participating Commonwealth agency or office.	
Service Prerequisites	1) None	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370219-A	Application Innovation Workshop	Per Workshop (one day)

Service Attribute	*Service Attribute Description*	
Service Name	Application Modernization Assessment	
Detailed Description	The Application Modernization Assessment assists clients in assessing how to best leverage disruptive trends like social computing, cloud computing, big data, and mobile to improve business operations and customer experience and is targeted towards organizations with complex environments and/or multiple areas of interest.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	What is required before this service or service element be ordered? 1) Selection of another service (what service?) 2) Solution Request submittal 3) Etc.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370220-A	Application Modernization Assessment – 1 Week	Per Assessment (One Week)
CCSU13370221-A	Application Modernization Assessment – 4 Weeks	Per Assessment (4 Weeks)

Application Testing Services

Service Attribute	*Service Attribute Description*	
Service Name	**Test Assessment**	
Detailed Description	Conduct an assessment of existing Testing and Quality Assurance procedures. Identify areas of improvement in the testing and Quality Assurance processes Summarize the findings and recommendations Conduct up to 4 discovery sessions, review existing test management and quality assurance process and artifacts Review and synthesize reviewed project artifacts, session notes, processes and prior project results to produce findings and options. Guide project team members in identifying potential issues encountered in everyday test scenario execution as well as options to address issues. Review testing and quality assurance options and support the program to implement next steps.	
Service Customers / Users	Business, technology or security managers of *Any participating Commonwealth agency or office*	
Service Prerequisites	Availability of supporting infrastructure and tools (software) solution to perform the assessment Define assessment scope	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**

CCSD13370222-A	Test Assessment	Per Assessment

Service Attribute	*Service Attribute Description*	
Service Name	**Test Estimation and Test Approach Planning**	
Detailed Description	Use of SEI and IEEE best practices for test estimation Creation of test approach with test strategy and test objective Create consolidated testing work plan Enterprise test management and Test Metrics Reporting Organize and conduct up to 4 workshop sessions to understand testing needs. Develop system test strategy and test approach for a .Net or Java application involving waterfall or agile development methods with up to 5 external agency interfaces Create an integration testing work plan in MS Project with up to 500 tasks outlining Commonwealth responsibilities and testing deliverables. Establish process and metrics for reporting testing progress and defects with daily, weekly and end of phase reporting frequency for up to 5 metric types.	
Service Customers / Users	Business, technology or security managers of Any participating Commonwealth agency or office	
Service Prerequisites	Availability of supporting infrastructure and tools (software) solution to perform the assessment Define assessment scope	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**

CCSD13370223-A	Test Estimation and test Approach Planning	• Per Assessment

Service Attribute	*Service Attribute Description*	
Service Name	**System Integration / Acceptance Testing and UAT Support**	
Detailed Description	Functional and non-functional system integration and acceptance test planning and execution User Acceptance Testing (UAT) coordination and support Testing scope management, scheduling, and resource planning. Each assessment supports a specific number of testing clarification sessions, screens, reports, interfaces and test scenarios as indicated below.	
Service Customers / Users	Business, technology or security managers of Any participating Commonwealth agency or office	
Service Prerequisites	Availability of supporting infrastructure and tools (software) solution to perform the assessment Define assessment scope	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSD13370224-A	System Integration / Acceptance Testing and UAT Support – Small	• Per Request / Up to 3 testing clarification sessions, up to 10 screens, up to 2 reports, No interfaces, 40-50 test scenarios
CCSD13370225-A	System Integration / Acceptance Testing and UAT Support – Medium	• Per Request / Up to 5 testing clarification sessions, up to 20 screens, up to 5 reports, u to 2 interfaces, 50-100 test scenarios

CCSD13370226-A	System Integration / Acceptance Testing and UAT Support – Large	• Per Request / Up to 19 testing clarification sessions, up to 30 screens, up to 10 reports, 5 interfaces, 100-250 test scenarios

Service Attribute	*Service Attribute Description*	
Service Name	**Automated Regression Testing**	
Detailed Description	Regression Testing Planning Automated regression testing and repository management Each testing assessment supports a specific number of automation scripts for an entire application as indicated below	
Service Customers / Users	Business, technology or security managers of Any participating Commonwealth agency or office	
Service Prerequisites	Availability of supporting infrastructure and tools (software) solution to perform the assessment Define assessment scope	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSD13370227-A	Automated Regression Testing – Small	• Per Request / Up to 20 automation test scripts for entire application
CCSD13370228-A	Automated Regression Testing – Medium	• Per Request / Up to 30 automation test scripts for entire application
CCSD13370229-A	Automated Regression Testing – Large	• Per Request / Up to 50 automation test scripts for entire application

Service Attribute	*Service Attribute Description*	
Service Name	**Test Data Management**	
Detailed Description	Management of test data including Test Data Automation PII Scrubbing Data Partitioning Each testing assessment supports a specific number of test data creation scripts for an entire application as indicated below Supported Platforms: QTP Microsoft Test Manager (MTM)	
Service Customers / Users	Business, technology or security managers of Any participating Commonwealth agency or office	
Service Prerequisites	Availability of supporting infrastructure and tools (software) solution to perform the assessment Define assessment scope	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSD13370230-A	Test Data Management – Small	• Per Request / Up to 20 data creation scripts for entire application
CCSD13370231-A	Test Data Management – Medium	• Per Request / Up to 30 data creation scripts for entire

		application
CCSD13370232-A	Test Data Management – Large	• Per Request / Up to 50 data creation scripts for entire application

Service Attribute	*Service Attribute Description*	
Service Name	**ADA Compliance Testing**	
Detailed Description	Testing and verification of application compliance with Americans with Disabilities Act Each testing assessment supports a specific number of screens for ADA compliance testing as indicated below Supported Platforms: AccVerify JAWS	
Service Customers / Users	Business, technology or security managers of Any participating Commonwealth agency or office	
Service Prerequisites	Availability of supporting infrastructure and tools (software) solution to perform the assessment Define assessment scope	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSD13370233-A	ADA Compliance Testing – Small	• Per Request / Up to 10 screens
CCSD13370234-A	ADA Compliance Testing – Medium	• Per Request / Up to 20 screens
CCSD13370235-A	ADA Compliance Testing – Large	• Per Request / Up to 30 screens

Load/Availability Testing

Service Attribute	*Service Attribute Description*	
Service Name	**Load Test Script Creation (Initial)**	
Detailed Description	The Load Testing Script Creation (Initial) service provides for the creation of a load testing scripts that allow agencies to mimic user interaction at identified production volumes. The intent is to exercise the application under load to analyze performance requirements and/or to identify performance tuning opportunities prior to the production release. The service provides the creation of: Load Test Scripts – A collection of scripts created from supplied processing requirements that will exercise the application under load. Script specification documents are a required input to detail process flow, user action, expected results, etc. Test data creation and set up is not included in this service. The output of the service is a collection of scripts, bundled into test scenarios that can be repeatedly executed for consistency verification and improvement quantification.	
Service Customers / Users	Business, technology or security managers of Any participating Commonwealth agency or office	
Service Prerequisites	Approvals from the Commonwealth/Unisys PMO Availability of supporting infrastructure and tools (software) solution to perform the assessment Design Specifications (template to be provided)	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**

CCSD13370236-A	Load Test Script Creation (Initial) - Small	Per Script (up to 20 pages)
CCSD13370237-A	Load Test Script Creation (Initial) - Medium	Per Script (up to 50 pages)
CCSD13370238-A	Load Test Script Creation (Initial) - Large	Per Script (up to 100 pages)

Service Attribute	*Service Attribute Description*	
Service Name	**Load Test Script Maintenance**	
Detailed Description	The Load Testing Script Maintenance service builds from the Creation service to keep scripts aligned with changes made to the application. As functionality changes, alterations to the scripts to are required to maintain the ability to test the application under load. Input to this service will be updated script design specification documents. The service provides the creation of: Updated Load Test Scripts – Updated scripts originally created in the Load Test Script Creation service that aligns with application functionality changes.	
Service Customers / Users	Business, technology or security managers of Any participating Commonwealth agency or office	
Service Prerequisites	• Approvals from the Commonwealth/Unisys PMO • Availability of supporting infrastructure and tools (software) solution to perform the assessment • Updated / Added Script Design Specification	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSD13370239-A	Load Test Script Maintenance - Small	Per Script (up to 20 pages)
CCSD13370240-A	Load Test Script Maintenance - Medium	Per Script (up to 50 pages)
CCSD13370241-A	Load Test Script Maintenance - Large	Per Script (up to 100 pages)

Service Attribute	*Service Attribute Description*	
Service Name	**Load Test Execution/Analysis**	
Detailed Description	This Service executes the load test scripts that have been previously prepared and performs analysis using the Silk Performer toolset. The results are provided as an output of the Load Test Execution/Analysis Service.	
Service Customers / Users	Business, technology or security managers of Any participating Commonwealth agency or office	
Service Prerequisites	• Approvals from the Commonwealth/Unisys PMO • Availability of supporting infrastructure and tools (software) solution to perform the assessment • Define assessment scope	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSD13370242-A	Load Test Execution/Analysis - Small	Per Test (up to 25 scripts)
CCSD13370243-A	Load Test Execution/Analysis - Medium	Per Test (up to 50 scripts)
CCSD13370244-A	Load Test Execution/Analysis - Large	Per Test (up to 100 scripts)

Service Attribute	*Service Attribute Description*	
Service Name	**Synthetic Transaction Modeling**	
Detailed Description		
Orderable Unit	• Simple/Small Transaction (up to 5 pages) • Medium Size / Complexity Transaction (up to 10 pages) • Complex/Large Transaction (up to 15 pages)	
Service Customers / Users	Business, technology or security managers of agency or enterprise	
Service Prerequisites	• Approvals from the Commonwealth/Unisys PMO • Availability of supporting infrastructure and tools (software) solution to perform the assessment • Define assessment scope	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSD13370245-A	Synthetic Transaction Modeling - Small	Per Model (up to 5 pages)
CCSD13370246-A	Synthetic Transaction Modeling - Medium	Per Model (up to 10 pages)
CCSD13370247-A	Synthetic Transaction Modeling - Large	Per Model (up to 15 pages)

Application Migration Services

Service Attribute	*Service Attribute Description*	
Service Name	**Enterprise Application Transition Strategy**	
Detailed Description	Develop a strategy to transition enterprise application infrastructure and applications for an agency to managed data center	
Service Customers / Users	Business, technology or security managers of Any participating Commonwealth agency or office	
Service Prerequisites	Approvals from the Commonwealth/Unisys PMO Availability of supporting infrastructure and tools (software) solution to perform the assessment Define assessment scope	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSD13370248-A	Enterprise Application Transition Strategy - Small	Per Assessment (one agency comprising of one business application having up to three environments, development, testing and production that are supported by up to 12 servers)
CCSD13370249-A	Enterprise Application Transition Strategy - Medium	Per Assessment (Develop transition strategy for one agency comprising of up to 2 business applications having up to three environments each, development, testing and production that are supported by up to 24 servers)

CCSD13370250-A	Enterprise Application Transition Strategy - Large	Per Assessment(one agency comprising of up to 4 business applications having up to three environments each, development, testing and production that are supported by up to 48 servers)
CCSD13370251-A	Enterprise Application Transition Strategy – Very Large	Per Assessment (one agency comprising of up to 6 business applications having up to three environments each, development, testing and production that are supported by up to 60 servers)

Service Attribute	*Service Attribute Description*	
Service Name	**Application Migration Plan**	
Detailed Description	Develop a plan for agency applications to migrate to a Unisys Managed Data Center	
Service Customers / Users	Business, technology or security managers of Any participating Commonwealth agency or office	
Service Prerequisites	• Approvals from the Commonwealth/Unisys PMO • Availability of supporting infrastructure and tools (software) solution to perform the assessment • Define assessment scope	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSD13370252-A	Application Migration Plan - Small	Per Assessment (up to one application that need to be migrated. This includes up to three application environments, development, testing and production that are supported by up to 12 servers)
CCSD13370253-A	Application Migration Plan - Medium	Per Assessment (up to two applications that need to be migrated. This includes up to three environments per application, development, testing and production that are supported by up to 24 servers)
CCSD13370254-A	Application Migration Plan -	Per Assessment (up to four applications that need to be

	Large	migrated. This includes up to three environments per application, development, testing and production that are supported by up to 48 server)

Middleware Application Services

Middleware Application Services - AIX

Service Attribute	*Service Attribute Description*
Service Name	WebSphere Build p-Series Standard (1 server)
Detailed Description	Identify performance and availability requirements Perform hardware selection; solicit physical build from client Baseline current environment and utilization (e.g., CPU, memory) Create high-level design using requirements in Assess phase and baseline build documentation Develop a project plan with milestones, dependencies and resource allocations Plan, track, document, and coordinate activities for the project Create data base or WAS-specific test plans and develop acceptance criteria Request Storage allocations per client defined requirements Work with client to confirm power up and burn-in of Server Install and configure AIX v6.x on 1 LPAR per server Install and configure Bundle Middleware Package Configure AIX and Bundle Middleware per customer build requirements Test hardware and software according to documented test plan Validate acceptance criteria have been met Turn-over system to customer and obtain sign-off Build from base level hardware with no OS pre-installed, physical servers are pre-installed in racks with all hardware installed, base OS, I/O, and HA configuration only (no applications), with base images and configuration standards supplied by customer.

Service Customers / Users	Any participating Commonwealth agency or office.	
Service Prerequisites	Software and/or hardware to complete service Access to affected systems and/or facilities.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370255-A	WebSphere Build p-Series Standard	Per Build

Service Attribute	*Service Attribute Description*
Service Name	WebSphere Build p-Series Complex (2 servers)
Detailed Description	Identify performance and availability requirements Perform hardware selection; solicit physical build from client Baseline current environment and utilization (e.g., CPU, memory) Create high-level design using requirements in Assess phase and baseline build documentation Develop a project plan with milestones, dependencies and resource allocations Plan, track, document, and coordinate activities for the project Create data base or WAS-specific test plans and develop acceptance criteria Request Storage allocations per client defined requirements Work with client to confirm power up and burn-in of Server Install and configure AIX v6.x on 1 LPAR per server Install and configure Bundle Middleware Package Configure AIX and Bundle Middleware per customer build requirements Test hardware and software according to documented test plan Validate acceptance criteria have been met Turn-over system to customer and obtain sign-off Build from base level hardware with no OS pre-installed, physical servers are pre-installed in racks with all hardware installed, base OS, I/O, and HA configuration only (no applications), with base images and configuration standards supplied by customer.
Service Customers / Users	Any participating Commonwealth agency or office.

Service Prerequisites	Software and/or hardware to complete service Access to affected systems and/or facilities.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370256-A	WebSphere Build p-Series Complex	Per Build

Service Attribute	*Service Attribute Description*
Service Name	WebSphere Upgrade p-Series Standard (1 server)
Detailed Description	Identify performance and availability profile Collect Performance Baseline Create high-level design using requirements in Assess phase and baseline build documentation Develop a project plan with milestones, dependencies and resource allocations Plan, track, document, and coordinate activities for the project Create application-specific test plans and develop acceptance criteria Request new hardware requirements based upon performance requirements Install and configure current version of target Bundle on 1 LPAR per server Test software according to document test plan Validate acceptance criteria have been met Turn-over system to customer and obtain sign-off This is Upgrade of WebSphere Application Server only - 1 version level upgrade only, OS will be at a version which support the upgraded WAS, base images and configuration standards to be supplied by client. Storage and SAN Fabric are client or other Bundle responsibility, with remote delivery for services is primary alternative, with on-site when necessary.
Service Customers / Users	Any participating Commonwealth agency or office.
Service Prerequisites	Software and/or hardware to complete service Access to affected systems and/or facilities.

Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.

Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370257-A	WebSphere Upgrade p-Series Standard	Per Upgrade

Service Attribute	*Service Attribute Description*
Service Name	WebSphere Upgrade p-Series Complex (2 servers)
Detailed Description	Identify performance and availability profile Collect Performance Baseline Create high-level design using requirements in Assess phase and baseline build documentation Develop a project plan with milestones, dependencies and resource allocations Plan, track, document, and coordinate activities for the project Create application-specific test plans and develop acceptance criteria Request new hardware requirements based upon performance requirements Install and configure current version of target Bundle on 1 LPAR per server Test software according to document test plan Validate acceptance criteria have been met Turn-over system to customer and obtain sign-off This is Upgrade of WebSphere Application Server only - 1 version level upgrade only, OS will be at a version which support the upgraded WAS, base images and configuration standards to be supplied by client. Storage and SAN Fabric are client or other Bundle responsibility, with remote delivery for services is primary alternative, with on-site when necessary.
Service Customers / Users	Any participating Commonwealth agency or office.
Service Prerequisites	Software and/or hardware to complete service Access to affected systems and/or facilities.

Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.

Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370258-A	WebSphere Upgrade p-Series Complex	Per Upgrade

Service Attribute	*Service Attribute Description*	
Service Name	DataPower Quick Start Services	
Detailed Description	Provide DataPower architectural review and design analysis, installation and configuration of appliance, guidance on monitoring techniques, and provide service function design and build. Includes base services setup of 5 Small services.	
Service Customers / Users	Any participating Commonwealth agency or office.	
Service Prerequisites	Software and/or hardware to complete service Access to affected systems and/or facilities.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370259-A	DataPower Quick Start Services	Per Quick Start

Service Attribute	*Service Attribute Description*	
Service Name	p-Series Support for WebSphere App Server (10 Instances)	
Detailed Description	This services bundle is to provide support for WebSphere App Server Instances on System p. This is support for 1 to 10 instances of the application server. 1 FTE in the bundle for one month. 12-month commitment;	
Service Customers / Users	Any participating agency/department.	
Service Prerequisites	None	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370260-A	p-Series Support for WebSphere App Server (10 Instances)	Per Request / Up to 10 WebSphere instances

Service Attribute	*Service Attribute Description*	
Service Name	p-Series Support for WebSphere App Server (25 Instances)	
Detailed Description	This services bundle is to provide support for WebSphere App Server Instances on System p. This is support for 11 to 25 instances of the application server. 2 FTEs in the bundle for one month.	
Service Customers / Users	Any participating agency/department.	
Service Prerequisites	12-month commitment;	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370261-A	p-Series Support for WebSphere App Server (25 Instances)	Per Request / Up to 25 WebSphere instances

Service Attribute	*Service Attribute Description*	
Service Name	p-Series Support for WebSphere App Server (40 Instances)	
Detailed Description	This services bundle is to provide support for WebSphere App Server Instances on System p. This is support for 26 to 40 instances of the application server. 3 FTEs in the bundle for one month.	
Service Customers / Users	Any participating agency/department.	
Service Prerequisites	12-month commitment;	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370262-A	p-Series Support for WebSphere App Server (40 Instances)	Per request / Up to 40 Websphere Instance

Service Attribute	*Service Attribute Description*	
Service Name	p-Series Support for WebSphere MQ Queue Managers (40 Instances)	
Detailed Description	This services bundle is to provide support for WebSphere MQ Queue Managers on System p. This is support for 1 to 40 instances of the Queue Manager. 1 FTE in the bundle for one month.	
Service Customers / Users	Any participating agency/department.	
Service Prerequisites	12-month commitment;	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370263-A	p-Series Support for WebSphere MQ Queue Managers (40 Instances)	Per request / Up to 40 Websphere Instance

Service Attribute	*Service Attribute Description*	
Service Name	p-Series Support for WebSphere MQ Queue Managers (80 Instances)	
Detailed Description	This services bundle is to provide support for WebSphere MQ Queue Managers on System p. This is support for 41 to 80 instances of the Queue Manager. 2 FTEs in the bundle for one month.	
Service Customers / Users	Any participating agency/department.	
Service Prerequisites	12-month commitment;	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370264-A	p-Series Support for WebSphere MQ Queue Managers (80 Instances)	Per Request / Up to 80 Websphere instances

Service Attribute	*Service Attribute Description*	
Service Name	p-Series Support for WebSphere MQ Queue Managers (120 Instances)	
Detailed Description	This services bundle is to provide support for WebSphere MQ Queue Managers on System p. This is support for 81 to 120 instances of the Queue Manager. 3 FTEs in the bundle for one month.	
Service Customers / Users	Any participating agency/department.	
Service Prerequisites	12-month commitment;	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370265-A	p-Series Support for WebSphere MQ Queue Managers (120 Instances)	Per Request / Up to 120 Websphere instances

Middleware Application Services – z-Series

Service Attribute	*Service Attribute Description*
Service Name	WebSphere Build z-Series Standard (1 subsystem without data sharing or clustering)
Detailed Description	Identify performance and availability profile Collect Performance Baseline Create high-level design using requirements in Assess phase and baseline build documentation Develop a project plan with milestones, dependencies and resource allocations Plan, track, document, and coordinate activities for the project Create application-specific test plans and develop acceptance criteria Request new hardware requirements based upon performance requirements Install and configure current version of target Bundle on 1 LPAR per server Test software according to document test plan Validate acceptance criteria have been met Turn-over system to customer and obtain sign-off This is build of a WebSphere Application Server. Base images and configuration standards to be supplied by client. Remote delivery for services is primary alternative, with on-site when necessary.
Service Customers / Users	Any participating Commonwealth agency or office.
Service Prerequisites	Software and/or hardware to complete service Access to affected systems and/or facilities.

Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370266-A	WebSphere Build z-Series Standard	Per Build

Service Attribute	*Service Attribute Description*
Service Name	WebSphere Build z-Series Complex (2 subsystems with data sharing and clustering across multiple CECs)
Detailed Description	Identify performance and availability profile Collect Performance Baseline Create high-level design using requirements in Assess phase and baseline build documentation Develop a project plan with milestones, dependencies and resource allocations Plan, track, document, and coordinate activities for the project Create application-specific test plans and develop acceptance criteria Request new hardware requirements based upon performance requirements Install and configure current version of target Bundle on 1 LPAR per server Test software according to document test plan Validate acceptance criteria have been met Turn-over system to customer and obtain sign-off This is build of a WebSphere Application Server. Base images and configuration standards to be supplied by client. Remote delivery for services is primary alternative, with on-site when necessary.
Service Customers / Users	Any participating Commonwealth agency or office.
Service Prerequisites	Software and/or hardware to complete service Access to affected systems and/or facilities.
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services

	Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370267-A	WebSphere Build z-Series Complex	Per Build

Service Attribute	*Service Attribute Description*
Service Name	WebSphere Upgrade z-Series Standard (1 subsystem without data sharing or clustering)
Detailed Description	Identify performance and availability profile Collect Performance Baseline Create high-level design using requirements in Assess phase and baseline build documentation Develop a project plan with milestones, dependencies and resource allocations Plan, track, document, and coordinate activities for the project Create application-specific test plans and develop acceptance criteria Request new hardware requirements based upon performance requirements Install and configure current version of target Bundle on 1 LPAR per server Test software according to document test plan Validate acceptance criteria have been met Turn-over system to customer and obtain sign-off This is upgrade of a single version of WebSphere Application Server. Base OS is at level required for upgrade of WAS. Base images and configuration standards to be supplied by client. Remote delivery for services is primary alternative, with on-site when necessary
Service Customers / Users	Any participating Commonwealth agency or office.
Service Prerequisites	Software and/or hardware to complete service Access to affected systems and/or facilities.

Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.

Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370268-A	WebSphere Upgrade z-Series Standard	Per Upgrade

Service Attribute	*Service Attribute Description*
Service Name	WebSphere Upgrade z-Series Complex (2 subsystems with data sharing and clustering across multiple CECs)
Detailed Description	Identify performance and availability profile Collect Performance Baseline Create high-level design using requirements in Assess phase and baseline build documentation Develop a project plan with milestones, dependencies and resource allocations Plan, track, document, and coordinate activities for the project Create application-specific test plans and develop acceptance criteria Request new hardware requirements based upon performance requirements Install and configure current version of target Bundle on 1 LPAR per server Test software according to document test plan Validate acceptance criteria have been met Turn-over system to customer and obtain sign-off This is upgrade of a single version of WebSphere Application Server. Base OS is at level required for upgrade of WAS. Base images and configuration standards to be supplied by client. Remote delivery for services is primary alternative, with on-site when necessary
Service Customers / Users	Any participating Commonwealth agency or office.
Service Prerequisites	Software and/or hardware to complete service Access to affected systems and/or facilities.

Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	Service Option Name	Orderable Unit / Restrictions per Unit
CCSI13370269-A	WebSphere Upgrade z-Series Complex	Per Upgrade

Service Attribute	*Service Attribute Description*	
Service Name	z-Series Support for WebSphere App Server (10 Instances)	
Detailed Description	This services bundle is to provide support for WebSphere App Server Instances on System z. This is support for 1 to 10 instances of the application server. 1 FTE in the bundle for one month.	
Service Customers / Users	Any participating Commonwealth agency or office.	
Service Prerequisites	12-month commitment;	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370272-A	z-Series Support for WebSphere App Server (10 Instances)	Per Request / Up to 10 instances

Service Attribute	*Service Attribute Description*	
Service Name	z-Series Support for WebSphere App Server (25 Instances)	
Detailed Description	This services bundle is to provide support for WebSphere App Server Instances on System z. This is support for 11 to 25 instances of the application server. 2 FTE in the bundle for one month.	
Service Customers / Users	Any participating Commonwealth agency or office.	
Service Prerequisites	12-month commitment	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370273-A	z-Series Support for WebSphere App Server (25 Instances)	Per unit as set forth above

Service Attribute	*Service Attribute Description*	
Service Name	z-Series Support for WebSphere App Server (40 Instances)	
Detailed Description	This services bundle is to provide support for WebSphere App Server Instances on System z. This is support for 26 to 40 instances of the application server. 3 FTE in the bundle for one month.	
Service Customers / Users	Any participating Commonwealth agency or office.	
Service Prerequisites	12-month commitment	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370274-A	z-Series Support for WebSphere App Server (40 Instances)	Per unit as set forth above

Service Attribute	*Service Attribute Description*	
Service Name	z-Series Support for WebSphere MQ Queue Managers (40 Queue Managers)	
Detailed Description	This services bundle is to provide support for WebSphere MQ Queue Managers on System z. This is support for 1 to 40 instances of the Queue Manager. 1 FTE in the bundle for one month.	
Service Customers / Users	Any participating Commonwealth agency or office.	
Service Prerequisites	12-month commitment;	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370275-A	z-Series Support for WebSphere MQ Queue Managers (40 Queue Managers)	Per unit as set forth above

Service Attribute	*Service Attribute Description*	
Service Name	z-Series Support for WebSphere MQ Queue Managers (80 Queue Managers)	
Detailed Description	This services bundle is to provide support for WebSphere MQ Queue Managers on System z. This is support for 41 to 80 instances of the Queue Manager. 2 FTE in the bundle for one month.	
Service Customers / Users	Any participating Commonwealth agency or office.	
Service Prerequisites	12-month commitment;	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370276-A	z-Series Support for WebSphere MQ Queue Managers (80 Queue Managers)	Per unit as set forth above

Service Attribute	*Service Attribute Description*	
Service Name	z-Series Support for WebSphere MQ Queue Managers (120 Queue Managers)	
Detailed Description	This services bundle is to provide support for WebSphere MQ Queue Managers on System z. This is support for 81 to 120 instances of the Queue Manager. 3 FTE in the bundle for one month.	
Service Customers / Users	Any participating Commonwealth agency or office.	
Service Prerequisites	12-month commitment;	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370277-A	z-Series Support for WebSphere MQ Queue Managers (120 Queue Managers)	Per unit as set forth above

User Experience (UX) Design

Service Attribute	*Service Attribute Description*	
Service Name	**User Experience Strategy**	
Detailed Description	• Facilitate user experience (UX) workshops • Define personas and user stories • Define success measurement • Develop UX Implementation Roadmap • Define Solution Business Case(s) • Each strategy service supports a specific number work workshops and user stories. The Large workshop also includes the Success Measurement, Implementation Roadmap and Solution Business Case deliverables.	
Service Customers / Users	Business, technology or security managers of any participating Commonwealth agency or office	
Service Prerequisites	• Availability of supporting infrastructure and tools (software) solution to perform the assessment • Define assessment scope	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSD13370278-A	User Experience Strategy - Small	Per Request / Up to 2 workshops, up to 5 user stories
CCSD13370279-A	User Experience Strategy - Medium	Per Request / Up to 5 workshops, up to 10 user stories

CCSD13370280-A	User Experience Strategy - Large	Per Request / Up to 5 workshops, up to 10 user stories, success measurement, implementation roadmap, solution business case

Service Attribute	*Service Attribute Description*	
Service Name	**User Experience Design**	
Detailed Description	• End User Research/Observation/Analysis • End User Usability Testing • Design Option Definition • Style Guide Design • Low Fidelity Sketches • High Fidelity Mock-ups • Interactive Prototype • Each Design service supports a specific number of user research sessions, design options, and screens Each service also includes low or high fidelity sketches, mock-ups, style guides and prototypes.	
Service Customers / Users	Business, technology or security managers of any participating Commonwealth agency or office	
Service Prerequisites	• Availability of supporting infrastructure and tools (software) solution to perform the assessment • Define assessment scope	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSD13370281-A	User Experience Design - Small	Per Request / Up to 2 user research sessions, 1 design option, up to 10 screens, low fidelity sketches.

CCSD13370282-A	User Experience Design - Medium	Per Request / Up to 2 user research sessions, 2 design options, up to 15 screens, low fidelity sketches, high fidelity mock-ups, style guide
CCSD13370283-A	User Experience Design - Large	Per Request / up to 5 user research sessions, 1 usability test, 3 design options, up to 25 screens, low fidelity sketches, high fidelity sketches, style guide, interactive prototype

Service Attribute	*Service Attribute Description*	
Service Name	**User Experience Prototype Development**	
Detailed Description	• Develop User Experience Artifacts • Images • Button Styles • "Response Web" CSS • Configurable "skins" • HTML structure and implementation patterns • Each prototype develop service supports a specific number of screens.	
Service Customers / Users	Business, technology or security managers of any participating Commonwealth agency or office	
Service Prerequisites	• Availability of supporting infrastructure and tools (software) solution to perform the assessment • Define assessment scope	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSD13370284-A	User Experience Prototype Development - Small	Per Request / Up to 10 screens
CCSD13370285-A	User Experience Prototype Development - Medium	Per Request / Up to 15 screens
CCSD13370286-A	User Experience Prototype	Per Request / Up to 25 screens

	Development - Large	

Data Quality Management (DQM) Analysis & Strategy

Service Attribute	*Service Attribute Description*	
Service Name	**Data Quality Management (DQM) – Analysis and Strategy**	
Detailed Description	Identify causes and develop strategies for overcoming inaccurate, incomplete and inconsistent data in enterprise systems. • Define Data Quality Requirements: Identify data components and its impact on business policies. Evaluate and categorize data errors in terms of data quality. • Profile, analyze, and assess Data Quality using data profiling tools and techniques. • Define Data Quality Metrics and Business Rules based on standard conformance and compliance templates • Evaluate and Design Data Quality SLA's and Procedures to measure and monitor compliance with defined data quality rules and SLA's	
Service Customers / Users	Business, technology or security managers of any participating Commonwealth agency or office	
Service Prerequisites	• Approvals from the Commonwealth/Unisys PMO • Availability of supporting infrastructure and tools (software) solution to perform the assessment • Define assessment scope	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSD13370287-A	Data Quality Management (DQM) - Small	Per Assessment / Up to 5 defined data tables; up to 5 GB

		data set size
CCSD13370288-A	Data Quality Management (DQM) - Medium	Per Assessment / Up to 20 defined data tables; Up to 30 GB data set size
CCSD13370289-A	Data Quality Management (DQM) - Large	Per Assessment / Up to 30 defined data tables; up to 50 GB data set size
CCSD13370290-A	Data Quality Management (DQM) Very Large	Per Assessment / Up to 40 defined data tables, up to 100 GB data set size

Information Management Services

Service Attribute	*Service Attribute Description*
Service Name	**Information Management Strategy**
Detailed Description	• Conduct an analyst of the current Information Management capabilities to identify "Where to Start" to accomplish Information Management needs • Conduct a strategy that identifies the multiple Analytic and Business Intelligence tools. • Determine the implementation of each tool against leading practices. o Tools include SAP Business Objects, SAP Data Integrator, Cognos Reporting, Informatica, Data Stage, Erwin data model and identification of the databases that support analytics. (i.e. Oracle, MS SQL Servers). • Identify options on how to manage and/or consolidate the toolsets across the Agency as needed for particular Analytic initiatives. • Each assessment include the development of an analytics/business intelligence tool strategy, a specific number of meetings and analysis of a specific number of tools as indicated below.
Service Customers / Users	Business, technology or security managers of any participating Commonwealth agency or office
Service Prerequisites	• Approvals from the Commonwealth/Unisys PMO • Availability of supporting infrastructure and tools (software) solution to perform the assessment • Define assessment scope
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.

Provider Part Number(s)	Service Option Name	Orderable Unit / Restrictions per Unit
CCSD13370291-A	Information Management Strategy – Small	Per Assessment / Analytics/Business Intelligence Tool Strategy, up to 2 meetings, analysis of up to 3 tools
CCSD13370292-A	Information Management Strategy – Medium	Per Assessment / Analytics/Business Intelligence Tool Strategy, up to 4 meetings, analysis of up to 6 tools
CCSD13370293-A	Information Management Strategy – Large	Per Assessment / Analytics/Business Intelligence Tool Strategy with up to 6 tools, up to 6 meetings, analysis of up to 9 tools
CCSD13370294-A	Information Management Strategy – Very Large	Per Assessment / Analytics/Business Intelligence Tool Strategy with up to 6 tools, up to 6 meetings, analysis of up to 12 tools

Service Attribute	*Service Attribute Description*	
Service Name	**Information Management Full Implementation Lifecycle**	
Detailed Description	Define analytical need of the Agency. Perform an analysis of the current analytics and reporting capability to identify the gap of current versus future reporting requirements: •□ Gather, Document and prioritize business requirements to identify Business Intelligence Reporting and Predictive Analytic requirements •□ Gather and document technical requirements •□ Identify data availability through a source system analysis •□ Document and review Information management rollout strategy to include in the Information Management Roadmap. •□ Each assessment include a specific number of workshops and the development of a specific number of metrics. The Large and Very Large assessments include a predictive model engine and mobile analytics.	
Service Customers / Users	Business, technology or security managers of any participating Commonwealth agency or office	
Service Prerequisites	•□ Approvals from the Commonwealth/Unisys PMO •□ Availability of supporting infrastructure and tools (software) solution to perform the assessment •□ Define assessment scope	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**

CCSD13370295-A	Analytics/Reporting Strategy – Small	Per Request / Up to 5 business/technical workshops, full development of up to 10 metrics.
CCSD13370296-A	Analytics/Reporting Strategy – Small	Per Request / Up to 10 business/technical workshops, full development of up to 20 metrics.
CCSD13370297-A	Analytics/Reporting Strategy – Large	Per Request / Up to 15 business/technical workshops, full development of up to 30 metrics, 1 predictive model engine, mobile analytics
CCSD13370298-A	Analytics/Reporting Strategy – Very Large	Per Request / Up to 20 business/technical workshops, full development of up to 50 metrics, 1 predictive model engine, mobile analytics

Enterprise Resource Planning (ERP) Management Services

Service Attribute	*Service Attribute Description*	
Service Name	**ERP Fit/Gap Analysis**	
Detailed Description	Fit/Gap analysis for a technical or functional upgrade , new functionality or new product integration including: Product Analysis against existing functionality Identification of Functional/Technical Gaps Proposed Options for Resolving Gaps Roadmap for implementation Proposed staffing	
Orderable Unit	Fixed duration of four weeks	
Service Customers / Users	Business, technology or security managers of any participating Commonwealth agency or office	
Service Prerequisites	Approvals from the Commonwealth/Unisys PMO Availability of supporting infrastructure and tools (software) solution to perform the assessment Define assessment scope	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSD13370299-A	ERP Fit/Gap Analysis	Per 4 week Assessment

Service Attribute	*Service Attribute Description*	
Service Name	**ERP Product Selection**	
Detailed Description	Product selection for software that can integrate with ERP suite but is not offered within core functionality deployed. This includes Business requirements gathering Determine viable products Evaluation criteria Product analysis	
Service Customers / Users	Business, technology or security managers of any participating Commonwealth agency or office	
Service Prerequisites	• Approvals from the Commonwealth/Unisys PMO • Availability of supporting infrastructure and tools (software) solution to perform the assessment • Define assessment scope	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSD13370300-A	ERP Product Selection – Viability Assessment	Per 4 week Assessment
CCSD13370301-A	ERP Product Selection – Product Analysis	Per 2 week Assessment

Enterprise Resource Planning (ERP) Application Security Services

Service Attribute	*Service Attribute Description*	
Service Name	**ERP Security Review and Segregation of Duties (SOD) Analysis**	
Detailed Description	Review design and implementation of security for gaps against leading practices. Review can be tailored to the agency's areas of concern such as: • Privacy considerations • Role design and implementation • Role and user level segregation of duties and regulatory compliance considerations • Configurable controls analysis Review the ERP security and control approach, assess gaps, develop roadmap, and conduct an educational presentation Use a proprietary tool, to evaluate configurable controls, critical access, and segregation of duties risk at the user and role level across ERP packages.	
Service Customers / Users	Business, technology or security managers of any participating Commonwealth agency or office	
Service Prerequisites	• Availability of supporting infrastructure and tools (software) solution to perform the assessment • Define assessment scope	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**

CCSD13370302-A	ERP Security Review and Segregation of Duties Analysis - Small	Per Assessment (Up to 25 users and roles)
CCSD13370303-A	ERP Security Review and Segregation of Duties Analysis - Medium	Per Assessment (Up to 100 users and roles)
CCSD13370304-A	ERP Security Review and Segregation of Duties Analysis - Large	Per Assessment (Up to 500 users and roles)

Service Attribute	*Service Attribute Description*
Service Name	**ERP Governance Risk and Compliance (GRC) Review**
Detailed Description	Review the Agency's production Governance, Risk and Compliance (GRC) set up and configuration to assist client in understanding how the organization's environment compares to leading practices. This can include one or more of the following capabilities: •□ User provisioning •□ Risk analysis •□ Emergency access •□ Entitlements management •□ Risk and control monitoring capabilities Perform a general assessment of the agency's GRC system documentation including design and configuration, understanding the implementation approach, and assessing the agency landscape. Suggest enhancement options
Orderable Unit	•□ Small: Review the agency's system configuration and parameters for ***one*** GRC capability •□ Medium: Review the agency's system configuration and parameters for up to three GRC capabilities •□ Large: Review the system configuration and parameters for up to five GRC capabilities
Service Customers / Users	Business, technology or security managers of any participating Commonwealth agency or office
Service Prerequisites	•□ Approvals from the Commonwealth Trusted Agent/Unisys PMO •□ Availability of supporting infrastructure and tools (software) solution to perform the assessment •□ Define assessment scope

Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.

Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSD13370305-A	ERP Governance Risk, and Compliance (GRC) Review - Small	Per Assessment (Agency System Configuration and Parameters for 1 GRC Capability)
CCSD13370306-A	ERP Governance Risk, and Compliance (GRC) Review - Medium	Per Assessment (Agency System Configuration and Parameters for 3 GRC Capabilities)
CCSD13370307-A	ERP Governance Risk, and Compliance (GRC) Review - Large	Per Assessment (Agency System Configuration and Parameters for 5 GRC Capabilities)

Communication Strategy

Service Attribute	*Service Attribute Description*	
Service Name	**Communication Strategy and Planning – Stakeholder Analysis**	
Detailed Description	• Conduct a stakeholder analysis to understand different groups and target appropriate communications for each type of stakeholder group. •	
Service Customers / Users	Business, technology or security managers of any participating Commonwealth agency or office	
Service Prerequisites	• Availability of supporting infrastructure and tools (software) solution to perform the assessment • Define assessment scope	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSD13370308-A	Stakeholder Analysis	Per Request

Service Attribute	*Service Attribute Description*	
Service Name	**Communication Strategy and Planning – Communications Plan**	
Detailed Description	• Create a communications plan that defines key message, forums, frequency of communications as well as recipients/participants, and the communication development and delivery approach	
Service Customers / Users	Business, technology or security managers of any participating Commonwealth agency or office	
Service Prerequisites	• Availability of supporting infrastructure and tools (software) solution to perform the assessment • Define assessment scope	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSD13370309-A	Communications Plan	Per Request

Service Attribute	*Service Attribute Description*	
Service Name	**Communication Strategy and Planning – Communications Delivery**	
Detailed Description	• Define the forms (formal and social) of communications to be used throughout the project lifecycle by establishing protocols for communications review, approval, and feedback mechanisms. Create agreed upon key communications that can be used throughout the project • For each defined project, the communication delivery service includes o The preparation of a comprehensive slide library with key graphics and messages that can be used in various communications throughout the project o Prepare and conduct up to 4 webinars o Create a project fact sheet o Establish a structure for a project newsletter •	
Service Customers / Users	Business, technology or security managers of any participating Commonwealth agency or office	
Service Prerequisites	• Availability of supporting infrastructure and tools (software) solution to perform the assessment • Define assessment scope	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**

CCSD13370310-A	Communications Delivery	Per Request

Infrastructure Virtualization and Migration Services

Service Attribute	*Service Attribute Description*
Service Name	CIRBA Software for Application and Infrastructure Mapping
Detailed Description	Short write up on what the Catalog item will do
Service Customers / Users	Any participating Commonwealth agency or office
Service Prerequisites	What is required before this service or service element be ordered? 1) Selection of another service (what service?) 2) Solution Request submittal 3) Etc.
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog

Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370311-A	CIRBA Software for Application and Infrastructure Mapping	Per Server to be Mapped

Service Attribute	*Service Attribute Description*	
Service Name	Application and Infrastructure Mapping with CIRBA	
Detailed Description	Short write up on what the Catalog item will do	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	What is required before this service or service element be ordered? 1) Selection of another service (what service?) 2) Solution Request submittal 3) Etc.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370312-A	Application and Infrastructure Mapping	Per Request

Service Attribute	*Service Attribute Description*	
Service Name	Application and Infrastructure Mapping with Virtualization and Consolidation Plan	
Detailed Description	Short write up on what the Catalog item will do	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	What is required before this service or service element be ordered? 1) Selection of another service (what service?) 2) Solution Request submittal 3) Etc.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
What Provider Part Numbers can be used to order this service?	Application and Infrastructure Mapping with Virtualization and Consolidation Plan	Per Request

Data Center Facility Services

Service Attribute	*Service Attribute Description*
Service Name	Security Caging – EDC
Detailed Description	This security caging provides a secure space sufficient to hold between 2 and 14 standard racks. The space is constructed of wire mesh panels with sliding entries. The cage sides will extend to the roof or will be topped; in addition, the cage will extend down through the raised floor to the concrete below providing a fully segregated space.
Service Customers / Users	Any participating Commonwealth agency or office
Service Prerequisites	The selection of this service requires the selection of other equipment or services to be placed within the cage including but not limited to fully managed servers, managed-only servers, or colocation services. Secure access control is not included and the type must be selected from the Catalog of Services. Video camera monitoring of the cage, its entrance or interior is optional and may be selected from the Catalog of Services.
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog

Provider Part Number(s)	Service Option Name	Orderable Unit / Restrictions per Unit
CCSU13370501-A	EDC Security Cage – Small	1 cage - 8 feet x 9 feet; 1 door; space is sufficient for 2 standard racks or cabinets; availability dependent upon space
CCSU13370502-A	EDC Security Cage – Medium	1 cage - 10 feet x 9 feet; 1 door; space is sufficient for 3 standard racks or cabinets; dependent upon available space
CCSU13370503-A	EDC Security Cage – Large	1 cage - 18 feet x 9 feet, 1 door; space is sufficient for 7 standard racks or cabinets; dependent upon available space
CCSU13370504-A	EDC Security Cage – Extra Large	1 cage - 18 feet x 15 feet; 2 doors; space is sufficient for 14 standard racks or cabinets in 2 rows; dependent upon available space

Service Attribute	*Service Attribute Description*	
Service Name	Security Caging – [redacted]	
Detailed Description	This security caging provides a secure space sufficient to hold between 2 and 14 standard racks. The space is constructed of wire mesh panels with sliding entries. The cage sides will extend to the roof or will be topped; in addition, the cage will extend down through the raised floor to the concrete below providing a fully segregated space.	
Service Customers / Users	Any	
Service Prerequisites	The selection of this service requires the selection of other equipment or services to be placed within the cage including but not limited to fully managed servers, managed-only servers, or colocation services. Secure access control is not included and the type must be selected from the Catalog of Services. Video camera monitoring of the cage, its entrance or interior is optional and may be selected from the Catalog of Services.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370314-A	[redacted] Security Cage – Small	1 cage - 8 feet x 9 feet; 1 door; space is sufficient for 2 standard racks or cabinets; availability dependent upon space

CCSU13370315-A	[redacted] Security Cage – Medium	1 cage - 10 feet x 9 feet; 1 door; space is sufficient for 3 standard racks or cabinets; dependent upon available space
CCSU13370316-A	[redacted] Security Cage – Large	1 cage - 18 feet x 9 feet, 1 door; space is sufficient for 7 standard racks or cabinets; dependent upon available space
CCSU13370317-A	[redacted] Security Cage – Extra Large	1 cage - 18 feet x 15 feet; 2 doors; space is sufficient for 14 standard racks or cabinets in 2 rows; dependent upon available space

Service Attribute	*Service Attribute Description*	
Service Name	Security Caging – [redacted]	
Detailed Description	This security caging provides a secure space sufficient to hold between 2 and 14 standard racks of up to 84" height. The space is constructed of wire mesh panels with sliding entries. The cage sides will be topped; in addition, the cage will extend down through the raised floor to the concrete below providing a fully segregated space.	
Service Customers / Users	Any	
Service Prerequisites	The selection of this service requires the selection of other equipment or services to be placed within the cage including but not limited to fully managed servers, managed-only servers, or colocation services. Secure access control is not included and the type must be selected from the Catalog of Services. Video camera monitoring of the cage, its entrance or interior is optional and may be selected from the Catalog of Services.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370318-A	[redacted] Security Cage – Small	1 cage - 8 feet x 9 feet; 1 door; space is sufficient for 2 standard racks or cabinets; availability dependent upon space

CCSU13370319-A	[redacted] Security Cage – Medium	1 cage - 10 feet x 9 feet; 1 door; space is sufficient for 3 standard racks or cabinets; dependent upon available space
CCSU13370320-A	[redacted] Security Cage – Large	1 cage - 18 feet x 9 feet, 1 door; space is sufficient for 7 standard racks or cabinets; dependent upon available space
CCSU13370321-A	[redacted] Security Cage – Extra Large	1 cage - 18 feet x 15 feet; 2 doors; space is sufficient for 14 standard racks or cabinets in 2 rows; dependent upon available space

Service Attribute	*Service Attribute Description*
Service Name	Security Caging – EDC - Setup
Detailed Description	This security caging provides a secure space sufficient to hold between 2 and 14 standard racks. The space is constructed of wire mesh panels with sliding entries. The cage sides will extend to the roof or will be topped; in addition, the cage will extend down through the raised floor to the concrete below providing a fully segregated space. The Setup service supports the planning and building services for the associated Security Cage.
Service Customers / Users	Any participating Commonwealth agency or office
Service Prerequisites	The selection of this service requires the selection of other equipment or services to be placed within the cage including but not limited to fully managed servers, managed-only servers, or colocation services. Secure access control is not included and the type must be selected from the Catalog of Services. Video camera monitoring of the cage, its entrance or interior is optional and may be selected from the Catalog of Services.
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog

Provider Part Number(s)	Service Option Name	Orderable Unit / Restrictions per Unit
CCSU13370514-A	EDC Security Cage – Small - Setup	1 cage - 8 feet x 9 feet; 1 door; space is sufficient for 2 standard racks or cabinets; availability dependent upon space
CCSU13370515-A	EDC Security Cage – Medium - Setup	1 cage - 10 feet x 9 feet; 1 door; space is sufficient for 3 standard racks or cabinets; dependent upon available space
CCSU13370516-A	EDC Security Cage – Large - Setup	1 cage - 18 feet x 9 feet, 1 door; space is sufficient for 7 standard racks or cabinets; dependent upon available space
CCSU13370517-A	EDC Security Cage – Extra Large - Setup	1 cage - 18 feet x 15 feet; 2 doors; space is sufficient for 14 standard racks or cabinets in 2 rows; dependent upon available space

Service Attribute	*Service Attribute Description*	
Service Name	Security Caging – [redacted] - Setup	
Detailed Description	This security caging provides a secure space sufficient to hold between 2 and 14 standard racks. The space is constructed of wire mesh panels with sliding entries. The cage sides will extend to the roof or will be topped; in addition, the cage will extend down through the raised floor to the concrete below providing a fully segregated space. The Setup service supports the planning and building services for the associated Security Cage.	
Service Customers / Users	Any	
Service Prerequisites	The selection of this service requires the selection of other equipment or services to be placed within the cage including but not limited to fully managed servers, managed-only servers, or colocation services. Secure access control is not included and the type must be selected from the Catalog of Services. Video camera monitoring of the cage, its entrance or interior is optional and may be selected from the Catalog of Services.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370518-A	[redacted] Security Cage – Small -	1 cage - 8 feet x 9 feet; 1 door; space is sufficient for 2 standard

	Setup	racks or cabinets; availability dependent upon space
CCSU13370519-A	[redacted] Security Cage – Medium - Setup	1 cage - 10 feet x 9 feet; 1 door; space is sufficient for 3 standard racks or cabinets; dependent upon available space
CCSU13370520-A	[redacted] Security Cage – Large - Setup	1 cage - 18 feet x 9 feet, 1 door; space is sufficient for 7 standard racks or cabinets; dependent upon available space
CCSU13370521-A	[redacted] Security Cage – Extra Large - Setup	1 cage - 18 feet x 15 feet; 2 doors; space is sufficient for 14 standard racks or cabinets in 2 rows; dependent upon available space

Service Attribute	*Service Attribute Description*	
Service Name	Security Caging – [redacted]	
Detailed Description	This security caging provides a secure space sufficient to hold between 2 and 14 standard racks of up to 84" height. The space is constructed of wire mesh panels with sliding entries. The cage sides will be topped; in addition, the cage will extend down through the raised floor to the concrete below providing a fully segregated space. The Setup service supports the planning and building services for the associated Security Cage.	
Service Customers / Users	Any	
Service Prerequisites	The selection of this service requires the selection of other equipment or services to be placed within the cage including but not limited to fully managed servers, managed-only servers, or colocation services. Secure access control is not included and the type must be selected from the Catalog of Services. Video camera monitoring of the cage, its entrance or interior is optional and may be selected from the Catalog of Services.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370522-A	[redacted] Security Cage – Small	1 cage - 8 feet x 9 feet; 1 door; space is sufficient for 2 standard

	- Setup	racks or cabinets; availability dependent upon space
CCSU13370523-A	[redacted] Security Cage – Medium - Setup	1 cage - 10 feet x 9 feet; 1 door; space is sufficient for 3 standard racks or cabinets; dependent upon available space
CCSU13370524-A	[redacted] Security Cage – Large - Setup	1 cage - 18 feet x 9 feet, 1 door; space is sufficient for 7 standard racks or cabinets; dependent upon available space
CCSU13370525-A	[redacted] Security Cage – Extra Large - Setup	1 cage - 18 feet x 15 feet; 2 doors; space is sufficient for 14 standard racks or cabinets in 2 rows; dependent upon available space

Service Attribute	*Service Attribute Description*	
Service Name	Enclosed Network Security Conduit	
Detailed Description	An enclosed network security conduit provides a physically secure path from one secure area to another for network cabling requiring physical segregation.	
Service Customers / Users	Any.	
Service Prerequisites	This service must be requested with another service that provides or includes network connectivity such as a fully-managed server or a co-location cabinet.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370322-A	4” Steel Security Conduit	Per foot; must be ordered for one of the in scope data centers.

Service Attribute	*Service Attribute Description*	
Service Name	Enclosed Security Cable Tray	
Detailed Description	An enclosed security cable tray provides a physically secure path from one secure area to another for cabling requiring physical segregation.	
Service Customers / Users	Any.	
Service Prerequisites	This service must be requested with another service that provides or includes network connectivity; typically requested with a security cage.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370323-A	Enclosed Security Cable Tray	Per foot; must be ordered for one of the in scope data centers.

Service Attribute	*Service Attribute Description*	
Service Name	Security Camera	
Detailed Description	A security camera placed as requested within the datacenters for the video monitoring of an entrance, cabinet, or area within the datacenter.	
Service Customers / Users	Any.	
Service Prerequisites	None.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370324-A	Security Camera	Per camera; time to install depends upon the capacity within the current video monitoring system

Service Attribute	*Service Attribute Description*	
Service Name	Access Control Panel	
Detailed Description	An access control panel for controlled access through doors such as those on security cages	
Service Customers / Users	Any.	
Service Prerequisites	None.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370325-A	Access Control Panel	Per panel; time to install depends upon the capacity within the existing access control system

Service Attribute	*Service Attribute Description*	
Service Name	Security Cabinet	
Detailed Description	A secure cabinet of standard footprint (2’ x 3’) including lockable front and rear doors.	
Service Customers / Users	Any participating Commonwealth agency or office.	
Service Prerequisites	None.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370326-A	Security Cabinet – Standard, Full	Per cabinet

Data Center Relocation Services

Service Attribute	*Service Attribute Description*	
Service Name	Lift and Ship of Servers	
Detailed Description	This servers includes the following services: 1) Unracking of the server 2) Packing the new server in preparation of shipment. 3) Shipment of the server to new location 4) Unpacking of the server 5) Cabling of the server in the new location 6) Racking the server in the new location.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	Not Applicable	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370327-A	Lift and Ship of Servers	Per Server

Service Attribute	*Service Attribute Description*	
Service Name	Data Center Relocation Services	
Detailed Description	Provide assessment and discovery services, move day planning and implementation for a lift and shift relocation for the entire enterprise data center. The complexity of a full data center build, move, relocate and maintaining operations is often poorly estimated by many enterprises during this critical activity. IBM has a great deal of experience in making the move as seamless as possible to provide continued operation	
Service Customers / Users	Any participating Commonwealth agency or office.	
Service Prerequisites	None	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370328-A	Data Center Relocation Services Plan	Per Plan

Service Attribute	*Service Attribute Description*	
Service Name	Transition Tools: EMC RecoverPoint Solution for migrations for 10,000 GB of SAN-attached Storage	
Detailed Description	This service is offered to the Commonwealth to aid in data migration and mitigate against application outages in cases where highly critical applications require near continuous availability.	
Service Customers / Users	The Service is Available to Any participating Commonwealth agency or office.	
Service Prerequisites	What is required before this service or service element be ordered? 1) The service may require a scheduled change outage window to complete a temporary break in data flow and attach the infrastructure. A second outage may be required to remove the infrastructure following migration.	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370329-A	Transition Tools: EMC RecoverPoint Solution for migrations for 10,000 GB of SAN-attached Storage	Per Package

Network and Security Services

IPV6 Services

Service Attribute	*Service Attribute Description*	
Service Name	IPV6 Strategy	
Detailed Description	Three phase approach to implementing IPV6 on the CoPA network. Phase 1 will be full network and application analysis of current IPv4 implementation and readiness of applications and LAN/WAN to support IPv6; Phase 2 will be a detailed plan to cut over both applications and LAN/WAN to IPv6; Phase 3 will be the cutover itself.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	1) What is required before this service or service element be ordered? Service will not be offered until all transition/transformation activities are completed.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSP13370330-A	IPV6 Strategy	Per Engagement

LAN Network Services

Service Attribute	*Service Attribute Description*	
Service Name	LAN Switch Installation for new Managed Only Racks	
Detailed Description	This service provides the installation and initial configuration of a network switches in a new rack with Managed Only or Co-Location equipment requiring network connectivity.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites		
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370331-A	LAN Switch Installation for new Managed Racks	Per Switch

Virtual Private Network Services

Service Attribute	*Service Attribute Description*	
Service Name	Virtual Private Network – Business Partner - Planning	
Detailed Description	Develop the design of the Virtual Private Network site to site connection for a Commonwealth Business Partner to enable controlled access to an application or service between the Agency's data center applications and the Business Partner.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites		
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370332-A	VPN – Business Partner - Planning	Per Request

Service Attribute	*Service Attribute Description*	
Service Name	Virtual Private Network – Business Partner - Implementation	
Detailed Description	Implement the Virtual Private Network site to site connection for a Commonwealth Business Partner to enable controlled access to an application or service between the Agency's data center applications and the Business Partner.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites		
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370333-A	VPN – Business Partner - Implementation	Per Request

Service Attribute	*Service Attribute Description*	
Service Name	Virtual Private Network – Business Partner - Modification	
Detailed Description	Modify an existing Virtual Private Network site to site connection for a Commonwealth Business Partner to enable controlled access to an application or service between the Agency's data center applications and the Business Partner.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	What is required before this service or service element be ordered? 1) Selection of another service (what service?) 2) Solution Request submittal 3) Etc.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370334-A	VPN – Business Partner - Modification	Per Request

Service Attribute	*Service Attribute Description*	
Service Name	Virtual Private Network – Business Partner - Decommission	
Detailed Description	Remove an existing Virtual Private Network site to site connection for a Commonwealth Business Partner to enable controlled access to an application or service between the Agency's data center applications and the Business Partner	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	If Business Partner access is still required after the removal of the VPN site to site tunnel, an alternative connection must be in place prior to the removal to limit the impact to the application's users.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370335-A	VPN – Business Partner – Decommission	Per Request

Service Attribute	*Service Attribute Description*	
Service Name	***Virtual Private Network – Commonwealth Agency - Planning***	
Detailed Description	Develop the design of a Virtual Private Network site to site connection between a Commonwealth Agency or Office and a Unisys team managed data center with Agency or Office hosted applications.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	What is required before this service or service element be ordered? 1) Selection of another service (what service?) 2) Solution Request submittal 3) Etc.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370336-A	VPN – Commonwealth Agency - Planning	Per Request

Service Attribute	*Service Attribute Description*	
Service Name	Virtual Private Network – Commonwealth Agency - Implementation	
Detailed Description	Implement Virtual Private Network site to site connection between a Commonwealth Agency or Office and a Unisys team managed data center with Agency or Office hosted applications.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites		
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370337-A	VPN – Commonwealth Agency - Implementation	Per Request

Service Attribute	*Service Attribute Description*	
Service Name	Virtual Private Network – Commonwealth Agency - Modification	
Detailed Description	Modify an existing Virtual Private Network site to site connection between a Commonwealth Agency or Office and a Unisys team managed data center with Agency or Office hosted applications.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites		
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370338-A	VPN – Commonwealth Agency - Modification	Per Request

Service Attribute	*Service Attribute Description*	
Service Name	Virtual Private Network – Commonwealth Agency - Decommission	
Detailed Description	Remove an existing Virtual Private Network site to site connection between a Commonwealth Agency or Office and a Unisys team managed data center with Agency or Office hosted applications.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	If access to the hosted applications is still required after the removal of the VPN site to site tunnel, an alternative connection must be in place prior to the removal to limit the impact to the application's users.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370339-A	VPN – Commonwealth Agency – Decommission	Per Request

Network Load Balancing Services

Service Attribute	*Service Attribute Description*	
Service Name	Hardware Network Load Balancer – Design and Implement	
Detailed Description	Design and Implement application services on a Hardware Network Load Balancer	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites		
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370340-A	Hardware Network Load Balancer – Design & Implement – Small	Per Request / Up to 2 servers and 1 Content Service
CCSU13370341-A	Hardware Network Load Balancer – Design & Implement – Medium	Per Request / Up to 5 servers and 2 Content Services
CCSU13370342-A	Hardware Network Load Balancer – Design & Implement - Large	Per Request / Up to 10 servers and 5 Content Services

Service Attribute	*Service Attribute Description*	
Service Name	Hardware Network Load Balancer - Modify	
Detailed Description	Modify application services on a Hardware Network Load Balancer	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	Application Service on Hardware Load Balancer implemented by the Design and Implement Service	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370343-A	Hardware Network Load Balancer – Modify – Small	Per Request / Up to 2 servers and 1 Content Service
CCSU13370344-A	Hardware Network Load Balancer – Modify – Medium	Per Request / Up to 5 servers and 2 Content Services
CCSU13370345-A	Hardware Network Load Balancer – Modify - Large	Per Request / Up to 10 servers and 5 Content Services

Service Attribute	*Service Attribute Description*	
Service Name	SSL Offloading on Network Load Balancer – Design and Implement	
Detailed Description	Design and Implement SSL Offloading services on a Hardware Network Load Balancer	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites		
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370346-A	SSL Offloading on Network Load Balancer – Design and Implement	Per Request / 1 URL for 1 Application

Service Attribute	*Service Attribute Description*	
Service Name	SSL Offloading on Network Load Balancer - Modify	
Detailed Description	Modify SSL Offloading services on a Hardware Network Load Balancer	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	SSL Offload for Application Service on Hardware Load Balancer implemented by the Design and Implement Service	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370349-A	SSL Offloading on Network Load Balancer – Modify	Per Request / 1 URL for 1 Application

Service Attribute	*Service Attribute Description*	
Service Name	Multi-site Global Network Load Balancer – Design and Implement	
Detailed Description	Design and Implement a Multi-Site Global Load Balancer service between two data centers	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites		
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370352-A	Multi-site Global Network Load Balancer – Design – Small	Per Request / Up to 2 servers and 1 content service across 2 sites.
CCSU13370353-A	Multi-site Global Network Load Balancer – Design – Medium	Per Request / Up to 5 servers and 2 content service across 2 sites.
CCSU13370354-A	Multi-site Global Network Load Balancer – Design - Large	Per Request / Up to 10 servers and 5 content service across 2 sites.

Service Attribute	*Service Attribute Description*	
Service Name	Multi-site Global Network Load Balancer - Modify	
Detailed Description	Short write up on what the Catalog item will do	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	Global Load Balancing for Application Service on Hardware Load Balancer implemented by the Design and Implement Service	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370355-A	Multi-site Global Network Load Balancer – Modify – Small	Per Request / Up to 2 servers and 1 content service across 2 sites.
CCSU13370356-A	Multi-site Global Network Load Balancer – Modify – Medium	Per Request / Up to 5 servers and 2 content service across 2 sites.
CCSU13370357-A	Multi-site Global Network Load Balancer – Modify - Large	Per Request / Up to 10 servers and 5 content service across 2 sites.

Reverse Proxy Services

Service Attribute	*Service Attribute Description*	
Service Name	Reverse Proxy Platform– Design and Implement	
Detailed Description	Design and Implement a Reverse Proxy to support Application services. This service covers the design and implementation of the Proxy platform.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	Per Application to be supported, the Reverse Proxy – Application Service – Design and Implement is required.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370358-A	Reverse Proxy – Design & Implement – Proxy Platform – Small	Per Request / up to 100 concurrent users, and 40 KBPS
CCSU13370359-A	Reverse Proxy – Design & Implement – Medium	Per Request /up to 200 concurrent users, and 60 KBPS
CCSU13370360-A	Reverse Proxy – Design & Implement - Large	Per Request / up to 500 concurrent users, and 80 KBPS

Service Attribute	*Service Attribute Description*	
Service Name	Reverse Proxy – Application Service - Design and Implement	
Detailed Description	Design and Implement a Reverse Proxy to support Application services. This service covers the design and implementation of the Application service on the proxy.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	Reverse Proxy Platform– Design and Implement supporting the number of concurrent users.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370361-A	Reverse Proxy – Design & Implement – Application Service – Small	Per Request / 1 Application, 1 URL, up to 100 concurrent users, and 40 KBPS
CCSU13370362-A	Reverse Proxy – Design & Implement – Application Service – Medium	Per Request / 1 Application, 1 URL, up to 200 concurrent users, and 60 KBPS
CCSU13370363-A	Reverse Proxy – Design & Implement – Application Service – Large	Per Request / 1 Application, 1 URL, up to 500 concurrent users, and 80 KBPS

Service Attribute	*Service Attribute Description*	
Service Name	Reverse Proxy – Application Service - Modify	
Detailed Description	Modify a Reverse Proxy to support Application services. This service covers the modification of the Application service on the proxy.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	Existing Reverse Proxy Application Service implemented by the Reverse Proxy – Application Service – Design and Implement service.	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name. Or To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370364-A	Reverse Proxy – Modify – Application Service – Small	Per Request / 1 Application, 1 URL, up to 100 concurrent users, and 40 KBPS
CCSU13370365-A	Reverse Proxy – Modify – Application Service – Medium	Per Request / 1 Application, 1 URL, up to 200 concurrent users, and 60 KBPS
CCSU13370366-A	Reverse Proxy – Modify – Application Service – Large	Per Request / 1 Application, 1 URL, up to 500 concurrent users, and 80 KBPS

Stealth Security Services

Service Attribute	*Service Attribute Description*	
Service Name	Stealth Starter Plan Service	
Detailed Description	This service will deploy the Stealth Solution in your infrastructure to be used to explore and validate the selected use case. Documentation of the use case testing and a summary of findings and recommendations will be provided.	
Service Customers / Users	Any participating Commonwealth agency or office requiring data in motion encryption	
Service Prerequisites		
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370367-A	Stealth Starter Plan Service – 2 weeks	Per Request / 2 Week Project

Service Attribute	*Service Attribute Description*	
Service Name	Stealth Secure Virtual Terminal Starter Plan Service Add-On	
Detailed Description	This service is an add-on module to the Stealth PoC to add Stealth Solution for Virtual Terminal to the PoC. This service adds an additional 2 weeks to the POC to provide for the design and creation of the USB images.	
Service Customers / Users	Any participating Commonwealth agency or office requiring data in motion encryption	
Service Prerequisites	Stealth Starter Plan Service	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370368-A	Stealth SSVT Starter Plan Add-On Service – 2 weeks	Per Request / 2 Week Project

Service Attribute	*Service Attribute Description*	
Service Name	Steal Discovery Service	
Detailed Description	The Unisys Stealth Solution Discovery Service is a facilitated, participant-driven activity focused on introducing you to the Unisys Stealth Solution and identifying Stealth use cases that best meet your business requirements. The discovery service will produce a high level architecture diagram that represents a suggested use for Stealth in the client environment.	
Service Customers / Users	Any participating Commonwealth agency or office requiring data in motion encryption	
Service Prerequisites	None	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370369-A	Stealth Discovery Service – 2 Weeks	Per Request / 2 Week Project

Service Attribute	*Service Attribute Description*	
Service Name	Stealth Design Service	
Detailed Description	The Unisys Stealth Solution Design Service draws on the infrastructure and requirements information gathered as part of the preceding Stealth service engagements and provides a technical plan for the implementation of Stealth as per the use cases identified by you.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	Stealth Discovery Service -2 Weeks	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370370-A	Stealth Design Service – 2 weeks	Per Request / 2 week Project

Service Attribute	*Service Attribute Description*	
Service Name	Stealth Deployment Service	
Detailed Description	The Unisys Stealth Solution Deployment Service is a follow-on service to the Unisys Stealth Solution Design Service. The purpose of this service is to install and configure the Unisys Stealth Solution infrastructure in your network and render your environment 'Ready for Use'.	
Service Customers / Users	Any participating Commonwealth agency or office requiring data in motion encryption	
Service Prerequisites	Stealth Design Service – 2 Weeks	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370371-A	Stealth Deployment Service – 2 Weeks	Per Request / 2 week Project

Service Attribute	*Service Attribute Description*	
Service Name	Stealth Network Appliance	
Detailed Description	Stealth appliances use military-grade technology and best practices to render end-users, servers and other IT assets undetectable on any available network. Additionally, cryptographic virtualization separates and secures users, functions and entire organizations into Communities-of-Interest, undetectable from each other and external malicious activities. Entry-Level end-point data protection appliance Specification: 3.1GHz Single Processor, 300Mb/Sec Mid-Level end-point data protection appliance Specification: 3.1GHz Single Processor, 800Mb/Sec Large-Scale end-point data protection appliance Specification: 2.9GHz Single Processor, 1Gb/sec	
Service Customers / Users	Any participating Commonwealth agency or office requiring data in motion encryption	
Service Prerequisites	Stealth Deployment Service – 2 Weeks Stealth Network Appliance – Annual Maintenance Stealth Client Licenses, or Stealth Server Licenses	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370372-A	Stealth Network Appliance (1000 Licenses, 300 Mbps)	Per Appliance
CCSU13370373-A	Stealth Network Appliance (1000 Licenses, 800 Mbps)	Per Appliance

CCSU13370374-A	Stealth Network Appliance (RPS, 1 Gbps)Stealth Deployment Service	Per Appliance

Service Attribute	*Service Attribute Description*	
Service Name	Stealth Network Appliance – Annual Maintenance	
Detailed Description	Stealth appliances use military-grade technology and best practices to render end-users, servers and other IT assets undetectable on any available network. Additionally, cryptographic virtualization separates and secures users, functions and entire organizations into Communities-of-Interest, undetectable from each other and external malicious activities. Entry-Level end-point data protection appliance Specification: 3.1GHz Single Processor, 300Mb/Sec Mid-Level end-point data protection appliance Specification: 3.1GHz Single Processor, 800Mb/Sec Large-Scale end-point data protection appliance Specification: 2.9GHz Single Processor, 1Gb/sec The Annual Maintenance service provides the manufacturers ongoing software support contract.	
Service Customers / Users	Any participating Commonwealth agency or office requiring data in motion encryption	
Service Prerequisites	Stealth Deployment Service – 2 Weeks	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370526-A	Stealth Network Appliance (1000 Licenses, 300 Mbps) – Annual Maintenance	Per Appliance
CCSU13370527-A	Stealth Network Appliance (1000 Licenses, 800 Mbps) – Annual Maintenance	Per Appliance

CCSU13370528-A	Stealth Network Appliance (RPS, 1 Gbps)– Annual Maintenance	Per Appliance

Service Attribute	*Service Attribute Description*	
Service Name	Stealth Client License	
Detailed Description	Stealth Concurrent Usage Licenses protecting a client endpoint such as a laptop or PC	
Service Customers / Users	Any participating Commonwealth agency or office requiring data in motion encryption	
Service Prerequisites	Stealth Network Appliance Stealth Client License – Annual Maintenance	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370375-A	Stealth Client License (1-24)	Per License / 1-24 licenses
CCSU13370376-A	Stealth Client License (25-49)	Per License / 25-49 licenses
CCSU13370377-A	Stealth Client License (50-99)	Per License / 50-99 licenses
CCSU13370378-A	Stealth Client License (100-249)	Per License / 100-249 licenses
CCSU13370379-A	Stealth Client License (250-499)	Per License / 250-499 licenses
CCSU13370380-A	Stealth Client License (500-999)	Per License / 500-999 licenses
CCSU13370381-A	Stealth Client License (1000+)	Per License / 1000+ licenses

Service Attribute	*Service Attribute Description*	
Service Name	Stealth Client License – Annual Maintenance	
Detailed Description	Stealth Concurrent Usage Licenses protecting a client endpoint such as a laptop or PC The Annual Maintenance service provides the manufacturers ongoing software support contract.	
Service Customers / Users	Any participating Commonwealth agency or office requiring data in motion encryption	
Service Prerequisites	Stealth Network Appliance	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370529-A	Stealth Client License (1-24) – Annual Maintenance	Per License / 1-24 licenses
CCSU13370530-A	Stealth Client License (25-49) – Annual Maintenance– Annual Maintenance	Per License / 25-49 licenses
CCSU13370531-A	Stealth Client License (50-99) – Annual Maintenance	Per License / 50-99 licenses
CCSU13370532-A	Stealth Client License (100-249) – Annual Maintenance	Per License / 100-249 licenses
CCSU13370533-A	Stealth Client License (250-499) – Annual Maintenance	Per License / 250-499 licenses
CCSU13370534-A	Stealth Client License (500-999) – Annual Maintenance	Per License / 500-999 licenses

CCSU13370535-A	Stealth Client License (1000+)– Annual Maintenance	Per License / 1000+ licenses

Service Attribute	*Service Attribute Description*	
Service Name	Stealth Client Expansion License	
Detailed Description	Stealth add-on licenses after initial installation protecting a client endpoint such as a laptop or PC.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	Stealth Network Appliance Stealth Client Licenses Stealth Client Expansion Licenses – Annual Maintenance	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370382-A	Stealth Client Expansion License (1-24)	Per License / 1-24 licenses
CCSU13370383-A	Stealth Client Expansion License (25-49)	Per License / 25-49 licenses
CCSU13370384-A	Stealth Client Expansion License (50-99)	Per License / 50-99 licenses
CCSU13370385-A	Stealth Client Expansion License (100-249)	Per License / 100-249 licenses
CCSU13370386-A	Stealth Client Expansion License (250-499)	Per License / 250-499 licenses
CCSU13370387-A	Stealth Client Expansion License (500-999)	Per License / 500-999 licenses

CCSU13370388-A	Stealth Client Expansion License (1000+)	Per License / 1000+ licenses

Service Attribute	*Service Attribute Description*	
Service Name	Stealth Client Expansion License – Annual Maintenance	
Detailed Description	Stealth add-on licenses after initial installation protecting a client endpoint such as a laptop or PC. The Annual Maintenance service provides the manufacturers ongoing software support contract.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	Stealth Network Appliance	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370536-A	Stealth Client Expansion License (1-24) – Annual Maintenance	Per License / 1-24 licenses
CCSU13370537-A	Stealth Client Expansion License (25-49) – Annual Maintenance	Per License / 25-49 licenses
CCSU13370538-A	Stealth Client Expansion License (50-99) – Annual Maintenance	Per License / 50-99 licenses
CCSU13370539-A	Stealth Client Expansion License (100-249) – Annual Maintenance	Per License / 100-249 licenses
CCSU13370540-A	Stealth Client Expansion License (250-499) – Annual Maintenance	Per License / 250-499 licenses

CCSU13370541-A	Stealth Client Expansion License (500-999) – Annual Maintenance	Per License / 500-999 licenses
CCSU13370542-A	Stealth Client Expansion License (1000+)– Annual Maintenance	Per License / 1000+ licenses

Service Attribute	*Service Attribute Description*	
Service Name	Stealth Server License	
Detailed Description	Stealth Concurrent Usage Licenses Protecting a server or virtual machine endpoint	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	Stealth Network Appliance Stealth Server Licenses – Annual Maintenance	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370389-A	Stealth Server License (1-4)	Per License / 1-4 licenses
CCSU13370390-A	Stealth Server License (5-9)	Per License / 5-9 licenses
CCSU13370391-A	Stealth Server License (10-24)	Per License / 10-24 licenses
CCSU13370392-A	Stealth Server License (25-49)	Per License / 25-49 licenses
CCSU13370393-A	Stealth Server License (50-99)	Per License / 50-99 licenses
CCSU13370394-A	Stealth Server License (100+)	Per License / 100+ licenses

Service Attribute	*Service Attribute Description*	
Service Name	*Stealth Server License – Annual Maintenance*	
Detailed Description	*Stealth Concurrent Usage Licenses Protecting a server or virtual machine endpoint* *The Annual Maintenance service provides the manufacturers ongoing software support contract.*	
Service Customers / Users	*Any participating Commonwealth agency or office*	
Service Prerequisites	*Stealth Network Appliance* *Stealth Server Licenses*	
Request the Service	*To request this service, submit a Solution Request in the online Enterprise Services Catalog*	
Provider Part Number(s)	***Service Option Name***	***Orderable Unit / Restrictions per Unit***
CCSU13370543-A	*Stealth Server License (1-4) – Annual Maintenance*	*Per License / 1-4 licenses*
CCSU13370544-A	*Stealth Server License (5-9) – Annual Maintenance*	*Per License / 5-9 licenses*
CCSU13370545-A	*Stealth Server License (10-24) – Annual Maintenance*	*Per License / 10-24 licenses*
CCSU13370546-A	*Stealth Server License (25-49) – Annual Maintenance*	*Per License / 25-49 licenses*
CCSU13370547-A	*Stealth Server License (50-99) – Annual Maintenance*	*Per License / 50-99 licenses*
CCSU13370548-A	*Stealth Server License (100+)– Annual Maintenance*	*Per License / 100+ licenses*

Service Attribute	*Service Attribute Description*	
Service Name	Stealth Server Expansion License	
Detailed Description	Stealth Concurrent Usage add-on licenses after initial installation Protecting a server or virtual machine endpoint	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	Stealth Network Appliance	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370395-A	Stealth Server Expansion License (1-4)	Per License / 1-4 licenses
CCSU13370396-A	Stealth Server Expansion License (5-9)	Per License / 5-9 licenses
CCSU13370397-A	Stealth Server Expansion License (10-24)	Per License / 10-24 licenses
CCSU13370398-A	Stealth Server Expansion License (25-49)	Per License / 25-49 licenses
CCSU13370399-A	Stealth Server Expansion License (50-99)	Per License / 50-99 licenses
CCSU13370400-A	Stealth Server Expansion License (100+)	Per License / 100+ licenses

Service Attribute	*Service Attribute Description*	
Service Name	Stealth Server Expansion License – Annual Maintenance	
Detailed Description	Stealth Concurrent Usage add-on licenses after initial installation Protecting a server or virtual machine endpoint The Annual Maintenance service provides the manufacturers ongoing software support contract.	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	Stealth Network Appliance Stealth Server Expansion Licenses	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370549-A	Stealth Server Expansion License (1-4) – Annual Maintenance	Per License / 1-4 licenses
CCSU13370550-A	Stealth Server Expansion License (5-9) – Annual Maintenance	Per License / 5-9 licenses
CCSU13370551-A	Stealth Server Expansion License (10-24) – Annual Maintenance	Per License / 10-24 licenses
CCSU13370552-A	Stealth Server Expansion License (25-49) – Annual Maintenance	Per License / 25-49 licenses
CCSU13370553-A	Stealth Server Expansion License (50-99) – Annual	Per License / 50-99 licenses

	Maintenance	
CCSU13370554-A	Stealth Server Expansion License (100+)– Annual Maintenance	Per License / 100+ licenses

Service Attribute	*Service Attribute Description*	
Service Name	Stealth Authorization Service License	
Detailed Description	Data protection authorization interface service License	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	Stealth Network Appliance Stealth client and/or server licenses	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370401-A	Stealth Authorization Service Stand Alone License	Per Service

Service Attribute	*Service Attribute Description*	
Service Name	Stealth Authorization Service License	
Detailed Description	Data protection authorization interface service License. Interfaces with AD/LDAP authorization scheme	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	Stealth Network Appliance Stealth client and/or server licenses	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370402-A	Stealth Authorization Service with AD/LDAP License	Per Service

Service Attribute	*Service Attribute Description*	
Service Name	Stealth Authorization Service License	
Detailed Description	Data protection authorization interface service License. Interfaces with a RADIUS (Remote Authentication Dial-In User Service) authorization scheme	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	Stealth Network Appliance Stealth client and/or server licenses	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370403-A	Stealth Authorization Service with RADIUS License	Per Service

Service Attribute	*Service Attribute Description*	
Service Name	Stealth Secure Virtual Terminal Boot Device	
Detailed Description	Customized Stealth Secure USB devices delivers Stealth software media to provide a data protection solution designed to provide an uncompromised internet business session through the use of a hardened, highly minimized operating system, a locked down browser and communications tunnel cloaked to those who are not pre-identified as part of the "secure community."	
Service Customers / Users	Any participating Commonwealth agency or office	
Service Prerequisites	Completion of the Stealth Design Service	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370404-A	Stealth Secure Virtual Terminal 4GB Windows Boot Device	Per Device

Security Services

Security Vulnerability Assessment

Service Attribute	*Service Attribute Description*	
Service Name	**Security Vulnerability Assessment – Infrastructure**	
Detailed Description	Identify potential security risks on the IT infrastructure using automated vulnerability scanning tools and manual assimilation. Use automated vulnerability scanning tools to identify potential security risks within the IT infrastructure	
Service Customers / Users	Business, technology or security managers of any participating Commonwealth agency or office	
Service Prerequisites	• Availability of non-production environment identical to the production environment or in case the assessment is done using the production environment an appropriate fail over plan should be established • Define scope of the assessment and availability of vulnerability testing tools	
Request the Service	To request this service, submit a Service Request and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSD13370405-A	Vulnerability Assessment – Infrastructure - Small	Per Assessment (Up to 3 Class C Networks with up to 60 hosts)
CCSD13370406-A	Vulnerability Assessment – Infrastructure– Medium	Per Assessment (Up to 5 Class C Networks with up to 125 hosts)
CCSD13370407-A	Vulnerability Assessment –	Per Assessment (Up to 10 Class

	Infrastructure– Large	C with up to 275)
CCSD13370408-A	Vulnerability Assessment – Infrastructure – Very Large	Per Assessment (Up to 1 Class B network with 500 hosts)

Service Attribute	*Service Attribute Description*
Service Name	**Security Vulnerability Assessment –** **Web/mobile application**
Detailed Description	Identify potential security risks on the web application, using automated vulnerability scanning tools and manual assimilation. Use automated vulnerability scanning tools to identify potential security risks within the applications (web/mobile).
Service Customers / Users	Business, technology or security managers of any participating Commonwealth agency or office
Service Prerequisites	• Availability of non-production environment identical to the production environment or in case the assessment is done using the production environment an appropriate fail over plan should be established • Define scope of the assessment and availability of vulnerability testing tools
Request the Service	To request this service, submit a Service Request and select the Enterprise Services Catalog item using the above Service Name.

Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSD13370409-A	Vulnerability Assessment – Web/Mobile Application - Small	Per Assessment (35 Custom Web Application Pages)
CCSD13370410-A	Vulnerability Assessment – Web/Mobile Application – Medium	Per Assessment (70 Custom Web Application Pages)
CCSD13370411-A	Vulnerability Assessment – Web/Mobile Application – Large	Per Assessment (100 Custom Web Application Pages)

CCSD13370412-A	Vulnerability Assessment – Web/Mobile Application – Very Large	Per Assessment (175 Custom Web Application Pages)

Service Attribute	*Service Attribute Description*	
Service Name	**Security Vulnerability Assessment – Database**	
Detailed Description	**Database assessment:** Perform a controlled vulnerability assessment on the target database infrastructure to identify potential security vulnerabilities that may lead to unauthorized information leakage or even lead to comprise of the database system. Supported database assessments: Oracle, Microsoft SQL Server, IBM DB2, MySQL, Lotus Domino and Sybase.	
Service Customers / Users	Business, technology or security managers of any participating Commonwealth agency or office	
Service Prerequisites	• Availability of non-production environment identical to the production environment or in case the assessment is done using the production environment an appropriate fail over plan should be established • Define scope of the assessment and availability of vulnerability testing tools	
Request the Service	To request this service, submit a Service Request and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSD13370413-A	Vulnerability Assessment – Database - Small	Per Assessment (3 database server running up to 5 instances or Oracle SIDs
CCSD13370414-A	Vulnerability Assessment – Database – Medium	Per Assessment (5 database servers running up to 10 instances or Oracle SIDs

CCSD13370415-A	Vulnerability Assessment – Database– Large	Per Assessment (10 database servers running up to 15 instances or Oracle SIDs
CCSD13370416-A	Vulnerability Assessment – Database – Very Large	Per Assessment (20 database servers running up to 30 instances or Oracle SIDs

Service Attribute	*Service Attribute Description*	
Service Name	Security Vulnerability assessment – Wireless infrastructure	
Detailed Description	Wireless assessment: Identify security vulnerabilities in the configuration or implementation of the target wireless LAN infrastructure. Perform controlled discovery of wireless access nodes, high level security analysis of the configuration, and assess the overall capability of the Wireless LAN infrastructure through the following tasks: □□ Wireless network profile □□ Wireless configuration and security	
Service Customers / Users	Business, technology or security managers of any participating Commonwealth agency or office	
Service Prerequisites	• □ Availability of non-production environment identical to the production environment or in case the assessment is done using the production environment an appropriate fail over plan should be established • □ Define scope of the assessment and availability of vulnerability testing tools	
Request the Service	To request this service, submit a Service Request and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSD13370417-A	Vulnerability Assessment – Wireless Infrastructure - Small	Per Assessment (up to 2 locations with a total of 25 total wireless access points

CCSD13370418-A	Vulnerability Assessment – Wireless Infrastructure – Medium	Per Assessment (two3cations with a total of 50 total wireless access points
CCSD13370419-A	Vulnerability Assessment – Wireless Infrastructure – Large	Per Assessment (4 locations with a total of 75 wireless access points)

Service Attribute	*Service Attribute Description*	
Service Name	**Vulnerability Assessment - Security Code Review**	
Detailed Description	Use static code review tools to perform security code review for identification of potential insecure coding practices within the custom web application source code. Supported custom web application technologies: Microsoft .NET framework, JAVA, Adobe Flash, JavaScript and AJAX	
Service Customers / Users	Business, technology or security managers of any participating Commonwealth agency or office	
Service Prerequisites	• Availability of non-production environment identical to the production environment or in case the assessment is done using the production environment an appropriate fail over plan should be established • Define scope of the assessment and availability of vulnerability testing tools	
Request the Service	To request this service, submit a Service Request and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSD13370420-A	Security Code Review - Small	Per Assessment (up to 500,000 lines of one web application custom source code. Perform manual verification on up to 15 vulnerabilities (up to four instances per vulnerability assimilated)
CCSD13370421-A	Security Code Review – Medium	Per Assessment (up to one million lines of one web application custom source code. Perform manual verification on up to 20 vulnerabilities (up to

		six instances per vulnerability assimilated)
CCSD13370422-A	Security Code Review – Large	Per Assessment (up to two million lines of one web application custom source code. Perform manual verification on up to 25 vulnerabilities (up to eight instances per vulnerability assimilated))
CCSD13370423-A	Security Code Review – Very Large	Per Assessment (up to 3.5 million lines of one web application custom source code. Perform manual verification on up to 35 vulnerabilities (up to 10 instances per vulnerability assimilated)

Security Risk Management

Service Attribute	*Service Attribute Description*
Service Name	**Security risk assessment**
Detailed Description	Conduct a security assessment of the agency's IT infrastructure security process and controls to identify gaps with relevant security guidelines and potential mitigation controls: •□ Commonwealth information security policy and standards •□ Internal Revenue Service publication 1075 •□ Health Information Portability and Accountability Act (HIPAA) •□ Criminal Justice Information Services (CJIS) •□ Pennsylvania Criminal History Records Information Act (CHRIA) •□ Payment Card Industry (PCI) •□ Family Educational Rights Protection Act (FERPA) •□ Social Security Administration (SSA) •□ Centers for Medicare and Medicaid Services (CMS) •□ National Institute of Standards and Technology (NIST) SP800-53 •□ ISO 27001:2005 •□ Other controls as agreed upon during scope discussions.
Service Customers / Users	Business, technology or security managers of any participating Commonwealth agency or office
Service Prerequisites	•□ Approvals from the Commonwealth Trusted Agent/Unisys PMO •□ Define scope of the assessment and availability of security risk assessment templates & tools

Request the Service	To request this service, submit a Service Request and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSD13370424-A	Security Risk Assessment - Small	Per Assessment (An Agency or Office with up to 99 employees & 1 Security Guidelines)
CCSD13370425-A	Security Risk Assessment – Medium	Per Assessment (An Agency or Office with up to 999 employees & 2 Security Guidelines)
CCSD13370426-A	Security Risk Assessment – Large	Per Assessment (An Agency or Office with up to 9,999 employees & 5 Security Guidelines)
CCSD13370427-A	Security Risk Assessment – Very Large	Per Assessment (An Agency or Office with 10,000+ employees & 10 Security Guidelines)

Service Attribute	Service Attribute Description	
Service Name	eGRC Platform – Install and Initial Setup	
Detailed Description	□□ Install eGRC solution suite along with supporting software (MS Silverlight and web server). □□ Enable database connectivity and setup standard user access (up to five (5) users. □□ Technology platforms: RSA Archer, IBM Open Pages, CA eGRC	
Service Customers / Users	Business, technology or security managers of any participating Commonwealth agency or office	
Service Prerequisites		
Request the Service	To request this service, submit a Service Request and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSD13370428-A	eGRC Solution – Install and Initial setup	• □ Per eGRC Implementation / One eGRC installation and standard initial configuration

Service Attribute	Service Attribute Description	
Service Name	eGRC Solution – Design and Configure	
Detailed Description	• Design and configure eGRC solution modules such as Risk Management, Policy Management and Enterprise Management (using RSA Archer). This activity include analysis of the current environment, correlating business and system requirements, design and configuration of eGRC solution. In addition we configure standard user access (up to five users) • Technology platforms: RSA Archer, IBM Open Pages, CA eGRC	
Service Customers / Users	Business, technology or security managers of any participating Commonwealth agency or office	
Service Prerequisites		
Request the Service	To request this service, submit a Service Request and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSD13370429-A	eGRC Solution – Design and Configure – Small	• Per Request / Up to one solution module
CCSD13370430-A	eGRC Solution – Design and Configure - Medium	• Per Request / Up to two solution modules
CCSD13370431-A	eGRC Solution – Design and Configure – Large	• Per Request / Up to four solution modules
CCSD13370432-A	eGRC Solution – Design and Configure – Very Large	• Per Request / Up to six solution modules

Service Attribute	Service Attribute Description	
Service Name	eGRC Solution – Develop Risk Assessment	
Detailed Description	• Work with the Commonwealth stakeholders to develop and establish one risk assessment questionnaire template based on regulatory requirements. This template allows the stakeholders to perform periodic risk assessments across the management, operational, and technology areas of the enterprise or IT infrastructure. • Technology platforms: RSA Archer, IBM Open Pages, CA eGRC	
Service Customers / Users	Business, technology or security managers of any participating Commonwealth agency or office	
Service Prerequisites		
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSD13370433-A	eGRC Solution – Develop risk assessment templates - Small	• Per Request / 1 risk assessment template with up to 50 questions
CCSD13370434-A	eGRC Solution – Develop risk assessment templates – Medium	• Per Request / 1 risk assessment template with up to 125 questions
CCSD13370435-A	eGRC Solution – Develop risk assessment templates – Large	• Per Request / 2 risk assessment templates with a total of 200 questions
CCSD13370436-A	eGRC – Develop risk assessment templates – Very Large	• Per Request / 2 risk assessment templates with a total of 300 questions

Security Configuration Review

Service Attribute	*Service Attribute Description*
Service Name	**Security Configuration Review**
Detailed Description	• Perform a review of the IT system's security configuration to identify potential vulnerabilities using leading industry practices such as IRS 1075 SCSEMs, NIST, SANS and Center for Internet Security (CIS). • Security configuration review of standard operating system platforms (instance) on up to three information systems: o Microsoft Windows (2000, XP, 2003, 2008,7 and 8) o UNIX Flavors of HP-UX, AIX, SCO and Tru64 o Linux flavors – Red Hat and SUSE o HP OpenVMS o Oracle Solaris o Other Security configuration review of three standard database solution instance – Oracle, Microsoft SQL Server, MySQL or IBM DB2. Security configuration review of three web server technology instance – Microsoft IIS, Apache Jakarta, Apache Tomcat and IBM WebSphere • Security configuration review of two boundary defense solution instance such as firewall, intrusion prevention system, antivirus, VPN and switch/router. • Security configuration review of one mainframe operating system instance – IBM zOS and UNISYS. • Security configuration review of three virtual infrastructure instance (VMWare ESX). • Security configuration review of one standard ERP solution – SAP, PeopleSoft and Oracle Applications.

Service Customers / Users	Business, technology or security managers of any participating Commonwealth agency or office	
Service Prerequisites	Scope of the assessment and availability of security configuration review tools	
Request the Service	To request this service, submit a Service Request and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSD13370437-A	Security Configuration Review (Standard OS Platform - up to 3 information Systems	Per Request
CCSD13370438-A	Security Configuration Review (3 standard database instances)	Per Request
CCSD13370439-A	Security Configuration Review (3 web server instances)	Per Request
CCSD13370440-A	Security Configuration Review (2 boundary defense devices)	Per Request
CCSD13370441-A	Security Configuration Review (One Mainframe OS Instance)	Per Request
CCSD13370442-A	Security Configuration Review (up to 3 Virtual infrastructure instances)	Per Request
CCSD13370443-A	Security Configuration Review (One standard ERP solution)	Per Request

Cyber Threat Intelligence (CTI) Analysis

Service Attribute	*Service Attribute Description*	
Service Name	**CTI - Diagnostic**	
Detailed Description	Analyze security event logs to identify those potential internal hosts that may be compromised and are attempting to communicate with malicious internet hosts. The analysis will include detection of potential internal devices to determine presence of rogue devices or devices exhibiting potential stealth-like characteristics	
Service Customers / Users	Business, technology or security managers of any participating Commonwealth agency or office	
Service Prerequisites	• Availability of system audit logs to perform the assessment • Define scope of the assessment and availability of system audit log analysis tools	
Request the Service	To request this service, submit a Service Request and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSD13370444-A	CTI-Diagnostic - Small	Per Assessment (1 of TB of audit logs and rogue device detection for up to 1,000 devices)
CCSD13370445-A	CTI-Diagnostic – Medium	Per Assessment (2 of TB of audit logs and rogue device detection for up to 2,000 devices)
CCSD13370446-A	CTI-Diagnostic – Large	Per Assessment (3 of TB of audit logs and rogue device detection for up to 3,500

		devices)
CCSD13370447-A	CTI-Diagnostic – Very Large	Per Assessment (4 of TB of audit logs and rogue device detection for up to 5,000 devices)

Service Attribute	*Service Attribute Description*	
Service Name	**Suspicious Program Diagnostic**	
Detailed Description	Identify potentially unwanted programs, malicious files, and unknown binaries on agency workstations and desktops	
Service Customers / Users	Business, technology or security managers of any participating Commonwealth agency or office	
Service Prerequisites	• Availability of system audit logs to perform the assessment • Define scope of the assessment and availability of system audit log analysis tools	
Request the Service	To request this service, submit a Service Request and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSD13370448-A	Suspicious Program Diagnostic - Small	Per Assessment (up to 25 standard configuration for Servers, workstations, or desktops)
CCSD13370449-A	Suspicious Program Diagnostic – Medium	Per Assessment (up to 100 standard configuration for Servers, workstations, or desktops)
CCSD13370450-A	Suspicious Program Diagnostic – Large	Per Assessment (up to 250 standard configuration for Servers, workstations, or desktops)
CCSD13370451-A	Suspicious Program Diagnostic – Very Large	Per Assessment (up to 1,000 standard configuration for Servers, workstations, or

		desktops)

Service Attribute	*Service Attribute Description*	
Service Name	**Remote Access Compromise Analysis**	
Detailed Description	Remote access logs are analyzed against current cyber intelligence data to expose compromised devices logging into the organization's network.	
Service Customers / Users	Business, technology or security managers of any participating Commonwealth agency or office	
Service Prerequisites	• Availability of system audit logs to perform the assessment • Define scope of the assessment and availability of system audit log analysis tools	
Request the Service	To request this service, submit a Service Request and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSD13370452-A	Remote Access Compromise Analysis - Small	Per Assessment (1 TB of Remote Access Audit Logs)
CCSD13370453-A	Remote Access Compromise Analysis – Medium	Per Assessment (2 TB of Remote Access Audit Logs)
CCSD13370454-A	Remote Access Compromise Analysis – Large	Per Assessment (3 TB of Remote Access Audit Logs)
CCSD13370455-A	Remote Access Compromise Analysis – Very Large	Per Assessment (4 TB of Remote Access Audit Logs)

Service Attribute	*Service Attribute Description*	
Service Name	**Insider Threat Detection Diagnostic**	
Detailed Description	An assessment of the organization's insider threat detection capability including review of existing logs that can reveal current or past insider threats. The review will also analyze recent incidents and recommend a roadmap for automating the capability	
Service Customers / Users	Business, technology or security managers of any participating Commonwealth agency or office	
Service Prerequisites	• Availability of system audit logs to perform the assessment • Define scope of the assessment and availability of system audit log analysis tools	
Request the Service	To request this service, submit a Service Request and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSD13370456-A	Insider Threat Detection Diagnostic - Small	Per Assessment (Agency or Office with up to 99 employees, up to 250 GB of Audit Logs, and up to 3 Interviews)
CCSD13370457-A	Insider Threat Detection Diagnostic – Medium	Per Assessment (Agency or Office with up to 999 employees, up to 500 GB of Audit Logs, and up to 5 Interviews)
CCSD13370458-A	Insider Threat Detection Diagnostic – Large	Per Assessment (Agency or Office with up to 9,999 employees, up to 1 TB of Audit Logs, and up to 10 Interviews)

CCSD13370459-A	Insider Threat Detection Diagnostic – Very Large	Per Assessment (Agency or Office with up to 10,000+ employees, up to 2 TB of Audit Logs, and up to 3 Interviews)

Service Attribute	*Service Attribute Description*	
Service Name	**Enterprise Fraud Program Assessment**	
Detailed Description	Review the agency fraud program to determine if the appropriate skill sets, processes, organization integration, and technologies are in place to detect/manage potential emerging fraud issues. This assessment includes a review of the agency's internet application transaction and web server logs to identify potential fraudulent transactions	
Service Customers / Users	Business, technology or security managers of any participating Commonwealth agency or office	
Service Prerequisites	• Availability of system audit logs to perform the assessment • Define scope of the assessment and availability of system audit log analysis tools	
Request the Service	To request this service, submit a Service Request and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSD13370460-A	Enterprise Fraud Program Assessment - Small	Per Assessment (Agency or Office with up 99 employees, 250 GB of Audit Logs, and up to 3 Fraud Detection Rule Sets)
CCSD13370461-A	Enterprise Fraud Program Assessment – Medium	Per Assessment (Agency or Office with up 999 employees, 500 GB of Audit Logs, and up to 5 Fraud Detection Rule Sets)
CCSD13370462-A	Enterprise Fraud Program Assessment – Large	Per Assessment (Agency or Office with up 9,999 employees, 1 TB of Audit Logs, and up to 5 Fraud

		Detection Rule Sets)
CCSD13370463-A	Enterprise Fraud Program Assessment – Very Large	Per Assessment (Agency or Office with up 10,000+ employees, 2 TB of Audit Logs, and up to 5 Fraud Detection Rule Sets)

Data Prevention

Service Attribute	*Service Attribute Description*	
Service Name	**Data Loss Prevention (DLP) – Network monitoring**	
Detailed Description	Establish a high level DLP governance model in addition to monitoring and reporting metrics. Design, implement and configure a DLP data-in-motion (network) solution to help detect/prevent inadvertent data loss by monitoring the network traffic.	
Service Customers / Users	Business, technology or security managers of any participating Commonwealth agency or office	
Service Prerequisites	• Approvals from the Commonwealth Trusted Agent/Unisys PMO • Availability of supporting network infrastructure, DLP hardware and software solution to perform the implementation • Define design and implementation scope of the DLP solution	
Request the Service	To request this service, submit a Service Request and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSD13370464-A	Data Loss Prevention - Network Monitoring - Small	Per Request (1 Egress Point, and 5 Small, and 1 Complex DLP Policies)
CCSD13370465-A	Data Loss Prevention - Network Monitoring – Medium	Per Request (2 Egress Points, 7 Small, and 2 Complex DLP Policies)
CCSD13370466-A	Data Loss Prevention - Network	Per Request (3 Egress Points, 9

	Monitoring – Large	Small, and 3 Complex DLP Policies)
CCSD13370467-A	Data Loss Prevention - Network Monitoring – Very Large	Per Request (4 Egress Points, 12 Small, and 5 Complex DLP Policies)

Service Attribute	*Service Attribute Description*
Service Name	**Data Loss Prevention (DLP) – Endpoint protection**
Detailed Description	Establish a high level DLP governance model in addition to monitoring and reporting metrics. Design, implement and configure a DLP data-in-use (endpoint) solution to help detect/prevent inadvertent data loss by monitoring activity at the endpoint (e.g. laptop, desktop).
Orderable Unit	Small (Very small agency): Design, Implement and configure the DLP solution for up to 150 IT infrastructure endpoints. Configure up to five Small and one complex DLP policies Medium (Small agency): Design, Implement and configure the DLP solution for up to 1,250 IT infrastructure endpoints. Configure up to seven Small and three complex DLP policies Large (Mid-size agency): Design, Implement and configure the DLP solution for up to 11,000 IT infrastructure endpoints. Configure up to nine Small and three complex DLP policies Very Large (Large agency): Design, Implement and configure the DLP solution for up to 25,000 IT infrastructure endpoints. Configure up to 12 Small and five complex DLP policies
Service Customers / Users	Business, technology or security managers of any participating Commonwealth agency or office
Service Prerequisites	• Approvals from the Commonwealth Trusted Agent/Unisys PMO • Availability of supporting network infrastructure, DLP hardware and software solution to perform the implementation • Define design and implementation scope of the DLP solution
Request the Service	To request this service, submit a Service Request and select the Enterprise Services Catalog item using the above Service Name.

Provider Part Number(s)	Service Option Name	Orderable Unit / Restrictions per Unit
CCSD13370468-A	Data Loss Prevention - Endpoint Protection - Small	Per Request (up to 150 IT infrastructure endpoints, 5 Small, and 1 Complex DLP Policies)
CCSD13370469-A	Data Loss Prevention - Endpoint Protection – Medium	Per Request (up to 1,250 IT infrastructure endpoints, 7 Small, and 3 Complex DLP Policies)
CCSD13370470-A	Data Loss Prevention - Endpoint Protection – Large	Per Request (up to 11,000 IT infrastructure endpoints, 9 Small, and 3 Complex DLP Policies)
CCSD13370471-A	Data Loss Prevention - Endpoint Protection – Very Large	Per Request (25,000 IT infrastructure endpoints, and 12 Small, and 5 Complex DLP Policies)

Service Attribute	*Service Attribute Description*	
Service Name	**Data breach diagnostic**	
Detailed Description	Support the Commonwealth to identify the IT infrastructure impacted by the data breach. Perform a forensic analysis and system audit log review of the impacted IT infrastructure to help determine: • How the system(s) were compromised, allowing the data breach to occur • The internal scope of the breach; i.e. How many other systems may have been involved, and may require further investigation/remediation to remove further threat of data loss. • The potential number of Personally Identifiable Information (PII) records affected by the breach	
Service Customers / Users	Business, technology or security managers of any participating Commonwealth agency or office	
Service Prerequisites	• Approvals from the Commonwealth Trusted Agent/Unisys PMO • Availability of system audit logs, supporting network infrastructure, and software	
Request the Service	To request this service, submit a Service Request and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSD13370472-A	Data Breach Diagnostics - Small	Per Assessment (Up to 3 Systems, 120 GB of File Storage, and 100 GB of uncompressed text Audit Logs)
CCSD13370473-A	Data Breach Diagnostics –	Per Request (Up to 10

	Medium	Systems, 120 GB of File Storage, and 500 GB of uncompressed text Audit Logs)
CCSD13370474-A	Data Breach Diagnostics – Large	Per Request (Up to 50 Systems, 120 GB of File Storage, and 2 TB of uncompressed text Audit Logs)

Mobile Security

Service Attribute	*Service Attribute Description*	
Service Name	**Mobile Device Management (MDM) – Design and implement**	
Detailed Description	Implementation of mobile security technology through a staged approach (e.g., test/pilot/production), to include technology configuration based on identified requirements and use cases, unit testing, user acceptance testing, post-deployment support.	
Service Customers / Users	Business, technology or security managers of any participating Commonwealth agency or office	
Service Prerequisites	• Approvals from the Commonwealth Trusted Agent/Unisys PMO • Availability of supporting infrastructure and software solution to perform the design and implementation • Define design and implementation scope	
Request the Service	To request this service, submit a Service Request and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSD13370475-A	Mobile Device Management (MDM) - Design and Implement - Small	• Per Request (up to 100 managed devices)
CCSD13370476-A	Mobile Device Management (MDM) - Design and Implement – Medium	Per Request (up to 250 managed devices)
CCSD13370477-A	Mobile Device Management (MDM) - Design and Implement – Large	Per Request (up to 1,000 managed devices)

CCSD13370478-A	Mobile Device Management (MDM) - Design and Implement – Very Large	Per Request (up to 2,000 managed devices)

Service Attribute	*Service Attribute Description*	
Service Name	**Mobile Security Strategy and Roadmap**	
Detailed Description	Design and deploy a requirements driven mobile security strategy and architecture that takes into account the mobile ecosystem, its inter-dependencies, the various organizational risks, the underlying mobile security objectives/approach and strategic choices.	
Service Customers / Users	Business, technology or security managers of any participating Commonwealth agency or office	
Service Prerequisites	• Approvals from the Commonwealth Trusted Agent/Unisys PMO • Define assessment scope	
Request the Service	To request this service, submit a Service Request and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSD13370479-A	Mobile Security Strategy and Roadmap - Small	• Per Request (up to 100 managed devices)
CCSD13370480-A	Mobile Security Strategy and Roadmap – Medium	Per Request (up to 250 managed devices)
CCSD13370481-A	Mobile Security Strategy and Roadmap – Large	Per Request (up to 1,000 managed devices)
CCSD13370482-A	Mobile Security Strategy and Roadmap – Very Large	Per Request (up to 2,000 managed devices)

Security Awareness Training

Service Attribute	*Service Attribute Description*	
Service Name	**Security Training Assessment**	
Detailed Description	Conduct a training assessment of the Commonwealth/Agency's existing training curriculum to identify gaps relevant to security protocols. The assessment includes: •□ Understanding existing security awareness •□ Identifying existing training curriculum and training history •□ Documenting knowledge gaps for each Agency •□ Identifying training requirements to mitigate knowledge gaps	
Service Customers / Users	Business, technology or security managers of any participating Commonwealth agency or office	
Service Prerequisites	•□ Approvals from the Commonwealth Trusted Agent/Unisys PMO •□ Define assessment scope	
Request the Service	To request this service, submit a Service Request and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSD13370483-A	Security Training Assessment - Small	Per Request (Agency or Office with up to 999 employees)
CCSD13370484-A	Security Training Assessment - Medium	Per Request (Agency or Office with up to 9,999 employees)
CCSD13370485-A	Security Training Assessment - Large	Per Request (Agency or Office with up to 10,000+ employees)

Service Attribute	*Service Attribute Description*	
Service Name	**Security training (design and delivery)**	
Detailed Description	• Develop specialized security training materials that describe the Commonwealth/agency's information security program & the individual's responsibility to protect Commonwealth data • Develop and provide a tailored security-related education & awareness workshops	
Service Customers / Users	Business, technology or security managers of any participating Commonwealth agency or office	
Service Prerequisites	• Approvals from the Commonwealth Trusted Agent/Unisys PMO • Define security awareness training scope and number of users to be trained	
Request the Service	To request this service, submit a Service Request and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSD13370486-A	Security Training - Design and Delivery -	• Per Request (Training Presentation Deliverable and one training session (Up to 4 Hours))

Identity & Access Management (IAM) Service

Service Attribute	*Service Attribute Description*
Service Name	**Access Management – Design and Implementation Service**
Detailed Description	Design and implement □□ Application access policies □□ User authentication □□ Single sign on, single logout if multiple applications are required to be configured □□ Identity provider □□ Service provider □□ Federation access policies Major technology platforms □□ CA SiteMinder/Federation □□ IBM Security Access Manager □□ IBM Tivoli Federated Identity Manager and Oracle Access Manager Small: Access Management solution design and implementation for standard applications based on web servers such as IIS or Apache platforms, with up to 50 role based access policies and/or an identity federated solution integration with a service provider/one identity provider Medium: Access Management solution design and implementation for the medium complex applications based on applications servers such as IBM WebSphere and WebLogic; with up to 100 role based access policies and Single Sign-On (SSO) Integration (or) IAM federated solution integration for up to two service providers/one identity provider □□ Large: Access Management solution design and implementation for complex applications such as SAP, Oracle EBS, SharePoint or large custom applications with up to 100 role based access policies and SSO integration (or) a federated solution integration for up to five service providers/one identity provider
Service Customers /	Business, technology or security managers of any participating

Users	Commonwealth agency or office	
Service Prerequisites	• Approvals from the Commonwealth Trusted Agent/Unisys PMO • Availability of appropriate IAM solutions and processes	
Request the Service	To request this service, submit a Service Request and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSD13370487-A	Access Management - Design and Implement - Small	• Per Request / Design and implementation for standard applications based on web servers such as IIS or Apache platforms, with up to 50 role based access policies and/or an identity federated solution integration with a service provider/one identity provider
CCSD13370488-A	Access Management - Design and Implement - Medium	Per Request / Design and implementation for the medium complex applications based on applications servers such as IBM WebSphere and WebLogic; with up to 100 role based access policies and Single Sign-On (SSO) Integration (or) IAM federated solution integration for up to two service providers/one identity provider
CCSD13370489-A	Access Management - Design and Implement - Large	Per Request / Design and implementation for complex applications such as SAP, Oracle EBS, SharePoint or large

		custom applications with up to 100 role based access policies and SSO integration (or) a federated solution integration for up to five service providers/one identity provider

Service Attribute	*Service Attribute Description*
Service Name	**Identity Provisioning and Management – Design and Implementation Service**
Detailed Description	Design and implement □ Identity provisioning and de-provisioning processes with default adapters □ Password management processes □ Delegated user administration model □ Setup entitlement repository and access certification campaign Major technology platforms □ CA GovernanceMinder and Identity Manager □ Aveksa Role Manager □ SailPoint Governance Platform and Compliance Manager □ IBM Security Identity Manager and □ Oracle Identity Manager Small: Implement provisioning solution for one user repository based on LDAP, Databases using out of the box provisioning connector, up to three single step approval workflows, and up to five provisioning policies. Medium: Implement provisioning solution for two user repositories based on Unix, LDAP, Databases using out of the box provisioning connector, up to three single step and multi-step approval workflows, and up to ten provisioning policies. Large: Implement provisioning for one complex system/application with up to 5 modules e.g. SAP, and Oracle ERP; up to three single step and multi-step approval workflows, and up to ten provisioning policies.
Service Customers / Users	Business, technology or security managers of any participating Commonwealth agency or office
Service Prerequisites	• □ Availability of appropriate IAM solutions and processes

Request the Service	To request this service, submit a Service Request and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSD13370490-A	Identity Provisioning and Management - Design and Implement - Small	Per Request / Standard: Implement provisioning solution for one user repository based on LDAP, Databases using out of the box provisioning connector, up to three single step approval workflows, and up to five provisioning policies.
CCSD13370491-A	Identity Provisioning and Management - Design and Implement - Medium	Per Request / Implement provisioning solution for two user repositories based on Unix, LDAP, Databases using out of the box provisioning connector, up to three single step and multi-step approval workflows, and up to ten provisioning policies.
CCSD13370492-A	Identity Provisioning and Management - Design and Implement - Large	Per Request / Implement provisioning for one complex system/application with up to 5 modules e.g. SAP, and Oracle ERP; up to three single step and multi-step approval workflows, and up to ten provisioning policies.

Service Attribute	*Service Attribute Description*	
Service Name	**Identity Governance and Management – Design and Implementation Service**	
Detailed Description	Use existing user provisioning process on the support platforms (described below) to setup entitlement repository and access certification campaign Major technology platforms CA GovernanceMinder and Identity Manager Aveksa Role Manager SailPoint Governance Platform and Compliance Manager IBM Security Identity Manager and Oracle Identity Manager	
Service Customers / Users	Business, technology or security managers of any participating Commonwealth agency or office	
Service Prerequisites	• Availability of appropriate IAM solutions and processes	
Request the Service	To request this service, submit a Service Request and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
	Identity Entitlement Provisioning and Management - Design and Implement - Small	Per Request (Provide entitlements and access certification for up to 2 applications)
	Identity Entitlement Provisioning and Management - Design and Implement - Medium	Per Request (Provide entitlements and access certification for up to 5 applications)
	Identity Entitlement Provisioning and Management - Design and Implement - Large	Per Request (Provide entitlements and access certification for up to 10

		applications)

Third Party Software

Service Attribute	*Service Attribute Description*	
Service Name	Unisys Mainframe – Software License Transfer	
Detailed Description	As part of the installation of a replacement Unisys Mainframe, software must be transferred. The following Server Options provide transfer fee support for the indicated Exhibit B.4 software.	
Service Customers / Users	Commonwealth Agencies with Unisys Mainframe	
Service Prerequisites	New Unisys Mainframe Installation or technology replacement	
Request the Service	To request this service, submit a Solution Request in the online Enterprise Services Catalog	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSU13370496-A	Unisys Mainframe – Software Transfer License – KMSYS	Per Request / Active Licenses on Unisys Mainframe
CCSU13370497-A	Unisys Mainframe – Software Transfer License – SMA OpCon	Per Request / Active Licenses on Unisys Mainframe
CCSU13370498-A	Unisys Mainframe – Software Transfer License – Sightline	Per Request / Active Licenses on Unisys Mainframe

Strategy Workshop Services

Service Attribute	*Service Attribute Description*	
Service Name	Cloud Transformation Workshop for Single Tower	
Detailed Description	This project focuses on the analysis of a single tower and its IT practices reviewing the current state, assessing gaps, making recommendations in the form of a roadmap where changes to the current state can provide quantifiable value. The workshop will diagnose, and prioritize the highest value actions that could be taken to improve the tower's overall quality and ROI. The typical workshop is a four week assessment for two consultants, and the four week workshop would focus on the single technology tower, and generate a generic engagement roadmap. Schedule would be contingent upon availability of all data at the start of the workshop.	
Service Customers / Users	Any affected agency/department.	
Service Prerequisites	None	
Request the Service	To request this service, submit a Service Request and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370499-A	Cloud Transformation Workshop for Single Tower	Per Workshop

Service Attribute	*Service Attribute Description*	
Service Name	Cloud Transformation Workshop	
Detailed Description	This project focuses on the analysis of datacenter workloads and IT practices and their effects on the economics of Cloud computing. This Cloud Transformation Workshop is a six weeks assessment for two consultants. The six week workshop would review up to 20 workloads on less than 125 servers and be contingent upon availability of all data at the start of the workshop.	
Service Customers / Users	Any affected agency/department.	
Service Prerequisites	None	
Request the Service	To request this service, submit a Service Request in the online Enterprise Services Catalog and select the Enterprise Services Catalog item using the above Service Name.	
Provider Part Number(s)	**Service Option Name**	**Orderable Unit / Restrictions per Unit**
CCSI13370500-A	Cloud Transformation Workshop	Per Workshop

Request for Proposal

RFP # 6100022698

Commonwealth of Pennsylvania
Office of Administration
Office for Information Technology

Data Center Computing Services

Schedule D

Transition Milestones

Milestones include the completion of all tasks, deliverables and interim milestones associated with such Milestone as set forth in the Transition Plan. The Earn Back period is thirty (30) calendar days from the Transition Milestone Due Date and applies to those Milestones indicated with "Y" in the Earn Back column. The Acceptance Criteria for each Milestone includes criteria described in Schedule F and Schedule K of the contract.

Note: If a Milestone is dependent on another Milestone and the first Milestone is missed, the subsequent Milestones remain in effect. An example is: if M-3 is missed, M-5 is still enforced.

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
M-1	Key Staffing	30 calendar days from Contract Effective Date	• Key Personnel team completed per Schedule G • Staffing plan approved • Detailed project organizational chart approved • Resumes for each key personnel listed on the team submitted • Staff contingency plan approved	$50,000 One-time	N	• Commonwealth review and approval
M-2	Contract Management Plan	45 calendar days from Contract Effective Date	• Delivery and acceptance of the following Deliverables from Schedule K: o D-11.01	$50,000 One-time	Y	• Commonwealth review and approval
M-3	Staffing	90 calendar days from Contract Effective Date	• Employee on-boarding completed o Identify positions that have been filled and are ready to work • Descriptions of Offeror's policies and training processes submitted and approved • Staff Tools fulfillment completed o Office Systems (PCs, printers, software) installed and operational – letter provided and approved	$150,000 One-time	Y	• Commonwealth review and approval

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
M-4	Datacenter Architecture Plan and Roadmap	90 calendar days from Contract Effective Date	• Delivery and acceptance of the following Deliverables from Schedule K: o D-01.01 o D-01.02 (Initial Deliverable Approval) o D-01.03 (Initial Deliverable Approval) o D-01.04 (Initial Deliverable Approval) o D-01.05 (Initial Deliverable Approval) o D-01.07 o D-03.01 o D-03.04 o D-03.08 o D-04.01 o D-04.05	$150,000 One-time	Y	• Commonwealth review and approval
M-5	Data Gathering	120 calendar days from Contract Effective Date	• Completion of Data Gathering o All data gathering checklists completed, validated, reviewed and approved • Delivery and acceptance of the following Deliverables from Schedule K: o D-10.01 • Completion, submittal and acceptance of data gathering report on B2B interface to Commonwealth's ITSM system that includes interfaces for the following:	$250,000 One-time	N	• Commonwealth review and approval

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			o Incident Management o Change Management o Problem Management o Known Errors o Request Management o Invoicing Process			
M-6	Detailed Transition Plan	180 calendar days from Contract Effective Date	• Completion and acceptance of the Detailed Transition Plan using Schedule M – Detailed Transition Plan • Delivery and acceptance of the following Deliverables from Schedule K: o D-05.01 o D-05.04 o D-05.10 • The Detailed Transition plan must contain: o An **overall (master) plan** which includes but is not limited to: ▪ Transition governance plan ▪ Transition risk and mitigation plan ▪ Due diligence timeline ▪ Configuration / testing verification ▪ Operational readiness o A **plan by Data Center** which includes but is not limited to: ▪ Transition governance plan ▪ Transition risk and mitigation plan	$150,000 One-time	N	• Commonwealth review and approval

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			▪ Due diligence timeline ▪ Configuration / testing verification ▪ Operational readiness o A **plan by Agency** which includes but is not limited to: ▪ Transition governance plan ▪ Transition risk and mitigation plan ▪ Due diligence timeline ▪ Configuration / testing verification ▪ Operational readiness o A **plan by Application** which includes but is not limited to: ▪ Transition governance plan ▪ Transition risk and mitigation plan ▪ Due diligence timeline ▪ Configuration / testing verification ▪ Operational readiness			
M-7	Commonwealth Compute Process Manual (CCPM)	120 calendar days from Contract Effective Date	• Delivery and acceptance of the following Deliverables from Schedule K: o D-02.01 o D-02.04 o D-02.09 o D-02.15 o D-02.17 o D-02.18 o D-02.23	$75,000 One-time	Y	• Commonwealth review and approval

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			o D-02.26 o D-02.29 o D-02.32 o D-02.37 o D-02.42 o D-02.47 o D-02.52 o D-02.57 o D-02.62 o D-02.67 o D-02.70 o D-02.75 o D-02.81 • Completion and Acceptance of final CCPM as listed within Schedule L of this contract. This includes but is not limited to: o Incident (including Security) o Problem o Change o Order/Request o Billing o Service Level			
M-8	Network Connectivity	120 calendar days from Contract Effective Date	• Completion and Acceptance of the Network Connectivity to the Commonwealth	$250,000 One-time	N	• Commonwealth review, testing and approval
M-9	Security	180 calendar days from	• Completion and acceptance of security architecture, solution, policies and	$250,000 One-time	N	• Commonwealth review and approval

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
		Contract Effective Date	procedures which included but is not limited to: o Delivery and acceptance of the following Deliverables from Schedule K: ▪ D-07.01 ▪ D-07.06 ▪ D-01.03 (Initial Deliverable Approval) ▪ D-09.01 ▪ D-09.02 o Implement security management plan o Implement security and firewall plan o Policies and procedures are in place for physical security o Policies and procedures are in place for data and network security o Policies and procedures are in place for personnel security, such as annual background checks o Security assessment is conducted to provide data safety and confidentiality			
M-10	ITSM System Integration	180 calendar days from Contract Effective Date	• Completion and Acceptance of Integration between Commonwealth's ITSM system and Offeror's ITSM System including but is not limited to: o Incident connectivity has been tested and incidents created and updated on either side flow back and forth between systems	$150,000 One-time	Y	• Commonwealth review and approval

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			o Problem connectivity has been tested and problems created and updated on either side flow back and forth between systems o Change requests connectivity has been tested and requests created and updated on either side flow back and forth between systems o Configuration items in both system CMDBs are reconciled o Test Invoices have been processed through the ITSM system to the Commonwealth's AP system o Reporting from Offeror's ITSM system is available to Commonwealth			
M-11	Financial Management	180 calendar days from Contract Effective Date	• Completion and acceptance of billing process and form of invoice approved • Schedule K Deliverable D-02.01 completed • Process implemented, tested and accepted providing an enterprise bill providing the details required by the Commonwealth	$75,000 One-time	Y	• Commonwealth review and approval
M-12	Operational Readiness	240 calendar days from Contract Effective Date	• Completion and acceptance of an Operational Readiness Report indicating Offeror is "Ready" to transition the Commonwealth's Applications and Services to other Datacenters. This report must include but is not limited to the following:	$150,000 One-time	N	• Commonwealth review and approval

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			o Delivery and acceptance of the following Deliverables from Schedule K: ▪ D-01.01 ▪ D-01.02 ▪ D-01.03 ▪ D-01.04 ▪ D-01.05 ▪ D-01.06 ▪ D-01.07 o Transition Project Office established and fully staffed o Program plan and architecture developed and approved by the Commonwealth o Processes and Tools implemented to support the transition change control, schedule, quality, communications, risk and issue management o Datacenter environment configured , tested and acceptance			
M-13	SSAE 16 Audit of EDC	12 months from Contract Effective Date	• Completion and Acceptance of SSAE 16 audit of the Commonwealth's EDC • Schedule K Deliverable D-08.02	$100,000 One-time	Y	• Commonwealth review and approval
M-14 (A)	DPH Transition Completed	18 months from Contract Effective Date	• Completion and acceptance of ALL applications transitioned from the DPH to new Datacenters which includes but is not limited to the following for each application:	$2,500,000 per month or partial month for six (6) months	N	• Commonwealth review and approval of work product plus assisting in data gathering, planning, ordering, implementing,

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			o High availability, backup and DR are operational for identified systems. o CCPM specific details for application are available in KMP. o Operations dashboards to report immediately on status and alerts for transitioned applications. o Service Level agreements are identified and supporting metrics in place. o System operational for scheduling and tracking of ticket-based tasks and incidents. o System is available to begin data collection to produce configuration, monitoring and management status reports. o Systems with DR plans have an updated DR plan and test scheduled. o Operational support assumed and workloads migrated. • High-Speed direct link to current DPH location is disconnected. • Signoff that all Services provided by DPH have been successfully transitioned			testing and accepting the transition of the applications
M-14 (B)	DPH Transition Completed	24 months from Contract Effective	• Completion and acceptance of ALL applications transitioned from the DPH to new Datacenters which includes but is not limited to:	$5,000,000 per month or partial month	N	• Commonwealth review and approval of work product plus assisting in data gathering, planning,

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
		Date	o High availability, backup and DR are operational for identified systems. o CCPM contains specific details for apps transitioned are available in KMP. o Operations dashboards are in place to report immediately on status and alerts for transitioned apps. o Service Level agreements have been identified and supporting metrics in place. o System is operational for scheduling and tracking of ticket-based tasks and incidents. o System available to begin data collection in order to produce configuration, monitoring and management status reports. o Systems with DR plans have a replacement plan and test scheduled. o Operational support has been assumed and workloads migrated. o High-Speed direct link to current DPH location is disconnected. o Signoff that all Services provided by DPH have been successfully transitioned			ordering, implementing, testing and accepting the transition of the applications
M-15	EDC Operational Transition Completed	12/31/2014	• Completion and acceptance of operational control and support of the EDC which includes but is not limited to the following:	$100,000 per month or partial month	N	• Commonwealth review and approval of work product plus assisting in data gathering, planning,

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			o Schedule K deliverable D-01 o Schedule K deliverable D-08.01 o Schedule K deliverable D-08.06 o Verification CMDB of record with Offeror's configuration info includes EDC assets and CI's o Service catalogs, processes, and procedures are transitioned o Multi environments/instances are available for identified systems o High availability, backup and DR are operational for identified system o CCPM specific details for applications are available in KMP. o Operations dashboards are in place to report immediately on status and alerts for apps o Service Level agreements have been identified and supporting metrics in place o System is operational for scheduling and tracking of ticket-based tasks and incidents o System is available to begin data collection in order to produce configuration, monitoring and management status reports o Transition orders completed and accepted by the Commonwealth			ordering, implementing, testing and accepting the transition of the applications
M-16	Department of Labor and Industry Datacenter	30 months from Contract	• Completion and acceptance of ALL applications transitioned from the DLI Datacenter to new Datacenters which	$5,000,000 One-time	N	• Commonwealth review and approval of work product plus assisting in data

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
	Transition Completed	Effective Date	includes but is not limited to the following: o Service catalogs, processes and procedures fully established, documented and approved o Multi environments and instances are fully functional for transitioned systems o High availability, backup and DR are operational for transitioned systems o CCPM contains specific details for apps transitioned are available in KMP o Operations dashboards are in place to report immediately on status and alerts for transitioned apps o Service Level agreements have been identified and supporting metrics in place o System is operational for scheduling and tracking of ticket-based tasks and incidents o System available to begin data collection in order to produce configuration, monitoring and management status reports o Transition orders completed and accepted by the Commonwealth			gathering, planning, ordering, implementing, testing and accepting the transition of the applications
M-17	Department of Revenue Datacenter Transition	30 months from Contract	• Completion and acceptance of ALL applications transitioned from the DOR Datacenter to new Datacenters which	$5,000,000 One-time	N	• Commonwealth review and approval of work product plus assisting in data

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
	Completed	Effective Date	includes but is not limited to the following: o Service catalogs, processes and procedures fully established, documented and approved o Multi environments and instances are fully functional for transitioned systems o High availability, backup and DR are operational for transitioned systems o CCPM contains specific details for applications transitioned are available in KMP o Operations dashboards are in place to report immediately on status and alerts for transitioned apps o Service Level agreements have been identified and supporting metrics in place o System is operational for scheduling and tracking of ticket-based tasks and incidents o System available to begin data collection in order to produce configuration, monitoring and management status reports o Transition orders completed and accepted by the Commonwealth			gathering, planning, ordering, implementing, testing and accepting the transition of the applications
M-18	Pennsylvania State Police Datacenter Transition	30 months from Contract	• Completion and acceptance of ALL applications transitioned from the PSP Datacenter to new Datacenters which	$5,000,000 One-time	N	• Commonwealth review and approval of work product plus assisting in data

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
	Completed	Effective Date	includes but is not limited to the following: o Service catalogs, processes and procedures fully established, documented and approved o Multi environments and instances are fully functional for transitioned systems o High availability, backup and DR are operational for transitioned systems o CCPM contains specific details for applications transitioned are available in KMP o Operations dashboards are in place to report immediately on status and alerts for transitioned apps o Service Level agreements have been identified and supporting metrics in place o System is operational for scheduling and tracking of ticket-based tasks and incidents o System available to begin data collection in order to produce configuration, monitoring and management status reports o Transition orders completed and accepted by the Commonwealth			gathering, planning, ordering, implementing, testing and accepting the transition of the applications
M-19	Department of Public Welfare Datacenter	30 months from Contract	• Completion and acceptance of ALL applications transitioned from the DPW Datacenter to new Datacenters which	$5,000,000 One-time	N	• Commonwealth review and approval of work product plus assisting in data

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
	Transition Completed	Effective Date	includes but is not limited to the following: o Service catalogs, processes and procedures fully established, documented and approved o Multi environments and instances are fully functional for transitioned systems o High availability, backup and DR are operational for transitioned systems o CCPM contains specific details for apps transitioned are available in KMP o Operations dashboards are in place to report immediately on status and alerts for transitioned apps o Service Level agreements have been identified and supporting metrics in place o System is operational for scheduling and tracking of ticket-based tasks and incidents o System available to begin data collection in order to produce configuration, monitoring and management status reports o Transition orders completed and accepted by the Commonwealth			gathering, planning, ordering, implementing, testing and accepting the transition of the applications

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
M-20	Department of Health Datacenter Transition Completed	30 months from Contract Effective Date	• Completion and acceptance of ALL applications transitioned from the DOH Datacenter to new Datacenters which includes but is not limited to the following: o Service catalogs, processes and procedures fully established, documented and approved o Multi environments and instances are fully functional for transitioned systems o High availability, backup and DR are operational for transitioned systems o CCPM contains specific details for apps transitioned are available in KMP o Operations dashboards are in place to report immediately on status and alerts for transitioned apps o Service Level agreements have been identified and supporting metrics in place o System is operational for scheduling and tracking of ticket-based tasks and incidents o System available to begin data collection in order to produce configuration, monitoring and management status reports o Transition orders completed and accepted by the Commonwealth	$5,000,000 One-time	N	• Commonwealth review and approval of work product plus assisting in data gathering, planning, ordering, implementing, testing and accepting the transition of the applications

UNISYS RESPONSE:

Transition milestones, including their timing, are documented in the Detailed Task Plan found in **Attachment 9 to Section 3.0 – Schedule M: Detailed Transition Plan.**

Request for Proposal

RFP # 6100022698

Commonwealth of Pennsylvania
Office of Administration
Office for Information Technology
Data Center Computing Services

Schedule E

Offeror Datacenter Locations

This page intentionally left blank.

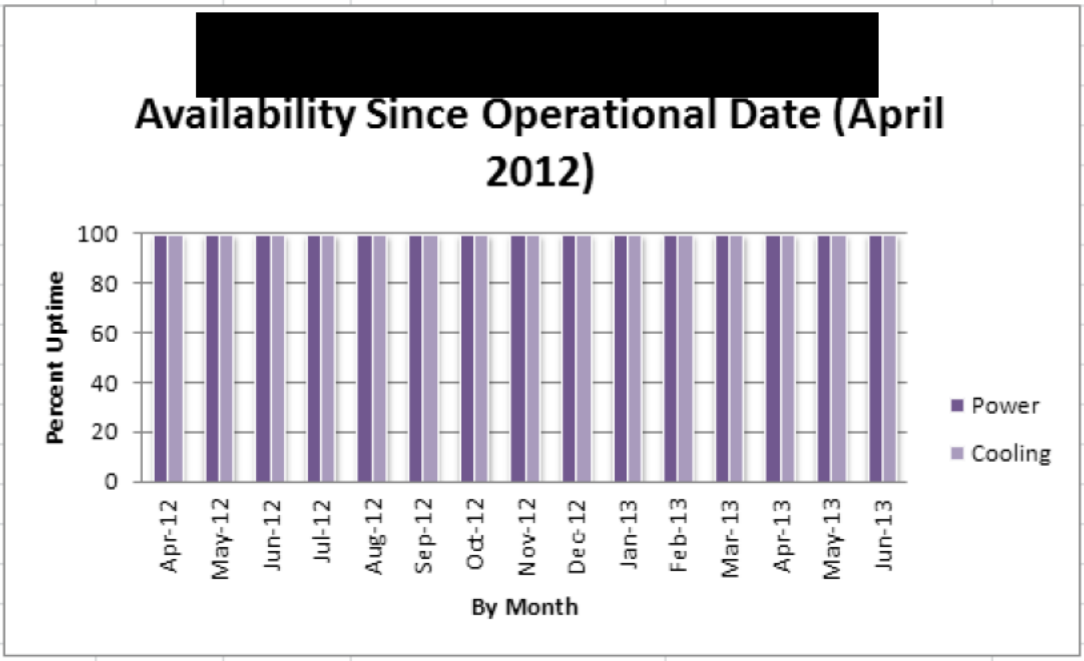
[The Offeror will list the address of proposed Datacenter locations that will host the Commonwealth's applications and data].

UNISYS RESPONSE:

Unisys [redacted]

- On the campus of [redacted]
- [redacted]
- Key data points:
  - Tier 3 equivalent facilities infrastructure with 2N+2 backup
  - Approximately [redacted] direct miles and [redacted] road miles between Harrisburg, Pennsylvania and [redacted]
  - Physical building security controls include 24x7 staffed guard stations and perimeter/interior video monitoring.
  - The Unisys area includes [redacted] square feet area supporting an active and protected electrical load up to 2.7 megawatts with a floor power density of 200 watts per square foot.
  - Floor space and power can be expanded.
  - Other [redacted] tenants occupy other buildings/vaults in this [redacted] building complex. Unisys occupies a private, secure, and fully isolated campus module.
  - The facility is accessible only by prior reservation or security clearance externally to the campus and through the facility's access-controlled passage ways via the security station and security doorways internally. Internal access without prior security clearance requires a security guard escort at all times
  - Availability report (on following page)

Month	Power	Cooling
Apr-12	100	100
May-12	100	100
Jun-12	100	100
Jul-12	100	100
Aug-12	100	100
Sep-12	100	100
Oct-12	100	100
Nov-12	100	100
Dec-12	100	100
Jan-13	100	100
Feb-13	100	100
Mar-13	100	100
Apr-13	100	100
May-13	100	100
Jun-13	100	100



Unisys [redacted]

- On the campus of the Unisys [redacted] facility
- [redacted]
- Key data points
  - Tier 3 equivalent facilities infrastructure
  - Approximately [redacted] direct miles and [redacted] road miles between Harrisburg, Pennsylvania and [redacted]
  - Physical building security controls include 24x7 staffed guard stations and perimeter/interior video monitoring
  - The Unisys [redacted] Data Center is a [redacted]-square-foot facility that is home to two distinct data centers: The main data center is a [redacted]-square-foot raised floor facility. The second data center ([redacted] consists of [redacted] square feet of raised floor that is Tier III compliant.
  - The Commonwealth area includes [redacted] square feet of area supporting an active and protected electrical load of 1.4 megawatts.
  - The Commonwealth IT environment will be isolated to a private, secure and fully isolated module – [redacted]
  - The facility is accessible only by prior reservation or security clearance at the security station and doorways internally. Internal access without prior security clearance requires a security guard escort at all times.
  - Availability Report (on following page)

Domain - Type	WW Enterprise Compute Measures	Nov-12	Dec-12	Jan-13	Feb-13	Mar-13	Apr-13	Goal PE 4Q12	Goal PE 1Q13	Goal PE 2Q13	Goal PE 3Q13	Goal PE 4Q13
Data Center - Capacity	Data Center Power Capacity %	38.0%	38.3%	38.3%	38.3%	29.1%	59.3%	>= 20.0%	>= 20.0%	>= 20.0%	>= 20.0%	>= 20.0%
Data Center - Capacity	Data Center Raised Floor Capacity %	24.1%	31.8%	31.8%	31.8%	35.4%	46.6%	>= 20.0%	>= 20.0%	>= 20.0%	>= 20.0%	>= 20.0%
ECP - Service Management	Data Center Up Time % - Avail/Year	100.000%	100.000%	100.000%	100.000%	100.000%	100.000%	>= 99.980%	>= 99.980%	>= 99.980%	>= 99.980%	>= 99.980%
ECP - Service Management	Data Center Up Time % - Avail/Year (T1)	100.000%	100.000%	100.000%	100.000%	100.000%	100.000%	>= 99.973%	>= 99.973%	>= 99.973%	>= 99.973%	>= 99.973%
ECP - Service Management	Data Center Up Time % - Avail/Year (T2)	100.000%	100.000%	100.000%	100.000%	100.000%	100.000%	>= 99.977%	>= 99.977%	>= 99.977%	>= 99.977%	>= 99.977%
ECP - Service Management	Data Center Up Time % - Avail/Year (T3)	100.000%	100.000%	100.000%	100.000%	100.000%	100.000%	>= 99.991%	>= 99.991%	>= 99.991%	>= 99.991%	>= 99.991%

Domain - Type	NA Enterprise Compute Measures	Nov-12	Dec-12	Jan-13	Feb-13	Mar-13	Apr-13	Goal PE 4Q12	Goal PE 1Q13	Goal PE 2Q13	Goal PE 3Q13	Goal PE 4Q13
Data Center - Capacity	Data Center Power Capacity %	53.8%	54.3%	54.3%	54.3%	36.2%	62.5%	>= 20.0%	>= 20.0%	>= 20.0%	>= 20.0%	>= 20.0%
Data Center - Capacity	Data Center Raised Floor Capacity %	22.5%	32.8%	32.8%	32.8%	26.5%	40.3%	>= 20.0%	>= 20.0%	>= 20.0%	>= 20.0%	>= 20.0%
ECP - Service Management	Data Center Up Time % - Avail/Year	100.000%	100.000%	100.000%	100.000%	100.000%	100.000%	>= 99.980%	>= 99.980%	>= 99.980%	>= 99.980%	>= 99.980%
ECP - Service Management	Data Center Up Time % - Avail/Year (T1)	100.000%	100.000%	100.000%	100.000%	100.000%	100.000%	>= 99.973%	>= 99.973%	>= 99.973%	>= 99.973%	>= 99.973%
ECP - Service Management	Data Center Up Time % - Avail/Year (T2)	100.000%	100.000%	100.000%	100.000%	100.000%	100.000%	>= 99.977%	>= 99.977%	>= 99.977%	>= 99.977%	>= 99.977%
ECP - Service Management	Data Center Up Time % - Avail/Year (T3)	100.000%	100.000%	100.000%	100.000%	100.000%	100.000%	>= 99.991%	>= 99.991%	>= 99.991%	>= 99.991%	>= 99.991%

- On the campus of [redacted]
- [redacted]
- Key data points
  - Tier 3+ equivalent facilities infrastructure.
  - Utilized if the optional subscription cold-site DR services for the IBM mainframe are continued.

Request for Proposal

RFP # 6100022698

Commonwealth of Pennsylvania

Office of Administration

Office for Information Technology

Data Center Computing Services

Schedule F

COPA Datacenter Statement of Work

Contents

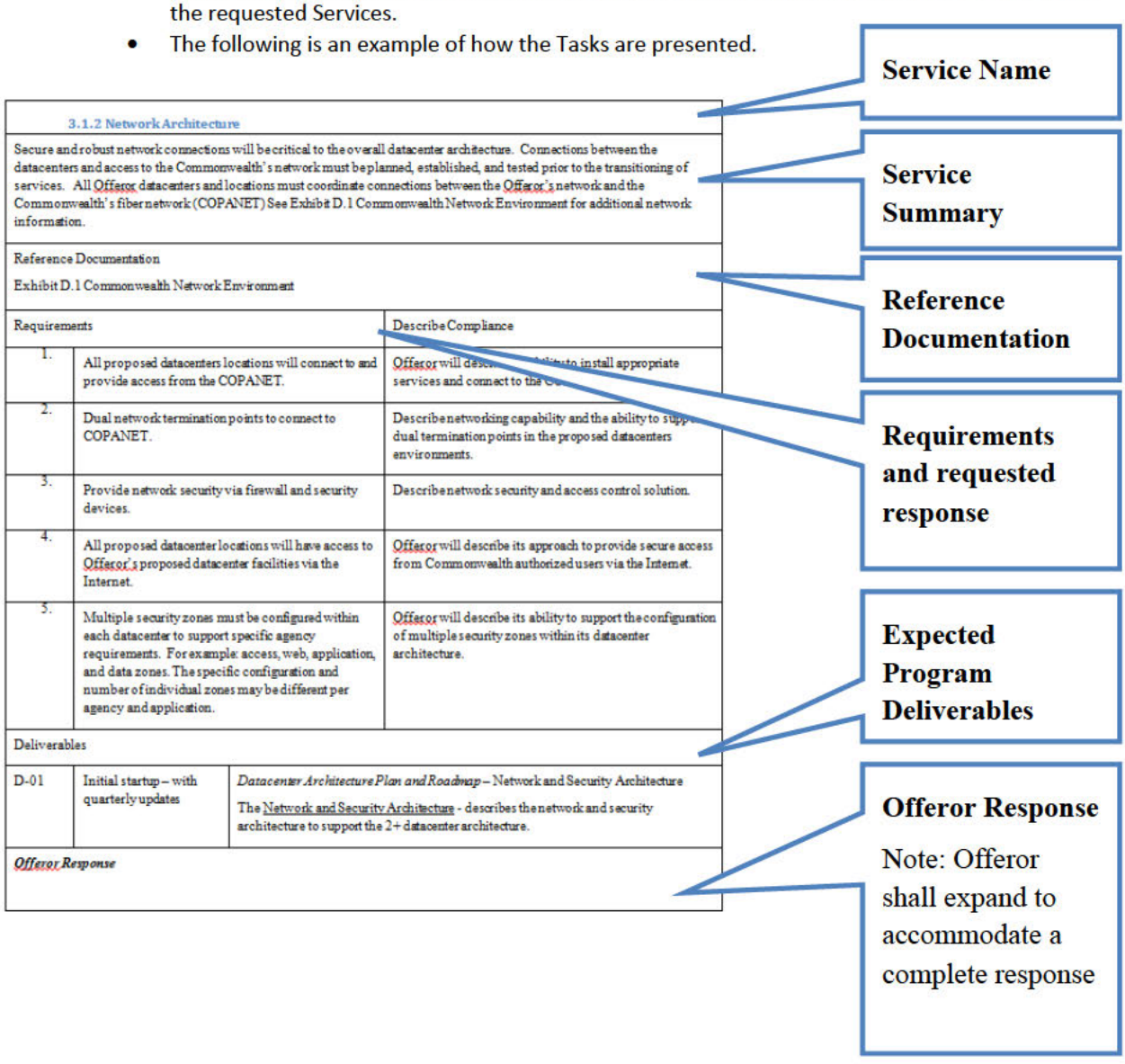
1 Offeror Guidelines 3
1.1 Offeror Instructions 3
2 Program Objectives and Summary Solution Requirements 4
2.1 Program Objectives 4
2.2 Service Level Agreements 6
2.3 Target Solution Requirements Overview 6
2.3.1 Target Datacenter 2+ Architecture 6
2.3.2 IP conversion strategy 7
2.3.3 Common Services Portfolio 8
2.3.4 Data Protection 9
2.3.4 Transition Services 20
3 Tasks 20
3.1 Establish Datacenter Architecture 20
3.1.1 Multi Datacenter Environment (2+ Architecture) 22
3.1.2 Network and Security Architecture 37
3.1.3 Datacenter Architecture and Technology 51

1 Offeror Guidelines

This Schedule contains the primary scope of Services required to support the Commonwealth's Enterprise Datacenter Services program. The Offeror must respond to the requirements contained in this Schedule according to the instructions provided below.

1.1 Offeror Instructions

- The Offeror's response to the RFP must reflect and comply with the information contained in this Schedule and any Referenced Schedules and Exhibits.
- The Offeror must provide responses to the section 3 Tasks. After reviewing each of the service requirement tables, the Offeror should provide its response. Responses must address the stated requirements as well the additional information on Offeror's approach and how it would deliver the requested Services.
- The following is an example of how the Tasks are presented.



3.1.2 Network Architecture		
Secure and robust network connections will be critical to the overall datacenter architecture. Connections between the datacenters and access to the Commonwealth's network must be planned, established, and tested prior to the transitioning of services. All Offeror datacenters and locations must coordinate connections between the Offeror's network and the Commonwealth's fiber network (COPANET) See Exhibit D.1 Commonwealth Network Environment for additional network information.		
Reference Documentation Exhibit D.1 Commonwealth Network Environment		
Requirements		Describe Compliance
1.	All proposed datacenters locations will connect to and provide access from the COPANET.	Offeror will desc… ability to install appropriate services and connect to the C…
2.	Dual network termination points to connect to COPANET.	Describe networking capability and the ability to supp… dual termination points in the proposed datacenters environments.
3.	Provide network security via firewall and security devices.	Describe network security and access control solution.
4.	All proposed datacenter locations will have access to Offeror's proposed datacenter facilities via the Internet.	Offeror will describe its approach to provide secure access from Commonwealth authorized users via the Internet.
5.	Multiple security zones must be configured within each datacenter to support specific agency requirements. For example: access, web, application, and data zones. The specific configuration and number of individual zones may be different per agency and application.	Offeror will describe its ability to support the configuration of multiple security zones within its datacenter architecture.
Deliverables		
D-01	Initial startup – with quarterly updates	*Datacenter Architecture Plan and Roadmap* – Network and Security Architecture The Network and Security Architecture - describes the network and security architecture to support the 2+ datacenter architecture.
Offeror Response		

2 Program Objectives and Summary Solution Requirements

2.1 Program Objectives

The Commonwealth is seeking to implement a new datacenter service model that will provide various infrastructures/computing platforms to service the needs of the Commonwealth in a secure and flexible manner. This initiative will realize the following objectives:

- Provide a reliable, flexible, secure, and robust IT infrastructure to support the transformation of the Commonwealth into an information-focused organization.
- Provide a multiple datacenter architecture utilizing the Offeror's proposed datacenter assets that will support the current and future capacity and service level demands.
- Include primary support for the Commonwealth's Enterprise Datacenter ([redacted] operations and its computing assets including but not limited to datacenter facilities operations and infrastructure support (see **Exhibits D.1 through D.7** [redacted] Exhibits for description of the facility, servers, storage and tape equipment).
- Leverage Offeror's established processes and tools necessary to ensure consistent and predictable pricing to facilitate accurate and timely budget projections.
- Provide engineering support that will anticipate changes in business and technical requirements and make recommendations for staying current with industry best practices.
- Ensure that the Offeror's datacenters adhere to the Commonwealth's contractual, regulatory, and policy compliance requirements for security, architecture, and systems development life cycle (SDLC) standards.
- Establish a tiered service/capability to support high-availability hosting, backup, and disaster recovery (DR) Services to maintain continuity of government operations.
- Provide multiple environments and instances to support the enterprise application portfolio. For example; Development, Integration, System / User Acceptance Test (SAT/UAT), Training, load Testing, Pre-Production and Production.
- Continue to consolidate Commonwealth datacenters to achieve cost savings, energy consumption reductions, optimal space utilization, and improvements in IT asset utilization in accordance with the government-wide datacenter consolidation initiative currently underway.

Currently, Commonwealth datacenter resources are decentralized, owned and operated under multiple datacenter service catalogs, processes and procedures. At times, this presents the Commonwealth with barriers to establishing interoperability between datacenters, implementing standard processes and procedures for datacenter oversight, and ensuring compliance with the same standards for datacenter operations. To resolve these issues, the Commonwealth intends, under this single procurement vehicle, to contract with a service provider that currently owns,

maintains and operates a group of geographically dispersed world-class datacenters (meeting or exceeding Tier 3 standards) located in the continental United States.

To satisfy the Commonwealth diverse datacenter requirements, the Offeror must be capable of providing the necessary infrastructure for the following critical purposes:

- Provide production, development and hosting of new and legacy business applications and databases that run on mainframes (IBM and Unisys), mid-ranges and distributed platforms
- Support options for high-availability, backup/recovery, and multiple levels of DR Services in support of the Commonwealth.

The Offeror's datacenter architecture must consist of multiple geographically dispersed datacenters, referred below as a 2+ (two-plus) architecture. The Offeror must utilize the [redacted] as one of its datacenters and propose a minimum of one additional datacenter to meet the 2+ architecture requirement. It is the Offeror's option to utilize the [redacted] as one of its primary datacenters within its proposed solution. It is the Commonwealth's requirement that the Offeror datacenters will have the ability to provide multiple levels of DR Services in the event of a disaster, which must also include an option to support high availability (HA) application infrastructures.

The Offeror is responsible for ensuring successful delivery of IT infrastructure Services, providing the Commonwealth with visibility into (performance, capacity, security, SLA's etc.), as well as, working in partnership with the Commonwealth as required to ensure seamless operations. In turn, the Commonwealth's role will be to provide oversight to ensure that the Offeror is delivering agreed-upon Services and that the business requirements are clearly communicated and satisfied, and provide timely feedback on contractor performance. Commonwealth agencies, OA/OIT and the Offeror will work together on IT planning, including service and capacity planning, strategic and tactical planning, and IT resource and budget planning. The Commonwealth believes that this combination of industry knowledge, government oversight, and collaboration will result in successful partnership between the private sector and the Commonwealth.

The datacenter approach must provide a computing infrastructure that delivers reliable, effective and technologically current Services seamlessly to the Commonwealth in a cost-effective manner. The cost for those Services must remain less than the cost the Commonwealth would have incurred for providing the same infrastructure itself. Applications hosted in the Offeror's datacenters must meet Quality of Service (QoS) requirements as determined by the Commonwealth agency application owners. The Commonwealth will avoid capital expenditure by acquiring Services through Capacity on Demand. The Commonwealth agencies will consume resources as a service and pay only for those resources that it uses. The Commonwealth and Offeror must engage in proactive oversight of datacenter operations. The Commonwealth requires visibility into the Offeror's management practices and effective monitoring channels that include the following:

- Program and project progress reports that track milestones, deliverables, risks, and financial data.
- Commonwealth Computing Procedures Manual (CCPM) that provides up-to-date detailed description of all processes and procedures used to support the computing needs of the Commonwealth via the Offeror's Knowledge/Service Management Portal (KMP). The CCPM must contain specific sections dedicated to the operational procedures for each Commonwealth datacenter customer.
- Scheduling and tracking of ticket-based tasks and incidents.
- Operations dashboards with status and alerts based on real-time and historic data collected by instruments, agents, scanners, and logs that monitor the hosted applications, batch operations, network, security, and service performance measures.
- Other configuration, monitoring and management status reports as needed.
- Recommendations and offerings by the Offeror for improved processes and procedures for delivery of Services that are based on a program of continuous quality and process improvement as implemented by the Offeror.

2.2 Service Level Agreements

The Commonwealth has proposed a baseline set of Service Levels which the Offeror is required to consider when developing its proposed solution. The Offeror is expected to provide multiple service tiers and associated service levels within each service offered. The Offeror is also required to have or implement a quality and process improvement program that focuses not on just meeting minimum requirements but on meeting or exceeding the target requirements.

2.3 Target Solution Requirements Overview

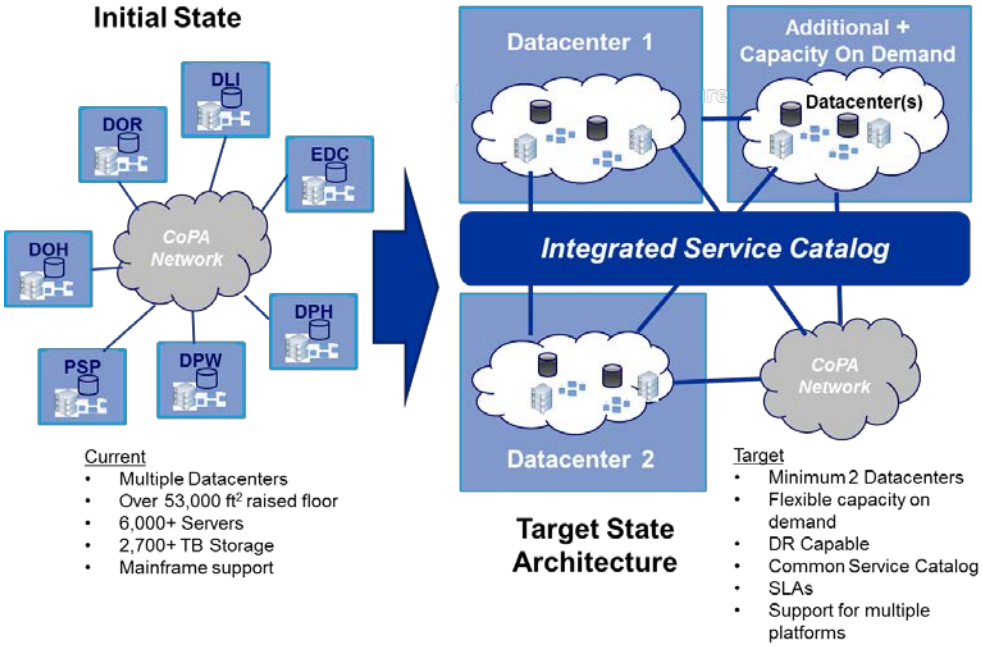
A key outcome of the Commonwealth datacenter strategy is to transition from the current individually managed datacenters with different levels of service to enterprise level datacenter architecture with a common set of basic Services combined with available specialized Services dependent upon specific customer requirements. To facilitate this request for Services, the Commonwealth has structured the solution requirements into three areas, as follows:

- Transition Services;
- Target Datacenter 2+ Architecture (includes operations support for the Commonwealth's [redacted] and
- Common Services Portfolio

2.3.1 Target Datacenter 2+ Architecture

The target architecture must leverage a minimum of two geographically separated datacenters located in the continental United States that would allow for enhanced disaster recovery capabilities as well as leverage excess capacity (virtual capacity on demand). The Commonwealth requires that the architecture include operations support for the [redacted] The Offeror must explain how it can leverage additional capacity from other datacenter resources within its provider network to satisfy the needs of the Commonwealth. The architecture will

include support for multiple computing platforms including but not limited to x86 (physical and virtual), midrange, mainframes, and storage systems. All of the Commonwealth computing workloads must be transitioned from the current state to the new target state architecture.



The 2+ datacenter architecture must include secure redundant network connections to the Commonwealth's network and the Internet. Offeror network connections must terminate at different end points within the Commonwealth's network. The Offeror is expected to implement a multi DR solution to limit the impact of any disruptive event at any datacenter location. This requirement is targeted for all systems that are currently covered by a DR solution. The solution must also have the capability to support future disaster recovery requirements by providing tiered DR capability within its datacenters.

Each datacenter must have the ability to support multiple security and network zones to support specific agency requirements. For example: access, web, application, and data zones. The specific configuration and number of individual zones may be different per agency and application.

To support the potential of future demand and Services beyond the capacity of the two datacenters, the Offeror must explain how it can leverage additional capacity from other datacenter resources within its provider network.

2.3.2 IP conversion strategy

The Offeror shall provide an IPv6 strategy which includes an enterprise migration plan to take the Commonwealth from the IPv4 address format to the IPv6 format.

The Offeror shall provide an infrastructure and equipment that supports IPv6 andIPv4, except were limited due to the requirement that the Initial transition approach of the Commonwealth's

mainframe and SAP environments must be as close to the Commonwealth's current configuration as possible. As technology refreshes replace this equipment, the infrastructure and equipment shall support IPv6 andIPv4

2.3.3 Common Services Portfolio

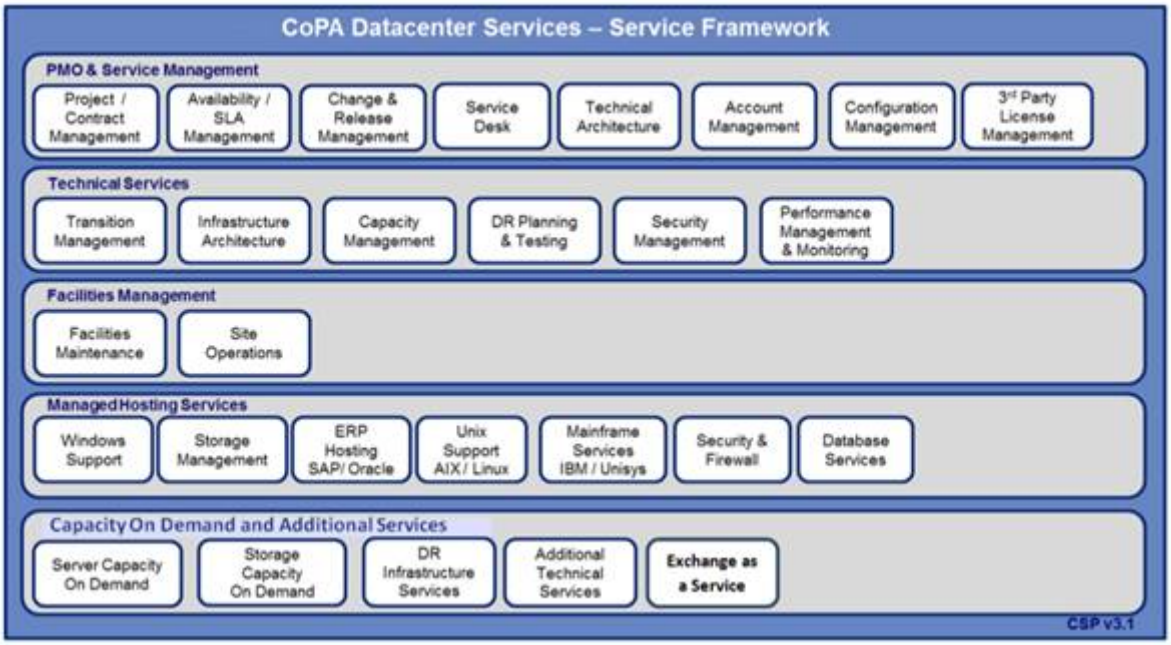
Based on the review of current and future requirements as well as industry offered Services; the following five (5) Key Services Areas will be used as a framework for the new datacenter common portfolio of Services.

Key Service Area Framework

	Key Service Area	Service Overview
1	Program Management Office (PMO) & Service Management	Provides for overall project management and operational service management (e.g. PMO, Account, Availability, Service Level Agreement (SLA))
2	Technical Services	Technical support services resources (e.g. Transition Management, Infrastructure Architecture, Capacity Planning)
3	Facilities Management	Facility operational support services (e.g. Facility Management, Operations Support)
4	Managed Hosting Services	Managed hosting/platform services for existing and future applications (e.g. Windows, Unix, SAP Hosting, Mainframe)
5	Capacity on Demand and Additional Services	Provides for additional capacity on demand offerings to support disaster recovery or increased demand for server and storage infrastructure (e.g. Cloud-centric offerings, Infrastructure as a Service (IaaS), Platform as a Service (PaaS)). Also access to additional skilled technology resources if required.

The Offeror is required to provide a complete set of Services within these service areas. The anticipated target Services are presented below and the requirements are further detailed in the Task section that follows.

Expanded Services Framework



2.3.4 Data Protection

The Offerors solution shall provide security of Commonwealth data. Offerors shall describe how they will ensure that all data (at rest and in transit) is kept secure and confidential. If Offerors proposed solution involves data residing or routing outside the continental United States; the Offeror shall disclose this in their proposal and describe how the data will be kept secure, confidential, and meet the security requirements as described in this RFP.

Offeror shall provide data protection Services including Data Loss Prevention (DLP) and Database Firewall (DBFW) Services to identify, monitor and protect sensitive and confidential Citizen Personal Identifiable Information (PII) in use, data in transit, and data at rest through deep content inspection and analysis of information exchange both at data storage locations and administrative/access endpoints.

Reference Documentation

Requirements		Describe Compliance
1.	DLP • Discover confidential data wherever it is stored, inventory sensitive data, and automatically manage data cleanup. • Monitor confidential data usage and provide enterprise visibility. • Enforce security policies to proactively secure data and prevent confidential data from leaving Commonwealth systems. • Manage policies across the enterprise, remediate and report on incidents, and detect content from centralized management platform.	Offeror must describe their approach to discover, manage, monitor, and enforce security for confidential data to meet Data Loss Prevention requirements.
2.	DBFW • Alert or block database attacks and abnormal access requests, in real time to protect against database attacks including SQL injection, Buffer overflow, Denial of Service. • Detect and patch database software vulnerabilities • Provide both agent based and network based database activity monitoring. • Audit all access to sensitive data by privileged and application users, and enforce corporate policies on data usage • Provide centralized management and advanced analytics • Discover new databases and database objects in scope for security and compliance projects and automatically apply appropriate protection and audit policies	Offeror must describe their approach to alert, detect, audit, monitor, manage, and discover attacks to meet Database Firewall requirements.
Deliverables		
Deliverables are defined in **Schedule K – Key Program Deliverables**		

Offeror Response

Introduction

"The wealth of personally identifiable information (PII) and sensitive business data makes states attractive targets for cybercriminals and hacktivists." – 2012 Deloitte-NASCIO cybersecurity study.

The Unisys team understands the importance that the Commonwealth places on safeguarding the privacy of and confidentiality of the Personally Identifiable Information (PII) entrusted by the Commonwealth's residents. Using our experience providing security and privacy services for over 12 years, the Unisys team will help the Commonwealth establish a data protection program that addresses evolving cyber threats.

State Government agencies hold a comprehensive repository of citizen PII, medical, and financial data. When such data is lost, it can spur citizen outrage, mistrust and attract media attention. Today's increasingly connected State Government IT infrastructure is under constant threat of unauthorized access or disclosure of sensitive data and attacks originating from cyber-criminal groups and hackers. This is evident from the recent data breach incidents in the State of South Carolina and in the State of Utah.

The dynamic evolution of the cybersecurity regulatory reforms, introduction of Health Information Exchanges (HIE) and Health Insurance Exchanges (HIX), and the use of electronic citizen data for online transactions presents significant pressure on the Commonwealth to address the ever-mounting security and privacy challenges. Further compounding this environment is the urgent need to address cyber security in order to mitigate the threat of disruption to the Commonwealth's operations and services. Citizen and business partner data, critical cyber infrastructure, and even national security can be compromised by deliberate attacks, cyber-wrongdoing, inadvertent security lapses, fraud and new vulnerabilities.

The Unisys team uses its time-tested **privacy and data protection methodology** to help the Commonwealth adopt an enterprise data protection program that robustly secures and keeps Commonwealth data confidential. Our solution uses both Data Loss Prevention (DLP) and Database Firewall (DBFW) to appropriately identify, monitor and protect sensitive and confidential citizen PII in use, data in transit, and data at rest at the data storage server locations and data center egress points. Our solution does not involve data residing or routing outside the continental United States. The Unisys team's solution focuses on both the technological solution and the "people and process" to support and interface with the technology solution, as illustrated in **Figure 2.3.4-1**:

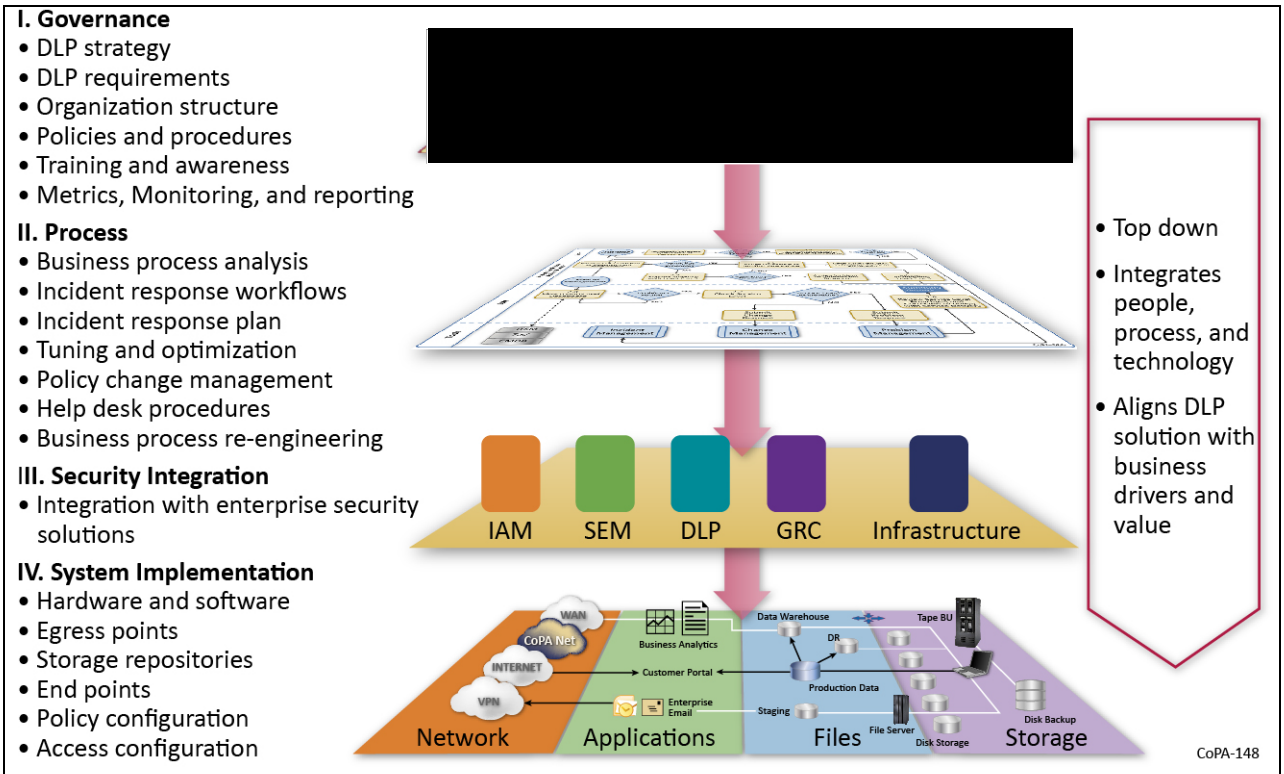


Figure 2.3.4-1. The Unisys Team's Holistic DLP Approach

Our Approach

The Unisys team has tailored its data protection methodology to meet the Commonwealth's data protection needs of preventing inappropriate storage, use, sharing, and transfer of confidential information through the design and implementation of data loss prevention and Web Application and Database firewall solutions. In the following sections, we have outlined our approach to designing a target architecture and outlining hardware and software requirements, developing an implementation plan for incremental roll-out, and implementing data at rest, data in motion, and data in use components including configuration, installation, and administration of DLP and DB firewalls.

1 DLP

1A Discover confidential data wherever it is stored, inventory sensitive data, and automatically manage data cleanup.

The first step in our DLP implementation process is **Scope and Plan**. The Unisys Team works with the Commonwealth and data center stakeholders to define the DLP requirements including business and technical requirements, sensitive data definition and network and storage details for databases. The Team also identifies the data server storage and the solution hosting environment. Then the team identifies the data center network infrastructure end points and egress points that handle confidential data.

Next, the second step in our process, **Discover and Classify Data**, begins. This step occurs during the transition phase of the contract. Confidential data is discovered during transition as part of the development of the initial security plan. We perform data discovery and data

classification assessment to indicate level of sensitivity of Commonwealth's PII and identify presence of PII data at rest. This step includes the following activities – Data classification and Data discovery, as detailed below:

- ***Activity 1 – Data Classification:*** We conduct and facilitate five workshops with the Commonwealth stakeholders to define a data classification standard for the Commonwealth's Personally Identifiable Information (PII), based on sensitivity of PII. For example, some of the categories include:
  - Special handling PII (that contains SSN, driver license number, FEIN, and Medicare ID)
  - Protected Health Information
  - Individual information
  - Sensitive PII (such as racial/ethnic origin, religious/philosophical beliefs, Trade-union membership and criminal convictions).
- ***Activity 2 – Data Discovery:*** We perform an assessment using the Symantec Data Loss Prevention (DLP) solution's data discovery tool on the Commonwealth selected data center IT infrastructure consisting of servers and databases to identify the PII data at rest. We perform the following tasks as part of this activity:
  - Document the results of the data discovery assessment in the IT asset inventory (inventory of sensitive data)
  - Use the data center security risk framework to identify appropriate data encryption requirements to appropriately protect the PII data and meet the relevant regulations, policies and standards.

The third step in our DLP Implementation Process is **Assess Data Loss Threats**. In this step, we identify the high risk infrastructure within the COPA network. We work with the Commonwealth and data center stakeholders to identify the IT infrastructure, locations, and business units that present the most risk to the Commonwealth (handling PII). We use the initial security plan/security management plan to identify the regulatory requirements, technical, operational, and other requirements for data protection solution functionality and processes to mitigate the risks identified.

The next step in our Process is **Define Data Protection Governance.** We collaborate with the Commonwealth and data center stakeholders to develop a governance model that will define required roles, responsibilities, and processes necessary to manage the data protection program effectively through its life cycle. The governance model will include:

- Identification of high risk infrastructure
- Personnel roles and responsibilities
- Solution configuration and maintenance
- Reporting and alerting procedures
- Training and awareness plan
- Key metrics for monitoring and reporting, and automatic data cleanup and data retention requirements.

1B Monitor confidential data usage and provide enterprise visibility.

The next step in our Process is **Design DLP Solution and Assess Infrastructure Readiness.** The Unisys team works with key Commonwealth stakeholder and the Unisys information security manager to assess infrastructure readiness for the rollout of the data protection program. This activity involves:

- Reviewing the data storage inventory of Citizen PII
- Identifying the critical infrastructure to support pilot rollout and identify readiness to support enterprise rollout
- Prioritizing data protection solution implementation within the Commonwealth defined data center migration groups
- Designing the network DLP solution on data center egress points in the Commonwealth's Enterprise Data Center environments
- Identifying the critical data storage server locations that requires periodic data at rest monitoring using the data discovery solution
- Identifying network DLP policies to monitor confidential data usage and provide enterprise visibility.

Once the appropriate DLP policies have been defined, they are implemented in the next two steps. Enterprise visibility is provided through the Security Incident and Event Monitoring (SIEM) tool during the Monitoring and Maintenance phase of the DLP Implementation Process.

1C Enforce security policies to proactively secure data and prevent confidential data from leaving Commonwealth systems.

In step 6, **Configure and Deploy pilot DLP solution**, Unisys works with the Commonwealth key stakeholders and the Unisys information security manager to establish and operationalize a pilot implementation plan for configuration and implementation of Symantec network DLP solution on one egress point. We implement five standard (out-of-the-box) network DLP policies selected by the Commonwealth as part of the pilot implementation. Once the pilot has run successfully, Step 7, **Configure and Deploy Enterprise DLP solution,** rolls out the DLP to the Commonwealth Enterprise. The Unisys team again works with the Commonwealth stakeholders and the Unisys information security manager to install and configure Symantec network DLP solution (using standard out-of-the-box policies) on the data center egress points, selected by the Commonwealth. These policies represent the security policies that are enforced by the DLP solution to proactively secure data and prevent confidential data from leaving Commonwealth systems.

1D Manage policies across the enterprise, remediate and report on incidents, and detect content from centralized management platform.

The 8th and last step of the DLP Implementation Process is a phase. During the **Maintain and Monitor** phase, Unisys staff maintains and monitors the operation of the DLP solution on an ongoing basis, including configuring the solution on additional egress points and managing and updating network DLP policies as necessary for the Enterprise. Unisys uses the DLP to prevent inappropriate storage, use, sharing, and transfer of confidential information. The DLP appliance outputs data to the SIEM tool for data correlation and centralized reporting. The SIEM, a centralized management platform, allows Unisys security staff to detect, report, and remediate data loss incidents.

1E Offeror must describe their approach to discover, manage, monitor, and enforce security for confidential data to meet Data Loss Prevention requirements.

The Unisys Team approach to discover, manage, monitor, and enforce security for confidential data to meet Data Loss Prevention requirements is detailed above in response to requirements 1.A – 1.D.

2 DBFW

2.A Alert or block database attacks and abnormal access requests, in real time to protect against database attacks including SQL injection, Buffer overflow, Denial of Service.

The Database Firewall (DBFW) Implementation Process is very similar to the DLP Implementation process. The first step in our Database Firewall (DBFW) Implementation Process is **Scope and Plan.** As in the DLP Implementation Process, the Unisys team works with the Commonwealth stakeholders and the designated information security manager to define the DBFW requirements, including business and technical requirements, sensitive data definition and network and storage details for databases. We identify the data server storage and solution hosting environment. The team also identifies the data center network infrastructure end points and egress points that handle confidential data.

The second step in our Database Firewall (DBFW) Implementation Process is **Design DBFW solution**. In this step, the Unisys team works with the Commonwealth stakeholders to identify the database instances that require the periodic/continuous monitoring using the DBFW solution including automatic detection of new databases within that instance. We identify and define the standard (out of the box) and complex DBFW policies to help alert or block database attacks and abnormal access requests and help protect against database attacks such as SQL injection, buffer overflow and denial of service. Next, our team identifies the critical infrastructure to support a pilot rollout of the DBFW solution and identifies readiness to support enterprise rollout. We define a pilot implementation plan to configure and implement the DBFW solution on three critical database instances. We also define an enterprise rollout plan to configure and implement DBFW solution implementation on the data center standard Oracle, Microsoft SQL Server, MySQL and IBM DB2 databases (selected by the Commonwealth).

In the next step, **Implement and Configure**, the Unisys team installs, configures and tests the data protection solution (using standard out-of-the-box policies) as part of the pilot and then the enterprise implementation to support DBFW solution on databases selected by the Commonwealth.

The last step, **Monitor and Maintain**, is the phase where Unisys staff maintains and monitors the operation of the DBFW solution on an ongoing basis, including configuring the solution on additional critical database instances and updating DBFW policies as necessary. Unisys uses the DBFW solution to alert and block database attacks and abnormal access requests. The DBFW solution outputs data to the SIEM tool for data correlation and centralized reporting.

Features of our solution:

- Continuous audit of all access to sensitive data by privileged and application users
- Alert on abnormal access requests and database attacks, in real time

- Accelerated incident response and forensic investigation through centralized management and advanced analytics
- Audit reports produced to demonstrate compliance with regulatory requirements.
- Databases and objects in scope for Compliance and Security Projects identified

2.B Detect and patch database software vulnerabilities.

The Unisys security team uses the DBFW solution to configure and enable standard database vulnerability detection rules/policies. These database vulnerability signatures are based on the vendor provided knowledge base that will be kept up-to-date by the Unisys security team.

Identifying and blocking potential database vulnerability exploit attempt: Using the updated database vulnerability signatures, the DBFW solution rules/policies identify and block potential exploit attempts. This helps in preventing potential exploitation of recently released database vulnerability signatures.

Patch management: In addition to the above described approach to use the DBFW to block potential database vulnerability exploits, we will notify the Commonwealth Chief Information Security Officer and the system owner and work with them to identify a patch for the impacted database system. The team will work will the Commonwealth to develop a mitigation plan and using the existing data center change management process, the database software will be patched to address the vulnerability (after the patch is provided by the database vendor and tested in a lower environment). As necessary, the Unisys security team will develop custom rules to prevent these vulnerabilities from reoccurring.

2.C Provide both agent based and network based database activity monitoring.

The Unisys team's DBFW solution provides both agent based and network based database activity monitoring. Our solution uniquely enables us to optimize our database activity monitoring implementation by combining agent-based monitoring and network activity monitoring. The database agents can be configured for monitoring local privileged activity exclusively, or for monitoring all database activity. This hybrid architecture provides the ability to perform comprehensive database auditing. The Unisys team works with the Commonwealth for the following scenarios:

- ***Privileged activity monitoring***: the database appliance monitors network activity and the agent is configured to monitor only local, privileged activity. This configuration provides complete coverage of all paths to the databases with minimal impact on the database server.
- ***Full agent-based monitoring***: the agent is configured to monitor database activity regardless of its source (network and local, privileged activity).This configuration is typically used when an appliance cannot be deployed in front of the database.

2.D Audit all access to sensitive data by privileged and application users, and enforce corporate policies on data usage.

The DBFW solution monitors and maintains an audit log of database operations (protected by the DBFW solution). We will use the following approach to help audit access to Commonwealth data and maintain a data usage policy:

- ***Data classification***: As part of the initial security plan described in the Security Transition section 3.3.2.2, the Unisys team will discover and classify PII data on Commonwealth agency systems. Once identified and tagged based on PII sensitivity, we will work with the Commonwealth to establish DBFW rules/policies for Commonwealth prioritized PII sensitivity types.
- ***Data access patterns***: The Unisys team uses the DBFW solution's standard out-of-the-box functionality to identify user access patterns to data. This helps establish a baseline of user activity for database operations including: Data Manipulation Language (DML), Data Definition Language (DDL) and Data Control Language (DCL) and usage of stored procedures.
- ***Detect potential data access violations***: The Unisys team uses the above described DBFW solution's standard out-of-the-box-functionality to configure and enable appropriate rules/policies to help detect potential data access violations to Commonwealth PII. In addition, the DBFW rules can help detect users performing unauthorized requests to the database and help disabling those users' access to the database.
- ***Reporting***: The Unisys team uses the DBFW solution's standard out-of-the-box functionality along with integration with SIEM solution to generate periodic reports to help monitor and review user access to data. In addition, we submit these reports as part of our monthly firewall logs to the Commonwealth.

2.E Provide centralized management and advanced analytics.

The DBFW solution monitors and maintains an audit log of the allowable database operations (those defined as allowable by the DBFW solution). Using the DBFW solution's standard, out-of-the-box DBFW solution capability, we are able to identify the following key parameters for a database operation:

- User performing the action
- Timestamp
- Database table accessed
- Database query/operation executed

Additionally, the DBFW audit logs will be integrated with the data center's SIEM solution. Using the standard out-of-the-box DBFW capability and SIEM solution, Unisys staff use data correlation techniques to perform analytics for discovering and responding to potential attacks against Commonwealth databases. This approach will help the Commonwealth to accelerate incident response and forensic investigation procedures.

2.F Discover new databases and database objects in scope for security and compliance projects and automatically apply appropriate protection and audit policies.

The Unisys team will use the DBFW solution along with the DLP solution's data discovery capability to discover identify new databases and database objects. We will work with the Commonwealth to identify the appropriate regulatory compliance requirements and the appropriate DBFW solution rules/policies for the newly identified databases and the database objects. The DBFW solution's identified standard out-of-the-box rules/policies will enable us to maintain the appropriate database protection measures.

2.G Offeror must describe their approach to alert, detect, audit, monitor, manage, and discover attacks to meet Database Firewall requirements.

The Unisys Team approach to alert, detect, audit, monitor, manage, and discover attacks to meet Database Firewall requirements is detailed above in response to requirements 2.A – 2.F.

Additional Solutions to Protect Data-in-Motion and Data-at-Rest

The Commonwealth also has access to the Unisys Stealth Solution and Data-at-Rest protection through the Enterprise Services Catalog.

The Unisys Stealth Solution™ renders users, data, and infrastructure undetectable to cyber criminals. Built to meet requirements of the U.S. Department of Defense to secure sensitive information, Unisys Stealth achieved the National Security Agency's National Information Assurance Partnership Common Criteria EAL-4+ certification; protecting data-in-motion across any network regardless if it is private or public.

Benefits of Unisys Stealth Solution include:

- Renders data, users, and sensitive data center dark to the outside world
- Securely protects the user, network, and data center
- Unprecedented security without an expensive reconfiguring of the network

Unisys also offers additional protection for stored data using encryption keys that are managed through a centralized key management process.

Benefits of Encrypting Data-at-Rest include:

- Minimizing the risk of loss or breach of sensitive information
- Encrypting sensitive stored data helps facilitate compliance with regulatory standards such as HIPAA.

Unisys Team Experience

The Unisys team's history demonstrates our commitment to providing our clients with leading security and privacy solutions. Our partner Deloitte's Security and Privacy Services practice, which consists of over 1,000 professionals in the United States, has been assisting clients with data protection strategy, and solution implementations, including technology integration (e.g., DLP, SIEM, IAM, Cyber Threat Intelligence, etc.) for many years.

Client	Project Description
Microsoft Corporation	Background: Microsoft is the worldwide leader in software, services and solutions that help people and businesses realize their full potential. Objectives: The Unisys team's objectives included: • Implementing a solution that meets the Payment Card Industry (PCI) data protection requirements • Identifying and protecting Microsoft's Intellectual Property data that includes source code, strategic plans, operational information

	• Performing a data discovery on 30,000 file shares, 12 terabytes of data and more than 120,000 SharePoint sites. Solution: The Unisys team's data protection solution leveraged the RSA DLP End Point to automatically provision and grid scan target systems. Benefits: The benefits obtained by Microsoft include • Highly scalable solution allowing rapid scanning • Better understanding of the location of high impact business information • Highly accurate results requiring far less manual intervention.
Accor North America	Background: Operator of 1,400+ hotel properties in U.S., Canada, and Mexico Objectives: The scope of work required The Unisys team to implement a data protection mechanism that that meets the Payment Card Industry (PCI) Data Security Standard on the several of the client's applications that processes PCI information. Solution: The Unisys team data protection solution implementation included: • Encryption of data at the point of capture to protect it at-rest and in-flight • Usage of RSA Key Manager and Application Security Manager to add encryption capabilities to core applications (Web and phone reservation systems, hotel point-of-sale) and manage encryption keys Benefits: The Unisys team's tailored approach helped the client rapidly implement encryption of customer data at the earliest point possible, in addition to securely managing the encryption keys. The RSA Key Manager architecture was designed to operate even when network connectivity is disrupted.

Benefits to the Commonwealth

Our consistent performance as a leader in security and privacy is a differentiator for us and of clear value for the Commonwealth. The Unisys team provides advisory and implementation services that focus on solving client needs from a business perspective. We bring a number of important attributes to this initiative:

- A Leading Security & Privacy Practice. Our national **Center for Security & Privacy Solutions** (Center) focuses on methodology development, thought leadership, subject matter specialists, leading-edge tools, and continuous monitoring of changing laws and regulations.
- Experienced team. The proposed team members have significant experience related to privacy, information security, and technology integration with the tools and processes related to data protection including Data Loss Prevention and Database Firewall.
- Broad industry experience. We possess deep knowledge of the state government sector and have worked successfully with the many state governments to help improve their security posture.

Our proven data protection methodologies, extensive experience in the federal and state government sectors, and seasoned security experts will result in an improved security posture for CoPA.

2.3.4 Transition Services

Transition to the new baseline datacenter architecture and common Services portfolio must be carefully planned and executed. The Offeror is required to provide a proven methodology and plan to establish the target environment and then conduct an orderly transition of existing infrastructure and Services to the new environment.

The Offeror must transition Services from the incumbent contractor where there is an incumbent contractor, as well as, transitioning Services located at the Commonwealth managed datacenters. The Offeror must identify critical success factors and risk mitigation strategies, and describe how it will coordinate and manage other Commonwealth contractor related activities impacting the Offeror's plan. The Offeror must provide an estimate of any required Commonwealth resources, including the skills needed and the duration required for each of the resources required in order for the Offeror to implement its solution. The Commonwealth expects to provide limited resources.

The Offeror must thoroughly plan, evaluate and propose comprehensive and realistic activities and timeframes for accomplishment of transition activities given identified parameters within the Commonwealth's requirements as described in Schedule K - Key Program Deliverables and Schedule D - Transition Milestones.

3 Tasks

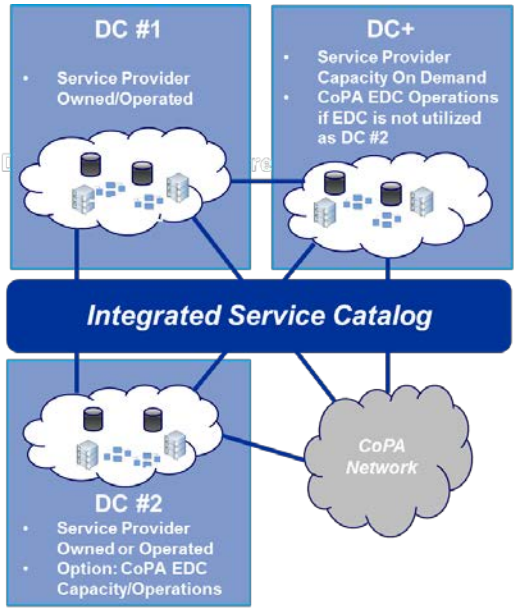
The Commonwealth has provided detailed information on the current environment for computing (mainframe, mid-range, x86, etc.), data storage, data backup (tape and other) and other datacenter related equipment in the referenced Exhibits. The Offeror shall utilize this information as the baseline requirement (in terms of Services, quantities and bandwidth) for developing its proposal.

3.1 Establish Datacenter Architecture

The Offeror must provide a multi-datacenter, multi-platform solution that will support the migration of all of the Commonwealth's current workloads. In order to support future Services, the Offeror must develop a proposal which will lead the Commonwealth into the future, and be able to address all current and future datacenter requirements. The Offeror must propose cost-effective, efficient, and forward-looking technologies for integrating Services and incorporate these technologies into its proposal. The Offeror must also address how it will allow for service updates and new technology offerings. The Offeror must describe how it will perform sizing exercises for different infrastructure to ensure the Commonwealth is getting a minimum of "like for like" or increased computing capabilities.

Baseline Architecture

In an effort to simplify the administration of IT assets, reduce IT costs, improve the provisioning of IT Services, and, in general improve the quality of IT Operations, the Commonwealth has established a preferred datacenter baseline target state architecture.



Baseline Datacenter Architecture

- Minimum 2 Datacenters
- Manage the CoPA EDC within architecture
- Flexible capacity on demand
- Redundant Secure Network Links between Datacenters and CoPA Network
- DR Capable
- Common Service Catalog
- SLAs
- Support for multiple platforms

The datacenter baseline target state architecture is based on a shared Services model in which a minimum of two geographically-separate datacenters (includes operations support for the [redacted] provide a wide range of common IT Services to the Commonwealth. While not necessarily mirror images of each other, each datacenter must be capable of supporting critical Commonwealth processing in the event the other datacenter goes offline (as, for example, in the event of a datacenter disaster). To address the need for additional capacity and new Services over time the Offeror may propose additional capacity beyond the two datacenters with secure connections to other Offeror capacity.

Initially, this target datacenter combination would host the Commonwealth's existing collection of shared information systems and currently outsourced Services. Over a prescribed period of time, the new datacenter architecture must support the transition of additional IT workloads presently being processed at a variety of datacenters owned and operated by Commonwealth agencies, thus permitting these datacenters to be decommissioned.

3.1.1 Multi Datacenter Environment (2+ Architecture)

The Offeror must provide a multi datacenter environment. All datacenters will be managed and maintained by the Offeror, including the Commonwealth's EDC and may be either a standalone facility, or integrated into existing qualified facilities. The multi datacenter environment is to facilitate high availability, capacity on demand, and the recovery of applications and Services that are deemed critical to the Commonwealth. The multi datacenter requirement is to provide a minimum of two datacenters. The Offeror may propose additional capacity and Services utilizing additional facilities beyond the two required datacenters.

Reference Documentation

Schedule E – Datacenter Locations

Exhibit A - Commonwealth Network Environment

Exhibit(s) D.1 through D.15 – Enterprise Datacenter (EDC) Exhibits

Requirements		Describe Compliance
•	The Offeror's datacenter architecture must consist of multiple geographically disbursed datacenters. Any datacenters being used in a back-up function must be at least 50 miles apart from the associated primary location for the service.	Offeror must describe the process of establishing a multi datacenter environment, including facility management, resource sharing, operational coordination, and inter-datacenter communications. Provide proposed datacenter architecture and locations. Using **Schedule E – Datacenter locations**, the Offeror must list the address of all proposed Datacenter locations that will host the Commonwealth's applications and data.
•	Tier III equivalent datacenter facilities proposed by the Offeror must have had consistent availability of 99.99% in the past six months as of December 31, 2011.	Offeror must provide current availability reports of its proposed datacenter(s) with its submittal.
•	The EDC assets will be managed and maintained by the Offeror. The current maintenance contract for the EDC servers is scheduled to expire on June 30, 2014.	Offeror must describe its approach to transition operations and management of the EDC infrastructure from the Commonwealth to the Offeror's support Services and how it intend to address the server maintenance expiration issue.

•	Each datacenters will have the capability to provide DR for the other, for identified critical applications.	Offeror must describe the process of providing DR for critical applications from one datacenter to the other. Also, describe additional DR Services if included in the overall proposed offering.
•	Datacenter sustainability.	Offeror must describe its methods of achieving datacenter sustainability, such as realizing a low Power Usage Effectiveness (PUE) ratio.
•	Robust physical security, including biometric access control, video surveillance, and routine security officer patrols.	Offeror must describe its security methods and techniques that will be used to protect Commonwealth computing assets and ensure compliance with Commonwealth security requirements.
•	In a datacenter environment that hosts both Commonwealth and non-Commonwealth clients, segregation of Commonwealth data, and computing resources from other clients' data and computing resources. The Offeror is required to provide system and data segregation between different agency application environments. Note: The Offeror may not use the EDC to provide services to Non-Commonwealth clients. The Commonwealth may permit the Offeror to provide services to COSTARS members if written permission is granted by the Commonwealth.	Offeror must describe its approach to provide Services in the event a datacenter will be shared with a non-Commonwealth client, describe how segregation of resources will be achieved and maintained. Offeror must describe how systems and data segregation can be maintained between different agency application infrastructure environments.
•	Elastic datacenter infrastructures to accommodate variable workloads.	Offeror must describe its computing and networking capabilities that will accommodate the growth or contraction of workloads.

•	24/7/365 staffing.	Offeror must describe the staffing model used to provide 24/7/365 staffing. Operations staff, technical support staff, security staff, and management. Offeror must address how it plan to manage security/background checks, monitoring and reporting on employees and how it will coordinate those requirements with Criminal Justice agencies.
•	Common work and meeting space.	Offeror must describe its capabilities to accommodate meeting and workspace for Commonwealth and Offeror IT staff and management.

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

Introduction

The Unisys data center architecture has been designed with the benefit of prior knowledge and awareness of the Commonwealth's IT environment and operation. Consideration of locations for multiple data centers has been actively pursued for over 18 months with study of sites inside and outside the Commonwealth.

Options were considered for available space and power, proximity to Harrisburg and each other and for each of the key infrastructure characteristics of security, scalability, flexibility, availability, and reliability.

Few sites met the several clip levels we set for each factor for the analysis of possible facilities that could ultimately be harnessed with the Commonwealth's [redacted] to meet the requirements we anticipated and ultimately see in the RFP.

In the end, Unisys selected two facilities from 18+ sites considered – facilities in [redacted] In addition, the Unisys team is maintaining its relationship with [redacted] as a site to provide mainframe DR services on a subscription basis, if the Commonwealth elects to continue the current mainframe DR approach (see **Figure 3.1.1-1** below).

Figure 3.1.1-1 – Proposed Commonwealth Data Center Locations

Unisys data center architecture provides flexibility, availability, reliability, and resiliency and provides locations allowing for the right placement of Commonwealth IT equipment. Our data centers are interconnected and operated as a unified whole. Unisys manages its facilities including the [redacted] as a single integrated unit. Unisys provides the data center resources that matches the best solution to the Commonwealth's IT requirements. Moreover, our architecture provides Commonwealth-focused data center operational coordination with a common management team and integrated process supported by common service management architecture across the environment.

For addresses, descriptions and additional documentation on proposed data centers, please refer to Schedule E "Datacenter Locations".

1 Multi Datacenter Architecture

1A The Offeror's datacenter architecture must consist of multiple geographically disbursed datacenters. Any datacenters being used in a back-up function must be at least 50 miles apart from the associated primary location for the service.

Unisys data center architecture provides flexibility, availability, reliability and resiliency and provides locations allowing for the right placement of Commonwealth IT equipment. Our data centers are interconnected and operated as a unified whole, and Unisys manages its facilities including the Commonwealth's [redacted] as a single integrated unit. To accomplish our intent, Unisys considered more than 18 sites and selected facilities in [redacted] to join with the Commonwealth's [redacted]. The IBM Data Center in [redacted] will continue to be available as an IBM Mainframe DR option. Each of the facilities has been considered for its location relative to Harrisburg, and each other with no facility within 50 miles of another allowing any site to maintain a suitable distance as a DR location for any other.

Each of the Unisys facilities maintains availability above 99.99% along with an engineering posture equivalent to Uptime Institute's Tier III.

1B Offeror must describe the process of establishing a multi datacenter environment, including facility management, resource sharing, operational coordination, and inter-datacenter communications. Provide proposed datacenter architecture and locations.

The facility locations have been selected with the following criteria:

- Deliberate engineering and construction that, if formally assessed, would find the facility equivalent to Uptime Institute's Tier 3 rating.
- Significant security treatments and a safety posture meeting the requirements of the Unisys delivery model for the Commonwealth's IT systems.
- Predictable and ready availability of sufficient and reasonably priced electric utility for the anticipated IT load.
- Present availability of high-speed and high-capacity networking to mitigate potential latency issues between sites, the [redacted] Commonwealth users and COPANET.
- Reasonable accessibility to Unisys service delivery teams and Commonwealth staff.
- Present capability of assuming either of or both production and recovery site operations.
- Immediate flexibility sufficient to permit growing or shrinking Commonwealth workloads.
- Capable of operating with the other Unisys data centers as a member of an interconnected and unified whole.

Engineering and Construction

Each facility was selected with an ability to meet and exploit the environment extremes common to their location. Steel and concrete construction was required along with interior floor loading characteristics that permit the variety of the Commonwealth's IT equipment.

Security and Safety

Each facility has both physical and logical security in place and ready to deploy down to the rack level if requested. Perimeter security is maintained by camera and an active physical security presence. All facilities include guard-controlled access to interior spaces. In each case, guard-controlled access to segregated data hall areas can be incorporated upon request.

Security systems whether access control, monitoring, or alarming are incorporated into the Unisys operational model permitting event correlation, logging and management alerting at all appropriate levels in the Unisys delivery team. These facility security systems are integrated with the service management ITSM systems allowing a facility component to the ITIL-aligned processes employed for the Commonwealth.

Access control systems include access to and within the facilities in all data centers. Access control is through a combination of keycard, keypad and biometric devices. In addition, access control systems including keypad and biometric authentication capabilities are available for the raised floor on areas segregated from portions of the Commonwealth's service area. The Commonwealth can request these services including security caging, security cabinets, and cabinet or cage-level monitoring (camera or access) down to the rack level from the Enterprise Services Catalog. For more information on security see Section 3.1.2, "Network and Security Architecture".

Electric Power

Each facility has been selected for its ability to provide continuous, efficient, cost-effective power. The Unisys team facilities provide between 2N+1 to 2N+2 redundancy. In addition, we have selected facilities with the capacity to grow to and beyond an estimate of the full requirement that the Commonwealth IT estate may have. The considerations include a review of the ability of local utilities to deliver electricity and the cost to meet and grow with the Commonwealth's use of each location.

High-Speed Networking

Unisys data center architecture includes a robust interconnection architecture to minimize network effects of data center separation and provide the ability for Commonwealth applications to connect where required. Access to a variety of network providers has also been incorporated into the evaluation of sites for the Commonwealth. Unisys prerequisites include the presence of multiple high-bandwidth, high capacity providers able to deliver to the site. Preference was given to sites with those providers whose existing infrastructure passed by if not into the location to minimize time to procure new and future service.

Unisys has selected and built carrier-neutral data center facilities, offering a variety of telecommunications carriers to choose from and a broad range of network solutions to satisfy connectivity requirements. The facilities boast numerous dark fiber providers, as well as lit fiber service providers as well.

For greater detail on networking between and within the Unisys sites see Section 3.1.2, "Network and Security Architecture".

Accessibility

The locations Unisys has selected were selected, in part, for their accessibility to both the Unisys and Commonwealth staff. Their proximity to Unisys locations or the Commonwealth reduces the cost and time for any required access to IT spaces or equipment. In particular, locations have been selected that are within driving distance of, close to a major airport or both.

Mission Flexibility

The diversity of the Commonwealth's IT estate set a criteria in Unisys selection for a space capable of addressing the entire range of power, cooling, and floor loading variations demonstrated from our experience with the Commonwealth and laid out in the RFP's exhibits. Further, the selections were made based on the ability of the space to grow with Commonwealth requirements without a heavy cost of preparing for that possibility in advance. Each site was evaluated with no set preference for a role as DR or production allowing the architecture to maintain flexibility. Examples of considerations given include the ability of the site to provide for a possible need for extra high density layouts, water-cooled equipment, and exceptional floor loading. Each site addresses those circumstances and holds the potential solution available to the architecture team needing to deploy them.

Unisys facilities are purpose-built for mission critical systems and applications. Data floor features like high power density, high cooling density, and ease of scalability enable customers to deploy a variety of IT environments in our data center facilities. High density production

environments, storage networks, and development environments are all easily supported within our facilities due to our ability to accommodate high rack power consumption and quickly add connectivity and power when requested. Customizable office space, fit up space, and testing space also gives the flexibility required to accomplish a variety of missions inside the Unisys data center facilities.

Scalability

Like mission flexibility, the selection of a site by the Unisys team, incorporated a concern for growth in the scale of the operation as well as scope for IT environment diversity. In particular, scalability has been addressed both in the facilities themselves and in their operations.

Scalable facilities of many types including pod and module architectures were considered. These choices, while extraordinarily flexible challenge many of the security requirements unique to the Commonwealth. Moreover, such facilities do not meet the requirement to have been operating for 6 months by December 31, 2012. Consequently, these options have been set back as deep options for future consideration.

The choices were then made between operating facilities with standing ready to meet such a need. Both [redacted] have this characteristic in two forms – active ready white space waiting for IT equipment and space, with and without grid but without the more significant electrical and mechanical subsystems representing major capital cost and therefore upward pressure on the ultimate cost of the Unisys bid.

Operationally, the Unisys solution incorporates a single, common space management team reporting to the Unisys account team. This single team has a holistic view that includes the [redacted] in the deployment of equipment to the sites during transition and migrations, and after. Unisys manages these facilities including the Commonwealth's [redacted] as a single integrated whole.

One of [redacted] major differentiators is the patented critical infrastructure that enables the facility to easily and massively scale without impacting customers. For the Commonwealth, this means that you do not have to worry about increasing a co-location footprint or committed power consumption – [redacted] infrastructure was designed from inception to scale without impacting customers IT systems or their reliability. The infrastructure delivery team is especially responsive to cross connect requests and electrical circuit requests.

1C Using Schedule E – Datacenter locations, the Offeror must list the address of all proposed Datacenter locations that will host the Commonwealth's applications and data.

The facilities' locations along with some key facts for each are provided in Schedule E.

2 Datacenter Availability

2.A Tier III equivalent datacenter facilities proposed by the Offeror must have had consistent availability of 99.99% in the past six months as of December 31, 2011.

Unisys data center facilities meet or exceed the Uptime Institute Tier III standard for concurrently maintainable data center site and infrastructure. The overall facility UPS topology

is a distributed redundant configuration. Unisys [redacted] uses a patented maintenance bypass isolation feature. This feature enables our [redacted] facilities to exceed Uptime Tier 4 standards for data centers to be concurrently maintainable or fault tolerant with a simultaneous utility outage. This innovative level of critical infrastructure redundancy has been termed 2N+2: two completely separate power paths from the power utility to the customer rack (2N) and all of the critical components in those two independent power paths have (at least) two extras for backup (N+2).

In addition, each of these facilities meet the requirement as amended in notes ("Addendum 16 Master Questions and Answers", page 29, item shown for Addendum 4 – Round 1, Part 2, #30) from the Commonwealth for a facility in operation with an availability at or above 99.99% in the six months prior to December 31, 2012. Documentation to support this requirement for each site is available upon request. Such documentation shows that Unisys facilities exceed the requirement.

2.B Offeror must provide current availability reports of its proposed datacenter(s) with its submittal.

Availability reports are included in Schedule E for [redacted]

3 EDC Assets and Transition

3.A The EDC assets will be managed and maintained by the Offeror. The current maintenance contract for the EDC servers is scheduled to expire on June 30, 2014.

3.B Offeror must describe its approach to transition operations and management of the EDC infrastructure from the Commonwealth to the Offeror's support Services and how it intend to address the server maintenance expiration issue.

Unisys evaluation of the Commonwealth facilities includes a detailed review of the infrastructure currently installed in the [redacted] This evaluation incorporates a wall-to-wall inventory to locate and identify all equipment along with a review of the maintenance status.

Upon completion, Unisys intends to recommend and consult with the Commonwealth on the options that can be pursued. These options are provided in the Technology Refresh plan and include:

- Provision of maintenance services for the equipment,
- Conversion of an asset to Unisys new Fully-Managed service,
- Commonwealth acquisition of new equipment that can be used with Unisys Managed-Only services and that is current for maintenance and warranty purposes.

Equipment that remains aged beyond warranty, support and maintenance will not be able to be serviced with any SLA coverage.

For more details on the Technology Refresh plan and approach refer to Schedule F, Section 3.2.1.5.1 "Technology Refresh".

For greater detail on the transition of the [redacted] management to Unisys please refer to Schedule

F, Section 3.3 "Transition Services" and Schedule M "Transition Plan".

4 DR Services

4.A Each datacenters will have the capability to provide DR for the other, for identified critical applications.

Unisys data center architecture provides an operational model that supports a strategic intent of maturing the Commonwealth's disaster recovery posture. Unisys selection of sites was from its team's portfolio of sites and beyond. The selection criteria included criteria based on the Commonwealth's IT Strategic Plan published in late 2011 for operational characteristics that are required in facilities supporting the Commonwealth. The evaluation of sites over the last 18+ months has always included a mutual DR characteristic. With the selected sites, Unisys has sites with Unisys [redacted] that can backup each other. Each has similar facilities infrastructure designed to provide a site ready to operate for the other where applications require.

Examples where this is the case appear throughout the solution such as the placement of the production Unisys mainframe in Unisys [redacted] with a DR peer in Unisys [redacted] In fact, where [redacted] was once a cold and warm DR site, now those application environments are in the [redacted] sites.

In addition, Unisys is able to adjust and widen its DR approach where cost or design dictate. An example is the incorporation of the existing use of the [redacted] facility into the data center fabric as a continuing cold site option for the IBM mainframes.

While these stand as options, Unisys decisions on how production and DR systems are deployed are not assumed. Agency use, including the use of the [redacted] as a participant in the architecture, will be a result of collaboration between the Unisys team and the agency in determining the best deployment for the best cost that meets an application's operating needs.

For example, the Department of Labor and Industry's application DR solutions may be migrated to the data centers in a number of ways, all of which Unisys will call on DLI for review and approval. In this case, specifically, the Unisys migration team along with its architecture, facility and space management team will work to gain DLI's insight and counsel to collaborate on the best solution for DLI.

For more information and greater detail on the Unisys disaster recovery services please see Schedule F, Sections 3.2.1.5.2 "IT Service Continuity Architecture", 3.2.2.4 "DR Planning and Testing" and 3.2.5.3 "DR Infrastructure on Demand".

4.B Offeror must describe the process of providing DR for critical applications from one datacenter to the other.

DR solutions for the Commonwealth's critical applications are available in most forms of DR in use today including cold-site subscription services. Unisys team has the unique advantage of being able to provide the range of services from Unisys operational DR support services to IBM's subscription services.

The Commonwealth's DR needs are met through the selection from the Enterprise Services Catalog with equipment designated for DR use and noting that placement is in support of an application's infrastructure. Identification of that system will then allow Unisys Space Planning to provide the options for the DR environment to the Commonwealth. Where a greater degree of consultation and collaboration is required, either Unisys or the Commonwealth may engage the other in a deeper review of the available options or discussion on how additional options may be provided.

In general, DR is provided by placing IT systems in the same facility for high availability, in another facility for continuous operation, or both for continuous availability. The Commonwealth may engage the Unisys team on the actual mechanisms for failover but these are considered specific to the application and the architectural responsibility of the application owner. Major elements of DR service exist and reside within the data center services including dual diverse network connections between each sites, along with backup/recovery services and data replication. These may be requested from the Enterprise Services Catalog.

For more information and greater detail on the Unisys disaster recovery services please see Schedule F, Sections 3.2.1.5.2 "IT Service Continuity Architecture", 3.2.2.4 "DR Planning and Testing" and 3.2.5.3 "DR Infrastructure on Demand".

4.C Also, describe additional DR Services if included in the overall proposed offering.

DR solutions for the Commonwealth's critical applications are available in most forms of DR in use today including cold-site subscription services of IBM Business Continuity and Recovery Services at [redacted]. The Unisys team has the uncommon advantage of being able to provide the range of services from Unisys operational DR support services to IBM's subscription services. The Unisys proposal includes this last optionally for the current mainframe environment. Similar services, while not in the Enterprise Services Catalog, are available by request. DR architectures that require site schemes beyond the sites provided are possible within the family of Unisys and IBM data centers. A service request can start the process with consulting or a request from the Enterprise Services Catalog.

5 Datacenter sustainability

5.A Offeror must describe its methods of achieving datacenter sustainability, such as realizing a low Power Usage Effectiveness (PUE) ratio.

Unisys data center architecture is uniquely sensitive to the environment. [redacted] has one of the lowest design PUEs in the data center industry. This industry-leading energy efficiency is achieved through innovative cooling system design using proven methods. The mechanical cooling plant utilizes air-cooled chillers, which keep water usage low due to its closed loop system. The air-cooled chillers also have an economization mode that is used when operating parameters are met to conserve energy usage by bypassing (securing) the refrigeration cycle and allowing the chiller to act as a carburetor does on a car.

In addition, [redacted] computer room air handler units are 100% outside air economization capable, a cooling mode which is utilized about 60% of the year, a big driver in low PUE. The cooling system in its entirely is completely automated, ensuring that the most energy efficient cooling method is employed to cool the data center and closely match cooling required with

cooling delivered.

The facility is designed to U.S. Green Building Council LEED Gold requirements and is designed to earn the EPA ENERGY STAR rating. Unisys [redacted] was the first multi-tenant colocation data center to earn the EPA ENERGY STAR, leading the industry to improve data center energy efficiency.

[redacted] uses integrated and sustainable design elements such as a 30-inch raised floor that maintains superior air flow around servers to maximize cooling efficiency. Unisys also maintains a glycol air conditioning system that is greater than 40 percent more efficient than those typically found at data centers. This system also uses "free cooling" when the outside temperature is below 50 degrees Fahrenheit, saving 8 percent of power consumption and cost. Other energy-saving equipment includes computer designed fluorescent lighting, central humidification systems, better cable management, and lower emitting emergency generators.

Matching air conditioning with power usage saves electric costs in the Commonwealth area in [redacted] This green operational procedure has served as a model for other Unisys data centers.

6 Physical Security

6.A Robust physical security, including biometric access control, video surveillance, and routine security officer patrols.

Offeror must describe its security methods and techniques that will be used to protect Commonwealth computing assets and ensure compliance with Commonwealth security requirements.

The Unisys data centers' architecture incorporates the latest in physical and operational security approaches.

[redacted] has deployed a centralized, electronic access control system that provides alarm monitoring points on all personnel and equipment doors, as well as intrusion detection throughout the facility. Photo ID badges with unique personal identification numbers, as well as biometric iris scanners, provide multiple levels of electronic access control, and also provide individual accountability throughout the facility. The site's security systems control physical and electronic access to the building, the data center floor, and each client's caged area or module. 3-factor identification is required to access the data floor. A fourth layer is required to access a client cage or module.

Each client's equipment within [redacted] data center is housed in a vault that is exclusively dedicated to the Commonwealth. Access is restricted to authorized personnel only with that list maintained via [redacted] online security portal. All data center visitors must pass through multiple security zones delineated by mantraps with card readers and keypads for personal identification numbers, as well as biometric iris scanners (each with a unique access list tied to each security device) to access any of the customer spaces.

Physical facility security includes a building-within-a-building design, ensuring there is no direct access to the data floor from the external walls of the facility. Over 150 steel and concrete bollards surround the [redacted] facility in front of parking and the main entrance. All other back-of-house Mechanical Electrical Physical (MEP) infrastructure and the shipping & receiving area is surrounded by steel fencing and secured with entrance gates and a guardhouse.

Cameras are located at every entrance, every mantrap, every data pod, the entire roof area, the back-of-house MEP area, and all parking lots. All cameras are PTZ CCTV, digitally recorded, monitored by security staff 24x7 (and the Network Operations Center for backup and situational awareness) and all footage is maintained for at least 90 days.

[redacted] is safe, secure, and protected from disruption or intrusion. All critical procedures, equipment, and software systems have a backup, an acceptable alternative, or a proven workaround solution for use in component or system failure. [redacted] also complies fully with industry guidelines for safety, fire protection, uninterruptible power supply, and security requirements. Each year, our facility is required to pass a SSAE-16 audit for its overall operations. Multiple SSAE-16 audits that are tailored for specific clients are also performed. [redacted] has ISO 27001 certification like the other Unisys data centers and Managed Services Centers around the globe.

[redacted] maintain similar security postures and have their facility alerts forwarded to the Unisys Commonwealth event management system for immediate notification of incidents to Unisys account managers, and where required, Commonwealth personnel.

7 System and Data Segregation

7.A "In a datacenter environment that hosts both Commonwealth and non-Commonwealth clients, segregation of Commonwealth data, and computing resources from other clients' data and computing resources.

Offeror must describe its approach to provide Services in the event a datacenter will be shared with a non-Commonwealth client, describe how segregation of resources will be achieved and maintained."

Unisys data center architecture provides for secure physical and logical separation from any adjacent facility or campus occupants, including an ability to provide similar segregation within the Commonwealth's IT services area. The Commonwealth's IT environment is secure physically and logically from other potential occupants of the facilities supporting it.

At the [redacted] facility, the Commonwealth environment will occupy an entire "data center vault" at the facility and have its own secure entrance and facility infrastructure. No other facility customers from the other data center vaults are able to access the Unisys Commonwealth data center vault. Additionally, within the vault, 12 ft. tall cage mesh partitions can be used to separate different environments and systems as required.

At [redacted] the Commonwealth of Pennsylvania environment takes a dedicated "data center area", Area F, and has its own security access controls and power and cooling infrastructure. No other Unisys customers are deployed to this area. In addition, the Commonwealth may select to install security caging with "slab-to-slab" steel wire-mesh fencing using the cages listed within the Enterprise Services Catalog or to a custom size via a service request.

7.B "The Offeror is required to provide system and data segregation between different agency application environments.

Offeror must describe how systems and data segregation can be maintained between different agency application infrastructure environments."

Note: The Offeror may not use the [redacted] to provide services to Non-Commonwealth clients. The Commonwealth may permit the Offeror to provide services to COSTARS members if written permission is granted by the Commonwealth.

Unisys data center architecture provides optional physical and logical segregation within the Commonwealth's physical and logical data center spaces. Within the Commonwealth colocation space, cage mesh partitions can be optionally used to separate different agency environments and systems as required. The Unisys infrastructure service delivery team will work with the Commonwealth to determine exact requirements for caged partitions within the already physically and logically separate Commonwealth/Unisys "data center vault."

In anticipation of this requirement Unisys has included a number of standard cages in the Enterprise Services Catalog that can be deployed within the sites. Security cages in small (8'x9'), medium (10'x19'), large (18'x9') and extra-large (18'x15') sizes are provided via the Enterprise Services Catalog for each location as space is available within each facility to combine with fully-managed, managed-only or co-location services options.

Additionally, there will be logical separation of agency data via [redacted] firewalls may be provided. For greater detail on logical security within the Unisys sites see Section 3.1.2, "Network and Security Architecture".

8 Elastic datacenter infrastructures to accommodate variable workloads

8.A Offeror must describe its computing and networking capabilities that will accommodate the growth or contraction of workloads.

Unisys datacenter architecture is designed to flex with the Commonwealth's need for growth or reduction in data center hosted services.

Unisys data center facilities are purpose-built for mission critical systems and applications. Data floor features like high power density, high cooling density, and ease of scalability enable customers to deploy a variety of IT environments in our data center facilities. High density production environments, storage networks, and development environments are all easily supported within our facilities due to our ability to accommodate high rack power consumption and quickly add connectivity and power when requested. Customizable office space, fit up space, and testing space also gives the flexibility required to accomplish a variety of missions inside the Unisys [redacted] data center facility.

One of Unisys [redacted] major differentiators is the patented critical infrastructure that enables easy and massive scaling of the facilities without impacting customers. For customers, this means that they don't have to worry about increasing their colocation footprint or their committed power consumption – Unisys [redacted] infrastructure was designed from inception to scale without impacting customers' IT systems or their reliability. The infrastructure delivery team is incredibly responsive to cross connect requests and electrical circuit requests.

9 "24/7/365 staffing."

9.A Offeror must describe the staffing model used to provide 24/7/365 staffing. Operations staff, technical support staff, security staff, and management.

Unisys data center staffing provides a single point of responsibility, contact, and management for all data center management supporting the common data center operational model. The Unisys security team is onsite 24x7. The security lobbies are staffed 24x7 by our security team. Training includes periodic training sessions as well as drill-type evolutions for the security staff.

Unisys provides dedicated network/security support staff at its facilities 24x7x365, coupled with automated tools that provide real time notification of suspected security intrusion events. Unisys Security Operations Center (SOC) is comprised of security support staff and a suite of automated tools that provide comprehensive 24x7x365 monitoring, alerting, and response to security events. Personnel follow specific instructions to mitigate issues according to the Security Incident Procedure (SIP) policy.

The Unisys Service Desk (Level 1) monitors the network/security team's response for security related incidents and escalates as appropriate. The Service Desk helps to provide that the Unisys network/security team responds even during off hours depending upon the SLA requirements for incident priority response. (See Section 3.2.4.6 for more on security.)

9.B Offeror must address how it plan to manage security/background checks, monitoring and reporting on employees and how it will coordinate those requirements with Criminal Justice agencies.

A criminal (misdemeanor and felony charges) background check that goes back 7 years is completed upon an offer of employment. The background check also encompasses national watch lists, education verification, and address verification. Each report is reviewed independently by HR personnel. Upon successful completion of the background check, we do a non-DOT instant 7 panel drug screen. The drug screen must be verified by HR personnel before the employee begins work at a Unisys team facility when they are working on or in the Commonwealth service areas.

Unisys is accustomed to completing Commonwealth specific background checks in accordance with the Commonwealth ITB. We will perform fingerprint background checks on all personnel required to do so per the CJIS policy and will execute Management Control Agreement (MCA) with PA State Police. As part of our ISO27001 certification, we perform an annual 3rd party/subcontractor review as well.

All employees and subcontractors providing data center services are subject to background checks and form signatures and completion of annual security training. Those that do not require physical access to the facility are subject to a one-time Department of Corrections (DOC) check and are not issued a badge. Per the Commonwealth policy on contractors, each user is also subject to an annual Pennsylvania Access to Criminal History (PATCH) background check.

Onsite data center employees and contractors are subject to an annual DOC background check, form signatures and a one-time PA State Police (PSP) fingerprint check.

See Section 5, "Personnel" for greater detail on these and related staffing items.

10 Common work and meeting space

10.A Offeror must describe its capabilities to accommodate meeting and workspace for Commonwealth and Offeror IT staff and management.

Unisys facilities provide meeting and work space for Unisys or Commonwealth staff needing access to Unisys Commonwealth service areas.

Unisys data centers are built for compliance, security, and space for IT servers to work. They are also designed with meeting and collaboration space for IT managers and data center professionals. In addition to the data center space, our facilities offer dedicated customer lounges with gourmet coffee and soft drinks, entertainment centers, dedicated customer conference rooms, IT workstations, and comfortable seating areas. Unisys facilities also offer highly customizable private office space which can be used as a NOC, testing and fit-up space, or traditional office space.

Unisys Harrisburg offices include spaces commensurate to the regular cadence of meetings for small and medium size groups including regular executive meeting space for confidential or sensitive discussions with the Commonwealth. In addition, Unisys has retained access privileges to Harrisburg University meeting and conference areas for large groups or when meetings have a need for significant multi-media and video technology content.

The Unisys team can make meeting space available in many of its facilities including the corporate meeting and training facilities in Blue Bell, PA, the [redacted], among many others. The Commonwealth is encouraged to contact the Unisys Agency Account Managers with any inquiry for available locations and possible costs that may be incurred.

Unisys Team Experience:

The Unisys Team manages over 400 of its own facilities world-wide. For a close example, Unisys currently operates and maintains the Commonwealth's Data PowerHouse. During our management tenure the facility has seen major facility refresh and upgrades on key data center infrastructure components including the power and cooling systems.

The team also manages far more than its own facilities and is engaged at customer facilities world-wide. By example, Unisys manages the two facilities established for the State of Texas Department of Information Resources in Austin and San Angelo, Texas. Our services for Texas have included the actual construction as well as the operation of the Austin facility, as well as recent upgrade planning. Services for both sites include the engineering, support and maintenance of the structure, power, cooling, fire suppression and security aspects of the facilities.

Mission critical data centers are often within the team's remit including those for major banks, transportation and logistics companies, telecommunications providers and manufacturers.

Benefits to the Commonwealth

The Commonwealth can benefit from the Unisys team in active management of its facilities as well as the direct benefit of using the team's own facilities. The Unisys team is in the business of keeping IT operating and that includes paying attention to the actual foundations for secure, reliable and available facilities to house IT environments. It is an expertise that the team has and must cultivate to keep the best and latest skill and technology in play for the

support of IT environments whether it is the latest in key system efficiencies leading to cost improvement or the recent opportunities in improving the engineering solutions that define our data centers.

3.1.2 Network and Security Architecture

Secure and robust network connections are critical to the overall data center architecture. Connections between the data centers and access to the Commonwealth's network must be planned, established, and tested prior to the transitioning of Services. All Offeror data centers and locations must coordinate connections between the Offeror's network and the Commonwealth's fiber network (COPANET).

Reference Documentation

Exhibit A - Commonwealth Network Environment

Exhibit P – Enterprise Internet Bandwidth Utilization

	Requirements	Describe Compliance
1.	All proposed datacenter locations will connect to and provide access from COPANET.	Offeror must describe its approach to connect to COPANET.
2.	Dual network termination points to connect to COPANET.	Offeror must describe its networking capability and the ability to support dual termination points in the proposed datacenters environments.
3.	Provide network security via firewall and security devices.	Offeror must describe its network security and access control solution.
4.	All proposed Offeror's datacenter facilities will have secure Internet access capabilities. Internet access must provide virus and intrusion protection systems with reporting capabilities.	Offeror must describe its approach to providing secure access from Commonwealth authorized users via the Internet. The Offeror must describe its approach to providing virus and intrusion protection and reporting.

5.	Multiple security zones must be configured within each datacenter to support specific agency requirements. For example: access, web, application, and data zones. The specific configuration and number of individual zones may be different per agency and application.	Offeror must describe its ability to support the configuration of multiple security zones within its datacenter architecture.
6.	Secure connections are required for traffic that may traverse between Datacenters and between Datacenters and Commonwealth. Encryption shall be a minimum of 128-bit and must be FIPS 140-2 certified to meet Criminal Justice Information Services (CJIS) requirements. (Refer to Pennsylvania State Police (PSP) Summary of CJIS Requirements and CJIS Security Policy.)	Offeror must describe its ability to provide secure network connectivity that meets the standards outlined in the requirement.
7.	Remote access to datacenters supporting CJIS systems must meet minimum security requirements identified in CJIS Security Policy. These requirements include but are not limited to identifying remote user's identity, IP address and connection must be FIPS 140-2 certified with a minimum of 128-bit encryption.	Offeror must describe its ability to comply with the security policies described in this requirement,

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

Introduction:

Unisys has designed a state of the art network and security solution that takes into consideration the current Commonwealth network and has laid out an architecture that is designed to support the Commonwealth well into the future. The highly experienced Unisys network and security team will review the network and security architecture outlined below with the Commonwealth agencies during transition to verify that requirements are agreed upon and accepted. In addition, the network and security team will implement the approved

architecture and maintain it through the Unisys standard ITSM processes.

Because the current Unisys network and security team understands the internal policies and procedures of the Commonwealth, Unisys strongly believes we are the lowest risk option to implement the new network design described in detail in the following sections. This detailed understanding of the existing Commonwealth's policies and current network design also verifies that the Unisys team will be able to deliver the solution in the least amount of time while meeting or exceeding all transition delivery milestones.

1 COPANET

1.A All proposed datacenter locations will connect to and provide access from COPANET.

Offeror must describe its approach to connect to COPANET.

As **Figure 3.1.2-1** below illustrates, the Unisys Team will be meeting the current COPANET connectivity requirements by connecting locally at [redacted] via 10 Gb Ethernet and via 2 x 1 Gb Ethernet connections to an alternate COPANET location from another data center. Should direct connectivity to the Verizon PIP network be required, Unisys can terminate Commonwealth provided PIP circuits on Unisys owned and managed equipment at the Unisys Data Centers.

In addition to the [redacted] two new data centers will be utilized – Unisys [redacted] and Unisys [redacted] In [redacted] a new connection to the existing COPANET node will be built using two 10 Gb fiber connections within the Commonwealth Technology Center [redacted]. Since the distance to connect [redacted] to COPANET is so short, these connections do not require a WAN circuit to be installed, thus saving cost. The [redacted] connectivity is shown on the far left diagram of **Figure 3.1.2-1** below:

[redacted]

Figure 3.1.2-1 – COPANET Connectivity

In the middle and far right side of the **Figure 3.1.2-1** above, COPANET connections to Unisys [redacted] and Unisys [redacted] are shown. Based on predicted future usage, both the Unisys [redacted] and Unisys [redacted] Data Centers will be connected to COPANET via 1 Gb circuits. To prevent a single point of failure in the connection to COPANET, the COPANET circuits from Unisys [redacted] and Unisys [redacted] will terminate in a different physical facility than the connection from the [redacted] The locations being considered to terminate these two Data Center circuits are 555 Walnut St. in Harrisburg and 400 North St. in Harrisburg, PA.

It should be noted that the circled numbers "9" and "10" in **Figure 3.1.2-1** indicate which logical circuit numbers were assigned to the various circuits being proposed for the Commonwealth, which will be explained in more detail in the next section. The point-to-point circuits 9 and 10 above will terminate on [redacted] routers in Unisys [redacted] and Unisys [redacted] on the COPANET side the circuits will terminate on existing [redacted] switch line cards, which currently form the edge connection point into COPANET.

In the [redacted] the two 10 Gb fiber connections will terminate directly on the new [redacted] core switches, while the other end of the connection will also terminate on existing [redacted] switch line cards. Unisys will be providing the necessary equipment to terminate these 10 Gb connections. The Commonwealth will be required to provide ports or line card availability on the COPANET nodes (PEs). Any additional PE equipment (line cards or SFPs) would be provided by Unisys.

2 Dual network termination points to connect to COPANET

2.A Offeror must describe its networking capability and the ability to support dual termination points in the proposed datacenters environments.

The new Commonwealth network's proposed design will have the following characteristics:

- The use of the current [redacted] Data Center;
- A Unisys [redacted] Data Center;
- A Unisys [redacted] Data Center;
- An [redacted], if the Commonwealth elects to continue with the current IBM mainframe DR approach (using existing the existing Verizon PIP connectivity);
- Diverse connectivity into existing COPANET nodes from the [redacted] Unisys [redacted] and Unisys [redacted] (described in detail in the previous section);
- Internet access for Unisys employees and Unisys 3rd parties will be provided at Unisys [redacted] and Unisys [redacted] to support Unisys management and tools traffic;
- The Unisys network design addresses both bandwidth and latency concerns;
- The Unisys network design includes both circuit and data center redundancy.

Figure 3.1.2-2 below shows an overview of the 10 new circuits that will be put in place to support the network design. The numbers are grouped together by color, with numbers 1-6 (yellow) used for high-speed backbone data center connectivity, 7-8 (green) for Unisys Internet tools connectivity, and 9-10 (purple) for COPANET connectivity:

Figure 3.1.2-2 – WAN Overview

At the heart of the new design is a high speed, fully redundant, low latency wide area network (WAN). This new backbone WAN will connect the [redacted] Unisys [redacted] and Unisys [redacted] sites together using two separate 10 Gb redundant paths between each site. Using standard [redacted] WAN load balancing across the links (per-destination load balancing), up to 20 Gb of bandwidth will be available between any of the 2 sites.

Figure 3.1.2-3 is a diagram that breaks out the 6 circuits that will be installed in support of this new backbone WAN network. The Unisys Team is confident this WAN design is the appropriate network solution to support the data transformation needs of the Commonwealth, given the amount of data that will likely need to traverse the network from the existing Commonwealth Data Centers to the new Unisys Data Centers. After the data center transition and transformation phases of the project are completed, a bandwidth analysis will be done to evaluate the circuit bandwidth. It is anticipated that less bandwidth will be needed in the steady state environment than during the transition and transformation stages.

Figure 3.1.2-3 – Data Center Connectivity

As shown in the **Figure 3.1.2-3** above, the fiber acquired from the telecommunication provider(s) will terminate directly on [redacted] core switches, allowing the deployment of [redacted] technology across all the three sites. Using [redacted] a Layer 2 multipath network will be built without the Spanning Tree Protocol (STP) being deployed. This new network design is particularly suitable for large virtualization deployments, private clouds, and high-performance computing environments. When deployed across multiple [redacted] chassis, [redacted] creates a flat data center switching fabric with:

- High switching capacity
- High cross-sectional bandwidth
- Low predictable latency

To address specific latency concerns regarding physical distance between the data centers, point-to-point telecommunication circuits will be deployed. Based on the fact that it takes approximately 1 millisecond (ms) for light to travel 100 miles, Unisys is estimating that round trip latency between any two of the three sites should be less than 30ms. The reason the latency is not less than 30ms is because additional latency (i.e., non-distance related) is added by the physical telecommunication equipment at either end of the circuit. Point-to-point circuits offer the lowest latency versus traditional network "cloud" or "star" topologies, as the distance the light needs to travel is considerably less.

In addition to Fabric Path (mentioned above) for steady state operations among the three data centers, the new Commonwealth network will be utilizing [redacted] technology during the transition in situations where the same IP subnets need to be maintained. Unisys experience is that IP addresses often need to be maintained either permanently or temporarily because of the number of servers being moved (servers in the same IP subnet cannot all be moved or relocated at the same time) or the hard coding of IP addresses in applications not allowing new IP addresses to be assigned. In either case, [redacted] on the [redacted] and [redacted] platforms is a technology that significantly

simplifies extending Layer 2 networks across distributed data centers without getting into complicated and unreliable tunneling technologies that were used in the past.

Unisys successfully utilized [redacted] technology recently on a similarly sized project when moving a large data center between states and where no IP readdressing was allowed by our customer. In that project it was necessary to maintain the same Layer 2 subnet across geographically large distances (high latency environment) and [redacted] performed as designed. When all the servers were migrated successfully, [redacted] was turned off.

[redacted]

As **Figure 3.1.2-4** above shows, [redacted] provides the Commonwealth with the ability to deploy virtual computing resources and clusters across geographically distributed data centers, delivering:

- Transparent workload mobility
- Business resiliency
- Superior computing resource efficiencies

Figure 3.1.2-5 – LAN Overview

At the [redacted] Unisys [redacted] and Unisys [redacted] locations, a completely new [redacted] LAN network will be built for the Commonwealth using state of the art [redacted] devices at the core, distribution, and access layers. Servers will have the ability to be connected to the network in either 10 Gb, 1 Gb, or 100 Mb configurations, with the network itself supporting high availability redundant uplinks, as shown in **Figure 3.1.2-5** above.

At the [redacted] the new [redacted] LAN will also connect to the existing [redacted] core network. By connecting the new [redacted] equipment in the [redacted] to the existing [redacted] equipment the Commonwealth will leverage the benefits of using existing infrastructure to reduce costs, as well as introducing new technology to significantly update the network with the latest equipment. The new [redacted] network for all three data centers will include 168 10Gb network ports and 1152 1Gb network ports.

Figure 3.1.2-6 below shows a more detailed LAN design for the three data centers.

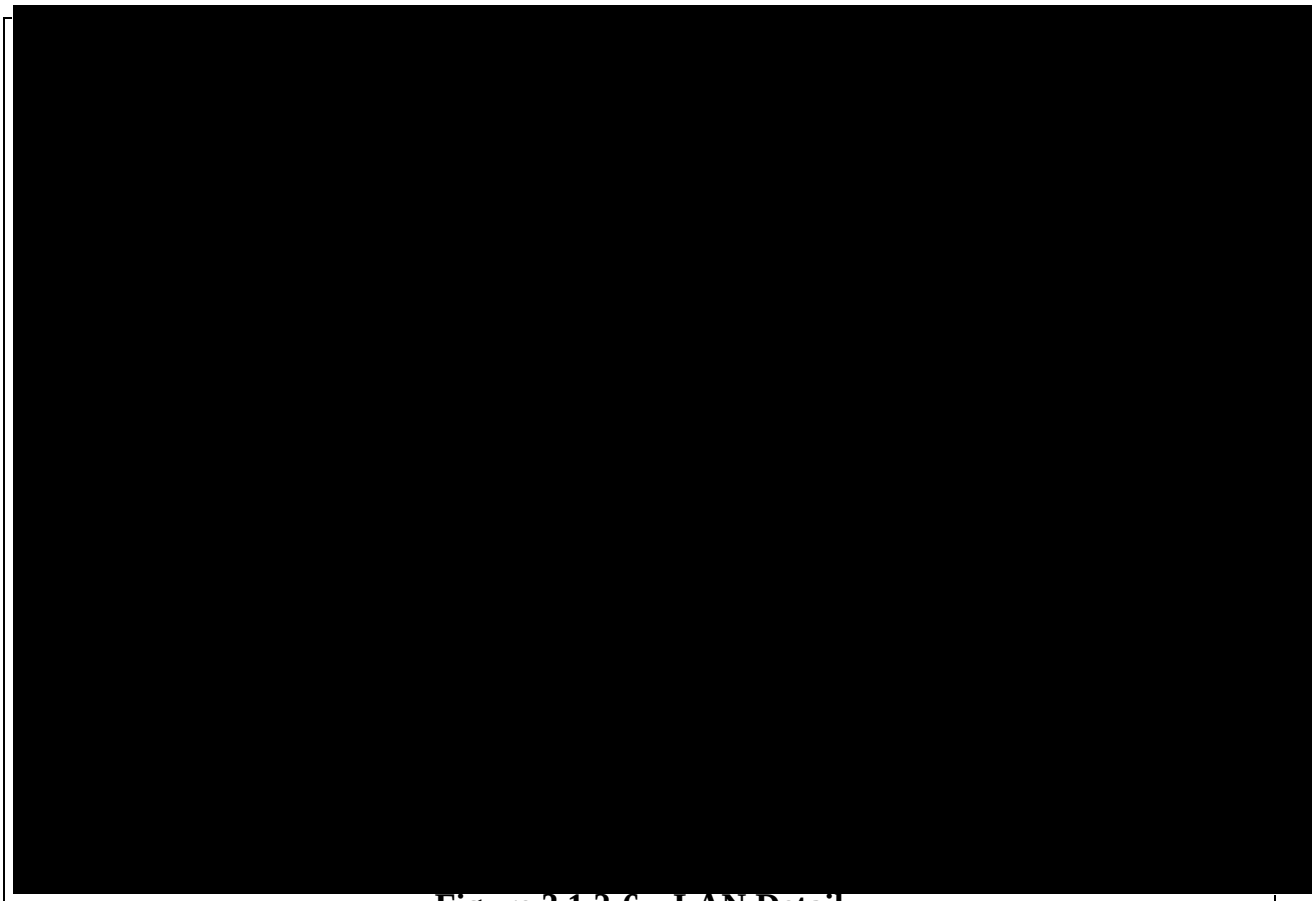


Figure 3.1.2-6 – LAN Detail

3 Network Security and Access Control

3.A Provide network security via firewall and security devices.

Offeror must describe its network security and access control solution.

[redacted] series firewall devices will be used as the enterprise class firewall at the [redacted] Unisys [redacted] and Unisys [redacted] In order to consolidate firewall and IPS functions, these [redacted] firewalls will also have built-in IPS sensors. All security products will send security alerts directly to the [redacted] product. The full capabilities of the firewalls and access control solution are described in more detail in the following sections.

4 Secure Internet access

4.A All proposed Offeror's datacenter facilities will have secure Internet access capabilities.

Offeror must describe its approach to providing secure access from Commonwealth authorized users via the Internet.

The [redacted] VPN client will allow secure Internet access capabilities for Unisys employees and Unisys 3rd parties. The Internet bandwidth Unisys is installing at Unisys [redacted] and Unisys [redacted] will be used for Unisys specific Internet facing management tools, such as [redacted] Unisys understands that the current Internet facing Commonwealth servers that are running today are going over Verizon managed circuits and that this solution will remain unchanged.

The current Verizon management and support of the Commonwealth's VPN firewalls will also remain unchanged.

Internet access of 300 Mb will be provided at both Unisys [redacted] and Unisys [redacted] as shown in **Figure 3.1.2-7** below. These circuits can be upgraded to 1 Gb on short notice, if necessary.

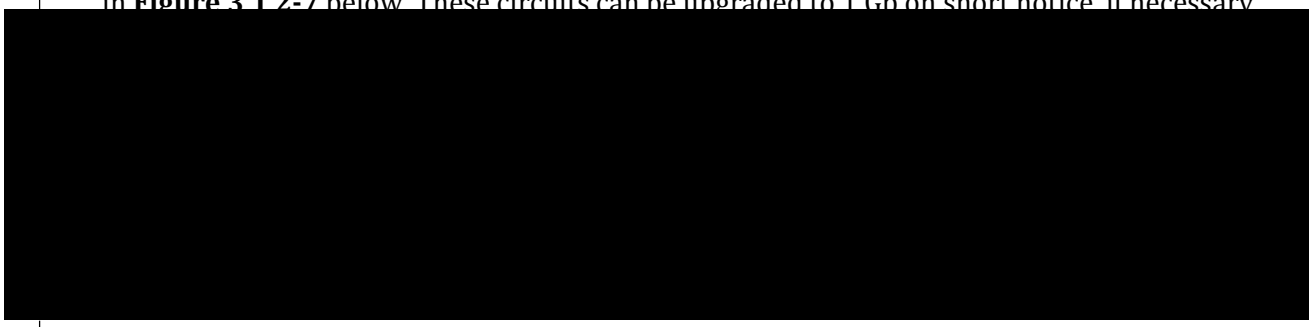


Figure 3.1.2-7 – Internet Connectivity

4.B Internet access must provide virus and intrusion protection systems with reporting capabilities.

The Offeror must describe its approach to providing virus and intrusion protection and reporting.

Our server virus protection offers comprehensive defense against complex attacks for both physical and virtual environments. It combines essential security technologies in a high performance agent with a single management console.

Below is a list of some standard virus protection report types:

- **Application and Device Control.** Events where some type of behavior was blocked
- **Audit.** Information about the policies that clients and locations use
- **Compliance.** Compliance status of your network
- **Computer Status.** Operational status of the computers in your network
- **Network Threat Protection.** Information about intrusion prevention
- **Risk.** Information on risk events on your management server and their clients
- **Scan.** Antivirus and antispyware scan activity
- **Systems.** Information on even times, types, sites, domains, servers, and severity levels

[redacted] firewalls will provide firewalling and IPS within the same appliances, enforcing and alerting on both firewall and IPS policy. Alerting, reporting, and logging will be provided by the [redacted]) and [redacted] products. For intrusion protection reports, all information will be pulled from the [redacted] tool, including proactive alerting from the [redacted] tool. The [redacted] provides both a pre-packaged reporting function and a customized reporting function. The reports can be easily scheduled and automatically sent in various graphical formats for review.

5 Security Zones

5.A Multiple security zones must be configured within each datacenter to support specific agency

requirements. For example: access, web, application, and data zones. The specific configuration and number of individual zones may be different per agency and application.

Offeror must describe its ability to support the configuration of multiple security zones within its datacenter architecture.

The Commonwealth network will be protected through a combination of network and security devices from several "best in class" vendors. The firewall vendor will be [redacted] Networks. The [redacted] devices will consist of a combination of devices. Protecting the [redacted] Unisys [redacted] and Unisys [redacted] will be [redacted] enterprise class [redacted] firewalls; protecting the front end Internet connections will be another set of [redacted] firewalls. The enterprise [redacted] [redacted] firewalls will also have built in IPS sensors.

The [redacted] [redacted] box is designed around the concept of multiple security zones. The [redacted] device supports various types of security zones, with the understanding that different agencies may have different requirements. From a Unisys perspective, security zones represent virtual sections of the network, segmented into logical areas. Security zones can be assigned to a physical interface or to a virtual system. When assigned to a virtual system, multiple zones can share a single physical interface.

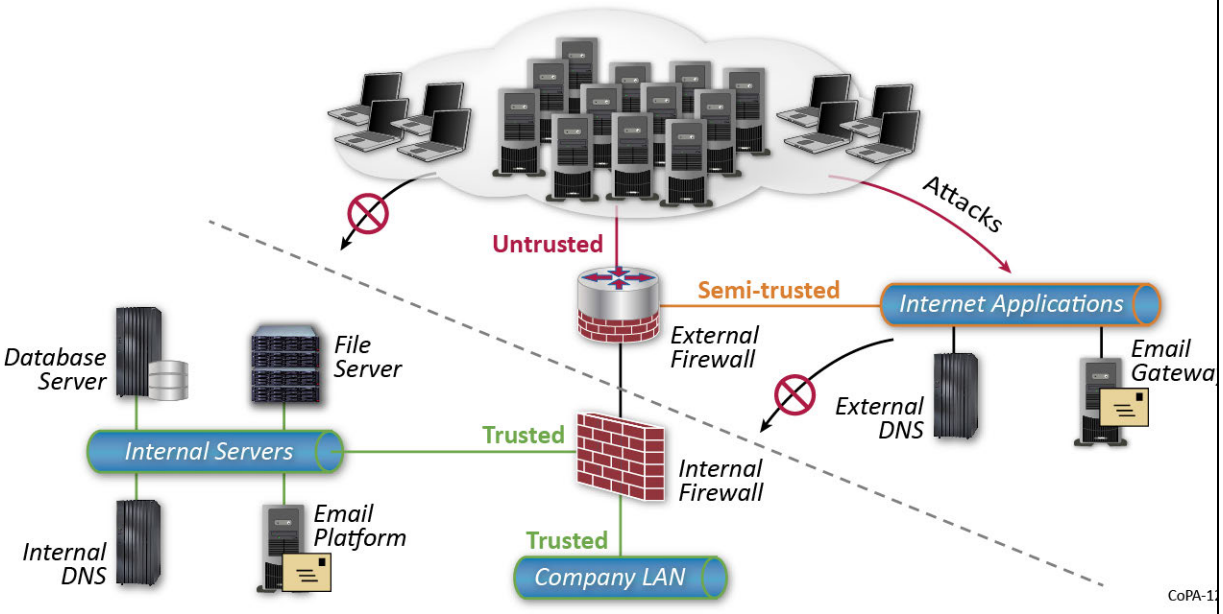


Figure 3.1.2-8 – Security Zones

Following the 4-Zone network architecture presented above in **Figure 3.1.2-8**, [redacted] Networks offers comprehensive, flexible, and robust security solutions that are ideally tailored for the requirements of the Commonwealth's new data centers. Unisys understands the Commonwealth's need for agencies and applications to be separated with firewalls and the [redacted] enterprise solution best meets this need.

[redacted] offers an unparalleled combination of features addressing these fundamental requirements:

- **Scale:** [redacted] solutions offer the processing scalability required to combat today's sophisticated threats. With the [redacted] Networks® [redacted] Series Services Gateways, [redacted]

offers firewalls that scale, both in terms of throughput and in the number of concurrent sessions, so they can accommodate the intensive security and bandwidth requirements of the next-generation data center.

- **Fabric architecture support:** [redacted] provides switches for fabric architectures, and is leading the way in delivering cohesive security integration in these environments. The [redacted] Series product line is designed to work with the scalable [redacted] fabric, ensuring optimal flexibility, scalability, and security in these emerging environments.
- **Visibility:** [redacted] security solutions can incorporate the required context, in real time, to provide effective, continuous policy enforcement. With AppSecure, [redacted] provides a deep understanding and visibility into application behaviors and weaknesses to prevent application-borne threats that are otherwise difficult to detect, let alone stop. In addition, [redacted] Networks Unified Access Control allows organizations to integrate user identities into their security policies. [redacted] also offers hypervisor integration that enables security teams to incorporate visibility into virtualized components in their security mechanisms.
- **Intelligent enforcement:** Finally, [redacted] offers solutions that can be deployed both on physical devices and in the hypervisor, enabling policy management and enforcement across the entire next-generation data center. As result, organizations realize stronger overall security, and security teams can implement faster configuration changes and reduce the errors that can create security exposures.

6 Secure Network Connectivity

6.A Secure connections are required for traffic that may traverse between Datacenters and between Datacenters and Commonwealth.

The requirement for secure connections is addressed through the use of dedicated point-to-point private connections with appropriate access and routing controls. On a case by case basis, Unisys has the capability to encrypt selected traffic between the data centers using the FIPS compliant [redacted] firewalls and offers the Unisys Stealth product as an Enterprise Services Catalog item. All Commonwealth agency to agency traffic may be encrypted, as required, using the [redacted] Firewalls with 128 bit encryption or higher.

6.B Encryption shall be a minimum of 128-bit and must be FIPS 140-2 certified to meet Criminal Justice Information Services (CJIS) requirements. (Refer to Pennsylvania State Police (PSP) Summary of CJIS Requirements and CJIS Security Policy.)

Offeror must describe its ability to provide secure network connectivity that meets the standards outlined in the requirement.

Unisys will coordinate with the Commonwealth as part of transition in determining the necessary encryption requirements. Where encryption is required, a solution will be provided that meets FIPS 140-2 and CJIS requirements. FIPS compliant [redacted] firewalls are capable of 128 bit encryption or higher, in cases where the above compliance is necessary Unisys is proposing that the Stealth product be available as an Enterprise Services Catalog item to meet regulatory requirements. Where necessary, Unisys will provide tunnel/VPN termination points for all traffic coming in over the Internet. The tunnels will be able to support 128 bit encryption or higher, where required. These tunnels will terminate on the [redacted] equipment. Between the [redacted] Firewalls and the Stealth product, Unisys will be able to meet all known Commonwealth regulatory requirements.

7 Remote Access

7.A Remote access to datacenters supporting CJIS systems must meet minimum security requirements identified in CJIS Security Policy. These requirements include but are not limited to identifying remote user's identity, IP address and connection must be FIPS 140-2 certified with a minimum of 128-bit encryption.

Offeror must describe its ability to comply with the security policies described in this requirement.

All remote access provided to in-scope CJIS systems will meet FIPS 140-2 certification and provide user identification and tracking, coupled with two-factor authentication. The [redacted] Firewalls and VPN termination equipment will be used as the termination point in the 3 data centers for all secure connections coming into the data centers from individual agencies. The SecureAuth VM Appliance will be used as the two-factor authentication method.

Unisys Team Experience

The Unisys team of network design engineers has been supporting the Commonwealth's network and security operations for several years at the DPH and the [redacted] This team, which includes the talents and Commonwealth experience of top-notch engineers, has a thorough understanding of the architectural design, details, and the interworking of COPANET and the processes associated with supporting Commonwealth business partners.

This team performed the initial transition of the agencies supported in the DPH from an architecture that consisted of isolated work group network switching configurations by agency, to the current enterprise level shared infrastructure core switching configuration that exists today. Our network design engineers are accustomed to supporting complex and secure enterprise network environments.

Unisys will provide to the Commonwealth a network management solution based on ITIL principals and delivered using proven processes that are part of the Unisys ITSM framework, integrated with cross-functional services delivered via the BMC Remedy tool suite.

The network design engineers will troubleshoot any faults using a suite of state-of-the-art management tools described in the previous sections. While performing fault isolation activities, Unisys will interface closely with the Commonwealth's telecommunication service representative, as necessary, to identify potential problems and initiate troubleshooting activities.

Changes to the Commonwealth's network, including network upgrades, will be accomplished using the standard ITSM change control process.

As part of the fault isolation process, Unisys works to resolve the problem in a timely manner in accordance with applicable SLAs. If the problem is the result of a software or configuration problem, the network design engineer will initiate the fix remotely; if the problem is the result of a hardware component failure, Unisys will engage the hardware vendor directly for a replacement part, if necessary. Some common network components will be held as spares in an on-site depot. Once the problem is resolved, Unisys will test the component to verify that the device is fully functioning.

In addition, Unisys has recently moved a large data center for the American Red Cross using the [redacted] technology to make sure that servers could remain on the same subnet with no IP

address changes. Unisys supports many other large networks for federal government and state agencies.

Benefits to the Commonwealth

The network management team's network design engineers deliver the following services to the Commonwealth:

- Configuration and management of enterprise core switching environments;
- Configuration and administration of network load balancing configurations;
- Hosting and operational support services for security products and firewalls located at the Commonwealth data centers;
- Network security configuration installations that protect the equipment and applications in the data centers from the 7 most common hacker attacks: Spoofing, Sniffing, Mapping, Hijacking, Trojans, DoS and DDoS, and Social engineering;
- Mainstream security hardware and software installation and maintenance utilizing current industry best practices sufficient to protect the enterprise class data center environments with a significant volume of sensitive class data;
- High availability enterprise data center networks administration and maintenance in support of contractual SLAs at all in-scope Commonwealth data centers;
- Fault notification, tracking, troubleshooting, isolation, and resolution;
- Full configuration management of covered network elements;
- Storage and backup of configuration files necessary to "roll-back" to a previously known state;
- Inventory reports detailing the managed elements and internal components;
- Ongoing performance analysis;
- Alert notifications and recommendations when network elements exceed mutually agreed performance thresholds;
- Periodic network reviews providing analysis and recommendations on identified network and security issues;
- Fully integrated service options, including infrastructure maintenance and help desk services;
- Audit and system logs of changes to the network showing date and specific types of changes.

3.1.3 Datacenter Architecture and Technology

The Offeror must evaluate the Commonwealth computing infrastructure(s) and develop and implement an IT architecture that will support all current systems and applications, utilizing existing and/or underutilized technologies where appropriate, to provide a high level of quality computing Services to the Commonwealth, in a cost effective manner. An overall review of all Commonwealth computing Services is required, as the requirement is to consolidate all Commonwealth based computing Services into the Offeror's data center architecture. This architecture design is to include the current DR programs and structure and will be implemented along with the production and testing environments.

The Offeror must provide a multi-platform solution that will support the migration of all of the Commonwealth's current workloads. The Offeror must address in its design how it will create a target environment that will minimize application latency concerns.

The Offeror must also develop a proposed infrastructure environment, which will lead the Commonwealth into the future, and be able to address all current and future data center requirements.

Reference Documentation

Exhibit A - Commonwealth Network Environment

Exhibit(s) B.1 through B.6 - Data PowerHouse (DPH) Exhibits

Exhibit(s) C.1 through C.13 - Department of Public Welfare (DPW) Exhibits

Exhibit(s) D.1 through D.15 - Enterprise Datacenter (EDC) Exhibits

Exhibit(s) E.1 through E.43 - Department of Labor & Industry (DLI) Exhibits

Exhibit(s) F.1 through F.4 - Department of Health (DOH) Exhibits

Exhibit(s) G.1 through G.16 - PA State Police (PSP) Exhibits

Exhibit(s) H.1 through H.8 - Department of Revenue (DOR) Exhibits

Exhibit(s) I.1 through I.13 - Commonwealth SAP Environment - Integrated Enterprise Services (IES) Exhibits

Exhibit L - Master Application Inventory

Schedule J.1 - Datacenter Service Level Management

Exhibit(s) M.1 through M.7 - Department of Corrections (DOC) and Pennsylvania Board of Probation and Parole (PBPP) Exhibits

Exhibit(s) N.1 through N.2 - PennDOT Exhibits

Requirements		Describe Compliance
1.	Develop the architecture and define the technology that will be used in the target datacenter environment to support the Commonwealth computing systems.	Offeror must describe the overall architecture and technologies that will be required to run the computing requirements for the Commonwealth.
2.	Provide all technical system support and reporting including: • Multi-Platform Systems Support • Multi-Tiered Storage Management • Network Management • Security Management • Capacity planning • Performance analysis and tuning • Technology Refresh/Life Cycle Management • Annual Audits and Certifications	Offeror must describe overall strategy to provide these Services for each component of its supporting architecture.
3.	Provide a storage management approach which meets the Commonwealth's needs. The storage management approach shall include, but not be limited to, the following: • **Basic** – based on Pay-As-You-Go allocation model with no upfront resource allocation and resources are reserved on demand per workload. (shared, multitenant) • **Committed** – based on Allocation Pool allocation model which gives a minimal initial commitment of resources plus the ability to burst above that minimum if additional capacity is needed – usually a percentage of resources reserved for agency with over-allocation. (shared, multitenant) • **Dedicated** – based on Reservation Pool allocation model – 100% of resources are reservation–guaranteed.	Offeror must describe overall strategy to provide these Services for storage management.

	(dedicated, single tenant)	
4.	Provide real-time monitoring and monthly reporting of system availability, performance, utilization, and efficiency.	Offeror must describe its overall strategy to provide real-time scheduled system performance, operations, monitoring and capacity reporting for the entire datacenter architecture. Offeror must describe its strategy to support or provide real-time system and/or application monitoring
5.	Disaster Recovery - Design a tiered DR solution to ensure that applications and associated hardware that currently have an active DR plan will continue to have offsite Services available in the event of a primary system outage. The tiered DR solution must include an option to support high availability (HA) architectures. Include tiered DR solution in the overall datacenter architecture design.	Offeror must describe its tiered approach to supporting the Disaster Recovery needs of the Commonwealth.
6.	Configuration Item Reconciliation The Offeror must perform an initial asset review of the targeted inventory for all datacenter configuration items (CI) that will be managed. The Offeror must reconcile and validate that appropriate relationships exist for all datacenter configuration information in the Configuration Management Database (CMDB) system. Offeror must ensure that CIs are properly mapped in order to support the established Service Level Agreements (SLAs). The Offeror will be required to provide an automated interface between its CMDB and the Commonwealth's CMDB.	Offeror must describe its approach to gathering this configuration information.

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

Introduction

The Unisys Team has evaluated the exhibits and schedules and used the evaluation as a basis for the solution. Unlike other vendors Unisys is distinctively poised to re-use, as appropriate, current Unisys owned and managed assets and can transition these from the existing data centers to new data centers. During Data Gathering and Transition Planning, Unisys will work with the Commonwealth to develop a consolidation plan to transition all Commonwealth based computing Services on an application by application basis to the Unisys provided data centers and the Unisys-managed infrastructure. We look forward to reviewing the flexible DR architecture and the production and testing environments included in the solution. For instance, the Commonwealth could consider reducing DR costs by allowing Test environments to be leveraged to become part of Production in the very unlikely event of an actual Data Center disaster.

The Unisys solution team has crafted a multi-platform solution across the towers of Windows and Linux server, AIX server, IBM Mainframe, IBM iSeries, Unisys Mainframe, Network, Storage and Monitoring that supports the migration of all specified workloads. The Unisys solution uses the IBM Flex chassis/blade technology to provide hardware that supports both physical and virtual Wintel and Linux environments as well as the AIX environment. The Unisys network solution, in particular, provides diverse network connections of sufficient bandwidth to anticipate network demands for Commonwealth applications.

The Unisys solution team has also proposed tools in the Enterprise Services Catalog that will help the Commonwealth to identify instances where application interfaces are highly dependent on close proximity. The identification of these interdependencies is critical during transition when Unisys will take care to bundle tightly coupled applications into coherent move groups. This transition planning leads to the creation of separate move groups and, by nature, these groups are internally more tolerant of longer latency.

The Unisys solution provides the Commonwealth a very flexible infrastructure environment that is highly modular, addresses the current data center requirements, and is highly flexible in anticipation of future data center needs. For instance, in the Server, Network, and Storage infrastructures the architects have taken a chassis/frame and capacity architecture approach. The Unisys solution team will be able to incorporate advances in both the blades and chassis as the Commonwealth requires additional capacity. In effect, this allows a rolling refresh as capacity increases and is coupled with a technology refresh following standard lifecycle management. The Storage and Network infrastructures follow a similar refresh path both at the next chassis/frame purchase and at the close of the lifecycle for equipment purchased during the early stages of the contract.

1 Datacenter Architecture and Technology

1.A Develop the architecture and define the technology that will be used in the target datacenter

environment to support the Commonwealth computing systems.

Offeror must describe the overall architecture and technologies that will be required to run the computing requirements for the Commonwealth.

The Unisys solution relies on the IBM [redacted] technology for both physical and virtual Wintel and Linux environments as well as the AIX environment. Detailed descriptions of this architecture are provided in Schedule F, Section 3.2.4.1 "Windows Support" and Schedule F, Section 3.2.4.4 "UNIX Support – AIX/Linux Approach".

The Unisys solution includes both [redacted] storage technologies. The unique partnership between Unisys and IBM provides the Commonwealth with a competitive bidding process within the Commonwealth's managed services. Another vendor might propose a single-vendor's monolithic storage frame to meet all of Commonwealth's requirements. Unfortunately this limits the Commonwealth's access to competitive pricing as technologies evolve with lower price points. Detailed descriptions of this architecture are provided in Schedule F, Section 3.2.4.2 "Storage Management".

The Network solution based on [redacted] and [redacted] technologies is detailed in Schedule F, Section 3.1.2 "Network and Security Architecture".

The Unisys Team proposes a [redacted] Mainframe. The processor will have four General Purpose (GP) processors, one z Integrated Information Processor (zIIP) and 6 Integrated Facility for Linux (IFL) processors tightly integrated with IBM storage, tape libraries, and IBM tools to provide the maximum utilization of the powerful compute platform, as described in detail in Schedule F, Section 3.2.4.5.2 "IBM Mainframe Services".

The Unisys mainframe team meets the requirements of the Commonwealth with a new mainframe platform and continued support for the steady reliable services provided in the current contract. The solution includes new Dorado and Libra mainframe environments for production, development and Disaster Recovery. These are offered via the Enterprise Services Catalog. These have been architected to match the characteristics and MIPS requirements as detailed in the Exhibits and descriptions in Schedule F, Section 3.2.4.5.1 "Unisys Mainframe Services"

2 Technical Support and Reporting

2.A Offeror must describe overall strategy to provide these Services for each component of its supporting architecture.

The Unisys strategy for providing these services is presented in organizational detail in Schedule F, Section 3.2.2.2 "Infrastructure Architecture" which presents the IT Service Management (ITSM) layer and the Infrastructure Architecture services that are monitored by the ITSM layer.

Critical to this interaction between the ITSM monitoring and the Infrastructure Architecture services are the tight binding of the ITSM Nagios collectors and the management utilities and tools provided by the vendors of the compute components for servers, storage, network, and mainframes.

As described in detail in Schedule F, Section 3.2.3.2 "Site Operations", the ITSM Nagios Collectors are the ITSM's eyes and ears on the services compute components and tools. The

ITSM "brain" is the [redacted] which provides, among other services:

- Analytics-based intelligence to maximize visibility and control of the Commonwealth's Utility computer model
- Proactive detection of initial issues coupled with Commonwealth-approved runbook automations to resolve incidents.

Provide all technical system support and reporting for Multi-Platform Systems Support

The Unisys Team provides technical support for a wide variety of compute services platforms including Windows, Linux, AIX, Mainframe, and Storage. By using the integrated service management platforms described in section Schedule F, Section 3.2.3.2 "Site Operations" and the multiple tiers of support described in each of the technology solutions in Schedule F, Section 3.2.4 "Managed Hosting Services" and Schedule F, Section 3.2.5 "Capacity on Demand Services", the Commonwealth gains the flexibility of meeting the individual needs for each application's compute infrastructure's deployment while also maintaining the common view of through the Services Portal and ITSM platform.

The reporting for services is provided through the Services Portal's online operational dashboard which is described as part of the Service Management solution in Schedule F, Section 3.2.3.2 "Site Operations".

2.B.3 Provide all technical system support and reporting for Network Management

The Unisys solution brings the Commonwealth's network infrastructure and network management up to the high standards and latest technology that Unisys currently maintains for its newest customers who invested in network technology refreshes as part of their migration into the Unisys-managed data centers.

In order to quickly analyze problems on the network or to isolate problems specific to an application, a distributed sniffer system will be deployed using NetScout. F5 load balancers will be deployed at the new data centers to load balance application traffic.

Unisys provides event management solutions to help provide network connectivity and consistent system response times. Unisys utilizes automated system management tool(s) to provide real- time monitoring and notification of server availability and response times including the stop and start times of servers to support SLA availability measurements. The following tools are the major toolsets to support network and system event management and monitoring.

[redacted]

For a complete understanding of how this subset of Event Management Tools supports enterprise Event Management please refer to Schedule F, Section 3.2.3.2 “Site Operations”.

2.B.4 Provide all technical system support and reporting for Security Management

As with the Network Management described above the Unisys solution brings the Commonwealth security management up to the latest technology and the standard by which Unisys manages its latest customers.

[redacted] firewalls will be deployed at the three data centers. The [redacted] platform is designed around the concept of multiple security zones. The [redacted] device supports various types of security zones, with the understanding that different agencies may have different requirements. From a Unisys perspective, security zones represent virtual sections of the network, segmented into logical areas. Security zones can be assigned to a physical interface or to a virtual system. When assigned to a virtual system, multiple zones can share a single physical interface. The [redacted] devices also utilize built-in IDS sensors.

Through the Enterprise Services Catalog, the Commonwealth also has access to the Unisys Stealth Solution.

The Unisys [redacted] renders users, data, and infrastructure undetectable to cyber criminals. Built to meet requirements for securing sensitive information for the U.S. Department of Defense, Unisys Stealth achieved the National Security Agency’s National Information Assurance Partnership Common Criteria EAL-4+ certification protecting data-in-motion across any network regardless if it is private or public.

Benefits of Unisys [redacted]

- Render data, users, and your data center dark to the outside world
- Securely protect the user, network, and data center
- Unprecedented security without an expensive reconfiguring of the network

2.B.5 Provide all technical system support and reporting for Capacity planning

Unisys provides the Commonwealth/Agencies with a comprehensive integrated IT Service

Management (ITSM) Architecture to run the computing requirements for the Commonwealth. The proposed ITSM Architecture will provide an effective and efficient operational platform to support the Commonwealth/Agencies application infrastructure for the following IT Service Management Processes:

- Event Management
  - Provide infrastructure monitoring for all server, storage and network platforms from a Single Pane of Glass (SPOG) using the [redacted] platform.
  - Leverage existing infrastructure monitoring tools and investments (e.g., [redacted]
- Incident, Problem, Change, Asset Configuration, Release, Service Level Management, Service Request Management, and Knowledge Management will all be implemented using the [redacted] Platform.
- Configuration Management (CMDB) in [redacted] applications using [redacted]
- Availability and Performance Management are supported by the centralized [redacted] Platform with availability and performance monitors (such as IBM System Resource Manager (SRM)) feeding this centralized platform.
- Capacity Management [redacted] to support enterprise capacity management and reporting across all server, mainframe, network and storage devices supporting Commonwealth/Agency applications
- Server and Network Administration using [redacted] for provisioning servers in the cloud environment, patching, software distribution, and compliance for network and server environments.
- Financial Management and Billing will be implemented using the [redacted] tool. It will be integrated with provisioned and requested services from [redacted] and other project sources to present a consolidated billing to the Commonwealth/Agencies.
- Service Validation and Testing (Load Testing – Silk Performer)
- Enterprise Services Catalog /Service Request Management will be implemented using [redacted]
- Reporting will be supported in the Real-time Dashboard, the [redacted]
- Enterprise batch scheduling and management platform is provided with [redacted] to support the Commonwealth/Agencies goal of one enterprise batch management platform while supporting existing batch management platforms [redacted]
- Database Management (optional service)
- Application Management (optional service) – [redacted]

2.B.6 Provide all technical system support and reporting for Performance analysis and tuning

As described in the above item 2.B.5, the Unisys solution relies on the integration of the [redacted] tool set within ITSM to manage Performance analysis. Unisys provides the

technical support required for the required tuning based on the performance analysis. The [redacted] performance tools are integrated through [redacted]. In **Figure 3.1.3-1** below, the [redacted] appears to the [redacted] infrastructure as if the [redacted] is a "Regional/Client Infrastructure".

[redacted]

2.B.7 Provide all technical system support and reporting for Technology Refresh/Life Cycle Management

As part of the overall architecture support, the Commonwealth's environment will be reviewed on a quarterly basis to identify technology, services or components which require replacement to maintain the Commonwealth's business needs and associated service levels. The review will include the following activities. The overall technology refresh plan will be documented in Key Deliverable D-03. This plan will be used for all Unisys supported environments.

Overall life cycle management is performed using the Technology Refresh Plan activities as described in Schedule F, Section.3.2.1.5.1 "Technology Refresh".

2.B.8 Provide all technical system support and reporting for Annual Audits and Certifications

The Unisys team manages regular audits through the Security Management office as described in Schedule F, Section 3.2.2.5 "Security Management". Within this organization the Audit and Regulatory Compliance function has accountability for Unisys Team compliance with Commonwealth IT policies and directives as well as federal and Commonwealth laws, regulations and policies, including the Criminal History Record Information Act (CHRIA), Health

Insurance Portability and Accountability Act (HIPAA), Criminal Justice Information Services (CJIS) regulations, the United States Social Security Administration (SSA)regulations, IRS (Internal Revenue Service) Publications, Commonwealth ITBs and the Payment Card Industry (PCI) standards. This function works with each agency to understand and verify compliance with laws, regulations, and policies as it pertain to each individual agency. The responsibility for conducting contractually required audits or arranging for participation in agency audits falls under this function.

Over the last twelve years the Unisys team has integrated these processes and oversights with the Commonwealth's oversight management. The integration of audits, oversight and remediation has protected the Commonwealth form the type of security breaches such as those that occurred at the State of South Carolina Department of Revenue (2012) and more recently at the State of Washington Office of the Courts.

The Unisys team manages Unisys-provided data centers to SSAE-16 annual audits and adjustments to remain in compliance and correct audit findings.

3 Storage Management

3.A Provide a storage management approach which meets the Commonwealth's needs. The storage management approach shall include, but not be limited to, the following:

Offeror must describe overall strategy to provide these Services for storage management.

Unisys proposes a modular approach to storage provisioning rather than deploying a large monolithic frame infrastructure. The focus on provisioning to smaller-sized frames allows the Unisys team to distribute storage systems across the "Basic", "Committed", and "Dedicated" service types that the Commonwealth seeks. By distributing these services across various frames the Unisys team can evolve an application from a "Basic" service on a shared multi-tenant frame to a "Dedicated" single-tenant frame without incurring the high overhead that would be required through the use of larger monolithic frames.

The Unisys Team recognizes that a fundamental application management requirement indicated by the Commonwealth is the ability to move data seamlessly between multiple data center locations to reduce risk and provide service resiliency. The Unisys strategy to provide these storage services provides multiple levels of storage replication services through the Enterprise Services Catalog. This allows the Commonwealth to select the tool that provides the right levels of replication to match the criticality of applications.

Detailed descriptions on the tools offered to the Commonwealth via the Enterprise Services Catalog are provided in Schedule F, Section 3.2.4.2 "Storage Management".

3.A.1 Basic – based on Pay-As-You-Go allocation model with no upfront resource allocation and resources are reserved on demand per workload. (shared, multitenant)

3.A.2 Committed – based on Allocation Pool allocation model which gives a minimal initial commitment of resources plus the ability to burst above that minimum if additional capacity is needed – usually a percentage of resources reserved for agency with over-allocation. (shared, multitenant)

3.A.3 Dedicated – based on Reservation Pool allocation model – 100% of resources are reservation–

guaranteed. (dedicated, single tenant)

The Commonwealth seeks a utility-based approach that allows maximum price flexibility in the Unisys-provided utility, Storage as a Service model. Within the capacities and tiers specified in the Schedule I Volumetrics tab Unisys is able to provide all of three of the requested service types: "Basic", "Committed" (i.e. Basic with bursting), and "Dedicated". Unisys proposes to meet the "Dedicated" single tenant service by providing dedicated physical hard drives so that these provide dedicated performance characteristics. If the Commonwealth seeks dedicated storage frame assets within the Storage as a Service infrastructure then Unisys proposes to discuss the basis for the reservation pool, including tenancy duration commitments as part of Data Gathering and Transition activities.

Unisys has provided a solution that projects reliance upon multiple [redacted] for Open Systems storage rather than adding this capacity to a few centralized Mainframe-class storage frames such as the [redacted] product lines. This provides the Commonwealth with a fine granularity of storage frames. Therefore Unisys anticipates that depending upon the capacity required for dedicated frames, the current solution has sufficient flexibility to accommodate dedicated storage capacity that is already included in the Schedule I "Volumetrics" capacity requests.

Unisys will integrate its ITSM Incident Management system with the Storage Management dashboards such the [redacted]

The integration of the [redacted] tools sets with the Unisys ITSM solution allows Unisys to set threshold bands and prioritize alerts to create appropriate incident tickets before preliminary indicators develop into actual service incidents or interruptions.

The tools also provide the Unisys Storage team with sufficient details to manage LUN status and investigate LUNS which have become "orphaned" and could be re-assigned to the allocation pool.

4 Real-time System and/or application monitoring and reporting

4.A Provide real-time monitoring and monthly reporting of system availability, performance, utilization, and efficiency.

Offeror must describe its overall strategy to provide real-time scheduled system performance, operations, monitoring and capacity reporting for the entire datacenter architecture.

Offeror must describe its strategy to support or provide real-time system and/or application monitoring

Unisys will utilize the [redacted] platform to monitor and manage availability and performance management across all the infrastructure supporting Commonwealth Agency applications (see **Figure 3.1.3-2**). It will be utilized to proactively manage and optimize application performance by avoiding costly outages, solving issues before service levels are impacted, accelerating mean-time-to-repair (MTTR), and extending mean-time-between-failure (MTBF). It reduces customer impact through predictive analytics and drives preventative automation across a single Proactive Operations platform.

[redacted]

The source performance monitors providing performance data include the following tools:

[redacted]

[redacted] automatically discovers and learns the behavior and performance trends for each of the monitored application service components (CI's); identifying normal and abnormal behavior. Unlike threshold-based monitoring systems, the analytics engine only generates events when there is significantly abnormal behavior. Based on these learned trends, the Commonwealth realizes significant reductions in the number of false events generated by reactive, threshold-based performance monitoring approaches. With fewer, more intelligent events. Unisys will support the Commonwealth by pinpointing and prioritizing the most critical business performance issues.

[redacted] applies real-time predictive root cause analytics to continuously sift through events and abnormalities collected from the application and infrastructure components that support the Commonwealth applications and business services, identifying a prioritized set of the most likely problem causes. The solution applies predictive correlation and filtering techniques that leverage real-time service relationships in the [redacted] and configuration changes collected from [redacted] (or any other change source), along with additional detailed diagnostic data. This information provides continuous visibility into problems as they develop; allowing Unisys support personnel to diagnose intermittent performance issues on-demand without requiring the effort to reproduce a problem. These tools allow Unisys technical support staff to remediate problems quickly and efficiently.

The monthly reporting of system availability, performance, utilization, and efficiency are provided through automation that the Unisys team routinely builds around the solution's ITSM infrastructure described in detail above.

5 Disaster Recovery

5.A Design a tiered DR solution to ensure that applications and associated hardware that currently have an active DR plan will continue to have offsite Services available in the event of a primary system outage.

The transition activity includes a review with the Unisys IT Risk Manager of offsite services currently in use and evaluating these in conjunction with the Enterprise Services Catalog offerings to provide current and long-term coverage for these assets.

5.B The tiered DR solution must include an option to support high availability (HA) architectures. Include tiered DR solution in the overall datacenter architecture design.

Offeror must describe its tiered approach to supporting the Disaster Recovery needs of the Commonwealth.

The Enterprise Services Catalog offerings for Disaster Recovery Service will appear alongside the offerings for production servers so that Agency staff ordering new production gear can specify the criticality of the applications being supported as well as the DR services required.

Alternately after a regular DRP review with the IT Risk Manager or at any time, an authorized Agency staff member may elect to use the Enterprise Services Catalog to augment existing

Production infrastructure with DR infrastructure to fill out gaps in the Agency's DRP.

The DR solution includes not only the same components available in the Production environment but also a rich diversity of DR Tiers allowing the Commonwealth to build sufficient high availability through the Disaster Recovery offering to match the Production equivalent for any application.

During planned Data Gathering workshops the Unisys team will present ways to reduce the Commonwealth's daily spend on Disaster Recovery services. It might not be prudent to assume that a perfect DR service is exactly equivalent to the Production services, as this represents a very high ongoing insurance premium against an event that is extremely unlikely to occur. Unisys currently supports customers in Unisys-provided DR sites who, for instance, provision the DR center at only 75% the compute capacity of what is provided in Production. In support of this cost savings Unisys is able to negotiate to an acceptable delivery schedule, invoked only after a disaster occurred, to bring the DR to full compute capacity. The customer realizes a 25% annual savings by taking on a relatively low risk

The Unisys solution includes these Tiered DR Services:

- Tier 1: Recovery from Tape Backup.
- Tier 2: Accelerated Recovery Tape Backup.
- Tier 3: Recovery from Backups replicated to DR via the [redacted] infrastructure.
- Tier 4: Recovery through asynchronous data replication for Open Systems SAN storage removing the need for Data Recovery.
- Tier 5: Data and O/S level replication for Virtual Windows/Linux instances removing the need for Data Recovery.
- Tier 6: With Agency approval the Tier5 offering can be configured to provide an automatic failover.

Following the review of existing Agency DRPs Unisys may propose alternate Tiers to meet any gaps discovered between broad Agency requirements and the Tiers above.

6 Configuration Item Reconciliation

6.A The Offeror must perform an initial asset review of the targeted inventory for all datacenter configuration items (CI) that will be managed.

The Unisys transition team will complete this initial asset review of the existing Commonwealth CMDB. This review includes interviews with Commonwealth and Agency application owners so that the review is inclusive of the matrix of applications that rely on common components in the CI.

6.B The Offeror must reconcile and validate that appropriate relationships exist for all datacenter configuration information in the Configuration Management Database (CMDB) system.

Offeror must describe its approach to gathering this configuration information.

Unisys will develop a Configuration Management Plan during transition that includes all Configuration Item's (CI's) , attributes and relationships that will be discovered, tracked, stored and maintained in the [redacted] and managed through the Change Management

Processes and procedures. The [redacted] toolset will be utilized across all targeted architecture infrastructure platforms to discovery and populate the [redacted] and the indicated relationships. During transition for each agency and data center – the Unisys Configuration Management Team working with the Unisys and Commonwealth/Agency transition teams will transition the identified, discovered and cleansed and reconciled CI's into the Unisys [redacted] to be managed going forward under Change Management Processes.

The Unisys Configuration Manager and support team will follow detailed processes and procedures to reconcile the information before populating the Unisys [redacted]. The Commonwealth/Agencies will be involved in processes and procedures during transition and ongoing to review and accept changes in configuration data that is stored in the [redacted]

Unisys will provide an automated interface between its CMDB and the Commonwealth's CMDB on a near real time electronic basis. This will be accomplished by utilizing the [redacted] to synchronize CMDB information as well as other ITSM information between the Unisys instance of [redacted] and the Commonwealth's instance of Remedy.

For a complete understanding of the Configuration process and supporting tools please refer to Schedule F, Section 3.2.1.7 "Configuration Management".

6.C Offeror must ensure that CIs are properly mapped in order to support the established Service Level Agreements (SLAs).

The Unisys solution complies with the Commonwealth's SLAs on this point.

6.D The Offeror will be required to provide an automated interface between its CMDB and the Commonwealth's CMDB.

As described above in item 6.A, the Unisys solution meets the Commonwealth's requirement to provide an automated interface between the Unisys and the Commonwealth CMDBs.

Unisys Team Experience

The Unisys Team has clients where we provide Data Center Architecture and Technology services such as American Red Cross, California State University, and the City of Minneapolis to name a few. The details of these clients can be found in Section 4.0, "Prior Experience".

The Unisys Team dedicated to the Commonwealth already uses most of the tools and processes described above. The proposed solution introduces new tools that are currently deployed and managed by the Unisys team for other customers. Thus the learning curve for the new tools has already been addressed by resident experts available to the Unisys/Commonwealth team.

Benefits to the Commonwealth

As the Commonwealth is well-aware, the Pennsylvania-based Unisys team dedicated to the Commonwealth's strategic and operations goals has established a well-honed governance process for providing the Commonwealth with forward-looking architecture proposals to

continuously update the Commonwealth's infrastructure. This process helped propel the Commonwealth to a contract extension with Unisys in 2008 that not only saved the Commonwealth hundreds of millions of dollars but resulted in a significant infrastructure refresh. The Unisys/Commonwealth Infrastructure Architecture governance process, jointly developed over prior years, has resulted in reliable and predictable services throughout transformation activities.

An example of these proven architecture services includes the project in 2008 to develop the high-capacity network to allow State Troopers to electronically transmit mug shots and better communicate with other agencies. Under the 18-month contract, Unisys upgraded the CLEAN system to allow state troopers to connect directly with other state, local and federal law enforcement officials. Unisys provided a high-bandwidth, high-availability network that included new features, such as the ability to transmit directly to troopers' cars. The new system replaced a Law Enforcement Message Switch with a new system based on an open architecture, accessible to Microsoft Windows-based users, as well as to users of the existing system.

3.2 Enable Common Service Portfolio

The Commonwealth currently bases its service management practices on the Information Technology Infrastructure Library (ITIL) v3, a worldwide recognized best-practice framework for the management and delivery of IT Services throughout their full life cycle. Accordingly, the Commonwealth requires that the Offeror's service management practices be based on the ITIL v3 framework and guidance. The Datacenter Architecture, which conforms to a service-oriented structure, is prescribed by the Commonwealth common service framework. The common service framework is comprised of 27 discrete IT Services divided into five (5) categories of service:

- **PMO & Service Management** – This category of service defines the overall datacenter management structure, including interactions with the Commonwealth and business partners.
- **Technical Services** – This category of service defines the datacenter architecture, and prescribes standards for datacenter continuity and security. This level also defines the workload transition process, for when Commonwealth Agencies migrate applications to the new datacenter computing Services model.
- **Facilities Management** – This category of service defines day-to-day datacenter operations and maintenance.
- **Managed Hosting Services** – This category of service defines a set of Commonwealth enterprise datacenter managed Services, each designed to accommodate the specific needs of the Commonwealth.
- **Capacity On Demand and Additional Services** – This category of service defines a set of infrastructure as a service (IaaS) offerings, each designed to provide just-in-time resources to the Commonwealth.

3.2.1 Program & Service Management

3.2.1.1 PMO & Contract Management

The PMO & Contract Management service is responsible for the overall program, projects, and contract elements, and will maintain an active working relationship with the Commonwealth project team. Offeror must assign an executive management team that will drive the processes to complete the due diligence required to make informed decisions and Services offerings that will meet the needs and requests of the Commonwealth. This executive team will also provide ongoing direction and leadership supporting the contract and designated Services, for the duration of the Contract.

The Offeror is required to provide and maintain operational, technical, and management staff contacts so that it is clear to the Commonwealth whom is the most direct contact for each operational area.

Reference Documentation

Schedule H - CCPM Commonwealth Computing Procedures Manual

Requirements		**Describe Compliance**
1.	Establish and maintain a program and project management framework, throughout the term of the contract.	Offeror must describe its proposed program and project management framework that will be used to support this contract.
2.	Establish and maintain a protocol for project estimation: ▪ Scope ▪ Hardware / Software ▪ Manpower to develop, test and implement ▪ All other resources required	Offeror must describe a project estimation protocol suitable for Commonwealth data-center migration projects.

3.	Collaboration meetings, technical exchanges, and forums – Through established procedures and meetings address in good faith all issues, needs, technical exchanges and forums with the Commonwealth team. Provide the technical knowledge, and knowledgeable staff, to effectively support and guide the Commonwealth's technology needs.	Offeror must describe how it will accomplish this.
4.	Translate the Datacenter contract requirements into measurable service level objectives, and codify those requirements by creating a set of service level agreements.	Offeror must provide examples of actual datacenter service level agreements, appropriately redacted to preserve client anonymity.
5.	Establish interim contract management procedures during the transition of datacenter Services. All interim contract management procedures must be negotiated in good faith and approved by both parties.	Offeror must describe an interim procedure to monitor and manage service delivery (conforming to Commonwealth policies and procedures) including but not limited to the following; Problem Management, Change Management, Service Level monitoring and reporting, physical and logical security, project management, etc. while the service is transitioned from the Commonwealth to the Offeror.
6.	Establish and maintain a process for change management for the Datacenter contract as requested or required. The final process developed must be coordinated with the Commonwealth contract compliance group and mutually agreed to by both parties.	Offeror must describe its proposed contract change management process.

7.	Subcontractor Relationship Management - Establish and enforce standards for ensuring subcontractor performance. The Offeror is responsible for all Services provided by subcontractors.	Offeror must describe its subcontractor relationship management process.
8.	Offeror must have experience in managing and supporting Managed Service Solutions for Datacenter Infrastructure Services.	Offeror must document its qualifications within its proposal.
9.	Offeror must have the capability to provide mainframe (IBM & Unisys) Services to support the current and future needs of the Commonwealth.	Offeror must document its qualifications within its proposal.
10.	Offeror must have experience managing and supporting SAP/Oracle ERP environments.	Offeror must document its qualifications within its proposal.
11.	Offeror must be an established firm which has provided hosted datacenter Services for a period exceeding three years	Offeror must document its qualifications within its proposal.
12.	Offeror must currently operate at least 3 Datacenters. Each of those datacenters have to have been operational for at least one (1) year and have a minimum five (5) clients hosted at each.	Offeror must document its qualifications within its proposal.

13.	Offeror must have experience handling comprehensive on-site operations and maintenance of Datacenter Physical Infrastructure Services. The Services must have been provided for a continuous period of at least one year during the last three years ending 2011. The Services may not have been terminated before completion of the relevant contract.	Offeror must document its qualifications within its proposal.

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

Introduction

The PMO serves as a central point of management for the overall program. Through the PMO, Unisys will manage continuous cross-organizational collaboration to achieve strategic business goals for the Commonwealth. The PMO organization serves to:

- Provide centralized and coordinated management of all initiatives and projects undertaken to support the data center compute services contract.
- Work in conjunction with Commonwealth leadership to establish a program governance structure.
- Focus on the coordinated planning, prioritization and execution of projects and subprojects that are tied to the Commonwealth's overall business objectives.
- Conduct activity ranging from providing supporting functions such as development of standardized policies and procedures to the direct management responsibility for achieving business objectives through day-to-day service delivery.
- Act as an integral stakeholder and key decision-maker along with the Commonwealth during the initiation stage of each project/initiative.
- Coordinate effective use of resources and capacity management across all projects and contract activities.
- Provide central point of communication management across projects and throughout agencies.
- Enforce the use of best practices, process standards and project methodology.

The Program Management Office is led by the Engagement Executive, [redacted] All

executives responsible for the seven aspects of the program report directly to Ann.

Figure 3.2.1.1-1 depicts the seven organizations with their basic functions, noting key personnel in red.

Figure 3.2.1.1-1. Seven Organizations Staffing Requirements

Support for the Commonwealth far exceeds the boundaries of the team defined above and detailed further within Section 5. Unisys executives are committed to the success of the Commonwealth all the way up to our Chief Executive Officer, [redacted] who serves as the Executive Sponsor of the Commonwealth of Pennsylvania. [redacted] reports directly to [redacted] Regional Vice President who has served the Commonwealth for the past 29 years building long-lasting executive relationships through 5 administrations. The Unisys Executive Leadership Committee discussed in the front of section 5.0 provides far-reaching support for the Harrisburg, PA based team throughout Unisys and partner leadership.

The **Program Management Office** is an integral part of the current program and has been enhanced over the current DPH PMO to manage the complexities of a much larger and very different DCCS program. This team is responsible for the governance and execution of the overall program, projects, and contract elements, and provides ongoing direction and leadership supporting the contract and designated services for the duration of the contract.

As shown in **Figure 3.2.1.1-2**, the PMO also has supporting staff responsible for the three major functions of Financial Management, Contract Management, and Vendor and Subcontractor Management. The PMO support team functions are further maturing under the new contract. Through the enhanced Financial Management function, this office provides accurate and cost-effective stewardship of IT assets and resources providing a truly transparent analysis of the Commonwealth spending on services. Other enhancements include dedicated focus on subcontractor accountability for performance of services throughout the contract term along with management of third-party software licensing and all maintenance agreements for hardware and software.

Figure 3.2.1.1-2. Project Office Support Team Duties and Staffing Requirements

1. ***Establish and maintain a program and project management framework, throughout the term of the contract. Offeror must describe its proposed program and project management framework that will be used to support this contract.***

The Unisys Team's strategy incorporates a comprehensive approach to transitioning and managing data centers. This proven methodology has been used in more than 187 public sector and commercial outsourcing engagements. In addition to internally consolidating 58 worldwide data centers into one, the Team has had proven success with large outsourcing clients such as United HealthCare, General Services Administration, PECO Energy, BASF, the State of Michigan, IRS, and Kodak.

Working with Unisys on the Data PowerHouse project provides the Commonwealth with years of experience and dedication to Commonwealth business, and will also eliminate the need for ramp up, training, and relationship building required for a new vendor. Leveraging the existing team enables us to provide stable service delivery going forward, and will facilitate the continuation of service improvement efforts already underway ensuring that Commonwealth business does not skip a beat. The Unisys Team has made an investment to certify all staff supporting the Commonwealth in ITIL V3 Foundations and our Service Management Platform is

based on ITIL V3. This depth of process and work ethic brings a strong base of repeatable, consistent development and operations support across the enterprise.

Incumbency Transition through steady-state operations is a key component of our work plan. As the incumbent vendor, Unisys will continue to provide outstanding service to the Commonwealth's mission-critical application infrastructure hosted in the Data PowerHouse, and provide staff augmentation to the operations in the Enterprise Data Center until each location is fully transitioned to the new model. Our incumbency provides us the unique ability to seed the transition and migration teams with knowledgeable resources that understand the Commonwealth infrastructure. This knowledge considerably reduces ramp-up time to train the staff on basic infrastructure support and the priorities and nuances of each agency. It is during this time that we will accelerate our focus on reforming our organizational structure and work processes to meet the changing requirements of the new model.

It is during Month 1 of transition that we will begin to bring key personnel on board to establish our PMO under the new contract starting with the Engagement Executive, [redacted], our Transition Executive, [redacted], the second Transition Manager, [redacted], and Senior Enterprise Infrastructure Architect, [redacted]. Positions currently held by [redacted] and [redacted] will be backfilled on the Data PowerHouse contract. This team will lead all aspects of the transition efforts. We will also bring on the Service Excellence Officer; [redacted] to build our Service Excellence Office that will initially reform workflows of existing ITIL aligned processes to meet the needs of the new model.

Unisys establishes clear delineation of project and program boundaries, and well-articulated outputs. Proper planning enables the program manager to define start and end dates that are based on detailed requirements and accurate cost and resource estimates. A well-defined scope and change control process has been adopted to manage these types of program variations. This includes resource planning and defining roles and responsibilities in advance.

Unisys will establish a framework that utilizes a PMI based methodology. The Unisys Global Project Management Practice (PMP) is an industry best practice approach that employs process, people, and technology to deliver projects on time and within budget. All Unisys project managers have access to the support and training of the Global Project Management Practice and are required to achieve PMI certification. This creates standard skill sets and consistent project delivery. Objectives of the practice include cost optimization (focus on estimating accuracy and cost management), continuous improvement (knowledge sharing, artifact reuse, lessons learned), and governance (tracking metrics, reviews, alignment with account management and client).

All projects managed for and on behalf of the Commonwealth will be delivered using a standard form and method traversing the following phases: Initiating, Planning, Executing, Monitoring and Controlling, Closing. Project collateral will be consistent, supportive, timely, and of a high quality. Communication plans and cadence will be agreed upon with the Commonwealth for each individual project. Unisys has demonstrated its commitment to rigorous project management methodology by delivering multiple parallel projects to the Commonwealth and will continue to do so. The project management approach is best described by the following:

Unisys Solution Delivery Framework (SDF)SM

Unisys has standardized the best project management practices, tested and proven by our experience, into our project management methodology named Solution Delivery FrameworkSM. This provides a formal, yet flexible, approach to formulating, implementing, and maintaining

information systems as driven by the business needs of our clients.

The SDF was developed to assist Unisys delivery teams in providing value-added services to clients, including strategic direction setting, organizational change, and the planning, design, and implementation of information systems. Our methodology, based on Project Management Institute (PMI) standards, is a combination of methods, techniques, and tools used by Unisys to deliver system solutions.

An essential aspect of the SDF is the application of quality management techniques requiring the use of processes, procedures, and guidelines to support the assurance of quality throughout the engagement. Quality assurance reviews are conducted at major checkpoint.

The Framework assists Unisys professionals in planning and managing resources to meet the client's business and technical requirements, on time and within budget.

The primary objective of the SDF is to provide the methods, techniques, and tools to manage one or more related projects, and the scope and flexibility of the SDF addresses small to large, complex engagements. Our four guiding principles are:

- Clear goals are essential for successful projects.
- Adherence to formal and constantly improving best practice processes will provide that all solutions and deliverable products meet their stated requirements.
- Planning and scheduling of all tasks and resources and subsequent monitoring, control, and reporting are essential to solution delivery.
- Agreement on deliverables and definition of an effective change management process are essential to achieving the project's goals.

Our framework provides best practices, templates and guidelines for all project phases from the initial proposal through project closeout.

2. Establish and maintain a protocol for project estimation:

Scope

Hardware / Software

Manpower to develop, test and implement

All other resources required

Offeror must describe a project estimation protocol suitable for Commonwealth data- center migration projects.

Estimating methods used by Unisys are tailored to the specific project. These methods are used to identify project scope, right-size hardware and software configurations, estimate manpower and other resource requirements to develop, test and ultimately implement the project.

The method used for most definitive estimates is to fully define and understand the scope, develop a Work Breakdown Structure (WBS) that encompasses all deliverables for the project, decompose the deliverables to sufficient depth to be able to estimate the components as tasks. Quantify the work breakdowns structure within the boundaries set by project scope. Then apply costing to each element of the work breakdown structure which is summed to a total cost.

As the WBS is formed, we develop extensive documentation for review (to obtain consistent pricing).

Early estimates may employ various means of cost modeling. The basic characteristics of effective estimating include: clear identification of task, broad participation in preparing estimates, availability of valid data, standardized structure for the estimate, provision for program uncertainties, recognition of inflation, recognition of excluded costs, independent review of estimates, and revision of estimates for significant program changes.

During the costing process, we follow a set of best practices that provide repeatable methods that result in high-quality cost estimates that are comprehensive and accurate and that can be easily and clearly traced, replicated, and updated.

The Unisys Team has 30 plus years of experience specific to Commonwealth projects and data center migrations. We take the approach noted above and apply the benefit of subject matter expertise that our Commonwealth experience provides. We employ a detailed estimating technique that generates estimates at the lowest level of detail and builds the summary estimates by rolling up the details. Applying the Delphi Technique of estimation, Unisys leverages corporate subject matter experts (SMEs) to develop estimates for a pre-determined set of tasks or project. A description of the work involved is provided to the SMEs before the exercise begins. The SMEs develop their estimates independently, discuss differences and assumptions, and then go through one or more revision cycles to reach a consensus.

3. Collaboration meetings, technical exchanges, and forums – Through established procedures and meetings address in good faith all issues, needs, technical exchanges and forums with the Commonwealth team. Provide the technical knowledge, and knowledgeable staff, to effectively support and guide the Commonwealth's technology needs. Offeror must describe how it will accomplish this.

Unisys understands the need for meetings to effectively and efficiently communicate important information to program stakeholders as part of a good governance model. However, management meetings are but one component of that communication and governance model.

There will be a three tier meeting structure that will provide visibility at all levels within our respective organizations.

1. *Tier 1 – Executive Governance and Steering Committees*
   The objective of these meetings is to focus on the strategy and goals of the engagement. This will serve to better align the IT initiatives with the business goals of the Commonwealth. These meetings will develop and review strategy for the engagement. It is a forum for sharing insights on application of industry best practices. These meetings should be held monthly early in the contract and quarterly as steady state operations are achieved.

2. *Tier 2 – Program Management*
   Program management meetings focus on operational performance. The objectives of these meetings are to manage performance and effectiveness, manage SLAs and communications, and provide a platform for continuous improvement. These meetings should occur weekly in the transition phase, and monthly as operations reach steady state.

3. *Tier 3 – Service Delivery Management Teams*
   These meetings are meant to handle day-to-day issues. They focus on daily operations, escalation management, 3rd party management and handoffs, and end-to-end incident management. These meetings would occur daily during transition and weekly after steady state is achieved.

All meetings require controlled agendas to verify that they are taking place per their agreed upon frequency and the meetings are productive for all parties. All points for improvement can be added to the CSIIP library to be jointly addressed by Unisys and the Commonwealth.

Examples of subject matter addressed through the meetings held at various levels include the following:

- **Transition and Transformation Plan Tracking** -- Gather status and metrics from Transition and Transformation activities, assess status and risk, identify issues and risks, design and implement mitigation for risks and corrective actions for issues, track to closure at subsequent meetings
- **Contractor Performance Reviews.** Gather status and metrics from Service level activities, Gather status and metrics from Transition, assess status and risk, identify issues and risks, design and implement mitigation for risks and corrective actions for issues, track to closure at subsequent meetings
- **Technical Exchange/Forums.** Will be planned and facilitated by the Enterprise Architecture team with agendas structured to address emerging technologies and their impact on Commonwealth Agency business. These forums promote collaboration and information sharing among agencies in a learning environment that provides structured vendor sessions and access to industry leaders with expertise on relevant technologies. Agendas will be jointly developed with input from the Unisys Team and the Commonwealth Agencies
- **Dispute Management.** Gather the facts, distill facts to relevant information, develop possible solutions, negotiate potential solutions with the disputing organizations, find common ground or acceptable compromise, implement solutions, track for recurring problems until situation is closed
- **Issues/Risk Database.** Track the progress and usefulness of the deployed Services, track the availability of unused services, track status and risk for services, track status and risk for projects. Produce reports for review and comment at meetings, gather information and assignments from meetings, confirm the staff responsible for the issue or risk is aware of guidance from leadership, record status from staff working the issue or risk.
- **Acquisition Planning.** Coordinate and conduct planning sessions to address the enterprise impacts for new hardware of software acquisitions, service deployments, and projects. Document findings in issues/risks database; confirm the staff responsible for the issue or risk is aware of guidance from leadership; record status from staff working the issue or risk.

Unisys will provide the technical knowledge, and knowledgeable staff, to effectively support and guide the Commonwealth's technology needs. An Agency Infrastructure Architect that reports to the Senior Enterprise Architect will be assigned to each agency and directly aligned to the Agency Account Manager to support this need.

4. Translate the Datacenter contract requirements into measurable service level objectives, and codify those requirements by creating a set of service level agreements. Offeror must provide examples of actual datacenter service level agreements, appropriately redacted to preserve client anonymity.

Unisys will work with the Commonwealth to establish Service Level Agreements based on the service levels noted in the Commonwealth's Schedule J.3. The Unisys Team has been managing to Service Level Agreements (SLA) with the Commonwealth on the DPH contract. In 2012, Unisys managed to 427 Commonwealth SLAs monthly, performing at a 99.9% achievement rate. These SLAs included the following:

- System Availability
  - High Availability – 99.9%
  - Non-HA Enterprise Class and Partitions – 99.8%
  - Non-HA Commodity – 99.5%
- Online Transaction Processing Systems availability
- Production Batch Completion On Time

In addition, Unisys has provided the following types of SLAs for other customers:

- Incident Management Response and Resolution
- Timely Incident Root Cause Analysis Reporting
- Backup Management
- Data Restore Timeliness and Accuracy
- Timely Response to Service Requests
- Timely Response to Change Requests
- SAN Availability
- Facility Environmental Controls
- Disaster Recovery Restore Time

The SLA table in **Figure 3.2.1.1-3** below shows actual Service Level Agreements for a redacted Unisys customer.

SLA Description	Required Achievement
Severity Level 1 Incident Acknowledgement Time	95% Response w/in 30 Minutes
Severity Level 2 Incident Acknowledgement Time	95% Response w/in 60 Minutes
Severity Level 3 Incident Acknowledgement Time	95% Response w/in 4 Hours
Severity Level 4 Incident Acknowledgement Time	95% Response w/in 8 Hours
Severity Level 1 Incident Resolution Time	95% Resolve w/in 4 Hours
Severity Level 2 Incident Resolution Time	95% Resolve w/in 6 Hours
Severity Level 3 Incident Resolution Time	95% Resolve w/in 1 Business Day
Severity Level 4 Incident Resolution Time	95% Resolve w/in 5 Business Days
Data Center Server Data Backups	98% On Time Completion
Data Center Server Data Restores	98% On Time Completion

System Change Success	98% Successful System Changes
Platinum Server Pool Availability	99.9% Aggregate Availability
Gold Server Pool Availability	99.5% Aggregate Availability
Silver Server Pool Availability	99.0% Aggregate Availability
Bronze Server Pool Availability	98.0% Aggregate Availability

Figure 3.2.1.1-3: Unisys Redacted Customer SLA Table

Please refer to Schedule J.3 for detail regarding how Unisys will translate and codify the SLA requirements.

5A. Establish interim contract management procedures during the transition of datacenter Services. All interim contract management procedures must be negotiated in good faith and approved by both parties.

Our Team's outsourcing expertise and our operational experience gained from our longstanding partnership with the Commonwealth Agencies will help to make the transition least disruptive to the Commonwealth's end users. Unisys will leverage the current contract management procedures as interim procedures during the transition period with minor modifications that provide the ability to make contractual changes for new service offerings such as on-demand services and the flexibility to make the switch from the fixed-price nature of the current contract to a consumption-based pricing model. These procedures are already approved and familiar to the Commonwealth and as the incumbent, puts Unisys in a good position to minimize any procedural changes.

Ultimately, contractual changes and Commonwealth invoicing will be facilitated using the Enterprise Services Catalog on the Services Portal. The Enterprise Services Catalog contains all data center compute services that can be purchased through the contract. The tool leveraged also provides the capability to track agency spending and automatically chargeback appropriately through the monthly invoicing process. The transition to this tool will involve collaboration with the Office of Administration and agency leadership to establish workflows aligned to change management process governance, and in accordance with agency approval limits, and to establish services to be included in the catalog.

In the interim, we will continue to use a paper based Change Order process. The high-level process in **Figure 3.2.1.1-4** below illustrates the process flow from the point that need is identified by an agency through solution implementation. The change order process is one step in that process.

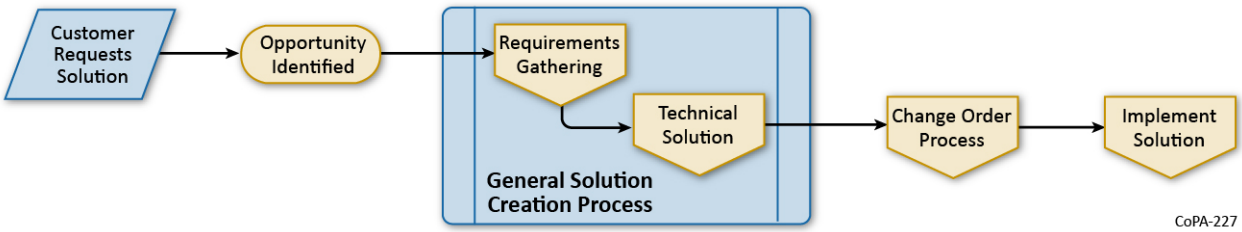


Figure 3.2.1.1-4: High Level Interim Contract Change Management Process

The Unisys Team will work with the Commonwealth to establish interim contract change management procedures. Minimally, the interim process will include the following steps:

1. The agency notifies the Unisys Agency Account Manager that it has a need for data center compute services.

2. The requesting agency, the Unisys Agency Account Manager (AAM) and the Agency Infrastructure Architect (AIA) will engage in requirements gathering.

3. The Unisys Contract Management team will create a paper based request for services form in a format agreed by the Commonwealth. The Contract Manager will document requirements provided by the AAM and AIA and send the form to the agency for approval of requirements.

4. Upon approval of requirements, the Unisys Agency Infrastructure Architect will develop and document the solution.

5. The Unisys Contract Manager will document the solution on the request for service form and provide the form to the agency leader with approval authority, and to the Office of Administration.

6. Receiving approval from the agency and the Office of Administration indicates the project and solution have been approved and can move forward to a change order.

7. The Change Order is a contractually binding document that serves as a means to modify Unisys scope on the data center compute services contract. Upon approval of a request for service, the change order document will be drafted in a format agreed by the Commonwealth.

8. The change order document will be completed to reflect any change in contractual scope and provided to the Contract Compliance team within the Office of Administration.

9. When the change order is approved by Unisys and Office of Administration authorized leadership, Unisys will implement the change to contract scope.

The paper-based change order process will also be leveraged as a means to document hardware and software additions and deletions as well as Service Level Agreements required based on the selected services. The paper-based process will be used in the interim until the Enterprise Services Catalog on the Services Portal and ITSM modules are fully operational. Services used by an agency will be documented by the Financial Management team who will manually track the services pending the availability of a fully operational Enterprise Services Catalog. This will enable agencies to take advantage of the consumption based model, which enables them to use services as needed and discontinue services when they are no longer needed. The information tracked by the Financial Management team confirms that the Commonwealth is only charged for services used. This process will be automated within the Enterprise Services Catalog post transition.

5B. Offeror must describe an interim procedure to monitor and manage service delivery (conforming to Commonwealth policies and procedures) including but not limited to the following; Problem

Management, Change Management, Service Level monitoring and reporting, physical and logical security, project management, etc. while the service is transitioned from the Commonwealth to the Offeror.

During the transition period, the Service Excellence Office which manages program quality will review existing service delivery processes used on the DPH contract. Those processes will be optimized and workflows adjusted to meet the needs of the new contract. Unisys will implement the ITIL compliant procedures for service delivery that will be used for the duration of the contract using workflows in the ITSM system.

Prior to the availability of the automated workflows and business to business connectivity to the Commonwealth's ITSM system, we will utilize the ITSM system in use on the DPH contract to record Problem Management, Change Management, Service Level Monitoring, Project Management, and all other service delivery data. Since that system is not connected to the Commonwealth's ITSM system, Commonwealth users can call the Unisys Service Desk to request services, changes and to report incidents. The Service Desk will then record the information into the Remedy system.

Existing Unisys DPH procedures will be followed in the interim for physical and logical security while these procedures are being drafted for the new contract. Security procedures will be drafted as part of the overall Security Plan key deliverable.

6A. Establish and maintain a process for change management for the Datacenter contract as requested or required. The final process developed must be coordinated with the Commonwealth contract compliance group and mutually agreed to by both parties. Offeror must describe its proposed contract change management process.

The process of Change Management is similar in nature to the interim process previously discussed in that an agency requests changes, requirements and solutions are created, and approvals are obtained, but the main difference is that a large portion of this process will be automated.

Contractual changes and Commonwealth invoicing will be facilitated using the Enterprise Services Catalog on the Services Portal. The Enterprise Services Catalog contains all data center compute services that can be purchased through the contract. The tool leveraged also provides the capability to track agency spending and automatically chargeback appropriately through the monthly invoicing process. The workflows in the Enterprise Services Catalog will be aligned to change management process governance, and in accordance with agency approval limitations.

The high-level process in **Figure 3.2.1.1-5** below illustrates the process flow from the point that need is identified by an agency through service implementation.

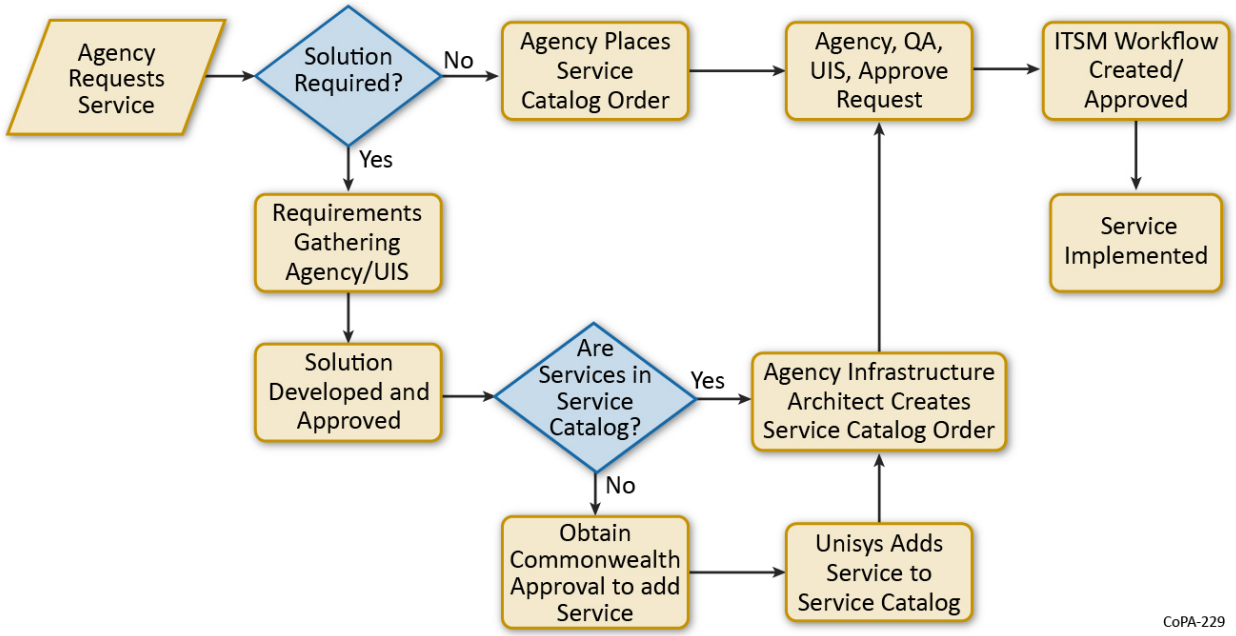


Figure 3.2.1.1-5 High Level Contract Change Management Process

During transition, the Unisys Team will work with the Commonwealth to establish long-term contract change management procedures. Our suggested approach is outlined in Figure 3.2.1.1-5 above. There are many types of change requests that will be executed using this process.

This discussion will address processing of a simple change first followed by the steps required to process a complex change. A simple change is defined as a request for a service or services for which an agency requires no assistance with the solution, and the services are defined in the Enterprise Services Catalog. A complex change is initiated when the complexity of the services needed requires Unisys architect assistance with developing a solution, and/or the services are not currently defined in the Enterprise Services Catalog.

Simple Change Process

1. The agency identifies services needed and places an order from the Enterprise Services Catalog located on the Services Portal. This process is similar to Internet shopping in that agencies can browse all of the services offered, select them for purchase, and place the order.

2. The order will automatically be routed to agency approvers, Unisys approvers, and Office of Administration approvers.

3. Once the order is approved by all parties, automated workflows will be initiated in the ITSM system. The automated workflows open change and service requests that are either automatically provisioned with runbooks or assigned to teams that will implement the new service. Upon approval of the request and ITSM, the services will be implemented.

Agencies also have the capability to use the same process to remove services that they no longer need.

Complex Change Process

1. The agency identifies a need for additional services and places a request for solution from the Enterprise Services Catalog. In this case one or both of the following are true:
   - Addition of the services requires a technology solution to be developed
   - The services needed do not exist in the Enterprise Services Catalog
2. The requesting agency, the Unisys Agency Account Manager (AAM) and the Agency Infrastructure Architect (AIA) will engage in requirements gathering. Requirements will be formally documented by Unisys and approved by the Commonwealth agency to confirm understanding of both parties.
3. Once requirements are approved, the Unisys AIA will develop a solution that will be formally reviewed with the agency. The agency will have the opportunity to recommend changes prior to solution approval.
4. When the solution is approved, the AIA will validate that all services needed are provided in the Enterprise Services Catalog. If there are services needed that are not in the Enterprise Services Catalog, Unisys will approach the Commonwealth to obtain approval to add services to the Enterprise Services Catalog.
5. At the point that all services are available to be ordered in the Enterprise Services Catalog, the AIA creates an order in the Enterprise Services Catalog.
6. The order will automatically be routed to agency approvers, Unisys approvers, and Office of Administration approvers.
7. Once the order is approved by all parties, automated workflows will be initiated in the ITSM system. The automated workflows open change and service requests that are automatically provisioned or are assigned to teams that will implement the new service. Upon approval of the request and ITSM workflows, the services will be implemented.

ITSM workflows will include ensuring that all post-implementation activities are completed at the appropriate time including tasks such as updating operational documentation and the Commonwealth Computing Procedures Manual, updating hardware and software asset information in the CMDB, and updating Service Level Management documentation to include new SLAs.

7. Subcontractor Relationship Management - Establish and enforce standards for ensuring subcontractor performance. The Offeror is responsible for all Services provided by subcontractors. Offeror must describe its subcontractor relationship management process.

Contracts with subcontractors will include all terms and conditions from the Commonwealth contract that are applicable to that subcontractor. There is a PMO Subcontractor Manager assigned to monitor contract compliance and work changes with all subcontractors as may be affected by prime contract change orders/contract changes. Subcontractors are held to the same level of performance as expected of Unisys employees. Our proposed list of subcontractor partners is included in Schedule L of our proposal.

All subcontractors will be governed by the Unisys Supply Management organization including contract terms, services scope, quality, and payments. As part of our subcontractor management process, the Unisys PMO Subcontractor Manager will monitor and measure performance of our subcontractors to verify that services provided are meeting the contract requirements. All quality and non-compliance issues will be managed by Unisys. The Subcontractor Manager will meet with each subcontractor on a monthly or quarterly basis to review status of program activity, the subcontractor's performance, upcoming requirements, pertinent change, incident and problem activity, and identification and remediation of potential performance issues.

Should it be necessary to replace a subcontractor providing service, Unisys will notify the Commonwealth of Pennsylvania with specific plans and a schedule for the subcontractor change. This notification will include a request for Commonwealth approval for the recommended replacement firm who will meet or exceed the qualification of the replaced subcontractor.

Our proposed list of subcontractor partners is included in Schedule L of our proposal and more details on their qualifications in Section 4.1, with past performance highlights in Section 4.5. Section F.3.2.1.1.3 Subcontractor Management provides more detail on Subcontractor Management.

8. Offeror must have experience in managing and supporting Managed Service Solutions for Datacenter Infrastructure Services. Offeror must document its qualifications within its proposal.

The Unisys Team possesses the ability to deliver cost-efficient, high quality, and state-of-the art IT outsourcing services including Managed Services Solutions for Data Center Infrastructure Services. Unisys has implemented global sourcing capabilities not just in the United States, but also in Eastern Europe, China, India, South America, and New Zealand.

Unisys has made strategic investments in system infrastructure, processes, tools, training, and people to build our global delivery model. **Figure 3.2.1.1-6** represents some of our corporate domestic, near shore, and offshore resource strengths in the areas of data center footprints.

[redacted]

Figure 3.2.1.1-6 Global Services Footprint

For worldwide volumes, global reach, and market position for services delivered similar to the Commonwealth of Pennsylvania, please see **Figure 3.2.1.1-7**.

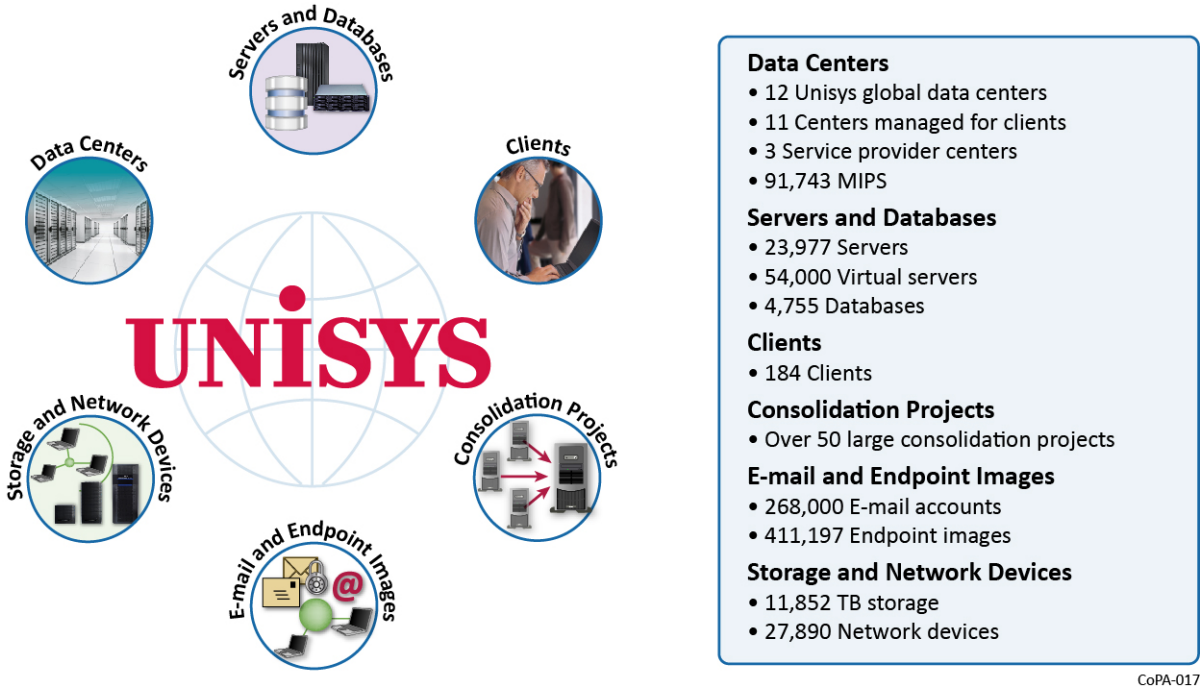


Figure 3.2.1.1-7 Global Services and Worldwide Volumes

Unisys has been managing the Commonwealth Data PowerHouse (DPH) Datacenter since 1999, having successfully transitioned seventeen (17) agencies within a twelve month period. Similar to the Commonwealth's [redacted] model of the new contract, IBM manages the Georgia Technology Authority's consolidated data center. It is a Tier 4 facility housing Midrange and Mainframe equipment and services.

In the United States, Unisys hosts 19 clients in the [redacted] and 9 clients in the [redacted]. The [redacted] acts as the disaster recovery facility for a number of our customers hosted in the [redacted].

9. Offeror must have the capability to provide mainframe (IBM & Unisys) Services to support the current and future needs of the Commonwealth. Offeror must document its qualifications within its proposal.

Unisys and IBM are uniquely qualified in that we would be supporting our own equipment. We have been supporting this equipment for the Commonwealth for nearly 60 years, including the 13 years for the Data PowerHouse.

The reference detail for IBM and Unisys mainframe support client references listed below are documented in Section 4.5 of the proposal.

1. The Internal Revenue Service (IRS): Unisys and IBM mainframes
2. Commonwealth of Pennsylvania: Unisys and IBM mainframes
3. Defense Information Systems (DISA): Unisys mainframes
4. State of Georgia: IBM mainframes
5. State of Washington: IBM mainframes

10. Offeror must have experience managing and supporting SAP/Oracle ERP environments. Offeror must document its qualifications within its proposal.

Unisys currently supports ERP environments for the Commonwealth's Integrated Enterprise System, the PA Liquor Control Board, and the Department of Revenue. As a result of the implementations of these Commonwealth SAP and Oracle ERP systems, Unisys is in the exclusive position of having gone through an actual transition, working closely with Commonwealth experts to build and improve their systems. Experience specific to the Commonwealth that was gained during these implementations is invaluable to future expansions and upgrades to these systems.

The reference detail for SAP support client references listed below are documented Section 4.5 of the proposal.

SAP Systems

1. Commonwealth – IES SAP General Accounting System
2. Commonwealth – DOR SAP Integrated Tax System
3. World Leading Brewery Company - SAP HCM ECC 6.0

The reference detail for Oracle ERP support client references listed below are documented Section 4.5 of the proposal.

Oracle Systems

1. Commonwealth - PLCB Oracle Enterprise
2. California State University – Unified University Management System
3. United Kingdom Ministry of Justice

11. Offeror must be an established firm which has provided hosted datacenter Services for a period exceeding three years. Offeror must document its qualifications within its proposal.

The 140-year history of Unisys is one of reliable, technically excellent, tenacious people helping businesses and governments protect their assets and apply information technology to achieve new levels of competitiveness and success. IBM with its rich 102-year history of innovations has significantly contributed to "making the world work better."

Unisys and IBM are established leaders in providing hosted data center services for many years. In fact, Unisys built the industry's first data center in 1946. For the past thirteen (13) years, Unisys and IBM have been successfully managing the on-site operations and maintenance of the Commonwealth's Data PowerHouse, as well as many other data centers as noted in 8A above.

12. Offeror must currently operate at least 3 Datacenters. Each of those datacenters have to have been operational for at least one (1) year and have a minimum five (5) clients hosted at each. Offeror must document its qualifications within its proposal.

Unisys currently operates 26 data centers, 12 of its own data center facilities, 11 client facilities, and 3 service provider facilities, all of which have been established for a minimum of one year. Unisys has at least three facilities, each with a minimum of 5 clients hosted. Our experience also includes managing the Commonwealth's Willow Oak data center since 1999.

13. Offeror must have experience handling comprehensive on-site operations and maintenance of Datacenter Physical Infrastructure Services. The Services must have been provided for a continuous period of at least one year during the last three years ending 2011. The Services may not have been terminated before completion of the relevant contract. Offeror must document its qualifications within its proposal.

Unisys subcontracts its data center facilities physical infrastructure management services to Jones Lang LaSalle (JLL). As the world's largest facilities management company, we entrust JLL with management of our data center physical infrastructure supporting our systems infrastructure that hosts the most mission-critical applications for our customers. JLL employs the best practices they have honed while managing critical environments and one-of-a-kind facilities on five continents. JLL has been managing Unisys Data Center facilities for over three years.

JLL also provides Facilities Engineering analysis support to provide infrastructure upgrade and capital investment requirements, end-of-service life assessments, Uptime Institute tier level

compliance currency, Infrastructure Change Management planning and oversight, and a host of additional technical support functions to provide ongoing, top notch facility performance.

Unisys currently provides data center facilities physical infrastructure management services in partnership with JLL in the Commonwealth's Willow Oak data center. For more details on Unisys facilities management, please reference Section F 3.2.3.1 Facilities Management.

Services have been provided for a continuous period of at least one year during the last three years ending 2011 from the Unisys facilities. The Services were not terminated before completion of any contract.

Unisys Team Experience

Unisys and our subcontractor IBM have been working with the Commonwealth supporting mainframe systems for many years, and have been managing the Commonwealth Data PowerHouse Data Center for more than 13 years. We are uniquely qualified as a result of the experience gained on the Commonwealth systems and business environments. Even more importantly, we have developed long term relationships and trust with Commonwealth staff. We do not provide a "one size fits all" solution, but work in partnership with each agency on their specific needs and requirements.

In addition, because we manage other data centers, we can leverage a broad base of expertise and staff as situations warrant. Throughout our response to this section, Unisys has cited numerous past experience citations including the ability to support managed data center services across a broad customer base, and a list of current customers that have agreed to provide references for us in the areas of ERP and Mainframe support services.

Benefits to the Commonwealth

We already have many of the Commonwealth process requirements in place, having developed them with the Commonwealth's specific needs and requirements in mind and with their input and participation. Therefore, interim procedures can be quickly implemented with minor adjustments to current procedures, reducing learning curves and duplication of effort. In choosing Unisys to continue data center services, transition risk and knowledge transfer is drastically reduced.

3.2.1.1.1 Financial Management

The Offeror must provide financial management for Services to provide accurate and cost effective stewardship of IT assets and resources. Financial management will be used to plan, control, and recover costs expended in providing the Services. Overall, the goal of financial management is to offer a truly transparent analysis of the Commonwealth spending on Services. In many cases, this analysis of efficiency will be used to create intelligent, metric-based cost-reduction strategies.

Clear and transparent invoicing, both for the Commonwealth and for individual agencies, will be required to insure integrity and accountability of all invoices. It is expected that invoicing may vary somewhat on a monthly basis whenever Services are either increased or decreased.

The Offeror is expected to work with the Commonwealth to identify major investments as part of the budgetary planning process. The Commonwealth will review strategic and tactical objectives as indicated in the planning process to measure impact on its budget(s).

A significant percentage of the Commonwealth's funding comes from federal sources. Offeror's must be able to provide detailed service information necessary to obtain the uninterrupted flow of federal funds.

On a monthly basis, the Offeror must present the Commonwealth with a single enterprise invoice and multiple agency invoices for chargeback purposes. The agency's invoices must include sufficient detail to validate and accurately allocate charges to funding sources based on actual usage.

The Offeror is required to capture and provide information related to monthly volumes of work, counts, and utilization of specific infrastructure areas. The Offeror and the Commonwealth will develop a set of detailed, equitable and repeatable chargeback procedures for each provided Service based on either actual monthly utilization or allocation methods depending on which is most appropriate. The chargeback procedures will include the ability to map to discrete programs and funding sources identified by agencies with this requirement.

The Offeror must integrate its Financial Management tool with the Commonwealth's Enterprise ITSM system which currently is BMC Remedy Billing module and processes; which may change during the term of the resulting contract. The Offeror must leverage any current chargeback procedures and implementation configuration to accelerate the implementation of the new system. The Offeror must expand the chargeback system to capture all related computing related charges associated with the Datacenter project.

Reference Documentation

N/A

Requirements		Describe Compliance
1.	Provide a uniform rate structure which charges the same rates for the same/similar Services.	Offeror must provide detailed descriptions on the type of Services included in its overall solution. Cost information must not be provided in the technical submittal.
2.	Monthly invoicing for Services will be provided to the Commonwealth. Invoicing will identify Services rendered, pricing, and agency specific service usage. Transparency in billing will identify service cost per agency. The Commonwealth does not have a common system for charge backs. Some current services are not charged back, and some are done manually. The selected Offeror must connect to the Commonwealth's ITSM system. The Commonwealth does not require a full charge back system. The agency invoices should provide billing detail so the agency has full transparency into the services it consumed. Billing details shall include all services procured by agency general ledger (GL) code. A service may be allocated across multiple GL codes. Identify method for adjusting agency level billing due to failing to meet SLAs.	Offeror must describe its process or policies that will address this requirement. Offeror must provide at least one relevant example from a prior engagement, in which it was engaged, that is similar to the needs of the Commonwealth.

3.	Flexible pricing will be applied when Services are either increased or decreased.	Offeror must describe its process or policies that will address the flexible pricing requirements. Offeror must provide at least one relevant example from a prior engagement, in which it was engaged, that is similar to the needs of the Commonwealth.
4.	Interim Financial Management Procedures will be required as the Commonwealth transitions its current architecture to the Offeror's Services.	Offeror must describe its approach and procedure(s) for providing invoices, invoice verification and charge back to datacenter customers including but not limited to the following; service components, asset management, asset transfer, forecasting, etc.
5.	During the term of the Contract, provide cost effective approaches and suggestions to improve Services while maintaining or lowering the cost for Services. For example as the industry costs for server and storage capacity are reduced over time, it is expected that there will be a continual cost reduction in like Services within this contract.	Offeror must describe its process or policies that will address this requirement. Offeror must provide at least one relevant example from a prior engagement, in which it was engaged, that is similar to the needs of the Commonwealth.
6.	Integrate Financial Management with other service management processes, especially with SLA, Capacity and Configuration Management.	Offeror must describe how it will accomplish this.

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

Introduction

Through the **Financial Management** function, the PMO provides accurate and cost-effective stewardship of IT assets and resources. They plan, control, and recover costs expended in providing the services offering a truly transparent analysis of the Commonwealth spending on services. Areas of responsibility under Financial Management include:

- **Budgetary Planning**: the budgetary planning function works with the Commonwealth to identify major investments as part of the budgetary planning process.
- **Invoicing**: the invoicing function provides clear and transparent invoicing, both for the Commonwealth and for individual agencies, and provides integrity and accountability of all invoices.
- **Financial Analysis**: the financial analysis function is responsible for the analysis of efficiency that will be used to create intelligent, metric based cost reduction strategies.
- **Chargeback**: the chargeback function provides the accurate capture and provision of information related to monthly volumes of work, counts, and utilization of specific infrastructure areas to provide the necessary transparency.

1A. Provide a uniform rate structure which charges the same rates for the same/similar Services.

Unisys will implement an Enterprise Services Catalog based upon the Service Tiers, Hardware Configurations and Operating Systems found in Schedule I– Offeror Pricing Forms. Utilizing this Enterprise Services Catalog, Unisys will establish standard configurations at a standard price, from which the Commonwealth can order incremental capacity across the hardware platforms within the enterprise. In developing the Enterprise Services Catalog pricing, a work breakdown structure was utilized that provided congruency between similar services.

1B. Offeror must provide detailed descriptions on the type of Services included in its overall solution. Cost information must not be provided in the technical submittal.

A complete list of our detailed descriptions of the type of services included in our offering can be found in Schedule C - Services Catalog. The detailed description of the services is provided throughout Schedule F – Statement of Work. Corresponding rates can be found in Schedule I – Offeror Pricing Forms. These rates will be used consistently to charge for services ordered by the Commonwealth agencies.

2A. Monthly invoicing for Services will be provided to the Commonwealth. Invoicing will identify Services rendered, pricing, and agency specific service usage. Transparency in billing will identify service cost per agency. The Commonwealth does not have a common system for charge backs. Some current services are not charged back, and some are done manually. The selected Offeror must connect to the Commonwealth's ITSM system.

The Commonwealth does not require a full charge back system. The agency invoices should provide billing detail so the agency has full transparency into the services it consumed. Billing details shall include all services procured by agency general ledger (GL) code. A service may be allocated across multiple GL codes.

Unisys has a good understanding and experience with the timing and processes associated with Commonwealth invoicing at the agency level. We will leverage the financial management component within Enterprise Services Catalog as part of the Services Catalog ordering system to pull monthly data by agency for specific services ordered during that billing month. The invoicing will be configured to provide various funding streams and GL codes as identified by each agency during implementation.

Each invoice item will provide the following information:

- Agency name
- Service Name
- Service Identifier (i.e. Product number)
- Unit Price
- Quantity
- GL Account Number (7 digits)
- Department Number (4 alphanumeric characters)
- Reporting Level(4 digits)
- Sub-account number (4 digits)
- SAP Fund number (10 digits)
- Cost Center number (10 Digits)
- Percent Allocation (percentage)

(The percent allocation is used if an invoice item is paid across differing Cost Centers.)

The Unisys ITSM system will have connectivity to the Commonwealth's ITSM system.

Identify method for adjusting agency level billing due to failing to meet SLAs.

The total amount of Service-Level Credits that Unisys will be obligated to pay to the Commonwealth, with respect to Service-Level Defaults occurring each month, will be credited on the invoice that contains charges for the month during which the Service-Level Default(s) giving rise to such credit(s) occurred. For example, the amount of Service-Level Credits payable with respect to Service-Level Defaults occurring in August shall be set forth in the invoice for the August Monthly Invoice Amount issued in September.

If Unisys fails to meet the "Earnback Minimum" objective, Service Level Credits will be calculated and applied on the next Billing Cycle.

2B. Offeror must describe its process or policies that will address this requirement. Offeror must provide at least one relevant example from a prior engagement, in which it was engaged, that is similar to the needs of the Commonwealth.

Any SLA credits that are immediately due to the Commonwealth for that month will be applied against the invoice amount. Unisys and the Commonwealth will establish a process that formally documents SLA violations and their potential for future invoice credit. All violations will be tracked until closure is reached; meaning that either a credit was triggered and invoiced to the Commonwealth or the penalty was earned back by Unisys.

Draft invoices will be generated and presented to the Commonwealth in advance of the invoice due date. Upon approval by the Commonwealth, the actual invoice will be generated and submitted to the Commonwealth per mutually agreed procedures.

On the IBM State of Georgia engagement, chargeback at the agency level is facilitated through the [redacted]. This tool automates the creation of agency level invoices. On this engagement, Service Level Agreements and credits are a part of the

governance structure. Credits are calculated and provided at the agency level.

3A. Flexible pricing will be applied when Services are either increased or decreased.

Based on components ordered from the Enterprise Services Catalog by each individual agency, total invoice amounts for the month will be computed by multiplying the units ordered by the rate from the Catalog of Services Rate Card. In managing the provision of Resource Units (RU), Unisys will maintain the flexibility to respond to changes in the Commonwealth's demand for services, particularly where agencies experience significant variations in demand.

Billable Resource Unit usage is measured on a monthly basis to determine an agency's requested utilization of such Resource Units. Starting on the Effective Date and monthly thereafter, Subcontractor will measure, track and report usage of Resource Units. Unisys method for measuring, tracking and reporting RUs will be reviewed with the Commonwealth prior to full implementation. The automated system used by Unisys to perform this responsibility will be configured to track and record all user entries, reports, modifications, and all other actions taken in relation to the billing source data. Unisys will be responsible for recording all payments due, and for reflecting these amounts in each Monthly Invoice, effective the month following completion and approval by the Commonwealth.

3B. Offeror must describe its process or policies that will address the flexible pricing requirements. Offeror must provide at least one relevant example from a prior engagement, in which it was engaged, that is similar to the needs of the Commonwealth.

The flexible pricing invoice process is described above. This approach has been used with data center services for the State of Texas, American Red Cross, California State University, City of Minneapolis, and data storage for the IRS.

4A. Interim Financial Management Procedures will be required as the Commonwealth transitions its current architecture to the Offeror's Services.

While the Enterprise Services Catalog is being developed and customized to meet all Commonwealth objectives and awaiting Commonwealth approval, Unisys will provide interim manual invoices that will be in an excel format similar to the current DPH invoices. The invoices will include adequate descriptive information, i.e. agency, description of charge, amount, and any required Commonwealth accounting distributions in order to be processed thru the Commonwealth's Financial Management system.

4B. Offeror must describe its approach and procedure(s) for providing invoices, invoice verification and charge back to datacenter customers including but not limited to the following; service components, asset management, asset transfer, forecasting, etc.

Unisys is in the unique position of being able to transition the current contract invoicing seamlessly into the invoicing of the new contract. Prior to the implementation of the Enterprise Services Catalog system and its workflow that will ultimately automate invoice generation, Unisys will continue to leverage manual processes to create invoices. Service components, asset management and transfer, and forecasting functions will be managed and tracked by the Service Excellence Office utilizing the Unisys ITSM system.

Unisys will work with the Commonwealth to define Services Catalog workflows to facilitate the online ordering and approval of the addition and removal of data center compute services. Following a test plan developed in conjunction with the Commonwealth, a complete monthly invoice will be generated in a test mode prior to live billing, utilizing test data so that the

complete process can be tested. This will be submitted to the Commonwealth, resulting in the full spectrum of billing data being confirmed prior to going live. Invoices will provide the level of detail from the Enterprise Services Catalog items.

5A. During the term of the Contract, provide cost effective approaches and suggestions to improve Services while maintaining or lowering the cost for Services. For example as the industry costs for server and storage capacity are reduced over time, it is expected that there will be a continual cost reduction in like Services within this contract.

Unisys will work with the Commonwealth to provide cost effective approaches and suggestions to improve services that may result in lower costs of services for the Commonwealth. Through the structure of this contract, there are opportunities for the Commonwealth to save costs using capacity on-demand resources designed for agencies to pay only for resources consumed. This is one opportunity where an agency can save on resources that are required on a short-term basis negating the need for extensive investments in hardware and software licensing to support a relatively short-term project.

Our Enterprise Services Catalog pricing depicted for each year of the contract takes into account reductions in the cost of technology based on standard industry lifecycles. We have anticipated that, in many cases, the price of technology will decline over time. In those cases, the rate card or Enterprise Services Catalog pricing has been adjusted to reflect the change.

In section 3.2.1.1.6 Continuous Service Improvement, more detail is provided regarding the Unisys Continuous Service Improvement and Innovation Program. The offerings of this program include identification, tracking and completion of initiatives designed to result in continuous improvement in the Commonwealth environment. This improvement can take many forms, including innovations that may result in cost savings to the Commonwealth.

5B. Offeror must describe its process or policies that will address this requirement. Offeror must provide at least one relevant example from a prior engagement, in which it was engaged, that is similar to the needs of the Commonwealth.

The process is described above. Unisys has provided various cost savings opportunities to the Commonwealth as the result of technological advancements through network upgrades, leveraging virtual server environments, providing upgraded mainframes at no additional cost, and leveraging enterprise storage solutions. In addition, as the Commonwealth faced extreme financial challenges over the years, Unisys has worked with the Commonwealth in a true partnership to identify ways to meet those challenges in a manner that saved the Commonwealth money without compromising services. This was evidenced in the contract extensions in 2002 and 2008.

6A. Integrate Financial Management with other service management processes, especially with SLA, Capacity and Configuration Management. Offeror must describe how it will accomplish this.

Support of the environment is accomplished via toolsets that Unisys will deploy for this contract including:

- [redacted]ent
- [redacted])
- [redacted]
- Extensive monitoring toolsets

Unisys will provide a Financial Management Process to support the Commonwealth with integration to many ITSM processes including:

- Enterprise Services Catalog
- Service Level Management
- Change
- Release
- Capacity
- Asset
- Configuration

The integration of the Financial Management Process with the ITIL processes listed above will be accomplished through the integration of process and technology. The Enterprise Services Catalog is managed from a centralized platform for all services and infrastructure that Unisys will provide to the Commonwealth. The Enterprise Services Catalog is maintained with all services, service levels, and billing data to provide transparency to the Commonwealth users using the Enterprise Services Catalog. The Enterprise Services Catalog process is integrated with the Unisys ITIL processes for Change Management, Capacity Management, Service Level Management, Capacity Management and Configuration Management ([redacted]).

Changes approved and deployed to the Enterprise Services Catalog also require changes within the supporting processes including:

- **Service Level Management.** Implementing or updating SLA's for new or updated Enterprise Services Catalog items
- **Release & Deployment.** Updating the workflow for provisioning new or updated Enterprise Services Catalog items
- **Capacity.** Establishing the tracking and forecasting usage and capacity for new or updated infrastructure services
- **Configuration Management.** Implementing new or updated CI's and attributes in the CMDB for new or updated Enterprise Services Catalog items
- **Financial Management.** Updating any billing codes, resource units, prices, integrations in order to bill the Commonwealth correctly

The [redacted] is instrumental to automating the integration of Enterprise Services Catalog and Financial Billing and Management Applications with all the various supporting processes. The Enterprise Services Catalog and Billing Applications are integrated in the [redacted], and includes the following components:

- **iCollaborate is a web-based front end that functions as the entry point into the Enterprise Services Catalog.** iCollaborate performs all authentication, authorization and role adjudication functionality based on integration with the Commonwealth's Active Directory service.

  iCollaborate contains the financial management and billing application which is tightly

integrated with the [redacted] Catalog and [redacted] and [redacted] to integrate all the necessary invoicing and financial management information. [redacted] Financial Billing integrates various sources of billing related data from the Enterprise Services Catalog, project service requests, provisioned infrastructure and Remedy CMDB information to prepare a consolidated invoice for the Commonwealth.

- **iRequest is the Enterprise Services Catalog component. For** the Commonwealth, the Enterprise Services Catalog will allow the user to specify what type of infrastructure service is required, what size is needed, and the support tier for the item being ordered.
- **iDeliver is a complete workflow automation engine.** The iDeliver component interfaces via API directly to the [redacted] for Server Automation, and [redacted]. The iDeliver component will coordinate all change and request management processes, and where automated server provisioning is supported, drive the build of the server environment. The PMG software suite also includes data for billing as well as online reporting for utilization, provisioning and de-provisioning.

Unisys Team Experience

Unisys has been working with the Commonwealth with financial management services as required by the current Data PowerHouse contract for more than 13 years. In addition, through other data center contracts, we have developed a variety of processes and financial models from which to leverage for the Commonwealth. A number of Unisys existing customers including California State University, the City of Minneapolis and the State of Texas have benefited from the ability to leverage flexible services that can be purchased via standard rate card unit pricing and used for the term required thus avoiding the need for capital investments to secure computing resources to meet short-term needs.

Benefits to the Commonwealth

We already have many of the Commonwealth process requirements in place, having developed them with the Commonwealth's input and participation. Therefore, existing procedures with slight modifications can be deployed as interim procedures, reducing learning curves and duplication of effort. The Unisys Team also has an in-depth understanding of the agency structure and the need for agency project level reporting and the importance of separate invoicing. Additionally, we have a proven track record of leveraging emerging technology to reduce overall cost to the Commonwealth and ultimately citizens of Pennsylvania.

3.2.1.1.2 Governance & Policy Compliance

Major IT decisions related to this Contract will be reviewed and approved according to the Commonwealth's governance policy. These decisions are critical to the success of the Commonwealth. IT governance addresses compliance initiatives, and satisfies the need for greater accountability for decision-making.

Reference Documentation

Schedule B - Governance

	Requirements	Describe Compliance
1.	Major IT decisions will be made under the guidance of the Commonwealth governance organization.	Offeror must describe its overall compliance policy and enforcement measures. Offeror must provide at least one relevant example from a prior engagement, in which it was engaged, that is similar to the needs of the Commonwealth.
2.	Design and architecture decisions will be made with a high level of integrity and advance the interests of the Commonwealth. All designs must be approved by the Commonwealth.	Offeror must describe the overall design and architecture methodology. Offeror must provide at least one relevant example from a prior engagement, in which it was engaged, that is similar to the needs of the Commonwealth.
3.	All policies and procedures will be executed in a consistent manner to ensure the Services are completed as planned and consistent with specifications. Audits will be conducted on a yearly basis to verify and report on compliance with policies and procedures.	Offeror must describe its compliance and audit policy and enforcement measures. Offeror must provide at least one relevant example from a prior engagement, in which it was engaged, that is similar to the needs of the Commonwealth.

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

Introduction

The IT infrastructure architecture being proposed provides a foundation for the applications which support the Commonwealth's business activities. By establishing an ongoing IT governance function, the Commonwealth will be able to maintain an alignment between the infrastructure architecture, provided services, business needs, application requirements, and compliance initiatives. The IT governance process shown in **Figure 3.2.1.1.2-1** below is supported by our enterprise architecture team and will interact with both the account's overall governance process and service delivery. More details about the overall process and governance structure can be found in section 3.2.1.5 Technical Architecture.

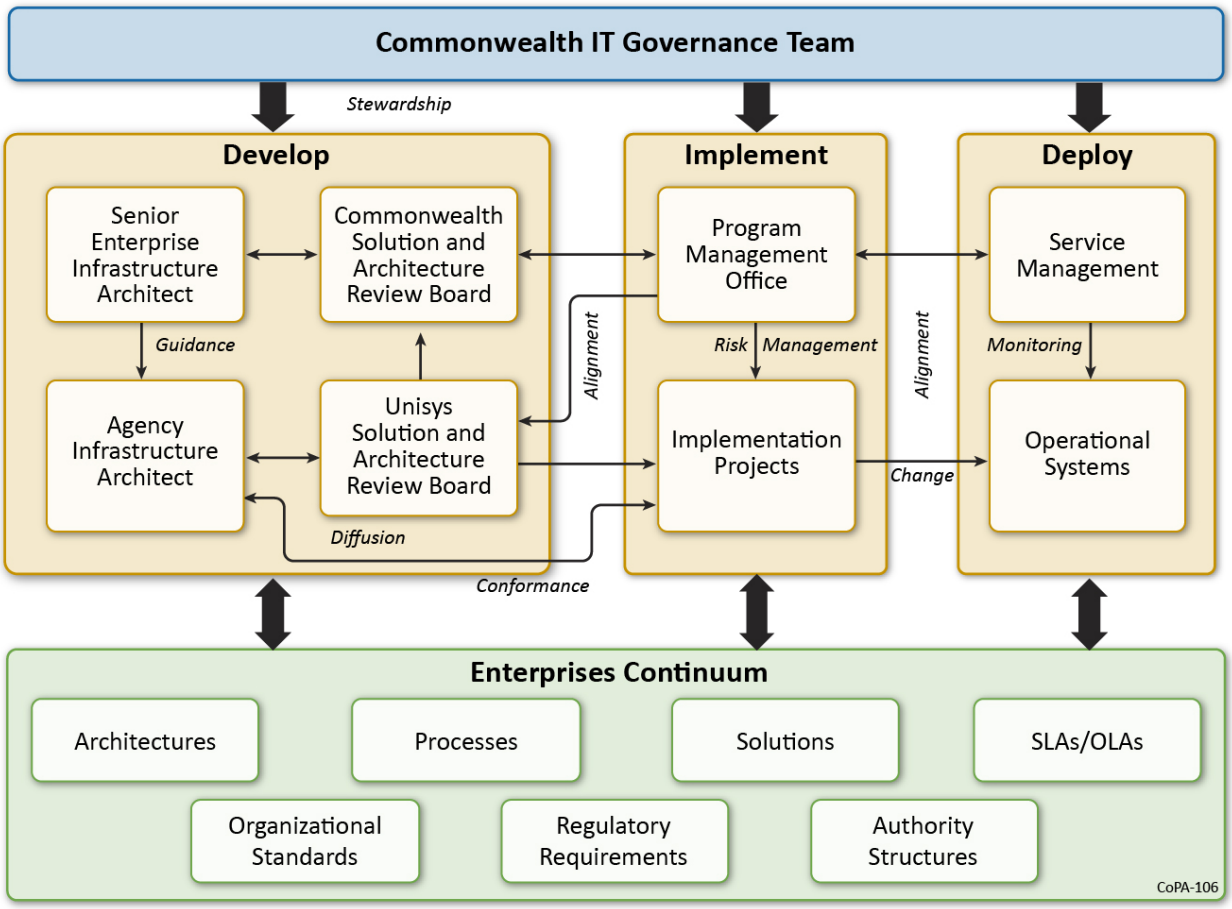


Figure 3.2.1.1.2-1 Unisys IT Governance Process for the Commonwealth

1. Major IT decisions will be made under the guidance of the Commonwealth governance organization. Offeror must describe its overall compliance policy and enforcement measures. Offeror must provide at least one relevant example from a prior engagement, in which it was engaged, that is similar to the needs of the Commonwealth.

The Commonwealth will be a key participant in major IT decisions for the infrastructure architecture and associated services supporting the Commonwealth's environment. The Unisys Team will use the IT governance activities to receive the Commonwealth's guidance and approval for requested solutions and major IT decisions. The Unisys Enterprise Architect team,

will establish a Solution and Architecture review process and organization which will be aligned to work with the Commonwealth's IT Governance team to review each solution and major IT decision prior to the implementation of each solution. The Senior Enterprise Infrastructure Architect will also work with the Program Manager and the Engagement Executive to communicate major IT decisions which have an impact to the overall account and may require review and approval by the Commonwealth's Contract Governance team.

2. ***Design and architecture decisions will be made with a high level of integrity and advance the interests of the Commonwealth. All designs must be approved by the Commonwealth. Offeror must describe the overall design and architecture methodology. Offeror must provide at least one relevant example from a prior engagement, in which it was engaged, that is similar to the needs of the Commonwealth.***

Unisys will develop solutions and provide architectures with a focus on quality to support the Commonwealth and its business needs. The architecture of the services provided by the Unisys team will be documented within the Key Deliverables D-01 (Datacenter Architecture Plan and Roadmap), D-03 (Technology Architecture and Refresh Approach), and D-04 (IT Service Continuity Architecture and Plan). Each of these documents will be reviewed within the Solution and Architecture Review Boards as part of Transition and when architecture changes are developed. Please see **Figure 3.2.1.1.2-2** below. To maintain the consistency and quality of the Commonwealth's requested services, each solution will be developed using a common set of activities which cover the solution development lifecycle up to the Agency's approval. This lifecycle includes the following activities.

- Receive Request
- Gather Requirements
- Review and receive Commonwealth approval for requirements
- Review current services against requirements
- Develop solution
- Review and approve solution within Unisys Solution and Architecture Review Board. The Unisys Solution and Architecture Review Board will be comprised of the Senior Enterprise Infrastructure Architect, Agency Infrastructure Architects, Chief Information Security Officer and technical support leads.
- Review and approve solution with Commonwealth Solution and Architecture Review Board. The Commonwealth Solution and Architecture Review Board should be comprised of the Unisys Enterprise Architect team, Unisys technical support leads (as needed), Commonwealth IT Governance participants, and Agency representatives (as needed).

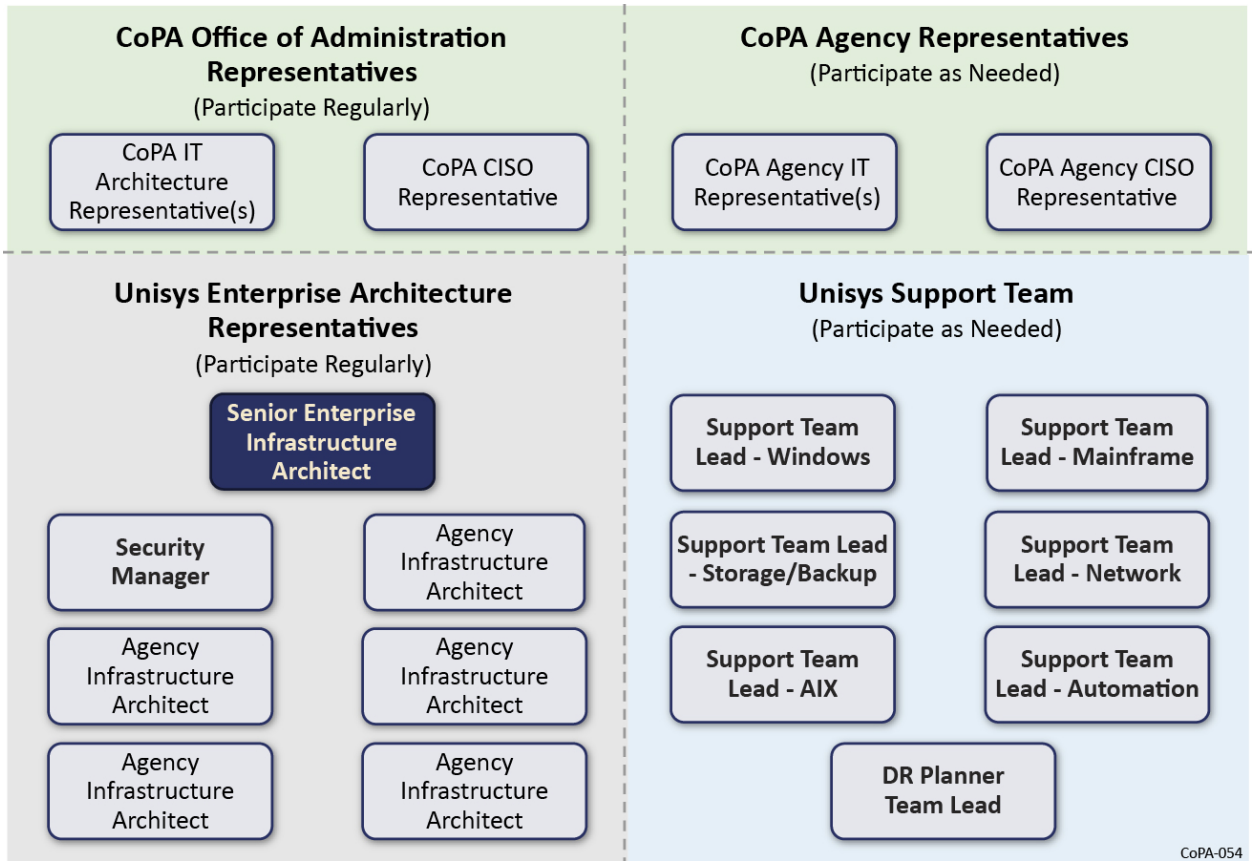


Figure 3.2.1.1.2-2 Unisys Enterprise Architecture Team for the Commonwealth

- Review and approve solution with Commonwealth Agency requestors
- Transfer to Project Implementation team.

With the American Red Cross account, the Unisys team develops solutions based on the requestor's requirements and reviews each solution in detail with the Red Cross' review board before the projects are approved for implementation.

3. All policies and procedures will be executed in a consistent manner to ensure the Services are completed as planned and consistent with specifications. Audits will be conducted on a yearly basis to verify and report on compliance with policies and procedures. Offeror must describe its compliance and audit policy and enforcement measures. Offeror must provide at least one relevant example from a prior engagement, in which it was engaged, that is similar to the needs of the Commonwealth.

Procedures used to provide data center compute services will be documented within the Commonwealth Computing Procedures Manual (CCPM). All members of the Unisys team will be trained to perform their duties in compliance with procedures outlined in the CCPM. Unisys will conduct annual SSAE 16 audits at its data center locations to audit our organization's compliance to processes and procedures. The scope of this audit also encompasses work completed by our subcontractors.

On the DPH contract, Unisys conducts a SSAE 16 SOC2 audit on an annual basis that serves to audit all operational policies and procedures. This audit is performed by KPMG who performs a

thorough review of processes and work products of Unisys and its subcontractor's compliance.

Unisys Team Experience

Unisys has more than 13 years of developing consistent policies and procedures specific to and in partnership with the Commonwealth of Pennsylvania through the Data PowerHouse. As part of the services provided currently to the Commonwealth, each solution is developed by collecting requirements from the Agency's technical team in participation with the Unisys account managers and appropriate solution representatives. The solution is designed based on consistent technical standards and reviewed with the requesting Agency's representatives throughout the development. Each solution is reviewed and approved by the Agency to confirm it will support the Agency's needs before the project is implemented.

With the American Red Cross account, the Unisys team develops solutions based on the requestor's requirements and reviews each solution in detail with the Red Cross' review board before the projects are approved for implementation. As the American Red Cross is an FDA regulated account, each solution includes the additional documentation to support the quality requirements.

Benefits to the Commonwealth

Unisys has familiarity with the Commonwealth's processes and procedures that no other vendor has. Transition time will be more seamless, reducing costs for Commonwealth staff in lost time and resources.

3.2.1.1.3 Subcontractor Management

The Offeror may provide some of its Services and offerings via subcontractors. The Offeror must be the prime provider of Commonwealth Services, and is responsible to contract with subcontractors, manage its subcontractors, and for Offeror's performance and the performance of its subcontractors throughout the term of the Contract.

Reference Documentation

N/A

	Requirements	Describe Compliance
1.	Obtain, manage, and be responsible for all Services or offerings provided by subcontractors. Subcontractors may change over the course of this contract. Offeror is required to notify the Commonwealth of the new subcontractor(s) and assure the Commonwealth that there will not be a conflict of interest, and that the new subcontractor meets or exceeds the qualifications of the replaced subcontractor. The Commonwealth must approve all subcontractors.	Offeror must describe / list all subcontractors that it will be utilize for this project. Describe process or policies that will address this requirement. Offeror must provide at least one relevant example from a prior engagement, in which it was engaged, that is similar to the needs of the Commonwealth.
2.	CJIS Security Policy requires fingerprint based background checks and executing a Management Control Agreement (MCA) and Security Addendum with the Pennsylvania State Police (additional information is provided in the PSP exhibit material).	Offeror must describe its process or policies that will address this requirement.

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

Introduction

Unisys will utilize subcontractors who have expertise above and beyond what Unisys could provide on our own. We understand the importance of managing subcontractors, as their performance is essential to our ability to meet our contractual requirements to the Commonwealth This also gives us the opportunity to support Small Diverse Businesses who might not otherwise have such opportunities, and provide them with the opportunity for mentoring with experienced corporate leaders. All subcontracts will be managed per the terms of the prime contract and will be held to the high performance standards Unisys requires of itself.

1A. Obtain, manage, and be responsible for all Services or offerings provided by subcontractors subcontractors may change over the course of this contract. Offeror is required to notify the Commonwealth of the new subcontractor(s) and assure the Commonwealth that there will not be a conflict of interest, and that the new subcontractor meets or exceeds the qualifications of the replaced subcontractor. The Commonwealth must approve all subcontractors. Offeror must describe / list all subcontractors that it will be utilize for this project. Describe process or policies that will address this requirement. Offeror must provide at least one relevant example from a prior engagement, in which it was engaged, that is similar to the needs of the Commonwealth.

Unisys will be delivering managed services to the Commonwealth as the prime contractor and will be responsible for all services and offerings provided by subcontractors. Our proposed list of subcontractor partners is included in Schedule L of our proposal.

All subcontractors will be governed by the Unisys Supply Management organization including contract terms, services scope, quality, and payments. As part of our subcontractor management process, the Unisys Program Management Office will monitor and measure performance of our subcontractors to verify that services provided are meeting the contract requirements. All quality and non-compliance issues will be managed by Unisys.

Subcontractors are governed by the Unisys PMO Subcontract Manager who will meet with each subcontractor to review status of program activity, the subcontractor's performance, upcoming requirements, pertinent change, incident and problem activity, and identification and remediation of potential performance issues.

Should it be necessary to replace a subcontractor providing service, Unisys will notify the Commonwealth of Pennsylvania with specific plans and a schedule for the subcontractor change. This notification will include a request for Commonwealth approval for the recommended replacement firm who will meet or exceed the qualification of the replaced subcontractor.

Unisys has relevant experience providing services to the Commonwealth on the Data PowerHouse project. In this project, Unisys has proven the effectiveness of strong partnerships with several subcontractors providing data center computing services including IBM, American Personnel Management Corporation and Innovative Business Concepts. We have significantly expanded our partnerships for the new data center compute services contract that features key partners IBM and Deloitte with augmentation by a team of 10 Small Diverse Businesses that bring various complementary services to the Unisys Team. Our proposed list of subcontractor partners is included in Schedule L of our proposal and more details on their qualifications in Section 4.1, with past performance highlights in Section 4.5.

2A. CJIS Security Policy requires fingerprint based background checks and executing a Management

Control Agreement (MCA) and Security Addendum with the Pennsylvania State Police (additional information is provided in the PSP exhibit material).

2B. Offeror must describe its process or policies that will address this requirement.

Unisys is accustomed to completing Commonwealth specific background checks in accordance with the Commonwealth ITB. We will perform fingerprint background checks on all personnel required to do so per the CJIS policy and will execute the MCA and Security Addendum with the PA State Police. As part of our ISO27001 certification, we perform an annual 3rd party/subcontractor review as well.

All employees and subcontractors providing data center services either remote or onsite are subject to background checks and form signatures as well as annual security training. Those that do not require physical access to the facility are subject to a one-time Department of Corrections (DOC) check and are not issued a badge. Per the Commonwealth policy on contractors, each remote user is also subject to an annual Pennsylvania Access to Criminal History (PATCH) background check.

Onsite Data Center employees and contractors are subject to an annual DOC background check, form signatures and a one-time PA State Police (PSP) fingerprint check. They are also required to have their picture taken for a Unisys employee or contractor badge and are required to take the annual security training.

Unisys Team Experience

Unisys has long-term established relationships with most of our selected team. The IBM subcontractor relationship on the DPH contract has truly proven the value of a "powerhouse" team that provides the strongest technology skill sets in the platforms developed by our respective companies. We are also very familiar with Commonwealth background check procedures and have followed them in support of Commonwealth contracts.

Benefits to the Commonwealth

As a result of our experience with these subcontractors and subcontracting in general, transition time and knowledge transfer will be minimized. There will not be relationship growing pains with the Unisys team that other teams may experience ensuring focus on the success of the Commonwealth's transition.

3.2.1.1.4 Business Partners Management

The Commonwealth has business partners such as banks and insurance companies that require connections to its hosted systems and applications. The Offeror must coordinate with the Commonwealth to support any Commonwealth – Business Partner agreements that require a committed connection to its hosted systems.

Reference Documentation

N/A

	Requirements	Describe Compliance
1.	The Offeror must provide coordination and support of Commonwealth – Business Partner agreements that require connections and Services to the Offeror's datacenter Services to ensure that any committed connections and service levels are maintained.	Offeror must describe its process or policies that will address this requirement.

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

Introduction

Unisys is committed to working with all Commonwealth Business Partners to affect efficient processes and successful service delivery. Our network team has worked diligently in the past to provide connectivity required by the Commonwealth in all aspects of the Data PowerHouse service delivery. We anticipate this to continue as the scope expands under this proposal.

1A. The Offeror must provide coordination and support of Commonwealth – Business Partner agreements that require connections and Services to the Offeror's datacenter Services to ensure that any committed connections and service levels are maintained.

1B. Offeror must describe its process or policies that will address this requirement.

The Commonwealth's requirements for Business Partner connections to hosted systems and applications in the Offeror's data center will be supported by the proposed solution. Unisys will work closely with the Commonwealth to coordinate and support the implementation of the connections of Commonwealth Business Partners to the data center services.

The transition planning process will include the assessment and detailed planning for support of the specific network and security requirements of each Commonwealth Business Partner. Additional telecommunication circuits and equipment to connect Commonwealth Business Partners to the proposed data center facilities are not included in this solution and will be the

responsibility of the Commonwealth.

We understand that the Commonwealth's Business Partners (BP) provide the physical circuits to the Commonwealth's BP network into the Commonwealth's Co-Location space within the [redacted] and DPH. The Business Partner determines the number, size and redundancy of the individual BP connections. Unisys will support these connections by providing Security, Access, and Network Connections to the Commonwealth Network, Floor/Cabinet Space, Cooling, and Power. The Commonwealth or the Business Partner is financially responsible for these circuits.

The Commonwealth can access the Enterprise Services Catalog for services pertaining to Business Partner connections such as colocation services to host, relocate connections to the Unisys data center, etc. When services are selected, we will work with Commonwealth Business Partners to plan for an effective relocation/installation of their connections in the [redacted] and the DPH to the Unisys data centers as necessary.

Unisys Team Experience

Unisys has developed a working relationship with Commonwealth staff currently providing this service. As a result of the Data PowerHouse contract and constantly expanding demands in this arena, Unisys has had to become familiar with the Commonwealth's responsibility in order to effectively support and complement network connectivity.

Benefits to the Commonwealth

Because Unisys has been delivering connectivity services for the past 13 years, the transition effort will be better understood mitigating risk of poorly planned transition of connectivity.

3.2.1.1.5 Additional Planning Services

The Commonwealth may use different/additional methods for requesting technical information and support. Depending on the type of request those methods could include but not be limited to:

- Statement of Objectives (SOO)
- Work Order
- Service Request
- Request for Technical Analysis
  - Cost-Benefit Analysis
  - Conceptualization
  - High Level Estimate (HLE)
  - Technical Opinion(s)

Reference Documentation

N/A

Requirements		Describe Compliance
1.	Statement of Objectives - Perform requested additional Services across various functional areas, where the work requires funding either because of materials needed or because the activity requested is not part of the base contract.	Offeror must describe its ability and timeframes to support these additional service requests.
2.	Work Orders - Perform work across various functional areas, where the work is considered part of the base contract and where no additional funding is required.	Offeror must describe its ability and timeframes to support these additional service requests.
3.	A Service Request will be used to request work within one functional area, where the work is considered part of the base contract and where no additional funding is required.	Offeror must describe its ability and timeframes to support these additional service requests.

4.	Requests for Technical Analysis will be used to seek information regarding potential technical solutions. The documents generated by the Offeror must provide the Commonwealth with direction regarding a specific technology and possibly the estimated cost to implement the solution. Four types of requests for technical analysis may be made by the Commonwealth. These requests are described below: • Cost-Benefit Analysis - A cost-benefit analysis is requested when the Commonwealth wants to know not only the implementation cost of a solution, but also the cost-benefit ratio for Commonwealth implementation of the solution. It may be used to analyze a single solution against the status quo, or compare the relative costs of multiple solutions. • Conceptualization - A conceptualization is requested when the Commonwealth has an objective, but is unsure about the possible technical means of fulfilling it. The Offeror must examine multiple paths for achieving the objective, and provide the technical benefits and consequences of the possible solutions presented. Costs are not considered in a conceptualization. • High Level Estimate (HLE or sometimes referred to as a rough order of magnitude ROM) - A	Offeror must describe its ability and timeframes to support these additional service requests.

	HLE is requested when the Commonwealth has a clear technical direction and needs rough estimates on the cost of implementing it. HLEs may be used to attach a cost estimate to a prior conceptualization or technical opinion produced by the Offeror. • Technical Opinion(s) - A technical opinion is requested when the Commonwealth has a specific technology or set of technologies it wants the Offeror to analyze for both technical merits and suitability for deployment in the Commonwealth environment. While product and operational costs provided in Offeror's literature may be considered in a technical opinion, the Offeror's deployment and operational costs will not be calculated or presented.	

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

Introduction

As the Commonwealth's business needs change, different types of requests may be submitted to the Unisys team for various solutions and activities. These requests can go from activities to perform regular pre-approved functions to complex solution development or investigations supporting Agency projects or plans.

Each type of Solution request will proceed through the following activities.

1. Service Request submittal
2. Requirements Gathering

3. Requirements Approval by Requesting Agency
4. Solution Development
5. Unisys Solution and Architecture Review
6. Commonwealth Solution and Architecture Review
7. Agency Approval
8. Transfer Approved Request to Implementation Project Team

1. Statement of Objectives - Perform requested additional Services across various functional areas, where the work requires funding either because of materials needed or because the activity requested is not part of the base contract. Offeror must describe its ability and timeframes to support these additional service requests.

The Commonwealth can submit Statement of Objectives solution requests to receive additional services for multiple functional areas which require additional materials or functions not available as a regular service from the base contract. The Agency Infrastructure Architects will develop and present the solution based upon the completion of the above activities. Depending on the complexity of the requirements, the solution can be presented within 4-6 weeks on average.

2. Work Orders - Perform work across various functional areas, where the work is considered part of the base contract and where no additional funding is required. Offeror must describe its ability and timeframes to support these additional service requests.

The Commonwealth can submit Work Order solution requests to receive additional services for multiple functional areas which do not require additional materials and functions are available as a regular service from the base contract. The Agency Infrastructure Architects will develop and present the solution based upon the completion of the above activities. Depending on the complexity of the requirements, the solution can be presented within 2-4 weeks on average.

3. A Service Request will be used to request work within one functional area, where the work is considered part of the base contract and where no additional funding is required. Offeror must describe its ability and timeframes to support these additional service requests.

The Commonwealth can submit Service Request to receive additional services for a single functional area and is defined as regular service from the base contract. For requests which are not defined within the CCPM as a Standard Service Request, the Agency Infrastructure Architects will develop and present the solution based upon the completion of the above activities. Depending on the complexity of the requirements, the solution can be presented within 1-2 weeks on average.

For Standard Service Requests, the request will be entered within the Enterprise Service Catalog and then routed to the appropriate support team to implement a scheduled change request. Standard Service Requests will include a completion due date.

4 Requests for Technical Analysis will be used to seek information regarding potential technical

solutions. The documents generated by the Offeror must provide the Commonwealth with direction regarding a specific technology and possibly the estimated cost to implement the solution. Four types of requests for technical analysis may be made by the Commonwealth. These requests are described below:

- ***Cost-Benefit Analysis - A cost-benefit analysis is requested when the Commonwealth wants to know not only the implementation cost of a solution, but also the cost-benefit ratio for Commonwealth implementation of the solution. It may be used to analyze a single solution against the status quo, or compare the relative costs of multiple solutions.***
- ***Conceptualization - A conceptualization is requested when the Commonwealth has an objective, but is unsure about the possible technical means of fulfilling it. The Offeror must examine multiple paths for achieving the objective, and provide the technical benefits and consequences of the possible solutions presented. Costs are not considered in a conceptualization.***
- ***High Level Estimate (HLE or sometimes referred to as a rough order of magnitude ROM) - A HLE is requested when the Commonwealth has a clear technical direction and needs rough estimates on the cost of implementing it. HLEs may be used to attach a cost estimate to a prior conceptualization or technical opinion produced by the Offeror.***
- ***Technical Opinion(s) - A technical opinion is requested when the Commonwealth has a specific technology or set of technologies it wants the Offeror to analyze for both technical merits and suitability for deployment in the Commonwealth environment. While product and operational costs provided in Offeror's literature may be considered in a technical opinion, the Offeror's deployment and operational costs will not be calculated or presented.***

Offeror must describe its ability and timeframes to support these additional service requests.

Requests for Technical Analysis - The Commonwealth can submit Technical Analysis solution requests to receive architectural or additional technical support. The Agency Infrastructure Architects will develop and present the estimate to produce the Technical Analysis based upon the completion of the above solution request activities. Depending on the complexity of the requirements, the solution to provide the technical analysis estimate can be presented within 2 - 4 weeks on average.

Technical Analysis requests can be submitted for several different types of activities. Each activity will require various amounts of time to complete and will be based upon the requirements provided during the initial solution requirements gathering. The resulting report for the technical analysis can be presented from 2-12 weeks after the approval of the analysis's estimate.

Cost-Benefit Analysis – The Unisys process steps to build a cost benefit analysis include the following actions: develop a list of alternative projects/programs; identify the stakeholders for each of the alternate projects; select measurements and measure all cost/benefit elements. Then we form work groups to assess and predict outcome of cost and benefits over relevant time period; convert all costs and benefits into a common set of numbers that can be compared; and then calculate net present value of project options. Using the available information we perform sensitive analysis and down select the options to a single choice. We document the choice, and provide the background data on the non-selected options to provide a complete picture.

Conceptualization – During Technical Analysis, Unisys Enterprise Architect team will identify and address possible options to achieve requirements. During the collection of options, we evaluate each option, consider the utility and ability to address the requirement, assess the vulnerability of the option (how stable it is when combined with other functions), and we determine the likelihood the option will meet requirements and consequences of using the

option on the rest of the system (interoperability and maintainability). We continue to identifying options and evaluating the utility by looking at the integrated effect (options joined together into a system to achieve the commonwealth requirements). From this conceptualization process emerges a framework to describe and produce the desired result.

High Level Estimate – Estimating methods used by Unisys are tailored to the specific project. The method used for most definitive estimates is to fully define and understand the scope, develop a work breakdown structure (WBS) that encompasses all deliverables for the project, decompose the deliverables to sufficient depth to be able to estimate the components as tasks. Quantify the work breakdowns structure within the boundaries set by project scope. Then apply costing to each element of the work breakdown structure which is summed to a total cost. As the WBS is formed, we develop extensive documentation for review (to provide consistent pricing).

Early estimates may employ various means of cost modeling. The basic characteristics of effective estimating include: clear identification of task, broad participation in preparing estimates, availability of valid data, standardized structure for the estimate, provision for program uncertainties, recognition of inflation, recognition of excluded costs, independent review of estimates, and revision of estimates for significant program changes.

During the costing process we follow a set of best practices that provide repeatable methods that result in high-quality cost estimates that are comprehensive and accurate and that can be easily and clearly traced, replicated, and updated.

Technical Opinion – Providing Technical Opinions is a 4-step process consisting of formulating alternative opinions, evaluating alternative plans, comparing alternative plans, and selecting the recommended integrated plan.

Formulate Alternative Opinions. Alternative plans are developed in a systematic manner to confirm that all reasonable alternatives are evaluated for feasibility. In addition to requirements, Commonwealth architectural guidelines are considered, interoperability, availability, maintainability, and reliability are considered. We also look at data restoration, service definitions, and service level agreement concepts when gathering data for technical opinions.

Evaluate Alternative Plans. The evaluation of each individual alternative consists of measuring or estimating the economic, environmental, and social effects of each plan, and determining the difference between the without- and with-project conditions. Feasible opinions (plans) are carried forward for comparison against one another.

Compare Alternative Plans. Alternative opinions (plans) are compared, focusing on the differences among the plans identified in the evaluation phase including commonwealth senior engineering comment. Differences between the benefits produced by the opinions are assessed. The overall strategic planning objectives are quantified and used for comparison/screening.

Select Recommended Integrated Plan. A recommended plan is identified from a cost effectiveness perspective and requirements allocation perspective The two plans are then combined into a third option to create the recommended technical opinion with two feasible opinions.

Unisys Team Experience

We are uniquely qualified as a result of the experience gained on the Commonwealth systems

and business environments. Even more importantly, we have developed long term relationships and trust with Commonwealth staff. We do not provide a "one size fits all" solution, but work in partnership with each agency on their specific needs and requirements.

In addition, because we manage other data centers, we can leverage a broad base of expertise and staff as situations warrant.

Benefits to the Commonwealth

We already utilize many of these techniques with the Commonwealth and can continue to build upon that foundation as needs change and expand. Processes are already in place, having developed them with the Commonwealth's specific needs and requirements in mind and with their input and participation. Therefore, lost time as a result of transition will be minimized, with reduced learning curves and less duplicate effort. In choosing Unisys to continue data center services, transition risk and knowledge transfer is drastically reduced.

3.2.1.1.6 Continual Service Improvement

The purpose of the Continual Service Improvement is to reduce risk, improve service quality, improve client satisfaction, and ensure service transparency through a continuous cycle of evaluation and improvement.

Reference Documentation

N/A

Requirements		Describe Compliance
1.	Reduce service risks.	Related to the project management and contract management role, Offeror must describe its methods for eliminating or mitigating service risks.
2.	Improve service quality.	Offeror must describe its methods for addressing continuous service improvement processes.
3.	Improve client satisfaction.	Offeror must provide examples of previous Offeror initiatives aimed at continually improving client satisfaction.
4.	Ensure service transparency.	Offeror must describe its methods for ensuring service transparency and providing visibility into service execution.
5.	Customer Satisfaction Surveys – Survey of Service Desk satisfaction is a key component of providing best in class customer service. Receive completed surveys of Service Desk satisfaction from the Commonwealth and tabulating results from such surveys	Offeror must describe its approach to perform surveys of Service Desk satisfaction for a subset of the problems, questions, or requests that are resolved by, or coordinated by, the Service Desk. Offeror must describe its approach to creating and advertising a web site for day-to-day feedback from datacenter customers which is accessible through the Offeror's KMP. Offeror must describe its approach to performing a customer satisfaction survey on a quarterly basis.

6.	Improve/reduce costs	Offeror must identify its methods for addressing continuous service improvement targeted at minimizing or reducing costs of Services and operations.

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

Introduction

Quality, Continuous Service Improvement and client satisfaction all begin with the voice of the client. Unisys recognizes the voice of the Commonwealth and the significant importance of quality and continuous service improvement to reduce risk, improve service quality, improve client satisfaction, and provide service transparency through a continuous cycle of evaluation and improvement within an IT infrastructure.

Customer Satisfaction. Unisys views quality and continuous service improvement as a critical success factor in driving customer satisfaction for the Commonwealth IT infrastructure. Unisys is establishing a dedicated Service Excellence Office (SEO) to proactively oversee quality management, continuous service improvement, ITIL process management, and customer satisfaction through a comprehensive Quality Plan which specifically addresses all stated requirements. We believe this is a key differentiator in our partnership with the Commonwealth.

Quality Planning. Unisys will develop, implement, manage and govern two detailed quality plans. The initial quality plan will be a Transition Quality Plan to confirm that quality is a primary focus in the critical transition of the Commonwealth agencies to the new data center compute services contract. Unisys will also develop and manage the IT Service Management Quality Plan, to oversee improvement on steady state ongoing operations. These plans will be documented, updated, and governed through the Commonwealth Computing Procedures Manual (CCPM). The SEO will use the quality plans to drive best in class services and the highest customer satisfaction experience throughout entire engagement with the Commonwealth.

Service Excellence Office. The SEO quality plan defines the Service Excellence Office. The SEO function provides definition and oversight of all ITIL process management and analysis functions including change management, release management, incident management, problem management, asset management, configuration and CMDB management, availability management, and service level management. Process managers and analysts working in the Service Excellence Office will audit process effectiveness, ensuring service delivery teams comply with proper execution of processes, and analyzing process trends for anomalies. Continuous Service Improvement programs in collaboration with Commonwealth agencies are managed by the Service Excellence Office.

Figure 3.2.1.1.6-1 Service Excellence Office Functions

The functions of the Service Excellence Office are shown in **Figure 3.2.1.1.6-1** above. The SEO will manage and drive quality across the Commonwealth's multi-dimensional, complex, and matrixed IT service delivery organizations. The SEO will standardize quality across Commonwealth agencies, Unisys, partner organizations, as well as across all ITIL IT services processes, IT monitoring and automation tools, and client satisfaction surveys and processes. Unisys will leverage the ITIL framework, ISO certifications, Six Sigma Lean tools, and our Continuous Service Improvement and Innovation Process (CSIIP) to proactively verify the highest quality IT services are being provided.

1 CI Service Risk

1.A Related to the project management and contract management role, Offeror must describe its methods for eliminating or mitigating service risks.

Risk management, independent quality audits, and business continuity management are integral quality management processes. Unisys is committed to managing risks and ensuring business objectives are achieved and ensuring quality processes are followed. Risk will be mitigated through the implementation of tight quality controls: standard policies, procedures, roles, risks assumptions, issues, and definitions (RAID) etc. Unisys will manage multiple risk registers for large projects, changes, implementations, and transitions. In addition Unisys will manage an overall Program Risk Register. The risk types, tools, analyses, and processes are outlined in **Figure 3.2.1.1.6-2** below.

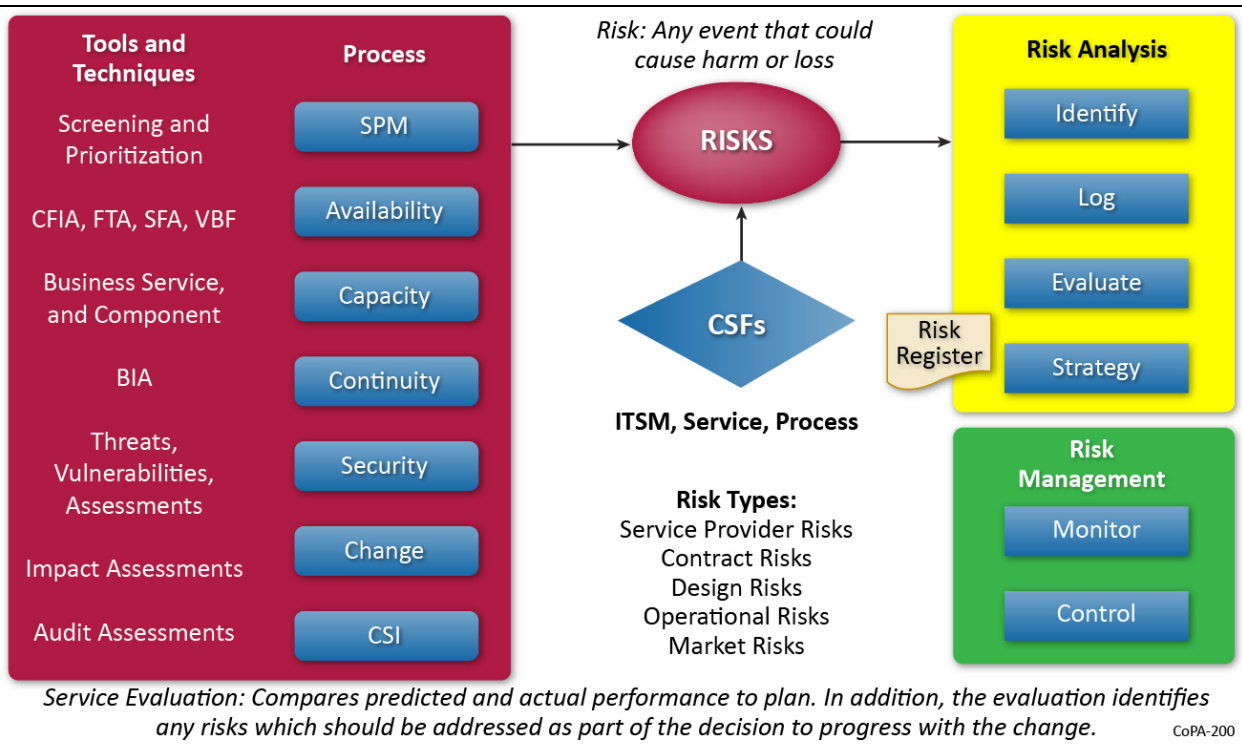


Figure 3.2.1.1.6-2 Reducing Service Risks

2 CI Service Quality

2.A Offeror must describe its methods for addressing continuous service improvement processes.

Improve service quality

To implement continuous service improvement and overall service quality, Unisys will implement an ITIL service delivery framework drives standardization and service excellence.

ITIL Service Delivery Framework – Driving Standardization and Service Excellence

The ITIL process management function is at the core of Service Excellence. This function effectively designs the management practices, processes, functions, roles, knowledge and skills the Unisys Team will use to enable us to deliver services that create value to the Commonwealth. Through IT Service Management, processes are developed and executed to facilitate the implementation and management of quality IT services which meet the needs of the Commonwealth. This discipline is essential to verify we consistently produce quality services in a timely and cost-effective manner.

Unisys engages in quality planning activities to verify changes are planned, documented, accomplished and evaluated. The quality planning process establishes quality goals and objectives are appropriate to meet the requirements of the Commonwealth.

Quality planning provides a framework to guide the evolution and continuous improvement of

the quality plans through the Plan-Do-Check-Act (PDCA) continuous improvement cycle.

PLAN - Who will do what by when? What materials are needed?

DO - Implement the plan

CHECK - Evaluate the effort and results

ACT - Identify actions that need to be taken

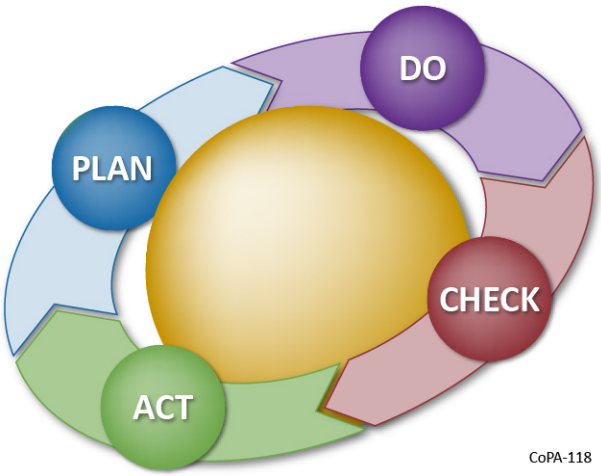


Figure 3.2.1.1.6-3: Plan-Do-Check-Act Cycle

The quality planning PDCA cycle pictured in **Figure 3.2.1.1.6-3** above requires input from each of the highly matrixed organizations and processes within the Commonwealth IT Infrastructure: Input will be proactively obtained from the Commonwealth agencies; Unisys; 3rd party partners; as well as from the ITIL management processes: Service request, capacity and performance, incident and problem, change and Release, availability, service level management; monitoring and automation tools and CSAT surveys. The outputs of each phase of the PDCA cycle provide the inputs to the subsequent phase. This PDCA will be proactively managed by the SEO during the Commonwealth Transition as well as through the steady state IT service delivery processes.

Continuous Service Improvement

Continuous Service Improvement and quality will be the key objectives of the Service Excellence Office. The SEO objectives will be to focus on increasing efficiency, maximizing effectiveness and optimizing the cost of Commonwealth IT services and the underlying IT Service management processes, while maximizing customer satisfaction. Unisys will continually align and re-align IT services to the changing business needs of the Commonwealth agencies by identifying and implementing improvements to IT services support business processes. SEO reviews, analyzes and makes recommendations on improvement opportunities in each ITIL lifecycle phase. These reviews, analyses, and recommendations will also leverage Six Sigma Lean methodologies to drive specific, measurable results. We identify and implement individual activities to improve IT service quality and improve efficiency and effectiveness of the ITIL processes. Quality standardization will be a major objective for the Service Excellence Office. This will improve the cost-effectiveness of delivering IT services to the Commonwealth while driving service excellence and maximizing customer satisfaction.

These Continuous Service Improvement objectives will be accomplished through listening to the voice of the customer, building effective relationships, learning each Agencies business goals and priorities, leading and managing ITIL processes, and delivering quality services to the Commonwealth. The SEO will proactively manage the ITIL lifecycle processes, while leveraging ISO certified processes, and best in class industry tools and methodologies. The SEO will

manage key continuous service improvement activities to confirm Unisys is meeting the Commonwealth's IT service objectives, and driving quality and client satisfaction within each Commonwealth Agency and its clients. Unisys SEO will review management information and trends to verify services are meeting agreed service levels, as well as to confirm the output of the ITSM processes are achieving the desired results. Unisys will leverage Six Sigma Lean practices to drive definitive results.

In addition conducting maturity assessments against the process activities and roles to highlight areas of improvement or concern will be a key focus, along with internal audits to verify compliance. Six Sigma Lean Kaizen workshops will be periodically conducted to identify and prioritize CSI opportunities, analyze data, and present recommendations to senior management to confirm Unisys is hearing the voice of the customer and meeting client expectations, while driving quality results. The SEO will work with all levels of Commonwealth management to confirm service improvement activities are receiving the necessary support and are resourced sufficiently to implement quality, best in class solutions. The SEO will proactively work with each Commonwealth agency to verify ITIL processes are consistently implemented and managed and quality standards are created and adhered to. Quality management reviews will be conducted consistently across the Commonwealth to drive continuous service improvement to drive value to the Commonwealth of Pennsylvania, through improved services, lower costs, improved return on investment, and improved quality, client satisfaction, and customer value.

The Unisys Resolution Optimization Model in **Figure 3.2.1.1.6-4** below provides a clear example of how Unisys will provide Continuous Service Improvement to the Commonwealth. The Unisys SEO organization will proactively manage IT incidents, problems, and changes through ITIL service management processes and operations. Leveraging ISO certified processes and Six Sigma Lean Tools to drive quality and client satisfaction. These processes will be managed across all of the Commonwealth agencies and domains. The Quality management processes will be standardized and be integrated across the Commonwealth agencies, Unisys, IBM, Deloitte, and the Small Diverse Businesses.

Unisys Resolution Optimization Model

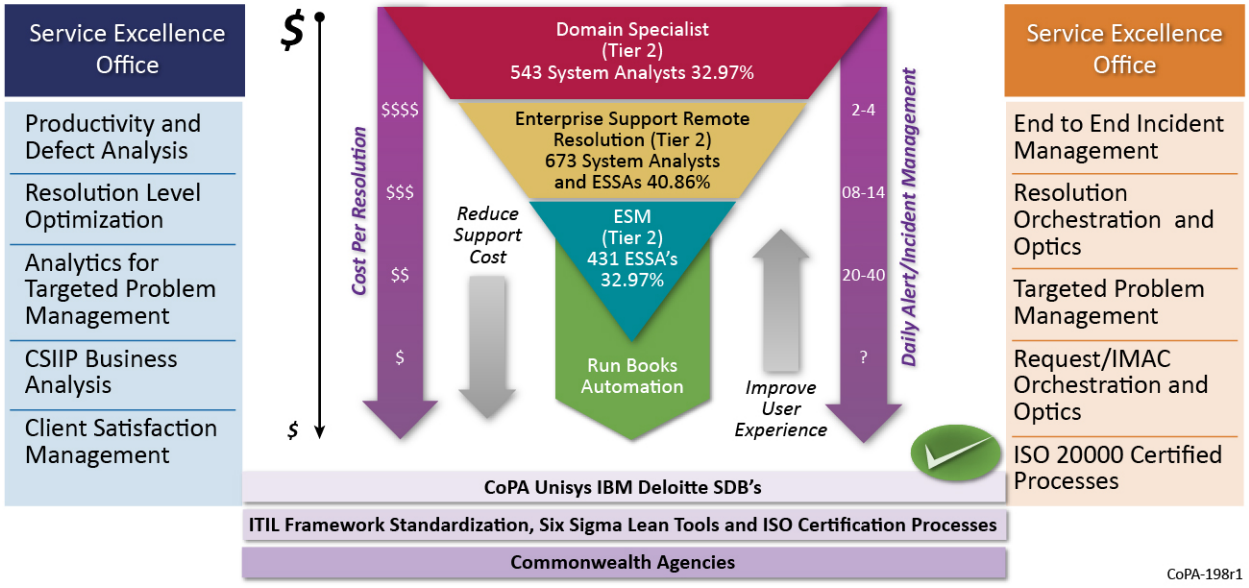


Figure 3.2.1.1.6-4 Unisys Resolution Optimization Model

3 CI Client Satisfaction

3.A Offeror must provide examples of previous Offeror initiatives aimed at continually improving client satisfaction

Improve client satisfaction.

The Project Quality Office is the independent organization within Unisys chartered as the key quality advisor to the operating groups on deal structures, risk management, and project performance. The PQO reviews and evaluates all aspects of proposals and project engagements with the goal to minimize risk while maximizing client satisfaction over the entire lifecycle.

Unisys will work with the Commonwealth to conduct two types of project reviews, Project Readiness Reviews (PRR) and Quality Assurance Reviews (QAR), to identify any potential problems or gaps.

The Project Readiness Reviews (PRR) is designed to verify: the project is properly planned; the project plans are sufficiently adequate, accurate and detailed; the projects contracted solution can be delivered on-time and on-budget; and the appropriate risk management is included (identify approaches to manage/mitigate risks). Unisys will conduct these project readiness reviews during major project implementations. These PRRs will specifically be conducted during transition to confirm a quality solution and implementation will be provided.

Unisys will also work with the Commonwealth to conduct quality assurance reviews (QAR). QARs will be performed periodically by independent reviewers, who are not part of the Unisys account team. This process provides a second level of quality and risk review using individuals who are independent of the Unisys client serving team. This process also provides an unbiased view of engagement progress, risk management actions, client satisfaction, and advice on solving problems and making improvements. The client interview is part of the QAR process.

Business Continuity Management (BCM)is an integral aspect of Corporate Governance and Unisys quality solution. BCM includes key areas of - disaster recovery, facilities, risk, HRM, supply chain , quality, health and safety, knowledge , emergency , and security management, crisis communication and public relations. Unisys provides for three levels of business continuity - basic, custom and emergency. Unisys will work with the Commonwealth to provide a comprehensive BCM program management, maintain a suitable BCM Policy, and verify decisions are made based on Business Impact Analysis (BIA). We will also create business continuity, crisis management, resource recovery and solution plans. The implementation of recovery plans will follow a defined and approved risk assessment methodology. Every Business Continuity Plan, Resource Recovery and Solution Plan, and Crisis Management Plan will be tested (annually at a minimum).

Risk Management, Independent Program Quality Office Audit Reviews, and Business Continuity Planning are key programs Unisys will provide and manage in order to minimize risk throughout the ITIL lifecycle phases.

4 CI Service Transparency

4.A Offeror must describe its methods for ensuring service transparency and providing visibility into service execution

Ensure service transparency.

In addition, Unisys will implement the Continuous Service Improvement and Innovation Process (CSIIP) and leverage Six Sigma Lean methodologies to govern the quality process and drive transparency for the Commonwealth for all the quality initiatives and process improvements. A CSIIP SharePoint portal will be created and maintained with all improvement and innovation actions. **Figure 3.2.1.1.6-5** demonstrates how we build business value into our support of the Commonwealth through careful application of 6 sigma lean methodologies. We accomplish assessments to baseline our current state of operations. Then we build principles of operation to guide data to day functions. Using CSIIP we clarify, optimize the concepts, and collaborate with a wide range of subject matter experts to verify we are focused on the right subjects for innovation. Then we focus our intent, proactively defining and designing the innovations which lead to improvement.

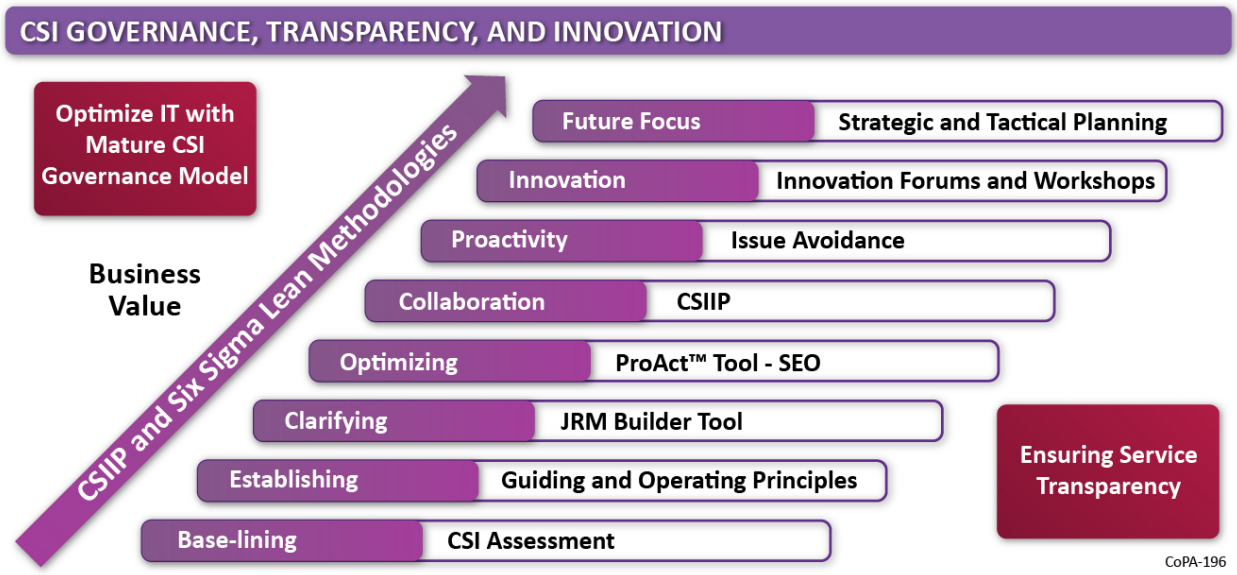


Figure 3.2.1.1.6-5 CSI Governance, Transparency and Innovation

We will build a CSIIP portal which will be accessible to all the Commonwealth agencies. The SEO and SSL team also support innovation activities managed through Innovation Workshops to collaborate with the Commonwealth agencies to plan and develop the future IT strategies and IT solutions.

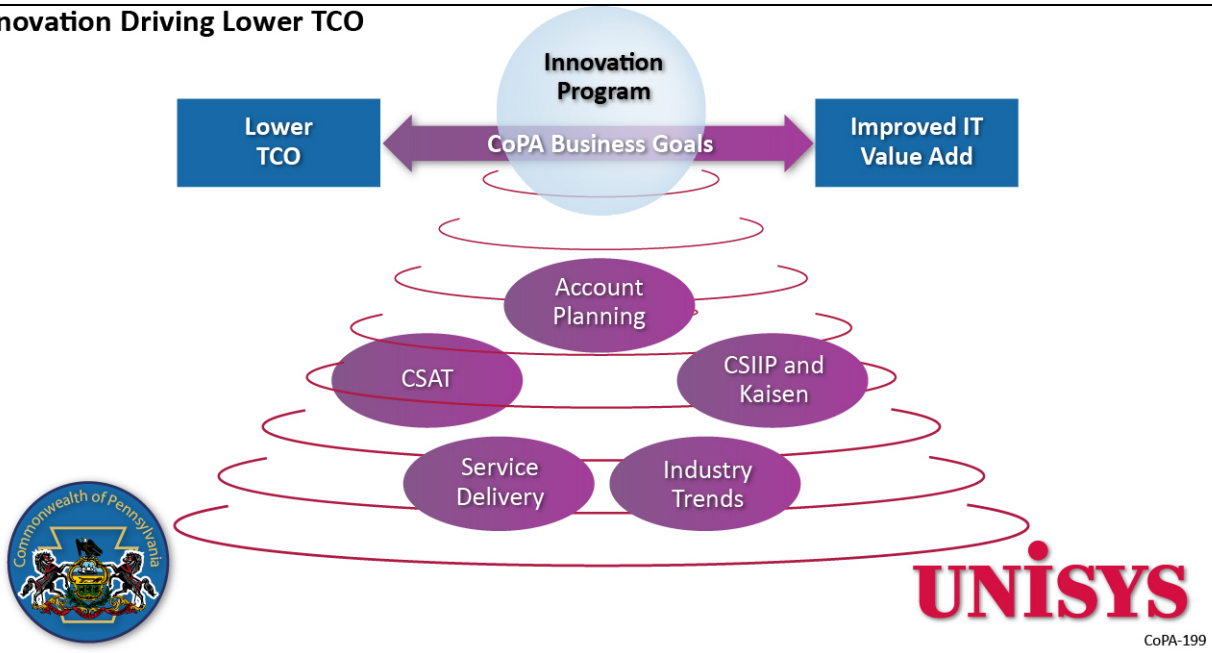


Figure 3.2.1.1.6-6 Innovation Driving Lower TCO

Our innovation program (see **Figure 3.2.1.1.6-6**) is driven by several concepts and programs. We are always gathering new industry trends and best practices for service delivery. We evaluate the trends and then gather metrics on our operations looking for places we can apply the industry best practices to drive down our TCO. Innovation is and continuous improvement is a central focus of our system architects as they support day to day operations.

5 CI Customer Satisfaction

5.A Survey of Service Desk satisfaction is a key component of providing best in class customer service. Receive completed surveys of Service Desk satisfaction from the Commonwealth and tabulating results from such surveys

Customer Satisfaction Surveys

Providing best in class ITIL V3 based IT service management and driving excellent client satisfaction is extremely important to Unisys and a key focus in our IT Solution. The SEO will manage a multi-pronged approach to client satisfaction. Data collection will be gathered across multiple levels to gain a clear understanding of the Commonwealth's satisfaction with the IT services being provided.

5.B Offeror must describe its approach to perform surveys of Service Desk satisfaction for a subset of the problems, questions, or requests that are resolved by, or coordinated by, the Service Desk.

The Service Desk will randomly survey Commonwealth clients who call into the Service Desk with a request or change which needs to be completed or an incident which needs to be resolved. Customer satisfaction surveys drive the Unisys client satisfaction program. Unisys conducts these surveys to confirm user satisfaction levels, identify opportunities to improve

agents and processes, and measure the qualitative aspects of providing Service Desk Services.

Unisys can expand and modify our customer satisfaction survey to include questions about the data center support dispatches, or we can conduct separate surveys for the separate Service Desk and data center functions. Customer satisfaction surveys complete the feedback loop between the user experience and the services received.

Unisys collects clearly defined performance criteria to permit analysis deemed important. For surveys of our Service Desk support, for example, we collect at least the agent's name, ticket number, narrative free-form text, and assessment ratings of the agent such as: courtesy and professionalism; technical knowledge; problem-solving skills; communication on ticket progress and resolution; and overall satisfaction.

Typically, we ask callers to rate performance for call responsiveness, problem resolution time, problem resolution quality, service orientation, and overall satisfaction.

Unisys sends a request to complete a customer satisfaction survey via e-mail to users who recently reported an incident via a phone call to our Service Desk. The e-mail contains a hyperlink which takes a user to a Web site to enter his or her responses on a HTML form. Responses are delivered back to our Service Desk by e-mail and collected in a database.

Unisys will use the information collected in our customer satisfaction survey as a basis for continuous improvement of service delivery. To calculate customer satisfaction, we take the sum of all scores for all surveys performed in a month and divide it by the total number of surveys performed in that month.

To conduct customer satisfaction surveys, Unisys uses an automated survey process and a set of questions for the end user to rate our service on a scale of 1 to 5:

5—Very Satisfied

4—Satisfied

3—Neither Satisfied nor Dissatisfied

2—Dissatisfied

1—Very Dissatisfied.

For questions the end user rates with a 1 or a 2, Unisys asks for supporting detail; we record this detail in the survey record and escalate customer satisfaction issues which require follow-up electronically to the Unisys Service Manager or the appropriate management representative. A survey follow-up process can consist of any one or all of the following:

- Review by a manager; review by a manager and an analyst or review by a service group
- Calling the end user to verify the rating, obtain additional information as required, and if possible, resolve the issue with the end user
- If applicable, retrieving the original incident call and listening to the recording for detailed information
- Creating and implementing a corrective action plan.

Unisys documents all survey follow-up activity and establishes corrective action plans, as

required. We end users to survey from the following criteria:

- End users with more than one service request in a 30-day period are surveyed for one request only.
- Service requests more than 7 days old are not surveyed.
- End users requesting not to be surveyed are not surveyed.
- Callers with invalid contact information are not surveyed.

5.C Offeror must describe its approach to creating and advertising a web site for day-to-day feedback from datacenter customers which is accessible through the Offeror's KMP.

Unisys will provide an Internet accessible Knowledge Management Portal (KMP) housed in the Unisys Service Portal tool. A Unisys Knowledge Manager will be responsible for working closely with the designated Commonwealth resources, as well as Data center Service Desk team, to keep the KMP current and relevant.

Training provided to data center customers (commonwealth employees) will always include a brief cameo discussion of the KMP. An option within the Knowledge Management Portal will be developed to allow for direct feedback from Commonwealth agencies and departments.

5.D Offeror must describe its approach to performing a customer satisfaction survey on a quarterly basis.

A formal client satisfaction survey will be conducted quarterly to clearly understand the client satisfaction of each agency and all of the ITIL service management operations areas. Unisys is currently providing these client satisfaction survey summary results to the Commonwealth. An example of these CSAT survey summaries by agency and operational area are shown in **Figure 3.2.1.1.6-7** below. Client facing leadership meetings between the Commonwealth CSAT Director and the Service Excellence Officer will be conducted quarterly to review this summary and the corresponding results from the multi-pronged input gathered through this robust CSAT process. Specific CSAT action plans will be documented and implemented to drive rapid service improvement if a remediation plan is required. This detailed CSAT process, analysis, and proactive communication will drive improved quality, greater transparency, while significantly improving the client experience.

Figure 3.2.1.1.6-7 DPH Agency Satisfaction Summary

6 CI Improve / reduce cost

6.A Offeror must identify its methods for addressing continuous service improvement targeted at minimizing or reducing costs of Services and operations.

Improve/reduce costs

Unisys is committed to providing the Commonwealth of Pennsylvania with best in class IT services, managed and driven through a dedicated Service Excellence Office. The SEO will drive Continuous Service Improvement throughout the ITIL V3 lifecycle. Standardization of ITIL V3 Frameworks, along with leveraging ISO certified processes, and Six Sigma Lean Tools will drive continuous service improvements. Governance, transparency and innovation workshops will verify the Commonwealth agencies plan and develop their future IT strategies and IT solutions. Risk management, independent quality audits, and business continuity planning will minimize risk throughout the ITIL V3 lifecycle phases.

Our method to identify and implement cost savings involves several activities. First we identify the strategy for improvement, define what will be measured, gather the data via carefully constructed surveys, audits, reviews, and process the collected data. We then analyze the gathered data to define cost saving action, test the cost saving action, and refine the cost saving

action as needed to confirm it will be effective. Finally, we implement the cost saving action to bring about the improvement. Once the cost savings action is in place, we define and collect metrics to monitor effectiveness of the cost savings action. We continue to adjust the cost savings activity to achieve the cost savings goal.

Our multipronged client satisfaction processes will verify Unisys clearly understands the voice of the customer, and will drive quality continuous improvement actions based collaborative feedback. All of this collectively represents Unisys Integrated Quality Plan for the Commonwealth of Pennsylvania shown in **Figure 3.2.1.1.6-8** below. This Quality Plan will provide the Commonwealth with the highest customer satisfaction experience, best in class quality IT services and ITIL processes, and a significant lower total cost of ownership.

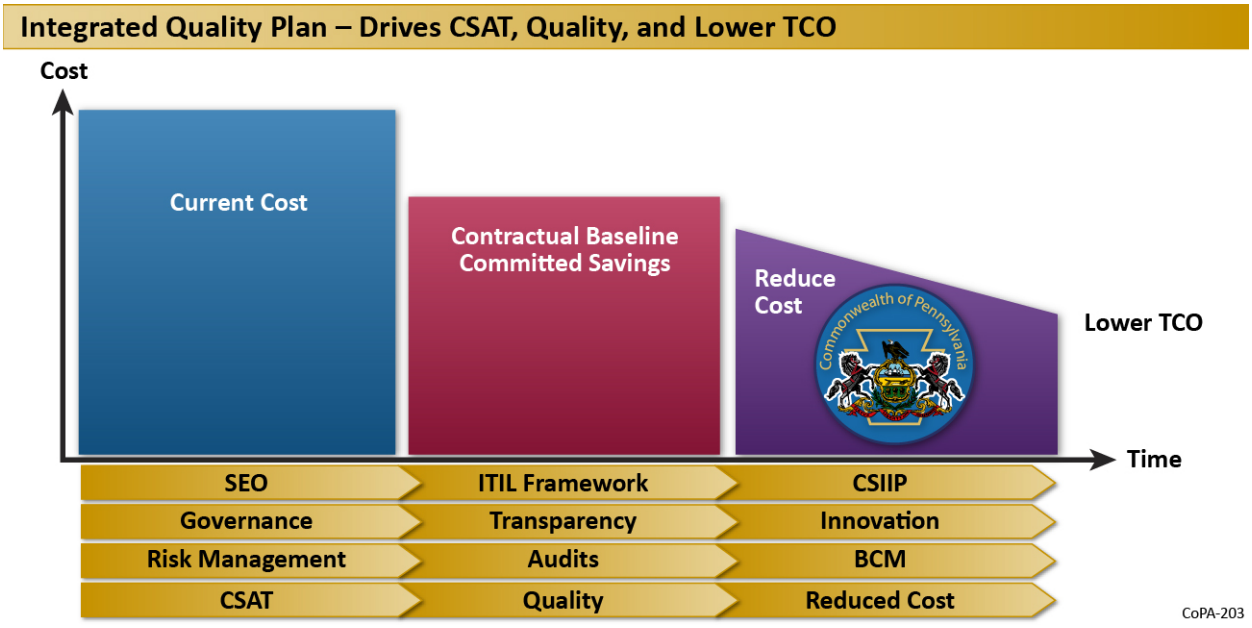


Figure 3.2.1.1.6-8 Unisys Integrated Quality Plan

3.2.1.2 Availability/SLA Management

The purpose of the System Availability and SLA function is to ensure that each service is delivered within, or exceeds, the agreed availability service level, and prescribed credits are received by the Commonwealth when the service level has not been achieved. Availability Management provides a point of focus and management for all availability related issues, ensuring that availability targets are established, measured, and achieved. The basic requirement is to balance the value and quality of Services with the costs of the Services. Availability and SLA management will be responsible for establishing and reviewing the SLA's to meet the Commonwealth's requirements. Offeror should review referenced exhibits for a list of SLAs and associated descriptions, tools and methodologies.

Availability/SLA Management ensures that datacenter service availability standards, as prescribed in appropriate datacenter SLAs, are achieved.

Reference Documentation

Schedule J.1 - Datacenter Service Level Management

Schedule J.2 - Datacenter Service Level Matrix

Schedule J.3 - Datacenter SLA Definitions

	Requirements	Describe Compliance
1.	Establish a formal Availability and SLA Management service. This service will include representatives from the Offeror and the Commonwealth for reviewing and approving the availability and SLA metrics. Offeror must publish the formal Availability and SLA Management plan based on a Services Catalog. Identify key Services and the associated level of availability or capacity as appropriate. Identify the Services that will be measured by an SLA. Define the basis the SLA service levels will be monitored and obtained. Obtain approval from the Commonwealth.	Offeror must describe its methodology and approach to Availability Management and Service Level Management.

2.	Identify Service Level Measurement Tools	Offeror must provide a list of those Service Level measurement and monitoring tools that it will use to measure and report Offeror's performance of the Services at a level of detail sufficient, as determined by the Commonwealth, to verify Offeror's compliance with those Service Levels described in **Schedule J.3 Datacenter SLA Definitions**. Offeror must review and update the required sections within Schedule J.3 Datacenter SLA Definitions. Offeror must complete the following sections in each of the Critical Service Levels and Key Measurements: • Collection Process – identify how the measurement data will be collected • Reporting Tools – identify any tools, automated or manual, that will be used • Raw Data Storage (Archives) – identify where data will be stored and accessible by the Commonwealth for further analysis. • Reporting Format/s – identify the proposed reporting format
3.	Integrate Availability Management with other service management processes, such as SLA, Capacity Management, Problem Management and Service Desk.	Offeror must describe how its proposed Availability Management process is integrated with other service management processes such as SLA, Capacity Management, Problem Management and Service Desk.

4.	Establish automated non-compliance indicators. Automatically e-mail the designated Commonwealth contact when SLA service parameters are not met. Create email notification groups by major service. Utilize this, or a similar process for outage notification.	Offeror must describe its process for managing Services performance.
5.	Investigate all instances of non-compliance. Notify the Commonwealth of an outage as defined in the CCPM. Complete a root cause analysis (RCA) for all major outages, and provide a detailed report to the Commonwealth and impacted user. Completion of the Incident report must occur within 2 days of the incident and the RCA within 10 days of the incident.	Offeror must describe its process for root cause analysis and for meeting the required SLAs. Offeror must include definitions of outage types and how it will make reports available to the Commonwealth.
6.	Identify integrated tools, methods, and activities to be used for reporting service and component availability. Ensure proactive measures to improve availability of Services are implemented whenever it is cost justified.	Offer must identify tools, methods, and activities it will use for reporting service and component availability. Offeror must describe its offerings in this area.
7.	Integrate Agency Availability Management processes with SLA Management. On a monthly basis, consolidate all system SLA availability reports into a management operations report, summarizing availability, outages, and SLA compliance by platforms.	Offeror must describe its offering in this area.

8.	Develop and maintain a Portal/Website for agencies to view operational status, planned maintenance, and component level outages.	Offeror must describe its Portal/Website to view operational status, planned maintenance and component level outages.

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

Introduction

Unisys will establish System Availability and Service Level Management (SLM) processes to help confirm that each service is delivered within, or exceeds, the agreed availability service level, and prescribed credits are received by the Commonwealth when the service level has not been achieved.

Availability Management provides a point of focus and management for all availability related issues, ensuring that SLA availability targets are established, measured, and achieved. The objective of this capability is to balance the value and quality of Services with the costs of the Services.

The Unisys Team will map critical Configuration Items (CIs) and relationships for infrastructure components to the Commonwealth/Agency Application CI during transition, using the mapping and discovery tools used to populate the Unisys CMDB. The Unisys Team will also utilize the current information from the Commonwealth to assist in this effort. The end result will be an approved mapping of an application to infrastructure with relationships that will be used to calculate application supporting infrastructure SLA's and assist in determining service impacts.

1 SLA, Availability Management and Service Level Management

1.A Offeror must publish the formal Availability and SLA Management plan based on a Services Catalog.

Unisys will publish a formal plan for supporting Availability and SLAs based on the agreed upon Services Catalog as represented in Schedule I of the RFP response. This is the outcome of the first few steps in the Availability Process described in 1.F below.

Establish a formal Availability and SLA Management service. This service will include representatives from the Offeror and the Commonwealth for reviewing and approving the availability and SLA metrics.

The Unisys Team will establish the governance for the Availability and SLA Management Service together with the Commonwealth during transition. The combined governance team will be comprised of PMO Representatives (Account Managers, Service Delivery Managers, Service Level Managers (Analysts), Financial Managers from both the Unisys Team and the

Commonwealth.

The Team will agree on the process for reviewing SLA results on a monthly basis to review:

- SLA results
- Acceptance of the results
- Exceptions to SLAs
- Required action items

The Team will also review and track SLA metrics, financial penalties, and earn backs.

1.B Identify key Services and the associated level of availability or capacity as appropriate.

Unisys will identify key services identified in the Enterprise Services Catalog through the relationships identified in the Unisys CMDB. Underpinning services are mapped to application services identified in the Enterprise Services Catalog with associated SLA's. In order to meet availability SLA's of the Enterprise Services Catalog Services, these underpinning services and SLA's are used to establish precedence and relationships for availability calculations.

Capacity information is stored in the Capacity Data Base described in the Unisys Capacity Management Solution described in Section F3.2.1.7 and is available as necessary to support any Availability Management calculations or reporting objectives.

1.C Identify the Services that will be measured by an SLA.

Services and associated SLA's are in the agreed to Enterprise Services Catalog and stored in the Unisys CMDB and Service Level Management (SLM) application. The Service Level Management application is used to calculate SLA's utilize the SLA information stored in the Unisys CMDB to calculate SLA compliance.

1.D Define the basis the SLA service levels will be monitored and obtained

The basis for obtaining the SLA definitions comes from the SLA definitions in Schedule J.3 of the RFP. These definitions will be used to configure the tools to monitor SLA compliance as shown in **Figure 3.2.1.2-1** below. Each SLA will be reviewed with the Commonwealth to determine the methods for gathering data used to calculate each agreed to SLA. The Commonwealth will approve these SLA monitoring methods during transition or for any required changes before they are implemented into production.

1.E Obtain approval from the Commonwealth

The Commonwealth will approve the methods for gathering data and measuring SLA results.

1.F Offeror must describe its methodology and approach to Availability Management and Service Level Management.

The following is the Unisys methodology and approach to Availability Management and Service Level Management for the Commonwealth agencies. These processes will be reviewed with the Commonwealth during transition and adjusted to meet Commonwealth requirements.

Availability Management

The Unisys Availability Management Process will be implemented during transition for the Commonwealth. The process and methodology outlined in **Figure 3.2.1.2-1** below will be reviewed and approved with the Commonwealth.

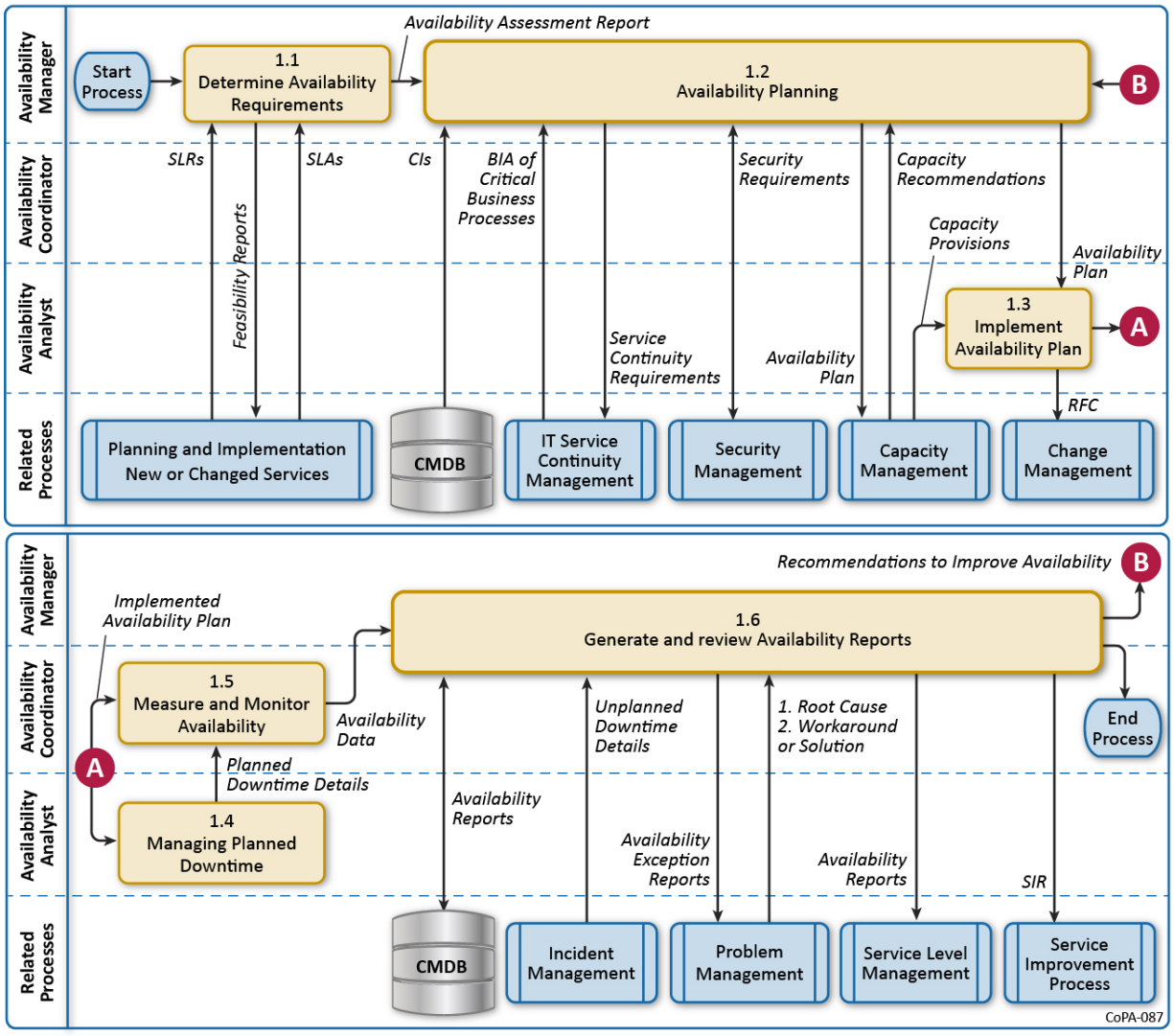


Figure 3.2.1.2-1 Availability Management Process

The following outline summarizes the Availability Process shown above. The details of this process will be determined during transition, reviewed with the Commonwealth for acceptance,

and documented in the CCPM.

1.1 Determine Availability Requirements

- Review SLA's with Commonwealth service owners and stakeholders
- Agree on revised SLA's where applicable using governance process
- Implement ongoing process to determine availability requirements
- Develop preliminary availability design for Commonwealth Agency services
- Assess service outages
- Develop countermeasures to prevent service outages
- Assess Internal/External suppliers for service components
- Prepare availability assessment report

1.2 Availability Planning

- Design solution with cost constraints and assumptions
- Review with Commonwealth agencies and modify design
- Test design and perform risk analysis
- Design solution meeting availability requirements
- Develop maintenance plan with underpinning agreements to support plan
- Review with Commonwealth agencies and obtain approval

1.3 Implement Availability Plan

- Implement and monitor availability plan
- Modify implementation as needed to meet plan
- Obtain Commonwealth agency signoff

1.4 Manage Planned Downtime

- Schedule maintenance activities
- Communicate the maintenance schedule
- Implement process to back out maintenance if necessary

1.5 Measure and Monitor Availability

- Monitor services and components
- Register incidents
- Review service outages and impacts
- Measure impact of outages
- Determine any changes required in availability design
- Process change requests if required

1.6 Generate and Review Availability Reports

- Consolidate IT component and service outage information

- Prepare availability reports
- Review and analyze reports
- Distribute availability reports
- Recommend availability improvements
- Update availability plan as required

Service Level Management

The Unisys Service Level Management (SLM) Process will be implemented during transition for the Commonwealth. The process and methodology outlined in **Figure 3.2.1.2-2** below will be reviewed and approved with the Commonwealth. This process will be reviewed with the Commonwealth during transition and adjusted to meet Commonwealth requirements.

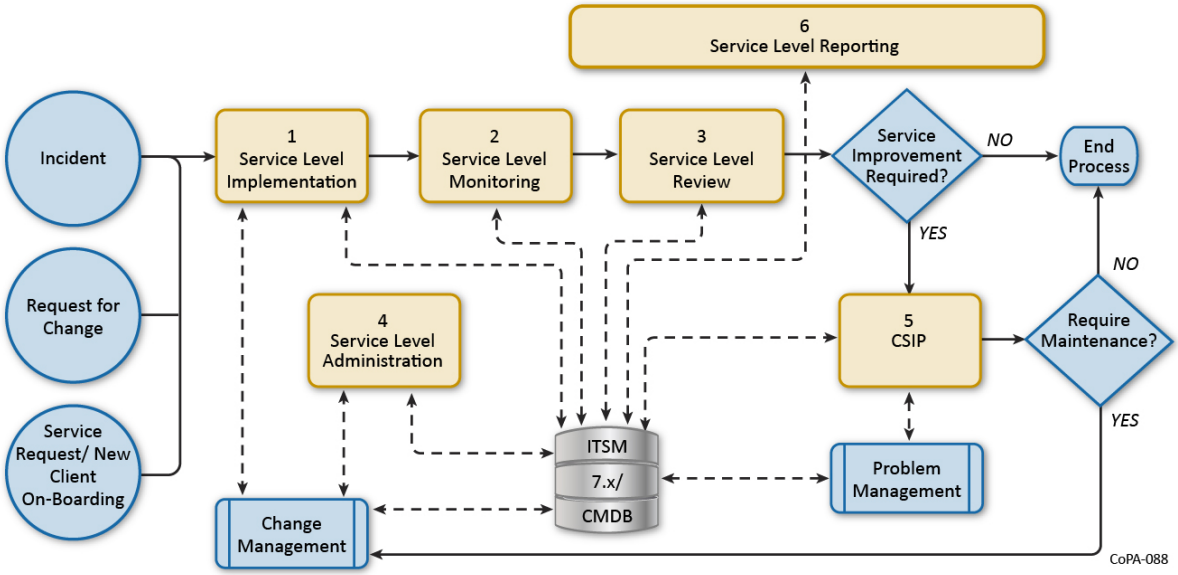


Figure 3.2.1.2-2 Service Level Management Process

The following outline summarizes the Service Level Management Process shown above. The details of this process will be determined during transition, reviewed with the Commonwealth for acceptance, and documented in the CCPM.

1. **Service Level Implementation.**

   Design SLA Framework. Use the Enterprise Services Catalog as an aid and design the most appropriate SLA structure to confirm that all services and customers are covered in a manner best suited to the organization's needs

   Determine, Document, and Agree to Requirements and Produce Service Level Requirements (SLRs). Once the Enterprise Services Catalog has been produced and the SLA framework has been agreed to, this activity drafts the SLRs.

   Review, Negotiate and Sign OLAs. Determines and negotiates the OLA requirements necessary for service delivery, and develops OLAs and obtains signatures for OLAs that

support the SLA.

Review, Negotiate & Sign Ucs. Reviews, negotiates, develops, and has signed the UCs that support the SLA and OLAs.

Create Service Level Agreement and Negotiate Terms. Drafts and negotiates the SLA that is needed to meet specified SLRs and objectives.

Activate the SLA. Oversees the signing and activating of the SLA.

2. **Monitor Service Performance Against SLA and Produce Service Reports.** Monitors performance in an ongoing manner and reports on specified service level measurement.
3. **Perform Service Level Review.** Performs periodic reviews of service level performance.
4. **Service Level Administration.** Conduct periodic reviews of SLAs with stakeholders to review SLA's and determine if any changes are required to support existing or modified SLA's
5. **Create a Service Improvement Plan (CSIP).** Creates a CSIP that is a formal plan to implement improvements to a process or IT service. A CSIP is managed as part of the Continual Service Improvement (CSI) element of ITSM.
6. **Service Level Reporting.** Produce SLA reports and make accessible to stakeholders with capabilities to drill down into details.

2 SLA Service level Measurement Tools

2.A Offeror must provide a list of those Service Level measurement and monitoring tools that it will use to measure and report Offeror's performance of the Services at a level of detail sufficient, as determined by the Commonwealth, to verify Offeror's compliance with those Service Levels described in Schedule J.3 Datacenter SLA Definitions.

Identify Service Level Measurement Tools

Figure 3.2.1.2-3 below shows the architecture and tools to support the Service Level Management measurement, monitoring and reporting.

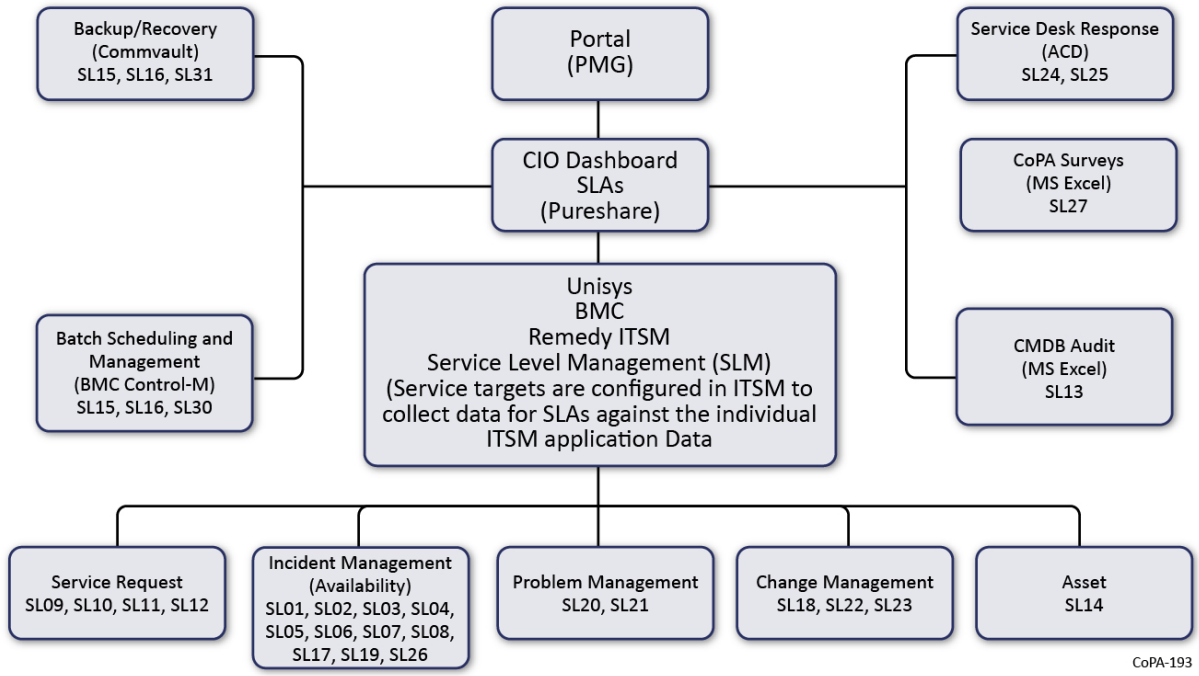


Figure 3.2.1.2-3 SLA Supporting Tools Architecture

The diagram shows how the various tools collect the data for calculating the SLA's for this contract and how the SLA's are reported in the Unisys Real-time Dashboard. Commonwealth stakeholders will be able to view the SLA compliance and drill down into supporting details. Monthly SLA reports are made available in the Unisys reporting Portal for the Commonwealth to access and review.

The Unisys and Commonwealth PMO will review and agree to the supporting tools, measures, monitors, and reports for SLA's calculations during transition using Schedule J.3 Datacenter SLA Definitions to verify compliance.

2.B Offeror must review and update the required sections within Schedule J.3 Datacenter SLA Definitions. Offeror must complete the following sections in each of the Critical Service Levels and Key Measurements:

Please refer to Schedule J.3, which is an attachment to Section 3 for a description of each SLA outlining the following:

- Collection Process – identify how the measurement data will be collected
- Reporting Tools – identify any tools, automated or manual, that will be used
- Raw Data Storage (Archives) – identify where data will be stored and accessible by the Commonwealth for further analysis.
- Reporting Format(s)

2.C Collection Process – identify how the measurement data will be collected

Please refer to the SLA Measurement Tools in **Figure 3.2.1.2-3** above which are used to collect measurement data for each SLA. Also, please refer to Schedule J.3. Section 3 for a detailed discussion for each SLA.

2.D Reporting Tools – identify any tools, automated or manual, that will be used

Please refer to the SLA Measurement Tools above **Figure 3.2.1.2-3** which are used to collect measurement data for each SLA. Also, please refer to Schedule J.3. Section 3.4 for a detailed discussion for each SLA.

2.E Raw Data Storage (Archives) – identify where data will be stored and accessible by the Commonwealth for further analysis.

Thirteen months (13) of online data supporting the SLA's will be retained in the Reporting tools shown above with a rotation to archive tape backup. This will allow the Commonwealth to review supporting details online up to 13 months. A data archive will exist on tape.

2.F Reporting Format/s – identify the proposed reporting format

Reporting formats for the online display of SLA's in Real-time Dashboard and monthly reporting for SLA performance will be reviewed and approved during the first six months of the contract in establishing the ITSM platform for operational readiness. The samples of report formats can be found in Schedule J.3, Section 3 for each SLA.

3 Integration, Availability integrated with SLA, Capacity

3.A Offeror must describe how its proposed Availability Management process is integrated with other service management processes such as SLA, Capacity Management, Problem Management and Service Desk.

Integrate Availability Management with other service management processes, such as SLA, Capacity Management, Problem Management and Service Desk

Unisys will integrate Availability Management with other service management processes, such as Incident , Problem and Change Management. These are the main processes for Availability SLA integration. Other processes contribute as necessary to support these including Configuration and Capacity Management.

For example, incidents that impact availability, are reviewed by the Unisys Availability Manager and Problem Manager in order to determine how to prevent availability issues in the future. The Availability and Problem Manager will make recommendations for change, and if accepted by the Commonwealth, will be processed through the Change Management Process. If the Change requires additional Capacity this will be coordinated with the Capacity Management Process.

The Service Desk is involved if the Availability Issue is reported by the Commonwealth agencies. The Service Desk will record an incident ticket that would follow the process

described above.

4. Service Performance Management

4.A Automatically e-mail the designated Commonwealth contact when SLA service parameters are not met. Create email notification groups by major service. Utilize this, or a similar process for outage notification.

Establish automated non-compliance indicators.

The Unisys Incident Management application as part of the ITSM Solution will automatically send email messages for SLA's exceeding thresholds to the appropriate stakeholders. These thresholds will be determined by the SLM Application(s) examining the CMDB structure to determine SLA precedence and relationships to notify stakeholders appropriately. Unisys will establish for all major services, email notification groups by major service to support notification of to all Unisys, Subcontractor and Commonwealth stakeholders.

Outage notifications are handled through the incident management process which will notify SLA stakeholders through email, and visually SLA violations and status will be displayed on the Real-time Dashboard which is available to all SLA stakeholders.

4.B Offeror must describe its process for managing Services performance.

The Unisys Service Level Management Analyst and the Unisys Account Managers are responsible for managing Services performance. Dashboards will be made available to assist with monitoring. This team will be notified of services performance incidents or SLA violations as described above in 4.A.

The Unisys Commonwealth Account Managers and service level analysts will review all Service Level breaches or approaching violations and lead corrective actions stemming out of Incident/Problem Investigations.

Unisys will investigate all instances of service performance SLA non-compliance or approaching non-compliance. If the Unisys Account Managers, Problem Manager or Service Level Management Analyst identifies potential issues from the dashboard reviews or automated incident notifications they will review and analyze the situation with the support teams. If the service levels are achievable a Problem Management case may be opened to investigate an issue. The Root Cause Analysis (RCA) is a collaborative effort of multiple teams to identify the reasons for the SLA breach. The possible solutions are identified to prevent the recurrences of similar failures in the future. The users and stakeholders are informed about the plans to prevent an SLA breach in the future.

The Service Level Management Analyst provides a consistent interface to the Unisys/Commonwealth PMO Teams for all service-level related issues. He/she provides the agreed service targets and the required management information to verify that those targets have been met. Where targets are breached, the SLM Analyst provides feedback on the cause of the breach and details of the actions taken to prevent the breach from recurring. The SLM Analyst and process provides a reliable communication channel and a trusted relationship with

the appropriate stakeholders for Unisys and the Commonwealth Agencies.

5 SLA Reporting, Root Cause analysis, outage reporting

5.A Notify the Commonwealth of an outage as defined in the CCPM. Complete a root cause analysis (RCA) for all major outages, and provide a detailed report to the Commonwealth and impacted user

Investigate all instances of non-compliance.

Unisys will investigate all instances of non-compliance using the Problem Management Root Cause Analysis Process and produce an RCA Analysis as described in **Figure 3.2.1.2-4** below.

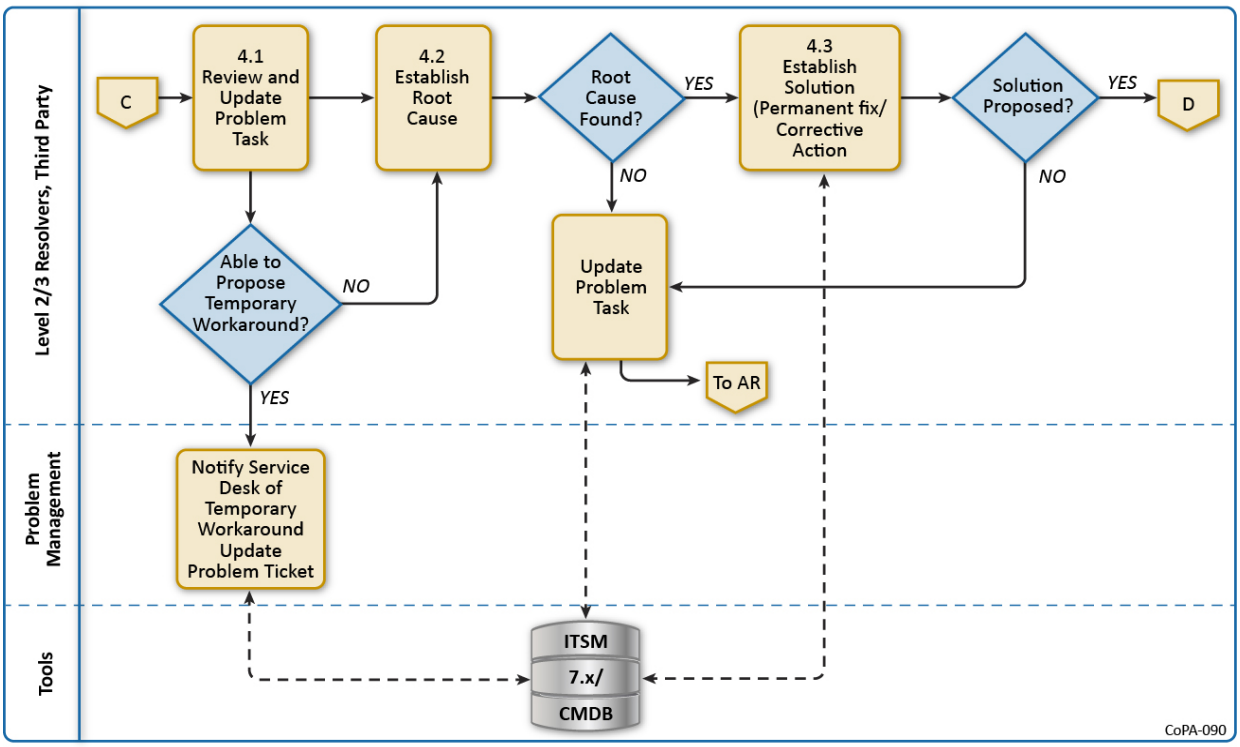


Figure 3.2.1.2-4 Problem Management – Root Cause Analysis Process

Root Cause Analysis (RCA)

4.1 Review and Update Problem Task - RCA involves investigation of the problem by the relevant Level 2 or 3 Technical Teams and/or Third-Party Vendor. The primary aim of this procedure is to determine a work-around and to establish the root cause.

The Root cause analysis procedure details the activities carried out to establish a work around/root cause and a permanent solution (corrective action).

Completion of the associated SLA incident report must occur within 2 days of the incident and

the Root Cause Analysis must be completed within 10 days of the incident.

The L 2/3 Resolver/Resolver Groups assigned with the Problem Tasks need to review and update the problem task with relevant information regarding the task assigned. If they are able to propose a temporary workaround for the problem, information needs to be sent to the Problem Management team and the Service Desk.

4.2 Establish Root Cause - Once the task has been reviewed and updated the next step would be to establish the root cause of the problem. Several different methods like the 5 why method or fishbone analysis could be used to get to root cause of the Problem. Once the root cause has been established, information needs to be updated in the problem task assigned. In the event root cause cannot be established the procedure would move directly to Analysis review.

4.3 Establish Solution - The next step in this procedure is establishing the permanent solution or the corrective action to fix the root cause of the problem. Once a solution is proposed it needs to be approved before it can be implemented. A proposed solution and change ticket is the outcome from this procedure.

The Change Process is used to review the recommended solution and approve or reject the solution. The approval or rejection of the Solution provided is done in consultation with the Unisys Account Manager and Support Team technical leads. This procedure also involves the creation and managing of Known Errors.

5.B Completion of the Incident report must occur within 2 days of the incident and the RCA within 10 days of the incident.

Per the root cause process described above, the incident report will be completed within 2 days and an RCA will be completed within 10 days of the incident.

5.C Offeror must describe its process for root cause analysis and for meeting the required SLAs.

See the complete root cause analysis process described above in 5.A above for meeting the required SLAs and taking any corrective actions through the Change Management Process.

5.D Offeror must include definitions of outage types and how it will make reports available to the Commonwealth.

Unisys will perform the following procedure to provide reports on outage types:

- Collect the service outage data.
- Assemble the team who is familiar with outages.
- Group related service outages together such as grouping by vendor, product, application, customer and project. This will leverage the CMDB relationships and SLA structure to assist in grouping, determining SLA priorities and precedence.
- Categorize each outage as “High, Medium and Low.”

- Focus on outages which are categorized as "High."
- Monitor "Medium" for future outages.
- Review the Root Cause of unavailability for the "High" outages.
- Rank related outages and their causes.
- Examine the reasons for the duration of the unavailability for each grouping of similar outages (for example, the outages might have occurred because of faulty hardware or software, but the duration of unavailability might have been extended by lack of tools, training, process, and resources).
- Review existing Operations procedures that were invoked or used during this outage and the Technical Support Staff who were involved in the outage or restoration.
- Determine if anything might have lessened the duration of the outages and list them (for example, the lack of tool, process and resources).
- Quantify the avoidable outage time (for example, if there was one (1) hour of down time resulting from trying to locate the proper tool, then the avoidable outage time is one (1) hour x the number of outages affected).
- Raise a Request for Change (RFC) to address the "High" outages with a suggested solution to prevent the down time.
- Summarize the number of outages analyzed, listing the avoidable outage time and suggestions for minimizing or avoiding the outage. Present the report to the Commonwealth agencies on a monthly basis.

6 SLA Availability Reporting tools

6.A Identify integrated tools, methods, and activities to be used for reporting service and component availability. Ensure proactive measures to improve availability of Services are implemented whenever it is cost justified.

All tools to support SLA Availability Reporting are shown in Section 2.A above.

The process, procedures and activities to support availability reporting are shown in Sections 1 (Process), 2 (Process Integration), 4 (Service Performance Management) and 5 (Reporting, Root Cause Analysis) and outage notification, all above.

Proactive measures are handled in the Unisys SEO and ITSM Continual Service Improvement Services as part of the Unisys SEO described in Section F3.2.1.1.6.

Please refer to Site Operations Section F3.2.3.2 for a complete integrated view of services management end-to-end.

6.B Offer must identify tools, methods, and activities it will use for reporting service and component availability.

Please review the description above in 6 A. for all tools, methods, and activities used for reporting service and component availability.

6.C Offeror must describe its offerings in this area.

Please review the description above in 6 A. for all tools, methods, and activities used for reporting service and component availability.

7 Integration, Availability integrated with SLA Management

7.A Integrate Agency Availability Management processes with SLA Management. On a monthly basis, consolidate all system SLA availability reports into a management operations report, summarizing availability, outages, and SLA compliance by platforms.

During transition, the Unisys Availability, Service Level Managers and PMO stakeholders will review the Commonwealth Agency processes for Availability and SLA Management to determine how best to incorporate these within the overall framework for management and reporting purposes.

The Availability Management Processes that Unisys will provide to the Commonwealth and Agencies are described above in Section 1.A. The Processes will be support the Commonwealth Agencies, incorporating an Agency specific procedures when approved by Unisys and the Commonwealth agencies during transition.

Availability reporting, outages and SLA compliance are displayed in the Unisys Real-time Dashboard with drill down capability to supporting details. Monthly SLA and operations reports will be made available in the Service Portal. All Commonwealth and Unisys stakeholders who need this information will have access to the Service Portal.

7.B Offeror must describe its offering in this area.

See offering above in 7.A.

8 Portal, SLA Web Portal

8.A Develop and maintain a Portal/Website for agencies to view operational status, planned maintenance, and component level outages.

Unisys will develop and maintain a Portal for the Commonwealth agencies to view operational status, planned maintenance, and component level outages. The following section discusses the Service Portal in detail.

8.B Offeror must describe its Portal/Website to view operational status, planned maintenance and component level outages

Commonwealth, Unisys and subcontractors will use a Portal and Real-time Dashboard integrated together to view SLA status, operational status, planned maintenance and component level outages.

Unisys will provide the Commonwealth with Portal access to view SLA status (See **Figure 3.2.1.2-5** below) , operational status, planned maintenance and component level outages with the following information:

- Service Status - SLAs
- Contract obligation and health
- Maintenance windows
- Enterprise device management and health
- Project management and health
- Drill down capability on any of the above (ticket data, outage data, project data)
- Agency specific operational views
- Standard periodic reports
- Knowledge Management Portal (KMP)

The Commonwealth agencies and stakeholders will be able to use the Services Portal and Real-time Dashboard to easily view the SLA status, operational status, any planned maintenance schedules, and drill down to see program level details supporting these metrics.

The following is an example of how SLAs will be reported near real time in the Real-time Dashboard available through the Services Portal.

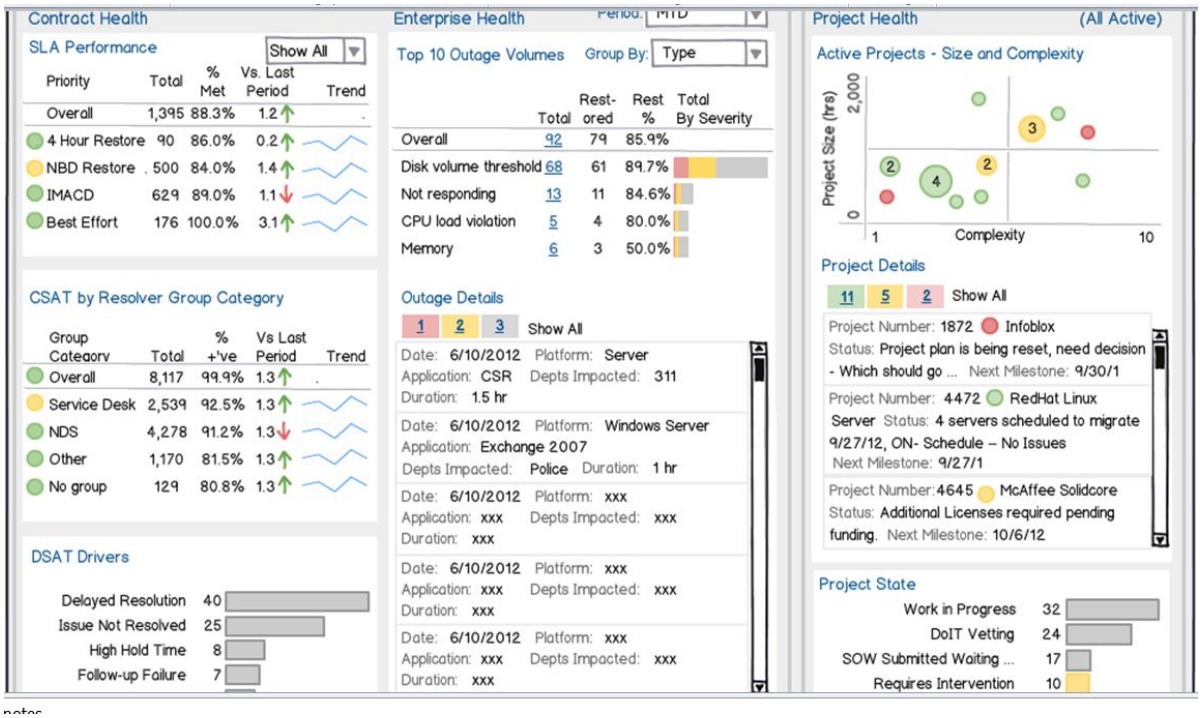


Figure 3.2.1.2-5 CIO Program Health Portal Dashboard

Unisys Team Experience

Unisys currently provides IT Service Management Services to more than 150 customers worldwide. Unisys is a leading provider of Managed Services utilizing an integrated suite of ITIL V3, ISO 20000 certified management processes and leading ITSM tools to provide outstanding service levels to our customers.

Unisys currently successfully manages more than 400 SLA's for the Commonwealth, achieving 99.7% SLA compliance in 2012.

Benefits to the Commonwealth

The Unisys value proposition for the Availability and Service Level Management Solution described above is summarized as follows:

- Reliable service level attainment and dependability to support the Commonwealth/Agency business and application consumers
- Flexibility to customize SLA's and meet them for the Commonwealth

3.2.1.3 Change & Release Management

Change & Release Management ensures that all changes within the datacenter environment are planned, executed, monitored, documented, and that the change produced the intended effect. The Offeror must establish the overall Change & Release Management function and manage the daily operations of the functions. This will ensure that all changes are processed in a uniform manner that required documentation, approvals, and notifications are completed before the change is implemented within each of the lower infrastructure environments and then moved into the production environment. Post implementation review and approval will require that all steps have been completed as documented, and within the time frame allotted. All change and release documentation must be maintained in a manner that will facilitate random compliance auditing. On a yearly basis, random selections of changes will be audited for compliance purposes.

Reference Documentation

Schedule H - Commonwealth Computing Process and Procedures Manual (CCPM)

Requirements		Describe Compliance
	Establish a formal Change & Release Management function. This function will include representatives from the Offeror and Commonwealth to support the review and approval of all changes. Offeror must publish the formal Change & Release Management plan. Identify key elements and roles; Request for Change Form & Process, Change Manager, Change Advisory Board, Emergency Change Advisory Board, Notification process, Change review process. The documentation and process will follow industry best practices. Train appropriate Commonwealth staff on the process as requested by the Commonwealth. The Offeror's Change Management & Release management process must consider and integrate with the Commonwealth's individual change management policies and procedures,	Offeror must described its proposed process and provide a sample overview of its process and procedures. Offeror must describe the system tool it will use to support the Change & Release Management processes. Offeror must describe how it will integrate its Change & Release Management tool with the Commonwealth's Enterprise ITSM solution. Offeror must describe its process and procedure for the Commonwealth to perform random audits.

	for example from January to May of each year, Department of Revenue (DOR) maintains a “no update policy” to DOR servers that have any production Tax-Related Applications running on them.	
1.	Institute a Change Advisory Board (CAB) The CAB members shall ensure that the requested changes are thoroughly checked and assessed from both a technical and business perspective.	Offeror must describe its proposed approach to creating a CAB and describe how members should be selected. Offeror must describe its approach to handling changes at an agency level. Offeror must provide a sample CAB organization and meeting schedule.
2.	Test infrastructure related changes & releases before implementation. This includes Offeror managed hardware and any Offeror managed software. Offeror must file a Pre-Change Test Plan, as part of the Change & Release request process, including results before final approval to proceed. Offeror must create and maintain test environments where testing will be conducted and evaluated prior to implementing any change into production environments.	Offeror must described its proposed process and provide a sample overview of process and procedures.
3.	Establish scheduled maintenance periods, and communicate the scheduled outages. Create a notification process for maintenance, emergency, and unplanned outages. Offeror must establish regular maintenance periods for each computing platform. Maintenance periods must be coordinated per agency due to different peak business requirements.	Offeror must describe its process for managing maintenance periods and system outages, with examples. The Offeror must provide an approach to managing multiple agency specific maintenance periods with different peak periods.

	Create mechanism to notify clients of expected and unexpected outages.	
4.	Notify affected Commonwealth agencies before and after any changes. Provide Change & Release Notifications prior to implementation via a central web site and e-mail.	Offeror must describe its proposed process and procedure related to notifications. Offeror must describe any other change notifications capabilities available to the Commonwealth.
5.	Validate all changes after implementation. Complete a post change review to validate the success or failure of the change or release, and post the information within the change record. Take follow up action as appropriate.	Offeror must describe its proposed process and procedure.
6.	Prepare back out procedures for all changes. As part of the Change & Release process, file a back out plan as appropriate to remove the change and restore Services to the prior level.	Offeror must describe its proposed process and procedure related to back out procedures.
7.	Track all (successes / failures) changes and produce Change & Release management statistics. Create and deliver a monthly Change & Release Management Report to the Commonwealth, detailing changes, implementation status, and outage time periods as compared to planned outage schedules.	Offeror must describe its proposed process and procedure.
Deliverables		
Deliverables are defined in **Schedule K – Key Program Deliverables**		
Offeror Response		
Introduction		

Unisys will implement a Change & Release Management Process to help confirm that all changes within the data center environment are analyzed, planned, tested, monitored, documented, and that the change produced has the intended effect for the Commonwealth.

All changes will be processed in a uniform manner with the required documentation, approvals, back out plans and notifications complete, before the change is tested and then released and deployed into the production environment.

Post implementation reviews will be conducted to help verify that all steps have been completed, documented , and released and deployed within the time frame allotted. All change and release documentation will be maintained in a manner that will facilitate random compliance auditing. On a yearly basis, random selections of changes will be audited for compliance purposes.

1 Change and Release Process, tools, integration, random audits

1.A Establish a formal Change & Release Management function. This function will include representatives from the Offeror and Commonwealth to support the review and approval of all changes

Unisys will Establish a formal Change & Relapse Management Process and supporting functions in line with ITIL V3 guidance.

The Change Management process shown in **Figure 3.2.1.3-1** below controls the life cycle of all changes. The goal is to respond to changing business requirements while maximizing value and reducing incidents, disruption, and rework. The objectives of this process are:

- To enable beneficial changes to be implemented with minimum disruption to IT service
- To confirm that changes are recorded and evaluated, authorized, prioritized, scheduled, tested, implemented, documented, and reviewed in a controlled manner.

The Change Management process verifies that any changes to service assets and CIs are properly planned, managed, and reviewed prior to their implementation and release.

The Change Management process and the Release and Deployment Management process closely govern the daily activities of the testing environment shared between Unisys and the Commonwealth's agency application testing environments for testing, evaluating, and deploying applications and services to the production data centers. This forms the basis for establishing an operational capability and serves as the foundation for other ITIL V3 processes that guide the day-to-day operation.

A normal change is a change that follows the normal Change Management process, requiring review and approval, etc. A standard change is a minor change with low risk that has been preapproved by the Change Manager because it follows a well-known and established procedure.

Unisys will establish formal Change and Release Management Processes in **Figure 3.2.1.3-1** below to help facilitate all changes within the data center environments are planned, executed, monitored, documented, and released and deployed to produce the intended outcomes. The

following Unisys Change and Release Management Processes will be reviewed and modified to meet the enterprise and agency specific Commonwealth requirements during transition.

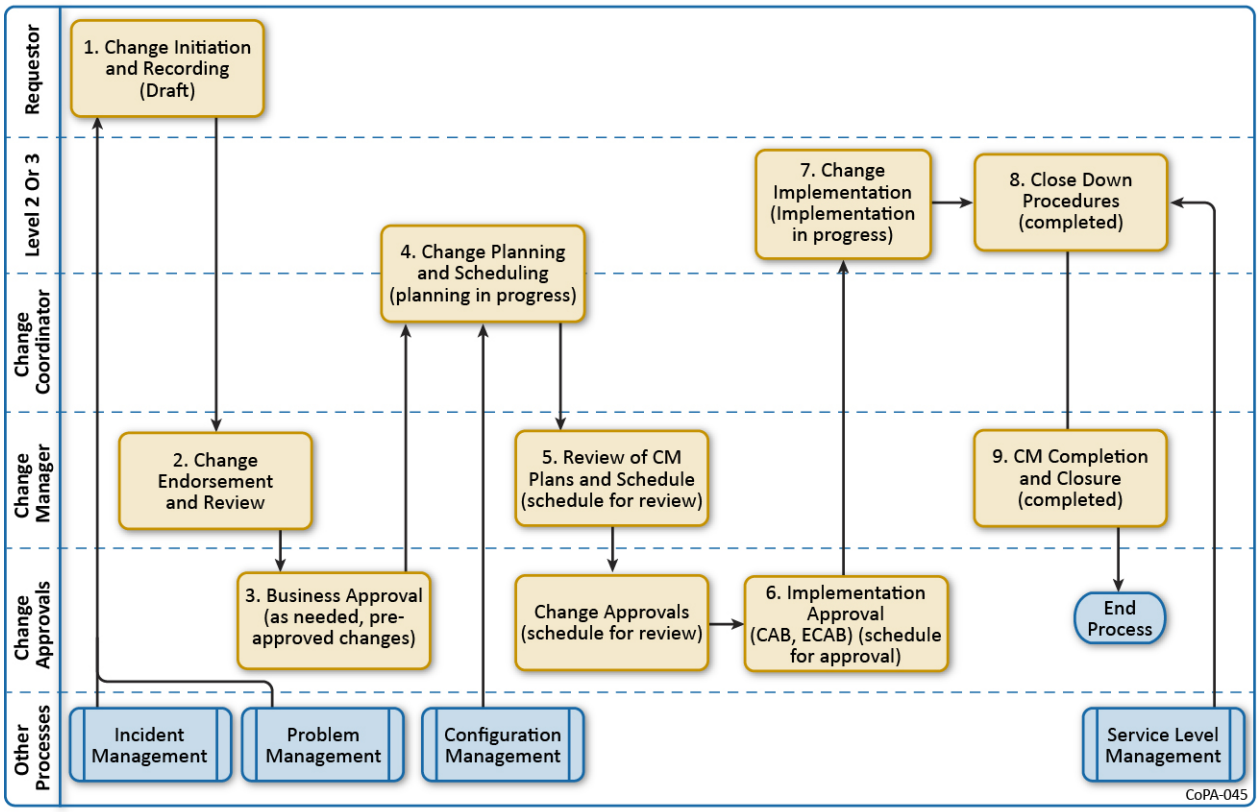


Figure 3.2.1.3-1 Change Management Process

1. Change Initiation and Recording - Receives Request for Change's (RFC's) from requestors. In some cases RFCs are logged on the requestor's behalf through the Service Desk.

2. Change Endorsement and Review - All RFCs are reviewed for completeness and accuracy, risk and potential impact on services.

3. Business Approval (pre-approved changes) – Receive business approval for pre-approved changes

4. Change Planning and Scheduling – Preliminary change planning for an RFC and Release Plan

5. Review of Change Management Plans and Schedule - Reviews the change to determine when it should be planned and scheduled for implementation. A forward schedule of changes is maintained for stakeholder review and approval.

   Change Approvals – Changes are approved at the proper level and with appropriate personnel depending on whether the change requests types are standard, emergency, expedited, latent or normal, and their potential impact and priority.

6. Implementation Approval – The Change CAB or Emergency Change Approval Board (ECAB) approval is obtained to implement changes to the production environment after reviewing test results.

7. Change Implementation – The change deployment team deploys the change during the approved maintenance window.

8. Close Down Procedures – Review the change request to determine its disposition after reviewing the change compliance with service levels.

9. Change Management Completion and Closure – Reviews the change implementation results including if it followed the release and deployment plan and was completed within the release window. The Change Manager reviews with the change stakeholders to determine satisfaction and success with the change implementation, lessons learned, and closure of the change.

Release Management Process

The Release and Deployment Management process, in the **Figure 3.2.1.3-2** below, delivers significant business value by delivering changes at optimized speed, risk and cost, and offering a consistent, appropriate and auditable implementation of usable and useful business services.

The Release and Deployment Management process covers the whole assembly and implementation of new and changed services for operational use, from release planning through Early Life Support (ELS).

As previously stated, the Release and Deployment Management process and the Change Management process closely govern the daily activities of Unisys and the Commonwealth's agencies testing, evaluating, and deploying applications and services to the production data centers.

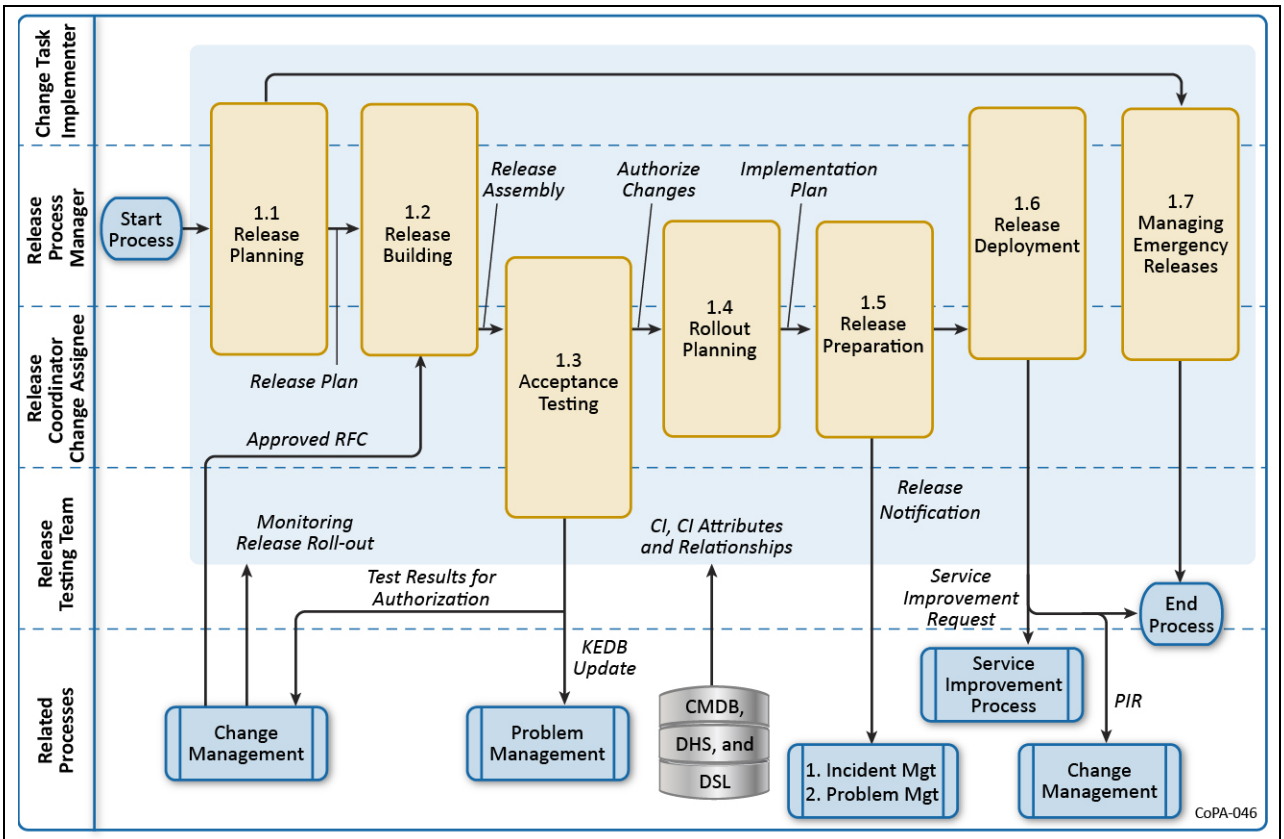


Figure 3.2.1.3-2 Release Management Process

1.1 Release Planning – The Release and Deployment Manager and the planning and support teams work on the service transition package to establish, review, and periodically update the release policy document and schedule for releases.

1.2 Release Building – After an RFC is validated and approved as part of the Change Management process, this activity begins the process of preparation for the release that includes one or several RFC's. This activity evaluates the service design baseline to confirm that the service release build and test begins with a stable, base-lined and approved design.

1.3 Release Acceptance Testing – Test Management personnel coordinate the plans and controls for testing execution. Testing aims to build confidence in the service capability prior to final acceptance during the pilot or Early Life Service Support. Testing is based on the test strategy and model for the service being changed. The test plans are followed for executing the tests and the results are summarized and presented to the CAB to gain approval for implementation planning and rollout.

1.4 Rollout Planning – The implementation plan for the Release is prepared and accepted.

1.5 Release Preparation – Prepares the organization and people for change, including the development of a detailed implementation plan that includes training, assigning individuals to specific process activities, etc.

1.6 Release Deployment – Transfer assets, transfer/transition businesses and organizations, deploy processes and materials, deploys Service Management capabilities, transfer services, deploy services, decommission services, and retire services.

Provide Early Life Support (ELS) – Provides a smooth transition for the new or changed service to Service Operations in a controlled manner and establishes the new service capability and resources are stable and operating according to specifications and SLA's.

Verify Deployment – After the deployment and ELS activities are completed, this activity verifies that users, Service Operations and other staff and stakeholders are capable of using or operating the service.

Review and Close Deployment – Reviews the deployment against the requirement. Deployment is completed with a handover of the support for the deployment group or target environment to Service Operations.

1.7 Managing Emergency Releases – Process to manage emergency releases with documentation following the emergency release and deployment activity.

The Change and Release Management Processes will minimize the impact of changes to mission critical services that Commonwealth agencies provide. The Unisys Change Management team will work with the Commonwealth Enterprise CAB and agency representatives to help verify that SLA's are met and risk managed appropriately based on priority, impact and urgency criteria. Changes that can be standardized and have lower risk will not be managed at the CAB level. Instead, they will continue to be managed and approved following a defined standard Change Management Process. This includes the use of standard template change procedures and maintenance windows for deploying standard changes. This will help to focus the CAB on managing those changes that have the most risk to disruption of critical services within and between agencies to help provide successful change and release deployment success.

1.B Offeror must publish the formal Change & Release Management plan. Identify key elements and roles; Request for Change Form & Process, Change Manager, Change Advisory Board, Emergency Change Advisory Board, Notification process, Change review process. The documentation and process will follow industry best practices.

Unisys will provide the Commonwealth with a Change and Release Management Plan during transition to the new ITSM Platform for Operational Readiness. The Table of Contents from a typical plan is outlined below:

1. Process, Procedures and work instructions (including RFC submittal form)
2. A RACI chart with key roles and responsibilities identified
3. CAB structure and governance
4. Release Management schedule and plan
5. Emergency Change Process and CAB
6. Change Notification Process
7. Change Post Implementation Review Process
8. An ongoing training plan for Change and Release Management roles
9. SLAs
10. Change and Release freeze periods for the Commonwealth /Agencies
11. Continuous Improvement Process and Plans

1.C Train appropriate Commonwealth staff on the process as requested by the Commonwealth.

Unisys will train the Commonwealth staff on the agreed upon Change and Release Management Processes agreed to during the transition period to the Operational Readiness ITSM Platform. This pertains to the other processes on this platform also and how they are connected.

1.D The Offeror's Change Management & Release management process must consider and integrate with the Commonwealth's individual change management policies and procedures, for example from January to May of each year, Department of Revenue (DOR) maintains a "no update policy" to DOR servers that have any production Tax-Related Applications running on them.

Unisys will consider and integrate the Commonwealth's Change Management Policies and procedures during transition to include change freeze periods for each agency.

1.E Offeror must described its proposed process and provide a sample overview of its process and procedures.

Please refer to 1.A above for a complete overview of the Change and Release Management Processes Unisys will review with the Commonwealth to agree to during transition.

1.F Offeror must describe the system tool it will use to support the Change & Release Management processes

Unisys will implement Change and Release Management processes on the Unisys ITSM platform. Please refer to Site Operations in Section 3.2.3.2 for a complete integrated overview of how Change and Release Management tools support the end to end service management capability. Please refer to 1.A above for the complete process descriptions of Change and Release Management.

1.G Offeror must describe how it will integrate its Change & Release Management tool with the Commonwealth's Enterprise ITSM solution.

The Commonwealth will utilize the Unisys Service Desk capability to process change requests. These change requests will be combined potentially with other approved change requests into release packages and processed through the release process and the individual changes will be deployed and closed out. All change requests will be synchronized with the Commonwealth ITSM System.

Unisys synchronizes all identified data between the Commonwealth and Unisys ITSM systems. This will provide the Commonwealth with enhanced capabilities and transparency and synchronized data between the two ITSM Systems (Unisys and the Commonwealth) via replication. During transition the replication requirements, triggers, outputs, timing of updates between the two systems will be defined, configured, and tested before being accepted by Unisys and the Commonwealth and deployed into the production environment.

1.H Offeror must describe its process and procedure for the Commonwealth to perform random audits.

Unisys supports random audits of the Change and Release Management process and procedures and effectiveness. This would include review of Change and Release Management tickets for closure as outlined below. The Commonwealth can select change and release tickets and participate in the closure reviews and post implementation reviews outlined below.

Change Management Completion and Closure – Reviews the change implementation results including if it followed the release and deployment plan and was completed within the release window. The Change Manager reviews with the change stakeholders to determine satisfaction and success with the change implementation, lessons learned, and closure of the change.

Review and Close Deployment – Reviews the deployment against the requirement. Deployment is completed with a handover of the support for the deployment group or target environment to Service Operations.

2 Change Advisory Board

"2.A Institute a Change Advisory Board (CAB)

1. The CAB members shall ensure that the requested changes are thoroughly checked and assessed from both a technical and business perspective."

Unisys will institute a Change Advisory Board (CAB)

The Change Advisory Board or CAB considers requests for change (RFC's) based on business needs and determines whether they should be accepted and implemented or rejected. Recommendations are based on several factors; for example, they could include impact, risk, priority and urgency on service and cost of change. The CAB has responsibility for reviewing RFCs (Requests for Change), analyzing and determining acceptance of all change requests. It is imperative that the CAB monitors and controls the use of the emergency change process and limits the number of emergency change requests, as they attract higher levels of risk.

The following actions are performed in a CAB meeting:

- Reviews and approves Changes on the basis of individual area of authority.
- Reviews Emergency Changes.
- Schedules Changes.
- Raises issues and concerns in areas such as risk mitigation, business impact and scheduling as appropriate.
- Reviews previous meeting minutes.
- Reviews failed Changes.
- Reviews Incidents caused by Changes.
- Reviews Progress reports on on-going Change Requests.
- Prioritizes Changes (as needed).
- Periodically validates Criteria of Change Requests to be assessed by the CAB.

- Validates/Approves FSC – identifies risks, impacts and gains client approval to delay Changes.
- Validates and updates any modifications to the Freeze periods, Business events, holidays and maintenance periods.

2.B Offeror must describe its proposed approach to creating a CAB and describe how members should be selected.

Unisys proposes the following approach to creating a CAB and how members should be selected.

The Unisys Change Manager will work with the Commonwealth Enterprise and Agency Change Managers during transition to the operationally ready ITSM platform to define the appropriate CAB structure for local Agency reviews of changes and how they will be processed through the Unisys and Commonwealth Enterprise CAB structure. It is important to get this structure correct in order to balance local and enterprise requirements for change and to keep it streamlined in order to facilitate change while managing risk. It is also important to balance emergency changes and engineering reviews to manage time effectiveness and manage risk while also helping to provide that the process does not become too bureaucratic.

CAB members are chosen to help verify that changes can be adequately assessed from both the business and technical viewpoint. **Figure 3.2.1.3-3** is a template for determining if members should be chosen to fill certain roles and responsibilities on each CAB. Unisys will collaborate with Commonwealth and agency leadership to define the following agency CAB membership roles.

Change Advisory Board				
Mandatory Attendees				
Member	Name	Email Address	Role	Permanent /Member by Change Requirement
Change Manager or an appropriate deputy (theatre/client/business unit or area specific)			Chair the Meeting	Permanent
Client Change Authority			Participant	Permanent (by client)
Client Business Continuity Authority (or appropriate deputy)			Participant	Permanent (by client)
Change Coordinator(s)			Scribe	Permanent
Configuration Manager			Participant	Permanent
Program Management Office			Participant	Permanent
Business Representatives			Participant	Permanent (Client & Unisys)

Business Testers			Participant	Permanent
Capacity Manager			Participant	Permanent
Security Manager			Participant	Permanent
Change Requester - (client or internal support personnel)			Participant	Member by Change Requirement
Change Assignee of Change being discuss at CAB			Participant	Member by Change Requirement
Client Service Delivery Managers			Participant	Member by Change Requirement
Experts/Technical Consultants (Production, Support, Development Analysts)			Participant	Member by Change Requirement
Service Desk Representative			For understanding impact to user experience	Member by Change Requirement
Suppliers, maintainers and developers (client suppliers, Unisys, or third-party contributors)			Participant	Member by Change Requirement
Client Service Owners			Participant	Member by Change Requirement
Office services and other non-IT supporting services			Participant	Member by Change Requirement
Business and technical Testers			Participant	Member by Change Requirement

Emergency Change Advisory Board				
Title	Name	Email address	Role	Permanent /Member by Change Requirement
Unisys Change Manager			Chairs the Meeting	Permanent
Unisys Change Coordinator			Facilitates the Meeting	Permanent
Service Delivery Manager			Participant	Member by Change Requirement
Service Desk Supervisor (for understanding impact to user community)			Participant	Permanent
Technical Service Owner			Participant	Member by Requirement
Incident Resolver			Participant	Member by Requirement
Relevant Client Service Owner			Participant	Member by Requirement
Experts/technical consultants			Participant	Member by Change Requirement

Figure 3.2.1.3-3 Change Advisory Board Template

2.C Offeror must describe its approach to handling changes at an agency level

Unisys proposes the following approach to handling changes at an agency level. Unisys will review the process below and incorporate agency requirements and modifications during transition. Unisys will:

- Conduct weekly Change Management meetings with Commonwealth and agency representatives to address all concerns prior to change implementations. Unisys will notify affected Commonwealth agencies before and after any changes.
- Establish scheduled maintenance periods, and communicate the scheduled outages to confirm Commonwealth agency maintenance windows are properly aligned with agency and Unisys resources.
- Manage multiple Commonwealth agency maintenance windows by using a flexible methodology to account for agency individual needs.
- Coordinate agency maintenance windows with Commonwealth agencies and establishes agency annual maintenance schedules.
- Utilize agency approved e-mail distribution accounts to broadcast upcoming maintenance windows and provide status updates during maintenance window.
- Deploy extensive maintenance playbooks that are aligned with the ITSM Change Management.
- Provide the Commonwealth with a daily Change Report, which includes all changes scheduled for installation. The contents of Daily Change Reports include:
  - The date the change is targeted for installation.
  - A description of the change.
  - Change request number.
  - The risk factor assigned to the change.
  - Business impact of installing the change.
  - The current change status.
  - The organizational unit assigned to the change with a contact person.
  - Estimated time of installation.
  - Change request records - changes submitted in the last 24 hours.
- Validate all changes after implementation to verify Commonwealth Agency compliance.
- Obtain Commonwealth Agency approvals prior to closing all implemented changes.

2.D Offeror must provide a sample CAB organization and meeting schedule.

The following is a sample CAB structure depicted in **Figure 3.2.1.3-4** to confirm Commonwealth agency changes are fully vetted before implementation.

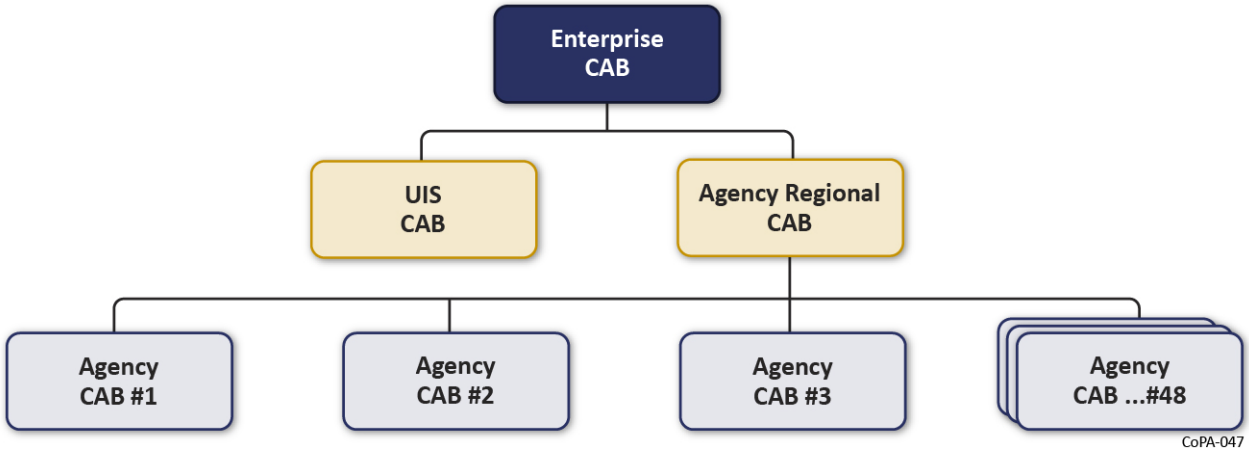


Figure 3.2.1.3-4 Change Advisory Board Sample Structure

The CAB meeting schedule will depend upon the structure for CAB's that is decided between Unisys and the Commonwealth during transition.

3 Test, Infrastructure, Test Plan

3.A Offeror must file a Pre-Change Test Plan, as part of the Change & Release request process, including results before final approval to proceed.

Test infrastructure related changes & releases before implementation. This includes Offeror managed hardware and any Offeror managed software.

Unisys will test infrastructure related changes and releases before implementation as per the process defined in **Figure 3.2.1.3-5** below. This includes Unisys managed hardware and Unisys managed software.

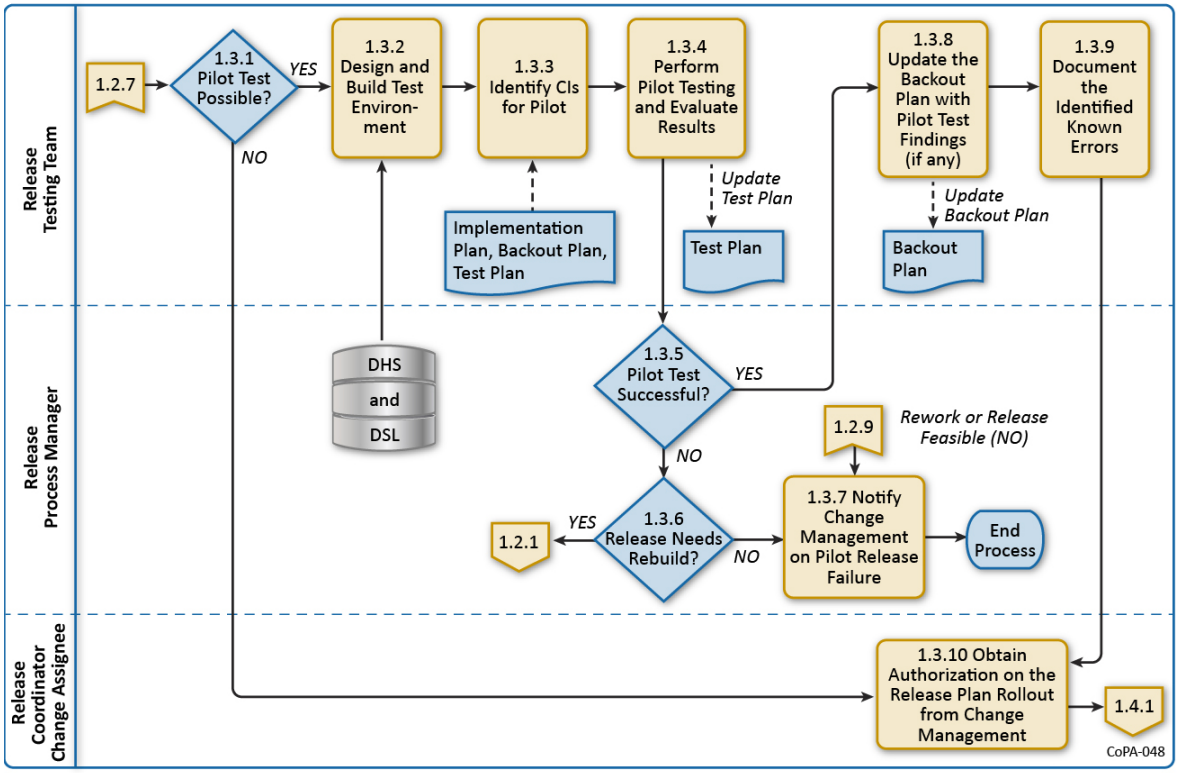


Figure 3.2.1.3-5 Release Testing Process

The Unisys process is to complete acceptance testing of infrastructure related changes and releases before implementation to prevent production services impact to Commonwealth Agencies. Unisys consistently follows the following process before migrating infrastructure related changes into the data center production environments. Prior to implementation, planned change requests are reviewed to confirm that:

- A Pre-Change Test Plan is completed and approved by Commonwealth agencies and the CAB
- Pilots are evaluated for release deployment of changes
- Test environments are planned to support Test Plan and then ordered by the Commonwealth through the Enterprise Services Catalog
- The change can be completed within the requested change window.
- Thorough testing in non-production environments has been accomplished by Vendor and the Commonwealth, as applicable.
- On-site coverage is provided or available via callout procedures.
- Back out plans and detailed instructions are in place.
- Installation instructions are understandable and complete.
- Test results are compiled, reviewed with the Commonwealth and retested after appropriate changes are made
- Commonwealth Agency and CAB approvals have been obtained prior to release and deployment

3.B Offeror must create and maintain test environments where testing will be conducted and evaluated prior to implementing any change into production environments

The Unisys Change & Release Management Team working with the Commonwealth will indicate what testing environments need to be ordered from the Enterprise Services Catalog in order to test specific change requests. This will be part of the Change & Release Management process and procedures.

3.C Offeror must described its proposed process and provide a sample overview of process and procedures.

Please refer to a sample process overview of test process and procedures in **Figure 3.2.1.3-5** above.

4 Scheduled Maintenance

4.A Establish scheduled maintenance periods, and communicate the scheduled outages. Create a notification process for maintenance, emergency, and unplanned outages

Unisys will create standard change windows for standard changes and release schedules for major releases. Unisys will create a standard method to notify the appropriate agency personnel of expected and unexpected outages. This will be completed through Agency CAB meetings for deployment approvals, electronic notifications and Remedy broadcast messages and Unisys/Commonwealth Portal messages.

4.B Offeror must establish regular maintenance periods for each computing platform. Maintenance periods must be coordinated per agency due to different peak business requirements.

Unisys will establish regular maintenance periods for each computing platform. Maintenance periods will be coordinated with each agency due to different peak business requirements.

4.C Create mechanism to notify clients of expected and unexpected outages

Unisys will create a mechanism to notify the appropriate agency personnel of expected and unexpected outages. This will be completed through Agency CAB meetings for deployment approvals, electronic notifications and ITSM system broadcast messages and Unisys/Commonwealth Portal messages.

4.D Offeror must describe its process for managing maintenance periods and system outages, with examples

Please refer to 4.E below for a description of the process for managing maintenance periods with outages with examples.

4.E The Offeror must provide an approach to managing multiple agency specific maintenance periods with different peak periods.

The process for managing maintenance periods is complex by nature for supporting many different agencies across the enterprise. This will have to be managed by SLA agreements, reviewing conflicts for releasing changes into the environment by utilizing the CMDB and application relationships to infrastructure to determine the best approach to accomplish particular types of changes. In some cases the release of changes will have to be managed in stages with a complete project plan, tested and released , in order to support SLA's and still meet the requirements for change management.

An example for managing maintenance periods and system outages with different peak period requirements involves Unisys managing the complex change request to upgrade the IBM Mainframe in 2011 to zEnterprise that involved multiple agencies. This required formally managing the change using formal project management disciplines to initiate, plan, execute, monitor and control, and close out the project in support of the change request. The key to the plan was getting the different agencies and stakeholder's requirements and developing a plan that would accommodate their requirements to support their customers.

5 Change and Release Notifications

5.A Notify affected Commonwealth agencies before and after any changes

Unisys will establish scheduled maintenance periods, and communicate the scheduled outages for release schedules in advance according to an agreed schedule. Unisys will create a notification process for maintenance, emergency, and unplanned outages.

Unisys will establish regular maintenance periods for each computing platform. Maintenance periods will be coordinated with each agency due to different peak business requirements.

Unisys will create a mechanism to notify the appropriate agency personnel of expected and unexpected outages. This will be completed through Agency CAB meetings for deployment approvals, electronic email notifications and Unisys/Commonwealth Portal messages.

Unisys will establish with the Commonwealth agencies, maintenance periods for system outages. The process will support multiple agency specific maintenance periods with different peak periods.

5.B Provide Change & Release Notifications prior to implementation via a central web site and e-mail.

Unisys will create a mechanism to notify the appropriate agency personnel of expected and unexpected outages. This will be completed through Agency CAB meetings for deployment approvals, electronic email notifications and Unisys/Commonwealth Portal messages

5.C Offeror must describe its proposed process and procedure related to notifications.

Unisys will notify affected Commonwealth Agencies with change and release notifications.

Unisys will notify affected Commonwealth agencies and stakeholders before and after any releases of approved changes as per the Release Communication process defined below in

Figure 3.2.1.3-6

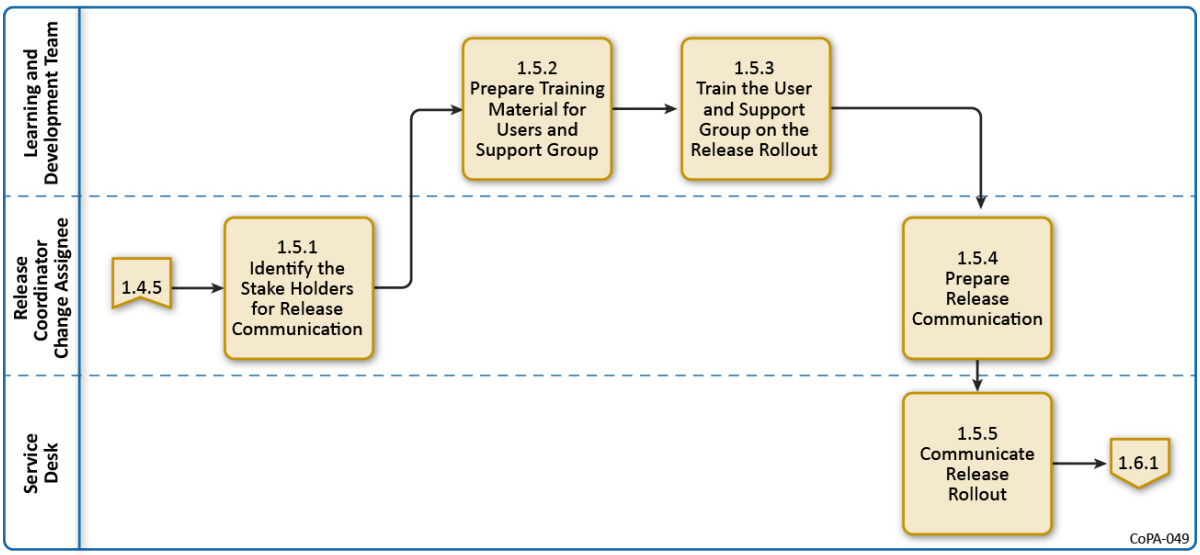


Figure 3.2.1.3-6 Release Communication Process

5.D Offeror must describe any other change notifications capabilities available to the Commonwealth.

Unisys will review with the Commonwealth during transition change notification through tools and processes to determine the most effective ways to notify stakeholders.

6 Change Review, Change Validation

6.A Complete a post change review to validate the success or failure of the change or release, and post the information within the change record. Take follow up action as appropriate

Validate all changes after implementation.

All changes are validated as part of the release process described above

6.B Offeror must describe its proposed process and procedure.

All changes and releases are reviewed by the implementation team to verify the change and release are technically implemented correctly and then with stakeholders to confirm that the change and release had the intended outcomes.

Depending on the size and risk of the change and release there may be an Early Life Cycle team to support the change and release for a period of time to confirm it is stable before the change and release tickets go through their post implementation closure process and procedures.

Please refer to the Change and Release Processes Closure process and procedures described above in section 1.

7 Change and Release Backout Process

7.A Prepare back out procedures for all changes.

All change requests will be required to have back out plans. These plans will be reviewed by the appropriate technical reviewer(s) of the changes. Depending on the risk of the change, a test of the back out plan may be required to be performed during the release testing process.

7.B As part of the Change & Release process, file a back out plan as appropriate to remove the change and restore Services to the prior level.

Unisys will require a back out plan for each change and release before a change and release is approved. The Change Manager and Release Manager working with the change implementation team, will determine when a release or individual changes need to be backed out.

7.C Offeror must describe its proposed process and procedure related to back out procedures.

Figure 3.2.1.3-7 below is the proposed process and procedure at a summary level for backing out a release.

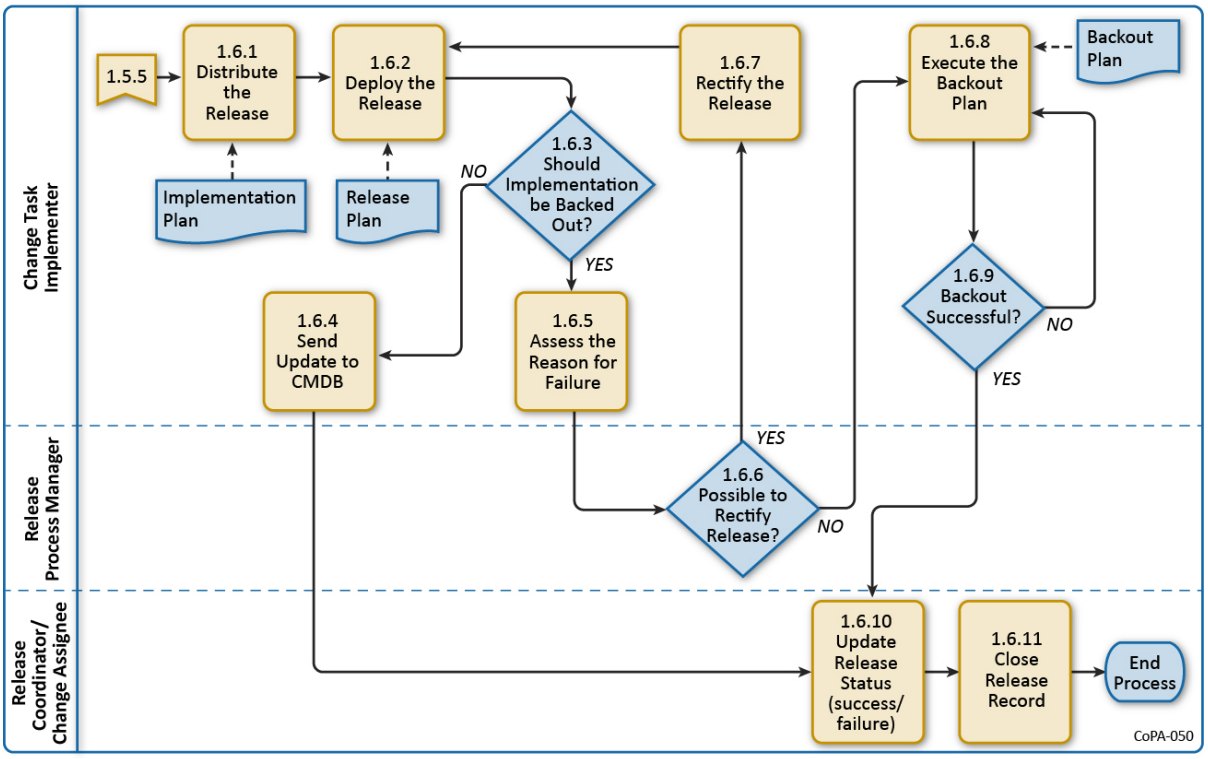


Figure 3.2.1.3-7 Release Back Out Process

1.6.3 Should Implementation Be Backed Out

Before proceeding with further deployment, the Change Task Implementer confirms whether the Deployed Release is working as planned together with the Change and Release Managers.

If the deployment is successful, then proceed to step "Send update to CMDB," to update the changes in the CMDB, or proceed to step "Assess the reason for failure," in the Release Management process workflow.

1.6.4 Send Update to the Configuration Management Database

If the release implementation is as expected, the Change Task Implementer sends the details of the changes affected due to release to the Configuration Manager to update the CMDB.

1.6.5 Assess the Reason for Failure

If the release implementation fails, the causes for the failure of the release are assessed, diagnosed, and documented. The determination for the implementation failure would be performed through a Post Implementation Review.

1.6.6 Possible to Rectify Release

The Release Process Manager decides whether rectifying the release is possible. If it is decided that the release cannot be rectified, then proceed to step, "Execute Back-out Plan," or proceed to step, "Rectify the Release," in the Release Management process workflow.

1.6.7 Rectify the Release

The Change Task Implementer tries to identify the reason for the failure in release implementation. If the reason for the failure and its remedial action are identified, then the Change Task Implementer proceeds with the deployment of the release.

1.6.8 Execute Back-out Plan

If the Release Process Manager has decided to abort the release, then the Change Task Implementer executes the steps detailed in Release Back-out Plan.

1.6.9 Back-out Completed Successfully

After executing the Back-out Plan, the Change Task Implementer validates if the release back-out was executed successfully. If the Back-out Plan executed successfully, proceed to step, "Update Release Status (Success/Failure)," or proceed to step "Execute Back-out Plan," in the Release Management process workflow.

1.6.10 Update Release Status (Success/Failure)

The Change Coordinator updates the status of release rollout with "Success," "Success with Issues," or "Failure" against the Change record based on the details provided by the Release Coordinator/Change Assignee and/or Change Task Implementer.

1.6.11 Complete Release Record

The Release Coordinator or Change Assignee completes the Change record.

8 Change and Release Statistics

8.A Track all (successes / failures) changes and produce Change & Release management statistics.

All change and release tickets which bundle changes to be deployed are tracked in the Unisys ITSM Suite. The details of the changes and releases are captured in these tickets and reported as described below.

8.B Create and deliver a monthly Change & Release Management Report to the Commonwealth, detailing changes, implementation status, and outage time periods as compared to planned outage schedules.

Unisys will create and deliver a monthly Change & Release Management Report to the Commonwealth, detailing changes, implementation status, and outage time periods as compared to planned outage schedules. The following is a standard report template that Unisys will deliver to the Commonwealth for Released Changes.

ID No	Related Changes	Description	Start Date Time	End Date Time	Clients Affected	Release Success / Failure	Impact	Root Cause	Corrective Actions	Responsibility for implementing corrective actions

8.C Offeror must describe its proposed process and procedure.

The process and procedure for reporting change and release ticket statistics is part of the overall Change and Release Management Processes described in 1.A.

The statistics reporting will be produced monthly in a format similar to what is shown above in 8.B.

Unisys Team Experience

Unisys currently provides IT Service Management Services to more than 150 customers worldwide. Unisys is a leading provider of Managed Services utilizing an integrated suite of ITIL V3, ISO 20000 certified management processes and leading ITSM tools to provide outstanding service IT services to our customers. Unisys currently successfully manages Change and Release Management for many of these customers.

Unisys has been managing Change and Release management for the Commonwealth DPH and [redacted] since 1999.

Benefits to the Commonwealth

The Unisys value proposition for Change and Release Management Solution to the Commonwealth is as follows:

- Unisys focuses on the Change and Release Management Processes from an ITIL best practices perspective, by actively managing changes with the highest risk to business applications and users. This helps to minimize impact to Commonwealth Mission critical

services. Standard changes with well documented procedures for implementation are handled through automated change and release approval procedures with summary change management review.

- Unisys has proven success in managing high risk changes for the Commonwealth that have multiple agency critical business risks associated with them.

3.2.1.4 Service Desk

As part of the Services, Offeror shall provide telephone support (e.g., a "Service desk") to the Commonwealth to assist the appropriate end users in determining, tracking and resolving questions regarding the Services. Offeror shall provide telephone support through such telephone support infrastructure maintained by the Offeror. This telephone service desk is to augment the required “online” Service Desk capabilities as set forth in the RFP.

The Service Desk will be the single point of contact for authorized Commonwealth users regarding incidents, which include events that cause or may cause an interruption or reduction of service, as well as requests for information, and requests for Services relating to all of the Services provided within the Offeror’s catalog of Services. The Offeror’s Service Desk must have processes for Service Delivery and Service Management that are ITIL-conformant. The Service Desk process includes Service Management processes: Incident Management, Problem Management, Change Management, Configuration Management and Service Request Management.

Currently most Commonwealth agencies provide a local Help Desk function to support staff’s desktops, local printing systems, applications, and the general public users it serves. The Offeror must develop a process and electronic connection to these agency Help Desks. The majority of the agency Help Desks utilizes the Commonwealth’s Enterprise ITSM. A connection between the Commonwealth’s Enterprise ITSM and the Offeror’s Service Desk will be required to keep Help Desk tools synchronized.

In addition, the Offeror must provide an Internet accessible KMP as a central repository for processes and procedures, communications plans, and other relevant documentation to be shared with the Commonwealth. Knowledge Management will be a function shared by the Commonwealth along with the Offeror. This will allow the Commonwealth to combine data from all Commonwealth agencies and the Offeror, reorganize it, make it understandable, and present it to the Commonwealth.

The Offeror must coordinate with the Commonwealth to provide feedback on the effectiveness and accuracy of KMP content. In addition, the Offeror must notify the Commonwealth when incorrect information is identified, reference material becomes outdated, or when the content is rendered inaccurate. At the Commonwealth’s discretion, the Offeror may be required to develop content, as needed, including answers to frequently asked questions, reference/educational materials, and other documents to be added at the Commonwealth discretion.

The Offeror must create and keep current a CPPM that documents the processes, procedures and timelines used to meet the requirements of this contract. The CPPM must provide detailed process descriptions to support the computing needs of the Commonwealth utilizing best practices and be made available (via Offeror’s Portal) to all Commonwealth agencies throughout the term of the contract.

Reference Documentation

Exhibit K - OA Enterprise ITSM System and Volumetrics

Schedule H - Commonwealth Computing Procedures Manual (CCPM)

Requirements		Describe Compliance
1.	Provide an integrated Service Desk process with the other Service Management processes, including Incident Management, Problem Management, Change Management, Configuration Management and Service Request Management. The final Service Desk processes and procedures must consider current Commonwealth service management policies and procedures.	Offeror must describe its Service Desk solution offering (processes, procedures, staffing, and technologies). Offeror must provide a sample of its KMP from a previous or current engagement of Offeror.
2.	Provide a Service Desk with processes and tools for Service Delivery and Service Management that are ITIL-conformant.	
3.	Seamlessly integrate the Service Desk (including tools, technology and processes) with the Service/Help Desk(s) of other identified Agency Service Desks as required. The Offeror must coordinate the integration of the proposed Service Desk with the Commonwealth's Enterprise ITSM System and other agency Help Desks as required. Integration with other agency ITSM systems is not required.	
4.	Analyze incident trends, and recommend and implement actions, with Commonwealth's approval, to reduce incidents.	
5.	Conduct random surveys of authorized	

	users of the Service Desk in accordance with the Commonwealth each month.	
6.	Develop and document processes regarding interfaces, interaction, and responsibilities between Level 1 Support personnel, Level 2 Support personnel, and any other internal or external persons or entities that may either submit notice of an incident or receive notice of an incident.	
7.	Ensuring staffing levels and work allocation remains appropriate to handle incident volumes and incident response targets.	
8.	Provide trained service desk personnel.	
9.	Ensure that the Service Desk is available at all times (i.e. 24 hours a day, 365 days a year).	
10.	Manage all Incidents and/or Service Requests from authorized users relating to Contracted Services.	
11.	Provide weekly reports to the Commonwealth on Service Desk activities, performance, and adherence to established SLAs. Service Desk reporting must include at a minimum: • Key issues relating to Service Desk processes, improvements, script development. • Status as to Service Desk staffing, training, and authorization. • Integration activities and issues with other Service Desks	

	belonging to the Commonwealth. • Trend analysis shall include (13) most recent months. If the Service has been in place less than thirteen months then trend analysis shall include all months of Service. • Calculate metrics and provide monthly reports. • Number of Contacts, to include all interactions (Calls, phone calls, electronic, automated or otherwise). • Number of calls abandoned, average call duration, average time to answer, average time to abandon. • Number and percentage of Contacts resolved. • Number and percentage of Contacts passed to other Service Desks. • Other pertinent information regarding Service Desk operation and performance.	
12.	Enable a KMP accessible by all authorized users. Content for the KMP will be approved by the Commonwealth.	
13.	Offeror must record all incidents, problems, service requests, change requests, and configuration information in the software recording tool. All updates to the record, contacts with clients or vendors, and resolutions will be recorded in a real-time and consistent manner. This recording tool	

	will house the KMP.	
14.	Monitor reporting system to ensure incidents and problems are being addressed to meet agreed SLAs.	
15.	Transition must include the transfer of system and application monitoring alerts with the ability to turn-off the problem alert process during maintenance windows and other scheduled outages.	Offeror must describe its approach to ensure alerts are transitioned successfully.
16.	Interim Support Desk Procedures will be required as the Commonwealth transitions from its current support architecture to the Offeror's Service Desk.	Offeror must describe an interim approach and procedure(s) for providing Service Desk operation throughout the transition to the Offeror's fully managed service.
17.	Incident Management - The Offeror's Incident Management process shall encompass Incident Management processes deployed across all Service Components that are designed to: restore service as quickly as possible, minimize disruption to the Commonwealth, aim for highest levels of availability and service quality, completely transparent and auditable delivery of service, and promote the highest level for user satisfaction.	Offeror must describe its Incident Management Process and how it will be applied to the overall IT Service Management Program for the Commonwealth.
18.	Problem Management - The Offeror's Problem Management Process must minimize the adverse effect on the business of Incidents and Problems caused by errors in the IT infrastructure, Applications, systems and supporting components, and proactively prevent the occurrence of Incidents and Problems by identifying	Offeror must describe its Problem Management Process and how it will be applied to the overall IT Service Management Program for the Commonwealth.

	and eliminating causes of failure.	

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

Introduction

Unisys understands the Commonwealth's need for a high-quality Service Desk to front-end outsourced data center support with predictable delivery. With the complexity of the Commonwealth's data center environment, you can trust Unisys to provide the critical Service Desk front end to our data center support program that delivers timely response, efficient resolution, and a high level of service for Incident Management and Problem Management.

Unisys will use our many years of experience in delivering services to the Commonwealth, and will Transition from the DPH Help Desk to an ITIL V3 based Service Desk. Resources with additional technical and Request Management experience will be put in place to provide the required support to deliver to the Commonwealth quality and service flexibility in support of the expanded data center services scope.

1 Service Desk Process, staffing, technology, experience

1.A Provide an integrated Service Desk process with the other Service Management processes, including Incident Management, Problem Management, Change Management, Configuration Management and Service Request Management. The final Service Desk processes and procedures must consider current Commonwealth service management policies and procedures.

The Service Desk Process will integrate with the other Service Management processes and procedures that we will implement including:

- Incident Management
- Problem Management
- Change Management
- Release Management
- Configuration Management
- Service Level Management
- Service Request Management.

All processes are supported by the Unisys ITSM Solution used to track and manage all service delivery and management functions.

During the transition of services, Unisys will conduct a series of workshops in which our base processes will be aligned with Commonwealth processes for the in-scope services to establish a common understanding and gain approval of the process framework deployed to support service delivery from Unisys.

1.B Offeror must describe its Service Desk solution offering (processes, procedures, staffing, and technologies).

The **Service Desk** function provides a central point of communication for all authorized Commonwealth users agency staff to report incidents, requests for information, and service requests relating to all of the services provided within the Enterprise Services Catalog. The Service Desk staff manages ITIL V3 conformant Service Management processes leveraging the ITSM Incident Management system that is electronically connected to Commonwealth agency help desks. This functional team also manages the Knowledge Management Portal, a central repository for processes and procedures, communications plans, and other documentation to be shared with the Commonwealth.

The Unisys Service Desk will be delivered from our Harrisburg, Pennsylvania location during core hours (Mon – Fri 7am – 6pm Eastern) with supplemental services provided after hours, weekends, and designated holidays from our U.S. based Managed Service Center (MSC) located in Salt [redacted] All personnel used in the delivery of the Commonwealth solution are U.S. based employees. This team will be utilizing the dedicated instance of the Unisys ITSM systems modules in support of this engagement.

Unisys believes that our success in quality delivery, employee satisfaction, and innovation is dependent upon training, active feedback coaching, and employee retention. Critical success factors for our training focus on increasing agent productivity and fostering skill development and career advancement.

Active feedback and coaching is the second method we apply for personnel development. We utilize both formal performance planning processes and informal, mentored feedback. The latter takes the form of call monitoring, shadowing, being shadowed and team oriented projects. These informal measures have proven invaluable in fostering a culture of can-do attitude and good collaborative work process development and re-engineering.

The Unisys Service Desk utilizes standard position descriptions and processes for the worldwide delivery of service desk services. These standards result in a worldwide consistency of service delivery. Skill levels maintained in the Commonwealth support team include:

- **Service Desk Agents** who possess basic technical knowledge of data center infrastructure, as well as effective customer service demeanor. Agents provide primary telephone support for approved Commonwealth users that call the Service Desk.
- **Service Desk Manager** who is the liaison between the Service Desk and Commonwealth management staff proactively monitors ACD queues to identify incidents affecting Commonwealth users of the Services or a significant number of End Users at a site. The manager also trains, supervises and guides agents working at the Service Desk.
- **Incident Managers** are the escalation point that leads the Service Desk effort in responding to Commonwealth user events or disruptions as quickly as possible, in order to minimize the adverse impact on business operations.
- The **Problem Manager** leads the Service Desk effort to identify, determines resolution or temporary work-around, and creates detailed documentation of the underlying problem that caused a disruptive incident (i.e. root cause analysis).
- The **Knowledge Manager** is responsible for ensuring that the Knowledge Management Portal is kept current with updated resolutions and information facilitating up-to-date communication between the Unisys team and the Commonwealth.

- The **Service Desk Reports Analyst** will be responsible for producing all Service Desk reporting including volume based statistics and required SLA reporting. This analyst works to identify positive and negative trends ensuring that in coordination with the Service Excellence Office, corrective action plans are established and monitored.

Additionally, the items below outline from a high level the functions that the Unisys team listed above will deliver from a data center Service Desk perspective.

Unisys will provide:

- Service Desk Agents and Management staff to be co-located with our Program Management Office (PMO) at the local Unisys Harrisburg office Monday – Friday 7am-6pm Eastern, with off-hours, holidays, and weekends supported from the Unisys Managed Service Center (MSC) located in Salt [redacted]
- Toll free 800 number for Commonwealth IT staff and Agency Help Desk resources to contact the Service Desk
- Integration interface between the OA ITSM and the Unisys ITSM system for bi-directional passing of data center incident and request tickets
- Service Portal with links to required CCPM, KMP, and Enterprise Services Catalog, all of which will be created and updated by Unisys.
- Internet accessible KMP housed in the Unisys Service Portal tool. A Knowledge Manager will be responsible for working with Commonwealth agencies and the Service Desk team to keep the KMP information current and relevant for the duration of the engagement.
- End to End Incident and Service Request Management
- Problem Management and Root Cause Analysis
- Field dispatch tools for Unisys to dispatch its engineers (and Partner resources) to perform onsite service in the data centers.
- Service Excellence Office for Trend analysis, service improvement, and incident reduction initiatives.

Unisys has designed the Service Desk response to the Commonwealth based on implementing the following core principles for both organizations:

Partnership

- Work together to inform and serve the Service Desk users, and enhance the experience of the services received;
- Foster a teaming attitude in order to perform, govern and enhance the Services;

Innovation

- Drive constant innovation throughout the life of the Agreement;
- Deliver meaningful innovation while providing a return on the Commonwealth's investment;
- Engage relevant SDB partners to bring creativity and diversity to the Service delivery team.

End-to-end service

- Provide a comprehensive Service Desk team that manages all elements and allows the Commonwealth to concentrate on core functions;
- Manage relevant parties involved in the delivery of the Services; and

Service Quality

- Deliver the Service Levels as agreed; Deliver a consistent service to the Commonwealth;
- Promote a culture of service improvement.

1.C Offeror must provide a sample of its KMP from a previous or current engagement of Offeror.

This section provides sample screenshots from a Knowledge Management Portal. The screenshot in **Figure 3.2.1.4-1** provides a sample of a homepage the user will see upon entering the KMP.

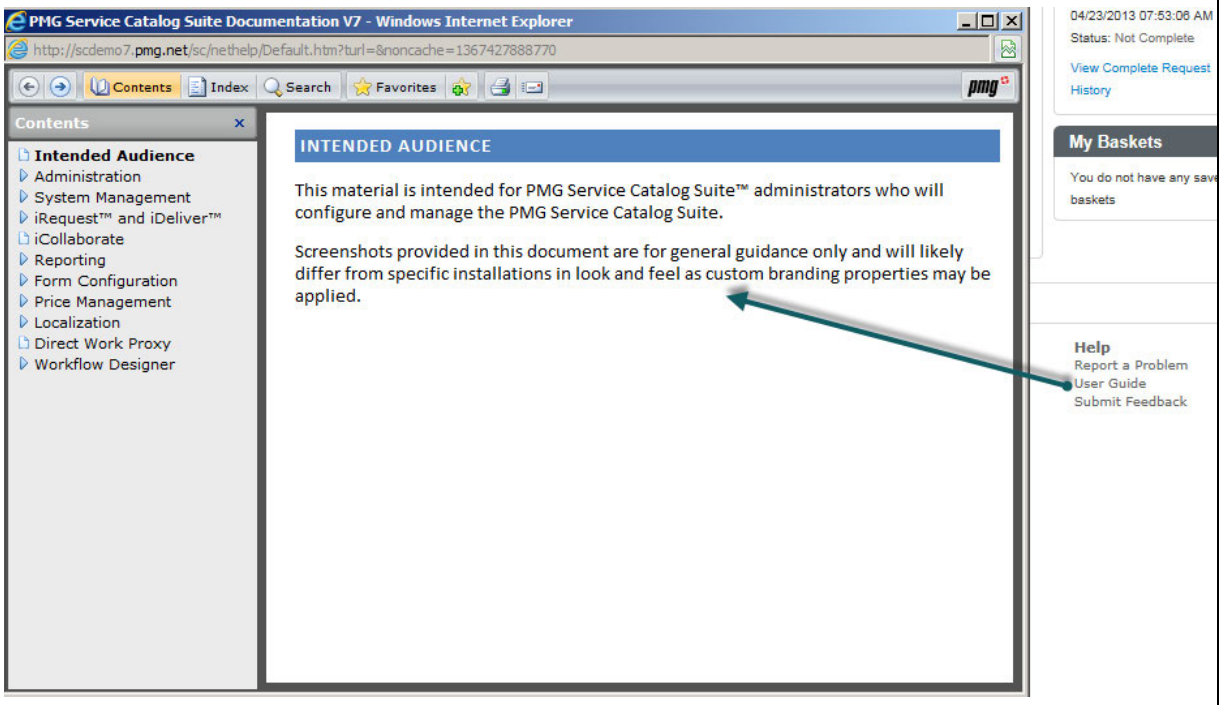


Figure 3.2.1.4-1 Sample Knowledge Management Portal Homepage

The Commonwealth user can select from a variety of options provided on the customized KMP homepage. Options for the Commonwealth will be determined during transition.

The sample homepage screenshot in **Figure 3.2.1.4-2** below provides a news, knowledge, and notification area on the homepage.

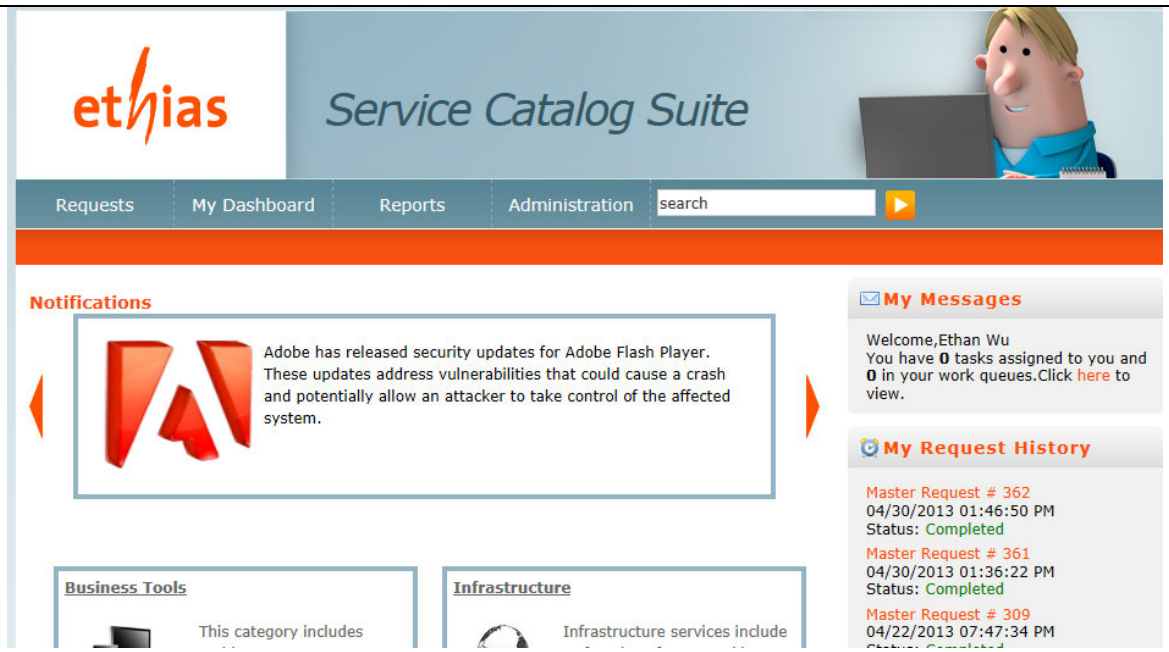


Figure 3.2.1.4-2 Sample Knowledge Management Portal Homepage

In Figure 3.2.1.4-3 below a KMP search box and the returned matching articles are shown.

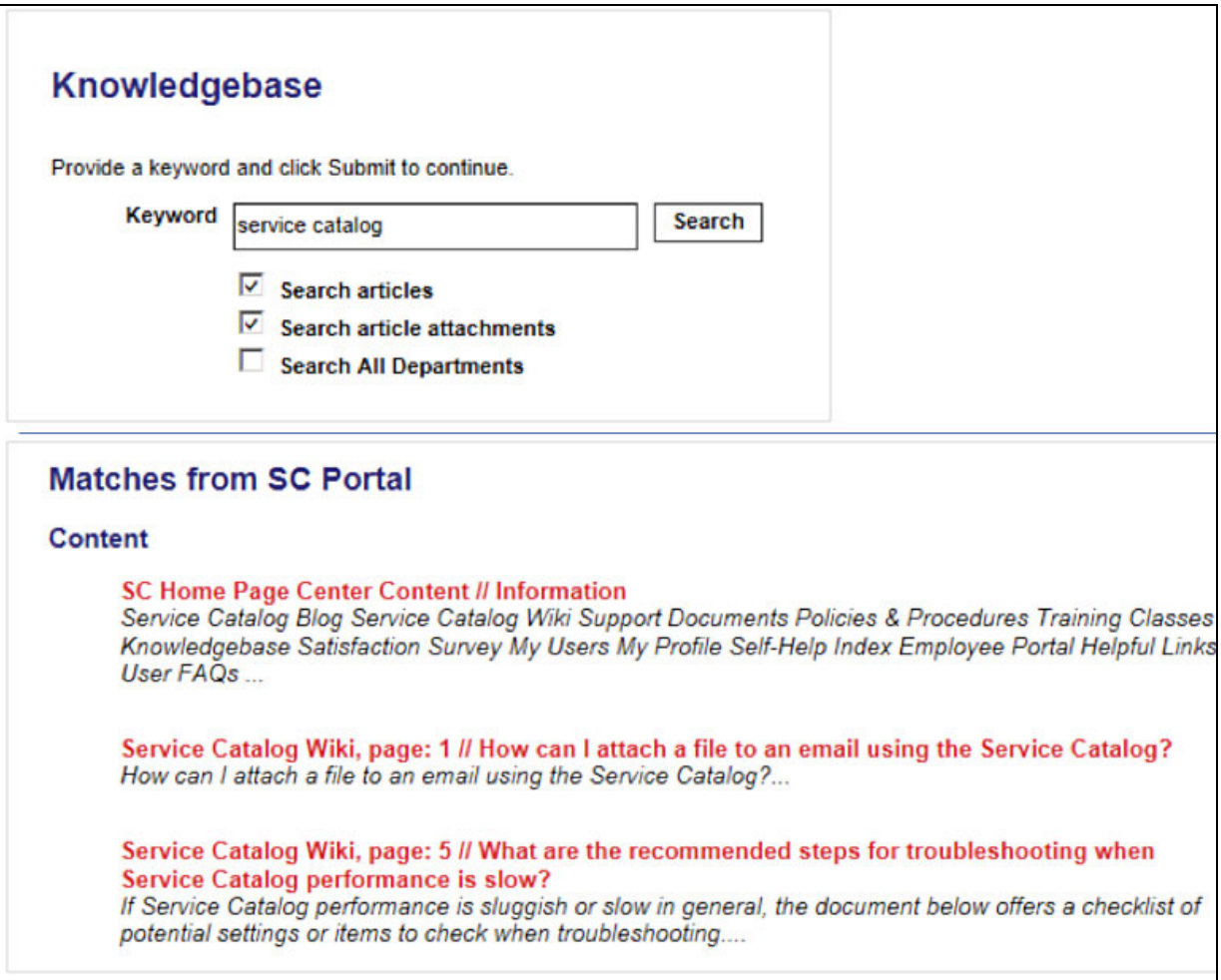


Figure 3.2.1.4-3 Sample Knowledge Management Portal Search

2 ITIL, Service Desk compliance

2.A Provide a Service Desk with processes and tools for Service Delivery and Service Management that are ITIL-conformant.

ITIL (the IT Infrastructure Library) is the most widely accepted approach to IT service management in the world. ITIL provides a comprehensive and consistent set of best practices for IT service management, promoting a quality approach to achieving business effectiveness and efficiency in the use of information systems.

ITIL V3 processes are well known as the de facto standard for service delivery and support in most IT organizations. Not only did Unisys implement these processes, but over the past few years we also developed procedures and work instructions that complement the ITILV3 Framework; these procedures and instructions take a process from a best practice to a powerful daily tool used throughout our global delivery organization. The supporting tools are aligned, consolidated, and rationalized so that Unisys can leverage the long history and legacy of service delivery with the process framework.

3 Integration, Service Desk Integration with other agencies

3.A Seamlessly integrate the Service Desk (including tools, technology and processes) with the Service/Help Desk(s) of other identified Agency Service Desks as required

The Offeror must coordinate the integration of the proposed Service Desk with the Commonwealth's Enterprise ITSM System and other agency Help Desks as required.

The Unisys Transition Team will work with the Commonwealth to develop the integration between the Unisys ITSM System and the Commonwealth ITSM System.
The integration will address process and technology requirements. The integration will be developed to pass information both ways between these systems in a near real-time fashion in order to support Commonwealth and Unisys personnel and partners to support services. The data that is required to be synchronized with the Commonwealth's ITSM System includes:

- Incident (Incident records)
- Problem (Problem records)
- Change (Change requests)
- Configuration (Services, Applications, supporting CI's)
- Asset (Billing data)

4 Incident trend analysis

4.A Analyze incident trends, and recommend and implement actions, with Commonwealth's approval, to reduce incidents.

The Service Excellence Office (SEO) is a Unisys team that will interact with our PMO and all service delivery teams that Unisys is providing. Our SEO's ultimate goal by providing incident trend analysis is to drive continuous improvement in service delivery, with concentration in the following areas:

- **Resolution Optimization and Incident Reduction.** The continual analysis of incidents, and accompanying enabling actions, to move resolutions towards the co-developed KMP content
- **Quality Oversight and Defect Management.** The reporting, analysis, and action plans for service defects, such as inaccurate incident records, incorrect diagnosis, and excessive resolution times
- **Service Management Optimization**. Variance and exception-oriented reporting and analysis that helps to guide Problem Management efforts as well as oversight of ticket coding accuracy and quality to create quality information for data analysis and mining
- **Strong Opportunity Pursuit and Corrective Action.** A tested method that applies the core principles of Six Sigma, incorporates use of Known Solutions Libraries to enable known solutions for previously experienced undesired conditions, and a highly structured investigative and recommendation process that addresses new unexpected, undesired conditions

The Unisys SEO positions us to deliver a unique approach to quality and continuous improvement, creating real, tangible business value for the Commonwealth. Honed by expert design, deep client experience, and collaboration with clients and business partners, our SEO will help your management team see value through Unisys innovation, thought leadership, and data intelligence.

5 Random Surveys

5.A Conduct random surveys of authorized users of the Service Desk in accordance with the Commonwealth each month

Customer Satisfaction Surveys drive the Unisys Client Satisfaction Program. Unisys conducts these Service Desk surveys to:

- Confirm user satisfaction levels
- Identify opportunities to improve agents and processes
- Measure the qualitative aspects of providing Service Desk Services.

Unisys can expand and modify our Customer Satisfaction Survey to include questions about the Data center support dispatches, or we can conduct separate surveys for the separate Service Desk and data center functions. Customer Satisfaction Surveys complete the feedback loop between the user experience and the services received.

Unisys collects clearly defined performance criteria to permit analysis that is deemed important. For surveys of our Service Desk support, for example, we collect at least the agent's name, ticket number, narrative free-form text, and assessment ratings of the agent such as:

- Courtesy and professionalism
- Technical knowledge
- Problem-solving skills
- Communication on ticket progress and resolution
- Overall satisfaction.

Typically, we ask callers to rate performance for:

- Call responsiveness
- Problem resolution time
- Problem resolution quality
- Service orientation
- Overall satisfaction.

Unisys sends a request to complete a Customer Satisfaction Survey via e-mail to users who recently reported an incident via a phone call to our Service Desk. The e-mail contains a hyperlink that takes a user to a Web site to enter his or her responses on a HTML form. Responses are delivered back to our Service Desk by e-mail and collected in a database.

Unisys will use the information collected in our Customer Satisfaction Survey as a basis for continuous improvement of service delivery. To calculate customer satisfaction, we take the sum of all scores for all surveys performed in a month and divide it by the total number of surveys performed in that month.

To conduct Customer Satisfaction Surveys, Unisys uses an automated survey process and a set of questions that ask the end user to rate our service on a scale of 1 to 5:

5—Very Satisfied

4—Satisfied

3—Neither Satisfied nor Dissatisfied

2—Dissatisfied

1—Very Dissatisfied.

For questions the end user rates with a 1 or a 2, Unisys asks the user to provide supporting detail; we record this detail in the survey record and escalate customer satisfaction issues that require follow-up electronically to the Unisys Service Manager or the appropriate management representative. A survey follow-up process can consist of any one or all of the following:

- Review by a manager
- Review by a manager and an analyst or review by a service group
- Calling the end user to verify the rating, obtain additional information as required, and if possible, resolve the issue with the end user
- If applicable, retrieving the original incident call and listening to the recording for detailed information
- Creating and implementing a corrective action plan.

Unisys documents all survey follow-up activity and establishes corrective action plans, as required. We determine calls to survey from the following criteria:

- End users with more than one service request in a 30-day period are surveyed for one request only.
- Service requests more than 7 days old are not surveyed.
- End users requesting not to be surveyed are not surveyed.
- Callers with invalid contact information are not surveyed.

6 Service Desk, Level 1 and level 2 process

6.A Develop and document processes regarding interfaces, interaction, and responsibilities between Level 1 Support personnel, Level 2 Support personnel, and any other internal or external persons or entities that may either submit notice of an incident or receive notice of an incident.

Unisys Incident Management process describes the interfaces, interactions and responsibilities of Level 1 and 2 support personnel in relationship to the complete Incident Management Process lifecycle. This is discussed in detail in the response to requirement 17 below.

7 Staff allocation

7.A Ensuring staffing levels and work allocation remains appropriate to handle incident volumes and incident response targets.

The Unisys Service Desk Manager (SDM), to be located onsite at our Harrisburg area service desk, is responsible for the day to day management of the Service Desk Agents and SLA achievement. The SDM monitors ongoing incident and service request volumes, and has the ability to scale up or scale down Agent staffing levels as needed with an eye on delivery within specified SLAs.

The SDM will use a Workforce Management tool to forecast volumes based on historical information, schedule agents, track agent adherence, and provide robust forecast and "actuals" reporting. The tool applies 24 months of call volume history to forecast monthly volumes, coupled with 13 weeks of the most recent history to calculate expected volumes in specific 15-minute call arrival patterns, using multiple "what-if" algorithms to produce optimal forecast, and recommend optimal scheduling.

8 Staff Training

8.A Provide trained service desk personnel

Unisys recognizes training as one of the critical facets of effective delivery, both to indoctrinate new resources onto the Service Desk and to maintain and continually enhance the skill capabilities of veteran resources to progress improvement and change initiatives. This section details the Service Desk training program for Commonwealth support resources.

The table below summarizes each training track, a high-level description of content, intended audiences, and anticipated duration. The information to follow will discuss how Unisys continually measures resource effectiveness, and leverages training to deliver continuous improvement, as well as how assessments are applied to immediately measure training effectiveness.

Service Desk Resource Training			
Course	Audience	Duration	Content
Unisys Service Desk	Service Desk Agents for the Service Desk	5 Days	• Administrative (Corporate Policies, Security, Time Keeping) • Customer Service (Customer Management, Call Control, Escalation Handling) • Key Systems and Tools (Call Management System, Knowledge Base, Help File, Remote Control) • ITIL/Service Management Overview • Commonwealth Training Track (see below)
Commonwealth Track Training (Commonwealth content)	All Commonwealth Support Resources	As Required (est. 5-10 days)	• Commonwealth - General • Commonwealth Agencies • Data center Services
Commonwealth Track Training (Unisys content, via Discovery and Ongoing	All Commonwealth Support Resources	As Required (est. 5-10	• Commonwealth Application, Infrastructure, Troubleshooting/ Problem Resolution

Knowledge Transfer)		days)	• Service Request Approvals, Processes and Procedures • Key Commonwealth External suppliers; functions and referral methods • Commonwealth Resolution Groups; functions and referral methods • Commonwealth Authorized User Differentiation and Recognition • Major and Critical Event Recognition and Handling
Continuous Improvement	All Commonwealth Support Resources	6-8 hours	Targeted training based on Quality and Resolution Optimization Program, Known Change, Tool Updates, and other required regular training

Effective training should result in measurable, tangible impact that contributes directly to the quality of service, and overall value to the Commonwealth.

9 Availability

9.A Ensure that the Service Desk is available at all times (i.e. 24 hours a day, 365 days a year).

Unisys will provide data center Service desk services on a 7x24 basis as required. The Automated Call Distribution (ACD) and ITSM systems we utilize enable Unisys to operate the Commonwealth Service Desk from multiple locations (Harrisburg M-F core hours; Salt Lake [redacted] Off-hours/weekends) as though they are a single virtual call center. This is a key component of our ability to apply the redundant, multi-center solution we have designed for the Commonwealth. The ACD will be programmed to re-direct calls from our Harrisburg Service Desk to a pool of Commonwealth-trained agents in [redacted] at the specified time each day. This also enables the natural redundancy afforded by multi-center solutions, as well as an ability to quickly tap into available capacity in [redacted] to provide quick "burstability" in the event of sudden, unexpected call volume that may hit the core Service Desk in Harrisburg. Additionally, in the rare instance that the Service Desk onsite in Harrisburg were to go down, all calls can be re-routed to [redacted] until Harrisburg is back online.

10 Incidents and Service Request Management

10.A Manage all Incidents and/or Service Requests from authorized users relating to Contracted Services.

The Unisys Service Desk will be the contact point for all data center-related Incidents and Service Requests. The Service Desk team will provide end-to-end management of all Incident and Requests, whether they are resolved at the Service Desk, or assigned to another designated Unisys, IBM, 3rd party, or internal Commonwealth resolver. A more detailed view of our end-to-end Incident Management process is provided below in our response below to #17 – Incident Management.

11 Service Desk, Weekly Reports

11.A Provide weekly reports to the Commonwealth on Service Desk activities, performance, and adherence to established SLAs. Service Desk reporting must include at a minimum:

Key issues relating to Service Desk processes, improvements, script development.

Status as to Service Desk staffing, training, and authorization.

Integration activities and issues with other Service Desks belonging to the Commonwealth.

Trend analysis shall include (13) most recent months. If the Service has been in place less than thirteen months then trend analysis shall include all months of Service.

Calculate metrics and provide monthly reports.

Number of Contacts, to include all interactions (Calls, phone calls, electronic, automated or otherwise).

Number of calls abandoned, average call duration, average time to answer, average time to abandon.

Number and percentage of Contacts resolved.

Number and percentage of Contacts passed to other Service Desks.

Other pertinent information regarding Service Desk operation and performance.

Unisys will implement a reporting solution for the Commonwealth that will deliver all of the detailed and summary Service Desk reports required as outlined at the top of this Section. The Reports will be created from data located within the Unisys ITSM system, as well as from our ACD, and will be posted on a Service Portal for access by designated Commonwealth management resources only. Additionally, the Service Delivery Manager will review the reports with your designated management team at designated intervals in order to address Critical open items and SLA achievement.

12 KMP

12.A Enable a KMP accessible by all authorized users. Content for the KMP will be approved by the Commonwealth.

Unisys will provide an Internet accessible KMP housed in the Unisys Service Portal. A Unisys Knowledge Manager will be responsible for working closely with the designated Commonwealth resources, as well as Data Center Service Desk team, to keep the KMP current and relevant. Unisys KM Technical Writers will be available to the Knowledge Manager to assist in developing content as required. This may include FAQ's and answers, service briefs, white papers, workarounds, or other documents as determined by the Knowledge Management and/or Commonwealth management. A sample of KMP screen shots is provided to our response to requirement 1C above.

13 Service Desk Recording Tool

13.A Offeror must record all incidents, problems, service requests, change requests, and configuration information in the software recording tool. All updates to the record, contacts with clients or vendors, and resolutions will be recorded in a real-time and consistent manner. This recording tool will house the KMP.

The Unisys Team will utilize a dedicated ITSM tool in order to record all incidents, problems, service requests, change requests and configuration information.

The Unisys Service Portal will house the KMP which is accessible to all authorized Commonwealth personnel.

14 Monitor Reporting

14. Monitor reporting system to ensure incidents and problems are being addressed to meet agreed SLAs

The Unisys Service Desk Manager (SDM), to be located onsite at our Harrisburg area service desk, is responsible for the day to day management of the Service Desk. This includes monitoring the end-to-end handling of Incidents and Problem activity in our ITSM system on an ongoing basis, with a special focus on active P1 and P2 Incidents. The Unisys PMO as well as the Incident Managers, Problem Managers, and Agents at the Service Desk, will utilize these reports to support attaining SLA's for Incidents and Problems.

15 Transition of Service Alerts

15.A Transition must include the transfer of system and application monitoring alerts with the ability to turn-off the problem alert process during maintenance windows and other scheduled outages.

Offeror must describe its approach to ensure alerts are transitioned successfully.

Unisys will adopt existing monitoring of infrastructure and application monitoring and direct all events to a centralized platform for event management in order to facilitate a timely transfer of an agency application monitoring or data center infrastructure when it makes sense to do so to minimize transition issues and support a timely transition.

This will allow Unisys to manage all infrastructure from a centralized event management platform thereby supporting an efficient and effective process for event management.

The Unisys Operations Team will have the ability to turn off automated incident creation in this centralized platform in support of maintenance windows for changes to applications or infrastructure Configuration Items (CIs). Unisys does not recommend turning off event management monitoring during a maintenance window.

16 Service Desk, Tiered Support, Transition Operations

16.A Interim Support Desk Procedures will be required as the Commonwealth transitions from its current support architecture to the Offeror's Service Desk.

16.B Offeror must describe an interim approach and procedure(s) for providing Service Desk operation throughout the transition to the Offeror's fully managed service

The existing Unisys Help Desk will continue to deliver service for DPH until the agreed 'Go Live' date for the new Unisys Service Desk team to take over responsibility for all of the data center services in scope for the engagement. While the current help desk is running as usual, behind the scenes Unisys will start the data gathering, data assessment, ITSM, Portal and KMP setup. In parallel the agent recruitment and training process will commence to get the additional new Agents in place and ready for a gradual Go Live period. Approximately 2-3 weeks before the scheduled Go Live period we will pilot handling a portion of the new expanded volumes to help the agents improve in a low volume live setting. This allows them to test the quality of the support scripts and help files that were developed during Transition, and give time to make adjustments as needed before a full go Live.

17 Incident Management

17.A Incident Management - The Offeror's Incident Management process shall encompass Incident Management processes deployed across all Service Components that are designed to: restore service as quickly as possible, minimize disruption to the Commonwealth, aim for highest levels of availability and service quality, completely transparent and auditable delivery of service, and promote the highest level for user satisfaction

The primary goal of incident management is to respond to issues and/or requests and return to normal operation as quickly as possible and minimize the adverse impact on business operations, thus ensuring the maintenance of the best possible quality and availability of levels of service. The incident management process records incidents, as well as service requests. Recording verifies that there are no lost incidents or service requests, allows the records to be tracked, and provides information to aid problem management and planning activities. The process includes the use of technology to provide self-service facilities to clients, providing them with flexible and convenient interfaces to the support function while also reducing the workload and personnel requirements of the service desk.

Incident management also includes the process of preventing the recurrence of faults, and the application of preventative maintenance to reduce the likelihood of faults occurring in the first instance.

It should be noted that the service desk owns the monitoring, communications, and resolution of all registered incidents. Although specialty groups may be called in to aid in the incident resolution, the service desk maintains ownership of the incident until it has been resolved and closed.

The effective management of incidents is a complex process that requires interaction with many other service management functions, most notably problem management, configuration management, and change management.

A more detailed description of the incident management process utilized by Unisys is as follows in our response to #17B below:

17.B Offeror must describe its Incident Management Process and how it will be applied to the overall IT Service Management Program for the Commonwealth.

The Unisys Team will utilize the following Incident Management Process framework shown below to support Incident Management for the Contract. The Unisys Incident Management Process is comprised of the following summary steps in **Figure 3.2.1.4-4** below:

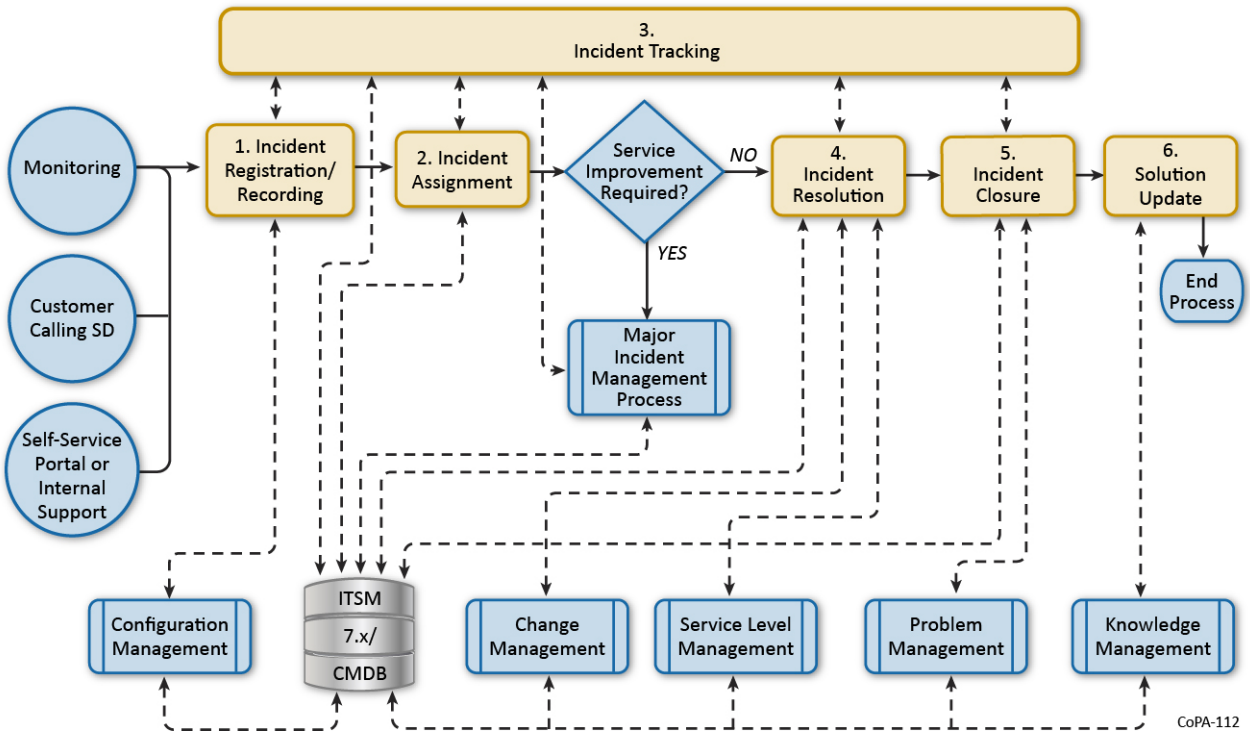


Figure 3.2.1.4-4 Incident Management Process

1. Incident Registration & Recording

Incident tickets can be detected and recorded several ways:

- The end user or Agency Service Desk will contact the Unisys Service Desk via telephone and the Unisys Service Desk will record the ITSM Incident Ticket
- The Unisys Event Management System will detect critical events that auto-generate an incident ticket into the Unisys ITSM Incident Ticket System

  or

- The Commonwealth's ITSM System will forward incident tickets to the Unisys ITSM Incident Ticket System

Classification & Initial Support

The service desk agent completes all required incident record data, validates stored information and gleans incident specific information from the end user. The unique incident record number is created and provided to the end user for reference purposes. While classifying the incident, the service desk agent will also classify the incident in regards to Impact, Urgency and Priority.

The Priority is defined by the expected effort. An incident with a low impact and average urgency that can be resolved with minor effort will be resolved immediately in most organizations (e.g. a password reset).

Severity	Definition
P1 – Critical	Severe Business Disruption
P2 – Major	Major Business Disruption
P3 – Medium	Minor Business Disruption
P4 – Low	Minor Disruption
P5 - Very Low	Inquiry

Initial support involves resolution of the incident to the satisfaction of the client by the service desk. The resolution may be derived from several areas, including:

- Identification of a known error
- Service Desk staff expertise
- A knowledge search.

Investigation & Diagnosis

Investigation and diagnosis is the process whereby the Level I Service Desk agent is able to resolve the incident to the satisfaction of the client without reference to any other support areas.

The service desk agent resolves incidents through the use of:

- Business specific processes and procedures documented within the client-specific knowledgebase
- Generic technical training, personal experience and technical knowledgebase information
- Remote access tools
- Mentor-type support from other Agent and Management resources within the service desk.

The Service Desk may be able to achieve this by matching the reported incident to a known error and providing details of the known resolution or workaround to the client. If a resolution is proposed by either source, then the known error database will be updated and full details of the resolution will be recorded against the incident record.

2. Incident Assignment

In cases where the initial Service Desk support team is unable to resolve the incident, the Service Desk agent will assign the incident in the ITSM System to a resolver group based on the incident classification. Depending on the type of incident, the resolver group may be a Level 1 or Level 2 Unisys Subject Matter Expert Architect or Client Engineer, or a Level 3 Commonwealth internal resolver or an external vendor. In all of these cases, the Service Desk retains ownership of tracking the incident against the escalation and response times and is

responsible for monitoring and tracking progress of the incident.

3. Incident Tracking

The Service Desk Incident Manager will track incident management queues to determine if an incident is approaching an SLA threshold or determine if it needs to be escalated to a functional resolver team or a vertical management team in order to resolve the incident.

4. Resolution & Recovery

The Service Desk or resolver group's focus is to restore the service to the client's satisfaction. When the service is restored the Service Desk Level I agent who owns the incident ticket will inform the ticket submitter and affected stakeholders that the service has been restored.

5. Incident Closure

The incident will be closed and the ITSM Incident Ticket updated when the workaround or resolution has been confirmed with the end user. If the incident is referred to a resolver group, it is the responsibility of the resolver group to close the incident in the Incident Management System upon successful resolution. Unisys will send email notifications to the end user to confirm that the incident is closed.

Service Desk Incident Managers monitor incidents placed in a resolved state and contact the initiator to confirm the resolution. This provides an independent check to verify that the initiator is happy with the support received and agrees that the incident has now been resolved.

18 Problem Management

18.A Problem Management - The Offeror's Problem Management Process must minimize the adverse effect on the business of Incidents and Problems caused by errors in the IT infrastructure, Applications, systems and supporting components, and proactively prevent the occurrence of Incidents and Problems by identifying and eliminating causes of failure.

The Unisys Problem Management Process, integrated with our Incident Management Process described above, will be utilized to minimize adverse business effects caused by IT infrastructure issues. A Problem Manager assigned to the engagement, as well as the back office Unisys Problem Management team, will take the lead on proactively working Problem identification and elimination.

18.B Offeror must describe its Problem Management Process and how it will be applied to the overall IT Service Management Program for the Commonwealth.

The Unisys Team will utilize the following Problem Management Process framework shown below to support Problem Management for the Contract. The Unisys Problem Management Process is comprised of the following summary steps in **Figure 3.2.1.4-5** below:

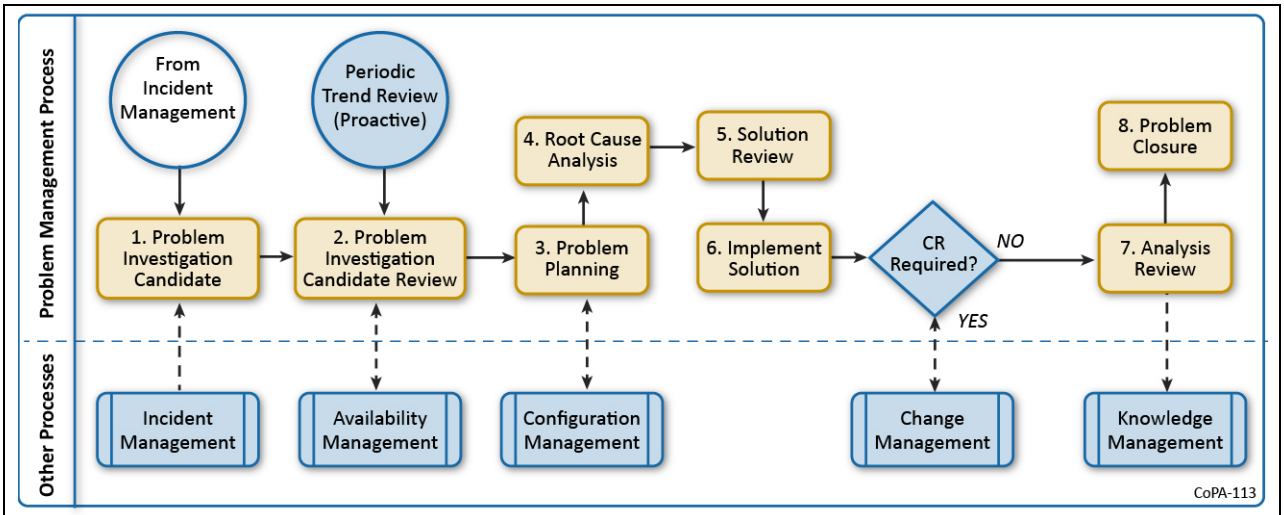


Figure 3.2.1.4-5: Problem Management Process

Unisys Problem Management Process

1. Problem Investigation Candidate

Unisys Problem Manager identifies a Problem from the following conditions:

- Multiple incidents that indicate an infrastructure problem. This is normally discovered by multiple end users reporting the same disruption
- A single incident recognized as a catastrophic problem that must be corrected immediately i.e. labeled as a major incident
- Proactive analysis of products and devices that indicates possible future system failure.

2. Problem Investigation Candidate Review

Unisys Problem Manager reviews a Problem validating the information to confirm it warrants investigation and either cancels the problem ticket or moves it to the next step of investigation, Problem Planning.

3. Problem Planning

Problem Planning is the procedure used by the Problem Manager/ Coordinator to plan the entire problem investigation including resources, timelines, kick-off meeting, creating and assigning problem root cause analysis tasks.

4. Root Cause Analysis

This stage involves investigation of the Problem by the relevant Level II or III Technical Teams and/or IV Third-Party Vendor. The primary aim of this procedure is to determine a work-around and to establish the root cause.

5. Solution Review

The Problem Manager reviews the recommended solution and approves or rejects the solution. The approval or rejection of the Solution provided is done in consultation with the SDM/Technical leads and the Commonwealth stakeholders. This procedure also involves the

creation and managing of Known Errors.

6. Solution Implementation
The Solution Implementation procedure is primarily used by the Level II/ III Resolver groups and Change implementers wherever a change is required to implement the suggested solution.

7. Analysis Review
The Problem Manager reviews the results and determines if the analysis is acceptable. This procedure also checks for the successful implementation of the proposed solution.

8. Problem Closure
The Problem Manager verifies the Problem has actually been solved. This procedure also includes managing the closure of Known Errors and impasse procedures where required.

Unisys Team Experience

Unisys has vast experience in providing Service Desk support services, with over 2800 resources handling over 8.5 million inbound events annually at our Managed Service Centers located worldwide. Over 3 million of these events are supported onshore in the U.S. by over 800 experienced resources. Gartner and Forrester have endorsed Unisys Service Desk Services in their most recent Analyst Reports.

- The Forrester Wave™: Global Workplace Services, Q1 2013 analysis has placed Unisys in the Strong Performer category of providers
- Gartner's 2012 Magic Quadrant for help desk outsourcing services lists Unisys in the 'Leaders and Visionaries' quadrant

Benefits to the Commonwealth

The Service Desk team will provide outstanding service to the Commonwealth users. For example, at our American Red Cross account, which transitioned to Unisys from another provider last year, Unisys has achieved the following results:

- In the data center, we are achieving 99.9% uptime at a 40% lower cost than with their previous provider.
- Service Desk wait time is down from more than 200 seconds to consistently below 30 seconds. Customer satisfaction rating is consistently above 4.2 out of 5.

For information regarding our value added services to American Red Cross refer to References Section 4.5.1.

3.2.1.5 Technical Architecture

The Technical Architecture function will oversee the ongoing design of the various computing platforms that will support the Commonwealth's existing computing topologies, as well as plan for the approaching consolidation of the Commonwealth datacenters. The intent is to design an infrastructure which will ultimately utilize multiple datacenters for processing, tiered DR Services, and on-demand Services in a secure environment. At the conclusion of the design, and after approval by the Commonwealth, the Offeror must document the environment via a Service Catalog.

Offeror must design the technical architecture of the computing systems based on current best practices, to support the evolving technologies and business needs of the Commonwealth. The volume of computing and storage will vary during the term of the contract due to applications development, testing, certification, the retirement of existing production environments, as well as cyclical processing demands such as the various tax seasons. The Offeror must be able to expand and contract service offerings based on Commonwealth needs in a timely and cost effective manner.

Reference Documentation

Exhibit A - Commonwealth Network Environment

Exhibit(s) B.1 through B.6 - Data PowerHouse (DPH) Exhibits

Exhibit(s) C.1 through C.13 - Department of Public Welfare (DPW) Exhibits

Exhibit(s) D.1 through D.15 - Enterprise Datacenter ([redacted] Exhibits

Exhibit(s) E.1 through E.43 - Department of Labor & Industry (DLI) Exhibits

Exhibit(s) F.1 through F.4 - Department of Health (DOH) Exhibits

Exhibit(s) G.1 through G.16 - PA State Police (PSP) Exhibits

Exhibit(s) H.1 through H.8 - Department of Revenue (DOR) Exhibits

Exhibit(s) I.1 through I.13 - Commonwealth SAP Environment - Integrated Enterprise Services (IES) Exhibits

Exhibit L - Master Application Inventory

Exhibit(s) M.1 through M.7 - Department of Corrections (DOC) and Pennsylvania Board of Probation and Parole (PBPP) Exhibits

Exhibit(s) N.1 through N.2 - PennDOT Exhibits

	Requirements	Describe Compliance
1.	Create a Service Catalog. Define the Services and platforms to be offered.	Offeror must describe the catalog of Services it proposes.

	Provide a detailed list of Services, via a common Service Catalog to be provided to the Commonwealth. Utilize an industry standard software product to ensure the detailed service offering is recorded.	Offeror must provide a sample of a Catalog of Services that includes both Services and platforms that it proposes.
2.	Design and build the IT architecture required to support the Services. Design and build the IT technical architecture to support the Services selected by the Commonwealth. Provide the design to the Commonwealth for review and approval prior to execution. All designs must be approved by the Commonwealth.	Offeror must describe its overall service design process.
3.	Design platform and support lifecycles. Provide a technical support staff structure for the Services and platforms to be offered. Support will consider all skills needed to plan, operate and support each technology platform.	Offeror must describe its proposed technical architecture team. Resumes for proposed key personnel must be provided as described in **Schedule G - Staffing Plan and Key Positions**.
4.	Define Technical Support Services. Provide the skills of and the size of the support staff to plan, manage, and operate the various IT infrastructure platforms.	Offeror must describe its proposed technical architecture team. . Resumes for proposed key personnel must be provided as described in **Schedule G - Staffing Plan and Key Positions**.
5.	Interoperability Strive to design architectures with system components that facilitate system data accessibility.	Offeror must describe its methodology and approach to designing technical architecture
Deliverables		
Deliverables are defined in **Schedule K – Key Program Deliverables**		
Offeror Response		

Introduction

The Unisys solution team presents considerable detail on the Enterprise Services Catalog and ITIL-based Service Design and functionality because these are the most critical elements in the design on any ITIL-based Managed Service solution. The ITIL V3-based Service Design includes not only the design of new services but also the changes and improvements to existing services through ITIL-defined processes.

The competitive advantage that Unisys offers the Commonwealth in this solution is deep expertise in using ITIL V3 based ITSM processes and Service Design processes to deliver higher productivity and costs savings for its customers.

The Unisys solution brings forward a staff of experienced technical architects who have provided service to Commonwealth agencies for decades. The Unisys Program Management Office provides the organizational structure by which the technical architects and the Senior Enterprise Infrastructure Architect meet regularly with Agency directors and business leaders. During these meetings the Unisys Enterprise Architecture staff seeks updates on near-term and long-term Agency strategic requirements. In addition, the Unisys PMO manages a regular schedule of Innovation Workshops led by Enterprise Architects who apprise Agency leaders of recent and forecasted technology innovations that may accelerate the Commonwealth's strategic interests.

1 Services Catalog

1.A Create a Services Catalog. Define the Services and platforms to be offered.

1.B Offeror must describe the catalog of Services it proposes.

The Unisys solution team brings forward an expanded more flexible ITSM Services Catalog that aligns to the Commonwealth's strategic initiatives. To further the Commonwealth's strategy to reduce costs, Unisys will implement an Enterprise Services Catalog based upon the Service Tiers, Hardware Configurations and Operating Systems found in Schedule I.

Utilizing this Enterprise Services Catalog, the Commonwealth can order incremental capacity across the hardware platforms within the enterprise. The Enterprise Services Catalog will allow the end user to first choose a high level service from the service family, a virtual or physical platform if applicable, then an operating system, followed by a server size. Lastly, the end user will choose a service tier where applicable.

The Enterprise Services Catalog is designed to be comprehensive and applied across the enterprise. For more information about the Unisys Enterprise Services Catalog, please review Section 3.4.4, Services Catalog.

1.C Provide a detailed list of Services, via a common Services Catalog to be provided to the Commonwealth. Utilize an industry standard software product to ensure the detailed service offering is recorded.

The Enterprise Services Catalog will be provided online through the Unisys Service Portal which is based upon PMG's Services Catalog platform. The Unisys governance process and

Unisys Service Design manage the detailed service offerings. The Commonwealth has access to the online Enterprise Services Catalog offering which provides an authoritative record of service offerings and the Commonwealth has access to the Unisys-maintained Change Management records of prior changes which can be used to summarize or evaluate the evolution of the Enterprise Services Catalog over time.

The Services Catalog (Schedule C) provides a detailed list of the services which will be provided to support the Commonwealth's requirements for Compute Services.

1.D Offeror must provide a sample of a Catalog of Services that includes both Services and platforms that it proposes

The Services Catalog (Schedule C) provides a list of the services which will be provided to the Commonwealth for both Services and platforms.

2 Service Design

The Unisys ITIL V3 based Service Design is managed at the Program Management Office level supported by the IT Services Management (ITSM) team to deliver the offerings available to the Commonwealth through the Service Portal as outlined in the upper three layers shown in **Figure 3.2.1.5-1**.

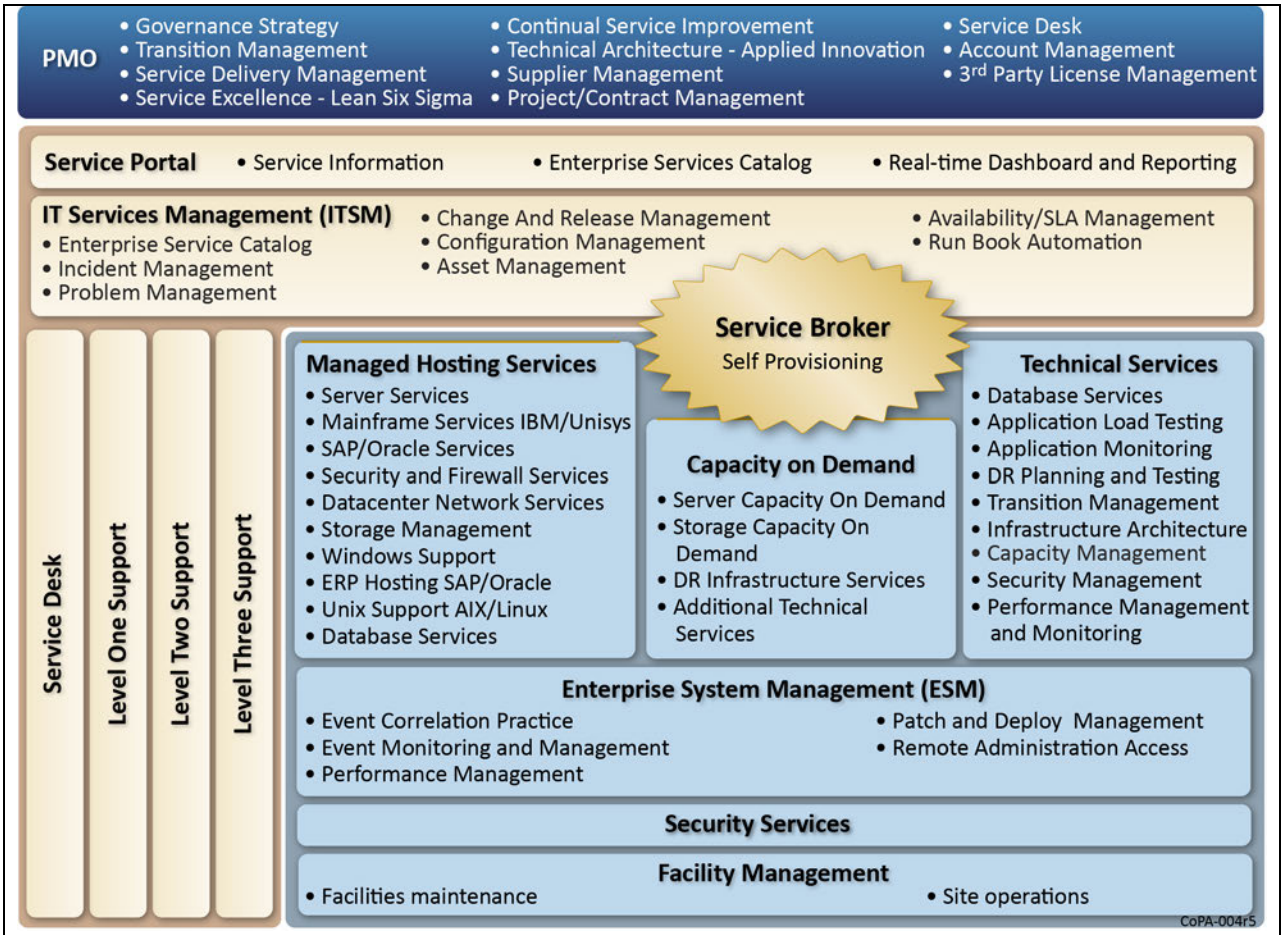


Figure 3.2.1.5-1 Component Based Operating Model

2.A Design and build the IT architecture required to support the Services

The Service Design includes the following ITIL V3 processes managed by the Unisys Program Management Office:

- Design Coordination: Coordinates service design activities within Unisys Governance so that Commonwealth agency input, requirements, and oversight are included.
- Services Catalog Management: Coordinate initial approvals for Services Catalog changes and the quality of the service descriptions and interdependencies.
- Service Level Management: Provides governance on changes to existing SLAs, when desired, and SLAs for new services.
- Risk Management: Provides Security and Continuity oversight for Services
- Capacity Management: The Unisys-provided and managed Capacity-on-Demand infrastructure
- Availability Management: the Unisys-provided management of metrics and improvements

for infrastructure availability

- IT Service Continuity Management: Provides Service Availability through DR and Continuity support to mitigate risks to services
- Information Security Management: Provides Service Confidentiality and Integrity to round out the Security Triad of Confidentiality, Integrity, and Availability.
- Compliance Management: Unisys management to the Commonwealth's Regulatory compliance
- Architecture Management: Unisys governance over technology life-cycles and innovations.
- Supplier Management: Unisys Program Office Management over the coordinated Unisys team

2.B Design and build the IT technical architecture to support the Services selected by the Commonwealth. Provide the design to the Commonwealth for review and approval prior to execution.

As shown in **Figure 3.2.1.5-1** above, the Unisys Program Management Office (PMO) provides the governance process around the design and build of the IT technical architecture. The Unisys PMO overlays commitments to Continual Service Improvement to deliver a much higher service value to the Commonwealth than that which another vendor would offer by simply following the proscribed process road maps.

2.C Offeror must describe its overall service design process.

The scope of Service Design is not limited to new services, but also includes the changes and improvements necessary to increase or maintain value to customers over the lifecycle of services, the continuity of services, achievement of service levels, and conformance to standards and regulations. It provides guidance on how to develop design infrastructure capabilities for Commonwealth applications and service management.

The primary goal of Service Design is to design IT services, together with the governing IT practices, processes and policies, to realize the Commonwealth's IT Service strategy and to facilitate the introduction of these services into the live environment ensuring quality service delivery, customer satisfaction and cost-effective service provision. Service Design for the Commonwealth/Agencies will be focused on Availability, Capacity and Service Level Management and is described in the following sections.

The Unisys Service Design process engages Commonwealth leadership through the PMO to set the design scope for Service Design changes. This initial review verifies that the Commonwealth can set priorities to Service Design changes that have the highest strategic or tactical value to the Commonwealth. The Commonwealth's approval is also required before Service Design changes can be introduced to the Enterprise Services Catalog and offered to Commonwealth Agencies.

3 Technical Architecture Team

3.A Provide a technical support staff structure for the Services and platforms to be offered. Support will consider all skills needed to plan, operate and support each technology platform.

Enterprise Architecture: The Enterprise Architecture function owns the development and management of the technology management program for the Data Center Services delivered. In collaboration with Commonwealth agencies, Agency Account Managers and the balance of the Unisys Team, this function provides leadership in the forecasting and outlook for new technologies and services to be added during the term of the program. This group provides guidance to IT operations in addition to performing planning, design, build, and transition support on all technical matters.

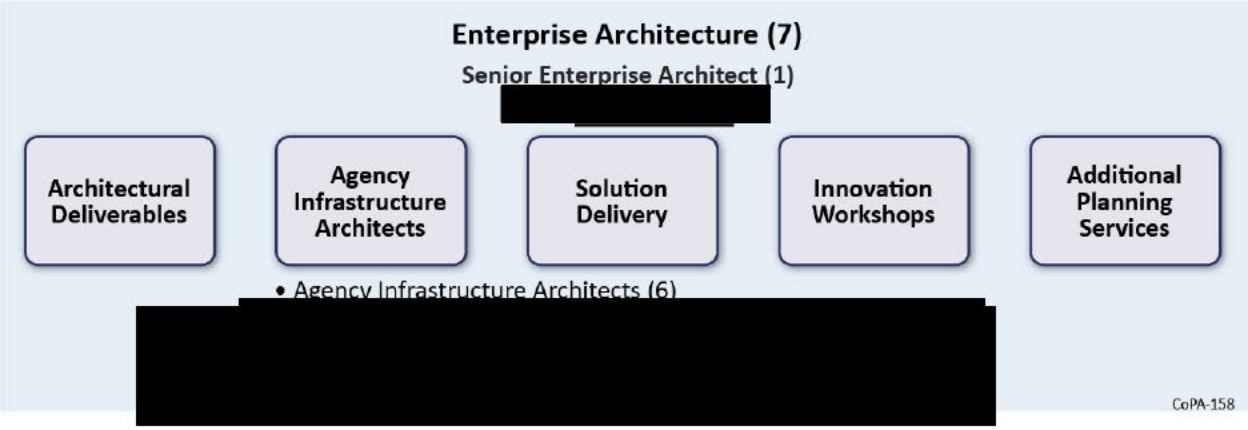


Figure 3.2.1.5-2: Enterprise Architecture – Functional Overview

The Architectural Deliverables function is responsible for the development and delivery of a number of key program deliverables including:

- **Data Center Architecture Plan and Roadmap** which includes the 2+ Data Center Architecture, the Data Center Network Architecture, and the Data Center Security Architecture.
- **Technology Architecture and Refresh Approach** which addresses Data Center Technology Refresh and Infrastructure Architecture strategy.

The Agency Infrastructure Architects are technology architects who bring a wide set of skills and experience that collectively cross all platforms and technologies supported under the Data Center Services contract. The architects, many with years in service to Commonwealth Agencies, are aligned to specific agencies and work hand-in-hand with the Agency Account Managers to verify that agency technology needs are fulfilled. They are responsible for the detailed design engineering of the Commonwealth's specific data center services design quotes and for coordinating Commonwealth related requests.

The Solution Delivery function is responsible for all aspects of the solution delivery including conducting the requirements definition process with the agency requesting service, development of a detailed technical solution, quantifying solution costs, and delivery of a viable proposal to the Commonwealth within established time frames.

The Innovation Workshops are essential to provide the opportunity for collaboration, technical information exchanges, and forums that will address issues, needs, and interests of the Commonwealth team. These innovation workshops are a key component of our overall Continuous Improvement Program.

The Additional Planning Services function provides the Commonwealth with different/additional methods for requesting technical information and support. Depending on the type of request those methods could include:

- Statement of Objectives (SOO)
- Work Order
- Service Request
- Request for Technical Analysis
  - Cost-Benefit Analysis
  - Conceptualization
  - High Level Estimate (HLE)
- Technical Opinion(s)

Unisys will establish and maintain an architecture office. The Senior Enterprise Architect, [redacted] will lead this office, and have six Agency Infrastructure Architects dedicated to him. The architecture office of the PMO will be responsible for the fulfillment of all architectural requirements contained within this RFP.

This team confirms the delivery of all required architecture related deliverables. They are fully accountable end-to-end for the solution delivery process. Enterprise Architecture works with the Commonwealth through Innovation Workshops to verify agency leadership is kept abreast of industry and technology trends. They are also required to provide additional planning services as needed by the Commonwealth to aid in their budgeting and technology planning processes.

The Senior Enterprise Architect is an Executive Level position that has the capability to reach into the sales organization, as well as the service delivery towers to draw additional architectural expertise as needed.

The Unisys Senior Enterprise Architect for the Commonwealth is a results-oriented leader with proven experience that has over 10 years of experience on accounts with increasing levels of complexity and responsibility. He has demonstrated the ability to handle increasing scope of responsibilities and to deliver deep and wide impact through innovative solutions to customer requirements for extremely large contracts.

The Agency Infrastructure Architects who staff this team are technology architects who bring a wide set of skills and experience that collectively cross all platforms and technologies supported under the Data Center Services contract. A number of our Agency Infrastructure Architects have been providing support to the Commonwealth for as many as 30 years. The architects are aligned to specific agencies and work hand-in-hand with the Agency Account Managers to confirm that agency technology needs are fulfilled. They are responsible for the detailed design engineering of the Commonwealth's specific data center services design quotes

and for coordinating Commonwealth related requests.

The Agency Infrastructure Architect will have primary technical solution responsibility and will verify the technical solution is state-of-the-art and fit for purpose. Primary responsibilities include:

- Ensuring that operational requirements of the Commonwealth are met by the technical solution deployed.
- Identification and planning of future technology updates.
- Data Center IT Design and Costing: Large scale architecture and implementation design. Design and application of best practices to optimize steady-state cost in pursuit of IT strategy and governance. Leadership role in adopting new technology to deliver cost savings and business goals.
- Technology and Architecture Strategies: Develop and Implement multi-generational strategic plans to restructure IT Infrastructure and implement a "best in class" application and data modeling framework. Leverage a variety of technologies and process to dramatically improve service while decreasing costs.
- Business Management: Full responsibility for developing business case support to underlie architecture change including milestone markers for cost savings during and following implementation
- Change management: Organizational transformation in support of successful IT implementations.

Unisys will develop solutions and provide architectures with a focus on quality to support the Commonwealth and its business needs. The architecture of the services provided by the Unisys team will be documented within the Key Deliverables D-01 (Datacenter Architecture Plan and Roadmap), D-03 (Technology Architecture and Refresh Approach), and D-04 (IT Service Continuity Architecture and Plan). Each of these documents will be reviewed within the Solution and Architecture Review Boards as part of Transition and when architecture changes are developed. To maintain the consistency and quality of the Commonwealth's requested services, each solution will be developed using a common set of activities which cover the solution development lifecycle up to the Agency's approval. This lifecycle includes the following activities.

i. Receive Request

ii. Gather Requirements

iii. Review and receive Commonwealth approval for requirements

iv. Review current services against requirements

v. Develop solution

vi. Review and approve solution within Unisys Solution and Architecture Review Board. The Unisys Solution and Architecture Review Board will be comprised of the Senior Enterprise Infrastructure Architect, Agency Infrastructure Architects, Chief Information Security Officer and technical support leads.

Review and approve solution with Commonwealth Solution and Architecture Review Board. The Commonwealth Solution and Architecture Review Board should be comprised

of the Unisys Enterprise Architect team, Unisys technical support leads (as needed), Commonwealth IT Governance participants, and Agency representatives (as needed).

See Figure 3.2.1.5-3 below.

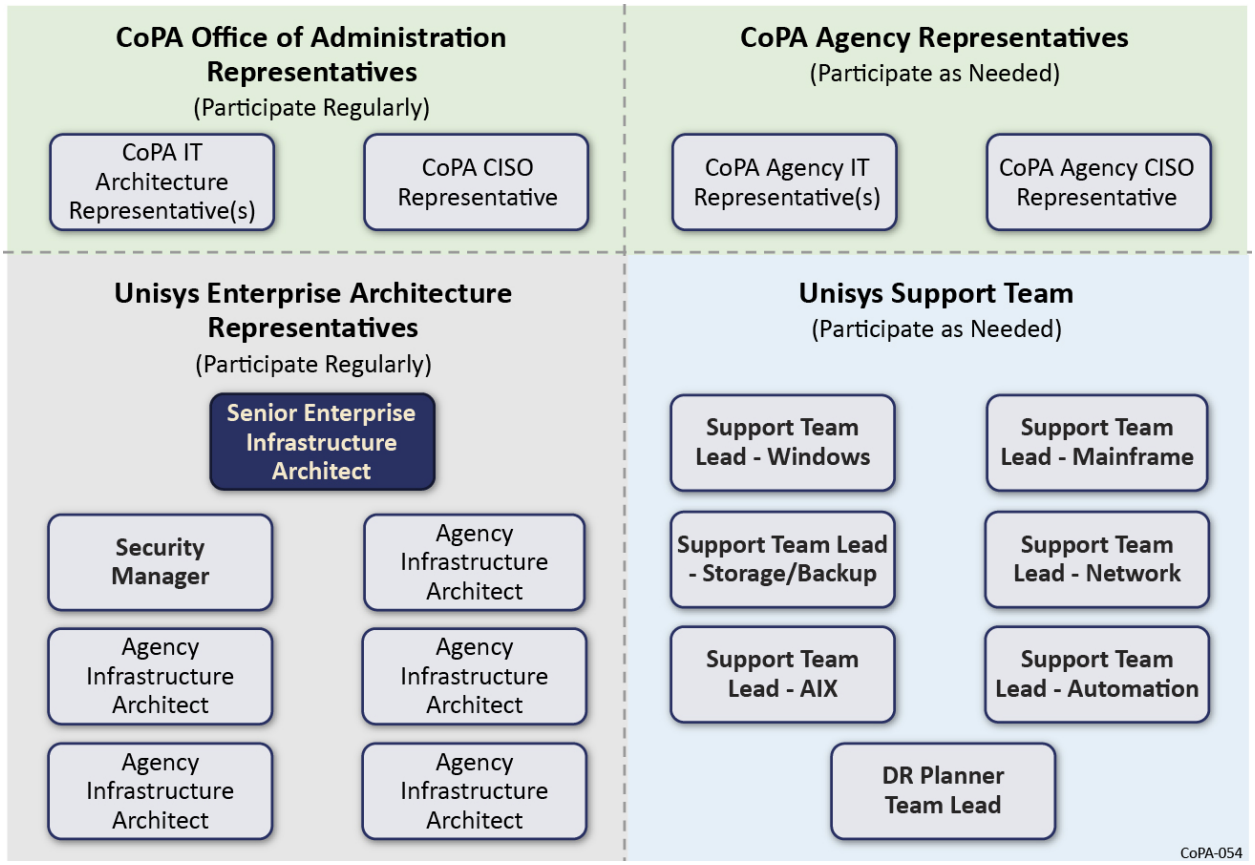


Figure 3.2.1.5-3: Enterprise Architecture – Representatives

vii. Review and approve solution with Commonwealth Agency requestors

viii. Transfer to Project Implementation team.

Design platform and support lifecycles.

As the Commonwealth's environment supports a diverse set of business activities and applications, the architecture team is composed of multi-discipline infrastructure architects. The architects will be organized to support the Commonwealth and the Program Management Office. The Agency Infrastructure architects will report to the Senior Enterprise Infrastructure Architect.

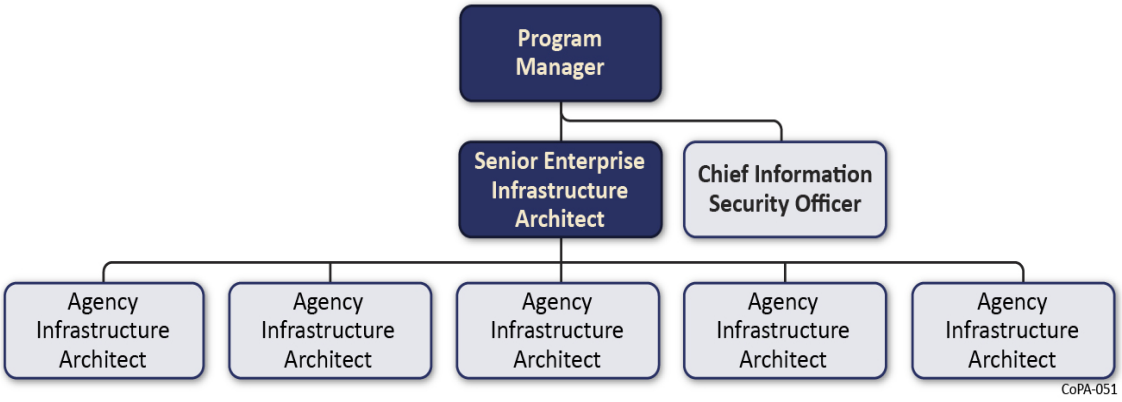


Figure 3.2.1.5-4: The Enterprise Architect team along with the CISO will develop solutions.

Based on an Agency's service request activity and types of infrastructure technologies used, an Agency will be assigned to an Agency Infrastructure Architect. The Agency Infrastructure Architect will work with the Agency Account Manager to understand an Agency's overall business needs, identify requirements, and define solutions to support the Agency's requests. Please see **Figure 3.2.1.5-5** below.

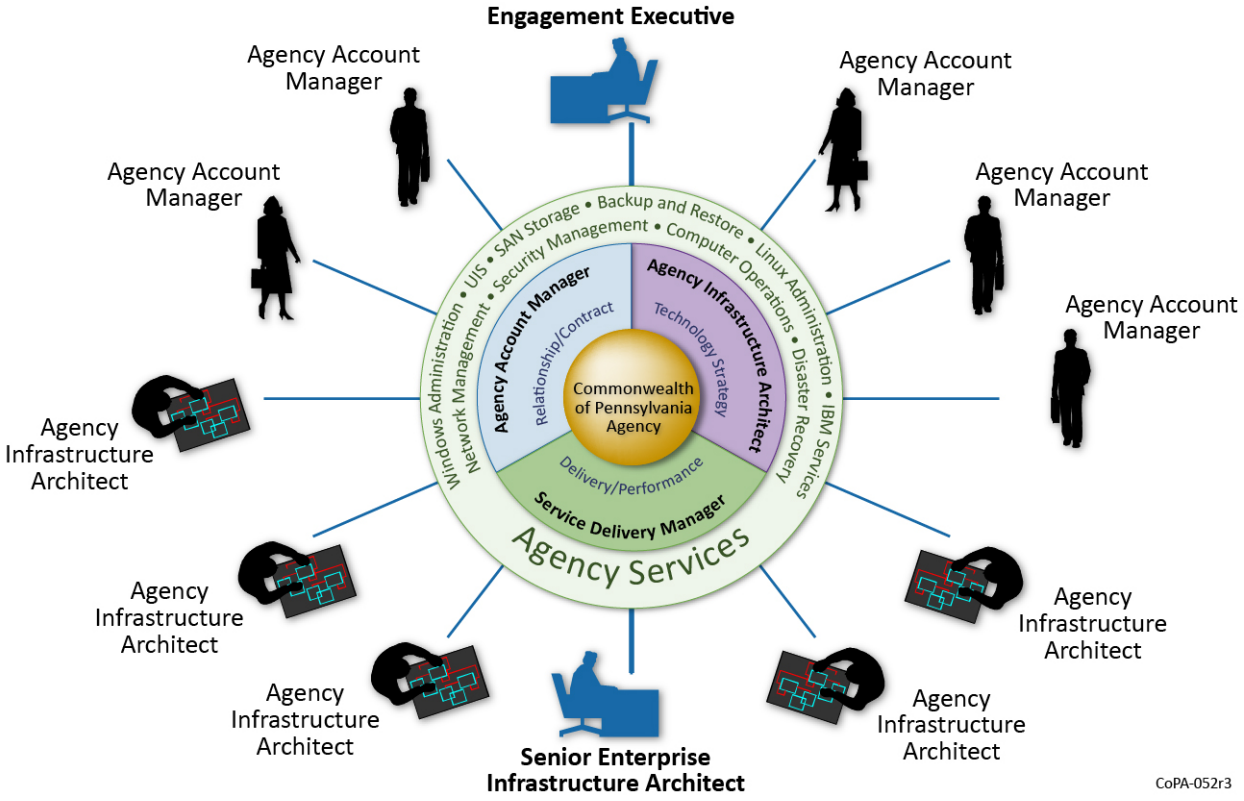


Figure 3.2.1.5-5: The Enterprise Architect team will work with the Agency Account Managers to understand the business needs and develop solutions for the Commonwealth.

3.B Offeror must describe its proposed technical architecture team. Resumes for proposed key personnel must be provided as described in Schedule G - Staffing Plan and Key Positions.

As the Commonwealth's environment supports a diverse set of business activities and applications, the architecture team is composed of multi-discipline infrastructure architects. The architects will be organized to support the Commonwealth and the Program Management Office. The Agency Infrastructure architects will report to the Senior Enterprise Infrastructure Architect. See **Figure 3.2.1.5-6.**

Resumes of named key personnel and representative resumes for personnel providing Technical Architecture Services are located in the tab marked Rep-Resumes in section 5.0 Personnel.

4 Technical Support Services

4.A Provide the skills of and the size of the support staff to plan, manage, and operate the various IT infrastructure platforms.

The Technical Architecture team is engaged to support the planning for various IT infrastructure platforms as part of the Service Design process described above.

Following ITIL V3 process guidelines the Technical Support Services are provided by a blend of cross-functional and tower-specific experts divided between Level 1, Level 2, and Level 3 support tiers. A detailed description for this staff as well as the escalation procedures to support and managed operations across various IT infrastructure platforms is located in Schedule F, Section 3.2.3.2.

4.B Offeror must describe its proposed technical architecture team. . Resumes for proposed key personnel must be provided as described in Schedule G - Staffing Plan and Key Positions.

In support of the Commonwealth's Compute Services, the Unisys team provides a diverse set of skills and resources. A table of these resources and skills along with resumes for key personnel and representative resumes is located in section 5.0 Personnel.

5 Interoperability

5.A Strive to design architectures with system components that facilitate system data accessibility.

Unisys had two governing principles in the design of the Commonwealth: first, standardization of the compute environment, as much as possible, in each of the hardware towers, and second, to technology that can be redeployed rapidly to other purposes. Unisys believe that from a server perspective, this is the easiest way to achieve the Commonwealth's goal of interoperability.

In particular these tower architectures have specific adaptations to increase interoperability and facilitate system data accessibility:

- ITSM Services Catalog
- Database and ERP
- Server

- Network
- Storage

IT Service Management Interoperability

The ITSM design that is detailed in Schedule F, Section 3.1.3 Data Center Architecture is designed to support service management of services and applications across diverse environments and architectures to support a service management focus. With a focus on Service Management the Commonwealth can implement business and applications services on interoperable technical platforms and manage the business and application technical services from a single ITSM platform.

Database and ERP Interoperability

As the core part of many applications, the database service was designed with flexibility and interoperability in mind. As part of the solution development activities, the Unisys team will work within the Commonwealth to design each database implementation to meet the requirements for the application including interoperability with other applications.

The database services are much more agile and cost-effective due to the underlying Enterprise Services Catalog that provides the computer infrastructure services of compute power, network, storage, and data protection through a variety of tiered options. The Commonwealth will be able to manage the flexibility of the services by running databases at higher utilizations rates with the security that additional resources can be purchased when needed and released when no longer needed.

Based on the current implementations of the Commonwealth's SAP and Oracle ERP systems, ERP interoperability is a major component of this implementation. By applying the governing design principles and using standardized infrastructure architectures as indicated above, the Commonwealth's ERP systems will have a flexible and interoperable environment. More specifically the Commonwealth's application architects can make use of the proposed, and evolving, Services Catalog to select appropriate utility resources to support the changing needs for the SAP and Oracle Test, Development, Q/A and Production environments. These application architects can use the Enterprise Services Catalog to order just-in-time infrastructure to test new application features. This relieves the application team of the need to justify significant up-front-spends to purchase infrastructure with long term commitments. Instead the application teams can establish lower-costs proof-of-concepts projects to prove-out the benefits of new application features. This will allow application architectures to be much more nimble in marrying new application features to tangible benefits to the Commonwealth with virtually no long-term investment in infrastructure. In addition to the flexibility provided by the Enterprise Services Catalog's just-in-time infrastructure application architects can scheduled longer duration tests in the permanent Test Environment specified in the Commonwealth's RFP and provided by the Unisys team solution.

Server Interoperability

By utilizing IBM Flex Blades within IBM Flex Chassis, the Commonwealth will be able to deploy physical and virtual workloads, on both AIX and Windows, within the same physical chassis.

This will allow the Commonwealth to quickly and efficiently re-align the compute infrastructure to meet all existing and future regulatory framework requirement where any type of physical isolation is required.

Network Interoperability

By co-locating AIX and Wintel (Windows and Linux) application workloads in the same chassis, network latency can be drastically reduced, and application management efficiencies recognized. By providing these capabilities, Unisys has created a unique solution that the Commonwealth's services can leverage for future application needs as well as regulatory framework requirements.

To further address application latency concerns that can reduce interoperability between applications, point-to-point high speed (10Gb) fiber links will be deployed between the data centers. Based on the fact that it takes approximately 1 millisecond (ms) for light to travel 100 miles, we are estimating that latency between any 2 of the 3 data centers should be less than 5ms. The reason the latency it is not less than 5ms is because additional latency (i.e., non-distance related) is added by the physical telecommunication equipment at either end of the circuit. Point-to-point circuits offer the lowest latency (versus network "cloud" or "star" topologies), as the distance the light needs to travel is the shortest.

Storage Interoperability

To meet the Commonwealth's goals of a flexible and cost-effective Utility model Unisys has relied on standard, market-leading Open Systems and Mainframe storage and backup vendors who have always designed and marketed their products with high flexibility to meet interoperability requirements.

Unisys has, in all cases, sought competitive pricing from at least 2 market-leading vendors for the components necessary to deliver the services sought by the Commonwealth. These market-leaders maintain, as part of their competitive advantage over niche-players, extremely comprehensive lists of servers, applications, appliances, and even network interconnect devices such as Host Bus Adapters (HBAs) in servers for storage connections and high-throughput IP-based ports in distribution layer switches.

Other vendors might bring forward niche-based solutions that offer a great many product models each designed to provide lowest costs for particular service segments. Unfortunately this approach too often locks a customer into long-term vendor locks as data volumes grow and it becomes costly to migrate data from the original niche product to the cheaper niche product that later displaces it.

Unisys has taken very seriously the Commonwealth's desire to take a 10-year focus on the delivery of storage and backup services and narrowed its vendor selection to these market leaders: EMC, IBM, Oracle/Sun backup systems and CommVault. Our partners have long-term product strategies that preserve the value of the current products provided in the Unisys proposal and have provided roadmaps for the refresh of these product lines in 5-years.

Unisys will conduct regular architecture review meetings with Commonwealth stakeholders to review the benefit that new technologies may bring to lower costs and increase service quality and flexibility for Commonwealth services. The Unisys solution team has favored current market-leading technology providers in the selection of infrastructure hardware, software, and

tools because these platforms provide the most interoperability across vendors in upstream or downstream technology layers. Thus as the server or network virtualization layers transform Unisys will be able to present opportunities to begin refreshing into these technologies or adding them as additional capacity is needed. This can be done without, for instance, requiring a replacement of the existing storage infrastructures which will continue to be interoperable across all new vendors and new server and network technologies.

5.B Offeror must describe its methodology and approach to designing technical architecture

Through the Service Design process described above, Unisys develops solutions and provides technical architectures with a focus on quality to support the Commonwealth and its business needs. The architecture of the services provided by the Unisys team will be documented within the Key Deliverables D-01 (Datacenter Architecture Plan and Roadmap), D-03 (Technology Architecture and Refresh Approach), and D-04 (IT Service Continuity Architecture and Plan). Each of these documents will be reviewed within the Solution and Architecture Review Boards as part of Transition and when architecture changes are developed. To maintain the consistency and quality of the Commonwealth's requested services, each solution will be developed using a common set of activities which cover the solution development lifecycle up to the Agency's approval. This lifecycle includes the following activities.

- Receive Request
- Gather Requirements
- Review and receive Commonwealth approval for requirements
- Review current services against requirements
- Develop solution
- Review and approve solution within Unisys Solution and Architecture Review Board. The Unisys Solution and Architecture Review Board will be comprised of the Senior Enterprise Infrastructure Architect, Agency Infrastructure Architects, Chief Information Security Officer and technical support leads as illustrated in the Unisys Enterprise Architecture Representatives in Question 3 above in **Figure 3.2.1.5-3.**
- Review and approve solution with Commonwealth Solution and Architecture Review Board. The Commonwealth Solution and Architecture Review Board should be comprised of the Unisys Enterprise Architect team, Unisys technical support leads (as needed), Commonwealth IT Governance participants, and Agency representatives (as needed).
- Review and approve solution with Commonwealth Agency requestors
- Transfer to Project Implementation team.

Unisys Team Experience:

Since 1999, the Unisys team has provided a variety of services to support the applications hosted in the Data Power House. As the Commonwealth's business needs have changed and grown, the Unisys Service Design team has worked with the Commonwealth to identify new technologies and services:

- **Shared Storage.** By introducing shared storage for agencies, the Commonwealth has

benefited from a cost effective solution to support the continuing growth in data.

- **Virtualization.** The use of [redacted] products has enabled to Commonwealth to reduce the hardware footprint while also supporting the continued increase in server capacity and flexibility.
- **Disk Based Backups.** The introduction of EMC's Data Domain disk backup technologies has provided flexibility in backing up the active data on many platforms including the IES SAP and DOR ITS platforms as well as a cost effective data replication option to support Disaster Recovery activities.

The Unisys Team dedicated to the Commonwealth has ready access to the Unisys Portfolio team which has developed the mature Unisys Service Design practices to evolve technical architectures for a broad based of Unisys customers.

The Australian National Audit Office Control (ANAO) (an equivalent office to the Federal GSA) asked Unisys to implement ITSM Services Catalog delivery. As a result of this request, Unisys provided these benefits:

- Incident Response Time improved from 80 to 98%
- Incident Resolution Time improved from 85 to 94%
- Incidents Logged reduced 30%, measured monthly
- Problem Resolution Time reduced from average of 28 to eight days
- Network Availability monthly average increased from 99.7% to 99.99%
- Business System Availability monthly average increased from 99.7% to 99.999%
- Improved Client Account Satisfaction Levels increased from 8 to 9.03 (scale to 10)
- Client User Satisfaction improved from 4.5 to 5.95 (scale to 7; optimal band 4.5 to 5)

Unisys was given the global TPI Sourcing Industry Award for Service Provider Excellence as a result of the ANAO improvements. These improvements also provided a 10% reduction in baseline costs that exceeded ANAO's expectations.

Benefits to the Commonwealth

The Unisys Team and the Commonwealth have, over the years, built a solid Service Design governance process that is flexible enough to expand to encompass all of the Commonwealth agencies. No other vendor brings this advantage of a proven, scalable Service Design infrastructure.

The proposed Service Design process is now overlaid with a specific Program Management Office responsibility to deliver Continual Service Improvement as part of the ITIL V3 based processes. Other vendors adopt ITIL V3 processes, Unisys improves on them in order to meet the Commonwealth's strategy of seeking continual cost reductions as part of the life cycle for services.

The Unisys Enterprise Services Catalog reduces transition costs by anticipating requirements that individual Agency applications will present. The Unisys Enterprise Services Catalog is architected to the specified RFP requirements but also anticipates services currently provided to DPH applications. The Unisys Team brings forward 12 years of experience that empowers

the Unisys to design a solution to optimize application stability and security of Commonwealth applications.

The Unisys Service Design process reduces transition costs by adapting rather than replacing existing Unisys/Commonwealth governance processes for Service Design. Other vendors will spend considerable time first learning and second integrating into the Commonwealth's OA and Agency structures and gaps in this initial effort will only be discovered during time-critical migrations when service offerings may need to be adjusted. By contrast adjustments to service design or offerings are already a regular review item within Unisys/Commonwealth governance meetings.

The Unisys Service Design process reduces transformation costs because the Enterprise Architecture team brings forward a founder's expertise on current Commonwealth architectures. Other vendors will approach transition and transformation as if the existing infrastructure poses threats of uncertainty and complexity. They will increase risks and costs during transition by proceeding with what they deem to be the minimum level of understanding required to move the Commonwealth to their new gear and remove the "uncertainty threat" as quickly as possible.

3.2.1.5.1 Technology Refresh

Technology refresh will be an ongoing activity required of the Offeror. The Offeror will prepare technology impact statements that address the key technologies planned for refresh or technologies identified to be of interest to the Commonwealth. These impact statements will provide a wide range of information, including the following matters applicable to the Offeror's environment:

- Technology trends
- IT Infrastructure Offeror releases and offerings
- IT Infrastructure Offeror retirement of older versions of products
- Proposed scheduling of Offeror releases into the datacenter environment
- Potential impact of the new releases on business applications in the datacenter infrastructure
- Potential impact of the new releases on deployment and operational processes
- Risk analyses with recommendations for mitigation of risks

The Commonwealth and the Offeror will review the impact statements. Based on these reviews, the Offeror must recommend a plan and schedule for technology refresh to the Commonwealth. Since the expected usable life of any hardware approved for the datacenter environment is about 36 months, the plan shall project an 18-month window into the future, and include resource estimates for each recommended refresh activity. Software refresh will depend on software releases and the Offeror must ensure operational compatibility with existing Commonwealth applications and/or functionality or must provide upgrade alternatives and options. The Offeror must obtain Commonwealth approvals prior to implementing technology upgrades that will affect Commonwealth operations.

Reference Documentation

N/A

	Requirements	Describe Compliance
1.	Update Technical Architecture approach and project plan including; Services Catalog, IT Architecture, and Technical support	Offeror must document its Technical Architecture approach and project plan including; Services Catalog, IT Architecture, and Technical support
2.	Technology refresh approach - describe methodology for reviewing and refreshing technology on a scheduled basis.	Offeror must describe its methodology for reviewing and refreshing technology on a scheduled basis.

3.	Technical Architecture Staffing	Offeror must identify its technical architecture organization and staff.

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

Introduction

As a recurring activity of the services and infrastructure lifecycle, Unisys will include a Technology Refresh planning program to support the Commonwealth's environment and operations. The Commonwealth benefits from the recurring plan and refresh activity as it provides replacement of individual installations and technologies and maintains the Commonwealth's applications and business functions. As part of the Technology Refresh program, Unisys will provide an impact statement during the planning activities. The impact statements will include:

1) Technology Trends

   a. Technology and service trends will be evaluated and monitored. As the Commonwealth's Business requirements change, the industry trends will be evaluated to map Commonwealth's identified requirements to new capabilities and technologies.

   b. As trends and new technologies are identified to provide improvements or meet requirements which cannot be met with the existing services, new services or changes to existing services will be recommended and developed with the Commonwealth's approval.

2) IT Infrastructure Offeror Releases and Offerings

   a. Working with the Commonwealth, the architect team will identify and recommend new offerings available from the team's portfolios to support the Commonwealth's ongoing business needs.

   b. As offerings and services are retired or upgraded, the architecture team will provide recommendations to support the updates or removals of services based upon the Commonwealth's business needs and requirements.

3) Proposed Release Schedule

   a. Schedules for introducing new technologies and services will be provided as part of the approval process. The release schedule will include testing and validation as well as the proposed roll out plan for new or upgraded services.

4) Impact of New Releases

   a. As new service or technology releases are defined and recommended, the impact to the Commonwealth's business application environment will be identified with the risks and associated mitigation recommendations.

   b. New technologies and services can require changes to the deployment and operational processes. Process changes will be evaluated to identify the impact and

the risk. The impact evaluation will include mitigation recommendations.

The impact statements will be included in the technology selection activities to add new technologies and services within the Commonwealth's environment. Not all new technologies and services will be used in the support of the ongoing Technology Refresh. Some of the new technologies and services will be made available as a separate option when it does not support current technology refresh requirements.

The Commonwealth Technology Refresh Plan will include the following activities and reviews. New requirements from the Commonwealth will not be directly supported within the Refresh Plan. A service request will be submitted for any Commonwealth environment which is expected to have a technology refresh, but has new requirements beyond the services or technology currently in place. By using the service request process, the new requirements can be defined and used to determine the overall solution required while also including the technology refresh.

1) Identification of the active hardware and software components which should be replaced within 18 months of the technology refresh planning period. Technical Iinfrastructure will be recommended based upon the replacement cycle defined for each technology. For Unisys Fully Managed Services supplied and supported components, the replacement cycle will be 60 months. Unisys supported Software will be reviewed and recommendations provided based upon the available product releases.

2) Review of the technology refresh recommendations with the Commonwealth to validate and approve components to be refreshed. The review will include the options for individual components to be used in the technology refresh, recommended refresh groups, and an initial estimate of resource activity.

3) Upon approval of selected components, Unisys will develop a technology refresh project plan which includes the activities to migrate the Commonwealth's applications, data, and services to the replacement technologies.

   a. To maintain alignment with solution delivery processes, a service request for the technology refresh project will be opened and the project activities tracked within the Service Request tool.

   b. If the Commonwealth rejects or requests a delay of a component refresh, an impact review and recommendation for changes to the Commonwealth's application assigned service levels will be developed and provided in substitution of technology refresh project plan. The Commonwealth must provide the final approval of the changes to the service levels for applications, technology or services which will not be refreshed.

   c. The Commonwealth must approve the project plan before the technology refresh project will begin.

1 Technical Architecture Approach

1.A Offeror must document its Technical Architecture approach and project plan including; Services Catalog, IT Architecture, and Technical support

1) Technical Architecture Approach

In support of the Commonwealth's service environment, an enterprise infrastructure

architecture practice will be established to manage and support Unisys technical design and capabilities implemented. The services will be defined within the Enterprise Services Catalog. As new services and technologies are approved for implementation, the Enterprise Services Catalog will be updated with new services and unit pricing. The Unisys Team provides skilled resources which are experienced and regularly trained on the products which support the services.

The architecture supporting the services and Commonwealth environment will be documented and updated within the following Key Deliverables. The initial copy of these deliverables will be published based upon the target dates defined within the Transition Plan located in Schedule M within section 3.0 Work Plan. The target dates for the key deliverables to meet the Schedule K (Key Deliverables) and Schedule M (Transition Plan) milestones.

1) D-01 Datacenter Architecture Plan and Roadmap

2) D-03 Technology Architecture and Refresh Approach

3) D-04 IT Service Continuity Architecture and Plan

The Technical Architecture team will also be supported by the Security Manager and infrastructure system support team leads during the development of solutions. To maintain the quality of the solutions and the technology refresh plan, the Security Manager and team leads will also participate as part of the Unisys Architecture and solution review team as voting members. Upon approval within the Unisys architecture and solution review team, the solutions and technology refresh plans will be presented to the Commonwealth for review and approval.

Solutions development, architecture changes, and technology refresh will follow a common process.

a. Service Request or recurring cycle

b. Requirements gathering

c. Requirements approval by agency (Service Requests only)

d. Solution Development

e. Internal solution and architecture review and approval

f. Commonwealth review and approval

g. Transfer to a solution fulfillment activity

2 Technical Architecture Refresh, scheduled

2.A Offeror must describe its methodology for reviewing and refreshing technology on a scheduled basis.

2) Technology Refresh Methodology

As part of the overall architecture support, the Commonwealth's environment will be reviewed on a quarterly basis to identify technology, services or components which require

replacement to maintain the Commonwealth's business needs and associated service levels. The review will include the following activities.

1) Using the data within the Asset Management and Configuration Management databases, identify the technical components within the Fully Managed, Managed Only, and Capacity on Demand environment which require replacement within the next 18 month period based upon the a 60 month replacement cycle.
2) Review End of Sales and Service Life notices from the Manufacturers to validate if a component has been discontinued or has available ongoing maintenance options.
3) Review ongoing Capacity and Performance reports to identify any components with a refresh requirement which have additional needs driving a requirement or opportunity to change the component's classification to a different component to maintain the functionality and service levels.
4) Identify replacement technical components based upon the current Enterprise Services Catalog offerings.
5) Validate replacement technical components meet the current requirements for the impacted Commonwealth applications.
6) Identify risk and impact for the Commonwealth environment to replace existing technical components or services.
7) Create technology refresh recommendations, impact and high level implementation plan.
8) Present the technology refresh plan to the Commonwealth using the Solution Architecture review process.
9) Upon approval the refresh plan, open service requests for each migration group and develop the detailed project plan for the migration plans.

3 Staff, Technical Architecture

3.A Offeror must identify its technical architecture organization and staff.

1) Technical Architecture Staffing

The Enterprise Architecture organization (**Figure**) owns the development and management of the technology management program for the Data Center Services delivered. Unisys will establish and maintain this architecture office led by our Senior Enterprise Infrastructure Architect, [redacted]), who reports to [redacted]. Reporting to [redacted] will be six dedicated Agency Infrastructure Architects. This organization has direct responsibility for the fulfillment of all architectural requirements of the program. The functions that fall under Enterprise Architecture include meeting Architectural Deliverables, Agency Infrastructure Architecture, Solution Delivery, Innovation Workshops, and Additional Planning Services.

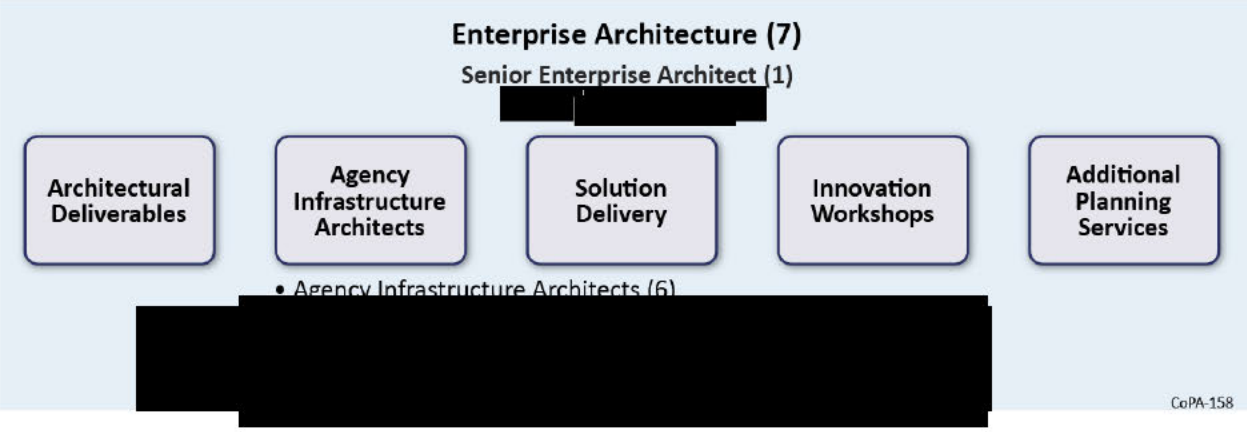


Figure 3.2.1.5.1-1. Enterprise Architecture Organization

This team is responsible for meeting **Architectural Deliverables,** including:

- **Data Center Architecture Plan and Roadmap,** which includes the 2+ Data Center Architecture, the Data Center Network Architecture, and the Data Center Security Architecture
- **Technology Architecture and Refresh Approach,** which addresses Data Center Technology Refresh and Infrastructure Architecture strategy.

Agency Infrastructure Architecture is comprised of technology architects who bring a wide set of skills and experience that collectively cross all platforms and technologies supported under the Data Center Compute Services contract. Several of our Agency Infrastructure Architects—including [redacted] have provided support to the Commonwealth for as long as 30 years. The architects are aligned with specific agencies and work hand in hand with the Agency Account Managers to enable agency technology needs to be fulfilled. They are responsible for the detailed design engineering of the Commonwealth's specific data center services, design quotes, and coordination of Commonwealth-related requests.

The technical architecture staff is described in Section F.3.2.1.5 Requirement 3. Each of the architects is introduced in more detail in Section 5.0 Personnel.

Unisys Team Experience

1) Commonwealth Data PowerHouse
   a. 2008 Renewal and Transition
      i. With the contract extension of 2008, Unisys executed a complex and comprehensive transformation throughout the entire Data PowerHouse. This transformation consisted of a vast technology refresh spanning all supported platforms and agencies with a new architecture approach. Previous to transformation, each agency application infrastructure platform was segregated from the others with its own separate system frames, storage units, tape silo, SAN and network switches. Unisys transformed the Commonwealth mission

critical applications from distinctly separate and siloed environments to an enterprise architecture consisting of highly redundant shared infrastructure components that could be leveraged by many agencies.

ii. The Transformation project spanned from July of 2008 through September of 2009, completing 3 months ahead of schedule. This project consisted of:

1. Introduction of [redacted] virtualized Windows environment including the virtualization of hundreds of servers,
2. Unisys mainframe environments were refreshed for [redacted] and the [redacted] providing more capacity, faster processors, the capability for metered [redacted] for [redacted] and the introduction of the [redacted] environment for the [redacted].
3. [redacted] mainframe customers were consolidated from [redacted] onto a [redacted]. This platform introduced the Integrated Facility for Linux used to host approximately 100 servers for [redacted] With this technology, [redacted] were able to take advantage Workload Capacity features that enable agencies to have access to additional idle processing capacity as long as they're meant allocation was not exceeded on a rolling four-hour average. The proactive implementation of this feature enabled the Commonwealth to avoid the need to procure additional MIPS for heavy processing time frames.
4. Several physical servers were upgraded and refreshed.
5. Consolidation of numerous workgroup network switches into a [redacted] core switching platform,
6. Reduction of more than [redacted] mass storage units to [redacted] units,
7. Implementation of disk-based backup on mainframe platforms,
8. Consolidation of numerous small tape silos into two large capacity tape silos shared by the entire enterprise,
9. Consolidation of agency SAN switching islands to an enterprise class core SAN switching infrastructure shared by all agencies.

iii. The process followed to execute the transformation included [redacted] Solution architects determined the most effective infrastructure to be used in the solution and how each agency could take advantage of the best features of the new architecture. Meetings were held to brief the agencies about technology changes, the benefits, and what to expect during the transformation project. An overall Transformation Executive managed the program working through project managers on the Harrisburg team with extensive experience supporting the Commonwealth for years. Program changes were implemented focusing on no more than two technology changes at a time. Workload and changes were distributed across the 15 month duration of the project. This enabled the Data PowerHouse team to tightly control change to the environment, and monitor the effectiveness of the change before proceeding to the next change. The approach was very successful resulting in most cases no impact to the majority of agencies.

iv. Consolidation of technologies, implementation of virtualization, and the

introduction of enterprise class devices resulted in millions of dollars of savings to the Commonwealth over the 5-1/2 year term. This transformation also provided smaller agencies with the opportunity to utilize enterprise class equipment that is highly available with inherent redundancy that they could not previously afford in a standalone environment.

2) Annual Technology Refresh

The Data PowerHouse monitors end of service life (EOSL) on devices so that technology refreshes can be funded and planned for in order to keep system availability high. All asset lifecycle dates are tracked in a database and verified during the maintenance contract renewal process. The capacity planning process is used to showcase devices which have or will reach EOSL in the near future. Asset selection for inclusion in the capacity planning process is done by identifying assets with a vendor published EOSL date.

When technology refreshes are necessary to provide high levels of system availability, the RFS process is used to document requirements and the appropriate solution to replace the devices which have reached end of service life. A solution is presented to the Commonwealth for consideration and if a change order is signed then implementation activity begins. The RFS process provides opportunity for continuous discussion on the requirements and possible solution options. If the Commonwealth makes the decision to fund the refresh then the solution will include support for implementation, testing, and cutover. This approach allows the transition to be well planned and executed to a schedule than support Commonwealth's business requirements.

The technology refreshes have primarily been focused on Unisys branded Dell hardware starting in 2012 as the environment was refreshed in 2008. This approach was primarily driven by a focus on asset management and the fact that Dell has a published 5 year service life on their commodity servers. In addition, TCIS watches the support notices on ES7000 servers and confirms that Unisys is proactively marketing a replacement product to address EOSL.

3) California State University

As a part of the 2011 Renewal for data center services for California State University, Unisys replaced the obsolete hardware and technologies within the production data center and included new features including a disaster recovery solution at a second data center.

4) City of Minneapolis

As part of ongoing operations, Unisys provides an annual technology refresh program for the data center infrastructure. The program reviews the current infrastructure for any equipment which is out of warranty or has reached the manufacturer's end of support. To reduce the impact to the City's business, Unisys works with the City's application support teams to coordinate the infrastructure upgrades with application upgrades whenever possible. When appropriate, Unisys provides recommendations to convert physical infrastructure to virtual to manage overall hardware costs of the environment during the technology refresh projects.

Benefits to the Commonwealth

The Unisys Team will work with the Commonwealth to develop technology refresh plans which not only replace the existing compute systems, but also incorporate newer technologies and

services over time to improve services, reduce cost, and meet changing needs.

3.2.1.5.2 IT Service Continuity Architecture

The Offeror's IT Service Continuity Architecture will provide tiered DR capabilities and Services for applications that have been identified by the Commonwealth. The Offeror must provide a Service Continuity solution that includes DR computing, storage, networking systems and recovery processes and will be included in the overall Commonwealth architecture design. Only critical applications and associated equipment identified by the Commonwealth will be addressed with DR systems. Additional information regarding Tiered Service Delivery and Tiered DR can be found in referenced supporting exhibits.

The Commonwealth will lead the Business Continuity effort with assistance from the Offeror.

Reference Documentation

Schedule J.1 - Datacenter Service Level Management

Requirements		Describe Compliance
1.	DR Architecture and Plan will be documented by the Offeror and approved by the Commonwealth.	Offeror must describe its infrastructure and service offering for a DR and Business Continuity Plan.
2.	IT Service Continuity Architecture and Plan - Backup hardware and software will be obtained, configured and available per an agreed to Service Level to process the identified critical applications. Where applicable, data will be electronically replicated (including disk-2-disk) to the backup systems (off site) to insure a successful recovery. Wherever data replication is not viable, backup tape data will be utilized.	Offeror must describe the design of its Tiered DR plan in the design of the Commonwealth technical architecture. Offeror must provide at least one relevant example from a prior engagement, in which it was engaged, that is similar to the needs of the Commonwealth. Offeror must describe its process for modifying the scope/service level for DR coverage.
3.	Recovery systems must be available via network access. Routing must be configured and tested during initial	Offeror must describe the network requirements of its DR plan in its proposed design of the network architecture.

	system architecture design. Include the network requirements of the DR plan in the design of the network architecture.	
4.	Recovery documentation for each identified system/ application will be required. Information will include the targeted backup hardware, software, networking changes, data location, restoration and access process, execution authorization, and notification to service owner when an application has been restored to service. Offeror must create recovery documentation for each system / application identified as a critical system where DR is required.	Offeror must provide at least one relevant example from a prior engagement, in which it was engaged, that is similar to the tiered DR needs of the Commonwealth.
5.	A DR support plan must be created. The DR team must notify the Commonwealth when a recovery plan will be put into action, and must manage questions and issues that may arise after implementation. Create a DR team that will manage the execution of the DR plan from declaration to recovery when required.	Offeror must provide at least one relevant example from a prior engagement, in which it was engaged, that is similar to the DR needs of the Commonwealth.
6.	For critical systems identified as having a current tested DR Plan within the DPH, the Offeror will update the associated DR test plans for the new target environment. Successful testing of each revised DR Plan is required prior to Commonwealth acceptance.	Offeror must provide its approach to creating and testing DR Plans.

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

Introduction

The Unisys solution includes an IT Risk Manager to work closely with the Commonwealth's Business Continuity personnel to frequently review, revise and update Agency Disaster Recovery Plans. These DRPs will be maintained in the new Unisys-managed online disaster recovery planning tool. The Unisys IT Risk Manager oversees all remediation efforts identified through twice-annual testing of each Agency's DRP.

The Commonwealth can implement granular tiers of Disaster Recovery services and even Business Continuity services to mitigate the risks associated with critical applications as described below.

1 DR, Data Recovery Architecture, Business Continuity Plan

1.A Offeror must describe its infrastructure and service offering for a DR and Business Continuity Plan.

The Unisys solution manages the infrastructure and service offering through the Infrastructure Architecture services described in Schedule, Section 3.2.2.2 (Infrastructure Architecture).

The DR services are available to Commonwealth agencies through the Enterprise Services Catalog which allows the agencies to select services to provide the quality of Disaster Recovery required to provide sufficient recovery times to critical applications in the unlikely event of a disaster.

2 IT Service Continuity Architecture and Plan

2.A IT Service Continuity Architecture and Plan - Backup hardware and software will be obtained, configured and available per an agreed to Service Level to process the identified critical applications.

The Unisys proposal includes a variety of data protection software tools to provide service continuity.

These software tools provide data protection for Commonwealth applications:

- [redacted] software manages nightly backups.
- [redacted] provides replication of backup data
- [redacted] provides data replication within [redacted] frames
- [redacted] provides data replication and snapshotting capability for [redacted]-based storage.
- [redacted] provides data replication with integration to the server O/S level for virtual

servers.

- [redacted] Storage Volume Controller provides replication and snapshot services.

More detailed descriptions are available in section F.3.2.4.2 Storage Management.

2.B Where applicable, data will be electronically replicated (including disk-2-disk) to the backup systems (off site) to insure a successful recovery

Unisys has provisioned DR that relies on both tape and disk based products to provide better recovery RPOs than tape based recovery. The Unisys has allotted sufficient Storage capacities from Schedule I Volumetrics to allow the Config4 servers to utilize SAN-based disk in order to meet the faster RTOs. These will be supplemented with application and host-based replication tools to meet the Platinum availability requirements.

2.C Wherever data replication is not viable, backup tape data will be utilized.

The Unisys solution provides a means for the Commonwealth, through the Catalog of Services items, to select sufficient resources to provision data replication as needed. Thus viability is not an issue. The Agencies of the Commonwealth are able to choose backup tape as a sole means of providing DR protection. The Unisys IT Risk Manager will help Agencies chose the appropriate means of providing cost-effective data protection while mitigating the risks associated with a data center disaster.

Unisys complies with requirement.

2.D Offeror must describe the design of its Tiered DR plan in the design of the Commonwealth technical architecture

The Enterprise Services Catalog offering includes these DR Tiers:

- Tier 1: Recovery from tape-based Backup within reasonable time frame.
- Tier 2: Recovery from a tape-based Backup with an accelerated process.
- Tier 3: Recovery from Backups replicated to DR via the [redacted] infrastructure.
- Tier 4: Recovery through asynchronous data replication for Open Systems SAN storage removing the need for Data Recovery.
- Tier 5: Data and O/S level replication for Virtual Windows/Linux instances removing the need for Data Recovery.
- Tier 6: With Agency approval the Tier5 offering can be configured to provide an automatic failover.

A detailed description has been provided in Section F.3.2.2.4 DR Planning and Testing.

2.E Offeror must provide at least one relevant example from a prior engagement, in which it was engaged, that is similar to the needs of the Commonwealth

The California State University (CSU) system relies upon Unisys for delivery of Disaster Recovery services. After years of reliable managed services for Production services CSU elected, after a competitive bid, to renew these services in the [redacted] Unisys data center and also expand services to include a complete Disaster Recovery service at the [redacted] Unisys data center.

The CSU infrastructure includes not only the world's largest PeopleSoft implementation but also file servers and applications rely upon but are less critical than the PeopleSoft servers.

Unisys provided a Tiered DR solution that provides both tape-based and disk-based data protection to deliver to a variety of RTO and RPO targets. Because CSU located its private clouds exclusively in Unisys-managed data centers they were able to take advantage of the Unisys Shared Storage rate-based data replication. Like the Commonwealth, CSU sought a pay-by-the-drink model rather than invest in upfront capital expenditures to acquire storage services.

The Commonwealth may opt to further reduce operating costs by leveraging the DR infrastructure to provide compute resources for development and testing. The Unisys team can help establish processes to set aside these test and development resources during DR testing exercises.

2.F Offeror must describe its process for modifying the scope/service level for DR coverage.

The Unisys Program Management Office manages the modification of scope and service levels for DR coverage within the context of ITIL V3 based Service Design. Through this process Unisys and the Commonwealth work together to define the requirements and benefits sought for needed service changes. This process is described in detail in the Technical Architecture services guide in section F.3.2.1.5 Technical Architecture.

The Commonwealth and the Agencies can change the scope or service levels for DR coverage for existing compute resources through the provisioning process initiated when the Commonwealth or its Agencies engage the Enterprise Services Catalog process to select or change DR services levels for compute assets.

3 DR, Recovery Systems

3.A Recovery systems must be available via network access. Routing must be configured and tested during initial system architecture design.

Include the network requirements of the DR plan in the design of the network architecture.

Offeror must describe the network requirements of its DR plan in its proposed design of the network architecture.

The Unisys solution leverages the same network for DR as it does for Production applications. The Unisys solution meets the COPANET connectivity requirements by connecting locally at [redacted] (DC1) via 10Gb Ethernet and via 2 x 1G Ethernet connections to an alternate COPANET location from another data center. Should direct connectivity to the Verizon PIP network be required Unisys can terminate Commonwealth provided PIP circuits on Unisys owned and managed equipment at the data centers.

In addition to DC1, two new data centers will be utilized – Unisys [redacted] (DC2) and Unisys [redacted] (DC3). In DC1, a new connection to the existing COPANET node will be built using two 10Gb fiber connections within the Commonwealth Technology Center located at 1 Tech Park in Harrisburg, PA. Since the distance to connect DC1 to COPANET is so short, these connections do

not require a WAN circuit to be installed, thus saving cost. The 1 Tech Park connectivity is shown on the far left in the diagram below (**Figure 3.2.1.5.2-1**)

Figure 3.2.1.5.2-1 Commonwealth Network Architecture

In the middle and far right side of the diagram above, COPANET connections to DC2 and DC3 are shown. Based on predicted future usage, both the DC2 and DC3 data centers will be connected to COPANET via 1 Gb circuits. To prevent a single point of failure in the connection to COPANET, the COPANET circuits from DC2 and DC3 will terminate in a different physical facility than the connection from DC1. The locations being considered to terminate the DC2 and DC3 circuits are

A deeper technical description is provided in section F.3.1.2 Network and Security Architecture.

4 DR, Recovery Documentation example

4.A Recovery documentation for each identified system/ application will be required. Information will include the targeted backup hardware, software, networking changes, data location, restoration and access process, execution authorization, and notification to service owner when an application has been restored to service.

Unisys proposes to rely upon the LDRPS online disaster recovery tool to maintain access to all DR run books so that these are always available to any Commonwealth or Unisys staff involved in executing DR tests or an actual Disaster Recovery.

In addition Unisys will exploit the full capabilities of the tool to build:

- Crisis management plans to fit each Agency's operational structure.
- Technology recovery plans to match a matrix management approach, including dependency mapping for the infrastructure supporting your applications.
- Critical application recovery plans to smoothly interface with your infrastructure recovery plans.
- Process or departmental recovery plans to support your planning decisions and strategies and to identify dependencies between critical business processes.
- Site event management plans to document how to deal with a specific incident at a

particular business location.

4.B Offeror must create recovery documentation for each system / application identified as a critical system where DR is required

The recovery documentation is created and maintained within the LDRPS online disaster recovery tool which is supplemented with critical documentation that is backed up with offsite copies specifically for use during both Disaster Recovery testing and in case of an actual, though unlikely, disaster.

4.C Offeror must provide at least one relevant example from a prior engagement, in which it was engaged, that is similar to the tiered DR needs of the Commonwealth.

Cross-Country DR for Telecommunication Service Provider: Unisys crafted a complex DR service infrastructure for a primary telecommunication service provider that uses Unisys-managed data centers for both Production and Disaster Recovery operations. See **Figure 3.2.1.5.2-2**.

Figure 3.2.1.5.2-2: Disaster Recovery Example: Telecommunication Supplier

The existing Unisys customer had been operating effectively with the Disaster Recovery services in a like-to-like Prod/DR fashion and sought to reduce costs and complexity while, if possible, improving DR services to reduce potential data loss during a Disaster event.

In pursuit of these business objectives and following the Unisys applied ITIL V3 Service Design process, the Unisys Enterprise Architecture team successfully designed and implemented a transition to a refreshed Infrastructure Architecture with a serve consolidation to greater reliance upon virtual server instances. This reduced complexity during recovery testing for DR

services. The refresh also included replacement of a tape-based DR recovery process to a disk-based infrastructure that reduced complexity and costs and improved overall service quality by reducing the time to recover services during a Disaster event.

California State University DR Services: When Unisys crafted the Disaster Recovery plan for the California State University system (CSU) they were reluctant to incur the cost of an identical compute power for a DR plan that they hoped never to use. Unisys presented two options to reduce cost:

1. For virtual servers the computer power was provisioned at a less than 100% of that available for production. CSU was willing to accept a diminished level of service immediately following an actual data center disaster and Unisys was able to propose a reasonable delivery date to augment the DR facility if an actual disaster occurred. The difference between the current computer power in the DR site and that of the Production data center delivers a monthly savings for CSU.
2. Unisys also provided a means for CSU to utilize assets provisioned for their DR plan as Test and QA/Dev servers under the agreement that if an actual disaster occurred then these services would be suspended so that these assets could be pulled into use as the Production infrastructure at the DR site. This allowed CSU to leverage the compute power of the DR site at relatively little risk.

The Agencies in the Commonwealth can, working with the Unisys IT Risk Manager, select servers and storage in the DR facility that would provide a diminished services in the event of an actual disaster. Given the unlikely chance of an actual disaster this would allow the Agencies to better balance the full cost of a Like-to-Like DR solution against the risk of occurrence of an actual disaster.

5 DR, Data Recovery Support Plan

5.A A DR support plan must be created. The DR team must notify the Commonwealth when a recovery plan will be put into action, and must manage questions and issues that may arise after implementation.

The activation of a recovery plan occurs only through escalation to appropriate Commonwealth and Agency leaders. During the process the Unisys Program Management Office engages technical and business continuity experts in order to present options and recommendations for Commonwealth leaders to that they are able to select the best service recovery option available to provide the least disruption to Pennsylvania constituents.

5.B Create a DR team that will manage the execution of the DR plan from declaration to recovery when required.

The Unisys proposes a dedicated DR team that will manage the execution of the DR plan from declaration to recovery when required.

However the Unisys proposal provides far more value to the Commonwealth than other vendors can provide in terms of Disaster Recovery and Business Continuity because the Unisys proposal provides the Commonwealth with continuity with the team that has performed

extremely well over the years. The Unisys disaster recovery team increased the quality and reliability of the Disaster Recovery services that support the Commonwealth. The Unisys proposal also elevates the importance of the service but placing it under a named resource in the Program Management Office under the title of IT Risk Manager.

5.C Offeror must provide at least one relevant example from a prior engagement, in which it was engaged, that is similar to the DR needs of the Commonwealth.

The Unisys Team provided the State of Alabama with a Disaster Recovery system with high availability needs that match the Tier5 offering in the Unisys proposal. The State of Alabama's Criminal Justice Information Center has similar security and compliance requirements to the Commonwealth's police and justice agencies.

Business Challenge: Improve Data

Delivery to Enhance Citizen Safety

The Alabama Criminal Justice Information Center (ACJIC) is a state agency providing local, state, and federal criminal justice agencies with the information needed to ensure citizen safety.

In 2004, ACJIC realized that gaps in its information technology were hindering communications and business continuity. It needed to more efficiently deliver critical information from its network and systems.

Maury Mitchell, Director of ACJIC explains, "We're connected to the FBI's National Crime Information Center, and we're in sync with all 50 states via the National Law Enforcement Telecommunication System. As such, our web applications handle about 18 million transactions a month. We were leasing space and time on the state's mainframe for data storage – a system we don't own – performing backups on tape and manually delivering them to a site a few blocks away for disaster recovery. We needed our own scalable, reliable, cost-effective system that would grow with our needs and provide hot failover."

ACJIC decided to change the way it was doing business. Jim Walker, Homeland Security Director for the State of Alabama, comments, "We had an opportunity to build redundancy into our system and improve the availability and use of information. We needed a solution that would build trust and deliver value to our user population." ACJIC explored several solutions and solution providers before choosing Unisys to help establish an IT infrastructure specifically designed to address the agency's requirements.

Enhancing officer and citizen safety while building trust among constituents – by re-engineering the IT infrastructure to improve communications and business continuity.

By implementing a solution based on Unisys ES7000/one and SafeGuard 30m technology, the Alabama Criminal Justice Information Center created a dependable, cost-effective system that delivers real-time information to end users, supports future growth, and provides robust, reliable operations.

Results: Unified Law Enforcement through a Real-Time Infrastructure

The center's more powerful and resilient IT infrastructure has improved real-time

communications among multiple levels of criminal justice agencies – enabling greater collaboration, and ultimately, a better response to criminal activities and other security concerns.

Metrics

- **Better Security:** Reduced downtime and risk – 24x7 availability with failover in less than one minute from the primary site to the disaster recovery site
- **Reduced Costs:** Lowered costs while processing some 18 million transactions monthly
- **Improved Satisfaction:** Enhanced citizen and officer safety by ensuring a constant flow of real-time information
- **Better Productivity:** Enabled one-to-two-second searches for up to 40 million records in the Law Enforcement Tactical System

6 Test, DR, Creating and Testing DR Plans

6.A For critical systems identified as having a current tested DR Plan within the DPH, the Offeror will update the associated DR test plans for the new target environment.

During transition the Unisys IT Risk Manager in the Program Management Office will review existing DR Plans for each Agency. This consultation builds our the initial Service baseline for the overall DR coverage for Commonwealth Agencies. The IT Risk Manager makes use of the Unisys Enterprise Architecture staff to provide consultative recommendations for migration of Agency compute assets into the new data centers with as well as for the provisioning of appropriate DR services.

The Commonwealth benefits from the current Unisys Disaster Recovery team who have continuously improved DR services to levels even better than the required SLAs. Unisys expects that with the acquisition of a Unisys-managed data center for DR and the increased frequency of testing, the team's performance will improve.

The Commonwealth benefits from the Online Disaster Recovery planning tool that can be used across all agencies. The Unisys Program Management Office will coordinate the agency-by-agency planning tasks. This coordination of activity will provide the Commonwealth with a common means of evaluating to overall IT Service Continuity afforded by the various plans. The IT Risk Manager in the Unisys Program Management Office will reference the tool to compare agency plans and notify the Commonwealth Office of Administration of any variances that lead to too large a gap in continuity plans or, conversely, high costs or over-preparedness relative to risks.

6.B Successful testing of each revised DR Plan is required prior to Commonwealth acceptance

Unisys complies with this requirement.

6.C Offeror must provide its approach to creating and testing DR Plans.

During transition the Unisys IT Risk Manager in the Program Management Office will review existing DR Plans for each Agency. This consultation builds our the initial Service baseline for

the overall DR coverage for Commonwealth Agencies. The IT Risk Manager makes use of the Unisys Enterprise Architecture staff to provide consultative recommendations for migration of Agency compute assets into the new data centers with as well as for the provisioning of appropriate DR services.

Following transition the Unisys IT Risk Manager meets with each Agency at least twice annually to review existing DR plans.

Unisys Team Experience

As described above, the Unisys team has provided significant savings for Unisys customers through creative Disaster Recovery services. The Unisys Team also benefits from supervision and innovations provided by the Unisys Director who serves as a Practice Lead for Disaster Recovery testing and service improvement. This director engages the IT Risk Manager in the Unisys Project Management Office for the Commonwealth to keep that Officer apprised of results from disaster recovery testing across the Unisys customer base. In this way the ITIL V3 Service Design process managed by the Unisys Program Management Office has the benefit of considering all recent Unisys Disaster Recovery innovations when apprising service changes for DR Services for the Commonwealth.

Benefits to the Commonwealth

The common disaster recovery services and testing that Unisys will bring to all participating Commonwealth Agencies will lower costs overall for the Commonwealth and provide a faster acceleration of DR service improvement for all Agency DR plans. The lessons learned during a single Agency's annual DR test can be applied across all Agencies fairly quickly because they will share common DR services and practices.

3.2.1.6 Account Management

The Account Management function is responsible to provide each Commonwealth agency with oversight of the contracted Services and support required to satisfy the Commonwealth's computing needs. The Account Manager will provide direct interface with the Commonwealth agencies ensuring daily operations and needs are provided, and create monthly operational summaries reporting to both the agencies and the Commonwealth. This report will address all operational events and issues that occurred during the month that would have effected service level attainments, problems and incidents, and recommendations for changes needed to provide continuous, secure computing Services. Each Commonwealth agency will interact with its assigned Account Manager to discuss needs, issues, problems or costs.

Reference Documentation

Schedule G - Staffing Plan and Key Positions

Requirements		Describe Compliance
1.	Assign an Account Manager to each identified agency. The Account Manager will be responsible for all Services provided, represent the Commonwealth agency's needs, and be the advocate for the agency throughout the Offeror's organization. Based on the size and application complexity of the Commonwealth agency, the Offeror must assign additional account management resources. Account Managers shall understand agencies line of business and business trend analysis. Offeror must assign a minimum of 6 dedicated account managers.	Offeror must identify its account management structure, roles, and responsibilities. The Offeror must provide resumes and qualifications for each of its proposed Account Managers and other key positions.
2.	Account Managers will meet with assigned agency contacts on a regular basis. It is anticipated that this will be at minimum weekly during the initial program start and through transition.	Offeror must describe its approach to meet this requirement.
3.	Meet with Commonwealth teams on a monthly basis. It is anticipated that this will be at minimum weekly during the initial program start and transition to monthly meetings with the Commonwealth teams to address problems and assure continuous service improvements.	Offeror must describe its approach to meet this requirement.
4.	Participate in agency-sponsored IT planning sessions on a quarterly basis. Offeror must schedule quarterly	Offeror must describe its approach to meet this requirement.

	computing capacity reviews to ensure sufficient processing capacity, needs, and issues are being addressed. Suggest changes when necessary.	
5.	Advocate for agency interests. Offeror's Account Management team will advocate for the Commonwealth's interests. For example, intervene with Service Desk personnel to resolve a major problem; problem escalation process, support root cause analyses process. Another example, coordinate with agency and service providers to ensure timing of technology refreshes have the least impact on the agency.	Offeror must describe its approach to meet this requirement.
6.	Monthly status reports - Ensure The Commonwealth is aware of operational status and project update information on a monthly basis. Create and deliver a monthly status report, summarizing operational metrics as defined in the CCPM, by service platform, including highlights and exceptions, and project status.	Offeror must describe approach and provide a representative sample report.

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

Introduction

The Unisys Account Management function is a long established function within the service delivery model. The objective of this function is to verify that Commonwealth agencies understand the terms of the Data Center Services Contract, and how it can be leveraged to meet requirements of each agency's business. The Agency Account Manager (AAM) assigned to a Commonwealth agency acts as a liaison between the Commonwealth agency and the Data Center Support Services organization. The AAM advocates on behalf of the agency to confirm contractual service levels are being met, problems and issues are quickly addressed and tracked properly, and costs are optimized wherever possible. The AAM coordinates and leads the effort

to implement any changes to service.

1 Staff, Account Management Structure, resume

1.A Assign an Account Manager to each identified agency. The Account Manager will be responsible for all Services provided, represent the Commonwealth agency's needs, and be the advocate for the agency throughout the Offeror's organization. Based on the size and application complexity of the Commonwealth agency, the Offeror must assign additional account management resources. Account Managers shall understand agencies line of business and business trend analysis.

Offeror must assign a minimum of 5 dedicated account managers."

Agency Account Management is the organization in which all Agency Account Managers report. These six managers serve the critical purpose of providing a single point of contact for agencies to the Unisys Team. These leaders are highly organized, resourceful and adept at bringing the right resources together to meet customer needs. Each individual selected has extensive experience managing customer relationships on outsourced data center services engagements with outstanding customer satisfaction.

Each of these team members has been supporting the Commonwealth of Pennsylvania on various engagements for years and understands the importance of dedicated agency focus and works to accomplish business objectives at the agency level. Their role is essential to ensuring that agency leadership understands how to leverage the contract to their benefit, and these leaders act as the agency's advocate on the Unisys team. Agency Account Management is led by the Agency Account Manager, Peter Cavanaugh who reports directly to [redacted] The Agency Account Managers are responsible for the four major functions of Contract Liaison, Agency Advocate, Agency IT Planning Sessions, and Monthly Status Reporting. They have all achieved ITIL V3 Foundations certification and most are PMP certified.

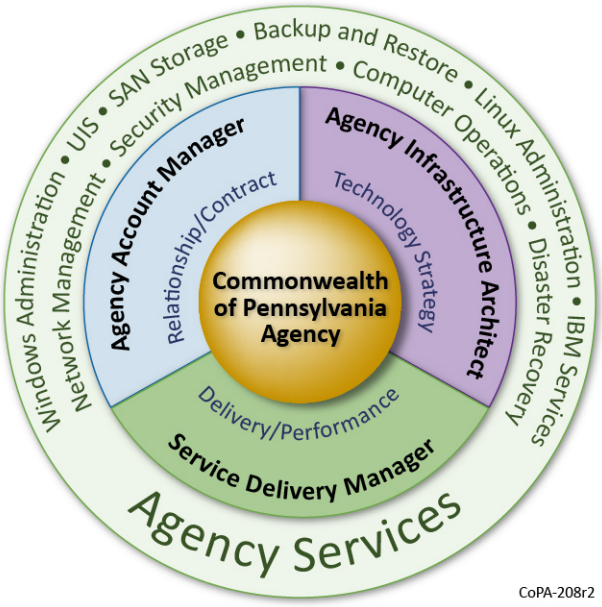


Figure 3.2.1.6-1 Agency Centric Team Approach

Account management resources will be assigned based on the size and application complexity

of the Commonwealth agency. We believe that our Agency Centric Team approach depicted in **Figure 3.2.1.6-1** will provide maximum leadership coverage for any particular agency regardless of size or complexity. Each team has a dedicated management structure that includes an Agency Account Manager who is responsible for managing the relationship with each agency supported and all aspects of the contract, an Agency Infrastructure Architect who is responsible for managing the Technology Strategy for assigned agencies, and the Service Delivery Manager who is responsible for end-to-end delivery performance and has direct oversight for managing all technicians aligned to the agencies supported by the team. The technical professionals managed by the Service Delivery Manager represent the technology disciplines necessary to provide comprehensive managed compute services to the Commonwealth. This model facilitates end to end accountability for availability and performance of Commonwealth application infrastructure supporting assigned agencies.

1.B Offeror must identify its account management structure, roles, and responsibilities.

The graphic below **Figure 3.2.1.6-2** depicts the functional roles of account management with its roles, responsibilities, and personnel specified. There are four primary functions associated with account management including Contract Liaison, Agency Advocate, Agency IT Planning Sessions, and Monthly Status Reporting.

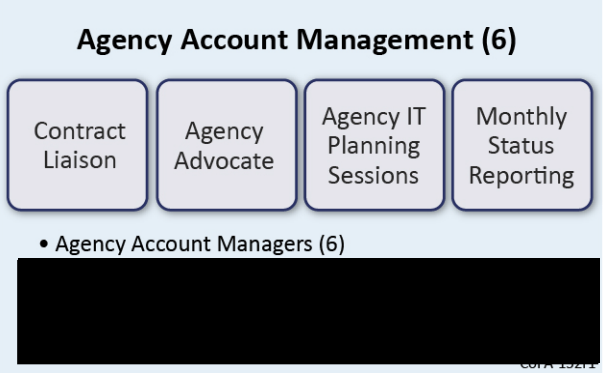


Figure 3.2.1.6-2 Agency Account Management Duties and Staffing Requirements

The **Contract Liaison** function owns the relationship at the agency level acting as a liaison between agency information technology staff and the Unisys Team. Agency Account Managers are responsible for understanding all Unisys services and providing guidance to the agencies in understanding how to leverage the contract to meet their Data Center needs. They maintain overall responsibility for sales, support, and operations ensuring that agreements are finalized and signed by all parties.

The **Agency Advocate function** provides that the Unisys Team understands agencies needs and requirements and advocates for agency and Commonwealth interests. This function provides the agencies with assistance needed to quickly navigate all facets of the Data Center Services support team.

The **Agency IT Planning Sessions** function in conjunction with Enterprise Architecture who briefs the Commonwealth on new services and technology, and is a key member of the agency's

planning team.

The **Monthly Status Reporting** function keeps contacts at the agency informed regarding service level performance. This function meets monthly with the agencies to address problems and provide continuous service improvements. This function is responsible for the creation of monthly operational summaries that will address all operational events and issues that occurred during the month that would have affected service level attainments, problems and incidents and recommendations for changes needed to provide continuous, secure computing Services.

The Agency Account Management organization chart is provided below **Figure 3.2.1.6-3.**

[redacted]

Figure 3.2.1.6-3 Agency Account Management Organization Structure

1.C The Offeror must provide resumes and qualifications for each of its proposed Account Managers and other key positions.

The key personnel of the Agency Account Management team consists of five **Agency Account Managers** introduced below including Peter Cavanaugh, [redacted] and [redacted] Account Manager resumes can be found under the Key Resume tab under Section 5 Personnel. A high level review of Agency Account Managers and their qualifications is provided below.

[redacted] **(based in Harrisburg, PA)** will be serving the Commonwealth as an Agency Account Manager under the new contract. He is a 23 year Unisys employee that has been working for the Commonwealth of Pennsylvania since 2002 in a variety of Project Management and Client Services Management roles supporting numerous Commonwealth organizations. Since 2005, he has been working on-site at the Commonwealth Technology Center in very close collaboration with the CTO, CISO, Client Management, Enterprise Data Center, Enterprise Networking and Security, Enterprise Services, GIS, PMO and many agencies.

[redacted] developed and introduced a customer satisfaction program for the Enterprise Data Center that continues today under the Enterprise Services as an important component of OIT's process for continuous improvement and building strategic relationships. Under this program, he facilitated regular communications and acted as a liaison for OIT with the CIOs for half of the agencies, describing the center's managed services programs, facility services and

benefits.

Communications, customer service and satisfaction, facilitation, infrastructure, project and program management, and strategic relationship building are common threads for more than a decade working with the Commonwealth and more than 20 years working for Unisys.

[redacted] **(based in Harrisburg, PA)** will be serving the Commonwealth as an Agency Account Manager under the new contract. He is a seven year Unisys employee that has been working for the Commonwealth of Pennsylvania for over 15 years providing technology solutions, consulting and complex project management services. For the past seven years, Brian has served the Commonwealth of Pennsylvania on the Unisys Data PowerHouse contract in various Service Delivery and Business Management roles acting as a liaison to the Office of Administration and agencies receiving service.

[redacted] provided exceptional leadership to the Data PowerHouse team through the alignment to ITIL best practices and the migration to the new ITSM Remedy system. With a service-centric approach, he has provided direction to the service delivery organization in support of complex solution/design implementation, managed service functions, quality improvement, and cost management activities. Brian is skilled at contract management and managing vendors and subcontractors ensuring shared accountability for outcomes.

[redacted] **(based in Harrisburg, PA)** will be serving the Commonwealth as an Agency Account Manager under the new contract. She has worked in the IT industry for 14 years, and is a five year Unisys employee supporting the Commonwealth of Pennsylvania as a Service Delivery Manager on the Data PowerHouse contract. Lydia has worked with numerous Commonwealth agencies to develop strong partnerships with agency leadership while aligning Unisys service delivery teams with executing policies and procedures as outlined in the contract with a focus on agency priorities and outstanding customer service.

[redacted] adroitly provides subcontractor oversight to provide top-notch service delivery across environments deployed at the DPH. She has managed numerous successful initiatives including new system implementations for the Pennsylvania Liquor Control Board and the Department of Health, along with hardware upgrades for the Department of State. Lydia is a superb communicator who verifies agency management is kept informed of initiative status, and she has received numerous accolades from Commonwealth management about her unwavering professionalism and skilled leadership.

[redacted] **(based in Harrisburg, PA)** will be serving the Commonwealth as an Agency Account Manager under the new contract. He has held a variety of IT leadership positions since joining IBM in 1976, and has worked with many Commonwealth agencies in the capacity of Service Delivery Manager for the past 12 years. He has a strong background and proven expertise in many IBM technologies including zSeries and iSeries technical management, support of the Disaster Recovery process, and relationship management. Barry possesses strong working knowledge of many Commonwealth agencies' business priorities, aligning cost-effective Data Center solutions to meet agency needs.

[redacted] has extensive experience managing Commonwealth agencies through planning and smooth execution of system migrations and upgrades to new hardware, and software product upgrades. He possesses superior knowledge of disaster recovery and business continuity planning demonstrated by creation of the disaster recovery plans supporting all IBM mainframe customers of the Data PowerHouse and coordination of all disaster recovery tests. Barry is

highly regarded as an expert in the field and for his knowledge of the Commonwealth as evidenced by commendable ratings in customer satisfaction surveys during his tenure.

[redacted] **(based in Harrisburg, PA)** will be serving the Commonwealth as an Agency Account Manager under the new contract. He has over 15 years of experience working in the IT industry, and has been supporting the Commonwealth of Pennsylvania since 1999, holding positions of progressive responsibility including his current role as the Service Delivery Manager at the Commonwealth's Enterprise Data Center. In this role, Kannan actively collaborates with many Commonwealth agency IT managers to formulate technology solutions to address business needs with long-term operational strategies that provide real value is delivered to the Commonwealth. Kannan is well versed with the Commonwealth standards and ITBs and has personally contributed to developing a few of the ITBs.

[redacted] understands the importance of agency participation in major consolidation and migration projects as he played a large role in architecting the e-Government server farm for the Commonwealth to host web applications for various agencies. On this project, Kannan leveraged excellent leadership and communication skills to provide direction to a team of technical consultants and to collaborate with over 40 agencies in their successful application deployment and operation, functioning as a liaison, moving ideas between the development community and the customer community to confirm the needs of the Commonwealth were represented in the design and delivery of the server farm.

2 PMO, Agency Meetings

2.A Account Managers will meet with assigned agency contacts on a regular basis. It is anticipated that this will be at minimum weekly during the initial program start and through transition. Offeror must describe its approach to meet this requirement.

Unisys AAMs recognize that each agency has different needs at different times and varying levels of activity associated with Data Center Compute Services. The AAM will work to identify and schedule the appropriate frequency, type of meeting with appropriate attendees to maximize productivity and effectiveness for the Commonwealth staff. Agendas are provided to all participants prior to meetings and meeting minutes are provided in a timely manner following the meeting. All action items from agency meetings are tracked and the AAM follows up to verify issues and actions are brought to closure.

3 PMO, Commonwealth Meetings

3.A Meet with Commonwealth teams on a monthly basis. It is anticipated that this will be at minimum weekly during the initial program start and transition to monthly meetings with the Commonwealth teams to address problems and assure continuous service improvements. Offeror must describe its approach to meet this requirement.

At a minimum, the following types of meetings are held:

- Monthly meetings of the operational personnel representing Commonwealth and Vendor to discuss performance any planned or anticipated activities and changes that might affect performance.
- During transition, meetings will be scheduled with Commonwealth designated agency contacts as needed and as applicable to each respective agency, at a minimum weekly. The

purpose of this meeting will be to address transition status, agency concerns and issues, develop resolutions jointly with affected Commonwealth participants, and to proactively minimize day-to-day agency business impacts.

- A monthly service review will be conducted to review performance against agreed service levels, current projects, potential capacity issues, and change order activity.
- Meetings as may be necessary and appropriate in the discretion of the Unisys and the Commonwealth.

The AAM is responsible to work with the agency to determine frequency and topic of all scheduled meetings.

Additionally, the Service Excellence Office described in Section 3.2.1.1.6 will lead meetings with agencies monthly to review completed and planned changes, service performance, incidents, problems, major project implementations, and any other item of interest for that month.

4 PMO, IT Planning Sessions

4.A Participate in agency-sponsored IT planning sessions on a quarterly basis. Offeror must schedule quarterly computing capacity reviews to ensure sufficient processing capacity, needs, and issues are being addressed. Suggest changes when necessary. Offeror must describe its approach to meet this requirement.

Unisys AAMs and Agency Infrastructure Architects forge a close working relationship with agency contacts, as well as their Commonwealth counterparts within the Office of Administration. AAMs will participate in all agency-sponsored IT planning sessions as requested by agency contacts, and will work with agencies to plan sessions important to the successful and improved operation of the agency.

AAMs schedule quarterly computing capacity reviews to confirm sufficient processing capacity for Commonwealth agencies. This provides a proactive approach to planning and preventing crisis situations that might otherwise arise during peak business cycles. AAMs conduct monthly performance reporting reviews and Capacity Planning process reviews two times per year. The Capacity Planning process is discussed in more detail in Schedule F, Section 3.2.2.3 Capacity Management.

5 PMO, Advocate Role

5.A Advocate for agency interests. Offeror's Account Management team will advocate for the Commonwealth's interests. For example, intervene with Service Desk personnel to resolve a major problem; problem escalation process, support root cause analyses process. Another example, coordinate with agency and service providers to ensure timing of technology refreshes have the least impact on the agency. Offeror must describe its approach to meet this requirement.

Unisys AAMs have a 10+ year history of performing this type of advocacy on behalf of Commonwealth agencies. The AAM acts as an extension of the agency management team to identify agency priorities and issues and leverages influence within the Unisys Team to communicate impactful agency information to obtain desired results on behalf of the agency. The AAM works closely with the Service Delivery Manager and Agency Infrastructure Architect to drive this information throughout the entire team supporting the agency. Some examples

include:

- Educating the Unisys Team on agency applications, their importance to citizens, and the criticality of the infrastructure
- Escalation of change activities to accommodate agency business needs
- Accommodating agency maintenance schedules through proactive Unisys resource realignments when required
- Communicating agency desires/constraints to Unisys personnel
- Facilitating the understanding of agency customer satisfaction feedback with Unisys personnel review
- Communicate agency business needs to Unisys staff to verify understanding
- Escalation of agency resource procurements to satisfy business needs and milestones
- Holds team accountable for completion of tasks and action items that are important to the agency
- Asserts the agency's position on business requirements when planning the timing of multi-agency outages

6 Monthly Status Reports, Sample Report

6.A Monthly status reports - Ensure The Commonwealth is aware of operational status and project update information on a monthly basis. Create and deliver a monthly status report, summarizing operational metrics as defined in the CCPM, by service platform, including highlights and exceptions, and project status. Offeror must describe approach and provide a representative sample report.

Unisys management will hold a monthly meeting with the Commonwealth Office of Administration and all participating agencies. The purpose of this meeting is to share information across the Commonwealth regarding performance successes and failures, service improvement initiatives, project status, and topics of interest that arise from time to time. This is an opportunity for the agencies to learn what other agencies are doing to improve their operations and to share ideas and information that is applicable to everyone. This encourages participation and enhances everyone's ability for process improvement across the Commonwealth.

There are two sample monthly reports being provided in the attachments**. Attachment F-1 - DPH Monthly Service Performance Management Meeting**, shows the monthly performance report delivered at an agency level and **Attachment F-2 - Managed Services IES and Unisys – Measurement Report**, is an example of the aggregated program view discussed in the previous paragraph. These monthly reports will be available to Commonwealth management via the Service Portal, and data of this nature can be accessed on a real-time dashboard on the Service Portal.

Unisys Team Experience

The Unisys Team has had team members representing the interests and acting on behalf of Commonwealth agencies on the Data PowerHouse contract for several years. They have been known as Customer Service Managers (CSMs) and Service Delivery Managers (SDMs), but functionally, the role is the same.

IBM provides very robust set of Account Management Services in conjunction with the Georgia Technology Authority. IBM staffs a position called the Program LifeCycle Manager (PLM). In this role the PLM is responsible to align with the Agency to understand and manage Program requirements on an End to End basis – from the time the Program is envisioned to the time the Program goes live.

Additionally IBM staffs a number of Architects assigned on an Agency basis who are responsible to understand and work with the agency in developing requirements for their service requests.

Benefits to the Commonwealth

Unisys has deep knowledge of the Commonwealth agencies, their priorities and their business. Our Agency Account Managers have worked with agency leadership for several years and understand the sensitivities of each agency, and will be matched to agencies where they add the most value. Our AAMs are respectful of the differences between agencies and will tailor support to the requirements of the agency rather than treating them like just another number.

3.2.1.7 Configuration Management

The Offeror's Configuration Management system must ensure complete and accurate recordkeeping relative to datacenter assets; hardware, operating system software, firmware, and network. The Offeror's Configuration Management Database (CMDB) system must be synchronized with the proposed datacenter Change and Release Management processes. Also included will be associations of infrastructure configuration items (CIs) and Agency application infrastructure to support application infrastructure related SLAs.

At the end of the contract the Offeror will be responsible to provide the Commonwealth with a final electronic copy of the CMDB.

The following list identifies but does not limit the roles and responsibilities that the Offeror must perform:

- Define and document Configuration Management standards and procedures per ITIL v3 standards.
- Establish an electronic interface to the Commonwealth's CMDB(s) to keep current both the Commonwealth's CMDB and the Offeror's CMDB.
- Establish process for tracking configuration changes
- Establish process interfaces to Incident and Problem Management, Change Management, technical support, maintenance and asset management processes
- Establish appropriate authorization controls for modifying configuration items
- Establish configuration baselines as reference points for rebuilds, and providing ability to

revert to stable configuration states

- Establish process for verifying the accuracy of configuration items, adherence to Configuration Management process, identify process deficiencies and recommend corrective actions

The Commonwealth will require online access to configuration related information and reports to satisfy application updates and audit requirements.

Reference Documentation

Schedule H - Commonwealth Computing Procedures Manual (CCPM)

Requirements		Describe Compliance
1.	Provide a documented process to track configuration changes accordingly to ITIL V3 framework	Offeror must describe how its Configuration Management System addresses the list of requirements described above. Offeror must provide a toolset description and an example of a configuration management system from a prior or current engagement of the Offeror.
2.	Per agency request, provide specific application related infrastructure component configuration information.	Offeror must describe how its configuration management systems can support this requirement.
3.	Provide current configuration reports at an agency level by datacenter component.	Offeror must describe its process to request configuration management reports. Offeror must provide a sample of a Configuration Management report used by Offeror on a current or previous engagement.
4.	Continuous review and updates to the Offeror's and Commonwealth's CMDB	Offeror must describe its approach to maintaining the accuracy of the CMDBs (Offeror & Commonwealth).
5.	CMDB that constitutes the common repository created by the Offeror to include, but not be limited to, location information, service information, configuration	Offeror must describe its approach to meet this requirement.

	information, application information, billing data, inventory data, and performance data. This data will be provided to the Commonwealth via electronic interface in a format approved by the Commonwealth.	

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

Introduction

Unisys will provide a Service Asset and Configuration Management Process and Configuration Management Data Base (CMDB) that will help to provide complete and accurate recordkeeping relative to service and application relationships, data center assets, hardware, operating system software, firmware, and network configuration items (CI's). The Unisys maintained CMDB system will be managed through the Change and Release Management Processes to help verify that all CI's are maintained timely and accurately.

Unisys will map the relationships of infrastructure configuration items (CIs) to Commonwealth/Agency application (CI's) that will be completed when agencies transition to Unisys managed infrastructure. These relationships will be used to support infrastructure availability SLA calculations, billing, etc. The following is the approach to transitioning the CMDB.

1. Determine requirements to support availability SLA's for each application or set of data center assets transitioned using the J3 definition for Infrastructure Availability

2. Determine the alternatives to establish the CMDB relationships to support these availability SLA's including:

   - Utilizing the Commonwealth / Agency CMDB sources
   - Discovery using [redacted]
   - Using the [redacted] utility to finalize the mapping labels, relationships etc. to support the SLA's
   - Obtaining the Commonwealth approval for the mapping during transition

Unisys will provide the Commonwealth with a final electronic copy of the CMDB at the end of the contract.

Unisys accepts full responsibility for maintaining the Configuration Management Process and CMDB to the levels of accuracy required by the SLA for CMDB accuracy.

Unisys will perform the following roles and responsibilities as it pertains to Configuration Management:

- Unisys will define and document Configuration Management Process and procedures per ITIL V3 guidelines and Unisys standards.
- Unisys will establish an electronic interface to the Commonwealth's CMDB(s) to keep current both the Commonwealth's CMDB and the Offeror's CMDB synchronized.
- Unisys will establish the process for configuration control to track and manage all configuration changes. This will be accomplished by implementing change and configuration management processes to verify that configuration analysts who will be responsible for making any required configuration changes to the CMDB are part of the change and release and deployment processes to register CMDB changes for specific types of change and release activities (e.g., break/fix replacements to infrastructure CI's, provisioning of new CI's, software updates, etc.). Also, the configuration analysts will verify that automated processes for provisioning infrastructure when selecting Enterprise Services Catalog items have updated the CMDB properly.

1 ITIL Framework, CM Process, ITIL Toolset example (experience)

1.A Provide a documented process to track configuration changes accordingly to ITIL V3 framework

Unisys will provide a documented process to track configuration changes using the ITIL V3 framework based on its proven enterprise process implemented for customers. This will be reviewed with the Commonwealth during transition and adjusted accordingly to fit any Commonwealth unique requirements.

The Service Asset and Configuration Management Process addresses service assets throughout the entire service life cycle. It provides a complete inventory of assets, and identifies the individuals responsible for their control. It includes:

- Full life cycle management of IT and service assets, from the point of acquisition through disposal
- Maintenance of the asset inventory

The Service Asset and Configuration Management (SACM) process provides a configuration model of the services, assets, and infrastructure that will contribute to meeting the ITSM objectives and to assist the Unisys team in meeting service levels, by recording the relationships between service assets that will be managed as CIs. Assets are elevated to Configuration Items (CI's) for management purposes by augmenting asset data with configuration details that will support the management goals of ITSM and assist the Unisys team in meeting SLA's.

The SACM process provides that selected components of a complete service, system, or product (the configuration) are:

- Identified, baselined, and maintained
- Controlled through the Change Management process
- Released into controlled environments with operational use allowed only on the basis of formal approvals

The scope for SACM may cover non-IT financial assets, including work products that are used to architect and document services, and CIs required supporting a service (e.g., documentation to support ongoing operations). The SACM scope covers interfaces to internal and external service

providers where there are assets and CIs that need to be controlled, e.g., shared assets.

The Unisys Configuration Management Process is summarized in **Figure 3.2.1.7-1** below.

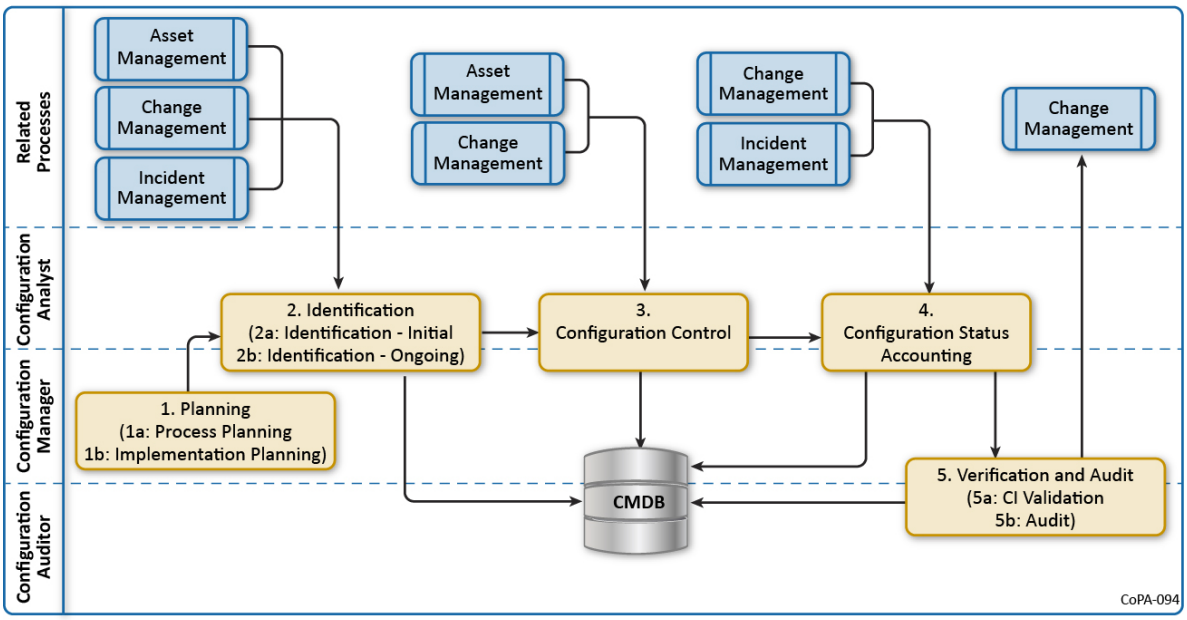


Figure 3.2.1.7-1: Configuration Management Process

1. Planning – This activity creates and delivers the Service Asset and Configuration Management plan. The Configuration Manager working with the Asset Manager(s) and Commonwealth Configuration Management team will develop and document a detailed Configuration Management Plan that will include:

   - Configuration Management Process and procedures
   - Configuration Items and Attributes
   - Reconciliation Processes and procedures
   - Audit Processes and procedures
   - Baseline Management and recovery procedures
   - Technology to support

2. Identification – This activity selects and identifies the configuration items for all of the infrastructure items supporting applications and services , including identification of CI owners, CI interrelationships, CI attributes, and configuration documentation. This includes allocating identifiers and version numbers for CIs, labeling each item, and entering it into the Configuration Management Database (CMDB).

3. Configuration Control – This activity verifies that only authorized and identifiable CIs are accepted and recorded and it provides that no CI is added, modified, replaced, or removed without the existence of the appropriate controlling documentation (e.g., an approved RFC

or an updated specification). These activities happen throughout the CI life cycle from deployment into production until disposal Configuration Control.

4. Configuration Status Accounting and Reporting – This activity governs the reporting of all current and historical data regarding each CI throughout its life cycle. This information allows changes to CIs and their records to be traceable (e.g., tracking the status of a CI as it moves from one state to another).

5. Verification and Audit – This activity includes a series of reviews and audits that verify the physical existence of CIs and check that they are correctly recorded in the Configuration Management system.

The Unisys Solution for the Configuration Management Process includes the people, process and technology to provide a comprehensive solution in support of the Commonwealth.

Unisys will provide a Configuration Management and Asset Management team to support the SACM processes and maintain the Asset and CMDB databases to the accuracy level defined in the CMDB Accuracy SL13. Please refer to the Service Excellence Office description in F3.2.1.1.6 for a more complete description of the organization.

The Configuration Management Process is described above for SACM. It will be implemented to support the other significant ITSM processes including:

- Asset
- Incident
- Problem
- Change
- Service Level Management
- Capacity

Assets will follow the financial asset management lifecycle for requisition, procurement, receipt, deployment, and retirement and form the foundation for Configuration Management (CMDB). The Configuration Management Team will identify assets that will become assets to maintain as Configuration Items (CI's) to track additional configuration related information in order to support ITSM processes and service management objectives.

1.B Offeror must describe how its Configuration Management System addresses the list of requirements described above (below).

Define and document Configuration Management standards and procedures per ITIL v3 standards.

Please refer to 1.A for the Configuration Management ITIL V3 process overview that Unisys will review with the Commonwealth during transition to the ITSM Operational Readiness Platform.

Establish an electronic interface to the Commonwealth's CMDB(s) to keep current both the Commonwealth's CMDB and the Offeror's CMDB.

Unisys will establish an electronic interface to the Commonwealth's ITSM Platform to keep current both the Commonwealth's CMDB and the Offeror's CMDB synchronized.

The Commonwealth will receive updates to the Commonwealth's CMDB for all CMDB data including but not limited to configuration information for servers, network, and storage CI's as well as relationship data between these CI's and applications where applications can be discovered.

This will meet the requirement of supplying the Commonwealth with service, application, configuration, and location inventory data.

Establish process for tracking configuration changes

This activity confirms that only authorized and identifiable CIs are accepted and recorded and it verifies that no CI is added, modified, replaced, or removed without the existence of the appropriate controlling documentation (e.g., an approved RFC or an updated specification). These activities happen throughout the CI life cycle from deployment into production until disposal Configuration Control

The Configuration Analyst will verify that all CI's are updated according to change and release management processes for:

- Standard RFC CI's that are released and deployed
- Automated discovery and CMDB updates
- Provisioned Enterprise Services Catalog items into production

Establish process interfaces to Incident and Problem Management, Change Management, technical support, maintenance and asset management processes

Unisys will establish process interfaces to Incident and Problem Management, and Change Management including technical support and maintenance procedures.

Incident and Problem Processes will be implemented to help confirm that all incidents and Problems are properly attached to CI's in the CMDB. This will support Problem Management in determining problematic CI's, establish problem records and determining root causes to process changes for eliminating defects in the infrastructure supporting Commonwealth applications. Unisys will implement technical support procedures and work instructions will be implemented to support use of the CMDB for all work activities requiring incident, problem, or change work tasks. Maintenance records and maintenance contracts with contact information for support activities will be accessible to the technical support teams.

Establish appropriate authorization controls for modifying configuration items

Unisys will establish appropriate authorization controls for modifying Configuration Items (CI's). During transition detailed process and procedures will be implemented to restrict CMDB update capabilities to the authorized the Unisys Configuration Management Team.

Establish configuration baselines as reference points for rebuilds, and providing ability to revert to stable configuration states

Unisys will establish configuration baselines as reference points for rebuilds, and providing ability to revert to stable configuration states. Configuration Management CMDB baselines will be established following reconciliation after major updates to the CMDB (e.g., after significant transitions, or major releases. A configuration management baseline strategy will be part of the Configuration Management Plan and reviewed as part of the transition and release plans. The baselines will be used in the event of required rollback, recoveries, or rebuilds.

Establish process for verifying the accuracy of configuration items, adherence to Configuration Management process, identify process deficiencies and recommend corrective actions

Unisys will establish process for verifying the accuracy of CI's, adherence to Configuration Management process, identify process deficiencies and recommend corrective actions. Unisys will implement periodic reconciliation procedures in support of the Configuration Management Process to help confirm the timeliness and accuracy of the CMDB. This involves detailed procedures to support several sources of CMDB updates including:

- Import of discovered data from the discovery tool (ADDM) to normalize and reconcile CI's before updating the CMDB.
- Auditing or updating release and deployment configuration changes in the CMDB
- Conducting periodic audits with the Commonwealth to identify and determine the root causes of any discrepancies including any process issues.

Figure 3.2.1.7-2 below shows the process for configuration discovery, normalization, and reconciliation , and updating the production CMDB.

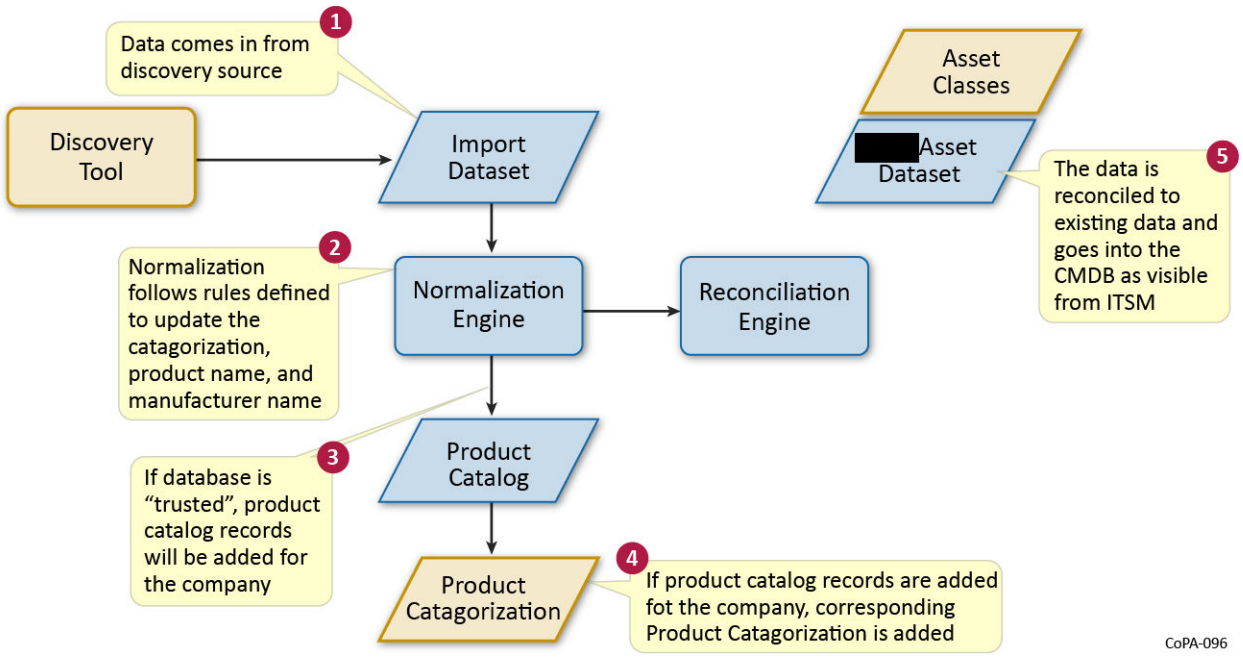


Figure 3.2.1.7-2 CMDB Discovery, Normalization and Reconciliation Process

The Commonwealth and Unisys will conduct CMDB audits following the process shown below in **Figure 3.2.1.7-3**, on a scheduled periodic basis in order to determine the accuracy of the CMDB and to determine any root cause for discrepancies discovered. The audits will be used to calculate the SL13 CMDB Content Accuracy and Timeliness SLA. Unisys proposes that the audit items include CI's and all selected attributes for each selected CI. CI's selected for audit should be limited to those items that can be discovered by the automated discovery tool [redacted].

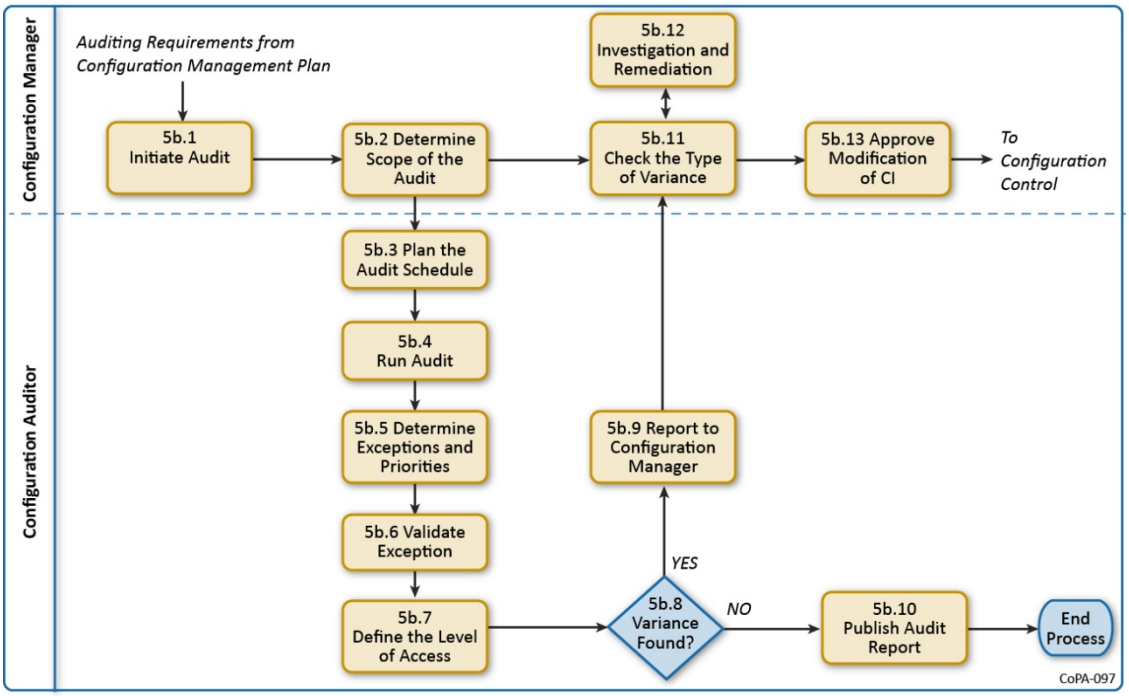


Figure 3.2.1.7-3 – CMDB Audit Process

Unisys will work with the Commonwealth to plan each audit. The criteria for selecting which CI's will be used for calculating SL13 will be random.

In addition to official Commonwealth audits of the CMDB, Unisys will also conduct internal CMDB process audits focused on helping to improve CMDB accuracy. These areas include:

- Change Management Reviews – check to verify changes that impact CI's have been updated properly in the CMDB
- Incident and Problem Management Reviews – Review incident and problem records associated with break fix items in the data centers and determine if the CI's have been properly recorded in the CMDB
- Change Management Software installation reviews – Review change requests associated with software installations or removal to confirm the CMDB reflects the proper recording of these changes

The formal CMDB audits will be jointly executed, the results compiled and reviewed. The SL13 calculation will be determined and the overall audit results will be summarized with supporting

details tracked, through the recording and processing of incident, problem and change records. Problem records will be created to perform root cause analysis for an identified exception in order to resolve any defect from a process, manual or automated step from updating the CMDB. Change records will be created and executed to eliminate the defect and the CMDB updated with the correct configuration item information.

1.C Offeror must provide a toolset description and an example of a configuration management system from a prior or current engagement of the Offeror.

Unisys has implemented a Configuration Management Solution for the Australian Government Department of Education and Training Administration (DETA) as an example. Unisys currently hosts (DETA) on its shared Global 7.6.04 ITSM platform. The CMDB configuration utilizes the [redacted] discovery toolsets for discovery of CI's to populate the populate the [redacted].

The following software components, descriptions and versions comprise the DETA CMDB solution implementation

[redacted]

2 CM Application CM

2.A Per agency request, provide specific application related infrastructure component configuration information.

Unisys will provide mapping of infrastructure to agency applications as part of the CMDB availability SLA transition services for agency applications onto Schedule I infrastructure.

This configuration information for each item supporting an Agency Application can be presented to the Agency Application stakeholders as views into the Unisys CMDB without having to request it specifically. Views for application owners can be configured to be viewed on

the Unisys ITSM Platform.

This same information is synchronized with the Commonwealth's CMDB and should be available for viewing and reporting from the Commonwealth's ITSM platform.

Following transition, Unisys offers a Services Catalog item for mapping specific application related infrastructure component configuration information for Commonwealth agencies. This will apply for changes to applications and their supporting infrastructure following transition. This service will be tiered according to the complexity of mapping infrastructure to specific agency applications (small, medium, complex). The service involves a workshop to review what current CI's the [redacted] have discovered, including all infrastructure and network related CI's and any components of the application. The Unisys Configuration Analyst will map and label infrastructure items to the application CI's, utilizing a mapping tool.

An additional Catalog Service is offered to monitor application workflow on supporting infrastructure including:

- Viewing discovered CI's supporting a specific application,
- Monitoring the transaction flows, queues and bottlenecks visually through each supporting CI.

This will help Commonwealth/Agency Application's teams troubleshoot applications in the test or production environments.

2.B Offeror must describe how its configuration management systems can support this requirement.

Please refer to 2.A to see the description of how these standard and catalog services support the Commonwealth/Agencies in providing application specific infrastructure component information.

3 CM Reporting, sample reports

3.A Provide current configuration reports at an agency level by datacenter component.

Unisys will provide configuration reports to Commonwealth Agencies for all data center CIs. Commonwealth users will be able to utilize the Unisys Portal and Real-time Dashboard to select reports and drill down to detailed reports accessible in the [redacted]. The following is a summary of Asset / Configuration Management standard reports:

Report Name	Description	Frequency
Software Licenses Management		
Software License Compliance Sub Reports: Software License	Displays the total number of software products that are compliant compared with the total number of software products that are non-compliant. This report includes discovered data elements, as well as client provided contract and license information.	Monthly

Compliance Detail report Compliance Summary for Software Product report Deployment Detail for Software Product report		
Software Inventory Profile for Licensable Products	Provide total number of software instances available in CMDB, broken down by product	Monthly
Enterprise Asset Management		
Inventory Profile Sub Reports: includes Inventory Profile-Drill-Down View report	Displays the total number of assets in the in the production CMDB grouped by Hardware and Software asset types.	Monthly
Asset Aging Sub Reports: Asset Aging-Drill-Down View report	Displays a summary of the aging of various assets in the production CMDB.	Monthly
Asset Relationship Analysis Sub Reports: Asset Relationship Analysis – Selection of assets	This report is used for selecting an asset for the Asset Relationship Analysis report. Report used to view the CIs and their relationships that exist in [redacted]	Ad-hoc (Account Team will have it cost involved for ad-hoc report) – 15 min Effort to run report
CIs Data Dump	Details of CIs (hardware and software) that for the selected company (i.e., Commonwealth Agency) and class for XLS format.	Weekly
Configuration Management Reports		
Deliverable Name	Description	Frequency
Discovery Datasets Comparison Sub Reports: Datasets Comparison-Drill-down View	Displays a summary of the comparison of discovery datasets within [redacted]. The differences between these datasets are displayed by hardware and software components. A drill down is available for components within each dataset to view its details, which are displayed in the Discovery Datasets Comparison-Drill-down View sub-report. This report also displays the changes in the CI data between	Daily/Weekly/Monthly

	each discovery scan.	
Staleness Analysis of Discovery Data Sub Reports: Staleness Analysis of Discovery Data -Drill Down I report Staleness Analysis of Discovery Data - Drill Down II report	Displays an analysis of CI discovery data. The report identifies those CIs that have remained undiscovered during the previous scans. All the CIs are grouped into various time intervals by last scan date. Drill-downs show the CIs belonging to various time intervals. Sub reports of this report include Staleness Analysis of Discovery Data -Drill Down I and Staleness Analysis of Discovery Data - Drill Down II report.	Monthly
Reconciliation Job Analysis	Displays the details of all reconciliation jobs that are set up in [redacted].	Daily/Weekly/Monthly(depends on Recon Job scheduled)

3.B Offeror must describe its process to request configuration management reports.

Commonwealth users will be able to utilize the Unisys Services Portal to select reports and drill down to detailed reports.

3.C Offeror must provide a sample of a Configuration Management report used by Offeror on a current or previous engagement

The following is an example of a Configuration Management Report from a current Unisys customer. This represents the Configuration Management CI relationships supporting an application with the associated incidents for each CI node. This report is online via the ITSM CMDB toolset and can be extracted into a Report format. Please see the example below in **Figure 3.2.1.7-4.**

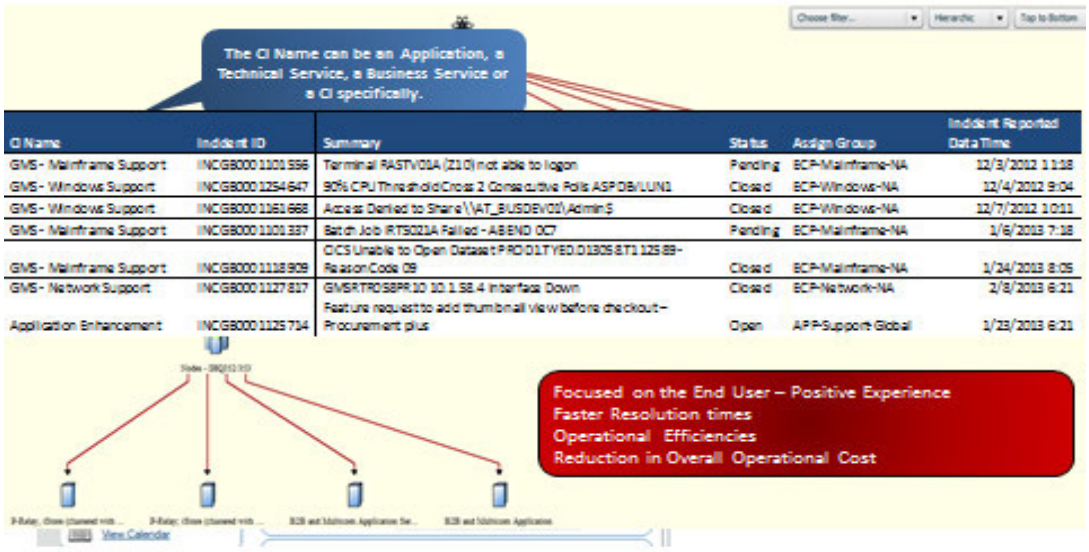


Figure 3.2.1.7-4 Configuration Management Report

4 CM, Continuous Review of CMDB

4.A Continuous review and updates to the Offeror's and Commonwealth's CMDB

Unisys will be conducting continuous reviews of the CMDB to help verify its accuracy as described above in 2.B. This is a combination of processes that support configuration control for change and release management, audits, and reconciliation procedures. The Unisys Remedy CMDB will be synchronized with the Commonwealth's Remedy CMDB.

4.B Offeror must describe its approach to maintaining the accuracy of the CMDBs (Offeror & Commonwealth

Unisys will establish process and procedures for verifying the accuracy of CI's, adherence to Configuration Management process, identify process deficiencies and recommend corrective actions. Unisys will implement periodic reconciliation procedures in support of the Configuration Management Process to help confirm the timeliness and accuracy of the CMDB. This involves detailed procedures to support several sources of CMDB updates including:

- Import of discovered data from the discovery tool (ADDM) to normalize and reconcile CI's before updating the CMDB.
- Auditing or updating release and deployment configuration changes in the CMDB
- Conducting periodic audits with the Commonwealth to identify and determine the root causes of any discrepancies including any process issues.

5 CM, CMDB Repository

5.A CMDB that constitutes the common repository created by the Offeror to include, but not be limited to, location information, service information, configuration information, application information, billing data, inventory data, and performance data. This data will be provided to the Commonwealth via electronic interface in a format approved by the Commonwealth.

Unisys will develop a detailed Configuration Management Plan during transition to identify with the Commonwealth Agencies, CI's and attributes to be managed for a complete CMDB data model and repository including but not limited to:

- Location information (where the asset resides)
- Service information (maintenance contracts and service contacts)
- Configuration information (for servers, mainframes, storage and LAN Network devices)
- Application information (for applications mapped to infrastructure)
- Inventory data for all assets under change control
- Performance data (maintained and reported in BPPM and Capacity Optimization Toolsets)
- Relationship data between CI's

5.B Offeror must describe its approach to meet this requirement.

There will be a heavy emphasis on using the CMDB discovery tool to initially populate and maintain the accuracy of the Unisys ITSM CMDB in ongoing operations and to also synchronize the Unisys CMDB from information stored in the Commonwealth CMDB. Unisys will work diligently to maintain the accuracy of manually entered CMDB data.

All CMDB information will be provided to the Commonwealth via electronic interface in a format approved by the Commonwealth. Unisys will provide a summary of standard Unisys [redacted] of CI's, attributes and relationships

Unisys Team Experience

Unisys currently provides IT Service Management Services to more than 150 customers worldwide. Unisys is a leading provider of Managed Services utilizing an integrated suite of ITIL V3, ISO 20000 certified management processes and leading ITSM tools to provide outstanding service IT services to our customers. Unisys currently successfully manages Service Asset and Configuration Management for many of these customers.

Currently, the Unisys Team successfully manages Service Assets for the Commonwealth.

Benefits to the Commonwealth

The Unisys value proposition for Service Asset and Configuration Management Solution is to maintain an accurate CMDB that represents the CI's and relationships supporting Agency Application CI's which will support adding the following value:

- Supporting availability infrastructure SLA's calculations for Commonwealth/Agency applications

- Avoiding significant service impacts by providing configuration management service impact information that allows Change Analysts to plan successful changes. This will prevent significant service impacts to Commonwealth application users.
- Eliminating infrastructure defects though the Problem Management Process utilizing CMDB data that links incidents to CI's. With these relationships established it is easier for the Problem Manager to identify service impacting defects to be eliminated through root cause analysis.

3.2.1.8 3rd Party License Management

Currently the Commonwealth manages over 2,000 business applications that require numerous software platforms and products. The Offeror's 3rd Party License Management service must ensure accurate inventory and licensing compliance for all Offeror provided infrastructure software products. The Offeror will be solely responsible for the management of all infrastructure software products provided through this contract.

The Offeror must coordinate with the Commonwealth to ensure compatibility between Commonwealth provided applications related software, and the Offeror provided infrastructure software. The Offeror must provide a method for tracking and reporting on both Offeror provided and Commonwealth provided software that will reside on the managed infrastructure.

The Offeror must provide the ability to purchase the Third Party Software listed in Exhibit B.4 - DPH - Third Party Software and additional third party software if required to provide the contracted services. The Offeror shall be responsible for the licensing and maintenance and support for the Third Party Software. The Commonwealth at its sole discretion may procure third party software from appropriate contracts.

The Offeror must provide the ability to purchase maintenance and support for the Third Party Software listed in Exhibit B.10 - DPH – Hybrid Third Party Software. The Offeror shall be responsible for the maintenance and support for the Third Party Software. The Commonwealth at its sole discretion may procure third party software maintenance and support from appropriate contracts.

Reference Documentation

Exhibit B.3 - DPH - Commonwealth Software Asset Listing

Exhibit B.4 - DPH - Third Party Software

Exhibit B.10 - DPH – Hybrid Third Party Software

See each target datacenter exhibits for current applications supported.

Requirements		Describe Compliance
1.	Provide, as requested, current software license reports for in scope infrastructure. For example specific OS version and patch levels per service instance.	Offeror must describe its approach to providing 3rd party software inventory and tracking per agency related infrastructure.
2.	Improve service quality, efficiency, and effectiveness.	Offeror must describe its methods to address continuous service improvement process

		related to 3rd party software management.
3.	Improve/reduce cost of service.	Offeror must provide examples of 3rd Party Software Management initiatives it has implemented and which may be utilized to achieve reduced costs of Services and to meet or exceeded ROI (Return on Investment) analysis projections.

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

Introduction

Unisys will provide 3rd Party License Management Service for the Commonwealth/Agencies and Unisys provided infrastructure software products. Unisys will be solely responsible for the management of all infrastructure software license products provided through this contract. The goals of this service are to:

- Verify software contract compliance (to avoid non-compliance legal issues and expenses)
- Manage costs of software inventory by matching requirements for use to needs
- Confirm software maintenance contracts are maintained on schedule through early notifications

1 Software License Inventory and Tracking

1.A Provide, as requested, current software license reports for in scope infrastructure. For example specific OS version and patch levels per service instance.

Unisys will provide software license reports for in scope infrastructure. These reports will include the level of detail agreed to and tracked in the [redacted] and Asset Management Database. These reports will include the OS versions they are running on and versions. Patch levels may be tracked and reported using the [redacted].

1.B Offeror must describe its approach to providing 3rd party software inventory and tracking per agency related infrastructure.

Unisys will implement the following process (**Figure 3.2.8.1-1**) to load and manage software license inventory and management to meet these goals:

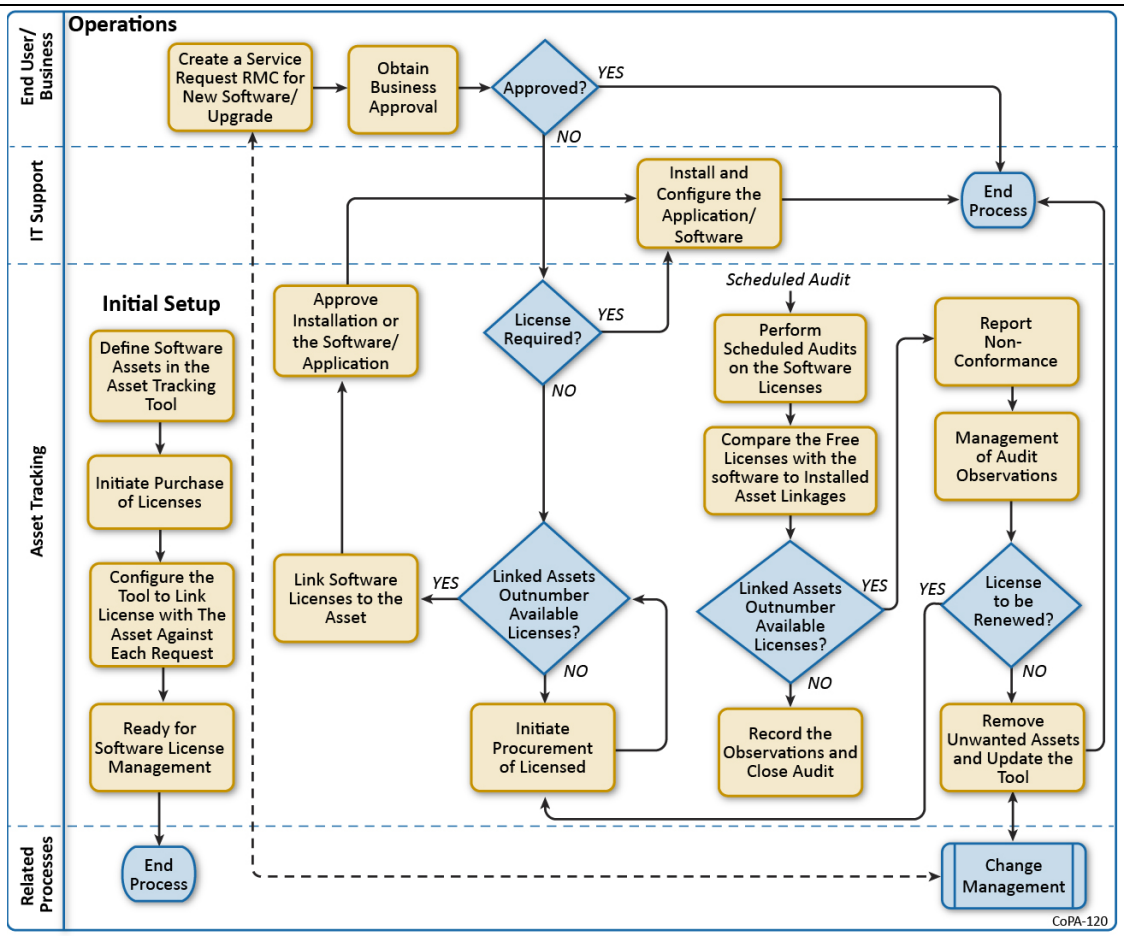


Figure 3.2.1.8-1: Manage Software License Process

The process for license tracking in transition and as an ongoing process involves the following activities:

i) Load all Unisys and Commonwealth software asset license contract information into the [redacted] Asset Management Contract application

ii) Load all software license certificates including the following data in the B[redacted] [redacted] for a Software License:

- certificate
- license type
- entitlements
- manufacturer
- product information

iii) Run discovery through [redacted] to identify all software installations

iv) Run the [redacted] software to build relationships between the discovered software CI's recorded in the [redacted] and the license certificates

v) Run the [redacted] to identify non compliant licenses and inventory for the Unisys and Commonwealth Asset Managers to audit the completeness and accuracy of

the information

vi) Identify any discrepancies in the information and make corrections

vii) Rerun Compliance Reports and 3Rd party software license inventory reports to get signoff from the Commonwealth and Unisys Asset managers that inventory is properly linked to license certificates in the production environment and the information is complete and accurate

viii) Provide notifications to Commonwealth/Agencies/Unisys and other Commonwealth service providers when there are software compliance issues or requirements for licenses to be purchased or retired from analysis of license inventory.

Unisys will coordinate with the Commonwealth to provide compatibility between Commonwealth provided applications related software, and Unisys provided infrastructure software. This will be managed through testing services provided in the Enterprise Services Catalog and ongoing change processes to evaluate the risk of any change in the production environment.

Unisys will notify the Commonwealth Asset Manager(s) of required maintenance agreements in a timely fashion to help confirm that these agreements are in place to support ongoing operations. Unisys cannot be held responsible to any delays on the Commonwealth's part for negotiation these contracts in support of SL14.

2 Continuous Improvement

Unisys follows a detailed set of processes and procedures as describe above to help verify that 3rd party software license information is maintained and reported accurately as an ongoing operation. This is a subset of the Asset Management Process and procedures. The Asset Manager will review all RFC's pertaining to 3rd party software to confirm that the information is properly recorded in the [redacted] he Asset Manager is also responsible for conducting audits of the software license information. The audits will reveal any inaccuracies in the information. Incident tickets and problem tickets will be opened for audit discrepancies. A problem ticket root cause will be determined for each information accuracy type and a change ticket will be opened to correct the root causes for these information problems related to 3rd party software licenses. Change tickets can be opened for any technical, process or personnel related issue. This is how Unisys will continue to maintain and improve the 3rd party software license tracking service's quality, efficiency and effectiveness.

3.B Offeror must provide examples of 3rd Party Software Management initiatives it has implemented and which may be utilized to achieve reduced costs of Services and to meet or exceeded ROI (Return on Investment) analysis projections.

An example of where Unisys has implemented or reduced costs involves the identification and quantification of actual software licenses that were underutilized for the PA Dept. of State who had 1500 Citrix XenApp licenses. After reviewing statistics on usage during the spring 2012 election, it was determined that the highest usage was 200 at any given time. During the full election cycle, the maximum number of users experienced was approximately 600. Unisys recommended to the PA Department of State to reducing software maintenance renewals by 750 licenses thereby yielding a cost savings of $69,600 over two (2) years.

Unisys Team Experience

Unisys has a long history of software license tracking with the Commonwealth and other customers. The Unisys processes for tracking software assets, license renewals are solid and effective to help provide the ongoing operations for the Commonwealth.

Benefits to the Commonwealth

The Unisys Solution for Software License Tracking involves the entire people, process and technology to deliver an effective solution for the Commonwealth. The software license assets are tracked in the [redacted] and linked effectively to the assets in the [redacted] so that the details of where the licenses are located and how they are used are known and reported. Software license reconciliation is performed using the [redacted] This means the Commonwealth can be confident that the risks for management of software licenses are mitigated for maintaining :

- Ongoing operations of the supporting infrastructure tools for Commonwealth/Agency applications
- Compliance for software licenses to help avoid penalties
- Notifications of software license maintenance renewals are processed and sent to asset managers in a timely manner

3.2.2 Technical Services

3.2.2.1 Transition Management (New Customer and/or Services)

The Transition Management service ensures the systematic planning, management, execution, and monitoring of major changes to the datacenter environment(s). This Services offering is to support new customers and/or new Services (i.e. remote file servers, remote databases, etc.). This service offering includes the phased migration of Commonwealth applications to the Offeror's managed service excluding initial transition.

Information and tasks pertaining to the transition of the initial Targeted Datacenters and Agencies can be found in Section 3.3 – Transition Services.

Reference Documentation

N/A

Requirements		Describe Compliance
1.	Transition Management Office - Create a Transition Management Office and team that will be responsible for the migration projects	Offeror must describe its transition management approach and its proposed transition team. Provide resumes for key

	of hardware and applications from the Commonwealth's locations to the new target datacenter environments.	members of the proposed transition team.
2.	Create a computing environment; hardware, software, network systems, peripherals, and devices as required to migrate the Services from the Commonwealth.	Offeror must discuss its approach to migrating the Commonwealth's computing platforms (mainframe, mid-range and x86) and associated infrastructure to the Offeror's proposed solution.
3.	Provide recommendations for the repurpose, replacement, or retirement of existing Commonwealth hardware, software, network systems, and peripheral devices as required after system migrations have been completed.	Offeror must discuss its approach.
4.	Optimize Current Process and Procedures – Coordinate with Commonwealth customer to review and plan for a transition of processes and procedures.	Offeror must describe its overall plan for optimization of the existing processes, procedures, tools, etc. to provide more efficient and effective Services. The description must include approach, plan, and methodologies.
5.	Develop detailed plans to migrate Commonwealth applications, and associated infrastructure from Commonwealth datacenters to the Offeror's datacenters. On a monthly basis, Offeror must create a report to detail the transition projects on the plan, status, risks, and the forecasted transition date.	Offeror must discuss its approach to support the migration of Commonwealth applications to the proposed solution including communicating and reporting on the migration plan, risks and schedule.
6.	Coordinate with Commonwealth applications project teams to plan and execute the application and infrastructure migration plans.	Offeror must discuss its approach.
7.	Revise datacenter disaster recovery plans on the occasion of major changes to the datacenter hardware,	Offeror must discuss its approach.

	software, or network portfolio.	
Continual Process Improvement		
8.□	Reduce service risks.	Offeror must provide examples of previous Offeror initiatives aimed at eliminating or mitigating service risks.
9.□	Improve service quality.	Offeror must provide examples of previous Offeror initiatives aimed at improving service quality.
10.□	Improve client satisfaction.	Offeror must provide examples of previous Offeror initiatives aimed at continually improving client satisfaction.
11.□	Provide service transparency.	Offeror must provide examples of previous Offeror initiatives aimed at providing service transparency; in particular, visibility into the service execution process.
12.□	Ensure service sustainability.	Offeror must provide examples of previous Offeror initiatives aimed at ensuring service sustainability; in particular, efforts targeted at cost containment and cost reductions.
13.□	Improve/reduce cost of service	Offeror must provide examples of previous technology initiatives implemented by Offeror that achieved reduced costs of Services and that met or exceeded ROI (Return on Investment) analysis projections.

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

Introduction

As new customers come on board or services are requested by the existing Commonwealth agencies, Unisys will utilize our standard transition methodologies and processes as the basis to develop the work plan. The size and makeup of the team will depend on the scope and complexity of the projects that have been identified. The project will be very similar to the Data Center Consolidation transition discussed in Schedule F, Section 3.3 within this document. At

the point in time additional customers are transitioned, standard tools and processes will be implemented which will reduce the transition of services to a minimal effort. The data center migration projects will have the same makeup as found in Schedule F, Section 3.3. These teams will work under the direction of the Project Management Office.

1 TPMO, Transition Management Approach

1.A Transition Management Office - Create a Transition Management Office and team that will be responsible for the migration projects of hardware and applications from the Commonwealth's locations to the new target datacenter environments.

1.B Offeror must describe its transition management approach and its proposed transition team. Provide resumes for key members of the proposed transition team.

The transition management approach will be similar to the approach employed during the Data Center Consolidation Program. The tools, processes and team makeup will be the same as the projects required to move DOR, DOH, PSP and DPW. As we initiate these projects, we will review lessons learned in each of those projects and use our continuous improvement process to make them better.

As new opportunities are identified, oversight responsibilities will go to the Project Management Office. Unisys will leverage our global transition team's processes, experience and staff much as we are doing for the Data Center Consolidation Project. The projects will fall under the guidance of the Project Management Office which will be led by [redacted]

The Transition Program Management Office (TPMO) will provide standards, oversight and cross-functional support to the project within the initial Transition and any future transition activity that may occur during steady state. This organization takes advantage of the collective experiences of Unisys, IBM, and prior experience of the staff. The TPMO organization structure, its roles and responsibilities are discussed in detail in Section 3.3.2.1 "Transition Program Management" . For key personnel resumes, please see the Key Resumes tab in Section 5, and for representative resumes, please see the Representative Resumes tab in Section 5.

2 Platform Migration

2.A Create a computing environment; hardware, software, network systems, peripherals, and devices as required to migrate the Services from the Commonwealth.

2.B Offeror must discuss its approach to migrating the Commonwealth's computing platforms (mainframe, mid-range and x86) and associated infrastructure to the Offeror's proposed solution.

Data Center migrations are complex projects which cannot utilize a one-size-fits-all method. As in the plan for migrating applications within the current scope of services, the Migration Project team will gather the application requirements, assess the requirements against the current environment and determine the appropriate course of action to be taken for each application and technical environment in scope. The possible solutions will include data transfer methodology such as over the wire to existing or new equipment in the target data center or lift-and-shift via tape backup or whole storage frame as appropriate. This will also include a determination on the best approach for migrating the servers either through lift-and-shift, over-the-wire operating system migration or greenfield installs onto seed hardware. The Capacity on Demand solution provided by Unisys can support a faster implementation project. For more information on Capacity on Demand, please see Section 3.2.5.1.

More detailed information regarding the Unisys transition approach can be found in Schedule M.

3 Repurposing, replacement, retirement

3.A Provide recommendations for the repurpose, replacement, or retirement of existing Commonwealth hardware, software, network systems, and peripheral devices as required after system migrations have been completed.

3.B Offeror must discuss its approach.

1) Recommendations for Technology Reuse after Migration

a. As part of the Transition planning process for each data center migration, Unisys will review the hardware; software; except applications; network systems, and peripherals devices to provide recommendations for the technology post-migration. The Technology Refresh activities will be used as a basis for the analysis and development of the recommendations. The following recommendations may be used by a subset of the options presented as part of the review.

i. Repurpose

1. Reusing the technology as a part of an Agency's Managed Only infrastructure at the Unisys managed data center. The technology may not be used in the same function as it was used previously, but it will be used until it is refreshed through the an approved Technology Refresh plan or retired when its function is no longer required.

ii. Replacement

1. Technology which has reached an end of life due to age or from technical changes in the architecture, but does have a match in the current Unisys Fully Managed service offerings will be recommended for replacement. Unisys will work with the Commonwealth to identify replacement technology. The recommendation may also generate additional service offerings.

iii. Retire

1. Technology which has reached end of life due to age or from technical changes in the architecture and has a functional match in the current Unisys Fully Managed service offerings will be recommended to be retired after its function has been migrated to Unisys Fully Managed hardware or software services.

4 Process Optimization

4.A Optimize Current Process and Procedures – Coordinate with Commonwealth customer to review and plan for a transition of processes and procedures.

4.B Offeror must describe its overall plan for optimization of the existing processes, procedures, tools, etc. to provide more efficient and effective Services. The description must include approach, plan, and methodologies.

The Transition of Services Project(s) will be dedicated to understanding and documenting the Commonwealth's current state environment. When these tasks are completed, the team will

turn its focus to identifying the gaps between current processes and the Unisys Team's best practices in order to develop a strong detailed plan for a seamless implementation and conversion to those appropriate best practices. The Unisys Team will apply their current experience and knowledge of the Commonwealth will enhance their ability to identify opportunities for transition improvements and expedite the transition. For a more detailed explanation please see Section 3, Attachment 89 "Schedule M: Detailed Transition Plan". Additional information on the Unisys Team's approach to Continuous Improvement can be found in Schedule F, Section 3.2.1.1.6.

During the initial transition of services project, the Unisys Team will meet with the Commonwealth and key agency representatives to gain insight needed to create an effective plan, and then to obtain concurrence on the plan.

5 Application Migration

Applications are the central focus of the Unisys Migration Strategy. As additional opportunities for consolidation are identified, the Unisys Team will continue to utilize the same processes as the initial transition program that can be found in Schedule F, Section 3.3.

5.A Develop detailed plans to migrate Commonwealth applications, and associated infrastructure from Commonwealth datacenters to the Offeror's datacenters.

The application migration processes for additional agencies and services will begin with a standard template and then customized for each situation. The final resulting plan will be developed based on number of factors including timing, planning, testing and method of migration, and will always be based on the specific needs and requirements of the applications being migrated. For more details, please see Schedule F, Section 3.3.

5.B On a monthly basis, Offeror must create a report to detail the transition projects on the plan, status, risks, and the forecasted transition date.

Similar to the migration projects that are currently in scope, the Unisys Team will provide weekly status which includes a current status of the project, a risk register which includes mitigation strategies and the up to date schedule. For additional details, please see Schedule F, Section 3.3.

5.C Offeror must discuss its approach to support the migration of Commonwealth applications to the proposed solution including communicating and reporting on the migration plan, risks and schedule

Unisys has developed a detailed multi-tier communication plan for the Data Center Transition services. Unisys will utilize a similar communications plan for the transition of new customer or new services. For additional information, please see Schedule F, Section 3.3

6 Application Migration Coordination

Coordinate with Commonwealth applications project teams to plan and execute the application and infrastructure migration plans.

Offeror must discuss its approach.

It is expected the Commonwealth application project teams will continue to be an integral part of the transition projects and attend all project meetings. The Unisys Team requests that an application owner be named for each application to be migrated. This role will be responsible for and authorized to make decisions on behalf of the application project team and users. In addition, the application owner will be expected to support all communications with the application project team and user community not directly involved with the project.

7 DR, Disaster Recovery Plan

7.A Revise datacenter disaster recovery plans on the occasion of major changes to the datacenter hardware, software, or network portfolio.

7.B Offeror must discuss its approach.

The specifics of the Commonwealth's new DR Infrastructure on Demand are detailed in the Schedule F, Section 3.2.5.3 DR Infrastructure on Demand section.

The Unisys IT Risk Manager in the Program Management Office will oversee an agency-by-agency review of each Disaster Recovery plan during transition. As part of this review, each Agency plan will be entered into the new online DR planning tool, Living Disaster Recovery Planning System (LDRPS). This transition process populates the LDRPS with the DR runbooks and provides the initial capture of the Commonwealth's Disaster Recovery capacity required.

Following transition, the Unisys IT Risk Manager in the Program Management Office will oversee the maintenance of the Commonwealth's new online disaster recovery tool as part of our proposal. The IT Risk Manager and DR Coordinators have broad oversight at the agency level and meet with agency leaders regularly to review, update, and maintain all Agency Disaster Recovery plans within the new online DR planning tool. As part of this governance the IT Risk Manager will review new service offerings to validate that new Customers and Services have been incorporated into Agency-level Disaster Recovery Plans. The addition of new Customers or Services will also initiate an action to schedule an oversight review with the appropriate agency-level leader.

The Unisys Team responsible for maintaining the Unisys-managed Disaster Recovery will rely on review of changes to the online Disaster Recovery planning tool, regular Disaster Recovery trend reports and new project roster reviews to gauge and maintain adequate supply and appropriate tiers of service in the Disaster Recovery sites.

Ultimately the above actions are tested for quality and completeness during two annual tests that the Commonwealth stipulates. Upon completion of the tests the Disaster Recovery Testing team will review all DR test results as part of the regular remediation and improvement cycles that follow any DR testing.

Continual Process Improvement

Unisys recognizes the significant importance of Quality and Continuous Service Improvement to:

1. Reduce service risk,
2. Improve service quality,
3. Improve client satisfaction,
4. Provide service transparency, and
5. Improve/reduce costs of service.

Through a continuous cycle of evaluation and improvement within an IT infrastructure, Unisys views quality and continuous service improvement as a critical success factor in driving customer satisfaction for the Commonwealth IT infrastructure. Each of the continuous service improvement areas identified above are driven through the tight integration of the following organizations, industry tools, proven processes and quality deliverables:

1. Service Excellence Office,
2. Quality Plans: transition and steady state service delivery
3. Industry standard frameworks and methodologies: ITIL, ISO, SSL
4. Industry accepted measurement tools
5. Continuous Service Improvement & Innovation Processes (CSIIP)
6. Risk management, audits and business continuity management
7. Client Satisfaction Surveys and Knowledge Management Portal

Collectively this represents Unisys Integrated Quality Plan for the Commonwealth of Pennsylvania.

Specifics on each of these areas are outlined in Schedule F, Section 3.2.1.1.6 Continuous Service Improvement. Highlights from this section are outlined below and requested service examples are provided at the end of this section.

8 CI Service Risk

8.A Offeror must provide examples of previous Offeror initiatives aimed at eliminating or mitigating service risks.

Identifying project risks, developing mitigation strategies, and developing contingency plans are vital to a successful project. Risk management is continuous and requires that proactive steps be built into the Project Management Plan. The Unisys Team will complete a detailed Risk Management Plan in conformance with the Unisys Services & Solution Delivery Framework (SDF) methodology. This will occur early during project or migration startup and create one of the first project deliverables. The SDF follows the approved approach to risk management based on the Project Management Institute (PMI) Standard—PMBOK. The Risk Management Plan will detail the process so all project participants have a clear and common understanding of how risks will be managed and their individual responsibilities. The SDF provides the

processes, techniques, and tools to support project management. Our four guiding principles are:

- Clear goals are essential for successful projects.
- Adherence to formal and constantly improving best practice processes will provide that all solutions and deliverable products meet their stated requirements.
- Planning and scheduling of all tasks and resources and subsequent monitoring, control, and reporting are essential to solution delivery.
- Agreement on deliverables and definition of an effective change management process are essential to achieving the project's goals.

Our framework provides best practices, templates, and guidelines for all project phases from the initial proposal, transition and migration, through implementation and project closeout. The risk management process is divided into two areas:

1. Risk Management Planning
   This area focuses on how to approach, plan, and execute risk management activities, including identification, assessment, and management of potential risks.
2. Risk Management Control
   This area focuses on the implementation of the processes and actions defined during risk planning. This includes the process for tracking risks, identifying new risks, executing risk response plans, and evaluating their effectiveness.

Risk management, independent quality audits, and business continuity management are integral quality management processes. Unisys is committed to managing risks and facilitating the achievement of business objectives the adherence to quality processes. We mitigate risk through the implementation of tight quality controls: standard policies, procedures, roles, risk assumptions, issues, and definitions, etc.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

9 CI Service Quality

9.A Offeror must provide examples of previous Offeror initiatives aimed at improving service quality.

Unisys will integrate new agencies, customers and services into our total quality approach. The quality approach begins with the Service Excellence Office. The SEO function provides definition and oversight of all ITIL process management and analysis functions. Process managers and analysts working in the Service Excellence Office are responsible for auditing process effectiveness, ensuring that service delivery teams comply with proper execution of processes, and analyzing process trends for anomalies. Continuous service improvement programs in collaboration with Commonwealth agencies are managed by the Service Excellence Office.

Through our Continuous Service Improvement and Innovation Process (CSIIP), the SEO reviews, analyzes and makes recommendations on improvement opportunities in each ITIL lifecycle phase. Unisys will leverage Six Sigma Lean tools and methodologies as well as ISO Certified internal audits to measure and maintain the highest quality services to the

Commonwealth.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

10 CI Client Satisfaction

10.A Offeror must provide examples of previous Offeror initiatives aimed at continually improving client satisfaction.

Client satisfaction is extremely important to Unisys and a key focus in our IT solution. The SEO will integrate new agencies, customers and services into our multi-pronged client satisfaction approach that includes Service Desk surveys on the caller's experience, an overall agency satisfaction survey, and quarterly surveys with the Office of Administration. Data collection will be gathered across multiple levels to gain a clear understanding of the Commonwealth's satisfaction with the IT Services being provided.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

11 CI Service Transparency

11.A Offeror must provide examples of previous Offeror initiatives aimed at providing service transparency; in particular, visibility into the service execution process.

The service organizations will use standardized ITSM services processes, IT monitoring & automation tools. ITSM processes will be documented in the Commonwealth Computing Procedures Manual (CCPM). The CCPM will be available to Commonwealth approved staff on the Knowledge Management Portal (KMP) providing desired transparency into service execution processes. Through the Real-time Dashboard, the Commonwealth will have access to current operational performance of their application infrastructure.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

12 CI Service Sustainability

12.A Offeror must provide examples of previous Offeror initiatives aimed at ensuring service sustainability; in particular, efforts targeted at cost containment and cost reductions.

Service will be sustained by integrating any new agencies, customers, or services into our standard operational and quality processes and methodologies leveraging ITIL processes, creating quality project plans, utilizing industry accepted measurement and monitoring tools, analyzing trending reports and providing proactive continuous service improvement throughout the IT lifecycle. These processes and methodologies enable new Commonwealth services to experience and sustain IT services and client satisfaction.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

Unisys continuous improvement examples

In 2010, the Integrated Enterprise System (IES) ERP environment was transitioned into the DPH by the Unisys Team. Leveraging lessons learned from the Pennsylvania Liquor Control

Board ERP transition of 2008, project plans were more formally documented and communication methods were improved for the IES migration. We are routinely learning from project activities. After the implementation of IES, the DPH team implemented a formal quality improvement program with IES consisting of a 48 question written survey, in-depth analysis, a formal management interview and joint development and tracking of action plans. This has resulted in a 30% increase in overall agency satisfaction in less than 2 years.

13 CI Improve or Reduce Cost

13.A Offeror must provide examples of previous technology initiatives implemented by Offeror that achieved reduced costs of Services and that met or exceeded ROI (Return on Investment) analysis projections.

Unisys is establishing a Service Excellence Office to proactively manage quality, continuous service improvement, ITIL process management, and customer satisfaction through a comprehensive quality plan that specifically addresses all of these areas. We believe this is a key differentiator in our partnership with the Commonwealth. Through this new organization and these quality plans, Unisys provides best in class services and the highest customer satisfaction experience, while reducing overall costs to the Commonwealth.

Unisys Team Experience

Unisys and IBM regularly handle large-scale incremental workload additions and deletions for data center outsourcing customers around the world. Most recently, we managed the integration of two brand-new Commonwealth customers into the DPH, the Pennsylvania Liquor Control Board and the Integrated Enterprise System (IES), both critical Commonwealth ERP systems. Additionally, we have performed significant technology refreshes, the largest of which was the transformation of 2008 and 2009, which provided new infrastructure to every agency supported in the DPH.

In 2012, the DPH team migrated critical applications for four agencies from the IBM z10 mainframe platform to the IBM z196 platform. This migration was conducted using the same project plans that were used to conduct the move to the IBM z10 in 2009 during transformation. All agency workload was relocated with minimal risk or disruptions.

It is through projects like these that the Unisys Team has gained considerable knowledge of agency configurations, priorities, and business needs. This knowledge will help us to effectively plan successful transitions for Commonwealth workload regardless of the scope and complexity.

Benefits to the Commonwealth

Unisys and IBM have worked together on migrations, technology refreshes, and changes in scope for the Commonwealth agencies for several years. Our processes have been honed to reduce risk and minimize downtime.

Unisys, IBM and Deloitte know the Commonwealth culture, know many of their environments and have strong relationships with the agencies. This knowledge and the relationships that have been forged over the years of working together give this team a significant advantage. We

know what to expect from each other, we know how each other works and we have large, strong companies behind us with a strong understanding of the industry and technologies.

Throughout the program you will no doubt see this team bringing in new team members who bring with them industry experience from other large companies. The synergies of combining the Commonwealth, Unisys, IBM, Deloitte and the diverse experience of the new team members will no doubt provide a world class solution for the Commonwealth which we believe can be achieved faster, with higher quality and a lower cost.

3.2.2.2 Infrastructure Architecture

The Infrastructure Architecture service will define and manage the scope and design of the infrastructure architecture for the computing systems to support the evolving needs of the Commonwealth. This range of Services includes design of the mainframe, mid-range, x86 servers, (both physical and virtual), Local Area Network (LAN), storage, backup systems, and the DR systems. The design will also need to detail how the most current data will be restored to the targeted DR system.

Efforts are underway to re-write many of the Commonwealth business applications. For example, some of the mainframe applications are being migrated to newer server based systems. The Offeror must consider the planned retirement of some of the mainframe workload, and at the same time consider the offsetting growth in other server platform environments.

At the direction of the Commonwealth, the Offeror must transition Commonwealth based computing infrastructure to one of the datacenters. The Offeror must work with the Commonwealth agencies to understand the systems involved, and the timeframe of these migrations. Working with the Commonwealth agencies, the Offeror must provide the design, project management, hardware and technical support required to test and migrate these systems to the new production environment. At its discretion, each agency will provide the applications staff to support the migrations.

The Infrastructure Architecture service will review and recommend hardware, software, and the technical configurations required to build the requested infrastructure environments. Prior to migrating each of the current application workloads to the new target infrastructure, the Offeror must work with each Commonwealth agency to develop a mutually agreed to Acceptance Test Plan that includes the testing of application infrastructure performance characteristics.

Reference Documentation

Exhibit A - Commonwealth Network Environment

Exhibit(s) B.1 through B.6 - Data PowerHouse (DPH) Exhibits

Exhibit(s) C.1 through C.13 - Department of Public Welfare (DPW) Exhibits

Exhibit(s) D.1 through D.15 - Enterprise Datacenter ([redacted] Exhibits

Exhibit(s) E.1 through E.43 - Department of Labor & Industry (DLI) Exhibits

Exhibit(s) F.1 through F.4 - Department of Health (DOH) Exhibits

Exhibit(s) G.1 through G.16 - PA State Police (PSP) Exhibits

Exhibit(s) H.1 through H.8 - Department of Revenue (DOR) Exhibits

Exhibit(s) I.1 through I.13 - Commonwealth SAP Environment - Integrated Enterprise Services (IES) Exhibits

Exhibit L - Master Application Inventory

Schedule J.1 - Datacenter Service Level Management

Exhibit(s) M.1 through M.7 - Department of Corrections (DOC) and Pennsylvania Board of Probation and Parole (PBPP) Exhibits

Exhibit(s) N.1 through N.2 - PennDOT Exhibits

Requirements		Describe Compliance
1.	Define the infrastructure technology Services to be offered. Provide a detailed list of Services and computer platforms to be provided to the Commonwealth.	Offeror must describe its ability to provide infrastructure technical Services across multiple computing platforms (mainframe, mid-range and x86). Include explanation of different service tiers (e.g. gold, silver and bronze).
2.	Design and build the IT infrastructure architecture to support the Services required by the Commonwealth. Design will provide as much interoperability and open standards as possible. All designs must be approved by the Commonwealth. Provide the design in a Visio format to the Commonwealth for review and approval prior to execution. This diagram will be dated and maintained as Services are altered for the duration of the engagement.	Offeror must describe its methodology and approach to infrastructure architecture design Services. Offeror must describe the documentation requirements, timelines for both normal requests and emergency situations. Offeror must provide representative sample of infrastructure design documentation.
3.	Address CJIS and Criminal History Record Information Act (CHRIA) requirements for agency application infrastructure designs where required. Some agency application infrastructure designs (e.g. PSP) require additional security and encryption level requirements imposed by CJIS.	Offeror must provide examples of its experience in designing infrastructures that adhere to CJIS and CHRIA requirements.
4.	SAP Infrastructure Design The Offeror's proposed target infrastructure design for the	Offeror must provide examples of its experience in sizing and design of SAP infrastructures. All designs must be approved

	Commonwealth's SAP environments must include a certified SAP sizing report prior to migration of the systems.	by the Commonwealth.
5.	Commonwealth Wide Area Net connectivity. Provide connectivity from the datacenter to the Commonwealth Network. Redundant network links are required.	Offeror must describe its capabilities to connect to and manage the requisite connections. Explain ongoing network support Services to manage these links including the ability to increase capacity as needed to support changes in the application infrastructure requirements.
6.	Develop Acceptance Test Plan. Prior to migrating each of the current application workloads to the new target infrastructure, the Offeror will work with each Commonwealth Agency to develop a mutually agreed to Acceptance Test Plan that includes the testing of application infrastructure performance characteristics.	Offeror must discuss its proposed approach to systems acceptance testing and include the approach to performance testing.
7.	Provide System Acceptance testing. The Offeror must conduct system acceptance testing, and provide the Commonwealth with written verification prior to declaring the system is fit for use. This acceptance test must include validation of infrastructure performance against system performance characteristics agreed to by both parties.	Offeror must discuss its proposed approach to systems acceptance testing.
8.	Ready for use certification	Offeror must provide the Commonwealth with written verification prior to declaring the Service is ready for use. The Service will not be considered ready for use until written acceptance is obtained from the Commonwealth.

9.	Support User Acceptance Testing.	Offeror must support the Commonwealth's user acceptance testing. The Commonwealth shall not be charged for Services until written acceptance is obtained from the Commonwealth.
10.	Provide Application Infrastructure environments. Provide non-production and production environments for each of the application computing platforms. The non-production environments will be used for testing new technologies and applications, updates and upgrades, prior to production implementations.	Offeror must describe its approach to the design and management of multiple application infrastructures. Identify proposed solution to individual or consolidated non-production environments for agencies.
11.	Design service lifecycle. Provide the infrastructure design for the Services and platforms to be offered. Provide ongoing evaluation and recommend new technologies to enhance, improve, and reduce the cost of Services.	Offeror must describe its approach to provide service lifecycle design for all Commonwealth computing platforms and associated infrastructures. Offeror must provide the Commonwealth and its agencies the ability to request new technologies to be available.
12.	Define Technical Support functions.	Offeror must list Offeror's support staff levels required to plan, manage, and operate the IT infrastructure, based on the various service levels offered.
Continual Service Improvement		
13.	Reduce service risks.	Relative to the service in question, Offeror must provide examples of previous Offeror initiatives aimed at eliminating or mitigating service risks.
14.	Improve service quality.	Offeror must provide examples of previous Offeror initiatives aimed at improving service quality.

15.	Improve client satisfaction.	Offeror must provide examples of previous Offeror initiatives aimed at continually improving client satisfaction.
16.	Provide service transparency.	Offeror must provide examples of previous Offeror initiatives aimed at providing service transparency; in particular, visibility into the service execution process.
17.	Ensure service sustainability.	Offeror must provide examples of previous Offeror initiatives aimed at ensuring service sustainability; in particular, efforts targeted at cost containment and cost reductions.
18.	Improve/reduce cost of service	Offeror must provide examples of previous technology initiatives implemented by Offeror that achieved reduced costs of Services and that met or exceeded ROI (Return on Investment) analysis projections.

Deliverables

Deliverables are defined in **Schedule K - Key Program Deliverables**

Offeror Response

Introduction

The Unisys team understands that this RFP is much broader and far more significant than simply consolidating infrastructure. In the same way, the Infrastructure Architecture service is about more than just providing platforms and technologies to the Commonwealth. Properly designed and implemented, architecture services become a powerful tool to be utilized by the Commonwealth to meet its compute needs now and in the future, while driving efficiency, scalability and compatibility into the enterprise. The essence of the Infrastructure Architecture service is optimized “compute services,” supporting the Commonwealth’s applications by providing the right service in the right capacity when it is needed and in a way that is cost effective, transparent, and secure.

As you will see below, the Unisys team has selected a common hardware platform, the IBM Flex system, for all AIX, Windows and Linux servers. This platform will deliver all IaaS and Fully Managed and Capacity on Demand services. Using a common hardware platform eliminates risk in interoperability, bringing the Commonwealth a common deployment process across all server platforms via the Enterprise Services Catalog. Standardized hardware platforms also allow powerful workflow automation to be deployed very quickly. Additionally, compute workloads on AIX, Linux and Windows can now share the same blade chassis backplane where necessary and mixed workloads can be completely isolated down to the chassis level. This confirms that the Unisys team can respond quickly and confidently to any future regulatory or compute

requirements in the future.

From a storage perspective, the Unisys team has taken the approach of providing choice to the Commonwealth. No longer is it necessary to sacrifice the benefits of one storage solutions to choose another. Both IBM and EMC solutions are available to the Commonwealth, again reducing the risk of incompatibilities and increasing operational stability and performance. By utilizing storage virtualization, the Unisys team will deploy a storage solution capable of isolation when needed, maximizing reuse of storage, and providing powerful building blocks on which to run disaster recovery.

The Unisys team's Infrastructure Architecture service is designed to provide power, flexibility and agility, stability and security to the Commonwealth in a cost effective manner. When the transition to the new service is complete and the benefits are realized, the industry will recognize this initiative for what it is—a paradigm shift in service delivery for state government.

1 Infrastructure Service Tiers

1.A Define the infrastructure technology Services to be offered.

The Unisys Team offers a solution that provides these managed infrastructure technology services:

- Unisys OS2200
- IBM zSeries
- IBM iSeries
- Network
- Security
- Server/Midrange
- Storage
- Backup
- Disaster Recovery
- IaaS Services
- Data center Facilities

1.B Provide a detailed list of Services and computer platforms to be provided to the Commonwealth.

Figure 3.2.2.2-1 below shows the computer platforms the Unisys team will deploy the following technologies as part of the Infrastructure Architecture services. Following, there is a description of each of the technologies, and overview of how the Unisys team will utilize those technologies, and the section of this proposal where further information can be found.

Figure 3.2.2.2-1 - Detailed List of Infrastructure Services

- [redacted] blade technologies will be utilized by the Unisys team to provide all x86 server services to the Commonwealth. The Flex Systems form the infrastructure for both virtualization and physical servers. Utilization of this technology provides the Commonwealth with power and agility, able to meet the compute needs of the Commonwealth now and into the future. For more information on how the Unisys team will utilize x86 Pure Systems, please refer to Schedule F, Sections 3.2.4.1, Windows Support; 3.2.5.1, Server Capacity on Demand, and the Linux section of 3.2.4.4 Unix Support.

- [redacted] is an AIX variant of the Flex Systems line of blade servers. The Unisys team will deliver all AIX services referenced in this RFP on this platform. Combined with the x86 Flex, the Unisys team brings to the Commonwealth the unique ability to co-locate AIX, Linux and Windows workloads in the same blade chassis. For more information on the use of the IBM pSeries Flex Systems, please see Schedule F, Section 3.2.4.4 Unix Support.

- [redacted] processor based mainframe which the Unisys team will utilize to deliver Unisys mainframe services to the Commonwealth. Please see Schedule F, Section 3.2.4.5 Mainframe Support for more information.

- [redacted] is an x86 processor based mainframe which the Unisys team will utilize to deliver Unisys mainframe services to the Commonwealth. Please see Schedule F, Section 3.2.4.5 Mainframe Support for more information.

- [redacted] is the mainframe on which the Unisys team will deliver both IBM mainframe and zLinux services to the Commonwealth. Please see Schedule F, Section 3.2.4.5 Mainframe Support for more information.

- [redacted] designed for high performance, reliability, and flexibility and will be utilized by the Unisys team to provide storage to the [redacted] mainframe. Please see Schedule F, Section 3.2.4.5 Mainframe Support for more information.

- [redacted] is a high-end disk storage system designed to provide consistent performance, high availability and simple usability. The [redacted] will be one of the storage platforms the Unisys team will utilize to deliver storage services to the Commonwealth. Please see Schedule F, Section 3.2.4.2 Storage Management for more information.

- [redacted] provides storage virtualization by presenting itself to server hosts as a storage device, and to storage devices as a server host. Utilization of the [redacted] brings power and agility to the Commonwealth at the storage layer, and compliments the virtualization at the server layer. Please see Schedule F, Section 3.2.4.2 Storage Management for more information.

- [redacted] is a virtualization engine (virtual tape library) for [redacted] mainframes that uses disk drives for cache to accelerate backup operations. The design is intended to protect data while having shorter backup windows. End-to-end encryption protects data in motion, on cache hard drives and on tape. Please see Schedule F, Section 3.2.4.2 Storage Management for more information.

- [redacted] is an enterprise class storage system, used by the Unisys team to deliver storage to open systems and [redacted] mainframes. Please see Schedule F, Section 3.2.4.2 Storage Management for more information.

- [redacted] Series storage devices provide both file and block storage services. The Unisys team will utilize the [redacted] Series as one of the storage options available to the Commonwealth through the Enterprise Services Catalog. Please see Schedule F, Section 3.2.4.2 Storage Management for more information.

- [redacted] as one of the options to provide the Commonwealth tape based backup and recovery services. Please see Schedule F, Section 3.2.4.2 Storage Management for more information.

- [redacted] will be used by the Unisys team to deliver VTL services for the [redacted] mainframes. Please see Schedule F, Section 3.2.4.2 Storage Management for more information.

- [redacted] is equivalent in many ways to the [redacted] capable of storage virtualization and replication of data and virtual machines across data centers. The Unisys team will use [redacted] as one of the storage service options for the Commonwealth. Please see Schedule F, Section 3.2.4.2 Storage Management for more information.

- [redacted] is a continuous data protection solution offered by [redacted] which supports asynchronous and synchronous data replication of block based storage. Please see Schedule F, Section 3.2.4.2 Storage Management for more information.

- [redacted] – The Unisys team will utilize [redacted] to perform de-

duplication of disk based backup. Please see Schedule F, Section 3.2.4.2 Storage Management for more information.

- [redacted] will be utilized by the Unisys team to provide tape based backup and recovery services to the Commonwealth. Please see Schedule F, Section 3.2.4.2 Storage Management for more information.

- [redacted] will be utilized by the Unisys team to provide tape based backup and recovery services to the Commonwealth. Please see Schedule F, Section 3.2.4.2 Storage Management for more information.

- [redacted] will be utilized by the Unisys team to provide tape based backup and recovery services to the Commonwealth. Please see Schedule F, Section 3.2.4.2 Storage Management for more information.

- [redacted] is a web-filtering, content caching internet perimeter security device for large enterprises. The Unisys team will deploy [redacted] to provide internet security and content filtering to the Commonwealth. Please see Schedule F, Section 3.1.2 Network and Security Architecture.

- [redacted] is a distributed sniffer system. The Unisys team will utilize [redacted] to quickly analyze problems on the network or to isolate problems specific to an application. Please see Schedule F, Section 3.1.2 Network and Security Architecture.

- [redacted] Nexus Routers and Switches – Long recognized as a leader in data center networking, the Unisys team will utilize [redacted] Nexus routers and switches to provide the Commonwealth LAN and WAN services. Please see Schedule F, Section 3.1.2 Network and Security Architecture.

- [redacted] Firewalls – The Unisys team will deliver network firewall services to the Commonwealth using [redacted] Firewalls. The [redacted] firewalls chosen by the Unisys team allow advanced functionality at the firewall layer. Please see Schedule F, Section 3.1.2 Network and Security Architecture.

- [redacted] load balancers deployed by the Unisys team will offer the Commonwealth ubiquitous load balancing of applications across data centers. Please see Schedule F, Section 3.1.2 Network and Security Architecture.

1.C Offeror must describe its ability to provide infrastructure technical Services across multiple computing platforms (mainframe, mid-range and x86). Include explanation of different service tiers (e.g. gold, silver and bronze).

The Unisys team has extensive experience operating and managing complex, mixed computing environments globally. This experience, combined with a common IT Service Management Platform and ITIL V3 aligned processes designed to maximize the capabilities of that platform, allow the Unisys team to manage a complex environment such as the Commonwealths, while increasing efficiency and bring savings year over year to the Commonwealth.

From the perspective of technical capabilities and the ability to provide Infrastructure Architecture services for the Commonwealth, the Unisys team has more experience on the critical platforms that house the Commonwealths applications than any other provider in the

industry. Whether it is Unisys or IBM mainframes, AIX, Windows, Linux or storage, the Unisys team can bring expertise and experience from level 1 though level 4. Additionally, the Unisys team has either in house level 4 expertise, or the close relationships that can be leveraged to bring that expertise to the Commonwealth.

The Unisys Infrastructure Architecture solution, combined with a common IT Services Management platform and ITIL V3 processes, provides a tightly integrated solution to manage the availability standards required in the Commonwealth RFP. The table below describes the characteristics associated with each of our levels of service.

Tiered Support Level	Description
Platinum	• **Provides 99.999% Application Infrastructure Availability** • **Server is monitoring via** [redacted] • **Fully Managed Services** • **Asset Tracked In CMDB** • **Requires 3 active servers load balanced and geographically dispersed**
Gold	• **Provides 99.99% Application Infrastructure Availability** • **Server is monitoring via** [redacted] • **Fully Managed Services** • **Asset Tracked In CMDB** • **Requires 2 active servers load balanced and geographically dispersed**
Silver	• **Provides 99.9% Application Infrastructure Availability** • **Server is monitoring via** [redacted] • **Fully Managed Services** • **Asset Tracked In CMDB**
Bronze	• **Provides 99.4% Application Infrastructure Availability** • **Server is monitoring via** [redacted] • **Fully Managed Services** • **Asset Tracked In CMDB**
Basic	• **Provides 98.5 % Application Infrastructure Availability** • **Server is monitoring via** [redacted] • **Fully Managed Services** • **Asset Tracked In CMDB**

Based on the tired Service Levels, the Unisys team will provide the Commonwealth a tiered approach to the UNIX environment. For the Platinum (99.999%) support level the Unisys team will enlist all three Unisys data center to provide an active-active-active solution with all components being fully redundant and each site supporting 50% of the peak load The three sites will provide redundancy and will allow for planned outages in one site at a time. For the Gold (99.99%) level support, the Unisys team will enlist two of the Unisys data centers and provide an active-active solution with all components being fully redundant with automatic failover. For Silver (99.9%) the Unisys team will require only one of the Unisys data centers for production. For Platinum, Gold and Silver support levels, clustering and/or load balancing (either application or infrastructure level) will be required. For Bronze (99.4%) and Basic support a single data center is sufficient and clustering is not required.

More details on the specific components required to meet the service tiers can be found in Schedule C – Services Catalog.

2 Architectural Design Service, sample

2.A Design and build the IT infrastructure architecture to support the Services required by the Commonwealth. Design will provide as much interoperability and open standards as possible. All designs must be approved by the Commonwealth

As described in Schedule F, Section 3.2.1.5 Technical Architecture, Unisys had two governing principles in the service design for the Commonwealth: first, standardization of the compute environment, as much as possible, in each of the hardware towers, and second, to leverage technology that can be redeployed rapidly to other purposes. The Unisys Team believes that from a server perspective, this is the easiest way to achieve the Commonwealth's goal of interoperability.

The infrastructure architecture services rely on the interoperability in the service design to provide uniform tools to manage and monitor the infrastructure services. The Unisys suite of infrastructure monitoring tools includes the Nagios collectors which use open standard SNMP protocols to monitor hardware and service components. The tool suite also includes the [redacted] tool, which provides storage management by relying on the open standard "Storage Management Initiative – Specification" SMI-S storage management protocol established by the Storage Network Industry Association.

While not technically an open standard the [redacted] provides a means of managing components across many vendor product lines and report on availability, capacity, and performance.

The Unisys Infrastructure Architecture uses an online Real-time Dashboard to provide the Commonwealth with access to automated data collection, visualization of graphical results, and focus on high-impact critical application components.

The Infrastructure Architecture relies upon hardware components that present opportunities for interoperability. The [redacted] for instance supports Windows, Linux, and AIX in virtual or physical instances. The proposed SAN solution provides interoperability between storage provided by many vendors and to all provided servers and tape drives.

By maintaining an architectural governance process which includes the Commonwealth's approval, the Unisys Team provides transparency into the overall architecture and design activities. The overall approach for architecture development including the Commonwealth's approval is in Section 3.2.1.5 Technical Architecture and the types of service requests are described in Section 3.2.1.1.5 Additional Planning Services.

2.B Provide the design in a Visio format to the Commonwealth for review and approval prior to execution. This diagram will be dated and maintained as Services are altered for the duration of the engagement.

As a part of the overall solution documentation, the Agency Infrastructure Architect will create a Visio diagram that provides a view of the solution's topology for review and approval prior to implementation. This diagram will be maintained in the Services Portal with version control to reflect any subsequent changes to the configuration.

2.C Offeror must describe its methodology and approach to infrastructure architecture design Services.

The Unisys Team uses a design methodology which covers activities from the initial requirements gathering to the final approval by the Commonwealth to maintain the consistency in the designs and service development.

The infrastructure architecture design services flow from the ITIL V3 Service Design process described in Schedule F, Section 3.2.1.5 Technical Architecture Requirement 2.

2.D Offeror must describe the documentation requirements, timelines for both normal requests and emergency situations.

Offeror must provide representative sample of infrastructure design documentation.

As the Commonwealth's business needs change, different types of requests may be submitted to the Unisys team for various solutions and activities. These requests can go from activities to perform regular pre-approved functions to complex solution development or investigations supporting Agency projects or plans.

The Unisys Enterprise Architecture group follows ITIL-based Service Design processes to gather, formalize, and deliver Infrastructure Architecture to meet the Commonwealth's strategic business initiatives.

The timeline to deliver the Infrastructure Architecture design solutions depend on a number of factors, including the type of request, the scope of request, urgency and the complexity. For example, Unisys expects to develop and present a solution within 2-4 weeks on average for a service request of an average complexity within one functional area. Additional details and guidelines are outlined in Schedule F, Section 3.2.1.1.5 Additional Planning Services.

The Enterprise Architecture uses standard documentation to capture Commonwealth and Agency requirements within Unisys Architecture templates that are build out to become infrastructure design documents. See **Attachment F-3 – AMOS Enterprise Architecture Project SOW** and **Attachment F-4 Technical Architecture Deliverable Guide** for two sample architecture template documents that are used to guide Unisys architects in the design of infrastructure architecture.

3 CJIS and CHRIA Examples

3.A Address CJIS and Criminal History Record Information Act (CHRIA) requirements for agency application infrastructure designs where required.

As part of the Transition planning and solution request activities, Unisys will work with the Commonwealth agencies to identify the regulatory requirements, including CJIS and CHRIA, which must be supported within the infrastructure architecture to deploy the agency applications on Unisys supported infrastructure. The Commonwealth's regulatory interpretations are an important part of how Unisys will identify and recommend the appropriate solution to meet and maintain the Commonwealth's regulatory compliance.

Unisys has included several options, including data in motion and data at rest encryption, to protect regulated data. As Pennsylvania State Police (PSP) and other agencies with CJIS or CHRIA requirements are migrated to Unisys supported infrastructure, the requirements from Exhibit G.7 (Summary of CJIS Requirements) will be used as the initial requirements to begin identifying CJIS and CHRIA regulatory requirements with designated agency participants including the Chief Information Security Officers (CISOs) of the Commonwealth and individual agencies.

Proposed solutions supporting regulatory requirements will go through a solution review and approval within the Unisys team and subsequently with the Commonwealth review boards and agency CISO before being implemented.

Unisys currently supports Commonwealth solutions with CJIS or CHRIA regulations. Unisys provides support for the infrastructure, including networks, servers, and storage, supporting PSP's CCHRI, CLEAN, Megan's Law and PATCH applications. Unisys works with PSP to maintain the infrastructure to PSP's facility and physical requirements for CJIS and CHRIA. Unisys also provides support for PSP during audits and develops solutions to update the infrastructure or physical environment's processes or implementation to maintain compliance.

In addition, Unisys has provided and continues to provide support for the CCHRI, CLEAN and PATCH applications themselves, including collaborating with PSP on defining the infrastructure requirements to meet CJIS and CHRIA requirements. [redacted] the proposed Unisys Security Manager, is part of the application support team and was responsible for meeting the CJIS and CHRIA requirements in the recently completed CLEAN upgrade.

3.B Offeror must provide examples of its experience in designing infrastructures that adhere to CJIS and CHRIA requirements

Apart from the Commonwealth experience referenced in 3A above, the Unisys Team designed a data and records management system for the Alabama Criminal Justice Information Center that was also required to meet the CJIS and CHRIA requirements.

The Alabama Criminal Justice Information Center (ACJIC) is a state agency providing local, state, and federal criminal justice agencies with the information needed to provide citizen safety.

ACJIC realized that gaps in its information technology were hindering communications and business continuity. It needed to more efficiently deliver critical information from its network and systems.

Maury Mitchell, Director of ACJIC explains, "We're connected to the FBI's National Crime Information Center, and we're in sync with all 50 states via the National Law Enforcement Telecommunication System. As such, our web applications handle about 18 million transactions a month. We were leasing space and time on the state's mainframe for data storage – a system we don't own – performing backups on tape and manually delivering them to a site a few blocks away for disaster recovery. We needed our own scalable, reliable, cost-effective system that would grow with our needs and provide hot failover."

ACJIC decided to change the way it was doing business. Jim Walker, Homeland Security Director for the State of Alabama, comments, "We had an opportunity to build redundancy into our system and improve the availability and use of information. We needed a solution that would build trust and deliver value to our user population."

ACJIC explored several solutions and solution providers before choosing Unisys to help establish an IT infrastructure specifically designed to address the agency's requirements.

Enhancing officer and citizen safety while building trust among constituents – by re-engineering the IT infrastructure to improve communications and business continuity.

By implementing a solution based on Unisys ES7000/one and SafeGuard 30m technology, the Alabama Criminal Justice Information Center created a dependable, cost-effective system that delivers real-time information to end users, supports future growth, and provides robust, reliable operations.

Results: Unified Law Enforcement through a Real-Time Infrastructure. The center's more powerful and resilient IT infrastructure has improved real-time communications among multiple levels of criminal justice agencies – enabling greater collaboration, and ultimately, a better response to criminal activities and other security concerns.

Metrics

- **Better Security:** Reduced downtime and risk – 24x7 availability with failover in less than one minute from the primary site to the disaster recovery site
- **Reduced Costs:** Lowered costs while processing some 18 million transactions monthly
- **Improved Satisfaction:** Enhanced citizen and officer safety by ensuring a constant flow of real-time information
- **Better Productivity:** Enabled one-to-two-second searches for up to 40 million records in the Law Enforcement Tactical System

4 SAP Design Examples

4.A The Offeror's proposed target infrastructure design for the Commonwealth's SAP environments must include a certified SAP sizing report prior to migration of the systems

A SAP sizing report is an important element of developing solutions to implement, upgrade or migrate SAP environments. As part of the Transition planning to migrate the SAP environments and during requirements gathering for solution requests, Unisys will work with the Commonwealth to identify the requirements and the product vendors to generate the SAP sizing report and other component recommendations.

Proposed solutions supporting the SAP implementations go through a solution review and approval within the Unisys team and subsequently with the Commonwealth review boards before being implemented.

During the data gathering phase, the IBM Insight for SAP utility program will be installed and run on the SAP systems of interest. The IBM Insight for SAP utility program and its subsequent reporting and analysis process provide a convenient, high-level, workload analysis for in-production SAP system landscapes. The analysis includes actual active user counts, machine utilizations, user/module load distributions, dialog counts, information about batch and reporting usage, system information and database information.

Output from the IBM Insight for SAP utility program and other information gained during the Due Diligence process will be used to perform SAP sizing.

4.B Offeror must provide examples of its experience in sizing and design of SAP infrastructures. All designs must be approved by the Commonwealth.

The Unisys Team has a global network of more than 35 SAP Competence and Excellence Centers including the flagship IBM SAP International Competence Center (ISICC) near SAP headquarters in Walldorf, Germany, which opened in 1993, that will support this process. The Commonwealth has utilized this process for successful sizing since the initial sizing for IES in 2001.

See **Attachment F-5 – Sample SAP Sizing Estimate**, for a recent sizing report.

The Unisys Team supports the Commonwealth's SAP initiatives through collaboration between the Commonwealth stakeholders and technology vendors as indicated in the following examples.

A large German multinational, technology-based group of manufacturers and developers of glass, special glass, specialty materials, components, and systems to improve how people live and work had a 5-year full outsourcing contract with an outsource vendor who competes with Unisys and who also held a managed services contract to operate all of the customer's business critical SAP systems and infrastructure.

In the course of a data center move, the customer began to have severe doubts about the incumbent's migration plan to move their global ERP system to a new German site. The customer lacked confidence in the provider's sizing and design of the new infrastructure and the transition plan overall.

In this case SAP recommended Unisys as a transition partner to the customer. Unisys was able to identify critical issues in the migration plan which the incumbent vendor recognized and corrected. As a result of this effort Unisys was hired to safeguard the ERP transition over Christmas.

As part of the Unisys on call support, the Unisys SAP team received calls on issues which they were able solve within 30 minutes resulting in a successful transition. As a result of this activity the customer has indicated a desire to bring Unisys expertise into future SAP projects.

In another example, a world market leader in special steels with approximately 350 subsidiaries and about 550 employees were undertaking a strategic effort to deploy SAP at their largest subsidiary.

Due to past project work, the Unisys SAP team was highly recommended by the SAP Chief

Infrastructure Architect and the Head of Operations. An internal business unit pushed the operation team into deploying IBM Power/AIX platform for the new SAP environment. This platform represented a break from their standard x86 computing resources.

The Unisys SAP team:

- Provided Sizing and Design for the new infrastructure
- Mentored the existing operations team in preparation for the IBM implementations with Unisys experience drawn from quite similar industries
- Tailored an implementation plan avoid some potential landmines e.g. using the processor clock speed as major decision criteria
- Opened a flood gate of access to Unisys expertise and access to key individuals with access to the Unisys real-world knowledge of SAP infrastructure environments together with the help of [redacted]´s and Intel´s development centers Led the operations team to strategic and vendor independent assessments to manage expectations for their internal business customers

As a result of this effort the customer continues to engage the Unisys SAP project team in cases where new projects reach beyond operations team's common skill sets.

5 Wide Area Net Connectivity

5.A Provide connectivity from the data center to the Commonwealth Network. Redundant network links are required.

The Unisys solution for intra-data center connections provides redundant and diverse connections. The Unisys Enterprise Services Catalog also includes methods by which the Commonwealth can expand bandwidth services as Agencies take advantage of replication services and disaster recovery services for critical applications.

For more details on the Network Architecture see Schedule F, Section 3.1.2.

5.B Offeror must describe its capabilities to connect to and manage the requisite connections

The fiber purchased from the telecommunication providers will terminate directly into [redacted] Nexus switches, allowing the deployment of [redacted] "[redacted] technology across the three sites. Using [redacted] a Layer 2 multipath network will be built without the Spanning Tree Protocol (STP) being deployed. This new network design is particularly suitable for large virtualization deployments, private clouds, and high-performance computing (HPC) environments.

The Unisys solution integrates SolarWinds with Nagios collectors to provide monitoring and management of the required circuits.

For more details on the Network Architecture see Schedule F, Section 3.1.2.

5.C Explain ongoing network support Services to manage these links including the ability to increase capacity as needed to support changes in the application infrastructure requirements.

The design is flexible enough that the solution can be adapted to higher capacity requirements if this becomes necessary as the Commonwealth's needs increase significantly.

The Commonwealth can request changes to the network capacity through the Enterprise Services Catalog to meet changing application bandwidth requirements. The Enterprise Services Catalog requests initiate the process flows to manage request fulfillment. The Enterprise Services Catalog request also initiates supplements to the bandwidth monitoring, reporting, and management infrastructures.

The ongoing network support is provided through the integration of network tools and components with the Nagios collectors. The Nagios collectors feed data concerning any service anomalies into the ITSM monitoring and incident infrastructure which is described in detail in Schedule F, Section 3.2.3.2 Site Operations.

6 Test, Acceptance Test Plan

6.A Prior to migrating each of the current application workloads to the new target infrastructure, the Offeror will work with each Commonwealth Agency to develop a mutually agreed to Acceptance Test Plan that includes the testing of application infrastructure performance characteristics.

Unisys will support each Agency migration team during the Transition planning cycle to develop an acceptance test plan to validate that supporting infrastructure required for the application has been successfully readied for normal operations. The Unisys Team will review and support the Commonwealth plan to designate groups of application support resources and the durations for each portion of the test. The test plan will be included in the overall migration plan and tracked as a project milestone. For detailed descriptions of the transition processes and procedures that will be followed to develop a mutually agreed to Acceptance Test plan for infrastructure that supports applications see Schedule F, Section 3.3 Transition Services.

6.B Offeror must discuss its proposed approach to systems acceptance testing and include the approach to performance testing.

Unisys recommends that the Commonwealth tests their applications using the available service level test infrastructure to validate that the application will operate and meet the requirements for the service level the Agency requests for each application.

The acceptance test plan will include the following elements at a minimum:

- Connectivity testing – Can the systems be reached from the required locations?
- Data Flow testing - Can the components of the application reach each other and other required applications?
- Failure testing – If a part of the system goes offline (e.g. web server), does the rest of the system compensate in the same manner as it did in the original environment?

For detailed descriptions of the transition processes and procedures that will be to the Commonwealth and its Agencies to validate systems acceptance testing for infrastructure that supports applications, see Schedule F, Section 3.3 Transition Services.

7 Test, Acceptance Testing

7.A The Offeror must conduct system acceptance testing, and provide the Commonwealth with written verification prior to declaring the system is fit for use. This acceptance test must include validation of infrastructure performance against system performance characteristics agreed to by both parties

The Unisys Team will include validation of infrastructure performance against system performance characteristics agreed to by the Commonwealth and provide written verification prior to declaring the system is fit for use. Unisys will work with manufacturers to obtain scripts or routines that can be executed to determine system level performance prior to application installation. Any system performance issues identified prior to application installation will be escalated to the vendor prior to declaring the system fit for use.

7.B Offeror must discuss its proposed approach to systems acceptance testing.

The following list represents the services the Unisys Team will perform for acceptance testing and support:

- System build – A joint Commonwealth and Unisys Team activity that provides the hardware and software environment for baseline test, development, quality assurance, and production environments. The baseline and development environments will need to be in place in time to support the start of the baseline testing stage. The Unisys Team is responsible for management and configuration of the operating system and associated components provided through the Enterprise Services Catalog.
- Baseline testing stage including test scripts – existing environment – This activity is performed by the Commonwealth with Unisys assistance to produce valid acceptance criteria along with test plans and accompanying data prior to the start of migration.
- Baseline testing stage including test scripts – new environment – The Unisys Team will run the previously specified acceptance tests developed during baseline testing on the incumbent systems against the ported applications running on the target platforms. This is done until the applications meet the success criteria defined by the acceptance test criteria developed during baseline testing. Once Unisys has validated that the base operating system functions to expected specifications Unisys will support the Commonwealth's application team efforts to test the application. At the Commonwealth's convenience the application can be moved to the appropriate compute resource on production-ready systems for final acceptance and consolidation testing.

8 Ready for Use Certification

8.A Offeror must provide the Commonwealth with written verification prior to declaring the Service is ready for use. The Service will not be considered ready for use until written acceptance is obtained from the Commonwealth.

As Unisys deploys a new service or technology, a written ready for use verification of the results of the system acceptance tests and met service requirements will be submitted to the Commonwealth for its acceptance. The customer services will not be migrated onto the new service or technology until the Commonwealth provides a written acceptance of the ready for use verification.

9 Test, User Acceptance Testing

9.A Offeror must support the Commonwealth's user acceptance testing.

The following list represents the services the Unisys Team will perform for the acceptance testing and support:

- Manage support for the Commonwealth testing and User Acceptance Runs (UARs) in collaboration with changes made to base operating system, operating system subsystems, software, database subsystems, data communications subsystems, compilers, programming languages, or operational/support tools.
- Support diagnostic and recovery tools.

9.B The Commonwealth shall not be charged for Services until written acceptance is obtained from the Commonwealth."

The Commonwealth will not be charged for services until Commonwealth written acceptance is obtained by the Unisys Team.

10 Application infrastructure Environment

10.A Provide non-production and production environments for each of the application computing platforms. The non-production environments will be used for testing new technologies and applications, updates and upgrades, prior to production implementations.

The Unisys Team understands the need to leverage a non-production environment to test updates and upgrades prior to production implementation. The Unisys solution includes the availability of computing platforms for test environments with servers for each of the configurations specified in the Schedule I, Volumetrics. As required, these can be provisioned via the Enterprise Services Catalog with storage quantities that match average storage quantities for servers based on the total server and storage counts in the Schedule I, Volumetrics.

10.B Offeror must describe its approach to the design and management of multiple application infrastructures.

Unisys manages multiple application infrastructures by embedding the logical application relationships to physical and virtual components within the sophisticated CMDB that provides the service mapping between applications and the supporting physical and virtual compute assets and services.

The selection of services and components from the Enterprise Services Catalog to support applications initiates the processes to update these selections with the appropriate application identifications within the CMDB.

The Unisys solution relies upon the CMDB process to audit and manage the multiple application infrastructures. The Commonwealth can define infrastructure bundles to track to specific application infrastructure. The Unisys ITSM infrastructure uses the CMDB and incident tickets logs to provide measurement and monitoring at the overall application layer.

More details descriptions of this process are available in Schedule F, Section 3.2.3.2 Site

Operations.

10.C Identify proposed solution to individual or consolidated non-production environments for agencies.

The Unisys solution provides extensive service options through the Enterprise Services Catalog to enable the Commonwealth to build individual or consolidated non-production environments to a variety of agency specifications.

11 Service Lifecycle

11.A Provide the infrastructure design for the Services and platforms to be offered.

Every service and associated technology and infrastructure proceeds through a lifecycle from concept to retirement. The actual lifecycle of individual services will be based upon several factors including ongoing business need, availability of technical components, and availability of replacement services. To support the Commonwealth's ongoing and changing business requirements, the Unisys team has developed the data center managed services with long and flexible lifecycles. In addition to the Technology Refresh Plan recommendation to upgrade or replace the technology deployments supporting many of these services, other elements of the service will be adjusted and updated over time through the continuous improvement process.

The enterprise architecture team will use Commonwealth requirements, portfolio offering, manufacturer updates, and industry trends to identify potential new service or technology offerings. In addition, the Commonwealth may request the Unisys team to review services or technologies by submitting a service request for a technical opinion, conceptualization, or cost-benefit analysis.

11.B Provide ongoing evaluation and recommend new technologies to enhance, improve, and reduce the cost of Services

All new or modified services and supporting technologies will follow the same activities before being implemented and made available for use within the Commonwealth environment.

- Requirements collected, reviewed and approved
- Solution documented
- Solution reviewed and approved by the Unisys Solution and Architecture Review Board
- Solution reviewed and approved by the Commonwealth Solution and Architecture Review Board
- Solution deployed and testing using an approved System Acceptance Test
- Approved by the Commonwealth for service implementation and requests.

Unisys will continue to provide Innovation Workshops for the Commonwealth. Unisys views these as essential to provide the opportunity for collaboration, technical information exchanges, and forums that will address issues, needs, and interests of the Commonwealth team. These Innovation Workshops are a key component of our overall Continuous Improvement Program. These Innovation Workshops also provide a forum by which Commonwealth leaders and the Unisys Enterprise Architecture team can establish baseline strategies and requirements to guide

the Unisys ITIL V3-based Service Design process described in Schedule F, Section 3.2.1.5 Technical Architecture.

11.C Offeror must describe its approach to provide service lifecycle design for all Commonwealth computing platforms and associated infrastructures.

The Unisys Program Management Office manages service lifecycle design through the ITIL V3-based Service Design processes described in Schedule F, Section 3.2.1.5 Technical Architecture, Section 3A. As outlined in this section, Unisys follows a ITIL-based governance process that engages the Commonwealth through the Senior Infrastructure Architect in the Unisys Program Management Office.

Unisys provides a Continuous Improvement goal that increases the value of the Unisys Service Design methodology. This value-add goal tends to push mature services to the forefront of the Service Design process because these tend to provide the easiest targets for Return-on-Investment discussions that provided a two-fold win for the Commonwealth: steady introduction of appropriate new technology to achieve strategic goals and a continuous refinement to ever more cost effective services.

11.D Offeror must provide the Commonwealth and its agencies the ability to request new technologies to be available.

The architects in 11.C plan to meet with Agency managers and directors regularly to present opportunities to introduce new technologies where these will provide value to the Commonwealth. The Agencies can also engage architects directly through the Unisys Program Management Offices.

The Unisys Enterprise architects will also use the Innovation Workshops described above as a forum to refine and detail requirements for services that take advantage of the strategic value that new technologies might provide the Commonwealth.

12 Staff, Technical Support

12.A Offeror must list Offeror's support staff levels required to plan, manage, and operate the IT infrastructure, based on the various service levels offered.

The Unisys Team has the required qualified and certified staff to plan, manage, and operate the infrastructure technology services provided to the Commonwealth. Details of the proposed staffing plan including staff levels are included in Section 5.0 Personnel.

Continual Service Improvement

Unisys recognizes the significant importance of Quality and Continuous Service Improvement to:

- Reduce service risk,
- Improve service quality,
- Improve client satisfaction,
- Provide service transparency, and

- Improve/reduce costs of service.

Through a continuous cycle of evaluation and improvement within an IT infrastructure, Unisys views quality and continuous service improvement as a critical success factor in driving customer satisfaction for the Commonwealth IT infrastructure. Each of the continuous service improvement areas identified above are driven through the tight integration of the following organizations, industry tools, proven processes and quality deliverables:

- Service Excellence Office,
- Quality Plans: transition and steady state service delivery
- Industry standard frameworks and methodologies: ITIL, ISO, SSL
- Industry accepted measurement tools
- Continuous Service Improvement & Innovation Processes (CSIIP)
- Risk management, audits and business continuity management
- Client Satisfaction Surveys and Knowledge Management Portal

Collectively this represents Unisys Integrated Quality Plan for the Commonwealth of Pennsylvania.

Specifics on each of these areas are outlined in Schedule F, Section 3.2.1.1.6 Continuous Service Improvement. Highlights from this section are outlined below and requested service examples are provided at the end of this section.

13 CI Service Risk

13.A Relative to the service in question, Offeror must provide examples of previous Offeror initiatives aimed at eliminating or mitigating service risks

The Commonwealth's State Police force and the Australian NSW Police Force share a near absolute aversion to the risk of data leakage given that this could put the lives of police officers at risk. Unisys deployed a secure imagery management system and forensic-grade storage solution to enable the NSW Police Force to store and manage digital images and video. The system allows police officers to manage digital evidence and streamlines the process of managing, sharing and accessing imagery, saving critical time in criminal investigations.

The NSW Police Force is the first police force in Australia to implement a digital imagery system of this scale – a solution able to manage and securely archive a large volume of images in a searchable central repository, making them quickly accessible for law enforcement purposes.

Challenge
Deploy a system that enables the NSW Police Force to securely store and share images to support police investigations.

Solution
A new digital imagery management system – installed, configured, deployed and managed by Unisys – that enables officers to quickly and easily categorize, archive, search and distribute

digital photographs, images and video. The system was built using a range of Microsoft technologies and runs on a combination of Unisys and EMC infrastructure.

Results
Provided the NSW Police Force with a secure, central repository for the storage and management of digital images taken by forensic teams, General Duties and Investigators during the course of investigations and by members of the general public. The system saves critical time in the law enforcement process and eliminates the risk of images and videos being accessed by unauthorized staff.

Metrics

- **Efficiency:** Reduced the time it took to process and deliver images from a crime scene from two to three weeks to less than three hours
- **Security:** Enabled police to secure images in a repository so they can't be accessed by unauthorized staff
- **Control:** Made it easier for police to demonstrate a 'chain of custody' that shows the date an original image was collected to eliminate the risk that the evidence could be misrepresented in court
- **Speed:** Allowed police to quickly and easily use images to create an electronic brief of evidence
- **Collaboration:** Made it easier for information to be shared across investigations so that the full value of digital imagery can be realized.

Unisys deployed a secure imagery management system and forensic-grade storage solution to enable the NSW Police Force to store and manage digital images and video. The system allows police officers to manage digital evidence and streamlines the process of managing, sharing and accessing imagery, saving critical time in criminal investigations.

The NSW Police Force is the first police force in Australia to implement a digital imagery system of this scale – a solution able to manage and securely archive a large volume of images in a searchable central repository, making them quickly accessible for law enforcement purposes.

14 CI Service Quality

14.A Offeror must provide examples of previous Offeror initiatives aimed at improving service quality.

Multisourcing Services Integration Helps Australian National Audit Office Control Costs and Improve IT Service Quality

The ANAO is a cornerstone of government accountability in Australia, providing Parliament with independent assessments of areas of public administration and assurance about public sector financial reporting. Each year, the ANAO conducts financial statement audits of approximately 300 government-controlled bodies and issues a range of financial statement audit opinions and performance audit reports, better practice guides, and newsletters.

Challenge
Optimizing the delivery of services to the business and developing highly efficient and collaborative partnerships in a multi-sourced environment.

Solution
By implementing Information Technology Infrastructure Library (ITIL) based service delivery policies and practices, building a robust IT governance framework and appointing Unisys as its Multisourcing Services Integrator (MSI) to manage its complex service provider environment, the Australian National Audit Office (ANAO) is achieving cost reductions, an improved end user experience and better support for business systems.

Results
Since the commencement of its current contract with Unisys, the ANAO is experiencing reduced costs, improved service provision to the business, a more productive multi-sourced environment, and a better overall end-user experience.

Metrics

- **Cost:** Achieved 10 percent reduction in baseline costs to the ANAO, surpassing its Gershon Review savings requirements, an independent review of the Australian Government's use and management of Information and Communication Technology (ICT)
- **Efficiency:** Improved incident and resolution times to more than 94 percent, reduced the number of incidents logged monthly by 30 percent and cut problem resolution from 28 days to eight days
- **Productivity:** Improved employee satisfaction and client account satisfaction ratings beyond optimal ratings for the IT department through enhanced delivery quality and increased network and business system availability to 99.99 percent

Solution at a Glance
In addition to IT Managed Services under the original contract, Unisys now provides:

- ITIL practices including:
  - Problem Management
  - Configuration Management
  - Capacity Management
- Enterprise Architecture Services
- Project Management Services
- Security Services
- Multisourcing Services Integration that drives:
  - Procurement Services
  - Relationship Management
  - Performance Management

For more details see: http://www.unisys.com/unisys/ri/cs/detail.jsp?id=1120000970016010172

15 CI Client Satisfaction

15.A Offeror must provide examples of previous Offeror initiatives aimed at continually improving client

satisfaction.

Breakthrough: A New Policy and Core Business Component-based Platform for Nationale-Nederlanden, ING.

Increasing sales by improving customer satisfaction and product innovation, and reducing costs.

Nationale-Nederlanden, a division of ING, and Unisys built a common component-based insurance platform that resulted in 80% straight-through processing and acceptance, faster time to market for new product introductions, and flexible pricing — realizing a 25% cost reduction.

Results:
A new policy and core business component-based platform.

Metrics

- Web-based extranet for intermediaries to gain immediate access to the back-office to obtain quotes, process contracts, and make changes
- 80% straight-through processing
- Three-tier global sourcing model which involved UK, The Netherlands, and India
- A service-oriented architecture that enables Nationale-Nederlanden to centralize back-offices on an international scale
- Reusable components to enable Nationale-Nederlanden to easily deploy additional solutions
- An industrialized methodology for product design and software development.

Business Challenge: Increasing Productivity and Efficiency

In today's highly competitive insurance market, customer satisfaction, product innovation, and cost reduction are not only key for running daily business operations, but also for competing with other insurers and complying with ever changing regulations.

"In our market, visibility is one of the key factors. Not only for running our daily business operations, but also to help us compete and comply. We have been able to realize this visibility through the choice we made in the development of brand new software solutions for policy processing, which have made a big difference for us," says Age Miedema, chief operations officer, Nationale-Nederlanden. As part of a new IT strategy, the Dutch-based insurer decided to contract Unisys to support the innovation of its application landscape. Nationale-Nederlanden now uses new component-based solutions for its life and general insurance business administrations. "We have made a giant step," says Miedema.

The Relationship: A Shared Vision and a Commitment to Execution
"Both parties invested extensively in the working relationship and talked a lot about the way the insurance market is developing," says Miedema. "Unisys proved to have a clear vision on the future of the financial services industry, and had an in-depth understanding of our business. We were able to combine these thoughts."

For more details see: http://www.unisys.com/unisys/common/download.jsp?d_id=17500019.

16 CI Service Transparency

16.A Offeror must provide examples of previous Offeror initiatives aimed at providing service transparency; in particular, visibility into the service execution process.

Creating a Transparent and Nimble Environment with Unisys Secure Private Cloud

For enterprises with large IT shops that are struggling to meet the demands of the users they serve in a timely manner while managing the growing complexity and cost of their IT infrastructure, Unisys Secure Private Cloud is a pre-integrated, internal private cloud solution that transforms data center operations into an agile, efficient and highly automated infrastructure.

Deploying Unisys Secure Private Cloud in your data center will increase transparency and agility, enabling you to deliver "just in time" services and reduce the wait time for resources from weeks down to minutes while lowering both capital and operating expenses.

What does Unisys Secure Private Cloud do for you?

- **Increase Productivity:** Manage 5 times or more virtual machines with existing staff
- **Improve Efficiency:** Increase utilization of resources up to 60% or more
- **Shorten Response Times:** Reduce provisioning times from weeks to minutes
  Reduce Costs: Eliminate manual processes and save operating expenses

Why Unisys?

- **Security:** Protects mission critical communication between virtual machines and enables the most secure multi-tenant environment.
- **Automation:** Leverages Unisyss experience in building and managing clouds to provide full compliance with existing best practices.
- **Open and Adaptable:** Seamlessly integrates with existing and new environments and management processes.
- **Transparency:** Usage monitoring and oversight of cloud resources enables show-back or a pay-per-use service model.
- **Holistic Approach:** Efficiently aligns IT to business objectives and provides best fit and function.

For more details see:
http://www.unisys.com/unisys/landingPages/index.jsp?id=1120000970017610154

An example:

TravelSky Chooses Unisys Secure Private Cloud Solution 2.1 to Meet Growing Transaction Volumes for China's Travel Agencies

TravelSky, the leading provider of information technology solutions for China's air travel and tourism industry, has renewed its services and technology relationship with Unisys China to further its cloud computing strategy. As a result, TravelSky will implement release 2.1 of the Unisys Secure Private Cloud Solution.

TravelSky Vice President Mr. Rong Gang said: "We have used the Unisys private cloud management software in our test and development environment to gain the flexible operational benefits of cloud computing within the security of our own data center. Now we are ready to apply it to a core production system. The Unisys solution provides highly automated operations and self-service provisioning of IT resources as needed so that we can quickly meet fluctuating business demand."

In the first phase of the private cloud implementation TravelSky built a test and development environment using release 1.4 of the Unisys Secure Private Cloud Solution.

In the second phase of the rollout, TravelSky will create a production private cloud environment based on release 2.1 of Unisys Secure Private Cloud Solution. This release features a new dashboard capability that gives administrators a single, integrated view of all cloud resources. The enhanced dashboard capability streamlines management of critical IT infrastructure and helps reduce overhead costs by making it easier to commission and decommission resources as needed.

The TravelSky production cloud will connect travel agencies and reservation systems via the Unisys Open Message Switching Engine (OMSE), a communications front end that allows travel agencies, airline reservation offices and external systems to communicate with the mission-critical TravelSky systems.

TravelSky also plans to use the enhanced user interface and automation capabilities of Unisys Secure Private Cloud Solution release 2.1 to customize the private cloud to offer the OMSE Gateway as software as a service (SaaS) to its partners and agents.

In addition, TravelSky aims to reduce its data center requirements and operational costs by migrating the OMSE onto a virtualized environment running on a Unisys ES7000 Model 7600R G3 Enterprise Server, which can consolidate up to 24 virtual servers onto a single machine.

"TravelSky's business involves many critical processes spanning the passenger, cargo, airline and airport aviation business, so they need a highly secure, scalable, and flexible IT infrastructure to meet changing demands in logistics, passenger services and other core applications," said Sue Carter, vice president, Technology Consulting and Integration Solutions, Unisys Asia Pacific. "The Unisys Secure Private Cloud Solution supports this by delivering the same attributes as a public cloud except from within TravelSky's own data center, providing cost-efficient access to 'just in time' resources that can be shared among user communities in a common infrastructure model but remain secure and isolated from each other."

Unisys has more than 45 years' experience providing advanced, mission-critical IT solutions to the aviation industry. Nineteen of the top 25 airlines – and more than 200 worldwide – rely on Unisys solutions. Asia Pacific aviation industry clients include Beijing Capital International Airport and Guangzhou International Baiyun Airport in China, Delhi International Airport Ltd and

Air New Zealand.

For more details see:
http://www.unisys.com/unisys/news/detail.jsp?id=1120000970020910149

17 CI Service Sustainability

17.A Offeror must provide examples of previous Offeror initiatives aimed at ensuring service sustainability; in particular, efforts targeted at cost containment and cost reductions.

The California State University system has been a long-time customer of Unisys and has expanded services over the years. Prior to the last contract renewal CSU was struggling to find cost reductions due to budget pressures in California. Unisys recommended that rather than refresh their aging storage infrastructure with new hardware purchases, CSU should migrate their data onto the Unisys Managed Storage Platform. This helped CSU avoid hundreds of thousands of dollars in capital expense and changed the entire nature of CSU infrastructure agility. During the migration process CSU was able to locate stale or seldom used data stores and eliminate these "just in case" storage allocations. Now when DBAs need short term access to storage for testing or development they can draw upon the "pay-when-you-need-it" Shared Storage pool and retired the storage and the associated costs when their project concludes.

18 CI Improve or Reduce Cost

18.A Offeror must provide examples of previous technology initiatives implemented by Offeror that achieved reduced costs of Services and that met or exceeded ROI (Return on Investment) analysis projections.

The Unisys Team is very proud to close out this section by reminding the Commonwealth of the journey and successes that we embarked on in 1999 and the early successes that may have faded from memory.

Business Challenge: Building a Framework for the Future
In 1999, the Commonwealth of Pennsylvania's IT landscape amounted to a disparate collection of systems and software that were "independently owned and operated" by the state's agencies, boards, and commissions.

With more than 20 mainframe-based agency data centers using duplicate equipment and staff to deliver similar services, the Commonwealth decided to centralize and consolidate its resources so it could achieve a 24/7 mission-critical operating environment and economies of scale, improve efficiencies, and redirect cost savings toward strategic initiatives.

Challenge
Consolidate a widely distributed technology landscape, centralize common services, standardize technology and processes, improve security, reduce costs, improve collaboration, and free up resources for strategic initiatives.

Solution
The Commonwealth of Pennsylvania has changed its approach to IT management through the Shared Infrastructure Services (SIS) initiative, which centralized governance, procurement, and management of IT hosting services. Supporting the Commonwealth SIS strategy is a shared

hosting services approach, which includes two data center environments – the Data PowerHouse (DPH) and Enterprise Server Farm (ESF). The DPH allowed the Commonwealth to consolidate 17 agencies' data centers into one and is a key component of the shared hosting services approach.

The ESF consolidated operational and technical support services for web hosting and messaging services for some 45 agencies and support for 90,000 email boxes.

Results: Cost Avoidance, Savings, and Agility
With a shared services model and consolidated IT infrastructure, the Commonwealth of Pennsylvania has already achieved extensive cost avoidance and savings that will continue to grow in the future as it further embraces a more mature services model, persists in enhancing shared hosting services, implements virtualization, and increases efficiencies across the agencies.

Metrics

- Cost: Achieved $317 million in cost savings via resource consolidation and increased efficiencies and anticipates an additional $240 million in savings and cost avoidance over the next five years
- Agility: Enhanced efficiency, security, availability, and disaster recovery via virtualized and dynamic server allocation capabilities that enable IT infrastructures to adapt to fluctuating workloads and maintain uptime in the event of an emergency
- Productivity: Improved ability to focus agency resources on core business activities.

The Unisys was again doubly proud in 2008 when the Unisys team was able to provide the Commonwealth with $240 million in savings through a mutually favorable contract extension.

Unisys Team Experience

The examples in the Continual Improvement sections showcase the Unisys team experiences and the values that Unisys has brought to customers and strives to bring again to the Commonwealth.

Benefits to the Commonwealth

As an over-arching organization principle for IT Services Management and Infrastructure Services, the Unisys Infrastructure Architecture services create the "factory" by which all other operations values, cost efficiencies, and improved services are delivered to the Commonwealth.

The primary competitive value that Unisys provides to the Commonwealth and its customers are the cost savings and service improvements that it builds by continuously focusing on how to achieve labor efficiencies in the monitoring and technical support of Infrastructure Architecture services.

The Commonwealth will realize cost efficiencies over time for Infrastructure Services because Unisys uses Six Sigma analytics driven by the Service Excellence Organization (SEO) within the Unisys Program Management Office (PMO) to refine steady state services and remove variability from expected outcomes.

The rich field of metrics and analytics provided to the Commonwealth through the real-time dashboard and the Services Portal will allow the Commonwealth sufficient transparency to be able to review services for anomalies in service or plateaus in service improvements. This

unprecedented depth of analytics will allow the Commonwealth to set directions on service changes and improvements that will provide the highest strategic value to the Commonwealth. In effect, the Commonwealth can steer the Unisys IT infrastructure to its preferred course of strategic achievements without having to focus on how Unisys manages the manipulation of the rudders to change course incrementally and cost effectively.

The Unisys provided ITIL V3-based Infrastructure Architecture services coupled with a deep reservoir of monitoring tools reduces risks for the Commonwealth because these processes and tools lay a foundation for proactive actions to avoid service interruptions. Unlike other vendors who might propose a base level of services to monitor equipment, the Unisys Team's proposal including the dashboards and analytics enables us to be proactive and focus on the course to strategic innovative initiatives.

3.2.2.3 Capacity Management

The Capacity Management activity focuses on the planning and scheduling of the Commonwealth's infrastructure capacity and growth. Capacity planning includes consideration of data communications, networking, processing, storage, and other environmental variables. The Offeror must issue periodic reports showing usage, trends, capacity forecasts, and recommendations for upgrades.

Processor capacity planning focuses on estimating, measuring, and reporting on the central processing unit (CPU) and memory usage, including peak usage and average usage over time.

Forecasting of each agency's application-based processor and memory usage will be determined using projected transaction and user volumes supplied by the Commonwealth. The Offeror must track application-based processor and memory usage and report the usage and trends to the Commonwealth. The Offeror must make periodic recommendations for upgrading existing server capacity.

Data storage capacity planning focuses on estimating, measuring, and reporting on data storage used per application over time.

Forecasting of application-based data storage usage will be provided by the Commonwealth. The Offeror must track current data storage usages and report the usage and trends to the Commonwealth. The Offeror must make periodic recommendations for upgrading existing data storage capacity.

New application infrastructure capacity planning focuses on estimating, measuring, and reporting on network, server, and data storage usage over time per application. New processing requirements will be established during testing in test environments. The Offeror must track application-based infrastructure usage. The Offeror must make monthly recommendations for upgrading existing infrastructure capacity.

The following list identifies but does not limit the roles and responsibilities that the Offeror must

perform:

- Establish comprehensive Capacity Management planning process
- Identify future business Commonwealth requirements that will alter capacity requirements
- Assess capacity impacts when adding, removing or modifying applications
- Capture trending information and forecast future agency infrastructure capacity requirements based on agency defined thresholds
- Recommend changes to capacity to improve service performance
- Assess impact/risk and any cost of capacity changes with agencies
- Maintain capacity levels to optimize use of existing IT resources and minimize agency costs
- Ensure adequate capacity exists within the IT environments

Reference Documentation

Schedule H - Commonwealth Computing Procedures Manual (CCPM)

	Requirements	Describe Compliance
1.	Working with each agency, develop the initial Capacity Management Plan based on an inventory and review of each of the agency applications and associated managed infrastructure. Develop the initial Capacity Management Plan and provide quarterly updates to the plan.	Offeror must discuss its approach to Capacity Management and provide a sample of a Capacity Management Plan.
2.	Meet with the Commonwealth and agency representatives on a monthly basis to assess the future datacenter resource requirements; processors, storage space, network (LAN & WAN), selected application transactions, and number of users, etc.	Offeror must discuss its approach to support the current and future needs of Commonwealth agencies. Offeror must provide a sample of a Capacity Management report that includes processor, storage, network and application metrics.
3.	Produce an annual datacenter Capacity Plan and Trend Analysis.	Offeror must discuss its approach to meet this requirement. Provide a sample Capacity Management Plan and Trend Analysis.

4.	Produce a monthly planned vs. actual resource usage report.	Offeror must discuss its approach. Provide a sample resource usage report.
5.	Recommend methods for reducing hardware “footprints”, e.g., replacing server storage with network attached storage and aggressive server virtualization.	Offeror must discuss its approach.
6.	Allow emergency or temporary orders for additional Services or capacity without a minimum service commitment.	Offeror must discuss its approach.
Continual Service Improvement		
7.	Reduce service risks.	Offeror must provide examples of previous Offeror initiatives aimed at eliminating or mitigating service risks.
8.	Improve service quality.	Offeror must provide examples of previous Offeror initiatives aimed at improving service quality.
9.	Improve client satisfaction.	Offeror must describe methods to continually improve client satisfaction.
10.	Provide service transparency.	Offeror must provide examples of previous Offeror initiatives aimed at providing service transparency; in particular, visibility into the service execution process.
11.	Ensure service sustainability.	Offeror must provide examples of previous Offeror initiatives aimed at ensuring service sustainability; in particular, efforts targeted at cost containment and cost reductions.
12.	Improve/reduce cost of service.	Offeror must provide examples of previous capacity initiatives implemented that achieved reduced costs of Services and that met or exceeded ROI (Return on Investment) analysis

		projections. If costs of Services increased due to increased required capabilities, so identify.

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

Introduction

Unisys will provide the Commonwealth with a Capacity Management System including the process, people, and industry leading technology to provide the Capacity Management planning and scheduling of the supporting infrastructure. Capacity planning includes data communications, networking, processing, storage, and other environmental variables. Unisys will provide periodic reports showing usage, trends, capacity forecasts, and recommendations.

We will provide processor capacity planning focused on estimating, measuring, and reporting on the central processing unit (CPU) and memory usage, including peak usage and average usage over time.

Unisys will provide Enterprise Services Catalog items that the Commonwealth/ agencies can select to provide the following capacity related analyses for supporting each Commonwealth/agency application selected. These services include:

- Forecasting workload of an agency's application infrastructure including server processor and memory usage using projected workload transaction and user volumes supplied by the Commonwealth.
- Tracking application-based processor and memory usage and reporting the usage and trends to the Commonwealth.
- Providing data storage capacity planning by estimating, measuring, and reporting on data storage used for supporting Commonwealth applications.
- Utilizing storage forecasts for each application provided by the Commonwealth to make periodic recommendations for upgrading or consolidating data storage capacity.
- Supporting capacity planning for new application infrastructure availability focused on estimating, measuring, and reporting on network, server, and data storage usage over time for each application. Unisys will track application-based infrastructure usage.
- Making recommendations for upgrading existing infrastructure capacity.

Unisys performs the following roles and responsibilities for Capacity Management:

- Establish the Capacity Management planning process
- Work with the Commonwealth to review future business requirements that will alter capacity requirements
- Assess capacity requirements and impacts when adding, removing or modifying

applications

- Capture trending information and forecast future agency infrastructure capacity requirements based on agency defined thresholds
- Recommend changes to capacity to improve service performance
- Assess impact/risk and any cost of capacity changes with agencies
- Maintain capacity levels to optimize use of existing IT resources and minimize agency costs
- Help to confirm adequate capacity exists within the IT environments for business requirements

1 Capacity Management Approach

1.A Working with each agency, develop the initial Capacity Management Plan based on an inventory and review of each of the agency applications and associated managed infrastructure.

Unisys follows the process framework shown in **Figure 3.2.2.3-1** below to complete a Capacity Management Plan that is developed annually and reviewed quarterly with the Commonwealth agencies. The initial plan will be developed during the transition phase working with the agencies.

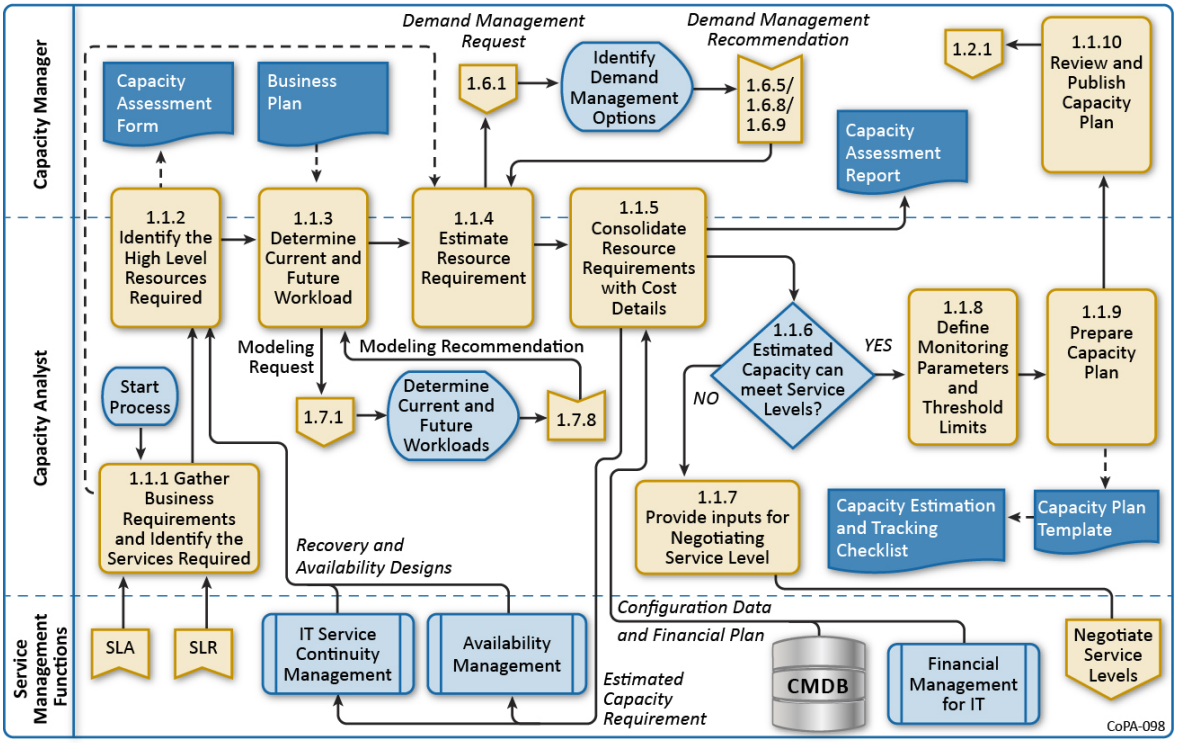


Figure 3.2.2.3-1 - Capacity Management Process

The Capacity Management Process consists of the following key activities:

1.1.1 Gather Business Requirements and Identify the Services Required

The Capacity Manager will review the SLAs for gathering the capacity requirements to meet the service targets, and for analyzing their impact on the existing SLAs.

The following details are identified from the SLA:

- The list of services including the Shared Services
- Dependency of each service with other services
- Service requirements and targets.

1.1.2 Identify the High-Level Resources Required for each Identified Service

The recovery design and the availability design from the IT service continuity management and availability management processes respectively are used for assessing the required resources. The resources include the infrastructure components to support the availability of an application.

Determining the high-level resource requirements refers to identifying the different type of infrastructure resources required for providing the service. The number of resources required is identified later during the resource estimation stage. The high-level resource requirements are captured in the capacity assessment form.

1.1.3 Determine Current and Future Workload (Optional Catalog Service for each Application infrastructure Capacity Plan)

The Commonwealth provided current workloads and future business requirements are assessed to predict the behavior of the services and to confirm that the adequate capacity is made available to meet the future demands. The Business Plan is created to identify the forecasted future business requirements.

For the existing services, the following information is gathered:

- Details of the resources supporting the service: type of resources, number of resources, and their role in providing the service (for example, primary/backup)
- Maximum usable capacity for each identified resource
- Different sources utilizing the resource (for example, source includes applications, project group, other resources)
- Utilization details of each resource for a defined period and for each source
- Current business volumetric/throughput for each service.

The current workload and future business requirement details help in understanding the following:

- Usage trend
- Predicting the future demands
- Risk and cause

For new services, data from similar services can be used for analyzing and predicting. The data

can also be gathered from the organization in similar service lines, international standards, or based on experience.

Analyzing the current workload and predicting the future demands will be done for each resource.

The modeling techniques such as trending, analytics, and simulation can be used to predict the workload behavior of the services and resources. The choice of modeling technique and the depth to which the data needs to be analyzed depends on the business need and criticality of the services.

The current and future workload details are captured in the capacity assessment form.

1.1.4 Estimate Resource Requirement (Optional Catalog Service to support Application Infrastructure Availability)

The resource estimation is done for identifying the right resources to meet the current and future needs of the business. The estimation should also cover the timeline by which the resource should be available. This helps in avoiding early investment and provides that the resources are available when needed.

The workload details and the identified high-level resources are assessed to estimate the number and capacity of the resources. Resource estimation also specifies the appropriate configuration for hardware resources, software versions and skillset requirements.

The resilience factors suggested by the availability management and recovery options from IT service continuity management should be taken into consideration while estimating the resources.

Different scenarios can be analyzed in order to provide the resource estimation at an optimal cost. To derive different scenarios, demand management options such as sharing the workload across different timelines and the splitting of workload with multiple resources can be considered.

The detailed resource requirements are captured in the capacity assessment form.

1.1.5 Consolidate Resource Requirements with Cost Details

The capacity estimates from various domains such as network, server, and storage resources are consolidated to identify the need for new resources and the use of existing resources.

The consolidated resource requirements are captured in the capacity assessment report.

1.1.6 Estimated Capacity Can Meet Service Level

The following are analyzed to determine if expected service targets can be met with estimated capacity

- SLA
- Workload
- Capacity requirement

1.1.7 Provide Inputs for Establishing Service Levels

The Capacity Analyst provides the inputs for establishing SLA's including:

- Estimated capacity
- Limitations and capability of the proposed technology

1.1.8 Define Monitoring Parameters and Threshold Limits

Defining the monitoring parameters and thresholds are necessary to proactively manage the capacity of the resources and to avoid over-utilization of the resources. Over-utilization of resources impacts the performance of the resources and can lead to the unavailability of the resources.

Appropriate monitoring parameters are identified based on the following:

- Resource type, purpose and its capabilities
- Projected workload
- Expected service targets.

Appropriate threshold limits are defined based on the following:

- Capacity of the resource
- Current peak and off-peak usages
- Timeline to resolve the threshold breaches
- Available solutions to fix breaches
- Expected service targets.

Also, the frequency in which these parameters need to be monitored has to be determined. Frequency refers to the time interval in which the parameters need to be monitored. These intervals must have enough granularity to capture transient peaks, e.g., backups impacting network traffic, batch processes impact online performance, etc.

1.1.9 Prepare Capacity Plan

The Capacity Plan is one of the key outputs of the Capacity Management process. The Capacity Plan has to be prepared at least annually and is reviewed, published quarterly or in line with the business or budgetary lifecycle.

The Capacity Plan describes the business capacity requirements and the planned service and restores capacity to meet the business requirements.

The Capacity Plan is prepared using the Capacity Plan template and includes the following details:

- Current and recent service provision
- Service forecasts

- Resource utilization
- Resource forecasts
- Business scenarios and key business events (e.g., year-end financials, retail sales periods, maintenance periods, etc., as appropriate)
- Monitoring parameters and threshold limits

1.1.10 Review & Publish Capacity Plan

The Capacity Plan is reviewed for its details of coverage and its accuracy.

The approved Capacity Plan is uploaded in the capacity database (CDB) and published after review with the relevant agency stakeholders.

The information from CDB is used to prepare the capacity management reports. This data is also utilized to generate capacity forecasts and to plan for future capacity requirements.

The Capacity Plan is one of the key outputs of the capacity management process shown in the process above. The Capacity Plan is prepared annually and is reviewed, updated, and published quarterly or in line with the Commonwealth budgetary lifecycle.

1.B Develop the initial Capacity Management Plan and provide quarterly updates to the plan.

Unisys will work with Commonwealth agencies to develop the initial capacity management plan and provide quarterly updates to the plan. Please refer to 1.A for the development of the Annual Capacity Plan and quarterly update process.

1.C Offeror must discuss its approach to Capacity Management and provide a sample of a Capacity Management Plan.

The end result of the above Capacity Management Planning Process is the Commonwealth Capacity Plan that follows the outline below:

- Introduction
- Scope
- Method
- Assumption and Constraints
- Business Scenarios
- Resource Capacity Summary
- Current Resource Usage
- Forecast Resource Usage
- Opportunities for Improvement
- Monitoring Standards

- Standards for Parameters and Thresholds
- Standards for Frequency and Data Retention
- Standards for Alerts and Escalation
- Recommendations

See Attachment F-6 for a sample capacity management plan.

2 Capacity Management Report Sample

2.A Meet with the Commonwealth and agency representatives on a monthly basis to assess the future datacenter resource requirements; processors, storage space, network (LAN & WAN), selected application transactions, and number of users, etc.

Offeror must discuss its approach to support the current and future needs of Commonwealth agencies.

Unisys will meet with the Commonwealth and agency representatives on a monthly basis to assess the future data center resource requirements including processors, storage space, network (LAN), selected application transactions, and number of users and other capacity management factors.

Current

Unisys will meet the current needs of Commonwealth agencies by performing daily, weekly and monthly reporting and perform the following capacity management tasks including:

- Review of current activity, including performance and capacity trend exceptions for significant service configuration items (CI's) for servers, storage and network CI's
- Review of significant Requests for Change (RFC) that impact capacity and performance. Determine if there is an impact on capacity workload for new or modified CIs and the potential impact on the performance of a service.
- Review of any significant incident tickets that have had an impact on service performance and SLA's to determine what action should be taken working with the Problem Manager and various stakeholders to process capacity management changes to rectify capacity related problems.
- Prepare recommendations

Future

The Commonwealth should request a capacity planning services in the Enterprise Services Catalog for each application it wants to have future infrastructure workload capacity analysis scenarios completed.

Unisys will complete the following types of activities utilizing the [redacted] t when these services are selected:

- Model estimated workload scenarios with application transaction estimates, usage estimates, and service projection data provided from the Commonwealth

- Setup capacity monitoring to track application infrastructure usage during testing and production
- Report application usage of infrastructure with trends reporting by application
- Review monitoring parameters and threshold limits
- Review application capacity usage trends on a quarterly basis with the Commonwealth
- Prepare recommendations for future capacity utilization

The Unisys capacity management team will identify under-utilized or over-utilized servers; accurately plan, implement, and support the Commonwealth's virtualization and cloud computing initiatives; and support optimizing data center resources.

2.C Offeror must provide a sample of a Capacity Management report that includes processor, storage, network and application metrics

See Attachment F-7 for a sample Capacity Planning report, that includes metrics in support of the Commonwealth Integrated Enterprise System (IES) SAP application environment.

3 Capacity Plan and Trend Analysis Report Sample

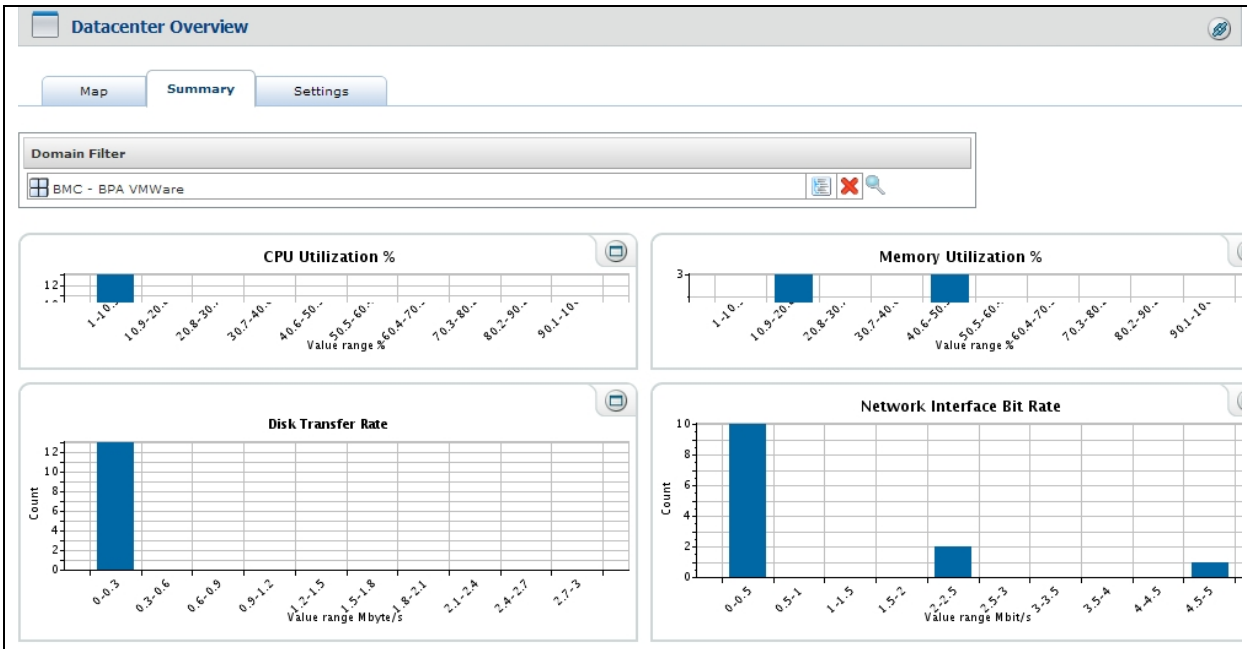
3.A Produce an annual datacenter Capacity Plan and Trend Analysis.

Offeror must discuss its approach to meet this requirement

The Unisys Capacity Management Team approach to meeting the requirement for an annual Capacity Management Plan is discussed in detail in response to 1 above. The Unisys Capacity Management Team will produce a monthly Capacity usage report for infrastructure CI's for the Commonwealth. The report will show trends against projected baselines and offer recommendations for review and action with the Commonwealth agencies.

3.B Provide a sample Capacity Management Plan and Trend Analysis.

Sample trend analysis is included in the Capacity Management Plan sample referenced in 1.C above. Additionally, see Attachment F-8, *Sample Monthly Server Capacity Report* and see Figure below for samples of monthly capacity usage report. The actual format will be determined with the Commonwealth during transition.



Export to | show/hide cols

Ranking Table

Rank	Name	CPU Utilization [%]	Memory Utilization [%]	Disk Transfer Rate [MB/sec]	Network Rate [Mbit/s]
1	isr-rh5-bpa-01	16.22%	93.51%	0.45	0.15
2	pe-pun-bcm-dv01	8.54%	89.37%	3.01	2.27
3	lex-rddomain-01	86.04%	0%	0	0
4	engw2k8x64sso8	59.52%	13.19%	0.33	0
5	lex-rd-esx-27	16.14%	48.16%	3.14	6.09
6	scaesx12-1	13.64%	47.53%	7.24	0.23
7	scaesx12-2	11.64%	46.33%	7	0.18
8	scaesx12-3	11.24%	46.13%	6.93	0.18
9	lex-rd-esx-20	11.64%	44.76%	2.42	1.54
10	lex-vSphere-02	15.27%	40.97%	1.47	0

1-10 of 888 results 0 selected Page Size: 10

Clear sorting

Figure Data Center Summary Report

4 Resource Usage Report Sample

4.A Produce a monthly planned vs. actual resource usage report.

The Unisys Capacity Management Team will produce a monthly capacity usage report for the Commonwealth. The report will show trends against projected baselines and offer recommendations for review and action with the Commonwealth/agencies.

4.B Offeror must discuss its approach

Unisys will produce standard monthly reports. It is the intention to automate this process where feasible, so that the Unisys Capacity Team can focus on exceptions, analysis and

recommendations for improving utilization of the infrastructure.

4.C Provide a sample resource usage report.

See Attachment F-8, Sample Monthly Server Capacity Report for a sample of this monthly capacity usage report.

5 Hardware footprint reduction

5.A Recommend methods for reducing hardware "footprints", e.g., replacing server storage with network attached storage and aggressive server virtualization.

The Unisys capacity management team working with Commonwealth agencies will recommend reducing hardware "footprints", e.g., replacing server storage with network attached storage and aggressive server virtualization. Please refer to Schedule F, Section 3.2.1.1.6 "Continuous Service Improvement" for the recommended approach to how Unisys improves overall operations. Additionally, the Capacity Manager utilizes enterprise capacity management toolset to actively pursue reducing hardware "footprints" for all Unisys managed infrastructure.

Also, please refer to the continuous improvement examples below for some examples of where Unisys has done this for the Commonwealth in past performance.

5.B Offeror must discuss its approach.

The Unisys capacity management team will utilize industry leading capacity management tool, [redacted] to model the Commonwealth application server virtualization, network and storage models to provide the Commonwealth with improved costs for service levels. The [redacted] tool supports using cost, service levels, server, network and storage policies, forecasts and historic performance data to forecast and model various alternatives to support Commonwealth applications and requirements.

6 Temporary or emergency service orders

6.A Allow emergency or temporary orders for additional Services or capacity without a minimum service commitment.

The Unisys Team will provide Capacity on Demand (COD) for Infrastructure as a Service (IaaS) servers and storage that the Commonwealth can order through the Enterprise Services Catalog. These services deliver to the Commonwealth infrastructure as COD that will support emergency, temporary, ad-hoc or unplanned capacity requirements for the Commonwealth agencies without a minimum service commitment.

6.B Offeror must discuss its approach

Unisys will have the ability to handle Enterprise Services Catalog requests for COD IaaS servers, storage and related network infrastructure through various technologies and processes to support provisioning servers and storage on demand.

Please refer to Schedule F, Section 3.2.5.1 "Server Capacity on Demand" and Section 3.2.5.2 "Storage Capacity on Demand" for a complete description of how server and storage COD IaaS

services will be approached for delivery to the Commonwealth without a minimum service commitment.

7 CI Service Risk

7.A Offeror must provide examples of previous Offeror initiatives aimed at eliminating or mitigating service risks.

Continual Service Improvement

Unisys recognizes the significant importance of Quality and Continuous Service Improvement to:

- Reduce service risk,
- Improve service quality,
- Improve client satisfaction,
- Provide service transparency, and
- Improve/reduce costs of service.

Through a continuous cycle of evaluation and improvement within an IT infrastructure, Unisys views quality and continuous service improvement as a critical success factor in driving customer satisfaction for the Commonwealth IT infrastructure. Each of the continuous service improvement areas identified above are driven through the tight integration of the following organizations, industry tools, proven processes and quality deliverables:

- Service Excellence Office,
- Quality Plans: transition and steady state service delivery
- Industry standard frameworks and methodologies: ITIL, ISO, SSL
- Industry accepted measurement tools
- Continuous Service Improvement & Innovation Processes (CSIIP)
- Risk management, audits and business continuity management
- Client Satisfaction Surveys and Knowledge Management Portal

Collectively this represents Unisys Integrated Quality Plan for the Commonwealth of Pennsylvania.

Specifics on each of these areas are outlined in Schedule F, Section 3.2.1.1.6 Continuous Service Improvement. Highlights from this section are outlined below and requested service examples are provided at the end of this section.

Risk management, independent quality audits, and business continuity management are integral quality management processes. Unisys is committed to managing risks and facilitating the achievement of business objectives the adherence to quality processes. We mitigate risk through the implementation of tight quality controls: standard policies, procedures, roles, risk

assumptions, issues, and definitions, etc.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

8 CI Service Quality

8.A Offeror must provide examples of previous Offeror initiatives aimed at improving service quality.

The quality approach begins with the Service Excellence Office who provides definition and oversight of all ITIL process management and analysis functions. Process managers and analysts working in the Service Excellence Office are responsible for auditing process effectiveness, ensuring that service delivery teams comply with proper execution of processes, and analyzing process trends for anomalies. Continuous service improvement programs in collaboration with Commonwealth agencies are managed by the Service Excellence Office.

Through our Continuous Service Improvement and Innovation Process (CSIIP), the SEO reviews, analyzes and makes recommendations on improvement opportunities in each ITIL lifecycle phase. Unisys will leverage Six Sigma Lean tools and methodologies as well as ISO Certified internal audits to measure and maintain the highest quality services to the Commonwealth.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

9 CI Client Satisfaction

9.A Improve client satisfaction.

Client satisfaction is extremely important to Unisys and a key focus in our IT solution. The SEO will integrate new agencies, customers and services into our multi-pronged client satisfaction approach that includes Service Desk surveys on the caller's experience, an overall agency satisfaction survey, and quarterly surveys with the Office of Administration. Data collection will be gathered across multiple levels to gain a clear understanding of the Commonwealth's satisfaction with the IT Services being provided.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

10 CI Service Transparency

10.A Provide service transparency.

Offeror must provide examples of previous Offeror initiatives aimed at providing service transparency; in particular, visibility into the service execution process

The service organizations will use standardized ITSM services processes, IT monitoring and automation tools. ITSM processes will be documented in the Commonwealth Computing Procedures Manual (CCPM). The CCPM will be available to Commonwealth approved staff on the Knowledge Management Portal (KMP) providing desired transparency into service execution processes. Through the Real-time Dashboard, the Commonwealth will have access

to current operational performance of their application infrastructure.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

11 CI Service Sustainability

11.A Ensure service Sustainability.

Offeror must provide examples of previous Offeror initiatives aimed at ensuring service sustainability; in particular, efforts targeted at cost containment and cost reductions.

Service sustainability will be provided by integrating any new agencies, customers, or services into our standard operational and quality processes and methodologies. Leveraging ITIL processes, creating quality project plans, utilizing industry accepted measurement and monitoring tools, analyzing trending reports and providing proactive continuous service improvement throughout the IT lifecycle will enable new Commonwealth services to experience and sustain best in class IT services and client satisfaction.

12 CI Reduce Cost of Service

12.A Improve/reduce cost of service.

The Service Excellence Office will proactively manage quality, continuous service improvement, ITIL process management, and customer satisfaction through a comprehensive quality plan that specifically addresses all of these areas. We believe this is a key differentiator in our partnership with the Commonwealth. Through this new organization and these quality plans, Unisys will drive best in class services and the highest customer satisfaction experience, while reducing overall costs to the Commonwealth.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

Unisys examples of continuous improvement A few examples of capacity management continuous service improvement that have been implemented or can be utilized to achieve reduced costs of Services and to meet or exceeded ROI (Return on Investment) analysis projections are outlined below:

1. Server Virtualization:
   The Unisys account management team has spearheaded cost savings for the Commonwealth by aggressively pursuing server virtualization efforts.

2. Storage Capacity Management:
   As part of the DPH's continuing improvements in its backup infrastructure, the DPH has improved the successful recovery an 8TB database archive for IES from 10.7 hours down to nearly 4 hours by improving the bandwidth from .75Tb/hour to 2TB/hour. The DPH accomplished this by bypassing the AIX VIO Shared Ethernet Adapter (SEA) built in restrictions and optimizing throughput between the media servers and the data domain.

3. Capacity Management – Secure private cloud:
   Unisys established a secure private cloud environment for the Commonwealth in a proof of concept. Four agencies participated in the pilot. The pilot provided the agencies

with access to a portal where they could provision servers with pre-determined configurations. Then they could stand up servers in 7 minutes through the portal, use them for a specific purpose, and then tear them down in minutes through the portal. The Commonwealth Department of State participated in the pilot and provisioned servers to test a production issue after receiving a call from operations. They fixed the application issue and tested it on the temporary servers and reduced the time to resolve the issue to minutes. These same concepts and types of technology will be utilized to provide the Commonwealth with Capacity on Demand.

4. Capacity Management - z10 Migration to z196 Processor:
The Commonwealth Department of Labor and Industry required services for much longer duration on the DPH mainframe platform than originally planned. The DPH team brought forth a solution to replace the z10 processor with a z196 processor. This offered a number of benefits to the Commonwealth including additional processor capacity, a boost in the integrated facility for Linux (IFL). The system also offered improved performance and increased processor speed with optimizations for DB2 and WebSphere, since this processor offered more capacity.

5. Capacity Management - IBM Business Class Mainframe processor MIPS
The z10 processor utilization rates were projected to exceed the capacity of the z10 mainframe within the year 2011 due to increases in unemployment compensation transaction workload and delays in the mainframe application modernization efforts. The Unisys Team was able to locate an IBM Business Class processor in excess inventory through our subcontractor IBM. This machine was equipped with the capacity required to support the Department of Corrections (DOC). At no additional cost to the Commonwealth, we seamlessly migrated DOC workload from the z10 mainframe system to the business class processor, providing 180 MIPS of capacity relief on the z10.

Unisys Team Experience

Unisys has many customers where the Unisys Capacity Management Team(s) are actively managing capacity for the infrastructure supporting critical business applications. Some of the customers here in the United States include:

- American Red Cross
- City of Santa Clara
- SMS800
- City of Minneapolis
- The Commonwealth of Pennsylvania

The Unisys Team has a history of improving capacity management with the Commonwealth as evidenced by the samples of continuous improvement provided above.

Benefits to the Commonwealth

The Unisys Capacity Management Solution provides a platform for the Unisys Team to manage capacity in support of Commonwealth agency applications and provide:

- Improved utilization of server and storage infrastructure
- Improved capacity services with ROI's that are compelling
- Capacity on Demand for emergencies, ad-hoc and unplanned requirements.

3.2.2.4 DR Planning & Testing

The DR Planning & Testing service ensures that the Offeror provides expert assistance in developing, documenting, deploying, and testing tiered datacenter recovery strategies that includes access for Commonwealth end users. This service will protect the identified applications processing at the datacenters, Commonwealth employees and constituents who utilize the application.

The Commonwealth will provide the Offeror with a list of agency applications that require a DR solution and related DR plan after contract is awarded. The Offeror is expected to provide DR Planning and Testing Services for agency applications that require DR Services. For Commonwealth agency applications that do not currently have DR plans, these Services will be provided in the event the Commonwealth elects to order DR services for these applications.

Reference Documentation

Exhibit B.5 - DPH - Agency Disaster Recovery Matrix

Schedule J.1 - Datacenter Service Level Management

Requirements		Describe Compliance
1.	Meet with the Commonwealth and agency representatives on an annual basis and upon request to assess its DR requirements. Post contract award, Offeror must document the Tiered DR plans in an online software program that will be available to Commonwealth and Offeror staff. The documented plans must be made available at the time each individual critical application is transitioned to the Offeror's managed Services.	Offeror must discuss its approach to providing a Tiered DR service offering to meet the needs of the agencies. Offeror must provide at least one relevant example from a prior engagement, in which it was engaged, that is similar to the DR needs of the Commonwealth. Offeror must discuss the DR capabilities that are included in its proposed Architecture.

2.	Review and update Disaster Recovery Plans (DRPs) - Offeror must review existing Disaster Recovery Plans (DRPs) to determine gaps in existing or future DR Services, within the first 120 days after the Effective Date. The Offeror must at least annually review and update the disaster recovery plans. Assist the Commonwealth in identifying dependencies/limitations to DR testing due to non-Offeror infrastructure.	Offeror must describe an approach to perform a gap analysis of the existing Disaster Recovery Plans (DRPs). Offeror must include a description of the process it will use to track and resolve all identified gaps.
3.	Provide the Commonwealth and agency representatives with access to an online DR planning tool.	Offeror must discuss its approach to meet this requirement. Identify and describe the proposed online DR planning tool.
4.	Provide the Commonwealth and agency representatives with access to an automated emergency notification system. This would be invoked on the occasion of a disaster or other emergency.	Offeror must discuss its approach to meet this requirement. Identify and describe the proposed emergency notification system that could be used to invoke a DR event.
5.	Assist the Commonwealth and agency representatives as requested to review agency identified critical business applications and related IT applications and infrastructure.	Offeror must discuss its approach to meet this requirement.
6.	Assist the Commonwealth and agency representatives as requested in developing, documenting, deploying, and exercising its tiered disaster recovery plans.	Offeror must discuss its approach and optional service offering. Offeror must describe its approach to perform a successful recovery test within 6 months of transition to the Offeror's Managed Service.
7.	Assist the Commonwealth and agency representatives as requested in coordinating disaster recovery	Offeror must discuss its approach and optional service offering.

	exercises. Frequency of DR exercises will be at the discretion of the Commonwealth. The Offeror must every six (6) months test the operability of the disaster recovery plan then in effect.	
8.	Assist the Commonwealth and agency representatives as requested in developing, documenting, deploying, and exercising its continuity of operations (COOP) and continuity of government (COG) plans.	Offeror must discuss its approach.
9.	Assist the Commonwealth and agency representatives as requested in integrating its disaster recovery plans into its COOP and COG plans.	Offeror must discuss its approach.
10.	As requested by the Commonwealth, evaluate the efficiency of business partner disaster recovery and/or business continuity plans.	Offeror must discuss its approach.
11.	In concert with the Commonwealth and agency representatives, lead the recovery operations as requested in the event of a disaster or other major disruption.	Offeror must discuss its approach and optional service offerings.
12.	Conduct disaster recovery planning and activities in accordance with the Business Continuity Institute Good Practice Guideline or similar standard.	Offeror must identify the standard and describe its approach to meet this requirement.
13.	Ensure DR Planning & Testing Services are documented in the Service Catalog.	Offeror must provide a prototype of this section of the Service Catalog.

Continual Service Improvement		
14.	Reduce service risks.	Relative to the service in question, Offeror must provide examples of previous Offeror initiatives aimed at eliminating or mitigating service risks.
15.	Improve service quality.	Offeror must provide examples of previous Offeror initiatives aimed at improving service quality.
16.	Improve client satisfaction.	Offeror must describe methods to continually improve client satisfaction.
17.	Provide service transparency.	Offeror must provide examples of previous Offeror initiatives aimed at providing service transparency; in particular, visibility into the service execution process.
18.	Ensure service sustainability.	Offeror must provide examples of previous Offeror initiatives aimed at ensuring service sustainability; in particular, efforts targeted at cost containment and cost reductions.
19.	Validate business case for cost of the service.	Offeror will provide examples to validate the projected cost savings or cost avoidance projected versus the cost of using this service.
20.	Improve/reduce cost of service.	Offeror must provide examples of previous disaster recovery initiatives implemented that achieved reduced costs of Services and that met or exceeded ROI (Return on Investment) analysis projections. If costs of Services increased due to increased required capabilities, so identify.
Deliverables		
Deliverables are defined in **Schedule K – Key Program Deliverable**		
Offeror Response		

Introduction

Over the years the Commonwealth has experienced continually improving data protection through the Unisys practice of providing regular tests of the Disaster Recovery Plans for Commonwealth agencies that already subscribe to these services.

In the new solution this practice of continual improvement through regular testing, remediation, refinement and capacity growth continues. The Unisys Disaster Recovery Team will provide a more diverse range of Disaster Recovery tiers for the Commonwealth and its agencies as described below.

1 DR, Annual DR Review, Example (experience)

1.A Meet with the Commonwealth and agency representatives on an annual basis and upon request to assess its DR requirements

Unisys has deep experience supporting current DPH disaster recovery plans. By choosing Unisys as a partner the Commonwealth benefits from this experience as well as the Unisys-implemented [redacted] Living Disaster Recovery Planning System (LDRPS) which will meet the Commonwealth's need for an online disaster recovery planning tool.

Commonwealth agencies also benefit from the implementation of the LDRPS infrastructure because the IT Risk Manager and DR coordinators in the Unisys team's Program Management Office will use the tool to import existing Agency DR plans as well as maintain updates to the plans on an annual basis as well as upon Agency request.

Unisys will meet with the Commonwealth and agency representatives on an annual basis and upon request to assess its DR requirements.

1.B Post contract award, Offeror must document the Tiered DR plans in an online software program that will be available to Commonwealth and Offeror staff. The documented plans must be made available at the time each individual critical application is transitioned to the Offeror's managed Services.

LDRPS will be populated with the Tiered DR Services described below and will be populated in conjunction with critical application migration to the Managed Services offered by the Unisys team.

1.C Offeror must discuss its approach to providing a Tiered DR service offering to meet the needs of the agencies.

The Commonwealth has specified two distinct RPOs for open systems servers in the Schedule I "Volumetrics" based on restore from backups. The Enterprise Services Catalog will also include costs for replication of disk-based backups from production to the DR facility as well as mainframe storage replication. These latter two tiers provide like-to-like services that exist in the current DPH infrastructure but are not called out in the RFP.

1.D Offeror must provide at least one relevant example from a prior engagement, in which it was engaged, that is similar to the DR needs of the Commonwealth.

The California State University (CSU) system recently renewed its long-term contract with

Unisys after a competitive bid that showed the value of the Unisys solution versus market alternatives. CSU was impressed with the Unisys managed services offering and opted to increase the Unisys scope to include a tiered Disaster Recovery system. Like the Commonwealth, CSU has critical applications that run on both physical and virtual instances of Windows and Unix operating systems.

1.E Offeror must discuss the DR capabilities that are included in its proposed Architecture

The capabilities are described in 1.C above.

2 DR, Review and Update DR plan, DR Plan Gap Analysis and Tracking

2A Review and update Disaster Recovery Plans (DRPs) - Offeror must review existing Disaster Recovery Plans (DRPs) to determine gaps in existing or future DR Services, within the first 120 days after the Effective Date.

The IT Risk Manager and DR coordinators will maintain a focus on maintenance and review of the Agency DRPs. Unisys expects, over time, that these will likely coalesce into a broadly comprehensive Disaster Recovery strategy that utilizes the Unisys multi-data center architecture and tiers of DR services.

As part of the transition, the IT Risk Manager will review the existing Disaster Recovery Plans to determine gaps within the first 120 days.

2.B The Offeror must at least annually review and update the disaster recovery plans.

Assist the Commonwealth in identifying dependencies/limitations to DR testing due to non-Offeror infrastructure.

Unisys IT Risk Manager will work with the agencies to review and update the DRPs on at least an annual basis.

For agencies with current subscriptions to Unisys-provided testing and services, Unisys already meets regularly to address recovery gaps and to review and examine recovery time and recovery point objectives based on the criticality of the application platforms. Thus tailored plans already exist for these Agencies and that will reduce the time needed by Unisys to integrate all agency DRPs within the Unisys-provided online disaster recovery tool and incorporate all DRPs under review and management by the Unisys Program Management Office.

For Agencies that do not currently use Unisys services, Unisys expects that the Commonwealth is currently served by a wide variety of Disaster Recovery plans maintained by each agency. On average Unisys expects that many agencies have adequate plans but within the variety Unisys expects to discover under-funded plans with significant gaps and over-funded plans that likely protect non-critical assets. Unisys has deep experience supporting current DPH disaster recovery plans. By choosing Unisys as a partner the Commonwealth benefits both from this experience as well as the Unisys-implemented [redacted] Living Disaster Recovery Planning System (LDRPS). Unisys seeks to bring all Agency DRPs within the proposed LDRPS framework so that Unisys can help the Commonwealth arrive at standardization in the Agency approaches to DR, coverage of the significant gaps and cost efficiencies through coverage appropriate to an

asset's criticality.

2.C Offeror must describe an approach to perform a gap analysis of the existing Disaster Recovery Plans (DRPs).

As described in 1.B, the IT Risk Manager will meet with directors on an agency-by-agency basis during transition to review existing DRPs and bring them into the Unisys-provided LDRPS online tool.

2.D Offeror must include a description of the process it will use to track and resolve all identified gaps.

The Unisys IT Risk Manager and members of the Unisys architecture team will meet with directors on an Agency-by-Agency basis to identify critical applications and the required Recovery Time Objectives and Recovery Point Objectives for these applications so they can be mapped to DR tiers in the Unisys-managed data centers. Any gaps identified in the DR plan will have solutions developed to close the gaps. To do this we will use the process described in this proposal to develop solutions for the Commonwealth moving forward.

3 Portal, Online DR Planning Tool

3.A Provide the Commonwealth and agency representatives with access to an online DR planning tool.

Offeror must discuss its approach to meet this requirement. Identify and describe the proposed online DR planning tool.

The Commonwealth seeks an easy-to-use online disaster recovery tool that will allow all agencies to maintain their diverse DRPs within a single tool.

Unisys proposes to leverage the [redacted] (LDRPS) to meet this requirement. This is the same tool which is currently in place to manage the DRP related to IBM mainframe services and the [redacted] facility. Unisys will exploit the full capabilities of the tool to build strong

- Crisis management plans to fit each agency's operational structure.
- Technology recovery plans delineating Unisys and Commonwealth responsibilities, including dependency mapping for the infrastructure supporting Commonwealth-managed applications. The matrix management will allow the Commonwealth oversight to how the Unisys DR teams manage a diverse set of critical and separate application groups within concurrent work streams and deliver to the required RPOs.
- Critical application recovery plans to smoothly interface with your infrastructure recovery plans.
- Process or departmental recovery plans to support your planning decisions and strategies and to identify dependencies between critical business processes.
- Site event management plans to document how to deal with a specific incident at a particular business location.

This proposed tool reduces the time needed to train users by providing step-by-step guidance

to plan builders. Agency planners are shown Unisys DR tiered offerings as well as [redacted] best practices and methodology while building customized DRPs.

4 DR, Emergency Notification System

4.A Provide the Commonwealth and agency representatives with access to an automated emergency notification system. This would be invoked on the occasion of a disaster or other emergency.

The Commonwealth seeks a common emergency notification tool that can be used to notify key agency personnel of any emergency situations that require immediate escalations and notifications.

The Commonwealth benefits from a partnership between Unisys and Everbridge to deliver a powerful, reliable and responsive Auto-Notification system. Furthermore through Incident Management on the Unisys ITSM we have the ability to automatically notify individuals of outages and escalate to right resources immediately for resolution.

4.B Offeror must discuss its approach to meet this requirement. Identify and describe the proposed emergency notification system that could be used to invoke a DR event.

Gartner Inc. has named Everbridge a leader in its 2012 Magic Quadrant for U.S. Emergency / Mass Notification Services (EMNS), which assesses vendors on their completeness of vision and ability to execute that vision.

Everbridge empowers better decisions with interactive communications throughout the incident lifecycle to protect your most important assets. Everbridge helps more than 30 million people communicate in a crisis and connect on a daily basis.

The company's notification platform is widely regarded for its:

- Elastic Infrastructure Model that delivers near infinite scale
- Advanced mobile connectivity
- Real-time reporting and analytics

Unisys will work with the Commonwealth to determine the proper list of key personnel to include on any auto-notification and the specific scope of notifications that the Commonwealth seeks.

5 Application Review, Critical

5.A Assist the Commonwealth and agency representatives as requested to review agency identified critical business applications and related IT applications and infrastructure

The Commonwealth seeks regular reviews of the Agency DRPs and critical business applications and aligns these to critical infrastructure. Unisys expects, over time, that these will likely coalesce into a broadly comprehensive Disaster Recovery strategy that utilizes the Unisys-maintained Disaster Recovery site with Tiers of DR services. This review process will confirm that DRPs are changed when changes to the application infrastructure occur.

5.B Offeror must discuss its approach to meet this requirement.

The Unisys Disaster Recovery Services function is responsible for the management of the Disaster Recovery Infrastructure On Demand service offering that verifies the availability of Disaster Recovery infrastructure; servers, storage systems, networking capabilities. The infrastructure provided will enable Commonwealth data centers to recover critical business applications and data in the event of a disaster. This function is performed by a complementary blend of resources from Unisys and IBM Global Services who possess comprehensive experience developing Disaster Recovery Plans and conducting routine testing exercises with agency participation across all platforms supported in the data center.

- **Disaster Recovery Planning*:*** The disaster recovery planning function provides that the Commonwealth receives expert assistance in developing, documenting, and deploying tiered data center recovery strategies that include access to the planning tool for Commonwealth end-users.

- **Disaster Recovery Testing*:*** The disaster recovery testing function provides assistance to the Commonwealth and agency representatives with exercising its tiered disaster recovery plans, which will occur on an annual or semi-annual basis.

Reporting to the Security Manager is the IT Risk Manager who is responsible for oversight of IT Continuity functions including Unisys business continuity planning and disaster recovery including coordinating required staff and resources to execute regular Unisys business continuity and disaster recovery testing and improvements. The IT Risk Manager, Kevin Gemmell, has worked in the capacity of this role on the Data PowerHouse contract for the past four years, identifying risk areas and establishing plans to mitigate them.

Unisys places high priority in establishing Disaster Recovery (DR) capabilities and aligning them with the Commonwealth's Business Continuity plans. We consider that our state government must successfully survive disasters that disrupt equipment, data, buildings and key personnel. Unisys assists organizations to carefully plan, prepare and test for such eventualities.

Unisys, as part of its overall Governance, will assist the Commonwealth in creating or revising its enterprise business continuity planning and business continuity management strategy.

Unisys believes this will complete the gap between the technical and business strategies enabling a complete holistic end to end approach for the Commonwealth's business continuity requirements.

As part of the on-going business continuity planning, Unisys assigns a Disaster Recovery Planner to continually keep the required documentation about the servers and services, communication plans and the operational procedures updated. In cooperation with the Commonwealth disaster recovery tests are conducted twice per year to verify the documentation, communication plans and operational procedures are working and that the operational personnel is trained for an emergency.

6 Test, Recurring Disaster Recovery

6.A Assist the Commonwealth and agency representatives as requested in developing, documenting,

deploying, and exercising its tiered disaster recovery plans

Unisys IT Risk Manager assists the Commonwealth and the agencies in bringing the Unisys DR capabilities to bear on the Commonwealth's business continuity and disaster recovery objectives. The IT Risk Manager consults and collaborates on how the various DR tiers meet the Commonwealth's requirements and on special solutions that need to be implemented.

6.B Offeror must discuss its approach and optional service offering.

The Unisys-provided testing will utilize Enterprise Services Catalog DR resources selected by the Commonwealth to meet DR RTO/RPO targets. Unisys plans for two tests per year for critical applications.

Prior to conducting the test, Unisys and the agency formulate recovery goals associated with each test. During the DR test, Unisys staff recovers the application infrastructure following the DRP. Once the application infrastructure has been recovered, the agency can begin its application testing. The DR coordinator provides overall management of the test and acts as the point of escalation for the Unisys Team and the agency participants. The coordinator records the timing and completion of all activities of the DR plan. Any problems encountered are recorded on an issues register to be escalated and addressed by the appropriate owning organization.

Unisys uses every DR test as a learning experience. We document issues, delays, and process efficiencies so that after-the-fact we can follow-up with process improvements and lessons learned that are implemented prior to the next test. A post-test review is conducted with the agency to verify that findings are appropriately documented, and follow-up actions have been assigned and completed. From there the report is created that documents the activity.

6.C Offeror must describe its approach to perform a successful recovery test within 6 months of transition to the Offeror's Managed Service

The Commonwealth seeks to begin DR testing within 6 months of transition to the new Unisys Managed Services contract. A DR Coordinator will coordinate testing activity with each agency as workload transitions into the managed service. The Commonwealth will be provided a single point of contact with whom to review the Unisys progress toward the specified date.

7 Exercise, DR

7.A Assist the Commonwealth and agency representatives as requested in coordinating disaster recovery exercises.

Unisys DR coordinator acts as a single point of contact for coordinating disaster recovery exercises. The Commonwealth uses the Unisys managed disaster recovery facilities in the new contract and has 24x7 access to the facilities versus the current [redacted] subscription-based access that adheres to tight schedules aligned to [redacted] priorities. This makes it much easier for the Commonwealth to choose or change the frequency of DR exercises at its discretion.

Unisys will apply its normal monitoring and management tools to the Disaster Recovery data

center equipment. So, unlike the existing [redacted] contract, the majority of the network infrastructure need not be specially built for the testing or for actual DR. The equipment is maintained in a "warm" status.

7.B The Offeror must every six (6) months test the operability of the disaster recovery plan then in effect

The Unisys Team has determined the labor required for this testing frequency and included this within the Enterprise Services Catalog offering for DR testing. The Unisys Team is able to provide this service based on our experience working with Commonwealth disaster recovery exercises.

7.C Offeror must discuss its approach and optional service offering

The Commonwealth benefits from more flexible test schedules and ready availability of DR assets within each Agency's DRP. The earlier tests performed with [redacted] needed to be squeezed into specific 72- to 96-hr slots because [redacted] scheduled continuous tests across its large customer base. This limited the Commonwealth's access to extensive tests across agencies. No such limitation exists with the Unisys-managed facilities.

Unisys is also able to make use of the LDRPS tool to monitor the capacity of the Unisys Disaster Recovery data center and advise Agencies on the need for capacity increases to match critical application capacities in Production.

8 Exercise for COOP, Continuity of Government (COG) Exercise

8.A Assist the Commonwealth and agency representatives as requested in developing, documenting, deploying, and exercising its continuity of operations (COOP) and continuity of government (COG) plans. Offeror must discuss its approach.

The Commonwealth is right to call out the distinction between its continuity of operations (COOP) and continuity of government (COG) plans. The Unisys IT Risk Manager will assist with both the continuity plans at the COOP and COG levels. He relies upon the LDRPS tool to assess gaps between agency plans and will schedule cross-agency meetings with the appropriate Agency Risk/Continuity Officers to stage table-top walkthroughs to simulate DR sequencing and identify gaps in sequencing and dependencies between agencies.

9 Integration, DR integrated into COOP and COG

9.A Assist the Commonwealth and agency representatives as requested in integrating its disaster recovery plans into its COOP and COG plans. Offeror must discuss its approach.

The Commonwealth recognizes that a cross-agency review of existing Disaster Recovery Plans (DRPs) will likely reveal gaps as well as over-spends. Unisys has proposed a cost-effective Disaster Recovery infrastructure as part of this proposal and can use this in discussions with agencies to benchmark existing plans. Furthermore, the Agencies can make cost-case comparisons as Unisys works with each agency to input the current DRPs into LDPRS.

10 DR, Business Partner Evaluation

10.A As requested by the Commonwealth, evaluate the efficiency of business partner disaster recovery

and/or business continuity plans. Offeror must discuss its approach.

At the request of the Commonwealth through the Enterprise Services Catalog, Unisys will evaluate the efficiency of business partner disaster recovery and business continuity plans.

11 DR, Recovery Operations Leadership

11.A In concert with the Commonwealth and agency representatives, lead the recovery operations as requested in the event of a disaster or other major disruption. Offeror must discuss its approach and optional service offerings.

The Commonwealth seeks a partner to lead the recovery operations in the event of a disaster or other major operations. In the event of a disaster, Unisys will take a leadership role, as requested by the Commonwealth and coordinate the execution of the Disaster Recovery Plan in coordination with the agency representatives.

By virtue of continuing DR testing across the Unisys customer base, the Unisys DR team develops overall best practices that are shared with the Unisys DR team dedicated to Commonwealth DR testing.

The Unisys Team has provided continuously improving Disaster Recovery services throughout the current DPH contract. We continuously apply lessons learned to refine processes to be incorporated in future tests or leveraged in the event of an actual disaster.

12 DR Planning Standards

12.A Conduct disaster recovery planning and activities in accordance with the Business Continuity Institute Good Practice Guideline or similar standard.

12.B Offeror must identify the standard and describe its approach to meet this requirement.

The Commonwealth cites the Business Continuity Institute Good Practice Guidelines in reference to business continuity standards. Unisys proposes an alternate and more targeted Good Practice guideline, namely the Unisys CSIIP program applied annually to the Commonwealth DR testing in conjunction with the [redacted] online LDRPS tool. Unisys notes that the BCI standard offers certification for its members for a very general and broad level of expertise with a certificate that is now based on 2010 practices. In contrast the Unisys CSIIP DR program applied to the Commonwealth provides metrics to measure the Commonwealth DRPs as well as providing proposals to continuously improve upon DR plans and approaches.

Unisys assesses itself through the newly developed ISO 22301-2003 standard and maintains a Certified Business Continuity Professional (CBCP) on staff who is trained in the 10 Professional Practices for Business Continuity Management offered by the Disaster Recovery Institute. This practice continues in the new contract.

13 Test, DR Planning and Testing Services

13.A Ensure DR Planning & Testing Services are documented in the Service Catalog.

13.B Offeror must provide a prototype of this section of the Service Catalog.

The Enterprise Services Catalog offering includes these DR Tiers:

- Tier 1: Recovery from backup tapes within reasonable time frame.

- Tier 2: Recovery from a backup tapes within an accelerated period.
- Tier 3: Recovery from backups and replicated data to DR via the [redacted] infrastructure.
- Tier 4: Recovery through asynchronous data replication for Open Systems SAN storage removing the need for data recovery.
- Tier 5: Data and O/S level replication for virtual Windows/Linux instances removing the need for data recovery.
- Tier 6: With Agency approval the Tier 5 offering can be utilized to provide an automatic failover capability.

These tiers benefit from the Unisys data center solution that has the added characteristic of geographically dispersed locations. With DR that requires geographically dispersed nodes, the [redacted] site enables the placement of systems in separate metrological and metropolitan regions and different seismic zones.

Continual Service Improvement

Unisys recognizes the significant importance of Quality and Continuous Service Improvement to:

- Reduce service risk,
- Improve service quality,
- Improve client satisfaction,
- Provide service transparency, and
- Improve/reduce costs of service.

Through a continuous cycle of evaluation and improvement within an IT infrastructure, Unisys views quality and continuous service improvement as a critical success factor in driving customer satisfaction for the Commonwealth IT infrastructure. Each of the continuous service improvement areas identified above are driven through the tight integration of the following organizations, industry tools, proven processes and quality deliverables:

- Service Excellence Office,
- Quality Plans: transition and steady state service delivery
- Industry standard frameworks and methodologies: ITIL, ISO, SSL
- Industry accepted measurement tools
- Continuous Service Improvement & Innovation Processes (CSIIP)
- Risk management, audits and business continuity management
- Client Satisfaction Surveys and Knowledge Management Portal

Collectively this represents Unisys Integrated Quality Plan for the Commonwealth of

Pennsylvania.

Specifics on each of these areas are outlined in Schedule F, Section 3.2.1.1.6 Continuous Service Improvement. Highlights from this section are outlined below and requested service examples are provided at the end of this section.

14 CI Service Risk

14.A Relative to the service in question, Offeror must provide examples of previous Offeror initiatives aimed at eliminating or mitigating service risks.

Risk management, independent quality audits, and business continuity management are integral quality management processes. Unisys is committed to managing risks and facilitating the achievement of business objectives the adherence to quality processes. We mitigate risk through the implementation of tight quality controls: standard policies, procedures, roles, risk assumptions, issues, and definitions, etc.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

15 CI Service Quality

15.A Offeror must provide examples of previous Offeror initiatives aimed at improving service quality.

The quality approach begins with the Service Excellence Office who provides definition and oversight of all ITIL process management and analysis functions. Process managers and analysts working in the Service Excellence Office are responsible for auditing process effectiveness, ensuring that service delivery teams comply with proper execution of processes, and analyzing process trends for anomalies. Continuous service improvement programs in collaboration with Commonwealth agencies are managed by the Service Excellence Office.

Through our Continuous Service Improvement and Innovation Process (CSIIP), the SEO reviews, analyzes and makes recommendations on improvement opportunities in each ITIL lifecycle phase. Unisys will leverage Six Sigma Lean tools and methodologies as well as ISO Certified internal audits to measure and maintain the highest quality services to the Commonwealth.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

16 CI Client Satisfaction

16.A Offeror must describe methods to continually improve client satisfaction.

Client satisfaction is extremely important to Unisys and a key focus in our IT solution. The SEO will integrate new agencies, customers and services into our multi-pronged client satisfaction approach that includes Service Desk surveys on the caller's experience, an overall agency satisfaction survey, and quarterly surveys with the Office of Administration. Data collection will be gathered across multiple levels to gain a clear understanding of the Commonwealth's satisfaction with the IT Services being provided.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional

details in this area.

17 CI Service Transparency

17.A Offeror must provide examples of previous Offeror initiatives aimed at providing service transparency; in particular, visibility into the service execution process.

The service organizations will use standardized ITSM services processes, IT monitoring and automation tools. ITSM processes will be documented in the Commonwealth Computing Procedures Manual (CCPM). The CCPM will be available to Commonwealth approved staff on the Knowledge Management Portal (KMP) providing desired transparency into service execution processes. Through the Real-time Dashboard, the Commonwealth will have access to current operational performance of their application infrastructure.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

18 CI Service Sustainability

18.A Offeror must provide examples of previous Offeror initiatives aimed at ensuring service sustainability; in particular, efforts targeted at cost containment and cost reductions.

Service will be sustained by integrating any new agencies, customers, or services into our standard operational and quality processes and methodologies. We leverage ITIL processes, create quality project plans, utilize industry accepted measurement and monitoring tools, analyze trending reports and provide proactive continuous service improvement throughout the IT lifecycle. This enables new Commonwealth services to experience and sustain IT services and client satisfaction.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

19 CI Business Case Validation

19.A Offeror will provide examples to validate the projected cost savings or cost avoidance projected versus the cost of using this service.

The Catalog of Services approach to provisioning DR services provides the Commonwealth with significant opportunities for cost savings. Most organizations approach Disaster Recovery as a Like-to-Like issue and sometimes build out a DR site that is identical in computer power as the Production data center. With the Catalog of Services the Commonwealth could better manage the cost of Disaster Recovery to the likely risks of an actual disaster. For instance, when Unisys crafted the Disaster Recovery plan for the California State University system (CSU) they were reluctant to incur the cost of an identical compute power for a DR plan that they hoped never to use. Unisys presented two options to reduce cost:

1. For virtual servers the computer power was provisioned at a less than 100% of that available for production. CSU was willing to accept a diminished level of service immediately following an actual data center disaster and Unisys was able to propose a reasonable delivery date to augment the DR facility if an actual disaster occurred. The difference between the current computer power in the DR site and that of the

Production data center delivers a monthly savings for CSU.

2. Unisys also provided a means for CSU to utilize assets provisioned for their DR plan as Test and QA/Development servers under the agreement that if an actual disaster occurred then these services would be suspended so that these assets could be pulled into use as the Production infrastructure at the DR site. This allowed CSU to leverage the compute power of the DR site at relatively little risk.

The agencies in the Commonwealth can, working with IT Risk Manager, select servers and storage in the DR facility that would provide a diminished services in the event of an actual disaster. Given the very unlikely chance of an actual disaster this would allow the Agencies to better balance the full cost of a Like-to-Like DR solution against the risk of occurrence of an actual disaster.

20 CI Improve or Reduce Cost

20.A Offeror must provide examples of previous disaster recovery initiatives implemented that achieved reduced costs of Services and that met or exceeded ROI (Return on Investment) analysis projections. If costs of Services increased due to increased required capabilities, so identify.

The Service Excellence Office will proactively manage quality, continuous service improvement, ITIL process management, and customer satisfaction through a comprehensive quality plan that specifically addresses all of these areas. We believe this is a key differentiator in our partnership with the Commonwealth. Through this new organization and these quality plans, Unisys will drive best in class services and the highest customer satisfaction experience, while reducing overall costs to the Commonwealth.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

Unisys examples of continuous improvement

Examples of continuous service improvement have been included below under Unisys Team Experience.

Disaster Recovery – Cost Reduction:

The VM replication improved the Recovery Point Objective of our NetBackup master servers from 24 hours down to approximately 6 hours. The reduction in effort resulted in lower labor costs to execute this first step in the DR process.

Disaster Recovery – File Replication Improvement:

The DPH has implemented Distributed File Systems (DFS) to replicate our DPH File Server down to [redacted] In the event of a true disaster, files to perform our duties during and after the DR will be available. Data replication occurs in real time and is de-duplicated over the wire thus saving bandwidth on the WAN link. This confirms that our documentation, recovery scripts and procedures are current and accessible at all times to support Commonwealth agencies during disaster recovery drill and in the event of an actual disaster. By avoiding having to ship tapes containing this information to [redacted] and having to restore them,

Unisys has improved the recovery time objective for disaster drills and disaster events.

Disaster Recovery – NetBackup improvement:

VM replication was implemented to improve the Recovery Point Objective of our NetBackup master servers from 24 hours down to approximately 6 hours. This change will also lower the time it takes to recover the NetBackup server in the DR environment from 2.5 hours to around 30 minutes expediting the start of DR database recovery efforts by almost 80 percent.

Disaster Recovery – recovery time improvement:

To improve disaster recovery times, we converted AIX mksysb to ISO images to facilitate a much faster server recovery time. Prior to this change, we used CD images or mksysb restores from tape. This resulted in an 85% improvement in recovery times.

Storage Replication improvement:

Storage replication solutions have been implemented for several agencies using the latest disk to disk replication technology. These solutions have enabled a reduced dependency on tape media and drives for backup while providing a disk to disk update to offsite data supporting both data backup as well as disaster recovery requirements. Ongoing research and trials are conducted in conjunction with product support organizations to confirm proper configuration and optimal performance for the technology supporting this critical managed service.

PSP VDI improvement:

The State Police was impacted when one of its barracks was closed down due to a mold infestation and they were unable to access computers and have staff in that location for weeks. They were interested in a business continuity plan that would enable them to have access to their files and applications from a remote location. We worked with them to establish a VDI proof of concept at the DPH. Using the Virtual Desktop Interface, they were able to access their information from iPads from any location.

Unisys Team Experience

The Continual Service Improvement sections above provide details of the Unisys Team's rich experience and the value that they have brought to the Commonwealth and its Agencies over the past many years. But the Commonwealth is likely unaware of the breadth of Unisys experience in providing reliable Disaster Recovery operations that provide significant value to customers.

Setting Customers on a course to DR

Unisys provides a service in the market called the Unisys Disaster Recovery

Architecture Service. As part of this service, the Unisys team conducts a comprehensive 2-day seminar to provide customers with a solid foundation on which to build an end-to-end application and data disaster recovery capabilities. This service mirrors the embedded service provided to the Commonwealth in this proposal and managed by the Unisys IT Risk Manager on

an agency-by-agency basis. For instance the Unisys Disaster Recovery Architecture Services provides:

- Reduction of costs through
  - The deployment of mature recovery services management
  - The collective disaster recovery architectures and processes financially rationalized against explicit, business-driven recovery targets
- Mitigated risk through
  - Knowledge transfer that allows each IT function to understand its specific role within the overall, end-to-end recovery process
  - Institution of proven and formalized recovery services management that yields reliable, disaster recovery capabilities
- Restored quality of service as shown by
  - Disaster recovery, service performance reviews that build confidence through "proof of delivery capability" reports - Actual disaster recovery costs that become transparent to the business

Saving Money with efficient DR

Solution

JMC Steel Group worked with Unisys to design and execute a sizeable data center migration and modernization initiative, which standardized the SAP infrastructures at two key data centers on a common hardware platform – and provided the bullet-proof disaster recovery capabilities these critical environments demand.

Results

Carrying out its data center transformation strategy enabled JMC Steel to better support the operations of two major manufacturing facilities. Plus, by making a robust disaster recovery capability a key component of the project, the company greatly improved its ability to avoid the numerous harmful effects of both planned and unexpected downtime.

Metrics

- **Resiliency:** 15-minute recovery time objective (RTO) established and confirmed via testing of automated backup and failover capabilities.
- **Performance:** 300 percent increase in hardware performance and 50 percent reduction in response times.
- **Cost avoidance:** $250,000 in lost revenue per four hours of downtime avoided.

Protecting Alabama State citizens through improved DR

The Alabama Criminal Justice Information Center (ACJIC) is a state agency providing local, state, and federal criminal justice agencies with the information needed to provide citizen safety. ACJIC realized that gaps in its information technology were hindering communications and business continuity. It needed to more efficiently deliver critical information from its network

and systems.

Unisys provided a real–time infrastructure with improved disaster recovery and business continuity through a turnkey solution comprising an ES7000/one enterprise server platform, Unisys SafeGuard 30m, and EMC SAN technology.

By implementing the system, ACJIC now has a dependable, cost–effective system that delivers real–time information to end users, supports future growth, and provides robust, reliable operations. It also provides system patches and updates with extreme ease and supports failover requirements. The result is enhanced officer and citizen safety while building trust among constituents.

Metrics

- **Better Security:** Reduced downtime and risk – 24x7 availability with failover in less than one minute from the primary site to the disaster recovery site
- **Reduced Costs:** Lowered costs while processing some 18 million transactions monthly
- **Improved Satisfaction:** Enhanced citizen and officer safety by ensuring a constant flow of real–time information
- **Better Productivity:** Enabled one–to–two–second searches for up to 40 million records in the Law Enforcement Tactical System

Protecting Workers' Compensation through improved IT and DR

EMC Insurance Companies has grown from a provider of workers' compensation coverage to one of the Iowa's largest property and casualty insurance providers – with over 20 branch locations and assets in excess of $3 billion.

A key factor catalyzing nearly 100 years of steady expansion has been EMC's commitment to cultivating successful, lasting relationships with independent agency partners. Yet, as these partnerships grow, so too do the demands for speedy, personalized service that is available around the clock.

With Unisys technology driving its consolidation, virtualization, and business continuity processes, EMC has established an environment that promotes responsiveness and agility across the organization. As a result, the company is better equipped to deliver and support the services that its wide network of branch locations and independent agents demand 24x7.

Metrics

- **Cost:** Consolidated and virtualized 150 existing servers down to 50.
- **Efficiency:** Streamlined disaster recovery procedures, including an 80% reduction in documented processes
- **Service:** Implemented platforms that keep mission-critical systems and applications available at all times

De Beers UK Streamlines and Strengthens IT Processes and DR

De Beers UK contracted Unisys to outsource and manage the full scope of its IT data center operations – from hosting critical applications to deploying business continuity measures to

providing technical and end-user support services.

The fully managed data center environment Unisys provided De Beers has enabled the company to improve the flexibility with which it can meet both current and future business and IT demands, eliminated the need to allocate in-house resources to routine IT management tasks, and provided the disaster recovery measures required to verify the company's infrastructure remains resilient and resistant to failure. What's more, the end-user support capabilities extended the company's resiliency gains to its employees, helping them remain productive and make positive contributions to important initiatives.

Challenge

Minimize the risk of an interruption to global operations, and better support the efforts of end users – without adding complexity or increasing management burden.

Solution

De Beers UK contracted Unisys to outsource and manage the full scope of its IT data center operations – from hosting critical applications to deploying business continuity measures to providing technical and end-user support services.

Results

The fully managed data center environment Unisys provided De Beers has enabled the company to improve the flexibility with which it can meet both current and future business and IT demands, eliminated the need to allocate in-house resources to routine IT management tasks, and provided the disaster recovery measures required to verify the company's infrastructure remains resilient and resistant to failure. What's more, the end-user support capabilities extended the company's resiliency gains to its employees, helping them remain productive and make positive contributions to important initiatives.

Metrics

- **Manageability:** Provisioned a new business intelligence application in four weeks
- **Recoverability:** Confirmed the resiliency of the new infrastructure via a full disaster recovery test

Benefits to the Commonwealth

The Unisys proposed Online Disaster Recovery Tool provides an opportunity for more cost effective Disaster Recovery services for the Commonwealth. Following transition when the Unisys IT Risk Manager had integrated Agency DR plans into the tool, the IT Risk Manager will be able to present the Office of Administration, a first-ever comprehensive and comparative view of the various Agency DR Plans. This will allow the Office of Administration (OA) to focus on those plans which appear to be paying for very high risk mitigation DR plans and review the cost efficiency on these outliers.

The Unisys proposed Online Disaster Recovery Tool will lead to far more consistent quality for Disaster Recovery services for the Commonwealth. This comprehensive and comparative view of the various Agency DR Plans also allows the OA to focus on those outlier Agencies who appear to have underfunded DR plans and are likely carrying much higher risks than might be appropriate.

The Unisys Team has consistently used lessons learned from Disaster Recovery tests to remediate existing DR plans to improve the overall quality of each DR plan. The Unisys Team

has also used these tests to propose Service Design changes that have reduced the costs of services by inserting reliable tools and processes to replace the sort of frenzied high-labor processes that would likely impede service recovery if a disaster actually occurred.

3.2.2.5 Security Management

The Security Management service must ensure the confidentiality, integrity and availability of Commonwealth information and infrastructure systems. All support and implementation activities must be conducted in accordance with, but not limited to, leading industry and Commonwealth standards, which include, but are not limited to, ISO 27001:2005 and ISO 27002:2005. The Offeror must support all related system audits at the Offeror's expense. The Offeror must maintain current security ISO 27001, ISO 9001 and ISO/IEC 20000 certifications.

The Offeror must comply with Commonwealth IT policies and directives as well as federal and Commonwealth laws, regulations and policies, including but not limited to the Criminal History Record Information Act (CHRIA), Health Insurance Portability and Accountability Act (HIPAA), Criminal Justice Information Services (CJIS) regulations, The United States Social Security Administration (SSA)regulations, IRS (Internal Revenue Service) Publications, Commonwealth Information Technology Bulletins (ITBs) and the Payment Card Industry (PCI) standards. The Offeror must work with each agency to understand and ensure compliance with all laws, regulations, and policies as they pertain to each individual agency.

Reference Documentation

Exhibit J.1 through J.3 - Commonwealth Security and Compliance Requirements

Exhibit G.6 - PSP - CJIS Security Policy

Exhibit G.9 - PSP – CCHRI

Exhibit G.7 - PSP - Summary of CJIS Requirements

Exhibit G.12 - PSP - CHRIA Handbook

Requirements		Describe Compliance
1.	Develop an annual Security Management Plan.	Offeror must describe its approach to Security Management and provide a sample of a Security Management Plan. Highlight how stated security objectives align with Commonwealth business goals, IT policies, and regulatory requirements.
2.	Deploy complement of network security systems. Implement at minimum: spam filtering, anti-virus, malware protection, firewall (web, application), intrusion prevention and detection,	Offeror must describe its proposed solution including the following: • Processes and Procedures • Tools / Applications • End User Reports

	web content filtering, virtual private network, and data loss prevention systems.	o Standard o Custom • Escalation Procedures Offeror must describe its prior experience relative to providing datacenter management and support of CJIS, CCHRI, HIPAA and PCI systems.
3.	Perform quarterly (at the Offeror's expense) Vulnerability Analyses (VA) and penetration testing to identify new or emerging information security threats. Perform penetration testing (at the Offeror's expense) and present the results of each VA on a quarterly basis. Should exposures be identified, plan and remediate the exposure in accordance with Commonwealth IT policy guidelines. Report results to the Commonwealth within the time set out in an applicable SLA. The above requirement will be for all systems/subsystems that the Offeror is responsible for including managed servers/virtual servers, network devices, security devices including , but not limited to, the following: • Performing web application firewall administration and securing web applications behind it. • Ensuring and maintaining PCI level 1 compliance. • Implementing DLP for the data center server assets to avoid a breach. • Implementing Database Firewall to secure database assets from breach.	Offeror must describe its capabilities and approach to performing vulnerability analysis and penetrating testing on a quarterly basis. Provide sample reports for each.

4.	Review network and other security logs for evidence of attacks. Utilize enterprise grade intrusion detection tool(s) to systematically identify, stop, and report security threats. Produce a monthly Security Log Analysis as part of the monthly status reports as described in RFP section IV-5 Reports and Project Control.	Offeror must describe its solution and approach.
5.	Apply operating system and other security patches. Implement a Patch Management Program to ensure the timely application of security updates on all infrastructure platforms in accordance with Commonwealth IT policy guidelines. The Patch Management Program must adhere to the Change Management process that includes Commonwealth approvals.	Offeror must describe its proposed Patch Management program.
6.	Restrict physical access to all network systems and equipment with biometric or other second factor access control systems.	Offeror must describe solution and approach to meet this requirement.
7.	Restrict access to all data in the Commonwealth network infrastructure. Restrict and control all data access right, groups and special permissions based on the data security program designed by the Commonwealth security team and/or specified by the agencies. Access level changes and	Offeror must describe solution and approach to meet this requirement.

	exceptions will be executed only when approved paperwork is complete and approved. A file of all access changes will be maintained by the Offeror for audit purposes. Offeror must support Commonwealth initiated security audits.	
8.	Evaluate the security standing of network-connected subcontractors. Conduct information security audits of prominent subcontractors on an annual basis.	Offeror must describe solution and approach to meet this requirement.
Continual Service Improvement		
9.	Reduce service risks.	Relative to the service in question, Offeror must provide examples of previous Offeror initiatives aimed at eliminating or mitigating service risks.
10.	Improve service quality.	Offeror must provide examples of previous Offeror initiatives aimed at improving service quality.
11.	Improve client satisfaction.	Offeror must provide examples of previous Offeror initiatives aimed at continually improving client satisfaction.
12.	Provide service transparency.	Offeror must provide examples of previous Offeror initiatives aimed at providing service transparency; in particular, visibility into the service execution process.
13.	Ensure service sustainability.	Offeror must provide examples of previous Offeror initiatives aimed at ensuring service sustainability; in particular, efforts targeted at cost containment and cost reductions.
14.	Improve/reduce cost of service.	Offeror will provide examples of Security Management initiatives that have been

		implemented or can be utilized to achieve reduced costs of Services and to meet or exceeded ROI (Return on Investment) analysis projections.

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

Introduction

The Unisys Team understands the vital importance of ensuring the confidentiality, integrity, and availability of Commonwealth data, applications, and critical systems. The security of the Commonwealth will be managed by the Unisys team in accordance with agency requirements for compliance with leading industry and Commonwealth standards such as ISO 27001:2005 and ISO 27002:2005 and Commonwealth IT policies and directives and federal and Commonwealth laws, regulations and policies. Unisys will work with each agency within the Commonwealth to understand their compliance requirements and verifies each agency meets applicable laws, regulations, and policies. These policies, directives, laws, and regulations include the Criminal History Record Information Act (CHRIA), Health Insurance Portability and Accountability Act (HIPAA), Criminal Justice Information Services (CJIS) regulations, the United States Social Security Administration (SSA) regulations, IRS (Internal Revenue Service) Publications, Commonwealth ITBs and the Payment Card Industry (PCI) standards. Unisys currently maintains current security ISO 27001, ISO 9001 and ISO/IEC 20000 certifications.

Security Management Organization

The Unisys security team will be organized as follows as depicted in **Figure 3.2.2.5-1**:

The Information Security function oversees the project to verify compliance with security standards and requirements and develops policies and provides periodic audits of processes and data to confirm compliance. The purpose of information security management is to align IT security with business security needs and verifies that the confidentiality, integrity and availability of the assets, information, data and services match the needs of the Commonwealth.

Information Security

Figure 3.2.2.5-1 - Information Security– Functional Overview

The IT Risk Management function is responsible for leading efforts associated with continuity of Unisys business and disaster recovery. This function also confirms that the required audits are conducted on an annual basis and that the Unisys Team participates as needed and Commonwealth audits.

The Audit and Regulatory Compliance function has accountability for Unisys Team compliance with Commonwealth IT policies and directives, and at the agency's direction federal and Commonwealth laws, regulations and policies, including the Criminal History Record Information Act (CHRIA), Health Insurance Portability and Accountability Act (HIPAA), Criminal Justice Information Services (CJIS) regulations, the United States Social Security Administration (SSA)regulations, IRS (Internal Revenue Service) Publications, Commonwealth ITBs and the Payment Card Industry (PCI) standards. This function works under the guidance of each agency to understand and verify compliance with laws, regulations, and policies as it pertain to each individual agency. The responsibility for conducting contractually required audits or arranging for participation in agency audits falls under this function.

The IT Continuity function is responsible for strategy and planning associated with continuity of our business as well as Commonwealth disaster recovery. This function leverages a disaster recovery planning tool that is shared with the Commonwealth to document disaster recovery and business continuity plans.

The Security Strategy function is responsible for development of the security plan and roadmap in collaboration with Commonwealth agencies.

The Security Policy, Planning and Governance function will meet with the Commonwealth's Security teams (OA & Agency) to participate in creating a comprehensive Security Program strategy. The Offeror and the Commonwealth Security teams will develop security awareness training content consisting of the Offeror's Security Plan documentation, Commonwealth OA and agency security policy guidelines. This function verifies the Unisys Team compliance with policy.

The Security Operations function is responsible for overseeing operational security functions including physical security and operational network security.

The Network Security function provides hosting and operational support services for security products and firewalls located at the data centers. These security devices and services protect the equipment and applications in the data centers from malicious attempts to penetrate the computing environment with worms, phishing, Trojan horse malware, and unlawful data access.

The Physical Security function provides robust physical security, including biometric access control, video surveillance, and routine security officer patrols ensuring Commonwealth and vendor assets are protected at all times.

The Information Security function oversees the project to provide compliance with security standards and requirements and develops policies and verifies periodic audits of processes and data to confirm compliance. The purpose of information security management is to align IT security with business security needs and confirms that the confidentiality, integrity and availability of the assets, information, data and services match the needs of the Commonwealth. Within this function, IT Risk Management, Information Security, IT Continuity, and ongoing audits are addressed.

The organization is led by the Security Manager. The Security Manager is the Unisys security leader who will observe all project activities to mitigate interference with the effectiveness of the Commonwealth's core operational business and to confirm that security policies and procedures are followed.

The Unisys Security Manager, [redacted] is a results-oriented leader with more than 15 years of experience supporting security product implementations, developing security strategy with Commonwealth CIOs. Mike is a seasoned professional with exceptional understanding of federal security regulations and compliance requirements. He is tasked with confirming Commonwealth regulatory compliance on this engagement and providing leadership on client projects by developing workable plans, limiting risk, and management of resources.

Reporting to the Security Manager is the IT Risk Manager who is responsible for oversight of disaster recovery including coordinating required staff and resources to execute regular Disaster Recovery testing and improvements. This individual also has dotted line responsibility for oversight of security operational staff which consists of three security-focused Network Design Engineers. The IT Risk Manager also manages SSAE-16 audits and arranges participation from the Unisys Team in agency audits. The IT Risk Manager, Kevin Gemmell, has worked in the capacity of this role on the Data PowerHouse contract for the past four years, identifying risk areas and establishing plans to mitigate them.

The Security Management service provides the technical capability to protect the confidentiality, availability and integrity of Unisys service enabling infrastructure, applications, and data as well as the Commonwealth's workloads and data. The Network and Infrastructure Security Technical Service provides building blocks and applications that instantiate and enforce security policy, protects data in motion and at rest, enables secure remote access, and identifies anomalous traffic and potentially malicious activities.

The service allows for the following:

- Management of security devices with in the data center infrastructure
- Establishing secure connections for data migration over VPN tunnels
- Implementation of internal firewalls to support a secure infrastructure
- Management and enforcement of security policies within the network.
- Surveillance, detection and prevention of anomalous traffic and potentially malicious activity.
- Secure data in motion and secure data at rest.
- Secure remote access connections into and out of the network.

1 Security Management Plan, Sample (example)

Develop an annual Security Management Plan. Offeror must describe its approach to Security Management. Provide a sample of a Security Management Plan. Highlight how stated security objectives align with Commonwealth business goals, IT policies, and regulatory requirements.

Security Management Process

Our security management process includes the following components:

Develop an Annual Security Management Plan

We will review and update the security management plan on an annual basis. **Figure 3.2.2.5-2** below illustrates our four step process to develop/enhance the security management plan:

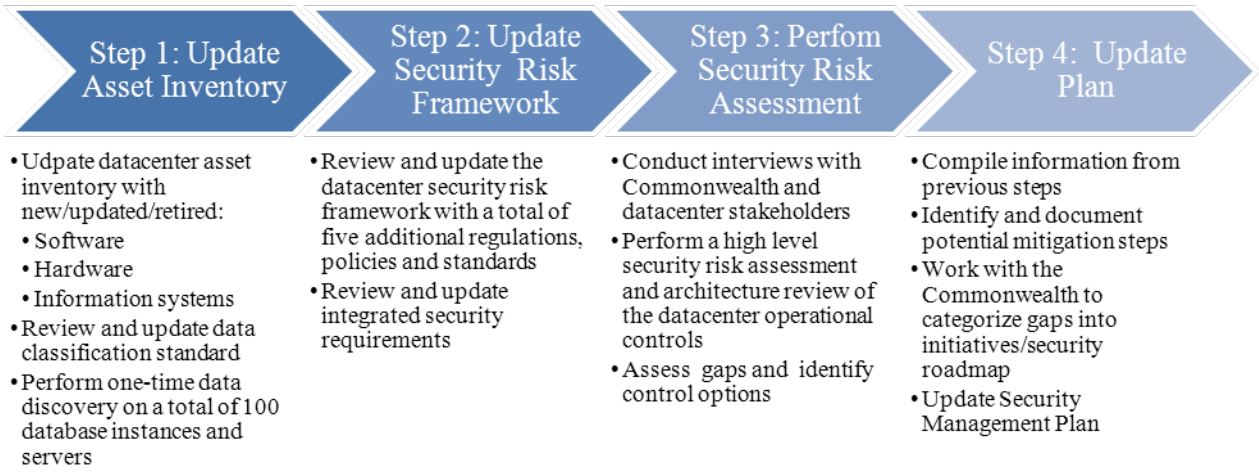


Figure 3.2.2.5-2 Security Management Plan Process

Each of the above illustrated steps are described below:

Step1 – Update data center asset inventory and perform data discovery. We will perform an annual review of the data center asset inventory and update the inventory with the new, updated and retired versions of software, hardware and information systems in addition to appropriate system owners. As part of this step, we work with the Commonwealth stakeholders to review and update the data center data classification standard. As part of this process, we review and update the current mapping of the data elements and their appropriate data classification categories in addition to data sensitivity levels.

We perform a one-time assessment using the Symantec Data Loss Prevention (DLP) solution's data discovery tool on the Commonwealth's data center infrastructure (a total of 100 servers and database instances) to identify the PII data at rest. We perform the following tasks as part of this activity:

- Document the results of the data discovery assessment in the IT asset inventory
- Identify appropriate data encryption requirements using the data center security risk framework to appropriately protect the PII data and meet the relevant regulations, policies and standards.

Step 2 – Update Security Risk Framework. We will review and augment the data center security risk framework with five additional security regulations and Commonwealth policies/standards that include revisions to:

- Commonwealth Information Technology Bulletins (ITBs)
- Federal security regulations such as Internal Revenue Services (IRS) publication 1075, Criminal Justice Information Services (CJIS), Health Information Portability and

Accountability Act (HIPAA) and United States Social Security Administration (SSA)

- Commonwealth regulations such as Criminal History Record Information Act (CHRIA)
- Industry standards and regulations such as Payment Card Industry (PCI) Data Security Standards (DSS) and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53.

These additionally identified requirements are then integrated with the data center security risk framework to identify additional data protection controls to meet the relevant regulations and business requirements.

Step 3 – Perform Security Risk Assessment and IT Architecture Review. We use the updated data center security risk framework to conduct a high level security risk assessment of the data center operational controls. In addition, we perform the IT security architecture review that includes specific components such as,

- Trust Zone Architecture.
- User Role Design.
- Authentication and Authorization.
- Data Protection.
- Security Audit Logs and SIEM.
- Data Privacy.

Step 4 – Update Plan. We will perform an annual update to the data centers' initial security plan with the results obtained through steps 1, 2 and 3. We will assess the gaps, and identify and document appropriate mitigation controls in the deliverable D-07.05 Security Management Plan. As part of this step, we will work with the Commonwealth stakeholders, conducting up to two meetings, to categorize gaps into appropriate initiatives, identify current posture and integrate the results with the security roadmap.

See Attachment F-9 for a sample Security Management Plan, entitled, "Commonwealth of Pennsylvania – Office of Information Technology Enterprise Data Center Security Management Plan".

2 Network Security System Architecture, Experience

2.A Implement at minimum: spam filtering, anti-virus, malware protection, firewall (web, application), intrusion prevention and detection, web content filtering, virtual private network, and data loss prevention systems.

2.B Offeror must describe its proposed solution including the following:
Processes and Procedures
Tools / Applications
End User Reports
Standard
Custom
Escalation Procedures

The Commonwealth is protected through the deployment of the following devices at all Internet

ingress points: Web & Application Firewall, Anti-Malware, IPS, Content Filter, VPN Concentrator and DLP, Processes and Procedures to address Acceptable Use, Physical & Logical Access Reviews and the applicable Commonwealth ITBs.

Web and database application firewalls will use the Imperva SecureSphere platform for proactive, real-time alerting and blocking of potential application threats. Data loss prevention (DLP), anti-virus, anti-malware, and spam filtering will be provided by Symantec Endpoint Protection, Data Insight Enterprise, and Network prevent platforms. Traditional network firewall, virtual private network (VPN), and Intrusion Prevention Services (IPS) services will utilize the [redacted] enterprise platform, with separate instances for each service to reduce maintenance downtime and impact.

All firewalls will be implemented using the least privilege policy per agency, blocking all traffic by default. Modification to the policy is accomplished via the change management process and requires agency approval. Unisys initially uses vendor standard security policies/configurations on the anti-virus and DLP platforms and works with the agencies and OA's Security Office to modify these as appropriate to meet Commonwealth security requirements.

Reporting will be provided from the individual tools, in addition to an aggregate view from the enterprise SIEM system. Examples of standard reports include: anti-virus compliance and auditing per system, dropped and suspicious firewall events, overall top enterprise threats from the SIEM, threat trending per month/quarter/etc. Custom reports may also be requested via the Enterprise Services Catalog and will be developed by working with the Commonwealth security staff to identify required information, trending, formatting, etc. from the individual tools as well as the enterprise SIEM.

There are well established and tested escalation processes in place to address incidents. Escalation processes are described in Schedule F, Section 3.2.1.4 "Service Desk". For security incidents, Commonwealth IT Security Incident Reporting Policy will also be followed.

2.C Offeror must describe its prior experience relative to providing datacenter management and support of CJIS, CCHRI, HIPAA and PCI systems.

Unisys currently supports agencies such as the Department of Public Welfare, Liquor Control Board, Department of Revenue, the Department of Health, and the Pennsylvania State Police in the DPH required to adhere to and be audited on the security standards of CJIS, CCHRI, HIPAA, PCI, NIST, FISMA and IRS. As required, Unisys supports Commonwealth agencies in complying with these stated security requirements by ensuring the appropriate complement of network security devices are implemented for each agency.

The Unisys Team has provided data center management in support of other government agencies in support of CJIS, CCHRI, HIPAA, and PCI systems. As an example, Unisys designed a data and records management system for the Alabama Criminal Justice Information Center that meets CJIS and CHRIA requirements. The Alabama Criminal Justice Information Center (ACJIC) is a state agency providing local, state, and federal criminal justice agencies with the information needed to provide citizen safety. ACJIC realized that gaps in its information technology were hindering communications and business continuity. It needed to more efficiently deliver critical information from its network and systems. ACJIC explored several solutions and solution providers before choosing Unisys to help establish an IT infrastructure specifically designed to address the agency's requirements.

3 Security, Quarterly Vulnerability Assessment, Penetration Testing

3.A Perform quarterly (at the Offeror's expense) Vulnerability Analyses (VA) and penetration testing to identify new or emerging information security threats

3.B Perform penetration testing (at the Offeror's expense) and present the results of each VA on a quarterly basis. Should exposures be identified, plan and remediate the exposure in accordance with Commonwealth IT policy guidelines. Report results to the Commonwealth within the time set out in an applicable SLA.

3.C The above requirement will be for all systems/subsystems that the Offeror is responsible for including managed servers/virtual servers, network devices, security devices including , but not limited to, the following:

Performing web application firewall administration and securing web applications behind it.

Ensuring and maintaining PCI level 1 compliance

Implementing DLP for the data center server assets to avoid a breach.

Implementing Database Firewall to secure database assets from breach.

Offeror must describe its capabilities and approach to performing vulnerability analysis and penetrating testing on a quarterly basis. Provide sample reports for each.

Perform Quarterly Vulnerability Analyses and Penetration Testing

Quarterly Vulnerability Assessment and Penetration Testing: The Unisys Team uses our demonstrated methodology and our deep experience in serving multiple agencies of Commonwealth and other public sector clients to perform the baseline security risk and vulnerability assessment. Our methodology has been well-honed to provide PCI level 1 compliance. We use our experience in delivering security risk and vulnerability assessment projects for several public sector clients including the Commonwealth to deliver this assessment. Using state-of-the-art tools that are consistent with leading industry practices such as National Institute of Standards and Technology (NIST) standard, Open Web Application Security Project (OWASP) and System Administration, Audit, Network, Security (SANS) guidelines, we tailor our assessment to meet the Commonwealth timelines and deliverable milestones.

We perform the following steps as part of the quarterly vulnerability assessment and penetration testing of the data center's IT infrastructure:

Steps	Unisys team performs the following activities to identify potential security risks and vulnerabilities within the data center infrastructure
Scope and Plan	Conduct one meeting with the data center stakeholders and the Commonwealth's "Trusted Agent" to • Document project requirements, scope and objectives • Identify Commonwealth's point of Contact ("Trusted Agent"). • Identify and document the time frame for conducting baseline security risk and vulnerability assessment.
Conduct vulnerability assessment	• Identify the Commonwealth's target IT and application infrastructure using passive scanning (from public resources such as Search Engines) • Work with the Commonwealth's stakeholders to understand the architecture, business logic/functionality, external dependencies, user roles and privileges within the target IT infrastructure and application • Identify, using passive scanning techniques, the technology and infrastructure dependencies • Perform active reconnaissance and identify network protocols present on the target infrastructure

	and web applications using network discovery (SolarWinds, Ping and Xprobe2) • Identify well-known open TCP ports and services present on the target infrastructure using leading port scanning tools (Nmap and SuperScan) • Perform infrastructure vulnerability tests using automated vulnerability scanning tools (Tenable Nessus and Rapid 7 Nexpose) on Commonwealth selected IT infrastructure. The tests will include performing vulnerability scans to meet the Payment Card Industry (PCI) Data Security Standard (DSS) vulnerability scanning requirements • Perform database vulnerability testing, using automated database vulnerability scanners (AppDetectivePro) on a total of Commonwealth selected standard database instances of Oracle, Microsoft SQL Server, MySQL and IBM DB2 • Conduct manual assimilation of the vulnerability scan results to identify false positives and manually verify the vulnerabilities identified by the vulnerability scanning tools.
Perform Penetration Testing	• Analyze the vulnerabilities in order to identify the penetration testing steps that can be performed – based on the identified hosts with vulnerabilities • Research, develop and prepare custom penetration test scripts/methods for the in-scope systems/vulnerabilities • Communicate the penetration test activity with the trusted agent and obtain the confirmation before performing the tests on the target environment • Support the Commonwealth to select the IT infrastructure to perform the penetration testing. The selected IT infrastructure for further analysis will help provide a representative view of the data center IT environment (e.g., different server OS levels, HW vendors, and server functions). We will document and discuss the appropriate exploitation steps with the Commonwealth before performing the tests • Perform the controlled penetration testing on Commonwealth selected IT infrastructure to exploit the identified vulnerabilities. We will use Rapid7 Metasploit to perform the penetration tests Note: The Unisys Team performs the vulnerability assessment and penetration testing on Commonwealth selected data center's IT network infrastructure. The vulnerability assessment and penetration testing does not include web application vulnerability testing and social engineering assessment
Perform Security Configuration Risk Review	• Perform security configuration risk review using the IRS 1075 based Safeguard Computer Security Evaluation Matrix (SCSEM) on Commonwealth selected IT infrastructure handling Federal Taxpayer Information (FTI). We will work with the Commonwealth to select the IT infrastructure that includes a representative view of the information technology environment of the data center such as • Web servers • Application servers • Database instances • Standard operating systems (SCO UNIX,Tru64 UNIX, HP-UX, IBM AIX, Linux – Red Hat, SUSE, Microsoft Windows 2000, 2003 and 2008) • Boundary protection devices: perimeter firewalls, Intrusion Prevention System (IPS), routers and switches.
Document Results and develop mitigation plan	• Notify immediately to the Commonwealth's "Trusted Agent" if high risk vulnerabilities are identified during the test window • Detailed description of test scripts used and steps followed to identify or exploit critical and high risk vulnerabilities • Document and submit the results of the quarterly vulnerability analysis and penetration testing as part of Deliverable #D-07.03 (Security Management Plan) • Work with the Commonwealth to prioritize the vulnerabilities identified and develop a mitigation plan.

Quarterly Cyber Threat Intelligence (CTI) diagnostic: To adapt to the growing

sophistication of detecting security threats, the Unisys team augments our quarterly vulnerability assessment with an emerging service – Cyber threat intelligence diagnostic. This service is a key differentiator where we help the Commonwealth stay abreast of advances in persistent security threats, help identify and reduce risks from emerging information security threats within the Commonwealth's data center infrastructure. As part of this service, we will perform the following activities

- ***Activity 1 – Intranet cyber compromise analysis:*** Through this activity, the Unisys team will identify potential Commonwealth data center servers that may be compromised and are attempting to communicate with known adversary controlled devices on the Internet. We perform this activity by analyzing Commonwealth's security audit logs from domain name server (DNS) logs, firewall logs and remote access logs of devices supporting critical data center servers. We will work with the Commonwealth's "Trusted Agent" prior to the start of the analysis to select the audit log time frame and document the scope of the analysis.
- ***Activity 2 – Rogue device discovery diagnostic****:* The Unisys Team will analyze the behavior of data center devices (IT infrastructure) to determine if the devices exhibit rogue or stealth-like characteristics. We will analyze the Network Dynamic Host Configuration Protocol (DHCP) and Address Resolution Protocol (ARP)/Content Addressable Memory (CAM) data from the data center's core network switches supporting critical data center servers. We will work with the Commonwealth's "Trusted Agent" prior to the start of the analysis to select the audit log time frame and document the scope of the analysis.

At the end of the quarterly diagnostic, we will work with the Commonwealth to prioritize the vulnerabilities identified and develop a mitigation plan.

Monthly CTI program diagnostic report: In addition to performing a quarterly CTI diagnostic, the Unisys team augments our approach with a monthly program diagnostic. Through this diagnostic, the Unisys team will analyze the data center servers to identify presence of potentially unwanted programs, malicious files, and unknown binaries. We will work with the Commonwealth's "Trusted Agent" prior to the start of the analysis to select the audit log time frame and document the scope of the analysis. At the end of this diagnostic, we will work with the Commonwealth to prioritize the vulnerabilities identified and develop a mitigation plan.

Unisys team's collaborative approach to work with the Commonwealth to perform this assessment

We work with the Commonwealth to identify a "Trusted Agent" to help facilitate the security risk and vulnerability assessment. The Trusted Agent is responsible to:

- Define scope, identify and prioritize the IT assets for the assessment
- Make decisions to proceed with applicable testing
- Coordinate the testing activity with stakeholders like IT infrastructure, application and data center service providers
- Coordinate with other commonwealth agencies (if applicable) during the testing activities
- Review the vulnerability reports and owns limited "as needed" distribution of the reports. The sensitive nature of information contained in the reports requires a specific

stakeholder being responsible for managing the communication aspects

- Identify mission critical systems of the Commonwealth, business partners or affiliates, and third parties, as applicable
- Identify the time period for communication to the appropriate stakeholders for high severity security vulnerabilities identified in production environment
- Coordinate and authorize the vulnerability assessment team access to the Commonwealth data center's information technology components considered for vulnerability assessment. In order to avoid interruptions, we recommend running many of the assessment tasks during non-business hours. At the Trusted Agent's direction, we execute as many of these tasks as practical during non-business hours
- Select the servers for the baseline security risk and vulnerability assessment based on business and security criticality
- Identify and provide the appropriate audit logs and data for performing the quarterly and monthly CTI diagnostic assessments.

We will facilitate with the Commonwealth and the data center stakeholders a backup of data and servers for the environments in addition to performing recovery procedures of systems, servers and applications in scope for this assessment.

In addition, we use leading industry vulnerability scanning tools that supports PCI scanning – Tenable Nessus and Rapid 7 Nexpose in addition to using Rapid 7 Metasploit to perform penetration test. We use AppDetectivePro to perform database security vulnerability assessment in addition to performing a security configuration review using leading industry standards such as IRS defined SCSEMs.

Our approach includes defining a mitigation plan and performing the appropriate mitigation steps/establish mitigation controls for the vulnerabilities identified.

The Unisys Team will use the Imperva SecureSphere platform as Web and database application firewalls for proactive, real-time alerting and blocking of potential application threats. Our approach for implementing DLP and Database Firewall to avoid breaches is detailed in Schedule F, Section 2.3.4 "Data Protection". Sample quarterly Vulnerability Analyses (VA) and penetration testing report, entitled, "Sample Security Assessment Report" is provided in Appendix F-10.

4 Security Attack and Threat Assessment

4.A Review network and other security logs for evidence of attack. Utilize enterprise grade intrusion detection tool(s) to systematically identify, stop, and report security threats. Produce a monthly Security Log Analysis as part of the monthly status reports as described in RFP section IV-5 Reports and Project Control.Offeror must describe its solution and approach

Review Network and Other Security Logs

Unisys will implement a security information and event management (SIEM) system that allows for proactive analysis of security logs from all security, network and system platforms. The SIEM collects, aggregates, analyzes, and correlates system logs to identify suspected security

incidents and confirms that the full path of attack is identified. The Unisys SIEM reviews logs from all sources and identifies immediate threats as well as perform historical analysis on previous events for trending and lower severity or persistent attacks. Suspected risks and threats immediately go through the incident management process for remediation, and follow up reporting are provided in standard formatting, with custom reporting also available.

The [redacted] intrusion prevention system (IPS) sends its logs to the SIEM for real time analysis and correlation with other device logs to determine possible malicious activity. This is accomplished with a signature based system capable of protocol and traffic anomaly detection, zero day protection, and application awareness. Suspected intrusions are blocked based upon the vendor recommended security rating and continually tuned for more accurate detection and less false positives.

The Commonwealth will receive a monthly security report detailing all security incidents, which will be provided to appropriate agency and OA security administration. See item 3 above for additional details on reports.

5 Patch Management

5.A Apply operating system and other security patches. Implement a Patch Management Program to ensure the timely application of security updates on all infrastructure platforms in accordance with Commonwealth IT policy guidelines. The Patch Management Program must adhere to the Change Management process that includes Commonwealth approvals. Offeror must describe its proposed Patch Management program.

Apply Operating System and Other Security Patches

Unisys will implement a complete Patch Management Process for the Commonwealth in accordance with OA ITBs, ITIL Change Management Process and vendor best practice recommendations. The Unisys technical support team will work with the Commonwealth Agencies to determine patch policies that should be applied to Configuration Items (CIs) supporting applications including OS, network, databases and middleware (CIs). The Patch Management Process will address policies, processes, procedures for the following:

- Sources of patches (how to obtain them from the OEMs)
- Toolsets that are employed to stage patches for possible deployment
- Change management procedures supporting the Change Management Process to identify, approve and manage deployment of patches
- Compliance procedures to include utilization of the toolsets to run compliance audits and identify out of compliance CI's with patch policies and approved changes
- Process and procedures to bring out of compliance CI's back into compliance

Unisys will follow the Change Management Process for applying patches to all IT infrastructure CI's with the Commonwealth's approval. This process will maintain the change record in the Unisys ITSM platform and also update the CMDB configuration management file after completion of the patch release and deployment process. The Unisys ITSM change record will be related to the CI's in the CMDB as an audit trail for patch changes upon the completion of the Release and Deployment Process.

The distributed IT infrastructure toolset to support the automation of patch release and deployment is [redacted] for Server and Network Administration. Unisys will maintain in this toolset the appropriate patch policies for determining patch deployment and compliance. The [redacted] Suite will be maintained with the current patches supplied by the OEM's and will be used to manage the distributed IT CI's.

Unisys approach to testing and validating updates to the all CI's is to follow the Release and Deployment Process for all changes into all production environments. The Release Process includes:

- Change ticket approvals
- Test planning and accepted test results
- Release and deployment planning including release back out plans
- Release testing for risky deployments
- Early life cycle support to help provide a successful deployment
- Release blackout for failed releases

6 Network Physical Access Restrictions

6.A Restrict physical access to all network systems and equipment with biometric or other second factor access control systems. Offeror must describe solution and approach to meet this requirement

Unisys takes a layered approach to security. Each facility has both physical and logical security in place. Managing access to systems starts with physically securing all network systems and equipment to prevent unauthorized personnel from gaining access. Perimeter security is maintained by camera and an active physical security presence. All facilities include guard-controlled access to interior spaces. Access control systems include access to and within the facilities in all data centers. Access control is achieved through a combination of identity management tools, namely keycard, keypad and biometric devices. Unisys will install badge reader systems and biometric or similar second-factor access control systems in a double-entry configuration. Additional rack-based key or biometric controls will be implemented as required. In this way, two factor access control is used to restrict physical network access. In addition, access control systems including keypad and biometric authentication capabilities are available for added security.

Unisys Security Operations Center (SOC) is comprised of security support staff and a suite of automated tools that provide comprehensive 24x7x365 monitoring, alerting, and response to security events.

7. Network Data Access Restrictions

7.A Restrict access to all data in the Commonwealth network infrastructure. Restrict and control all data access right, groups and special permissions based on the data security program designed by the Commonwealth security team and/or specified by the agencies. Access level changes and exceptions will be executed only when approved paperwork is complete and approved. A file of all access changes will be maintained by the Offeror for audit purposes. Offeror must support Commonwealth initiated security audits. Offeror must describe solution and approach to meet this requirement

Unisys will implement a "need to know" and "least privilege" policy in accordance with Commonwealth logical and data access policies. System administrators will set up user accounts with appropriate levels of data access to restrict and control the access rights of system users based on their role and group designations as specified by the Commonwealth or specific Commonwealth agencies. Changes and exceptions will only be made by Unisys upon the receipt of approved documentation from the Commonwealth or Commonwealth agency management. Unisys will perform monthly reviews of logical access changes and will support and fully participate in all Commonwealth initiated security audits. Unisys will maintain a log of all access changes for audit and review at the Commonwealth's request.

8 PMO, Subcontractor Security, Security Audits

8.A Evaluate the security standing of network-connected subcontractors. Conduct information security audits of prominent subcontractors on an annual basis. Offeror must describe solution and approach to meet this requirement.

The Commonwealth benefits from Unisys compliance with the ISO27001 standard where auditing of all third parties on an annual basis is a requirement. The number of network connected subcontractors will be very limited and third-party personnel will be required to pass a security background check based on the FBI CJIS policy or applicable security standard based on the specific system or data access. All subcontractors will be listed in the administrative database that tracks on-board and off-board activities for project resources. Monthly access checks will be matched against a list of subcontractors with local or remote access and login passwords will be required to be changed every 90 days. Unisys tracks any deviations from this standard in its Corrective Action Plan (CAP) registry that will be reviewed by a Security Working Group every 30 days. Subcontractors who attempt to circumvent these controls will have their access removed indefinitely.

Continual Service Improvement

Unisys recognizes the significant importance of Quality and Continuous Service Improvement to:

- Reduce service risk,
- Improve service quality,
- Improve client satisfaction,
- Provide service transparency, and
- Improve/reduce costs of service.

Through a continuous cycle of evaluation and improvement within an IT infrastructure, Unisys views quality and continuous service improvement as a critical success factor in driving customer satisfaction for the Commonwealth IT infrastructure. Each of the continuous service improvement areas identified above are driven through the tight integration of the following organizations, industry tools, proven processes and quality deliverables:

- Service Excellence Office,
- Quality Plans: transition and steady state service delivery

- Industry standard frameworks and methodologies: ITIL, ISO, SSL
- Industry accepted measurement tools
- Continuous Service Improvement & Innovation Processes (CSIIP)
- Risk management, audits and business continuity management
- Client Satisfaction Surveys and Knowledge Management Portal

Collectively this represents Unisys Integrated Quality Plan for the Commonwealth of Pennsylvania.

Specifics on each of these areas are outlined in Schedule F, Section 3.2.1.1.6 Continuous Service Improvement. Highlights from this section are outlined below and requested service examples are provided at the end of this section.

9 CI Service Risk

9.A Relative to the service in question, Offeror must provide examples of previous Offeror initiatives aimed at eliminating or mitigating service risks.

Risk management, independent quality audits, and business continuity management are integral quality management processes. Unisys is committed to managing risks and facilitating the achievement of business objectives the adherence to quality processes. We mitigate risk through the implementation of tight quality controls: standard policies, procedures, roles, risk assumptions, issues, and definitions, etc.

In order to proactively identify possible network security risks, the Data PowerHouse implemented intrusion detection services in 2010 for all COPANET/MAN connections. This technology, coupled with the [redacted] MARS logging analysis platform, allows Unisys to identify and correlate IDS, firewall, and network switch/router logs for additional protection against the growing number of network based security threats. Suspected events are investigated and reported to the OA's Security Office, which allows the Commonwealth to gain even greater insight into potential risks of their hosted systems and eliminate or mitigate those service risks.

Unisys currently performs physical (with DGS) and logical access reviews in conjunction with agencies and OA.

10 CI Service Quality

10.A Offeror must provide examples of previous Offeror initiatives aimed at improving service quality

The quality approach begins with the Service Excellence Office who provides definition and oversight of all ITIL process management and analysis functions. Process managers and analysts working in the Service Excellence Office are responsible for auditing process effectiveness, ensuring that service delivery teams comply with proper execution of processes, and analyzing process trends for anomalies. Continuous service improvement programs in collaboration with Commonwealth agencies are managed by the Service Excellence Office.

Through our Continuous Service Improvement and Innovation Process (CSIIP), the SEO reviews, analyzes and makes recommendations on improvement opportunities in each ITIL

lifecycle phase. Unisys will leverage Six Sigma Lean tools and methodologies as well as ISO Certified internal audits to measure and maintain the highest quality services to the Commonwealth.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

11 CI Client Satisfaction

11.A Offeror must provide examples of previous Offeror initiatives aimed at improving service quality

Client satisfaction is extremely important to Unisys and a key focus in our IT solution. The SEO will integrate new agencies, customers and services into our multi-pronged client satisfaction approach that includes Service Desk surveys on the caller's experience, an overall agency satisfaction survey, and quarterly surveys with the Office of Administration. Data collection will be gathered across multiple levels to gain a clear understanding of the Commonwealth's satisfaction with the IT Services being provided.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

In late 2009 Unisys began offering vulnerability scanning for nearly all agencies in the Data PowerHouse in order to expose potential security vulnerabilities and confirm that Commonwealth mission critical systems are patched accordingly. This incremental service provides scheduled reports on a quarterly basis that the DPH service delivery staff review with the agency to confirm they are able to continuously improve their security posture and reduce overall risk.

Unisys created a baseline security policy and quarterly access review with IES to improve logical access reviews.

12 CI Service Transparency

12.A Offeror must provide examples of previous Offeror initiatives aimed at providing service transparency; in particular, visibility into the service execution process.

The service organizations will use standardized ITSM services processes, IT monitoring and automation tools. ITSM processes will be documented in the Commonwealth Computing Procedures Manual (CCPM). The CCPM will be available to Commonwealth approved staff on the Knowledge Management Portal (KMP) providing desired transparency into service execution processes. Through the Real-time Dashboard, the Commonwealth will have access to current operational performance of their application infrastructure.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

The Unisys Data PowerHouse began offering self-service firewall log review to selected agencies that requested this feature in 2012. This allows hosted agencies such as IES and the PA State Police to review the firewall logs that pertain to their managed systems for dropped or accepted packets, reducing their troubleshooting times and expediting the overall firewall

change process for them. Agencies with self service capability have praised Unisys for this ability to get a glimpse into their operational network security policy, ensuring that when they are troubleshooting application issues, or deploying new services, they are able to identify and/or anticipate what changes will need to be implemented on the DPH firewalls.

Unisys will produce quarterly vulnerability reports and submit them directly to agency personnel for review and discussion.

13 CI Service Sustainability

13.A Offeror must provide examples of previous Offeror initiatives aimed at ensuring service sustainability; in particular, efforts targeted at cost containment and cost reductions.

Service will be sustained by integrating any new agencies, customers, or services into our standard operational and quality processes and methodologies. We leverage ITIL processes, create quality project plans, utilize industry accepted measurement and monitoring tools, analyze trending reports and provide proactive continuous service improvement throughout the IT lifecycle. This enables new Commonwealth services to experience and sustain IT services and client satisfaction.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

14 CI Improve or Reduce Cost

14.A Offeror will provide examples of Security Management initiatives that have been implemented or can be utilized to achieve reduced costs of Services and to meet or exceeded ROI (Return on Investment) analysis projections.

The Service Excellence Office will proactively manage quality, continuous service improvement, ITIL process management, and customer satisfaction through a comprehensive quality plan that specifically addresses all of these areas. We believe this is a key differentiator in our partnership with the Commonwealth. Through this new organization and these quality plans, Unisys will drive best in class services and the highest customer satisfaction experience, while reducing overall costs to the Commonwealth.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

As a part of the 2008 contract extension to the Data PowerHouse, Unisys began a firewall consolidation initiative tied to the increasing use of shared infrastructure components and firewall virtualization. Prior to this, agencies in the DPH used separate physical Check Point firewalls. These were consolidated onto a shared [redacted] firewall service module (FWSM) platform, with each agency retaining a logical firewall partition with distinct security policy and configurations. This allowed for a significantly less complex hardware environment and reduced maintenance and licensing costs.

Unisys requested and was granted quarterly meetings with the Commonwealth Security Manager to discuss audit, compliance and IT risk issues. Through these meetings, Unisys has been able to gain better insight into ITB updates, statewide security initiatives and emerging threats, and, as a result, avoided the need to enter the RFS process for security improvements.

Unisys has also taken advantage of state contract licensing for anti-malware software providing the Commonwealth with lower license costs.

Unisys Team Experience

City of Minneapolis IT Support

In January 2003, the City of Minneapolis awarded Unisys Corporation a 7-year IT outsourcing contract to manage the City's complete IT infrastructure, from the data center to desktops and mobile devices. Under the contract, Unisys supports multiple city agencies, including the Mayor's Office, City Council, Police and Fire Departments, and the Office of Public Works.

The scope of services includes providing:

- Data center administration and management;
- Network and systems monitoring and management;
- Desktop support services, including desktops, laptops, peripherals; iPads
- Service Desk services;
- Security Analytics and vulnerability services
- Disaster Recovery services; and
- Technology refresh of laptops, desktops, servers,

Technologies supported include, Windows, UNIX, Unisys, EMC, Oracle, and the Windows Office Suite. Unisys took ownership of the City's existing servers, storage, PCs and printers. The servers and storage were moved to the Unisys IT Outsourcing Service Centers in [redacted] Minnesota and Roseville, Minnesota. This hardened data center facility provides 24x7x365 availability and application support in a secure, high performance, highly-scalable environment. This transition was accomplished in a record 10 months instead of the projected 18-24 months.

Today, Unisys manages and supports over 200 servers and 3,000 desktops for the City. Included among the systems being hosted are the servers supporting the City's Web development and client-facing production Web services servers. Unisys provides full managed hosting services for these servers.

Federal Security Operations Center Support

Unisys has provided decades of mission-critical enterprise security experience with large-scale deployments including Federal agencies. For example, Unisys collaborated with the USDA Agriculture Security Operations Center, 14 product vendors, and 7 technology vendors to implement a forward-thinking security solution to enhance proactive identification and defensive response to cyber security threats at strategic USDA locations throughout the United States.

The implementation of the USDA Security Sensor Array (SSA) was achieved by integrating and incorporating a comprehensive, consolidated, top-down security toolset of seven COTS products and several technologies—the first solution of its kind to be deployed throughout a cabinet-level department in the Federal Government. Within SSA site implementations, seven strategic security technologies were integrated to provide real-time security awareness and understanding of existing and future threats against the USDA assets.

Each SSA includes Security Information and Event Management (SIEM), Intrusion Detection/Prevention System (IDPS), Malware Detection/Prevention System (MDPS), Network Behavior Analysis (NBA), Secure Socket Layer (SSL) Decryption, Packet Analysis, and Data Loss Prevention (DLP). In addition to enterprise visibility and control, the solution provides local visibility and the capability to resolve Inspector General, OMB, and other security audit findings. SSA delivers the needed protections for USDA. This solution protects 250,000 network nodes at 5,000 locations throughout the United States.

Benefits to the Commonwealth

The Unisys Team, through its extensive security operations expertise, will provide the Commonwealth with:

- Low risk data center transition to a secure environment
- Proven security analytics, vulnerability assessments, and mitigation strategies.
- Advanced cyber situational awareness and intelligence analysis capability
- Leveraged security strategic planning and design, integrating current tools and organizational structures.
- Operational efficiencies from streamlined incident management
- Accelerated system development, integration, and deployment, with decreased implementation and operational risks.
- Assurance of a secure operational cyber environment through an integrated approach to risk management.

3.2.2.6 Performance Monitoring & Management

The Performance Monitoring & Management Service of the infrastructure components, databases, and applications provide the critical input for meeting service level commitments. Performance monitoring is a proactive method to identify and respond to system database, processor utilization, or environmental problems that may affect the Services, or might negatively affect Services in the near future. The selected performance monitoring tools will also provide one of the key inputs for calculating SLAs, and the associated monthly evaluation and reporting needs.

The Offeror must collect performance information and report on infrastructure and application

performance status on a daily basis using performance management and monitoring tools.

All tracked performance information must be reported daily, including processing performance, network (LAN / WAN) performance, and storage performance data. The Offeror must determine trends in conjunction with the Commonwealth, and all trends will be reported to address, if necessary, any changes from an established baseline. Forecasts of future usage will be determined based on expected growth in application transaction volume and expected deployment of future applications.

The Offeror must provide a base level of performance monitoring for key infrastructure components such as server, storage, network, and security. Additional Performance Monitoring Services such as database and application monitoring will be offered to the Commonwealth as an additional level of service.

Agency applications may require additional application level monitoring provided and managed by the Commonwealth Agencies. The Offeror must allow additional Commonwealth based monitors to be installed and managed by individual Commonwealth Agencies.

Reference Documentation

Schedule J.3 - Datacenter SLA Definitions

	Requirements	Describe Compliance
1.	Identify the performance monitor software tool(s) that will be used to monitor selected infrastructure Services. The selected infrastructure service will be presented to the Commonwealth for approval.	Offeror must describe its proposed performance management toolset.
2.	Create and maintain performance monitoring procedures for each platform to ensure each system is monitored in a consistent manner. All identified systems will be monitored under the parameters established in the CCPM.	Offeror must describe its approach to monitoring performance across multiple platforms and environments including the following: • Process and Procedures • Tools / Applications • End User Reports o Standard o Custom • Escalation Procedures

3.	Performance information reporting - Collect and report on the performance data on a monthly basis. Offeror must utilize these reports to ensure SLA's are being achieved. A monthly report will be created to provide a review of how well the systems are performing. Also, provide daily reporting. Recommend system changes to correct over and under system utilization, as well as system upgrades as appropriate. These reports and recommendations will be shared with the Commonwealth. Daily performance reports summarizing incidents for the past 24-hours and immediate reports of incidents and routine status reports of incidents in progress for resolution such as a network or server outage that impacts Commonwealth Services. Examples of automated notifications include, but are not limited to, drive full (Warning, critical), unscheduled reboots, server instability, etc. and to be defined in the CCPM. Offeror must have to ability to provide performance information on a daily, weekly, and monthly basis.	Offeror must provide sample performance monitoring reports and approach to supporting daily, weekly and monthly reporting. Offeror must describe its approach to provide Commonwealth the ability to utilize Offeror's monitors (tools) as well as adding its own.
4.	Support the load testing of applications by providing additional targeted performance monitoring Services during the testing period. This service will be made available as an additional service. Provide load-testing performance monitoring as an add-on service.	Offeror must describe its monitoring capabilities and tools to support load-testing performance.

5.	Performance Monitoring training - Provide the Commonwealth with training on the use of performance management tools and reporting.	Offeror must describe its training approach to provide this training to Commonwealth users.
6.	Support for agency level monitors - agency applications may require additional application level monitoring to be provided and managed by the Commonwealth agencies. Support synthetic transactions in applications to create a “dashboard” view that applications are working properly. The Offeror must allow additional agency based monitors to be installed and managed by individual Commonwealth Agencies.	Offeror must describe its approach to meet these requirements.
Continual Service Improvement		
7.	Reduce service risks.	Relative to the service in question, Offeror must provide examples of previous Offeror initiatives aimed at eliminating or mitigating service risks.
8.	Improve service quality.	Offeror must provide examples of previous Offeror initiatives aimed at improving service quality.
9.	Improve client satisfaction.	Offeror must provide examples of previous Offeror initiatives aimed at continually improving client satisfaction.
10.	Provide service transparency.	Offeror must provide examples of previous Offeror initiatives aimed at providing service transparency; in particular, visibility into the service execution process.

11.	Ensure service sustainability.	Offeror must provide examples of previous Offeror initiatives aimed at ensuring service sustainability; in particular, efforts targeted at cost containment and cost reductions.
12.	Improve/reduce cost of service.	Offeror must provide examples of Performance Monitoring and Management initiatives that have been implemented or can be utilized to achieve reduced costs of Services and to meet or exceeded ROI (Return on Investment) analysis projections.

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

Introduction

Unisys will provide a comprehensive Performance Monitoring and Management Service to support the Commonwealth/agency services, applications and supporting infrastructure components. Unisys will provide a base level of performance monitoring and management for the following infrastructure Configuration Item's in support of availability and performance SLA's defined in Schedule I, represented by the Enterprise Services Catalog:

- Servers (Mainframes and distributed servers)
- Network (LAN and security devices (e.g., firewalls)
- Storage

In addition to the base level of performance monitoring for the Unisys Team managed infrastructure, the following additional services will be optionally provided to the Commonwealth/Agencies and are available to be order via the Enterprise Services Catalog:

- AppDynamics Infrastructure Performance Monitoring
- Application infrastructure capacity planning
- Commonwealth databases management

The Unisys Team will utilize the proposed Unisys ITSM Centralized Event and Performance Management Toolset to receive and manage performance events from the various IT event management performance monitors for the infrastructure CI's.

A comprehensive set of processes and procedures will be established to support service design processes including performance management and service level management (SLAs) specifically. During service design, SLAs will be tested for achievability before releasing a new

or modified service into the production environment.

Service Operations processes identify performance issues through monitoring performance events and the creation of incidents following the Incident and Problem Management Processes. Well-defined escalation procedures will be implemented to help provide performance incident resolution according to their SLA requirements.

Unisys will provide standard daily performance reports and monthly performance trend reports for base level performance management. The Commonwealth can request custom reports via the Enterprise Services Catalog.

1 Monitor Performance Toolset

1.A Identify the performance monitor software tool(s) that will be used to monitor selected infrastructure Services

Unisys will utilize the [redacted] platform depicted in **Figure 3.2.2.6-1** to monitor and manage performance across services, applications, databases, security, environmental and infrastructure supporting Commonwealth Agency applications.

Unisys will utilize [redacted] to proactively manage and optimize infrastructure performance by avoiding costly outages, solving issues before service levels are impacted, accelerating mean-time-to-repair (MTTR), and extending mean-time-between-failure (MTBF). This reduces customer impact through predictive analytics and drives preventative automation across a single platform.

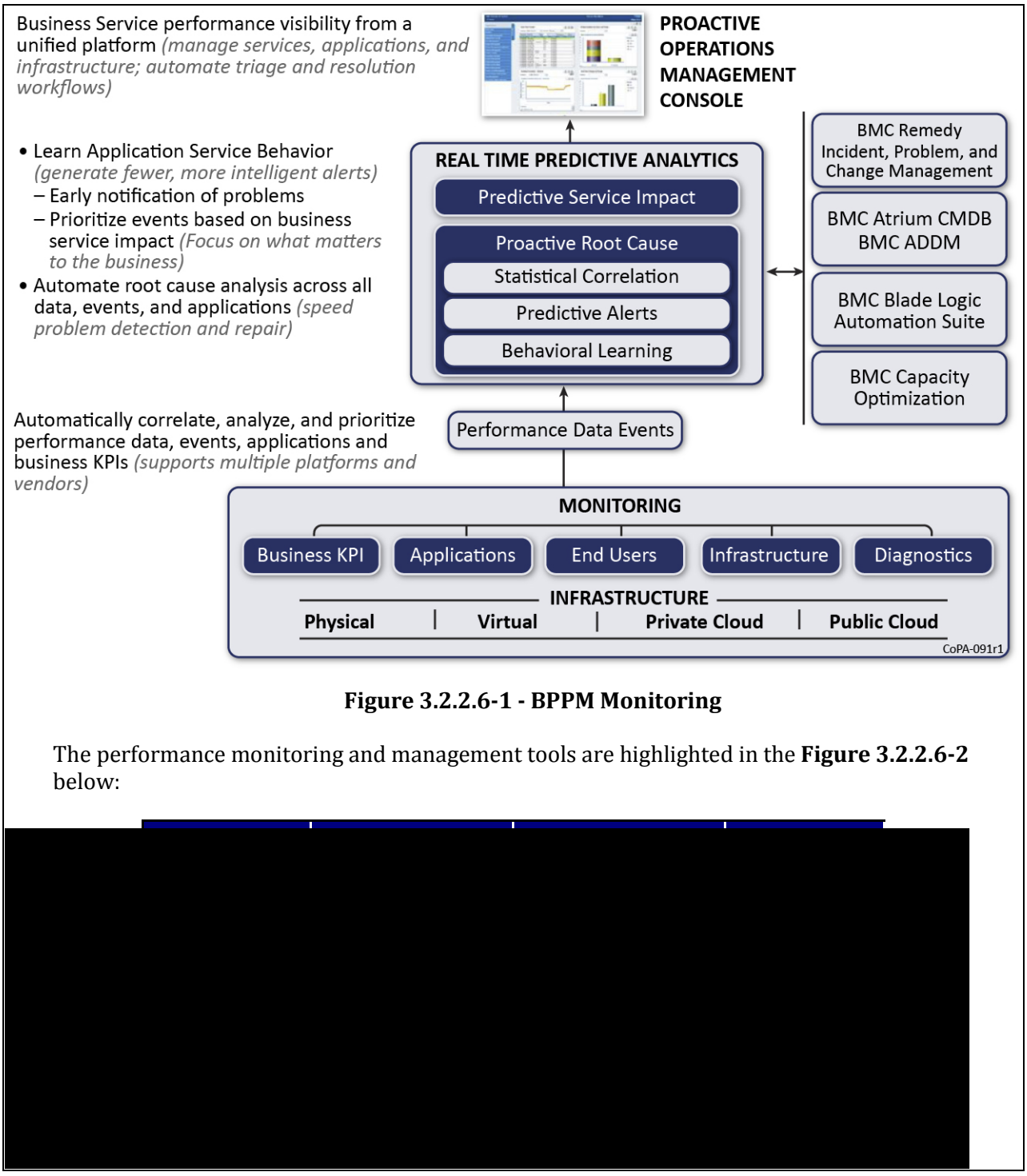


Figure 3.2.2.6-1 - BPPM Monitoring

The performance monitoring and management tools are highlighted in the **Figure 3.2.2.6-2** below:

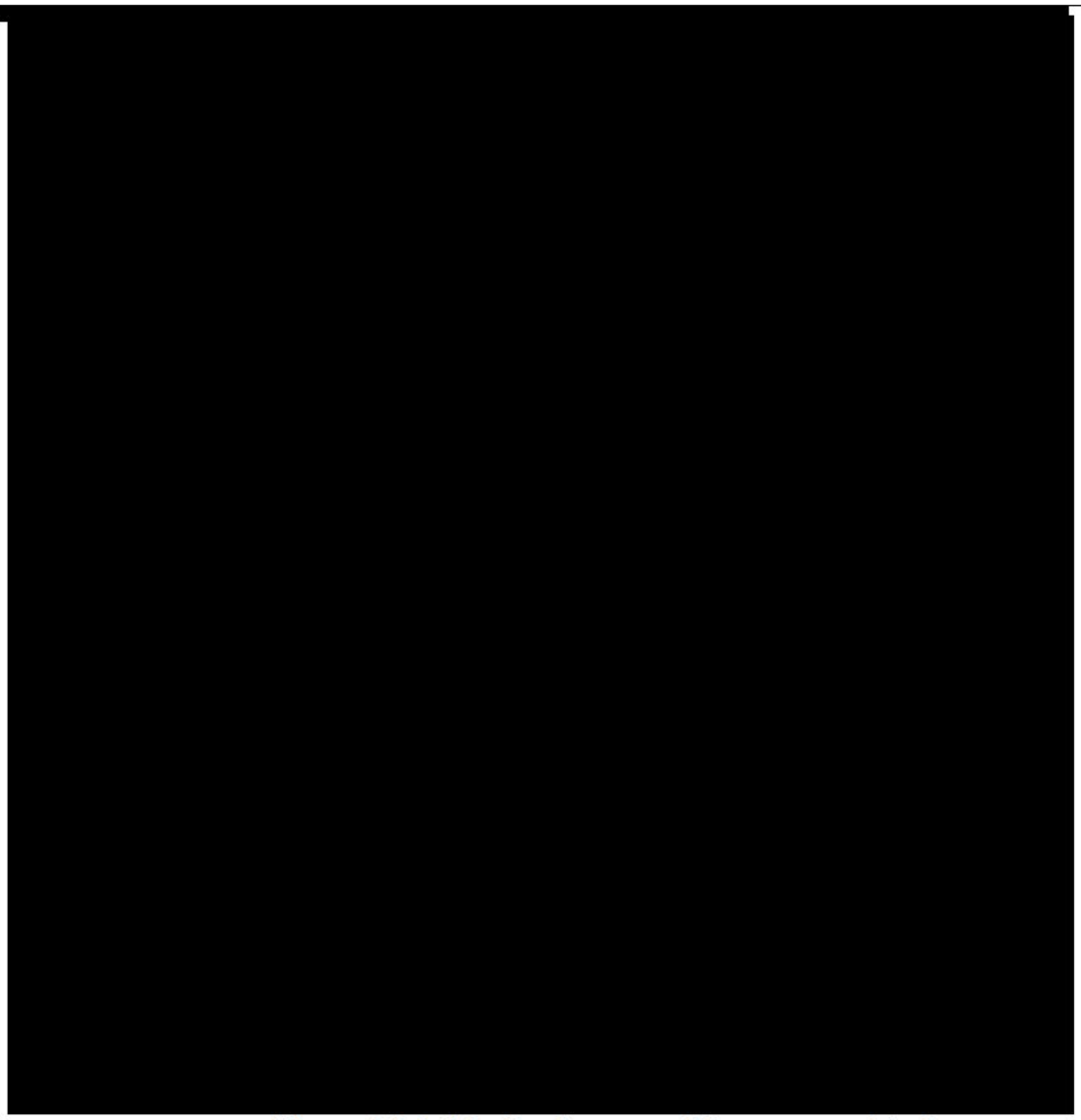


Figure 3.2.2.6-2 - Performance Management Tools

[redacted] automatically discovers and learns the behavioral and performance trends for each of the monitored infrastructure components; identifying normal and abnormal behavior. Unlike threshold-based monitoring systems, the [redacted] analytics engine only generates events when there is significantly abnormal behavior. Based on these learned trends, the Commonwealth realizes significant reductions in the number of false events generated by reactive, threshold-based performance monitoring approaches with fewer, more intelligent events. Unisys supports the Commonwealth by pinpointing and prioritizing the most critical business performance issues.

[redacted] applies real-time, predictive root cause analytics and continuously sifts through events and abnormalities collected from the infrastructure components that support the Commonwealth applications and business services, identifying a prioritized set of the most likely problem causes. The solution applies predictive correlation and filtering techniques that leverage real-time service relationships in the [redacted]

and configuration changes collected from [redacted] (or any other change sources), along with additional detailed diagnostic data. This information provides continuous visibility into problems as they develop; allowing Unisys support personnel to diagnose intermittent performance issues on-demand without requiring the effort to reproduce a problem. As a result, Unisys personnel can remediate problems quickly and efficiently.

For virtualized and cloud services, [redacted] provides monitoring and analysis of virtual and cloud components and their mapping to physical resources. It learns and keeps continuous track of the behavior of physical, virtual, and cloud components and their relationships with one another, and recognizes unique features of these environments, such as clustering and motion. This provides complete visibility, eliminates gaps in root cause, detects potential capacity issues, and eliminates pointless events that can be generated when dynamic changes occur that have no impact on actual performance or availability. As a result, the Unisys and Commonwealth agency application support teams can virtualize and cloud-enable more production applications with this reliable performance monitoring toolset

1.B The selected infrastructure service will be presented to the Commonwealth for approval

The performance monitoring toolsets for the infrastructure service will be reviewed with the Commonwealth for approval.

1.C Offeror must describe its proposed performance management toolset.

Please refer to the performance management toolsets described in 1.A above.

2 Monitor Performance across multiple platforms

2.A Create and maintain performance monitoring procedures for each platform to ensure each system is monitored in a consistent manner. All identified systems will be monitored under the parameters established in the CCPM.

The Unisys Team will create and maintain performance monitoring process and procedures for each platform to help confirm each system is monitored in a consistent manner.

The Unisys Team will review with the Commonwealth stakeholders the performance monitoring thresholds for each platform and the detailed procedures for handling performance events during transition for Commonwealth agency review and approval. The agreed upon procedures for each platform will be made available in the CCPM. The CCPM will accessible to authorized Unisys and Commonwealth users through the Unisys Portal and knowledge management capability.

2.B Offeror must describe its approach to monitoring performance across multiple platforms and environments including the following:

Process and Procedures

Unisys will provide the Commonwealth with a complete Performance Management Process and industry leading technology to manage the performance of infrastructure that the Unisys Team is responsible for in the support of the Commonwealth's services and applications. Performance Management includes consideration of data communications, networking, processing, storage, and other environmental variables. Unisys will provide periodic reports showing performance trends. The Unisys Team and the agencies will utilize these performance trend reports to make recommendations for change.

The Performance Management Process is to help confirm that service performance achievements meet or exceed all of their agreed performance SLA's.

The Unisys Performance Management Process is shown in **Figure 3.2.2.6-3** below:

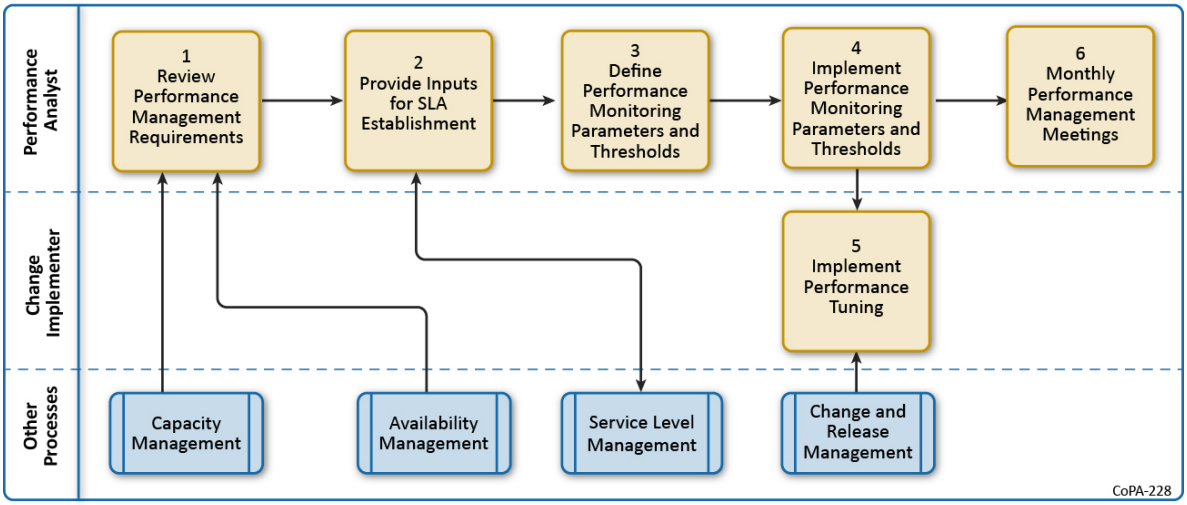


Figure 3.2.2.6-3 - Performance Management Process

Unisys will meet with agency representatives on a monthly basis to review performance requirements and trends for processors, storage, and network (LAN) Configuration Items (CIs).

Tasks required to meet the needs of Commonwealth Agencies daily, weekly and monthly performance management include:

1. Review Performance Management Requirements

Review of the following current and future performance management impacts:

- Review Capacity Plan
- Review Availability Plan and SLA's
- Review current RFC's with performance management impacts

2. Provide inputs for SLA establishment

- Provide data to the Unisys and Commonwealth PMO regarding performance management requirements affecting availability SLA attainment
- Adjust performance management requirements based on results from SLA adjustments

3. Define Performance Monitoring Parameters and Thresholds

The monitoring parameters and thresholds will be identified, which will help in proactively supporting availability and performance SLA requirements. This is also help in proactively managing the capacity of the resources and avoiding over-utilization of resources. Over-utilization of resources impacts the performance of the resources and can lead to the unavailability.

Appropriate monitoring parameters are identified based on the following:

- Resource type, purpose and its capabilities
- Projected workload
- Expected service targets

Appropriate threshold limits are defined based on the following:

- Capacity of the resource
- Current peak and off-peak usages
- Timeline to resolve the threshold breaches
- Available solutions to fix breaches
- Expected service targets

In addition, the frequency in which these parameters need to be monitored has to be determined. Frequency refers to the time interval in which the parameters need to be monitored. These intervals must have enough granularities to capture transient peaks, e.g., backups impacting network traffic, batch processes impact online performance, etc.

4. Implement Performance Thresholds and Monitoring

The Unisys Team will implement the Performance Management Thresholds and Monitor using the Performance and Event Management Platform described in Section 1.A above. The Unisys Team will monitor performance and make recommendations for tuning infrastructure CI's.

5. Implement Performance Tuning

A Unisys Team managed CI needs to be tuned for optimal usage during the implementation, transition of a new or changed service to handle the predicted workload

When a service breach occurs due to poor performance, the tuning options will be defined according to the standard solutions available with the respective product documentation, Problem Management knowledgebase, and technical reference books/articles or newly developed solutions to fine-tune the performance.

6. Monthly Performance Management Meetings

Monthly Performance Management Meetings are held with the Commonwealth/Agencies to:

- Review Requests for Change (RFC's) impacting service performance and capacity

- Review incidents and problems impacting service performance
- Review change requests to improve or tune service performance on managed infrastructure
- Review performance trends of the existing significant service components (CI's) for network (LAN), Server, and Storage.

Tools and Applications

Please refer to requirement 1.A above.

End User Reports (Standard and Custom)

Please refer to Schedule F, Section 3.2.2 "Technical Services" for standard reports.

Custom reports are available via the Enterprise Services Catalog.

Escalation Procedures

Please refer to Schedule F, Section 3.2.3.2 "Site Operations" for detailed Escalation Procedures.

3 Monitor Performance, Reporting

3.A Performance information reporting - Collect and report on the performance data on a monthly basis. Offeror must utilize these reports to ensure SLA's are being achieved. A monthly report will be created to provide a review of how well the systems are performing

Unisys will collect and report on the performance data for infrastructure supporting Commonwealth applications on a daily, weekly and monthly basis. The specifics will be agreed to during transition. These performance reports will be leveraged in support of SLA achievement.

Unisys will review performance reports, SLA reports and the cycle for making these reports available in the Services Portal during transition. Unisys will obtain the Commonwealth's approval for the reports and reporting cycle.

Please refer to Schedule F, Section 3.2.2 "Technical Services", for standard performance, availability and SLA reports.

3.B Also, provide daily reporting. Recommend system changes to correct over and under system utilization, as well as system upgrades as appropriate. These reports and recommendations will be shared with the Commonwealth.

The daily reports will be shared with the Commonwealth via the Services Portal. The Unisys capacity manager and performance analysts provide recommendations for system changes to correct over and under system utilization including upgrades based on the performance

reports.

3.C Daily performance reports summarizing incidents for the past 24-hours and immediate reports of incidents and routine status reports of incidents in progress for resolution such as a network or server outage that impacts Commonwealth Services.

Incident reports summarized by incident category will be provided to the Commonwealth on a daily basis. This includes performance related incidents as a separate category.

Incidents with critical service impact will be reported in the Unisys Portal in a dashboard format. Routine incident reports including performance related items will be reported with status on resolution.

3.D Examples of automated notifications include, but are not limited to, drive full (Warning, critical), unscheduled reboots, server instability, etc. and to be defined in the CCPM.

The Unisys Team has a standard set of monitoring thresholds and alerts for infrastructure CI's utilizing the proposed monitoring tools. Unisys Team will review these thresholds with the Commonwealth and will document the threshold and alerts in the CCPM. Automated incidents will be created for specific alerts. The following are a few examples of performance related alerts.

1. Alert: Available Megabytes of Memory is too low

   Source: Microsoft Windows Server 2008 R2 Enterprise

   Path: Server Name

   Alert description: The threshold for the Memory\Available MBytes performance counter has been exceeded. The value that exceeded the threshold is: 94.333333333333329.

2. Alert Severity: 1

   Alert: High CPU Process List Alert.

   Source: Server Name

   Path: xxxxxx

   Alert description: Event Description: The processes using greater than 90% CPU at present are:

   ArcMap (13528): 98%

3.E Offeror must have to ability to provide performance information on a daily, weekly, and monthly basis.

See 3.A above.

3.F Offeror must provide sample performance monitoring reports and approach to supporting daily, weekly and monthly reporting.

Unisys will collect and report on the performance data for infrastructure supporting Commonwealth applications on a daily, weekly and monthly basis. The specifics will be agreed to during Transition. Reports will be posted to the Services Portal for Commonwealth review.

Unisys will review standard reports for performance monitoring during transition and agree to the cycle of reporting for daily, weekly and monthly reports. Sample performance reports are in Attachment F-11.

3.G Offeror must describe its approach to provide Commonwealth the ability to utilize Offeror's monitors (tools) as well as adding its own.

Unisys will support the Commonwealth agency application owners by providing dashboard views of performance monitoring for the infrastructure supporting agency applications. The agency application owners also have access to all performance reports through the Services Portal. This should satisfy performance management and monitoring requirements for the agencies' application owners. When more in depth performance monitoring is required this can be accomplished in several ways:

- A Change Request to the PMO Governance following the development of performance standards during transition.
- Services Catalog Requests for more in-depth performance management and monitoring.

4 Monitoring Capabilities, Load Testing Performance

4.A Support the load testing of applications by providing additional targeted performance monitoring Services during the testing period. This service will be made available as an additional service.

Unisys will support the load testing of applications by providing targeted performance monitoring Services during the testing period.

This service is provided when the Commonwealth requests infrastructure with SLA's for availability and performance. Therefore, monitoring for these performance requirements to support SLA's is provided in the test environment. Unisys will provide the performance management tools to support availability and performance monitoring on these servers during load testing. Standard performance reporting is provided during load testing for the Commonwealth. Additional targeted performance monitoring and reporting during load testing periods can be requested through the Enterprise Services Catalog.

4.B Provide load-testing performance monitoring as an add-on service.

Please refer to 4.A above.

4.C Offeror must describe its monitoring capabilities and tools to support load-testing performance.

Please refer to the performance monitoring tools outlined in 1.A above.

5 Training, Performance Monitoring

5.A Provide the Commonwealth with training on the use of performance management tools and reporting

Offeror must describe its training approach to provide this training to Commonwealth users.

Unisys will provide training to Commonwealth agency users on how to utilize the standard performance monitoring dashboard views and reports. This can be accomplished during transition and performed thereafter on an as needed basis.

6 Monitor Agency Application

6.A Support for agency level monitors - agency applications may require additional application level monitoring to be provided and managed by the Commonwealth agencies.

Please refer to 3.G above.

6.B Support synthetic transactions in applications to create a "dashboard" view that applications are working properly.

Please refer to 3.G above.

6.C The Offeror must allow additional agency based monitors to be installed and managed by individual Commonwealth Agencies

Please refer to 3.G above.

6.D Examples of automated notifications include, but are not limited to, drive full (Warning, critical), unscheduled reboots, server instability, etc. and to be defined in the CCPM.

Please refer to examples shown in 3.D above for examples of notification.

Continual Process Improvement

Unisys recognizes the significant importance of Quality and Continuous Service Improvement to:

- Reduce service risk,
- Improve service quality,
- Improve client satisfaction,
- Provide service transparency, and
- Improve/reduce costs of service.

Through a continuous cycle of evaluation and improvement within an IT infrastructure, Unisys views quality and continuous service improvement as a critical success factor in driving customer satisfaction for the Commonwealth IT infrastructure. Each of the continuous service improvement areas identified above are driven through the tight integration of the following organizations, industry tools, proven processes and quality deliverables:

- Service Excellence Office,
- Quality Plans: transition and steady state service delivery
- Industry standard frameworks and methodologies: ITIL, ISO, SSL
- Industry accepted measurement tools
- Continuous Service Improvement & Innovation Processes (CSIIP)
- Risk management, audits and business continuity management
- Client Satisfaction Surveys and Knowledge Management Portal

Collectively this represents Unisys Integrated Quality Plan for the Commonwealth of Pennsylvania.

Specifics on each of these areas are outlined in Schedule F, Section 3.2.1.1.6 Continuous Service Improvement. Highlights from this section are outlined below and requested service examples are provided at the end of this section.

7 CI Service Risk

7.A Offeror must provide examples of previous Offeror initiatives aimed at eliminating or mitigating service risks.

Risk management, independent quality audits, and business continuity management are integral quality management processes. Unisys is committed to managing risks and facilitating the achievement of business objectives, the adherence to quality processes. We mitigate risk through the implementation of tight quality controls: standard policies, procedures, roles, risk assumptions, issues, and definitions, etc.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

8 CI Service Quality

8.A Offeror must provide examples of previous Offeror initiatives aimed at improving service quality.

The quality approach begins with the Service Excellence Office. The SEO function provides definition and oversight of all ITIL process management and analysis functions. Process managers and analysts working in the Service Excellence Office are responsible for auditing process effectiveness, ensuring that service delivery teams comply with proper execution of processes, and analyzing process trends for anomalies. Continuous service improvement programs in collaboration with Commonwealth agencies are managed by the Service Excellence Office.

Through our Continuous Service Improvement and Innovation Process (CSIIP), the SEO reviews, analyzes and makes recommendations on improvement opportunities in each ITIL lifecycle phase. Unisys will leverage Six Sigma Lean tools and methodologies as well as ISO Certified internal audits to measure and maintain the highest quality services to the Commonwealth.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

9 CI Client Satisfaction

9.A Improve client satisfaction.

Offeror must describe methods to continually improve client satisfaction.

Client satisfaction is extremely important to Unisys and a key focus in our IT solution. The SEO will integrate new agencies, customers and services into our multi-pronged client satisfaction approach that includes Service Desk surveys on the caller's experience, an overall agency satisfaction survey, and quarterly surveys with the Office of Administration. Data collection will be gathered across multiple levels to gain a clear understanding of the Commonwealth's satisfaction with the IT Services being provided.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

10 CI Service Transparency

10.A Provide service transparency.

Offeror must provide examples of previous Offeror initiatives aimed at providing service transparency; in particular, visibility into the service execution process

The service organizations will use standardized ITSM services processes, IT monitoring & automation tools. ITSM processes will be documented in the Commonwealth Computing Procedures Manual (CCPM). The CCPM will be available to Commonwealth approved staff on the Knowledge Management Portal (KMP) providing desired transparency into service execution processes. Through the Real-time Dashboard, the Commonwealth will have access to current operational performance of their application infrastructure.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

11 CI Service Sustainability

11.A Ensure service Sustainability.

Offeror must provide examples of previous Offeror initiatives aimed at ensuring service sustainability; in particular, efforts targeted at cost containment and cost reductions.

Service is sustainable by integrating any new agencies, customers, or services into our standard operational and quality processes and methodologies. This will be accomplished by leveraging ITIL processes, creating quality project plans, utilizing industry accepted measurement and monitoring tools, analyzing trending reports and providing proactive continuous service improvement throughout the IT lifecycle will enable new Commonwealth services to experience and sustain IT services and client satisfaction.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional

details in this area.

12 CI Reduce Cost of Service

12.A Improve/reduce cost of service.

Offeror must provide examples of previous capacity initiatives implemented that achieved reduced costs of Services and that met or exceeded ROI (Return on Investment) analysis projections. If costs of Services increased due to increased required capabilities, so identify.

The Service Excellence Office will proactively manage quality, continuous service improvement, ITIL process management, and customer satisfaction through a comprehensive quality plan that specifically addresses all of these areas. We believe this is a key differentiator in our partnership with the Commonwealth. Through this new organization and these quality plans, Unisys will drive best in class services and the highest customer satisfaction experience, while reducing overall costs to the Commonwealth.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

Unisys examples of continuous improvement

A few examples of continuous service improvement have been included below under Unisys Team Experience.

Unisys Team Experience

A few examples of Performance Monitoring & Management Continuous Service Improvements, that have been implemented or can be utilized to achieve reduced costs of services and to meet or exceeded ROI (Return on Investment) analysis projections are outlined below:

Leveraging of the DPH to support [redacted] for remote monitoring:

The Unisys DPH Team was leveraged to provide remote support to the 3000+ servers supported by the [redacted] By leveraging the DPH 24x7 Level 1 staff, this has allowed [redacted] staff to focus more on the overall support of these environments. DPH staff monitors, troubleshoots and escalates to [redacted] staff based on alerts received from the SCOM monitoring tool running in the [redacted]

Reporting - IES Performance Management Reporting:

Since the introduction of IES to the DPH, the IES Monthly Performance Reporting has evolved. At the request of IES, a number of requested modifications were made to the standard Monthly Performance Reports. Through the leveraging of several monitoring tools, SCOM being the most significant, we are providing the Bureau with enhanced reporting. These modifications allow the Bureau greater in-sight to their current performance and usage. At the request of IES management, beginning in March 2013, we improved the reporting again by developing and adding an Executive Management Summary Dashboard to be included in each month's reporting. This allows IES senior management a quick look at their overall performance indicators focusing on exceptions without the need to scrutinize the entire report.

Tools - Monitoring:

In order to proactively monitor potential performance issues in the shared XIV Storage

environment, the Unisys DPH Team has implemented threshold policies through SCOM monitoring to report XIV storage latency time. This logic notifies us early on of an internal XIV failure and the repercussions on connected hosts.

Unisys currently provides IT Service Management Services to more than 150 customers worldwide. Unisys is a leading provider of Managed Services utilizing an integrated suite of ITIL V3, ISO 20000 certified management processes and leading ITSM tools to provide outstanding service IT services to our customers. Unisys currently successfully manages Performance Monitoring and Management for many of these customers.

Unisys has been managing Performance Management and Monitoring for the Commonwealth DPH and [redacted] since 1999.

Benefits to the Commonwealth

The Unisys value proposition for performance monitoring and management to the Commonwealth is simple, for the Unisys Team to provide reliability of infrastructure to support applications and services for the Commonwealth.

The Unisys Team focuses on providing reliable infrastructure that performs to meet SLAs for so the Commonwealth Application Owners can depend on this infrastructure to provide reliable services to application users.

The Commonwealth agencies can depend on Unisys to provide reliable services.

3.2.3 Facilities Management

3.2.3.1 Facilities Architecture / Maintenance

The Facilities Architecture and Maintenance service will provide and staff a minimum of two fully operational datacenter facilities in a multi datacenter mode. This service will require the integration and alignment of the non-core Services, including those relating to the premises, required to operate and maintain a datacenter that will fully support the core objectives of this project.

These datacenters will be geographically dispersed to provide protection from regional disruptions such as weather, power or other emergencies. The process of locating and managing these physical environments will include defining the physical site requirements, selecting appropriate facilities, and designing effective processes for monitoring and maintaining environmental Services and managing physical access. Effective management of the physical environment reduces the possibility of service interruptions due to unauthorized access and damage to computing equipment and personnel. Please review Exhibit D.7 - [redacted] Facility Summary for information regarding the [redacted] facilities.

Facilities Management includes all aspects of providing and managing the physical environment. For example, power and power distribution, cooling and ventilation, fire detection and suppression, building security and access control, and environmental monitoring are all required. Listed below are the basic Services required, but not inclusive of all Services needed, to manage an enterprise class datacenters required by the Commonwealth.

Reference Documentation

Exhibit D.7 - [redacted] Facility Summary

	Requirements	Describe Compliance
1.	Safe and secure datacenter. Two layers of authentication and appropriate clearances will be required. Provide datacenter environments which are secured to ensure that only authorized personal have physical access to the buildings, systems and all levels of data. This includes data storage within networked storage devices, servers, tapes, diskettes, optical and paper formats.	Offeror must describe its proposed facilities security program.

	Comply with the security requirements of the Commonwealth. Immediately inform the Commonwealth of any vulnerability or weakness in the Services, and recommend a solution or mitigation. Offeror must assess the [redacted] facilities and provide a report to the Commonwealth as it pertains to required security upgrades.	
2.	Provide fully redundant environmental Services. To include, but not limited to, HVAC, UPS conditioned power and distribution, generator backup, automated transfer switch, fire suppression system. Offeror must integrate its Facilities Management process with Service Management processes, especially Change Management, Incident Management, Service Continuity Management and Availability Management. Offeror must confirm its ability to provide, manage, maintain and operate multiple Tier 3 equivalent facilities. Offeror must assess the [redacted] facilities and provide a report to the Commonwealth as it pertains to required HVAC and power upgrades.	Offeror must describe solution and approach to meet this requirement. Offeror must provide details and supporting documentation on its proposed facilities and tier rating.
3.	Staff the datacenters with appropriate operational and management levels of personnel 24/7/365. Critical engineering and management staff will be available to the Commonwealth Monday through Friday, between 8am – 5pm Eastern time excluding Commonwealth observed	Offeror must describe its proposed facilities staffing approach, including its staffing approach related to the [redacted]

	holidays. Access to operational staff will be available 24/7/365. Video surveillance system will be utilized at all entry points and throughout the datacenter and tape storage areas. Datacenter Staff will be required to adhere to the Commonwealth requirements for background checks and security clearances. Offeror shall be required to monitor the status of staff and to take appropriate action for staff found to subsequently have violated prescribed legal or ethical standards as described in **Schedule G –Staffing Plan and Key Positions**. Such violations shall be immediately reported and appropriate actions taken. Commonwealth verification of the requirements will be necessary prior to staff working on Commonwealth related systems.	
4.	Procurement Planning - Provide program and processes to alter the datacenter environment and to refresh the environmental Services at end-of-life, and as additional Services are needed.	Offeror must describe its facilities management processes, including those related to the [redacted]
5.	Physical Access to Facilities- Coordinate with the Commonwealth to provide for physical access and facilitate inspections by government authorities (including the Commonwealth) for auditing the conduct of government business. Offeror must assess the [redacted] facilities and provide a report to the Commonwealth as it pertains to required physical access to the [redacted] facility.	Offeror must describe its facilities access policies and procedures.

6.	SLA Reporting - Identify and create environmental service level objectives in the form of SLAs, and report on the service availability, problems, and corrective actions on a monthly basis. Offeror must assess the [redacted] facilities and provide a report to the Commonwealth as it pertains to monitoring, maintain and reporting on [redacted] SLAs.	Offeror must describe how it monitors and manages facility availability.
7.	The facilities must be designed and operated with environmentally friendly equipment and techniques, and be SSAE 16 compliant. Offeror must assess the [redacted] facilities and provide a report to the Commonwealth as it pertains to monitoring, maintaining and reporting on [redacted] SLAs.	Offeror must list all compliance ratings achieved at the proposed datacenters. Offeror must provide copies of annual SSAE 16 audits for all datacenters used to service the Commonwealth (and its agencies) at the Offeror's expense.
8.	Offeror must schedule (at its expense) a SSAE 16 audit of the [redacted] datacenter no more than 12 months after the effective date of the contract.	Offeror must provide proof of a valid (updated) SSAE16 certification in the form of audit findings report prior to implementing any Commonwealth service in any other proposed datacenter.
Continual Service Improvement		
9.	Reduce service risks.	Offeror must provide methods to eliminate or mitigate service risks.
10.	Improve service quality.	On a quarterly basis, Offeror must recommend to the Commonwealth team any facility changes that would be appropriate to maintained or improve SLA commitments.
11.	Improve client satisfaction.	Offeror must provide examples of previous

		Offeror initiatives aimed at continually improving client satisfaction.
12.	Ensure service transparency.	Offeror must provide methods and practice to ensure service transparency, providing visibility into service execution.
13.	Improve/reduce cost of service.	Offeror must provide examples of Facilities Management initiatives have been implemented or can be utilized to achieve reduced costs of Services and to meet or exceeded ROI (Return on Investment) analysis projections.

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

Introduction

Facilities Management is critical to the overall success of the Unisys Team and the Commonwealth. Management of the [redacted] Data Center Facility will be performed in a manner similar to that of the Data PowerHouse, and integrated with the operations at Unisys [redacted] These operations are performed to adhere to OSHA and SSAE-16 audit requirements. Unisys as the tenant at the [redacted] will perform management functions on behalf of the Commonwealth to include general maintenance, improvements and housekeeping for the data center. The Unisys Facilities Procedures Plan provides a proven framework for all facility-related work performed at the facilities. All facility management work detailed will be subject to the Change Management process.

The Facilities Management Plan provides job requirements for facility-related work such as electrical, mechanical, and general construction installations, furniture installations, or other services within the [redacted] facility. Specific requirements are established for all contractors, equipment installations and deliveries, equipment de-installation and shipping. These procedures are specific and must be followed as described in the plan.

In addition, the procedures in this plan include the framework to coordinate all contractor work for the [redacted] facility and the facilities. Procedures are included which pertain to all contractor work requirements for the following:

- Computer Room Work Requirements
- Lockout/Tagout
- Hot Work, Cutting, and Welding
- Raised Floor Maintenance

- Fire Suppression Shutdown
- Environmental, Safety & Health

1 Facility Security Program

1.A Safe and secure datacenter. Two layers of authentication and appropriate clearances will be required.

Each facility has both physical and logical security in place and ready to deploy down to the rack level if requested. Perimeter security is maintained by camera and an active physical security presence. All facilities include guard-controlled access to interior spaces. In each case, guard-controlled access to segregated data hall areas can be incorporated upon request.

Access control systems include access to and within the facilities in all data centers. Access control is through a combination of keycard, keypad and biometric devices. In addition, access control systems including keypad and biometric authentication capabilities are available for the raised floor on areas segregated from portions of the Commonwealth's service area. The Commonwealth can request these services including security caging, security cabinets, and cabinet or cage-level monitoring (camera or access) down to the rack level from the Enterprise Services Catalog.

Unisys Security Operations Center (SOC) is comprised of security support staff and a suite of automated tools that provide comprehensive 24x7x365 monitoring, alerting, and response to security events. Personnel follow specific instructions to mitigate issues according to the Security Incident Procedure (SIP) policy.

See Schedule F, Section 3.1.1 "Multi Datacenter Environment (2+ Architecture)" for additional, related material on the Unisys Data Center Architecture's Security approaches.

1.B Provide datacenter environments which are secured to ensure that only authorized personal have physical access to the buildings, systems and all levels of data. This includes data storage within networked storage devices, servers, tapes, diskettes, optical and paper formats.

Unisys data center architecture provides secure physical and logical separation from any adjacent facility or campus occupants, including an ability to provide similar segregation within the Commonwealth's IT services area. The Commonwealth's IT environment is secure physically and logically from other potential occupants of the facilities supporting it.

Unisys data center architecture provides optional physical and logical segregation within the Commonwealth's physical and logical data center spaces. Within the Commonwealth colocation space, security partitions can optionally be used to separate different agency environments and systems as required. The Unisys Team would work with the Commonwealth to determine the exact requirements for caged partitions within the already physically and logically separate Commonwealth/Unisys "data center vault." In anticipation of this requirement, Unisys has included a number of standard cages that can be deployed within the sites.

1.C Comply with the security requirements of the Commonwealth.

Unisys complies. Please see Schedule F, Section 3.1.1 "Multi Datacenter Environment (2+ Architecture)" for additional details.

1.D Immediately inform the Commonwealth of any vulnerability or weakness in the Services, and recommend a solution or mitigation.

Unisys Security Operations Center (SOC) is comprised of security support staff and a suite of automated tools that provide comprehensive 24x7x365 monitoring, alerting, and response to security events. The Unisys ITSM event management systems provide monitoring, alerting and triggers to response for infrastructure events including events sourced within the facilities' infrastructure. This includes automated notification to designated commonwealth representatives as required

Events that are caused by operational or physical design weakness are addressed immediately with any required coverage. This is done pending long-term changes initially addressed by Unisys Facilities Management and the Unisys architecture team and agreed upon with the Commonwealth. This process is managed through the change management and architectural governance processes.

1.E Offeror must assess the [redacted] facilities and provide a report to the Commonwealth as it pertains to required security upgrades.

The [redacted] Assessment project planned for the transition period evaluates the [redacted] facility and provides a report that meets the requirements of key deliverable D-01.01 as described in Schedule K. The physical and logical security assessment of the facility identifies required [redacted] facility security upgrades.

1.F Offeror must describe its proposed facilities security program.

Unisys data centers' architecture incorporates the latest in physical and operational security approaches.

Unisys [redacted] has deployed a centralized, electronic access control system that provides alarm monitoring points on all personnel and equipment doors, as well as intrusion detection throughout the facility. Photo ID badges with unique personal identification numbers, as well as biometric iris scanners, provide multiple levels of electronic access control, and provide individual accountability throughout the facility. The site's security systems control physical and electronic access to the building, the data center floor, and each client's caged area or module. 3-factor authentication is required to access the data floor. A fourth layer is required to access a client cage or module.

Both Unisys [redacted] and Unisys [redacted] have physical and logical security in place and ready to deploy down to the rack level if requested. Perimeter security is maintained by camera and an active physical security presence. In all cases, guard-controlled access to segregated data hall areas can be incorporated upon request.

Security within the [redacted] Data Center includes 24-hour guard protection, a proximity badge access control system, interior and exterior video surveillance consisting of cameras and recorders with some having motion detection sensors. Access within the facility to restricted or sensitive areas is controlled by the badge control system and is limited to individuals on a "need to have" basis.

Access control on the raised floors is through a combination of keycard, keypad and biometric devices. In addition, access control systems including keypad and biometric authentication

capabilities are available for the raised floor on areas segregated for the entire or within for a portion of the Commonwealth's service area. Security systems whether access control, monitoring, or alarming are incorporated into the Unisys operational model and ITSM tools permitting event correlation, logging and management alerting at all appropriate levels in the Unisys delivery team.

Building and Access Control is performed at the [redacted] through the use of building access cards maintained by the Commonwealth and augmented with the use of established Bio-Metric scanning devices. Building and Access Control for initial access into Unisys facilities is through the use of Security Guards to verify authorized access based on badge access or authorized visitor access. Badge readers or biometric scanning devices are used at access points throughout the facilities to allow deeper access only to those individuals requiring access to specific resources. The access levels are reviewed on a monthly basis by the Unisys Security Manager, Commonwealth Facilities Manager and Unisys Facility Manager for accuracy and updates.

2 Environmental Services Redundancy

2.A Provide fully redundant environmental Services. To include, but not limited to, HVAC, UPS conditioned power and distribution, generator backup, automated transfer switch, fire suppression system.

Unisys facilities were selected for the Commonwealth with an ability to meet and exploit the environment extremes common to their location. Steel and concrete construction was required along with interior floor loading characteristics that permit the variety of the Commonwealth's IT equipment.

Each facility has been selected for its ability to provide continuous, efficient, cost-effective power and environmental conditions. The Unisys team facilities provide between 2N+1 and 2N+2 redundancy. In addition, we have selected facilities with the capacity to grow to and beyond an estimate of the full requirement that the Commonwealth IT estate may have. The considerations include a review of the ability of local utilities to deliver electricity and the cost to meet and grow with the Commonwealth's use of each location.

Unisys data center facilities meet or exceed the Uptime Institute Tier III standard for concurrently maintainable data center site and infrastructure. The overall facility UPS topology is a distributed redundant configuration. Unisys [redacted] uses a patented, maintenance, bypass isolation feature. This feature enables our [redacted] facilities to exceed Uptime Tier 4 standards for data centers to be concurrently maintainable or fault tolerant. Because of this technology, the facility is concurrently maintainable and fault tolerant, with a simultaneous utility outage. This innovative level of critical infrastructure redundancy has been termed 2N+2: two completely separate power paths from the power utility to the customer rack (2N) and all of the critical components in those two independent power paths have (at least) two extras for backup (N+2).

[redacted] fire suppression system utilizes a multi-zone, dual-interlock, pre-action, dry pipe fire suppression system with intelligent smoke and thermal detectors which require both sensors in the same zone to detect an alarm condition in order to admit water into the pipes inside a critical area. Sprinkler heads are also fitted with a high-temperature fusible head in order to preclude admitting water into a computer room area where no fire is present. The fire

suppression and alarm system is integrated into the Network Operations Center and security office monitoring systems. In the event of a fire, all fire rated doors automatically close but still allow for egress.

Non-critical environments are protected by wet sprinkler systems with protection/notification as required by local ordinances/codes.

At [redacted] fire and smoke detection is provided by a Fenwal Vesda HSSD air sampling system. Fire suppression is provided by a wet pipe sprinkler system. These approaches meet NAFP standards, and they are augmented by a PAL under-floor water detection system.

2.B Offeror must integrate its Facilities Management process with Service Management processes, especially Change Management, Incident Management, Service Continuity Management and Availability Management.

Each of the Unisys facilities' Building Management Systems including their power and environmental control systems will be linked to the Unisys ITSM environment. This integration will permit monitoring integration and correlation giving a holistic view – utility to application infrastructure – view of all facets of the IT environment. With this linkage, security, power, and environmentals become measurable elements of the heartbeat of the Commonwealth's IT estate. The result is that the buildings become active members in the incident, service continuity and availability management processes.

In addition, a common Data Center Infrastructure Management (DCIM) system using the [redacted] family of tools integrates with the ITSM environment. The system along with Unisys facilities staff and space planners enables the environment of the facilities to become managed components of the Commonwealth environment and participants in the policy and processes enabled ITSM for change, release, asset, and configuration management.

Finally, it is Unisys plan to integrate the [redacted] into the ITSM environment with integration of its BMS into the Unisys ITSM environment and extend the Unisys DCIM system to cover the [redacted] its systems, floor space, and cable management.

2.C Offeror must confirm its ability to provide, manage, maintain and operate multiple Tier 3 equivalent facilities.

The Unisys Team currently manages over 400 of its own data centers for its clients globally including the Commonwealth's Data PowerHouse. A majority of these locations are at or above an equivalent Tier 3 rating. These facilities include the Unisys [redacted] and the [redacted] sites proposed here for the Commonwealth.

2.D Offeror must assess the [redacted] facilities and provide a report to the Commonwealth as it pertains to required HVAC and power upgrades.

2.E Offeror must describe solution and approach to meet this requirement.

The [redacted] Assessment in deliverable D-01.01 includes the power and HVAC systems. These are evaluated for alignment with contract requirements and facility objectives. In addition, the

assessment evaluates on the ability of and requirements for the facility to meet, to have monitored, to operate and to maintain the installed infrastructure and [redacted] SLAs. Finally, the assessment anticipates a statement of direction and objectives for the [redacted] in the Data Center Architecture Plan and Roadmap's Implementation section.

2.F Offeror must provide details and supporting documentation on its proposed facilities and tier rating.

Please see **Schedule E: Data Center Locations** for additional information on the proposed facilities. In addition, Unisys would like to extend an offer to the Commonwealth to visit our proposed facilities and meet our facilities management team.

3 Staff, Facility Staffing Approach, [redacted] Staffing Approach

3.A Staff the datacenters with appropriate operational and management levels of personnel 24/7/365. Critical engineering and management staff will be available to the Commonwealth Monday through Friday, between 8am – 5pm Eastern time excluding Commonwealth observed holidays. Access to operational staff will be available 24/7/365. Video surveillance system will be utilized at all entry points and throughout the datacenter and tape storage areas.

Each facility maintains an active staff 24x7; in addition, engineering and management staff is always available to the Commonwealth during regular business hours. However, the Commonwealth has 24x7 access to operational staff via the service desk and access to the facilities can be arranged as needed within the security parameters established in the CCPM and consistent with both Unisys and Commonwealth policy.

Video surveillance includes both exterior and interior surveillance at all Unisys-managed facilities. For more detailed information please refer to Schedule F, Section 3.1.1 "Multi Datacenter Environment (2+ Architecture)".

3.B Datacenter Staff will be required to adhere to the Commonwealth requirements for background checks and security clearances. Offeror shall be required to monitor the status of staff and to take appropriate action for staff found to subsequently have violated prescribed legal or ethical standards as described in Schedule G –Staffing Plan and Key Positions. Such violations shall be immediately reported and appropriate actions taken. Commonwealth verification of the requirements will be necessary prior to staff working on Commonwealth related systems.

All Unisys staff who has physical or logical access to the data center will adhere to the Commonwealth ITBs related to background checks and security clearances. This includes initial checks prior to hire as well as annual checks. Documentation related to the background checks will be shared with the Commonwealth to enable verification prior to staff working on Commonwealth systems.

The Unisys team will comply with the legal and ethical standards as described in Schedule G. Any violations will be immediately reported and appropriate actions taken per requirements.

3.C Offeror must describe its proposed facilities staffing approach, including its staffing approach

related to the [redacted]

The Facilities Management function is responsible for management of the Commonwealth's Enterprise Data Center and Unisys Tier 3+ equivalent facilities from which services are provided. Services include Computer Operations, Systems Monitoring, Batch and Media Management. This function is staffed with a qualified on-site support team 24 hours a day, seven days a week. The team uses an extensive suite of automation tools ensuring consistency and accuracy of services provided, and expeditious alerting of changes to the facility and systems environments.

The services provided by the on-site team for each facility including the [redacted] provide security management, media management and facilities management. In addition, the Unisys Team includes staff for computer operations and monitoring, and batch services that are operating out of the Unisys Harrisburg Operations Center and in continuous communication with each facility's on-site personnel.

For details on the staffing approach for the facilities and their operations, please refer to Section 5.0 "Staffing Plan" for facilities and operations.

4 Facility Management Approach, [redacted] Management Approach

Facilities Management is critical to the overall success of the Commonwealth. Management of the [redacted] Data Center Facility will be performed in a manner similar to that of Unisys management of the Data PowerHouse. Furthermore, the [redacted] facility management will be integrated with that for Unisys [redacted] and Unisys [redacted] and be performed to adhere to OSHA and SSAE 16 audit requirements. Unisys as the tenant will perform management functions on behalf of the Commonwealth to include general maintenance, improvements and housekeeping. The Unisys Facility Procedures Plan provides a proven framework for facility-related work performed at the [redacted] facility. All facility management work detailed is subject to the Change Management process and supported by the Unisys ITSM tools.

4.A Procurement Planning - Provide program and processes to alter the datacenter environment and to refresh the environmental Services at end-of-life, and as additional Services are needed.

The Unisys solution manages data center upgrades and new technologies through ITIL V3 processes within Service Design, which manages new services and changes to services to meet the Commonwealth's strategy to improve services and cost efficiencies. The Service Design process described in Schedule F, Section 3.2.1.5 "Technical Architecture" also manages the requirements and capacity needed within the Infrastructure Architecture Services framework as described in Schedule F, Section 3.2.2.2 "Infrastructure Architecture".

This approach includes lifecycle management of facilities infrastructure and capacity.

4.B Offeror must describe its facilities management processes, including those related to the [redacted]

The Facility Management Plan provides job requirements for facility-related work such as electrical, mechanical, and general construction installations, furniture installations, or other services within the [redacted] or Unisys facilities.

Specific requirements are established for all contractors, equipment installations and deliveries, equipment de-installation and shipping. The procedures in this plan include the framework to coordinate all contractor work for the [redacted] facility and the Unisys facilities. Procedures are

included which pertain to contractor work requirements for the following:

- Computer Room Work Requirements
- Lockout/Tagout
- Hot Work, Cutting, and Welding
- Raised Floor Maintenance
- Fire Suppression Shutdown
- Environmental, Safety & Health

Contractor performing facility-related work such as electrical, mechanical and general construction installations, furniture installations, or other services affecting the [redacted] facility and the Unisys facilities must follow the work rules. Non-conformance to these work rules is grounds for contractor removal from the [redacted] facility and the Unisys facilities. These rules include:

- Contractor activity must be coordinated through the Unisys facility manager.
- A Work Coordination Form must be completed by the Unisys project manager and submitted to the Unisys Operations Manager and Data Center Manager not less than seven days before commencement of work for major projects or 2 days for minor work.
- Work activities requiring Commonwealth management or [redacted] Facility approval will require additional time for approval.
- Unisys project managers may not schedule contractor work without prior approval.
- Contractors arriving for work that are not pre-authorized are not granted admission to the facility.
- As necessary, the Unisys project manager and contractor representative will be requested to attend a pre-work coordination meeting.
- All contractors must conform to Unisys Environmental, Health, and Safety rules.
- All contractors must conform to Unisys Security procedures.
- All contractors must either be escorted or obtain a visitor's pass.

For detail on when these work rules are engaged in the support of facility infrastructure refresh see Schedule F, Section 3.2.3.2 "Site Operations."

Unisys is committed to responsible environmental management. We take a proactive role in maintaining a safe and healthy workplace, operating our facilities in an environmentally sound manner, and promoting programs that support environmental stewards. It means conducting business in a responsible manner, with respect and concern for the environment. It is a matter of strictly adhering to local, national, and international laws governing environmental protection and offering environmentally responsible services. On a regular basis, regulatory compliance validation reviews are performed at Unisys locations to evaluate conformity with location-specific environmental regulations and established Unisys best practices.

Third-party assessments are performed independent of internal reviews to add objectivity to the evaluation process. Unisys has not received a notice of violation or a fine for non-

compliance of environmentally related matters in the past three or more years. To foster this commitment, Unisys has assembled a staff of qualified professionals possessing extensive experience. These skilled professionals are responsible for identifying and resolving environmental, safety, and health issues in a timely, cost-effective and technically sound manner. Environmental Programs that Unisys currently manages are:

- ISO 14001 Environmental Management Systems
- Carbon Footprint
- Pollution Prevention
- Solid Waste Recycling
- Vital Resource Conservation
- Energy Conservation
- Green Lights Partner
- End of Life Product Disposition Program
- Product reuse and recycling programs
- Lithium Batteries Recycling Program
- Printer cartridge recycle program
- Environmentally safe packaging
- Clean Air Program
- Travel Reduction
- Ozone Depleting Substances (ODS) Management
- Design for the Environment Product Program
- Supply Chain Information
- Environmentally-Safe Packaging
- Community Commitments & Concerns
- Employee Health and Safety
- Health and Safety Program Management
- Management of Injuries and Illnesses
- Hardware Dismantling and Selective Treatment
- WEEE-Compliant Instructions for Hardware Disassembly
- Environmental Recognitions and Awards

5 Facility Access Policies and Procedures

5.A Physical Access to Facilities- Coordinate with the Commonwealth to provide for physical access and facilitate inspections by government authorities (including the Commonwealth) for auditing the conduct of government business.

Unisys welcomes the Commonwealth to visit facilities supporting the Commonwealth's IT

services. However, to maintain the security and operational posture Unisys requests that designated Commonwealth individuals provide at least 24-hours' notice to their Unisys Agency Account manager, if possible, who will contact the Unisys Team's Data Center and Facility Manager. This advance notice allows Unisys to prepare for the potential interruption that the visit may incur in the regular operation of the facilities. If warning is not possible, Unisys requests patience while we arrange access and facility escort.

For longer periods of access such as for lengthy audit processes or a series of recurring visits, Unisys requests 2 weeks' notice to include times of access and names of those needing entry, which must come from designated Commonwealth individuals given the express authority to make such requests. This form of request provides Unisys sufficient time to prepare security arrangements that may include verification of the request with proper Commonwealth authorities and security staff and the scheduling of Unisys security personnel to be present, to escort and enable access and to monitor the area and visitors.

In the event that circumstances require sudden and unanticipated access to the facility by authorized Commonwealth representatives, the Unisys Data Center and Facilities Manager will contact his Commonwealth counterpart to alert them to the circumstances and consult on the appropriate course. In such instances, Unisys requests the Commonwealth's patience. Unisys does not allow visitors into facilities under its management without a Unisys facilities team member who has the express authority to escort. When presented with the access request, Unisys places that team member at the disposal of the visitor as expeditiously as possible and per the Commonwealth's instruction.

Ultimately, Unisys objective is to maintain the security and operational standing of the facilities and maintain Unisys responsibility to the Commonwealth for facilities dedicated to the Commonwealth's IT services while permitting, to the degree possible, the proper exercise of government.

5.B Offeror must assess the [redacted] facilities and provide a report to the Commonwealth as it pertains to required physical access to the [redacted] facility.

The [redacted] Assessment in deliverable D-01.01 includes security, power and HVAC systems. These are evaluated for alignment with contract requirements and facility objectives. In addition, the assessment evaluates on the ability of the facility to meet, to have monitored, to operate and to maintain the installed infrastructure and [redacted] SLAs.

The [redacted] Assessment's findings are interpreted with respect to the Commonwealth's SLAs for the contract. Recommendations are then developed on the gaps that the current [redacted] facility has in meeting the SLAs. This interpretation includes consideration of the integration of the facility's BMS system into the Unisys ITSM service management tooling and the implementation of the common facilities DCIM system based on [redacted]

Finally, the assessment is anticipatory to a statement of direction and objectives for the [redacted] within the evolving Data Center Architecture Plan and Roadmap's Implementation Roadmap section. These objectives will reflect the recommendations derived from findings in the areas of electric power systems, HVAC systems, fire detection and suppression systems, building and access control processes and systems and environment management.

5.C Offeror must describe its facilities access policies and procedures.

Unisys owned or managed facilities are secured with physical surveillance including a security guard force that provides security and safety, access control systems on both exterior and interior points to control access to only authorized individuals, and 24x7 video surveillance systems that monitor and digitally record onsite activities.

Employee clearance includes background verification, Unisys confidentiality agreements, ethics training with annual certification, and information security training with annual certification.

Procedures for employees and vendors to access data centers include:

- Data Center Safety and Work Rules Certification prior to granting unescorted access.
- All employees must have a valid Smart Card to gain access into the building using the badge reader system.
- All non-Unisys personnel must check in and gain authorization for entry into the building through the security guard. Must be certified for unescorted access.
- There are 3 levels of data center access security:
  1. General access into the building
  2. Data floor
  3. Secure Cages on the data floor
- Multiple levels of approval are required to gain approval for access to the Data Floor areas.

6 SLA Reporting, Facilities Availability

6.A SLA Reporting - Identify and create environmental service level objectives in the form of SLAs, and report on the service availability, problems, and corrective actions on a monthly basis.

Unisys measures its facilities management against key performance indicators such as the availability of its major infrastructure equipment such as the components of the electrical power systems, or the response to change and problem management activities within the facility. Unisys data center SLAs can incorporate the [redacted] to provide both individual site and an overall view of the environment supporting the Commonwealth's IT systems.

As a starting point, Unisys proposes to incorporate an SLA reflecting uptime availability. As an example, please see the availability report shown for the [redacted] data center in **Schedule E "Data Center Locations".**

With the completion of deliverable D-08 "Facilities Management Plan" D-08.01, Unisys can recommend additional SLAs that may offer other views for the data centers separately and as a combined environment. The SLAs to be recommended may include SLAs for the availability of power from generators or UPS. Upon completion of the [redacted] SSAE-16 audit, deliverable D-08.02, a review of the SLAs offered for the facilities can occur to determine if additional SLAs are appropriate, at what levels and with what remediation upon an SLA miss.

6.B Offeror must assess the [redacted] facilities and provide a report to the Commonwealth as it pertains to monitoring, maintaining and reporting on [redacted] SLAs.

The Unisys operations of the [redacted] are integrated into the range of SLA monitoring and reporting processes and tools implemented for the services provided. These include reporting on SLAs and availability of the [redacted] To accomplish this integration, Unisys intends to integrate the [redacted]

building management system into the Unisys ITSM environment.

6.C Offeror must describe how it monitors and manages facility availability.

Unisys [redacted] uses a number of tools for the monitoring and management of the facility's availability including:

- GE iFIX for monitoring of the overall electrical plant.
- Schneider Citect for monitoring of the mechanical plant.
- TrendPoint for branch circuit breaker monitoring.
- Intellibatt for battery monitoring.
- SynapSense for data center environmental monitoring

Unisys [redacted] is monitored through a sophisticated and integrated Building Monitoring System, where over 2000 points are monitored on the system. Raised Floor support equipment is monitored with a Liebert SiteScan System with monitor and trending capability. Computer Room Air Conditioners (CRAC) unit return air temperatures are monitored and trended, any CRAC alarms are sent to the Siemens Building Management System (BMS) and are responded to by two teams – security guards and BMS mechanics. These two 7x24 on-site teams double check to verify that each alarm is addressed. Other important parameters monitored are Data Center Efficiency and Power Utilization Effectiveness (PUE), PDU kilowatt load, UPS kilowatt load, utility and generator loads and status. Virtually any alarm available on a device is tracked and responded to with the BMS system.

The [redacted] Data Center Infrastructure Management (DCIM) tool is used to track all IT equipment installed in the facilities including the [redacted] Rack level monitoring of planned and actual (where available) racks loads are tracked to anticipate circuit loading or cooling hot spot issues prior to installation of equipment. All cable connections are tracked in [redacted] if Unisys installs the equipment.

Ultimately, the management and monitoring systems and processes of [redacted] are tied into the Unisys ITSM system to provide a single environment from which to manage the data centers. Alerts and alarms from the facility systems are integrated into the Unisys ITSM including those available from the [redacted] BMS. Unisys solution includes the implementation of the [redacted] DCIM tool for the space and cable management of the [redacted] as a member of the Unisys facilities solution for the Commonwealth.

7 Compliance Ratings, SSAE 16 Audits

7.A The facilities must be designed and operated with environmentally friendly equipment and techniques, and be SSAE 16 compliant.

Unisys complies. Please refer to Schedule F, Section 3.1.1 "Multi Datacenter Environment (2+ Architecture)" items 5A and 6A for additional details.

7.B Offeror must assess the [redacted] facilities and provide a report to the Commonwealth as it pertains to monitoring, maintaining and reporting on [redacted] SLAs.

The [redacted] Assessment in deliverable D-01.01 includes security, power and HVAC systems. These are evaluated for alignment with contract requirements and facility objectives. In addition, the

assessment evaluates on the ability of and requirements for the facility to meet, to have monitored, to operate and to maintain the installed infrastructure and [redacted] SLAs.

The [redacted] Assessment's findings will be interpreted with respect to the Commonwealth's SLAs for the contract. Recommendations will be developed on the gaps that the current [redacted] facility has in meeting the SLAs. This interpretation includes consideration of the integration of the facility's BMS system into the Unisys ITSM service management tooling and the implementation of the common facilities DCIM system based on [redacted]

Finally, the assessment is anticipatory to a statement of direction and objectives for the [redacted] within the evolving Data Center Architecture Plan and Roadmap's Implementation Roadmap section. These objectives will reflect the recommendations derived from findings in the areas of electric power systems, HVAC systems, fire detection and suppression systems, building and access control processes and systems and environment management.

7.C Offeror must list all compliance ratings achieved at the proposed datacenters.

Please see Schedule E for documentation of recent certifications achieved at Unisys [redacted] and Unisys [redacted] In addition Schedule F, Section 3.1.1 "Multi Datacenter Environment (2+ Architecture)" item 6A.

7.D Offeror must provide copies of annual SSAE 16 audits for all datacenters used to service the Commonwealth (and its agencies) at the Offeror's expense.

Please see Schedule E for copies of reports from recent SSAE 16 audits for Unisys [redacted] and Unisys [redacted] Annual SSAE 16 audits will be conducted for the Unisys data centers and [redacted] and copy of these reports will be provided to the Commonwealth. For more information see Schedule F, Section 3.1.1 "Multi Datacenter Environment (2+ Architecture)" item 6A.

8 SSAE 16 Audits

8.A Offeror must schedule (at its expense) a SSAE 16 audit of the [redacted] datacenter no more than 12 months after the effective date of the contract.

An SSAE 16 audit is planned for the [redacted] within the first 12 months of the contract start date. In addition, this audit will become an element of similar annual audits for Unisys [redacted] and Unisys [redacted] Please see Schedule E for recent SSAE 16 audit reports for those sites. Additional information is in Schedule F, Section 3.1.1 "Multi Datacenter Environment (2+ Architecture)" item 6A.

8.B Offeror must provide proof of a valid (updated) SSAE16 certification in the form of audit findings report prior to implementing any Commonwealth service in any other proposed datacenter.

Please see Schedule E for copies of the current SSAE 16 audits for Unisys [redacted] data centers.

Continual Service Improvement

Unisys recognizes the significant importance of Quality and Continuous Service Improvement to:

- Reduce service risk,
- Improve service quality,
- Improve client satisfaction,

- Provide service transparency, and
- Improve/reduce costs of service.

Through a continuous cycle of evaluation and improvement within an IT infrastructure, Unisys views quality and continuous service improvement as a critical success factor in driving customer satisfaction for the Commonwealth IT infrastructure. Each of the continuous service improvement areas identified above are driven through the tight integration of the following organizations, industry tools, proven processes and quality deliverables:

- Service Excellence Office,
- Quality Plans: transition and steady state service delivery
- Industry standard frameworks and methodologies: ITIL, ISO, SSL
- Industry accepted measurement tools
- Continuous Service Improvement & Innovation Processes (CSIIP)
- Risk management, audits and business continuity management
- Client Satisfaction Surveys and Knowledge Management Portal

Collectively this represents Unisys Integrated Quality Plan for the Commonwealth of Pennsylvania.

Specifics on each of these areas are outlined in Schedule F, Section 3.2.1.1.6 Continuous Service Improvement. Highlights from this section are outlined below and requested service examples are provided at the end of this section.

9 CI Service Risk

9.A Offeror must provide methods to eliminate or mitigate service risks.

Risk management, independent quality audits, and business continuity management are integral quality management processes. Unisys is committed to managing risks and facilitating the achievement of business objectives, and the adherence to quality processes. We mitigate risk through the implementation of tight quality controls: standard policies, procedures, roles, risk assumptions, issues, and definitions, etc.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

10 CI Service Quality

10.A On a quarterly basis, Offeror must recommend to the Commonwealth team any facility changes that would be appropriate to maintained or improve SLA commitments.

The quality approach begins with the Service Excellence Office. The SEO function provides definition and oversight of all ITIL process management and analysis functions. Process managers and analysts working in the Service Excellence Office are responsible for auditing process effectiveness, ensuring that service delivery teams comply with proper execution of

processes, and analyzing process trends for anomalies. Continuous service improvement programs in collaboration with Commonwealth agencies are managed by the Service Excellence Office.

Through our Continuous Service Improvement and Innovation Process (CSIIP), the SEO reviews, analyzes and makes recommendations on improvement opportunities in each ITIL lifecycle phase. Unisys will leverage Six Sigma Lean tools and methodologies as well as ISO Certified internal audits to measure and maintain the highest quality services to the Commonwealth.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

11 CI Client Satisfaction

11.A Offeror must provide examples of previous Offeror initiatives aimed at continually improving client satisfaction.

Client satisfaction is extremely important to Unisys and a key focus in our IT solution. The SEO will integrate new agencies, customers and services into our multi-pronged client satisfaction approach that includes Service Desk surveys on the caller's experience, an overall agency satisfaction survey, and quarterly surveys with the Office of Administration. Data collection will be gathered across multiple levels to gain a clear understanding of the Commonwealth's satisfaction with the IT Services being provided.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

12 CI Service Transparancy

12.A Offeror must provide methods and practice to ensure service transparency, providing visibility into service execution.

The service organizations will use standardized ITSM services processes, IT monitoring and automation tools. ITSM processes will be documented in the Commonwealth Computing Procedures Manual (CCPM). The CCPM will be available to Commonwealth approved staff on the Knowledge Management Portal (KMP) providing desired transparency into service execution processes. Through the Real-time Dashboard, the Commonwealth will have access to current operational performance of their application infrastructure.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

13 CI Improve or Reduce Cost

13.A Offeror must provide examples of Facilities Management initiatives have been implemented or can be utilized to achieve reduced costs of Services and to meet or exceeded ROI (Return on Investment) analysis projections.

The Service Excellence Office will proactively manages quality, continuous service

improvement, ITIL process management, and customer satisfaction through a comprehensive quality plan that specifically addresses all of these areas. We believe this is a key differentiator in our partnership with the Commonwealth. Through this new organization and these quality plans, Unisys will drive best in class services and the highest customer satisfaction experience, while reducing overall costs to the Commonwealth.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

Unisys examples of continuous improvement

Examples of continuous service improvement have been included below under Unisys Team Experience.

Unisys Team Experience

Throughout the contract, Unisys has provided all facilities related maintenance and upkeep of the Commonwealth Data PowerHouse. In early 2011, Unisys undertook an internal initiative to be more "green". A complete analysis was performed and through numerous projects, we have reduced the overall Power Usage Effectiveness (PUE) rating from 1.8 to 1.5. Additionally, we had doubled the under floor pressure within the data center creating a more efficient airflow. There is also a current initiative for the replacement of the T-12 fluorescent lighting with the more energy efficient T-8 fluorescent lighting. While the IT energy load has increased with the addition of new hardware, our overall energy efficiency has improved.

Benefits to the Commonwealth

The Commonwealth benefits with Unisys oversight of its facilities by having an experienced company that makes its living keeping IT running. Failing to do so is like a bank failing to keep enough in the vaults – customers will not come back. Unisys has been operating Commonwealth facilities for 14 years and is now offering to place the Commonwealth in its own primary locations that benefit from the best and latest approaches that IT service providers provide to customers and that keeps them returning to solid, efficient, secure, flexible and scalable facilities that provide cost effective bases for our client's IT home.

3.2.3.2 Site Operations

The Site Operation service will provide datacenter operations staff and management to operate and monitor the IT computing equipment and Services being provided. The staff will interface with Commonwealth staff to institute best practice datacenter Services. Datacenter operations include, but are not limited to, management of the computing platforms, storage, local area networking, security firewall, tape backup, and offsite tape rotation systems.

Reference Documentation

Exhibit – D.7 - EDC Facility Summary

Exhibit G.6 - PSP - CJIS Security Policy

Exhibit G.9 - PSP – CCHRI

Exhibit G.7 - PSP - Summary of CJIS Requirements

Requirements		Describe Compliance
1.	Monitor and operate the various computer systems, network, network and local disk storage and firewall security systems. Provide datacenter operations staff to monitor the computer system platforms, associated disk systems, networking Services and firewall and security systems. Ensure proper equipment operations, timely batch jobs processing and appropriate response to any abnormal end and error conditions. The Offeror will support application specific operations as determined by the application owner. This includes executing the troubleshooting procedures required by the application owners as detailed within the CCPM. This may include operational activities and initial troubleshooting steps, contact and escalation lists (aka “Run Book”). This information will be maintained by the Offeror on an application by application basis and will be hosted within the Knowledge Management Portal. A daily operations batch schedule report will be created and used to log normal / abnormal conditions. Abnormal conditions will be investigated for problem	Offeror must describe its facilities site operations including monitoring and general upkeep of the facilities including the following: • Processes and Procedures • Tools / Applications • End User Reports o Standard o Custom • Escalation Procedures

	determination and rerun. Any abnormal condition that cannot be corrected will be referred to technical support staff for resolution. Properly clean and maintain equipment to minimize problems and outages, at intervals established with the Commonwealth or in compliance with stated and written specifications. Offeror must assess the EDC facilities and provide a report to the Commonwealth as it pertains to monitoring, maintaining and operating the installed infrastructure.	
2.	For the systems that utilize tape backup Services, Offeror must provide a structured tape management approach. For systems that utilize disk-2-disk backup approach Offeror must provide a structured disk-2-disk approach. Manage and maintain the tape backup system and Services. Rotate designated tapes to, and returned from approved offsite storage location. Maintain detailed audit log of tape movement. Some agency applications fall under additional CJIS and CCHRI security requirements for tape backups. Provide datacenter operations staff to manage and maintain the tape management system. Tapes will be rotated to, and returned from an approved offsite vaulting subcontractor. An automated software process will be utilized to report the completion status of backup processing, with electronic notification	Offeror must describe its tape management approach and describe the process to work with the Commonwealth Agencies to provide a classification and categorize tapes per the type of data contained on the tapes. Offeror must describe its disk-2-disk backup approach. Offeror must assess the EDC tape backup facilities and provide a report to the Commonwealth as it pertains to manage and operated the installed tape backup systems and media operations.

	of failures sent to Offeror technical support, and identified Commonwealth staff for follow up and corrective action. Provide the facilities to Retrieve External Storage Media from on-site and off-site storage as requested by the Commonwealth or as required in an emergency. Wipe or erase the data and configuration information resident on the media prior to disposal or re-use, and in accordance with Commonwealth standards. Dispose of retired media in an environmentally sound manner after purging any Commonwealth data using Commonwealth, and/or Federal guidelines/policies prior to disposing of media. Operate media libraries and library management systems as required to provide the Services. Maintain an existing inventory control system to properly manage External Storage Media in storage and prepare them for shipment to the contingency site.	
3.	Monitor physical access and security of the datacenter. Video surveillance is required. Staff the datacenter with appropriate level of staff and management 24/7/365. The Offeror must monitor physical access to the datacenter and respond to security incidents in a consistent and auditable manner. All breaches will be reported to the	Offeror must describe its physical access and security monitoring approach for proposed Offeror datacenters including staff roles, responsibilities and background check process. Offeror must assess the EDC current physical access and security plan and provide a report to the Commonwealth as it

	Commonwealth for review and follow up action as required. Monitoring of the video system for all entry points and throughout the datacenter and tape storage areas will be included in this responsibility. Offeror will be required to adhere to the Commonwealth requirements for background checks and security clearances. Commonwealth verification that the requirements have been met will be necessary prior to Offeror working on Commonwealth related systems.	pertains to any required upgrades.
4.	Manage and maintain equipment configuration inventory system. Provide staff to create and maintain a configuration record for all hardware and software components in the datacenter. This must be an accurate record of all software, computing, disk storage, tape, network, racking, cables, and environmental equipment.	Offeror must describe the proposed approach to managing the support of its datacenter technology.
5.	Provide programs and processes to alter the operational environment, and to refresh the Services at asset end-of-life or implementation of new technology Services, as these Services are needed.	Offeror must describe solution and approach to meet this requirement.
6.	Identify and create service objectives for the site operational Services in the form of SLAs, and report on the service availability, problems, and corrective actions on a monthly basis.	Offeror must describe how it monitors and manages facility operations to meet/exceed the agreed to availability service levels.
Continual Service Improvement		
7.	Reduce service risks.	Offeror must provide methods to eliminate

		or mitigate service risks.
8.	Improve service quality.	On a quarterly basis, Offeror must also recommend to the Commonwealth team any site operational changes that would be appropriate to maintained or improve SLA commitments.
9.	Improve client satisfaction.	Offeror must provide examples of previous Offeror initiatives aimed at continually improving client satisfaction.
10.	Ensure service transparency.	Offeror must provide methods and practices to ensure service transparency, providing visibility into service execution.
11.	Integrate Continuous Improvement Program processes into Availability Management and Service Level Management.	Offeror must describe offering in this area including the projected impacts/benefits.
12.	Improve/reduce cost of service.	Offeror must provide examples of Site Operations initiatives that have been implemented or can be utilized to achieve reduced costs of Services and to meet or exceeded ROI (Return on Investment) analysis projections.

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

Introduction

To support facilities site operations including monitoring and general upkeep of the facilities that support the computing platforms Unisys developed a component-based compute support model as depicted in **Figure 3.2.3.2-1.** This model provides the site operations model to support the requirements in the RFP and puts them in a logical view that the Commonwealth can easily visualize.

Figure 3.2.3.2-1 - Component Based Operating Model

The Component Based Operating Model is broken down into the following components to support the requirements within the RFP:

1. **Program Management Office –** Establish a local and dedicated Program Management and Service Excellence Office that provides a focus on governance, a drive toward continued value, and cost savings by deploying Lean Six Sigma practices based on studies of cycle time and defect analysis from events that are extracted from the IT Service Management platform. By removing cycle time waste and defects of the operating environment, Unisys will provide the Commonwealth with continued cost savings and a higher quality IT compute environment. This same office is responsible for the ongoing governance of driving continuous service improvement and innovation.

2. **Service Portal –** Create an enterprise services portal, enterprise services catalog, and real-time dashboard to provide a single interface to all agencies to interact, provision, and be able to determine the performance of the IT operating environment in near real time. Each agency will have its own personality that is configurable, being able to develop a look and feel of its own when coming to the services portal to provide each agency with personalization and autonomy. Each agency can determine the services it wants to publish or offer, provision, and report on, in near real-time, while still having access to the overall view of the enterprise.

3. **IT Service Management –** Deliver an enterprise IT Service Management platform based on ITIL V3 best practices and Lean Six Sigma that drives the maturity of the IT operating model with a goal of achieving an efficiency gain of approximately 5 percent year over year. Of significant importance is the development of an enterprise wide Configuration Management Database (CMDB) that defines the service that IT delivers to the Commonwealth. The creation of services in the CMDB will allow the Commonwealth to proactively determine business impact by determining a fault before it occurs and allowing maximum use of IT resources to reduce ongoing cost. Each agency will have its own instance in the service management environment to provide operating autonomy; Unisys will provide a federated service management environment to the OA so it has the overall view of the total IT operating environment at the Commonwealth. The Commonwealth can be comfortable knowing that Unisys supports a multitude of IT Service Management Systems, including [redacted] and [redacted] Our Component-based Operating model can be enabled with any one of the named IT Service Management Platforms.

4. **Managed Hosting Services and Capacity on Demand –** Enable an adaptive, flexible, and secure hardware compute environment that is based on a consumptive utility model with a "no volume commit" attribute that provides the agencies with the autonomy to perform their IT functions and meet their business requirements. In the Unisys compute model, there is fundamentally no difference between Managed Hosting Services and Capacity on Demand because they are served from the same hardware platforms and managed by the same ITSM management platform. As an innovation effort, and to make sure the Commonwealth is aligned with market trends, the Unisys Team includes optional Virtual Private Cloud offerings from Microsoft and [redacted] in the Enterprise Services Catalog. From Microsoft, we included Azure, Office 365, and Dynamics. From [redacted] we included its new offering in the marketplace for virtual private cloud capacity for Windows.

5. **Service Broker –** Unisys will provide the Commonwealth with a consolidated, optimized, and centralized multitenant compute environment in which the agencies will not have to compromise their control by being able to self-provision workloads using an Enterprise Services Catalog. Once ordered from the Enterprise Services Catalog, the request will be processed through ITSM for change approval. When the request is approved, the Service Broker will invoke an automated runbook to execute the provisioning effort. Once the provisioning effort is complete, the runbook will update the Configuration Management Database. Agencies will be able to maintain a very real level of control over their compute environment required to meet the business need. As an innovation effort, the Enterprise Services Catalog and Service Broker will be an integrated pair to provision not only capacity from the private cloud environment we are providing the Commonwealth, but also services from partners such as IBM, Microsoft, and [redacted] Our vision for the Enterprise Services Catalog and Service Broker is you can provision any service from any provider at anytime with "no commit" that is then managed by the Component Based Compute Model provided in this RFP. One provisioning model and one management model will unify the compute model for the Commonwealth and provide the business flexibility and optimized compute environment the Commonwealth is looking for.

6. **Technical Services –** Unisys will provide a set of selectable services that can be procured from the Enterprise Services Catalog to manage given applications in the Commonwealth agencies. These technical services can be people- or management-based services and can be procured in a consumption-based approach.

7. **Security Services –** Achieve and maintain a robust and comprehensive security

environment that meets the IT Security policies set forth by the Commonwealth. This security environment will be managed by Deloitte, which has years of experience working with the Commonwealth to create, implement, and manage security policies.

8. **Facility Management –** Provide the ongoing management for all data centers whether Unisys or Commonwealth owned facilities.

9. **Service Desk –** The Service Desk will take calls from IT support staff to log incidents that were not automatically generated from the event monitoring system. The Service Desk will use knowledge management to try to resolve an event within an agreed time. If the event cannot be resolved in the agreed time, it will be escalated to Level 1 Support. During normal business hours, this team will be located in Harrisburg.

10. **Level 1 Support –** Level 1 Support manages all events that are automatically generated from the hardware and application environments as well as resolving incidents that are received from the Service Desk. Level 1 will use various tools, runbooks, and knowledge management to resolve incidents. If the incident is not resolved within a given time, it will be escalated to Level 2 Support. During normal business hours, this team will be located in Harrisburg.

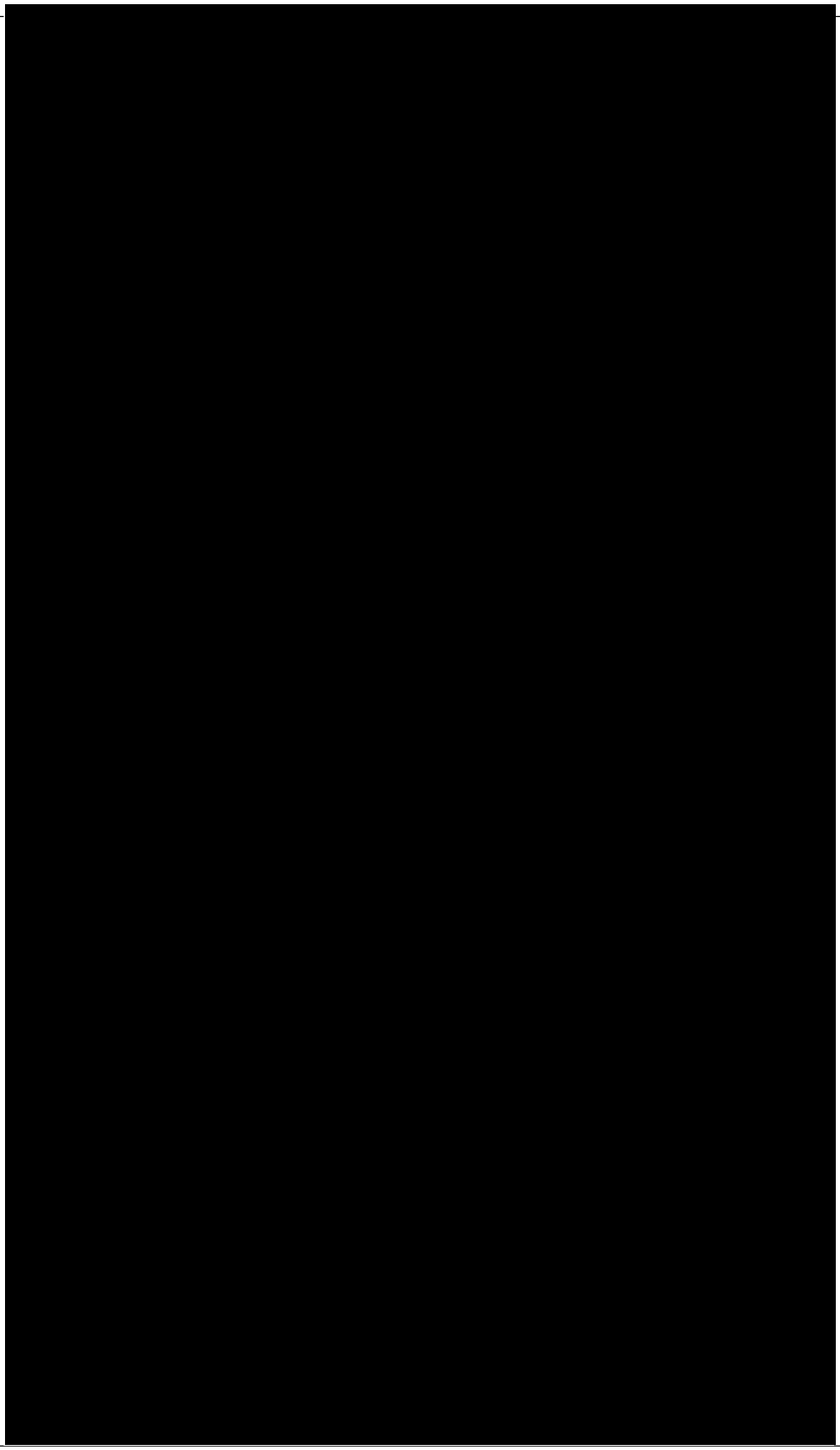
11. **Level 2 Support –** Level 2 Support is a team of very knowledgeable resources who can solve a wide array of Commonwealth application compute issues. This team largely knows the individuals in the agencies and has an ongoing relationship with them. When Level 2 Support believes it cannot resolve the incident in a timely way, it will pull in Level 3 Support resources. During normal business hours, this team will be located in Harrisburg.

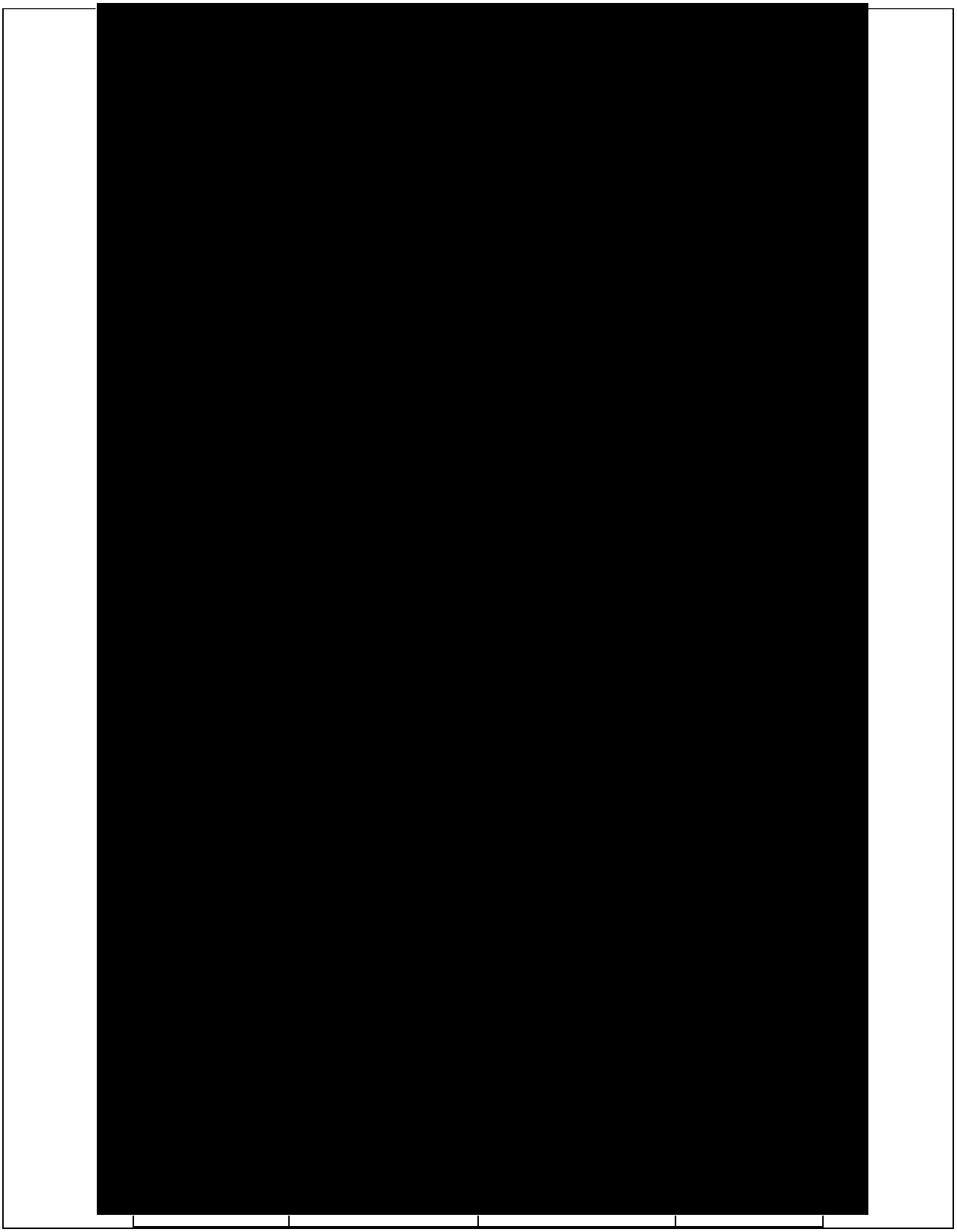
12. **Level 3 Support –** Level 3 Support is a team of architecture experts that deeply understands the compute architecture that supports the Commonwealth applications. This team is also an integral part of driving continuous improvement plan by identifying inefficiencies in the compute architecture. During normal business hours, this team will be located in Harrisburg.

To enable this Component Based Operating Model Unisys plans to implements, operate, and support a comprehensive and integrated Information Technology Service Management (ITSM) platform based on ITIL V3 and Enterprise Systems Management (ESM) platform dedicated to the cross-functional process support for services provided to the Commonwealth for this contract. The proposed ITSM and ESM Architecture, shown in **Figure 3.2.3.2-2**, provides an effective and efficient operational platform to support the Commonwealth's agencies application environments.

Figure 3.2.3.2-2 - Unisys ITSM and ESM Integrated Architecture.

To enable the Component Based Operations Model it takes a great number of tools that are seamlessly integrated as a whole. These tools are summarized below in the **Figure 3.2.3.2-3.**





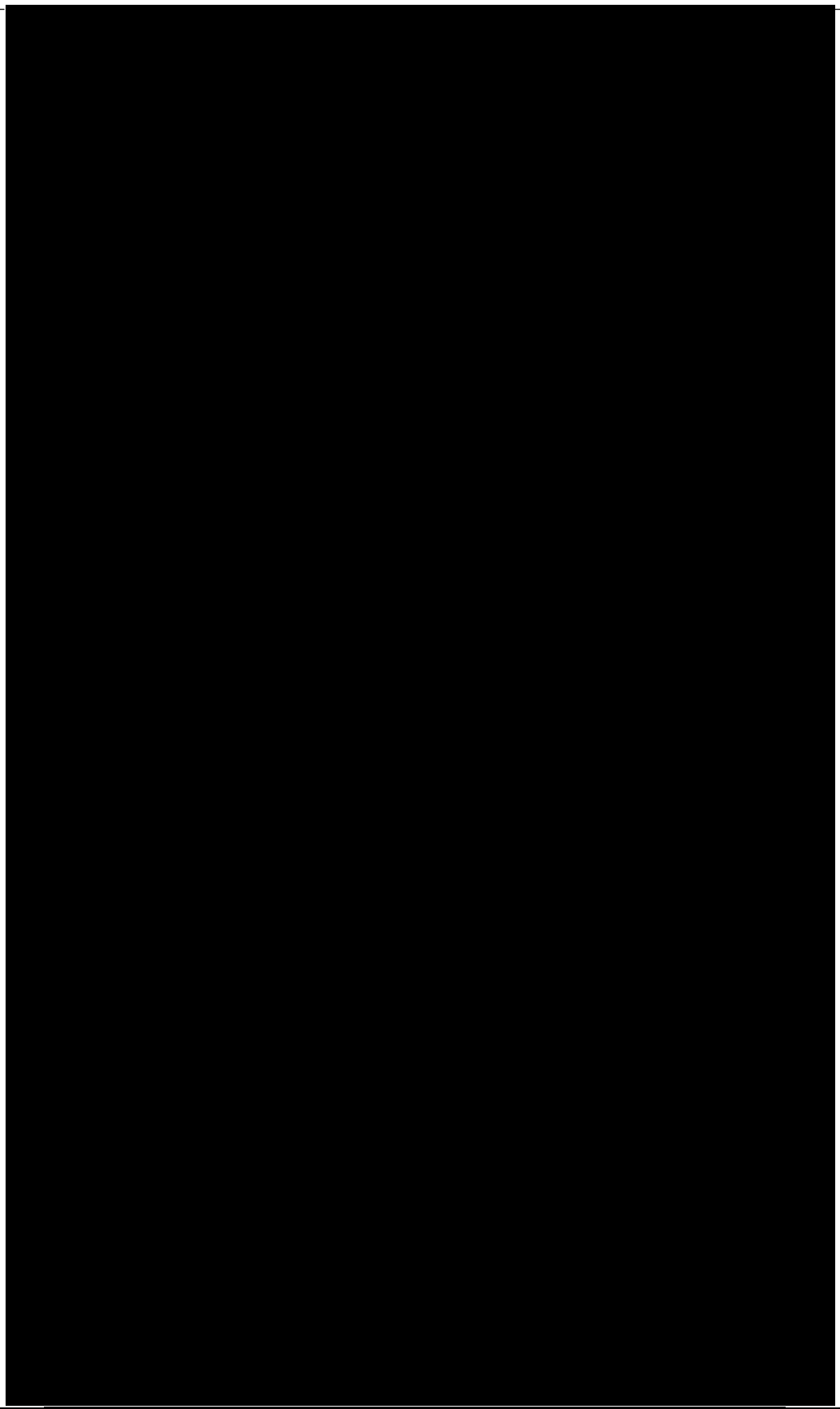


Figure 3.2.3.2-3 - Unisys ITSM and ESM Tools

1 Site Operations and Maintenance

1.A Monitor and operate the various computer systems, network, network and local disk storage and firewall security systems.

See the overview in the introduction provided above for an explanation on providing monitoring and operation to support the computing platforms required in this RFP. For detailed information on each platform refer to each compute platform section for an in depth explanation of how they will be monitored and operated.

1.B Provide datacenter operations staff to monitor the computer system platforms, associated disk systems, networking Services and firewall and security systems

The Unisys Team will provide an operations staff that is largely located in the primarily support center in Harrisburg, PA; however to support all computing facilities and off hours business support Unisys will have a small amount of supplemental support staff located in [redacted]

1.C Ensure proper equipment operations, timely batch jobs processing and appropriate response to any abnormal end and error conditions.

The Unisys Service Delivery Team verifies proper equipment operations. The Unisys Service Delivery Team confirms timely batch job processing and response to abnormal error conditions. Any abnormal end and error condition will generate an event in the event management system and will automatically generate an incident ticket that the operations staff will receive address and resolve.

1.D The Offeror will support application specific operations as determined by the application owner. This includes executing the troubleshooting procedures required by the application owners as detailed within the CCPM. This may include operational activities and initial troubleshooting steps, contact and escalation lists (aka "Run Book").

The Unisys Service Delivery Team will have an extensive set of run books to support the infrastructure for application owners. During transition, these run books will be augmented with run books reviewed and approved from the Commonwealth and will be stored in the Knowledge Management Portal (KMP) CCPM procedures and run books. These runbooks will be available within the KMP that is located within the Services Portal.

1.E This information will be maintained by the Offeror on an application by application basis and will be hosted within the Knowledge Management Portal.

Unisys complies. See 1.D above.

1.F A daily operations batch schedule report will be created and used to log normal / abnormal conditions

Unisys will create a daily operations batch schedule report that logs normal/abnormal conditions with a focus on exceptions.

1.G Abnormal conditions will be investigated for problem determination and rerun. Any abnormal condition that cannot be corrected will be referred to technical support staff for resolution.

Abnormal error conditions in batch jobs will be investigated, workarounds determined and rerun. Incident tickets will be opened following the incident management process to determine a resolution and eliminate defects from the batch job.

1.H Properly clean and maintain equipment to minimize problems and outages, at intervals established with the Commonwealth or in compliance with stated and written specifications

The Unisys Service Delivery Team defines and executes preventative maintenance for all supported facilities and infrastructure. These preventative maintenance procedures will be reviewed and approved during Transition and stored in the CCPM on the KMP.

1.I Offeror must assess the [redacted] facilities and provide a report to the Commonwealth as it pertains to monitoring, maintaining and operating the installed infrastructure.

Unisys complies. Refer to Schedule F, Section 3.1.1 "Multi Datacenter Environment (2+ Architecture)" and Section 3.2.3.1 "Facilities Management" for more information.

1.J Offeror must describe its facilities site operations including monitoring and general upkeep of the facilities including the following:

Processes and Procedures

Please refer to the introduction this section above for an explanation on facilities site operations.

Tools / Applications

The tools for site operations are provided in the introduction section above.

End User Reports (Standard and Custom)

Standard End user Reports are summarized in Section 3.3.2 Standard Reports. Custom reports are available via the Enterprise Services Catalog.

Escalation Procedures

Escalation Procedures are described in the Incident Management Process, which can be found in detail in the Service Desk section 3.2.1.4 of this document.

2 Structured Tape Management Approach

2.A For the systems that utilize tape backup Services, Offeror must provide a structured tape management approach.

The media management function provides a structured tape management approach for all systems that utilize tape backup services. This function manages and maintains the tape backup system and services rotating designated tapes to and from approved off-site storage locations tracking all tape movement in a detailed audit log. Practices under this function meet CJIS and CCHRI security requirements for media management and proper disposal.

Based on the differing operating environments supported there will be various software used in the Tape Management areas. These differing operating environments include:

- Unisys IX Mainframe
- Unisys NX Mainframe
- IBM Mainframe
- Open Systems

Management and maintaining of the tape backup system is a key factor in the overall availability and recoverability of any given environment. Working with the individual agencies, tape library staff establish retention periods for the given tape media based on the cycle of the backup being created. All movement of media to the approved offsite storage location is electronically documented in the software associated with the operating environment and with the approved offsite vendor. All media identified for shipment to the approved offsite storage location is picked based on the automated software, scanned and packaged in separate agency containers. Agency applications that fall under additional CJIS, CCHRI and IRS security requirements are loaded and secured in locked containers.

The media management team provides professional handling of all Commonwealth data residing on tape media. Media Management responsibilities include:

- Through a structured tape management approach, media is inventoried and prepared for shipment off-site to a secure storage vault where can be accessed in the event of a facility disaster
- Management and maintenance of the tape backup system and Services
- Rotation of designated tapes to, and from approved offsite storage location maintaining a detailed audit log of tape movement
- Wiping or erasing the data and configuration information resident on the media prior to disposal or re-use, and in accordance with Commonwealth standards
- Disposal of retired media in an environmentally sound manner after purging any Commonwealth data using Commonwealth, and/or Federal guidelines/policies prior to disposing of media

- Maintaining an existing inventory control system to properly manage External Storage Media in storage and prepare them for shipment to the contingency site.

Standard scheduled rotation of tape media occurs daily.

2.B For systems that utilize disk-2-disk backup approach Offeror must provide a structured disk-2-disk approach.

The Unisys solution includes the [redacted] infrastructure that has worked well for the Commonwealth since Unisys brought forward this innovation as part of the existing service design process. The Commonwealth agencies order capacity via the Enterprise Services Catalog, which initiates the provisioning processes.

2.C Manage and maintain the tape backup system and Services. Rotate designated tapes to, and returned from approved offsite storage location.

As described above in 2.A rotations occur daily and comply with Commonwealth requirements.

2.D Maintain detailed audit log of tape movement. Some agency applications fall under additional CJIS and CCHRI security requirements for tape backups.

The Unisys solution provides for physical encryption of all media and includes detailed audits of tape movement from Unisys-managed data centers to the [redacted] facilities which provide offsite storage in the Unisys solution. These Unisys tape movement logs are compared with the [redacted] receipt logs for tape media movement as part of the detailed audit process.

2.E Provide datacenter operations staff to manage and maintain the tape management system. Tapes will be rotated to, and returned from an approved offsite vaulting subcontractor. An automated software process will be utilized to report the completion status of backup processing, with electronic notification of failures sent to Offeror technical support, and identified Commonwealth staff for follow up and corrective action.

Unisys complies. The [redacted] software manages the reporting of completion status of backup processing. The [redacted] is integrated with the [redacted] in the IT Service Management (ITSM) infrastructure to provide automated escalation processes including, as desired by the Commonwealth, notification to Commonwealth staff. Unisys IT Service Management will also manage direct escalation to Commonwealth technical staff when required for resolution of incidents.

2.F Provide the facilities to Retrieve External Storage Media from on-site and off-site storage as requested by the Commonwealth or as required in an emergency.

As and when restores are required, detailed processes and procedures will be defined in CCPM to request and retrieve media. The ITSM team also manages to emergency requirements using processes agreed upon with the Commonwealth.

2.G Wipe or erase the data and configuration information resident on the media prior to disposal or re-use, and in accordance with Commonwealth standards.

As described above in 2.A, the Media Management team manages re-use of media or degaussing and media disposal as required.

2.H Dispose of retired media in an environmentally sound manner after purging any Commonwealth data using Commonwealth, and/or Federal guidelines/policies prior to disposing of media.

The Unisys solution includes degaussing equipment to purge data and destroy media prior to disposal following environmentally sound processes. Agencies may request additional security precautions for tapes containing highly sensitive data. These measures include overwriting all areas on the tape - three times, or degaussing. These measures will be documented and noted on the inventory sheet when the tape is placed in the box. The wiping of tape media prior to re-use is handled with the use of a DOD rated tape degausser.

2.I Operate media libraries and library management systems as required to provide the Services.

Unisys complies.

2.J Maintain an existing inventory control system to properly manage External Storage Media in storage and prepare them for shipment to the contingency site.

The Unisys Team requires no additional transition efforts to manage the existing inventory and can prepare them for shipment to contingency sites as determined during data gathering activity.

2.K Offeror must describe its tape management approach and describe the process to work with the Commonwealth Agencies to provide a classification and categorize tapes per the type of data contained on the tapes.

The Unisys Team provides these tape management approaches for the current Commonwealth and proposes to rely on these processes within this new solution's Service Design. Additional specifics are included in 2.A through 2.K above. Agencies may request additional security precautions for tapes containing highly sensitive data.

2.L Offeror must describe its disk-2-disk backup approach.

As described above, the Unisys solution includes the proven [redacted] infrastructure that has worked well for the Commonwealth since Unisys brought forward this innovation as part of the existing Service Design process.

In the new Capacity-on-Demand solution, the Commonwealth agencies order capacity via the Enterprise Services Catalog, which initiates the provisioning processes.

2.M Offeror must assess the [redacted] tape backup facilities and provide a report to the Commonwealth as it pertains to manage and operated the installed tape backup systems and media operations

The Unisys Team can provide this assessment and report within the first 12 months.

3 Monitor, Physical Access and Security Monitoring Approach

The Unisys facilities used in this configuration will be staffed with on-site personnel 24 hours a day seven days a week who monitors physical access and security of the data center. Each site has its own complement of physical security guards who make regular premises rounds, log their inspections, and escort all data center visitors. This team will monitor physical access to the data center and respond to security incidents in a consistent and auditable manner. All breaches will be reported to the Commonwealth for review and follow up action as required. Monitoring of the video system for all entry points and throughout the data center and tape storage areas is included in this responsibility.

3.A Monitor physical access and security of the datacenter. Video surveillance is required.

Video surveillance includes both exterior and interior surveillance at all Unisys-managed facilities. For more detailed information please refer to Schedule F, Section 3.1.1 "Multi Datacenter Environment (2+ Architecture)".

3.B Staff the datacenter with appropriate level of staff and management 24/7/365.

The Unisys solution includes the staff to meet this requirement. Details are provided in the overall Staffing Plan in Section 5 Personnel.

3.C The Offeror must monitor physical access to the datacenter and respond to security incidents in a consistent and auditable manner. All breaches will be reported to the Commonwealth for review and follow up action as required. Monitoring of the video system for all entry points and throughout the datacenter and tape storage areas will be included in this responsibility.

The Unisys Team will continue to comply with this requirement.

3.D Offeror will be required to adhere to the Commonwealth requirements for background checks and security clearances. Commonwealth verification that the requirements have been met will be necessary prior to Offeror working on Commonwealth related systems.

All Unisys staff who has physical or logical access to the data center will adhere to the Commonwealth ITBs related to background checks and security clearances. This includes initial checks prior to hire as well as annual checks. Documentation related to the background checks will be shared with the Commonwealth to enable verification prior to staff working on Commonwealth systems.

3.E Offeror must describe its physical access and security monitoring approach for proposed Offeror datacenters including staff roles, responsibilities and background check process.

The Unisys Team will continue to comply with this requirement by providing interior and

exterior video surveillance for Unisys-managed facilities. The Unisys Security Manager in the Program Management Office oversees the implementation of background check, security policies, and appropriate security audit processes to manage staff security.

For more details, see Schedule F, Section 3.5.4.7 "Security Management Plan".

3.F Offeror must assess the [redacted] current physical access and security plan and provide a report to the Commonwealth as it pertains to any required upgrades.

The Unisys Team can provide this assessment and report within the first 12 months.

4. Datacenter Configuration Management

4.A Manage and maintain equipment configuration inventory system.

Please refer to 4.B below. All components in the data center will be stored in the Unisys ITSM Configuration Management Database and will be marked as an asset.

4.B Provide staff to create and maintain a configuration record for all hardware and software components in the datacenter. This must be an accurate record of all software, computing, disk storage, tape, network, racking, cables, and environmental equipment.

The Unisys solution includes the [redacted] software solution from [redacted], a sophisticated Software as a Service (SaaS) solution for modeling critical data center physical infrastructure. With a data-driven model behind its powerful graphical capabilities, it effectively addresses the important issues of people, power, and space that occur in managing IT infrastructure.

The Unisys Team has supplemented this sophisticated tracking, monitoring, and reporting software suite with an integrated system of hand-held devices that allow scans of racks of hardware components for auditing, inputting, and reporting. The tool is also integrated with the Microsoft Visio product so that the Commonwealth will have access to sophisticated and detailed data center Visio drawings generated automatically from these scans. Other vendors might not include this feature but promise to provide staff to produce these artifacts. Sadly, under this approach, it is nearly impossible to hire enough staff to compete with the Unisys automation and thus the alternate labor-based proposals are vastly inferior.

4.C Offeror must describe the proposed approach to managing the support of its datacenter technology.

The Unisys solution manages data center support within the Infrastructure Architecture Services framework as described in Schedule F, Section 3.2.2.2 "Infrastructure Architecture". This approach includes lifecycle management of facilities infrastructure and capacity.

5. Datacenter Upgrade and New Technology Approach

5.A Provide programs and processes to alter the operational environment, and to refresh the Services at asset end-of-life or implementation of new technology Services, as these Services are needed.

The Unisys solution manages data center upgrades and new technologies through ITIL V3 processes within Service Design, which manage new services and changes to services to meet

the Commonwealth's strategy to improve services and cost efficiencies. The Service Design process describes in Schedule F, Section 3.2.1.5 "Technical Architecture" also manages the requirements and capacity needed within the Infrastructure Architecture Services framework as described in Schedule F, Section 3.2.2.2 "Infrastructure Architecture".

This approach includes lifecycle management of facilities infrastructure and capacity.

5.B Offeror must describe solution and approach to meet this requirement.

As described above, Unisys follows ITIL V3-based processes to manage data center upgrades and new technologies as part of service design to improve operations with new technology or to introduce new services. Using the standard ITIL V3 service design process, Unisys adds a requirement of continual service improvement to drive a more active approach to continual improvements.

6. Monitor, Facility Operations Monitoring Approach

6.A Identify and create service objectives for the site operational Services in the form of SLAs, and report on the service availability, problems, and corrective actions on a monthly basis.

The Unisys solution provides Facilities Operations and Monitoring to support the Application Infrastructure Availability SLAs specified by the Commonwealth and includes monthly reporting to support the SLA achievements.

6.B Offeror must describe how it monitors and manages facility operations to meet/exceed the agreed to availability service levels.

The [redacted] solution described in Section 5 includes monitoring and management of facilities operations and components and is integrated within the [redacted] collectors and incident/escalation processes in order to meet/exceed the agreed to availability service levels.

Continual Service Improvement

Unisys recognizes the significant importance of Quality and Continuous Service Improvement to:

- Reduce service risk,
- Improve service quality,
- Improve client satisfaction,
- Provide service transparency, and
- Improve/reduce costs of service.

Through a continuous cycle of evaluation and improvement within an IT infrastructure, Unisys views quality and continuous service improvement as a critical success factor in driving customer satisfaction for the Commonwealth IT infrastructure. Each of the continuous service improvement areas identified above are driven through the tight integration of the following organizations, industry tools, proven processes and quality deliverables:

- Service Excellence Office,
- Quality Plans: transition and steady state service delivery
- Industry standard frameworks and methodologies: ITIL, ISO, SSL

- Industry accepted measurement tools
- Continuous Service Improvement & Innovation Processes (CSIIP)
- Risk management, audits and business continuity management
- Client Satisfaction Surveys and Knowledge Management Portal

Collectively this represents Unisys Integrated Quality Plan for the Commonwealth of Pennsylvania.

Specifics on each of these areas are outlined in Schedule F, Section 3.2.1.1.6Continuous Service Improvement. Highlights from this section are outlined below and requested service examples are provided at the end of this section.

7 CI Service Risk

7.A Offeror must provide methods to eliminate or mitigate service risks.

Risk management, independent quality audits, and business continuity management are integral quality management processes. Unisys is committed to managing risks and facilitating the achievement of business objectives to adhere to quality processes. We mitigate risk through the implementation of tight quality controls: standard policies, procedures, roles, risk assumptions, issues, and definitions, etc.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

8 CI Service Quality

8.A On a quarterly basis, Offeror must also recommend to the Commonwealth team any site operational changes that would be appropriate to maintained or improve SLA commitments.

The quality approach begins with the Service Excellence Office. The SEO function provides definition and oversight of all ITIL process management and analysis functions. Process managers and analysts working in the Service Excellence Office are responsible for auditing process effectiveness, ensuring that service delivery teams comply with proper execution of processes, and analyzing process trends for anomalies. Continuous service improvement programs in collaboration with Commonwealth agencies are managed by the Service Excellence Office.

Through our Continuous Service Improvement and Innovation Process (CSIIP), the SEO reviews, analyzes and makes recommendations on improvement opportunities in each ITIL lifecycle phase. Unisys will leverage Six Sigma Lean tools and methodologies as well as ISO Certified internal audits to measure and maintain the highest quality services to the Commonwealth.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

9 CI Client Satisfaction

9.A Offeror must provide examples of previous Offeror initiatives aimed at continually improving client satisfaction.

Client satisfaction is extremely important to Unisys and a key focus in our IT solution. The SEO will integrate new agencies, customers and services into our multi-pronged client satisfaction approach that includes Service Desk surveys on the caller's experience, an overall agency satisfaction survey, and quarterly surveys with the Office of Administration. Data collection will be gathered across multiple levels to gain a clear understanding of the Commonwealth's satisfaction with the IT Services being provided.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

10 CI Service Transparency

10.A Offeror must provide methods and practices to ensure service transparency, providing visibility into service execution.

The service organizations will use standardized ITSM services processes, IT monitoring and automation tools. ITSM processes will be documented in the Commonwealth Computing Procedures Manual (CCPM). The CCPM will be available to Commonwealth approved staff on the Knowledge Management Portal (KMP) providing desired transparency into service execution processes. Through the Real-time Dashboard, the Commonwealth will have access to current operational performance of their application infrastructure.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

11 Integration, CI Service Integration into Availability Management

11.A Offeror must describe offering in this area including the projected impacts/benefits.

Service will be sustained by integrating any new agencies, customers, or services into our standard operational and quality processes and methodologies leveraging ITIL processes. This includes creating quality project plans, utilizing industry accepted measurement and monitoring tools, analyzing trending reports and providing proactive continuous service improvement throughout the IT lifecycle. This will enable new Commonwealth services to experience and sustain IT services and client satisfaction.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

12 CI Improve or Reduce Cost

12.A Offeror must provide examples of Site Operations initiatives that have been implemented or can be utilized to achieve reduced costs of Services and to meet or exceeded ROI (Return on Investment) analysis projections.

The Service Excellence Office will proactively manages quality, continuous service improvement, ITIL process management, and customer satisfaction through a comprehensive

quality plan that specifically addresses all of these areas. We believe this is a key differentiator in our partnership with the Commonwealth. Through this new organization and these quality plans, Unisys will drive best in class services and the highest customer satisfaction experience, while reducing overall costs to the Commonwealth.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

Unisys examples of continuous improvement

Examples of continuous service improvement have been included below under Unisys Team Experience.

Unisys Team Experience

Data Center

Throughout the contract, Unisys has provided all facilities related maintenance and upkeep of the Commonwealth Data PowerHouse. In early 2011, Unisys undertook an internal initiative to be more "green". A complete analysis was performed and through numerous projects where we have reduced the overall Power Usage Effectiveness (PUE) rating from 1.8 to 1.5. Additionally, we had doubled the under floor pressure within the data center creating a more efficient airflow. There is also a current initiative for the replacement of the T-12 fluorescent lighting with the more energy efficient T-8 fluorescent lighting. While the IT energy load has increased with the addition of new hardware, our overall energy efficiency has improved.

Unisys Facility Environmental Management

Unisys is committed to Responsible Environmental Management. At Unisys, we believe we must take a proactive role in maintaining a safe and healthy workplace, operating our facilities in an environmentally sound manner, and promoting programs that support environmental stewards. It means conducting business in a responsible manner, with respect and concern for the environment. It is a matter of strictly adhering to local, national, and international laws governing environmental protection and offering environmentally responsible products. On a regular basis, regulatory compliance validation reviews are performed at Unisys locations to evaluate conformity with country-specific environmental regulations and established Unisys best practices. Third party assessments are performed independent of internal reviews to add objectivity to the evaluation process. Unisys has not received a notice of violation or a fine for non-compliance of environmentally related matters in the past three or more years. To foster this commitment, Unisys has assembled a staff of qualified professionals possessing extensive experience. These skilled professionals are responsible for identifying and resolving environmental, safety, and health issues in a timely, cost-effective and technically sound manner. Environmental Programs that Unisys currently manages are:

- ISO 14001 Environmental Management Systems
- Carbon Footprint
- Pollution Prevention
  - Solid Waste Recycling
- Vital Resource Conservation

- Energy Conservation
- Green Lights Partner
- End of Life Product Disposition Program
- Product reuse and recycling programs
- Lithium Batteries Recycling Program
- Printer cartridge recycle program
- Environmentally safe packaging
- Clean Air Program
- Travel Reduction
- Ozone Depleting Substances (ODS) Management
- Design for the Environment Product Program
- Supply Chain Information
- Environmentally-Safe Packaging
- Community Commitments & Concerns
- Employee Health and Safety
- Health and Safety Program Management
- Management of Injuries and Illnesses
- Hardware Dismantling and Selective Treatment
- WEEE-Compliant Instructions for Hardware Disassembly
- **Environmental Recognitions and Awards**
  - Unisys Mission Viejo facility was selected by the State of California as one of the winners of the "Flex Your Power Energy Award" for exceptional leadership and contributions to promoting energy conservation. In addition, the Mission Viejo site received certificates of appreciation from the South Coast Air Quality Management District (SCAQMD) for achieving the On Road Motor Vehicle Mitigation Options Emission Reduction Target.
  - In 2009, Unisys was named in the Black Book of Outsourcing as one of the top 50 "green" outsourcing providers in the world
  - Honored at the 2008 Computerworld Green IT Symposium in Washington, D.C. as one of the top five companies in the category of Green IT facilities for the Unisys Data Center in [redacted] Minnesota.

Benefits to the Commonwealth

The Unisys Team's expansive experience managing data centers globally will continue to reduce costs of data center management for the Commonwealth. Unisys applies the same standardization of ITIL V3 services processes to managing data centers within the Infrastructure Architecture framework as Unisys does for all components within the data center. This standardization of management process across all Unisys Managed facilities

depicted in **Figure 3.2.3.2-4** below means that when data center management innovations are refined in, say, Sydney, Australia, the new service practice comes before the Unisys/Commonwealth Service Design reviews to explain and implement the benefits for the Commonwealth.

Figure 3.2.3.2-4 - Unisys Managed Data Centers

The Unisys Team reduces the risks that other vendors will bring to the transition. The Unisys Team has deep expertise in delivering services and support to critical Commonwealth applications. The Unisys Team will utilize this expertise to provide recommendations on data center locations for infrastructure architecture componentry.

The Unisys Team further reduces transition risks because we clearly understand that transition requires moving your applications and data not simply replacing hardware and shuffling people. The Unisys Team has already has conducted 2 major and very successful transitions in the last 12 years. This deep knowledge will be invaluable to the Commonwealth and the Office of Administration as individual Agencies seek expertise guidance in transition and migration.

3.2.4 Managed Hosting Services

For all Managed Hosting Services, the Offeror must actively monitor the daily operations of the infrastructure used to provide the services. The Offeror must execute the troubleshooting procedures required by the application owners as detailed within the CCPM. This may include operational activities and initial troubleshooting steps, contact and escalation lists (aka “Run Book”). This information will be maintained by the Offeror on an application by application basis and will be hosted within the Knowledge Management Portal.

3.2.4.1 Windows Support

This service will provide hosting, operations and support Services for Microsoft Windows based servers (physical and virtual) located at the central datacenters. Offeror must support various hardware systems and various versions of the Microsoft operating systems, and support service software. The Offeror must provide support for both physical and virtual servers. Currently the Commonwealth utilizes virtualization technology from [redacted] and Microsoft's Hyper-V. See attached Exhibits for hardware and software details. The number and level of support staff members required to perform the below listed tasks will be determined by the Offeror, based on number of Commonwealth clients, hardware, software, and operating systems being serviced.

Listed below are the basic Services required, but not inclusive of all Services needed, to manage an enterprise class datacenter required by the Commonwealth. Offeror must include these Services within the base level of Services in this Offering. Change requests will be approved and authorized using the change management process.

Reference Documentation

Exhibit B.1 – DPH - Asset List

Exhibit B.2 - Commonwealth Owned DPH IT Assets

Exhibit C.1 – DPW - Room 105 and CAO Servers – Storage

Exhibit D.1 - [redacted] - Server Inventory

Exhibit D.2 - [redacted] - Switch Summary

Exhibit D.3 - [redacted] - Storage Summary

Exhibit D.5 – [redacted] - DOT Datacenter Inventory

Exhibit E.1 - DLI - Datacenter Inventory Template

Exhibit F.1 - DOH - Datacenter Inventory

Exhibit F.2 - DOH - DPH Asset List

Exhibit F.3 - DOH - DPH COPA Software Asset IBM

Exhibit F.4 – DOH – Physical Servers

Exhibit G.1 - PSP - Datacenter HW Inventory

Exhibit G.3 - PSP - DPH Asset List

Exhibit H.1 - DOR - Datacenter Inventory

Exhibit H.2 - DOR - DPH Asset List

Exhibit H.4 - DOR - SAP TRM System

Exhibit I.1 - IES - DPH COPA Owned IT Assets

Requirements		Describe Compliance

1.	Monitor local operations, troubleshoot and resolve operational issues.
	
	Actively monitor the daily operations of all MS Windows servers. Maintain a log for each server detailing hardware / software configuration and critical service operations. Document review of the system logs on a weekly basis to ensure critical system Services are processing without errors. Complete weekly server log indicating which logs were reviewed, date and initial the log.
		Offeror must describe its approach to supporting Windows based server environment including the following:
		
		• Processes and Procedures
		• Tools / Applications
		• End User Reports
		  o Standard
		  o Custom
		• Tiered Service/Support Levels
		• Escalation Procedures

2.	Monitor system backup processing on a daily basis. Review daily backup log for successful completion. Note failures, and correct the problems. Create problem record for any abnormal condition and any repairs that have been made, re-execute as appropriate. An automated software process will be utilized to report the completion status of backup processing, with electronic notification of failures sent to Offeror technical support, and identified Commonwealth staff for follow up and corrective action.	Offeror must describe its approach to performing an initial review and audit of the backup policies, procedures and reports, to ensure the accuracy of the backup schedules, retention periods, target directories, and recovery point objectives. Offeror must describe its approach to identify gaps and potential risks, and how those gaps and risks will be resolved. Offeror must describe how the authorized Commonwealth users will have online access to backup logs.
3.	Provide Microsoft Hyper-V and [redacted] trained staff holding manufacturer recognized certifications for hardware and software technical support. Post award; provide the Commonwealth a resume or CV for each operational staff member	Offeror must submit a representative sample of staff resumes typically provided for these positions detailing their experience, education, and certifications.

	assigned to this engagement. A copy will be maintained on Offeror file including verified background clearances as required.	
4.	Provide cost effective operational and technical support for the Windows computing platform. Provide platform level operational and technical support for the computing platform. Provide Level 2 and Level 3 Support to the Service Desk and/or Commonwealth Users. Provide a tiered level of support Services (e.g. Gold, Silver, and Bronze). Provide technical advice and support to the Application Development and Maintenance (ADM) and Database Administration (DBA) staffs, as required. Post award; provide Commonwealth with a resume or CV for each operational staff member assigned to this engagement. A copy will be maintained on Offeror file.	Offeror must describe its approach to providing and maintaining different tiered levels (i.e. Level 2 & Level 3 Technical Support) of support. Offeror must provide a representative sample of available tiered service support Services.
5.	Ensure network connectivity and consistent system response times. Utilize automated system management tool(s) to ensure real- time monitoring and notification of server availability and response times. Stop / Start times of servers will be a source of input for SLA measurements. Identify tool set(s).	Offeror must describe its real-time monitoring approach and its toolset for providing and maintaining network availability and performance. Offeror must identify tools it uses to support network availability and performance.
6.	Ensure server operating systems are	Offeror must describe its approach to patch

	maintained with the current patch level, based on the Services provided by the server. Analyze monthly service patches and determine which need to be applied, by server type. Create a change record, log the update in the server log, install based on server maintenance schedule and update the server configuration record. Notify impacted Commonwealth users immediately of any unscheduled service interruptions via email/web. The Offeror must be document normal work hours and holiday schedules with each agency to determine the contact method and escalation process of each Commonwealth agency.	management. Offeror must identify tools it uses to manage system patches. Offeror must describe its approach to testing and validating updates to the OS and 3rd Party software that it supports. Offeror must describe its approach to communicate unscheduled and scheduled outages, including escalation process.
7.	Provide a review and analysis of system performance/capacity to determine if current performance/capacities are sufficient to support the needs of the stakeholders.	Offeror must perform an initial review and audit of the current usage, procedures and reports and provide an analysis of the current usage, processes and reports currently being supported. Offeror must document its review and audit findings and recommendations.
8.	User Account Management - Provide certified operating system administration staff to create and maintain the registration of profiles, associated groups, and the security permissions required to service the approved client base of the operating systems.	Offeror must describe its approach to managing user accounts.
9.	Procurement Planning Provide program and processes to refresh the hardware at asset end-of-life, and as upgrades are needed to	Offeror must describe its programs and processes for procuring new or upgraded systems.

	meet anticipated growth in utilization.	
10.	SLA Reporting Collect actual system availability, utilization and response time data. On a monthly basis, Offeror must create a Service Level Agreement report for the Commonwealth team.	Offeror must describe processes and toolsets it uses for monitoring and maintaining service levels. Offeror must provide a representative sample of an SLA report.
11.	Installation of Windows updates/patches must be coordinated by Agency. For IES, windows version upgrades must be SAP certified. Coordinate at an agency level and account for any required patching as technology upgrades require.	Offeror must describe its programs and processes for applying system updates/patches.
12.	The Offeror must provide Software License Management.	Offeror must describe solution and approach to meet this requirement.
Continual Service Improvement		
13.	Reduce service risks.	Offeror must provide methods to eliminate or mitigate service risks.
14.	Improve service quality.	On a quarterly basis, Offeror must also recommend to the Commonwealth team any system changes that would be appropriate to maintain or improve SLA commitments.
15.	Improve client satisfaction.	Offeror must provide examples of previous Offeror initiatives aimed at continually improving client satisfaction.
16.	Ensure service transparency.	Offeror must provide methods and practices to ensure service transparency, providing visibility into service execution.
17.	Improve/reduce cost of service.	Offeror must provide examples of Windows Support initiatives that have been implemented or can be utilized to achieve reduced costs of Services and to meet or

		exceeded ROI (Return on Investment) analysis projections.

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

Introduction

Windows is a key server platform for the Commonwealth of Pennsylvania's application hosting platform. With the aggressive move to standardization and virtualization the Commonwealth lays out in the Volumetrics tab of Schedule I, it's clear that Windows as both a physical and virtual platform will continue to be an important part of the Commonwealth's application strategy well into the future. Unisys has proven, over the course of the current contract we can meet and exceed the needs of the Commonwealth. The response to this RFP is meant to show that Unisys, in cooperation with the Commonwealth, can take support for this, and other platforms, to the next level to provide the Commonwealth with the next generation of application infrastructure. Such an infrastructure is one that includes unified server management tools, closely aligned processes and automation to deploy new capacity, and patch servers to deliver proper maintenance and security levels, and remediate common issues.

1 Server Environment Operations Approach, MS Windows

1.A Monitor local operations, troubleshoot and resolve operational issues.

Unisys will provide hosting and operation support services to the Commonwealth of Pennsylvania for required versions of Windows systems at the Commonwealth [redacted] and Unisys data centers. Staffing required to perform the operational tasks listed below will be located on-site in Harrisburg with off hours support located in Salt Lake [redacted] Our monitoring and troubleshooting operations are detailed further in paragraph 1.B of this response.

1.B Actively monitor the daily operations of all MS Windows servers.

Offeror must describe its approach to supporting Windows based server environment including the following:

process and procedures

tools/ applications

end user reports (standard and custom)

tiered Service / support Levels

escalation procedures

Processes and Procedures

Our goal is to confirm that all services are managed in a structured, process-oriented way so the Commonwealth can see measurable improvements in the quality of the services delivered. The processes and procedures for providing Windows infrastructure managed services will be

documented in the CCPM which will be reviewed and approved by the Commonwealth. The scope of these processes and procedures will be based on the ITIL V3 framework as well as technology best practices for support of the Commonwealth Windows platform.

Processes and procedures will be developed for the following areas:

- Server technology support – build and maintain for hardware, software, connectivity
- Vendor management – technical support, maintenance coverage, and remote access capabilities
- Platform specific procedures – customer notification, technical support escalations patching process/schedule, security monitoring, and log reviews

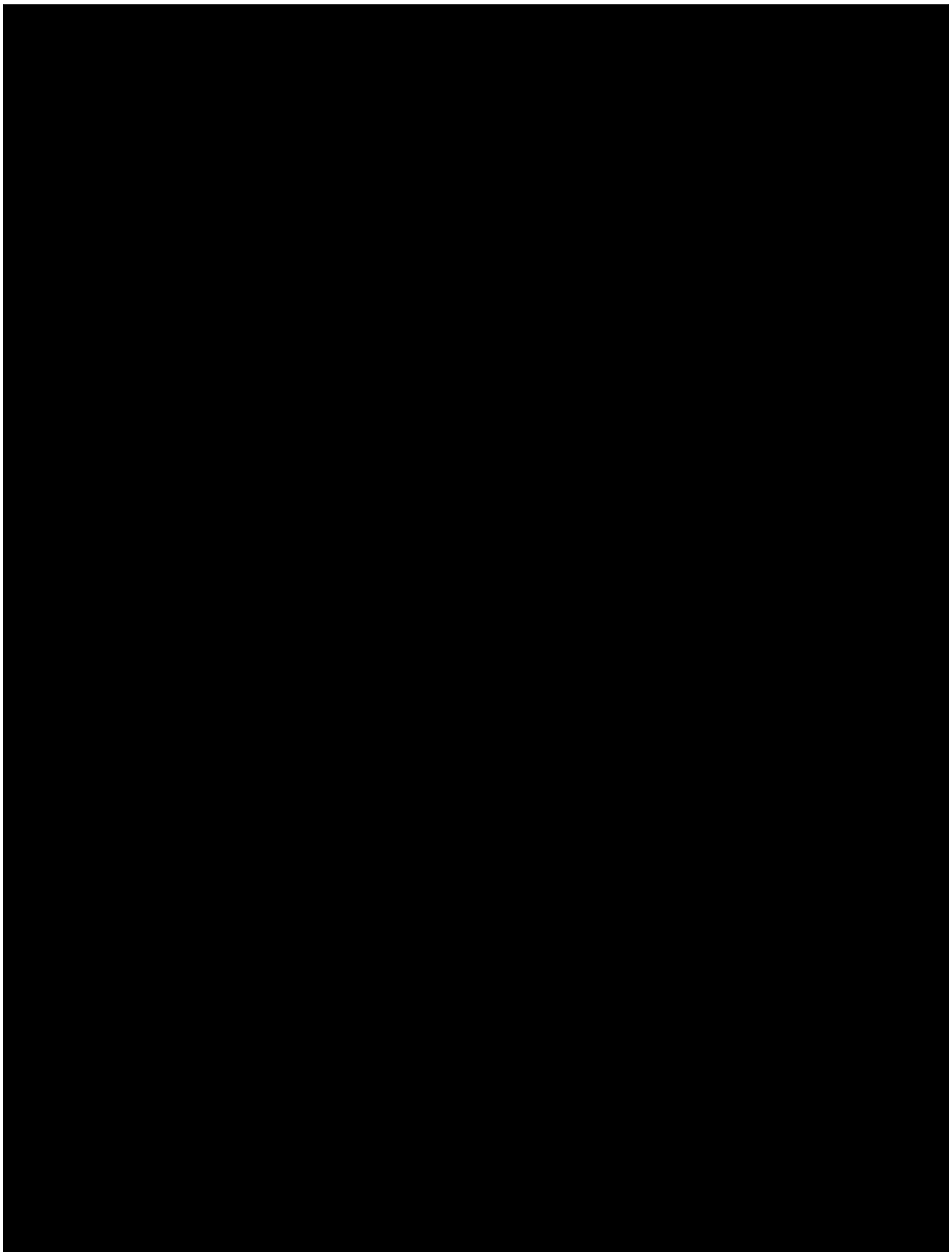
Tools/Applications

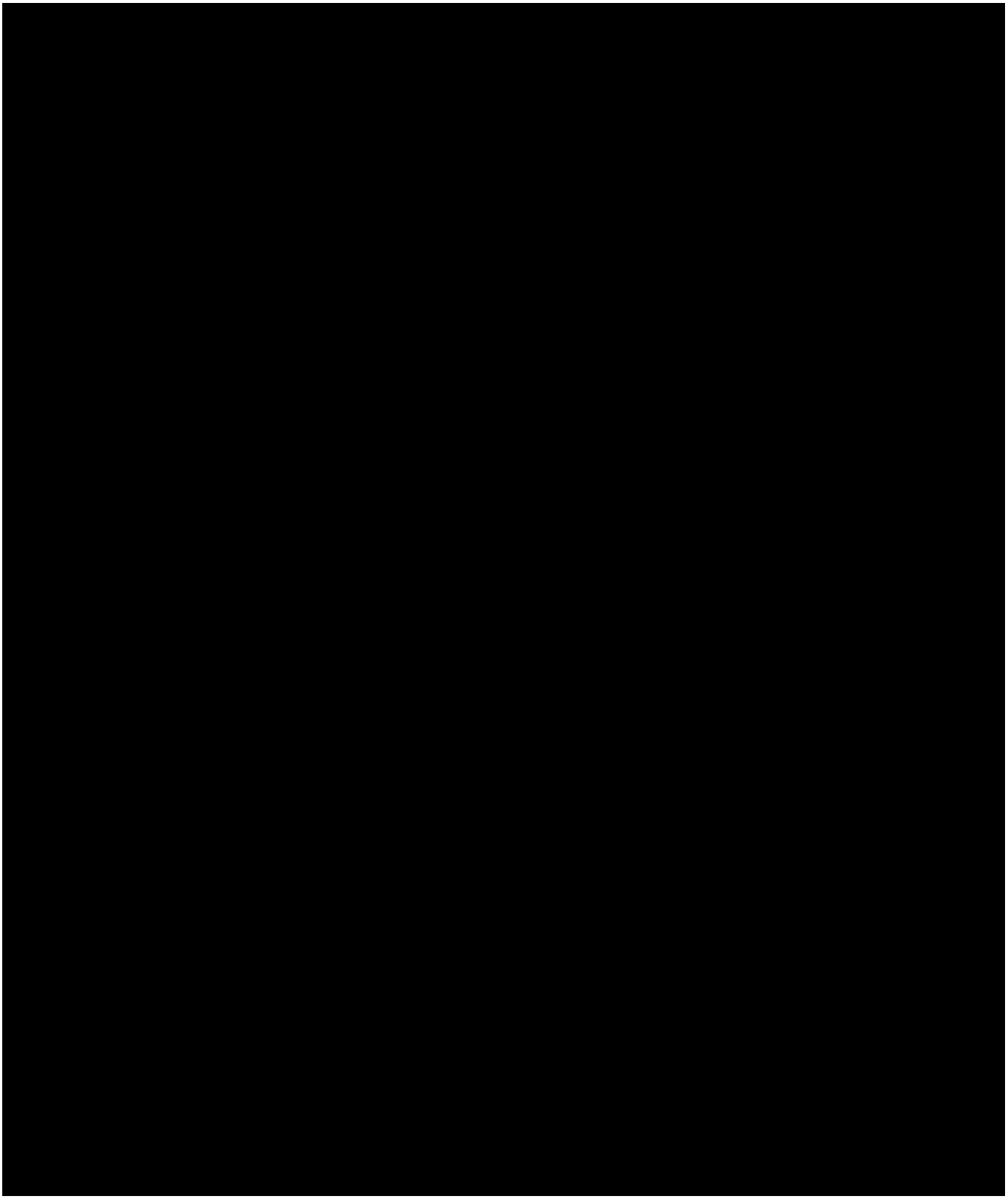
Unisys has outlined the approach to monitoring operations and supporting automated remediation over time from a common enterprise infrastructure platform across all technical towers for the Commonwealth in F3.2.3.2 Site Operations. The following is an overview of how all platforms, including the Windows environment, will be monitored and managed.

Unisys will implement, support, and operate a comprehensive and integrated Information Technology Service Management (ITSM) Architecture dedicated to the cross functional process support for all services provided to the Commonwealth for this contract. The proposed ITSM Architecture, shown in **Figure 3.2.4.1-1**, will provide an effective and efficient operational platform to support the Commonwealth's agencies application infrastructure for the following ITIL V3 (Information Technology Infrastructure Library) Service Management Processes.

Figure 3.2.4.1-1 - Proposed Unisys ITSM Integrated Architecture

The Integrated ITSM Management Platform software tools are summarized in the **Figure 3.2.4.1-2**.





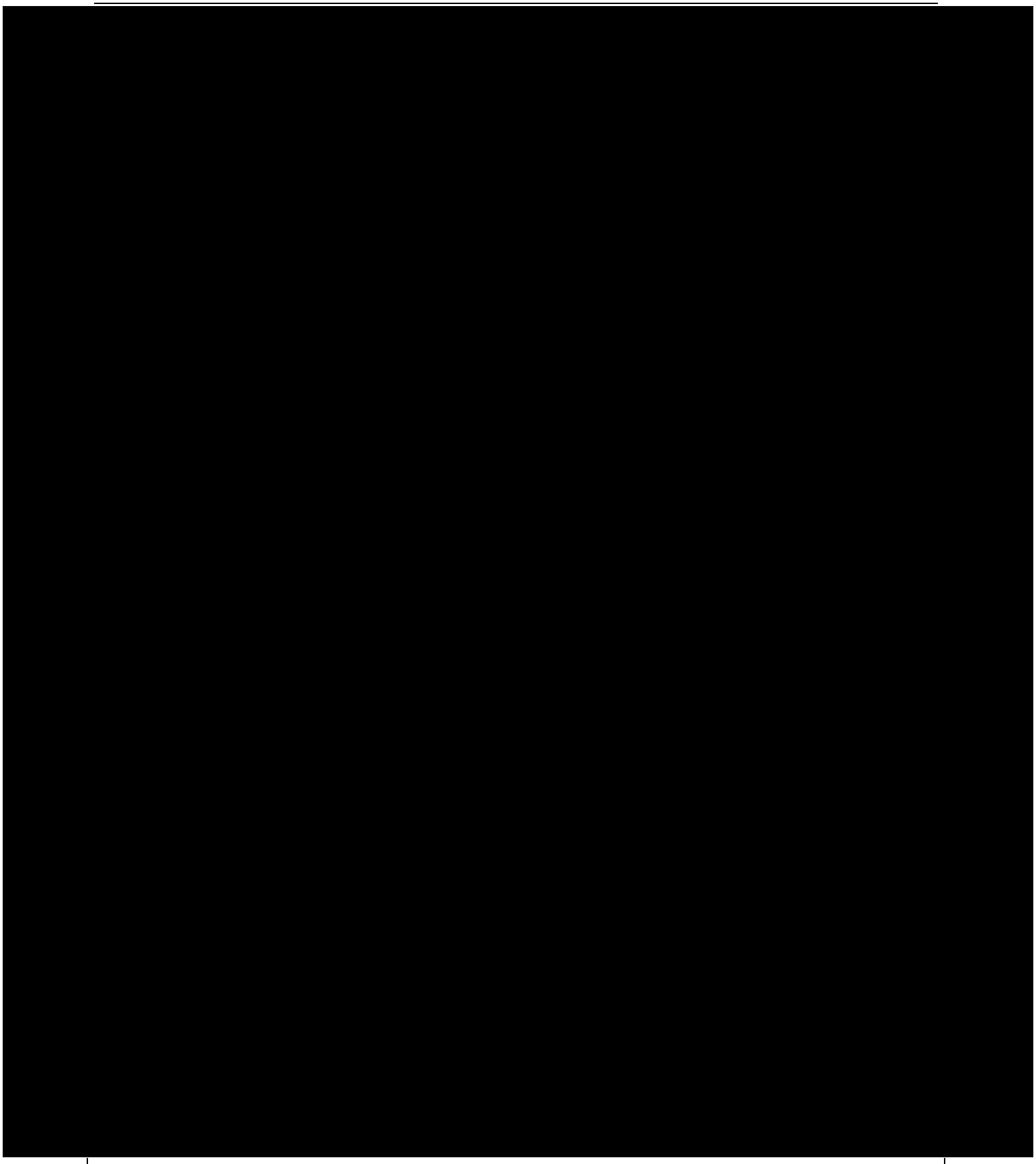


Figure 3.2.4.1-2 - Unisys ITSM Tools

Unisys will assess the Commonwealth's current ITSM toolsets during transition. Assessment results determine which tools will be supported within this overall target ITSM proposed architecture, replaced, or eventually migrated to the target environment ITSM tools shown in **Figure 3.2.4.1-2**. Some of the tools that will be evaluated and assessed during transition include:

- MS SCOM
- MS SCCM

The resulting architectural decisions will be reviewed and approved by the Commonwealth's agencies. Some identified tools will continue to offer the functionality they currently providing, but will be integrated into the overall ITSM proposed architecture.

End User Reports

- Standard Reports are summarized in 3.3.2.
- Custom Reports are offered by Unisys as a Catalog Service

Tiered Service/Support Levels

The Commonwealth of Pennsylvania has indicated in Schedule J.2 - Datacenter Service Level Matrix the desired service tiers/support levels. In the design of the Services and the infrastructure needed to deliver those Service to the Commonwealth, the Unisys Team defined the Service Tiers to align to those requirements. A fuller explanation and representative sample of all the Services provided in this structure can be found in the response to Schedule F, Section 3.2.1.5, sub-requirement 1. The service tiers in the Unisys solution are as follows:

Tiered Support Level	Description
Platinum	• Provides 99.999% Application Infrastructure Availability • Server is monitoring via Nagios • Fully Managed Services • Asset Tracked In CMDB with relationships • Requires 3 servers load balanced and geographically dispersed
Gold	• Provides 99.99% Application Infrastructure Availability • Server is monitoring via Nagios • Fully Managed Services • Asset Tracked In CMDB with relationships • Requires 2 servers load balanced
Silver	• Provides 99.9% Application Infrastructure Availability • Server is monitoring via Nagios • Fully Managed Services • Asset Tracked In CMDB with relationships
Bronze	• Provides 99.4% Application Infrastructure Availability • Server is monitoring via Nagios • Fully Managed Services

	• Asset Tracked In CMDB with relationships
Basic	• Provides 98.5 % Application Infrastructure Availability • Server is monitoring via Nagios • Fully Managed Services • Asset Tracked In CMDB with relationships

Escalation Procedures.

Escalation procedures are part of the Incident Management Process described in F3.2.1.4 Service Desk. Escalation procedures will be configured with the [redacted] to support meeting SLA's proactively with automated escalations when incidents are approaching SLA violations. Also, there is a proactive escalation process for incident tickets supported by the Unisys service desk which manages all escalations for normal operations. The Unisys PMO will be involved with any critical escalations as a senior Account Manager will be managing the technical response team and Service Desk communications for critical Priority 1incidents. This includes well defined communications and notifications, status updates, and procedures to support restoring services effectively and efficiently.

For additional details please see Schedule F, Section 3.2.3.2 Site Operations.

1.C Maintain a log for each server detailing hardware / software configuration and critical service operations.

The Unisys Team will maintain a log for each server detailing hardware/software configuration and critical service operations using the Configuration Management Database (CMDB) and automated discovery and dependency tool. By maintaining the log for each server as an entry within the CMDB, the Commonwealth and the Unisys Team's Systems Administrators have access detailing all pertinent server information, including but not limited to hardware/software configuration, critical service operations, past errors that impact critical system Services, and major outage information. Reports from the CMDB are available to the Commonwealth via the online Real-time Dashboard.

1.D Document review of the system logs on a weekly basis to ensure critical system Services are processing without errors.

The Unisys Team will collect each server's system logs and using the log management tool's report management functions, validate that critical system services are operating correctly on a weekly basis. In addition to the weekly review, the log management tool is integrated with the Enterprise System Management (ESM) toolset to automate notification of errors and events identified within the logs. As part of the notification, for system services operating with errors, an incident ticket will be created.

1.E Complete weekly server log indicating which logs were reviewed, date and initial the log.

The Unisys Service Delivery Manager will complete a weekly server log indicating which logs were reviewed, date and initial the log. A copy of this log will be made available to the Commonwealth on the Real-time Dashboard for review. These logs will be retained for one

year.

2 System Backup Policy Review and Audit

The full details of the innovative backup service provided to meet the Commonwealth's data protection needs are included in the F.3.2.4.2 Storage Management.

2.A Offeror must describe its approach to performing an initial review and audit of the backup policies, procedures and reports, to ensure the accuracy of the backup schedules, retention periods, target directories, and recovery point objectives.

The Unisys Team will conduct an initial review and audit of the backup policies, procedures and reports, to verify the accuracy of the backup schedules, retention periods, target directories, and recovery point objectives. The detailed process for conducting this audit, and how the audit findings will be communicated back to the Commonwealth can be found in Schedule F, Section 3.2.4.2, subsection 4.

2.B Offeror must describe its approach to identify gaps and potential risks, and how those gaps and risks will be resolved.

During transition and transformation, the Unisys solution includes an extended onsite presence of a CommVault technical manager who will aid the Unisys Team in the search for existing gaps and risks, along with potential improvements to the backup systems during the transition phase of the solution. This technical expert has extensive experience in implementations and in identifying value-add opportunities. The skills of this technical expert are married to the Unisys Team's extensive expertise around current backup operations. Jointly they will lead the transition to a more cost effective CommVault backup infrastructure. The Unisys Team, working with the CommVault technical manager, will manage the review and audit of backup clients that move from the legacy system into the CommVault system. During transition a like-to-like set of backup policies, procedures, reports, schedules, retention periods, target directories, and recovery point objectives are built out. The Unisys Team can then present the Commonwealth with for opportunities to further optimize the infrastructure to improve the quality of services or provide better cost efficiencies for the same services.

The Unisys Backup team will compare the backup inventory of clients and policies to the CMDB inventory to locate "negative" gaps in case a server or critical data set is introduced into the Fully Managed environment and, through unlikely process failures, was not also protected with sufficient backup resources. The Unisys governance processes and the processes generated by the Unisys solution's Enterprise Services Catalog are designed to remove such failures. Additionally, a compare of Backup infrastructure inventory from the backup tools perspective with the CMDB can locate a gap should one occur as an additional level of protection.

The activities to perform the gap analysis are described in F.3.2.4.2, Requirement 4.

2.C Monitor system backup processing on a daily basis.

Unisys has a proven automated approach to monitoring daily backups, eliminating the need to maintain staff to watch the nightly progress of backups. In most cases simply re-starting a backup results in a successful backup because needed resources are tied up during peak times but become available a short time later. Unisys automates the restart process to occur

automatically. If the restarted backup fails then incident tickets are created to alert the team. With this approach, critical issues get right to Level 2 and Level 3 support personnel without ever involving Level 1 support staff. Unisys will produce daily reports of backup successes.

2.D Review daily backup log for successful completion. Offeror must describe how the authorized Commonwealth users will have online access to backup logs.

The Commonwealth benefits from the Unisys approach to automated monitoring of backup success rates as detailed above.

This automation of incident ticketing provides the Commonwealth with another advantage. During service delivery reviews the Commonwealth can review response times to failures that might put critical applications at greater risk. Through the incident severity rating processes Unisys has the ability to adjust severity levels so that incidents that are closer to critical applications can receive prioritized support responses.

The Commonwealth will have the ability to designate application owners who require read access to the backup management console so that these individuals have ready access to monitor both the success and failure rates for backups as well as the backup content. As often happens, some applications require specific bundles of directory backups and this access provides application owners a means of validating that any customized backups have been implemented properly and are running correctly.

2.E Note failures, and correct the problems.

If automated restart fails, the failed backups automatically create incident tickets which are escalated from Level 2 through Level 3 support groups as necessary until resolved.

2.F Create problem record for any abnormal condition and any repairs that have been made, re-execute as appropriate.

Incident tickets are created automatically and create a record of abnormal conditions. Following ITIL V3 based processes Level2 and Level3 will review incidents for root causes that create multiple tickets. This identification of problems allows the team to establish workarounds and request architecture reviews as necessary. Repairs are driven by incident tickets that are automatically generated by the Nagios collectors which review system logs for hardware.

2.G An automated software process will be utilized to report the completion status of backup processing, with electronic notification of failures sent to Offeror technical support, and identified Commonwealth staff for follow up and corrective action.

The backup software produces daily, weekly, and monthly reports like the one shown below. The Nagios collectors in the ITSM infrastructure will create tickets automatically upon a failure of a backup for action by Level2, and Level3 support as necessary. The Commonwealth can elect as many personnel as they wish to receive notifications of these incident tickets, their status, and their resolution.

3 Staff, MS Hyper-V and [redacted] Resumes

3.A Provide Microsoft Hyper-V and [redacted] trained staff holding manufacturer recognized certifications for hardware and software technical support.

Offeror must submit a representative sample of staff resumes typically provided for these positions detailing their experience, education, and certifications.

The Unisys Team will include qualified and certified Hyper-V and [redacted] resources. Representative resumes for personnel providing Hyper-V and [redacted] Services are located in the tab marked Rep-Resumes in Section 5.0 Personnel.

3.B Post award; provide the Commonwealth a resume or CV for each operational staff member assigned to this engagement.

Post award, Unisys will provide to the Commonwealth the applicable resumes of operational staff that perform Hyper-V and [redacted] support for systems on which Commonwealth applications reside. Representative resumes for personnel providing Hyper-V and [redacted] Services are located in the tab marked Rep-Resumes in Section 5.0 Personnel.

3.C A copy will be maintained on Offeror file including verified background clearances as required.

Unisys will maintain a copy of all background clearances, resumes on file, either electronically or via paper copy.

4 Service Desk, Tiered Support

The proposed solution includes a robust technical support staff with the necessary skills to provide the managed services requested by the Commonwealth of Pennsylvania in this RFP. The staffing levels are determined based on key performance indicators which specify the expected number of devices to be supported by each member of the technical team. The team will be staffed with junior and senior positions to provide coverage for Level 2 and Level 3 technical support requirements.

4.A Provide cost effective operational and technical support for the Windows computing platform.

The Commonwealth of Pennsylvania has included in this RFP all the elements needed to achieve measurable and ongoing cost effective operational and technical support for the Windows platform. Unisys will realize these cost efficiencies by properly integrating these pieces into a unified Enterprise Service Management Solution. Included in the response to this RFP are tool sets that align closely existing process, reducing the risk of adopting new processes and tools. Unisys will also deploy additional automation that will server to realize further efficiencies. Finally, Unisys unique Continual Service Improvement Implementation Program will drive efficiency into the enterprise by continually reviewing outages, incidents, and other operational data to make specific recommendations to the Commonwealth to enable further efficiency.

The Unisys Team has included the cost efficiencies gained through adoption of the IT Service Management platform, ITIL V3 aligned processes utilization of a common server platform and through the deployment of automation into the solution.

4.B Provide platform level operational and technical support for the computing platform.

In addition to providing the required resources, the Unisys Team will be focused on proper work allocation and skills development. The Unisys ITSM system will be the primary tool used to allocate work across the various service towers providing communications and control capabilities for delivering the services. Skills development will be provided with formalized training programs and peer mentoring assignments to allow for on the job training opportunities.

4.C Provide Level 2 and Level 3 Support to the Service Desk and/or Commonwealth Users.

Offeror must describe its approach to providing and maintaining different tiered levels (i.e. Level 2 & Level 3 Technical Support) of support.

The proposed solution includes a robust technical support staff with the necessary skills to provide the managed services requested by the Commonwealth of Pennsylvania in this RFP. The staffing levels are determined based on key performance indicators which specify the expected number of devices to be supported by each member of the technical team. The team will be staffed with junior and senior positions to provide coverage for Level 2 and Level 3 technical support requirements. Human resource actions including writing position descriptions, development plans, and funding for certifications are all targeted and provides that the technical support resources are prepared to support the managed services.

To support the operational and technical needs of the Commonwealth, the Unisys Team will deploy incident, problem and change management processes that define the flow of support from the Service Desk up through Level 3 support. These processes are closely aligned to the common IT Service Delivery platform. For more detailed information on these processes, please refer to Schedule F, Section 3.2.3.2.

4.D Provide a tiered level of support Services (e.g. Gold, Silver, and Bronze).

Offeror must provide a representative sample of available tiered service support Services.

In order to provide customization and flexibility to Commonwealth agencies, the Unisys Team offers tiered levels of managed services for Capacity on Demand servers. These tiers offer various levels of administrator experience, on-site coverage and responsiveness SLA's. The tiers are designed to allow for flexibility to manage mission critical as well as development or demonstration environments.

The following table highlights the available tiers and associated descriptions.

Tiered Support Level	Description
Platinum	• Provides 99.999% Application Infrastructure Availability • Server is monitoring via Nagios • Fully Managed Services • Asset Tracked In CMDB **with relationships** • Requires 3 servers load balanced and geographically dispersed
Gold	• Provides 99.99% Application Infrastructure Availability • Server is monitoring via Nagios • Fully Managed Services

	• Asset Tracked In CMDB with relationships • Requires 2 servers load balanced
Silver	• Provides 99.9% Application Infrastructure Availability • Server is monitoring via Nagios • Fully Managed Services • Asset Tracked In CMDB with relationships
Bronze	• Provides 99.4% Application Infrastructure Availability • Server is monitoring via Nagios • Fully Managed Services • Asset Tracked In CMDB with relationships
Basic	• Provides 98.5 % Application Infrastructure Availability • Server is monitoring via Nagios • Fully Managed Services • Asset Tracked In CMDB with relationships

4.E Provide technical advice and support to the Application Development and Maintenance (ADM) and Database Administration (DBA) staffs, as required.

Unisys will have a team of technical architects dedicated to the Commonwealth of Pennsylvania and Commonwealth agencies whose responsibilities will include providing technical consultation and advice to the Commonwealth's ADM and DBA groups.

4.F Post award; provide Commonwealth with a resume or CV for each operational staff member assigned to this engagement. A copy will be maintained on Offeror file.

Post award, Unisys will provide to the Commonwealth the applicable resumes of operational staff.

5 Monitor Network Connectivity

5.A Ensure network connectivity and consistent system response times.

Offeror must describe its real-time monitoring approach and its toolset for providing and maintaining network availability and performance.

Offeror must identify tools it uses to support network availability and performance.

Unisys will deploy the SolarWinds tool to monitor the Commonwealth network. SolarWinds provides network availability and performance monitoring and network traffic bandwidth throughput monitoring. From a server perspective, Nagios will be used to confirm server availability on the network. When either of these tools detects an event, an event is sent to the Event Management system, where the event is correlated, and an intelligent ticket is opened with the proper resolver group. For a complete understanding of how this subset of Event Management Tools supports enterprise Event Management please refer to 3.2.3.2 Site Operations.

5.B Utilize automated system management tool(s) to ensure real- time monitoring and notification of

server availability and response times. Stop / Start times of servers will be a source of input for SLA measurements. Identify tool set(s).

Unisys will provide event management solutions to help provide network connectivity and consistent windows systems response times. Unisys will utilize the Unisys ITSM applications to record incidents tickets that are generated from windows monitoring tools to provide real- time monitoring and notification of server availability and response times including the stop and start times of servers to support SLA availability measurements. SLA availability measurements are measured in the Unisys ITSM Service Level Management Application and displayed in the Real-time Dashboard available to Commonwealth agency personnel. The following tools are the major toolsets to support network and system event management and monitoring.

Monitoring Software	Managed Configuration Items (CIs)	Monitoring and Management Functionality
SolarWinds	LAN Devices including: • Switches • Routers • Load Balancers • Firewalls	Provides deep network device availability and performance monitoring , DNS, IP address management, network configuration management, and network traffic bandwidth throughput monitoring
Nagios	• Microsoft servers • Databases • Network Devices • Storage Hardware	Provides a standard set of availability, performance and critical service monitors developed by Unisys for monitoring across infrastructure items including: • Servers • Network devices (switches, routers, etc.)) • Storage devices Middleware • Applications (e.g., Exchange, Citrix XenApp)

6 Patch Management

6.A Offeror must describe its approach to patch management.

The Unisys Team will follow the Commonwealth of Pennsylvania's ITB for patch policy, "ITB-SYM006 - Desktop and Server Software Patching Policy" for patching of Windows servers.

The Unisys Team will follow the Change Management Process for applying patches to the production windows environment. This process will maintain the change record in the [redacted] and also update the CMDB configuration management file upon deployment for windows server environment Configuration Items (CIs). The Change Record will be related to the CI's in the CMDB as an audit trail for changes to Windows CI's upon the completion of the Release and Deployment Process for changes.

6.B Offeror must identify tools it uses to manage system patches.

The toolset to support the automation of patch release and deployment is [redacted]

[redacted] Unisys will maintain in this toolset the appropriate patch policies for determining patch deployment and compliance. The [redacted] will be maintained with all the current patches supplied by the OEM's and will be used to manage the production state of patch deployment in the windows environment. The following table shows all tools utilized in the management of system patches.

[redacted]	Functionality
	Maintains all current patches released by Microsoft for the Windows operating system. Performs the patching of systems.
	Provides the following functionality related to patching: • Incident management • Change management
	Configuration Items (CI) are automatically updated as needed post patching.
	Updates the CMDB with any needed additions to the CI

6.C Offeror must describe its approach to testing and validating updates to the OS and 3rd Party software that it supports.

Unisys approach to testing and validating updates to the Windows OS and 3rd party software in the Windows environment is to follow the Release Process for all changes into all production environments. The Release Process includes:

- Change ticket approvals
- Test planning and accepted test results
- Release and deployment planning including release back-out plans
- Release testing for risky deployments
- Early life cycle support to help deliver a successful deployment
- Release back-out for failed releases

6.D Ensure server operating systems are maintained with the current patch level, based on the Services provided by the server.

The performance of Windows system administration covers the following services related to maintaining the patch levels of Windows systems:

- Installation/maintenance of OS/OS patches/OS utilities.
- Problem determination/resolution for OS/OS patches/OS utilities.
- Review/recommend new OS/OS patches/OS utilities versions/patches.
- Install/upgrade OS/OS patches/OS utilities.

- The Unisys Team will setup and perform backup/recovery of OS and OS utility files prior to the patching activities
- Participate in the Change Management and Problem Management processes.

Unisys complies with the requirement.

6.E Analyze monthly service patches and determine which need to be applied, by server type.

The Unisys Team will analyze monthly patches to determine which need to be applied, taking into account those cases when multiple agencies utilize shared infrastructure.

The Unisys Team will then make recommendations to the Commonwealth on which systems need patching, and a recommended schedule for deploying the patches. Unisys will then work through the Change Management process to coordinate with each agency the deployment of system patches.

6.F Create a change record, log the update in the server log, install based on server maintenance schedule and update the server configuration record.

Unisys will follow the Change Management Process for applying patches to the production windows environment. This process will maintain the change record in the [redacted] platform and also update the CMDB configuration management file upon deployment for windows server environment Configuration Items (CIs). The Change Record will be related to the CIs in the CMDB as an audit trail for changes to Windows CI's upon the completion of the Release and Deployment Process for changes.

6.G Notify impacted Commonwealth users immediately of any unscheduled service interruptions via email/web.

Offeror must describe its approach to communicate unscheduled and scheduled outages, including escalation process.

Unisys approach to communicating unscheduled outages is to send notifications to key stakeholders for the Commonwealth/Agencies/Unisys/Third Parties depending on the outage. This will be through email, voice, Services Portal and Remedy broadcast capabilities. The same communications will be used for scheduled outages with additional communications in forward schedules of change reports.

Escalations for unscheduled outages are handled through the standard processes for managing incidents. Unisys service desk will manage all incidents and confirm that proper escalation communications to key Commonwealth/Unisys/Third Parties personnel are managed. The [redacted] application will also be configured to escalate incident tickets based on incident priorities and SLAs to verify that incidents tickets are being managed to SLA times for incident response and resolution.

To support the operational and technical support needs of the Commonwealth, the Unisys Team will deploy incident, problem and change management processes that define the flow of support from the Help Desk up through Level 3 support. These processes are closely aligned to

the common IT Service Delivery platform. For more detailed information on these processes, please refer to Schedule F, Section 3.2.3.2.

6.H The Offeror must be document normal work hours and holiday schedules with each agency to determine the contact method and escalation process of each Commonwealth agency.

Unisys will document and update yearly normal work hours and holiday schedules for each agency. This documentation will be used as a data feed into the operational documentation listing escalation processes and contact methods Unisys is to use when contacting agency personnel.

7 System Performance and Capacity Assessment

The initial review and audit of the current usage of the Commonwealth's compute infrastructure will be performed in two phases, aligned to the sub-requirements of this Section (7.A, 7.B, and 7.C).

7.A Provide a review and analysis of system performance/capacity to determine if current performance/capacities are sufficient to support the needs of the stakeholders.

The first phase will be accomplished as Unisys prepares to migrate the existing workload from each of the existing Commonwealth data centers into the new data centers. During this time, Unisys will deploy tools to collect and analyze all aspects of the Commonwealths current compute usage. Analysis of these workloads will be used to determine the optimal method for migrating these servers. This analysis will also serve as a baseline against which future capacity planning can be compared.

The second phase will occur when Unisys deploys the new Capacity planning process and tools into the Commonwealth compute environment. This phase will perform two functions…it will cover those servers not covered in phase one, and will perform a new audit once the workloads have been deployed in the new data centers.

7.B Offeror must perform an initial review and audit of the current usage, procedures and reports and provide an analysis of the current usage, processes and reports currently being supported.

As part of transition, and as each Commonwealth agency is migrated to the new services, the Unisys Team will gather and review all current Commonwealth usage, procedures, and reports, and perform a gap analysis against the planned usage, procedures and reports presented throughout this solution. Once the gap analysis has been completed, the Unisys Team will review all findings with the Commonwealth team.

7.C Offeror must document its review and audit findings and recommendations.

The final audit findings and recommendations will be presented to the Commonwealth by the Unisys Enterprise Architecture Team.

8 User Account Management

8.A Provide certified operating system administration staff to create and maintain the registration of profiles, associated groups, and the security permissions required to service the approved client base of the operating systems.

Offeror must describe its approach to managing user accounts.

Unisys Windows support team will provide user profile, group and security permission management on individual Windows servers. For servers operating on an Active Directory domain, Unisys will work with Commonwealth Active Directory support team to request changes in the Active Directory environment to support user, profile, group or security permissions changes. All changes for user account management will be initiated through the service request and change management process and will require an approved change record for implementation. The process for user account management will be documented within the CCPM.

9 Procurement Planning

9.A Provide program and processes to refresh the hardware at asset end-of-life, and as upgrades are needed to meet anticipated growth in utilization

Offeror must describe its programs and processes for procuring new or upgraded systems.

Procurement management is defined by the Unisys as Technology Refresh and as Capacity Management and Forecasting. These two are further defined as follows:

a. Technology Refresh Plan

i. As part of the overall architecture support, the Commonwealth's environment will be reviewed on a quarterly basis to identify technology, services or components which require replacement to maintain the Commonwealth's business needs and associated service levels. The review will include the following activities. The overall technology refresh plan will be documented in Key Deliverable D-03. This plan will be used for all Unisys supported environments including the Commonwealth Windows systems.

1. Using the data within the Asset Management and Configuration Management databases, identify the technical components within the Windows system environment which require replacement within the next 18 month period based upon the a 60 month replacement cycle.
2. Review End of Sales and Service Life notices from the Manufacturers to validate if a component has been discontinued or has available ongoing maintenance options.
3. Review ongoing Capacity and Performance reports to identify any components with a refresh requirement which have additional needs driving a requirement or opportunity to change the component's classification to a different component to maintain the functionality and service levels.
4. Identify replacement technical components based upon the current Enterprise Services Catalog offerings
5. Validate replacement technical components meet the current requirements for the impacted Commonwealth applications.

6. Identify risk and impact for the Commonwealth environment to replace existing technical components or services.

7. Create technology refresh recommendations, impact statements, and high level implementation plan.

8. Present the technology refresh plan to the Commonwealth using the solution architecture review process.

9. Upon approval of the refresh plan, open service requests for each migration group and develop the detailed project plan for the migration plans.

b. Capacity Management and Forecasting

ii. The Commonwealth Windows systems will be monitored and reported from the Event Management Platform ([redacted]) [redacted] and from the [redacted] toolset to support the windows Capacity Management requirements. As part of the Capacity and Performance Management processes, , the performance and capacity reports will be generated and reviewed with the Commonwealth on a regular basis.

iii. During transition the windows environment capacity requirements will be assessed as part of the establishment of the Performance and Capacity Management Processes described in Schedule F, Section 3.2.2.6 and 3.2.2.2. The assessments will be used to generate capacity and performance management recommendations and plans. . The Unisys Capacity Manager and Performance Analyst will work with the Commonwealth/Agencies to forecast windows workload requirements in order to support the current and forecasted workload, as well as establish the monitoring requirements to support the ongoing daily assessment of the workload performance on the windows platform in total and by agency. Any recommendations to increase, modify or decrease windows capacity will be processed through the Change Process after reviewing recommendations with Commonwealth Stakeholders in the Capacity and Performance regularly scheduled meetings where trends, issues and forecasts are discussed and reviewed.

iv. As part of the annual Capacity and Forecast planning activity, Unisys will work with the Commonwealth to identify what changes in growth are expected and provide recommendations on additional upgrades.

v. In addition to the Commonwealth's growth forecasting information, Unisys will use the data within the Capacity Management, Asset Management and Configuration Management databases and identify the technical components within ERP system environment which require upgrades or additional infrastructure to support the forecasted growth requirements.

vi. Identify replacement or upgrade technical components based upon the current Enterprise Services Catalog offerings and the vendor's available products.

vii. Validate that the identified upgrades or additional components meet the current and forecasted requirements for the impacted Commonwealth ERP system.

viii. Identify risk and impact for the Commonwealth Windows systems to upgrade or add additional components.

ix. Create the capacity upgrade recommendations, impact statements, and high level implementation plan.

x. Present the capacity upgrade plan to the Commonwealth using the solution architecture review process.

xi. Upon approval of the capacity upgrade plan, open service requests for upgrade project and develop the detailed project plan.

The overall approach to technology refresh is described in Section 3.2.1.5.1 Technology Refresh.

10 SLA Reporting

10.A Collect actual system availability, utilization and response time data. On a monthly basis, Offeror must create a Service Level Agreement report for the Commonwealth team.

Offeror must describe processes and toolsets it uses for monitoring and maintaining service levels.

Unisys will establish an SLA process and technical architecture to support all SLA's for this contract. See the overview in F3.2.1.2 Availability/SLM. Level 1 of the SLM process is outlined in **Figure 3.2.4.1-3** below:

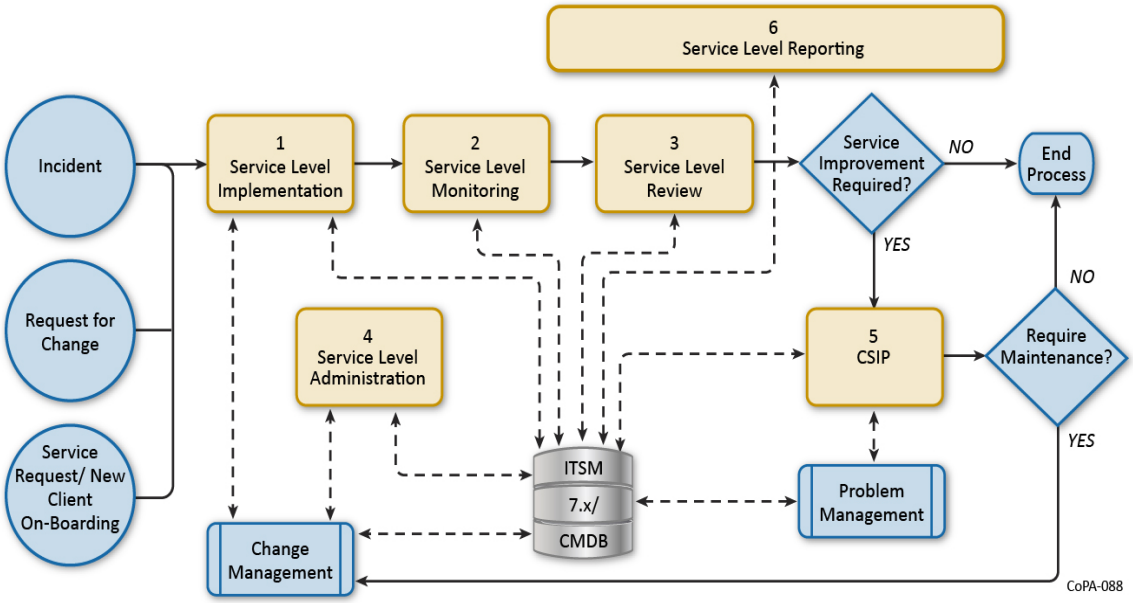


Figure 3.2.4.1-3 - Service Level Management Process

Unisys will provide a detailed set of processes and procedures to support Service Level Management during transition of this contract. The process and procedures will support this top level view of the process which includes:

1. Service Level Implementation
2. Service Level Monitoring
3. Service Level Review
4. Service Level Administration
5. Service Level Improvements (CSIP)
6. Service Level Reporting

Unisys will provide the technical architecture and toolsets to support monitoring and maintaining service levels for the windows platform. The Unisys ITSM Service Level Management (SLM) Application provide by [redacted] will be used as the single unified platform to manage Service Level Agreements for Commonwealth agencies. The Unisys ITSM Service Level Management provides a continuous real-time platform for defining, measuring, monitoring, reporting, and reviewing the performance of SLA's (per J1 – J3) for windows services to make sure that adequate levels of service are delivered in alignment with the Commonwealth's objectives for service delivery. The business contract will contain agreements in which the levels of service are specified. These agreements consist of individual service targets or goals that are used to evaluate whether the agreement is in compliance.

The Service Level Management Application uses all the other Unisys ITSM modules as inputs to determining if an SLA is in compliance. The Unisys ITSM modules used for transaction inputs to determine if service level targets and goals are in compliance include:

- Incident Management
- Problem Management
- Change Management
- Asset/Configuration Management
- Performance/Capacity Management

The [redacted] Application and in some unique cases other tools as described in F3.2.1.2 will be used to push near real time SLA reporting into the Real-time Dashboard reporting tool.

Offeror must provide a representative sample of an SLA report.

See figure below, a Sample Application Infastructure SLA report and **Figure 3.2.4.1-4** sample Real-time Dashboard screenshot.

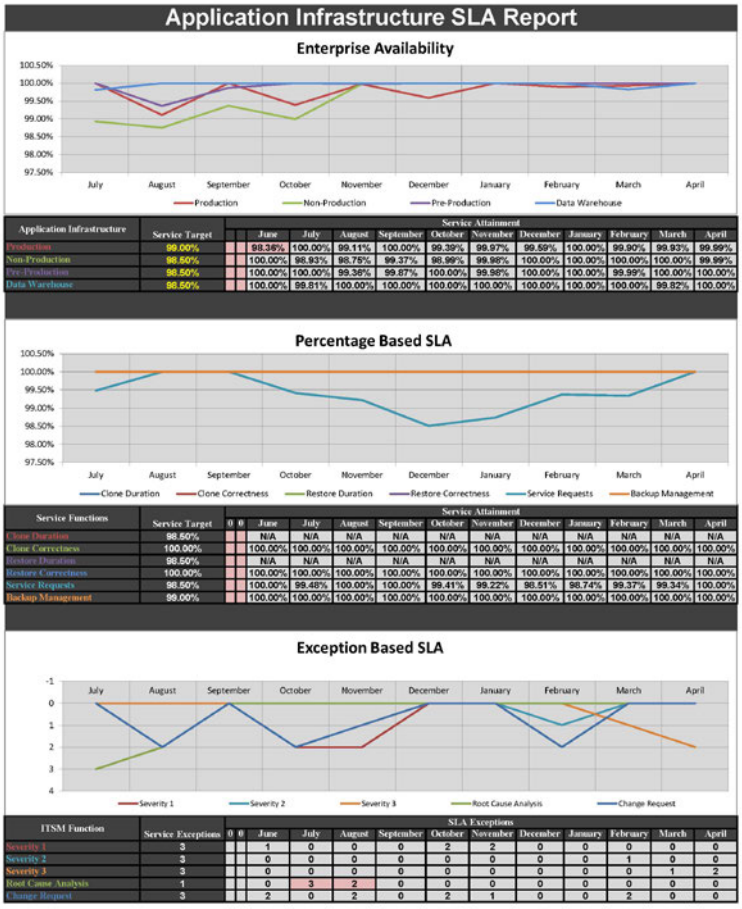


Figure Sample Application Infastructure SLA report

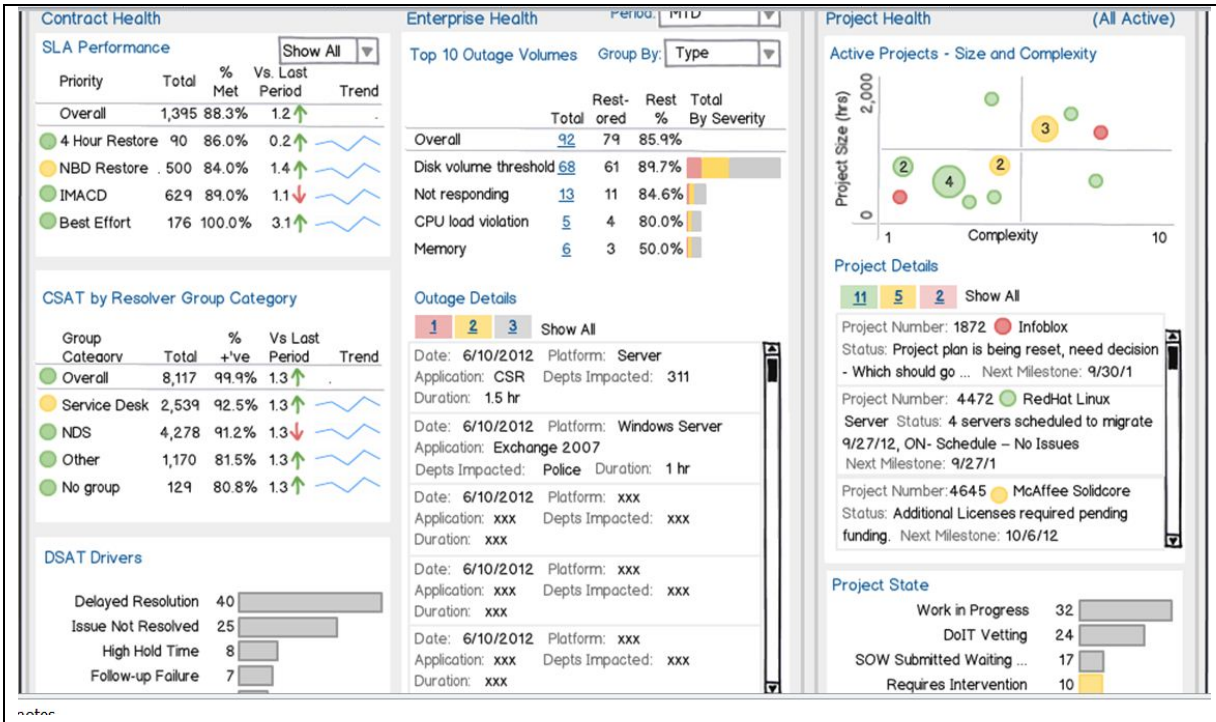


Figure 3.2.4.1-4 - Sample Real-time Dashboard Screenshot

11 Patch, Installation of Windows Updates and Patches

11.A Offeror must describe its programs and processes for applying system updates/patches.

Unisys has a solid track record working with the Commonwealth to adapt processes such as our patch management process to a multi-tenant infrastructure, including the coordination of patches with all agencies on the infrastructure being updated. Please see the response to requirement 6 immediately above for details on Unisys programs and processes for applying system updates/patches.

11.B Coordinate at an agency level and account for any required patching as technology upgrades require

Installation of Windows updates/patches must be coordinated by Agency.

As described in sub-requirement 6 above, Unisys will work with the Commonwealth to adapt its patch management process to a multi-tenant infrastructure, including coordination of patches with all agencies on the infrastructure being patched.

11.C For IES, windows version upgrades must be SAP certified.

The Unisys Team will work with Microsoft to verify that version upgrades applied to IES Windows servers are SAP certified, and include a statement of SAP certification in the change request prior to submission to the Change Advisory Board.

12 Software License Management

12.A The Offeror must provide Software License Management.

Offeror must describe solution and approach to meet this requirement.

Unisys will provide Software License Management for all infrastructure including windows

platforms. Unisys will provide 3rd Party License Management service for the Commonwealth and Unisys provided infrastructure software products. Unisys will be solely responsible for the management of all infrastructure software license products provided through this contract. The goals of this service are to:

- Confirm software contract compliance (to avoid non-compliance legal issues and expenses)
- Manage costs of software inventory by matching requirements for use to needs
- Verify software maintenance contracts are maintained on schedule through early notifications

Unisys will coordinate with the Commonwealth to verify compatibility between Commonwealth provided applications related software, and Unisys provided infrastructure software. The following is the approach Unisys will execute during transition and as an ongoing process to provide 3rd party software license inventory and tracking per agency related infrastructure.

a) Load all Unisys and Commonwealth software asset license contract information into the [redacted]

b) Load all software license certificate , license type, entitlements, manufacturer, and product information into the [redacted] for the Software License Contract

c) Run discovery through [redacted] tools to identify all software installations

d) Run the [redacted] software to build relationships between the discovered software CI's recorded in the [redacted] and the license certificates

e) Run the [redacted] to identify noncompliant licenses and inventory for the Unisys and Commonwealth Asset Managers to audit the completeness and accuracy of the information

f) Identify discrepancies in the information and make corrections

g) Rerun Compliance Reports and 3Rd party software license inventory reports to get signoff from the Commonwealth and Unisys Asset managers that inventory is properly linked to license certificates in the production environment and the information is complete and accurate

h) Provide notifications to Commonwealth/Agencies/Unisys and other Commonwealth service providers when there are software compliance issues or requirements for licenses to be purchased or retired from analysis of license inventory.

13 CI Reduce Service Risk

Continual Service Improvement

Unisys recognizes the significant importance of Quality and Continuous Service Improvement to:

- Reduce service risk,
- Improve service quality,

- Improve client satisfaction,
- Provide service transparency, and
- Improve/reduce costs of service.

Through a continuous cycle of evaluation and improvement within an IT infrastructure, Unisys views quality and continuous service improvement as a critical success factor in driving customer satisfaction for the Commonwealth IT infrastructure. Each of the continuous service improvement areas identified above are driven through the tight integration of the following organizations, industry tools, proven processes and quality deliverables:

- Service Excellence Office,
- Quality Plans: transition and steady state service delivery
- Industry standard frameworks and methodologies: ITIL, ISO, SSL
- Industry accepted measurement tools
- Continuous Service Improvement & Innovation Processes (CSIIP)
- Risk management, audits and business continuity management
- Client Satisfaction Surveys and Knowledge Management Portal

Collectively this represents Unisys Integrated Quality Plan for the Commonwealth of Pennsylvania.

Specifics on each of these areas are outlined in Schedule F, Section 3.2.1.1.6 Continuous Service Improvement. Highlights from this section are outlined below and requested service examples are provided at the end of this section.

13.A Reduce service risks.

Risk management, independent quality audits, and business continuity management are integral quality management processes. Unisys is committed to managing risks and facilitating the achievement of business objectives the adherence to quality processes. We mitigate risk through the implementation of tight quality controls: standard policies, procedures, roles, risk assumptions, issues, and definitions, etc.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

14 CI Service Quality

14.A Improve service quality.

On a quarterly basis, Offeror must also recommend to the Commonwealth team any system changes that would be appropriate to maintain or improve SLA commitments.

The quality approach begins with the Service Excellence Office who provides definition and oversight of all ITIL process management and analysis functions. Process managers and analysts working in the Service Excellence Office are responsible for auditing process effectiveness, ensuring that service delivery teams comply with proper execution of processes, and analyzing process trends for anomalies. Continuous service improvement programs in collaboration with Commonwealth agencies are managed by the Service

Excellence Office.

Through our Continuous Service Improvement and Innovation Process (CSIIP), the SEO reviews, analyzes and makes recommendations on improvement opportunities in each ITIL lifecycle phase. Unisys will leverage Six Sigma Lean tools and methodologies as well as ISO Certified internal audits to measure and maintain the highest quality services to the Commonwealth.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

15 CI Client Satisfaction

15.A Improve client satisfaction.

Offeror must provide examples of previous Offeror initiatives aimed at continually improving client satisfaction.

Client satisfaction is extremely important to Unisys and a key focus in our IT solution. The SEO will integrate new agencies, customers and services into our multi-pronged client satisfaction approach that includes Service Desk surveys on the caller's experience, an overall agency satisfaction survey, and quarterly surveys with the Office of Administration. Data collection will be gathered across multiple levels to gain a clear understanding of the Commonwealth's satisfaction with the IT Services being provided.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

16 CI Service Transparency

16.A Ensure service transparency.

Offeror must provide methods and practices to ensure service transparency, providing visibility into service execution.

The service organizations will use standardized ITSM services processes, IT monitoring and automation tools. ITSM processes will be documented in the Commonwealth Computing Procedures Manual (CCPM). The CCPM will be available to Commonwealth approved staff on the Knowledge Management Portal (KMP) providing desired transparency into service execution processes. Through the Real-time Dashboard, the Commonwealth will have access to current operational performance of their application infrastructure.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

17 CI Improve or Reduce Cost

17.A Improve/reduce cost of service.

Offeror must provide examples of Windows Support initiatives that have been implemented or can be utilized to achieve reduced costs of Services and to meet or exceeded ROI (Return on Investment) analysis projections.

The Service Excellence Office will proactively manages quality, continuous service improvement, ITIL process management, and customer satisfaction through a comprehensive quality plan that specifically addresses all of these areas. We believe this is a key

differentiator in our partnership with the Commonwealth. Through this new organization and these quality plans, Unisys will drive best in class services and the highest customer satisfaction experience, while reducing overall costs to the Commonwealth.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

Unisys Team Experience

The Unisys Team has a vast experience supporting Windows systems at the Commonwealth and a number of our other customers for a number of years. Some specific examples related to the Commonwealth are listed below.

- **Windows Terminal Server optimization for DOS (Department of State) SURE Voter Registration Environment.** The Unisys Team tweaked, tuned, and optimized the Windows operating systems and terminal server's environment. This improvement and optimization allowed the agency to get more user sessions per servers and provided faster logon and logoff times, more smooth operations using their applications. Currently we are able to get 35 user sessions per server which is an achievement beyond expectations for an application server given the amount of resource allocation.
- **MSSQL Server replication and high availability for an International Logistics Company.** The enterprise environment consisted of many warehouses, car factories, and distribution centers around the nation. Each location had dedicated infrastructure services such as, MSSQL, AD, and TS environment. Challenge was to create a high available SQL server environment in the main office and setup MSSQL server's replication from remote sites to the main office. This provided;
  a. High availability for remote sites.
  b. Almost real time data replication.
  c. Elimination of excessive backup solutions in remote locations.
  d. Significantly reduce SLA penalties. (In car factories, stopping the production line due to IT problem for even a few minutes can result in high SLA penalties. In case of a local site failure, this logic enabled the site to point the systems to the main office in a very short period of time avoiding SLA penalties.)
     - Prior to 2002 at DPW, the first 2 Unisys ES7000/100 systems were used to host application testing environments such as Integration and Systems Acceptance Testing of human services applications as well as other partitions for FTP, SMS and other testing such as Oracle database. Eventually these 2 systems were upgraded via a hardware upgrade to /200 systems. In the summer of 2002, DPW migrated its production HCSIS and Compass human services applications, followed shortly by MCI, from the mainframe over to open systems running on 2 Unisys ES7000/230 systems. The web applications ran in a Microsoft NLB cluster across the 2 ES7000/230 systems. The operating system at the time was Windows 2000 Datacenter Edition. The use of OpenTi by DPW also provided additional benefit and aided in the migration of applications from the mainframe to open systems. OpenTi provided DPW the capability to access both open systems and mainframe databases from the same application program. Never before did they have this capability. All of this paved the way for application migration from the

mainframes to open systems and eventually into the DPH.

- Also around July 2002, DPW began to migrate their Oracle Databases off a Sun 15k system to Unisys ES7000/420 Itanium systems in the DPH. This was the first time DPW utilized Itanium systems and eventually led to the elimination the Sun system and was a first for DPW running Oracle on Windows.

Benefits to the Commonwealth

The Unisys Team's Windows infrastructure design was designed to deliver value to the Commonwealth through the following attributes:

- Standardization – by standardizing on IBM's Flex System platform for Windows, Linux, AIX and Capacity on Demand, the Unisys brings a powerful, cross platform capability to the Commonwealth that simplifies management and provisioning moving forward.
- Efficiency – Utilizing IBM Flex System across multiple platforms drives efficiency into all process, from patch management to service delivery, resulting in year over year efficiency gains that benefit the Commonwealth throughout the length of the contract.
- Manageability – The common IT Service Management platform is leveraged across all hardware platforms, allowing for even more efficiency at the service delivery level. The capability to manage and maintain the full breath of the Commonwealth enterprise in a single, highly integrated toolset will allow the Unisys Team to offer new services in the future to meet changing demands.
- Optimization – Through a rigorous capacity management process and toolset, the Unisys Team will aggressively optimize existing capacity, and allow us to make timely, specific virtualization and consolidation recommendations to the Commonwealth to meet its goal of increased virtualization and to prevent virtual sprawl.
- Automation – The Unisys Team will use the same Enterprise Services Catalog and automated run books to provision and manage Windows systems as all other systems. The tools being deployed allow for increased automation across the enterprise in ways that will directly benefit the Commonwealth.
- Agility – With all the standardization being done, it would be very easy to lose sight of the need for an agile infrastructure. By utilizing a Real-time Dashboard for Windows, Linux and AIX, the Commonwealth will have the ability to quickly reconfigure systems due to changing regulatory frameworks, even down to the ability to isolate workloads on AIX, Windows and Linux within the same chassis, a capability unique in the marketplace. In short, the server infrastructure can be rapidly changed as need to meet challenges in the future.

3.2.4.2 Storage Management

The Storage Management service will provide hosting and operational support Services for storage management systems. Storage management systems must be maintained at current support levels for optimal performance, recoverability, and secure operations. Systems will be located in the Offeror's datacenters. The Offeror must support the hardware and software components of these systems.

The proposed storage management service and solution must address adherence to multiple security and compliance requirements relating to the storage and management of multiple types of data assets (e.g. CHRIA law, criminal history).

Reference Documentation

Exhibit B.1 - DPH - Asset List

Exhibit B.2 - DPH - Commonwealth Owned DPH IT Assets

Exhibit C.1 - DPW - Room 105 and CAO Servers – Storage

Exhibit D.1 - [redacted] - Server Inventory

Exhibit D.2 - [redacted] - Switch Summary

Exhibit D.3 - [redacted] - Storage Summary

Exhibit D.5 - [redacted] - DOT Datacenter Inventory

Exhibit E.1 - DLI - Datacenter Inventory Template

Exhibit F.1 - DOH - Datacenter Inventory Template

Exhibit F.2 - DOH - DPH Asset List

Exhibit F.3 - DOH - DPH COPA Software Asset IBM

Exhibit F.4 – DOH – Physical Servers

Exhibit G.1 - PSP - Datacenter HW Inventory

Exhibit G.3 - PSP - DPH Asset List

Exhibit G.12 - PSP - CHRIA Handbook

Exhibit H.1 - DOR - Datacenter Inventory

Exhibit H.2 - DOR - DPH Asset List

Exhibit H.4 - DOR - SAP TRM System

Exhibit I.1 - IES - DPH COPA Owned IT Assets

Requirements		Describe Compliance
1.	Monitor local operations, troubleshoot and resolve operational issues. Monitor system backup processing on a daily basis. Actively monitor the daily operations of all storage units. Maintain a log for each storage unit. Complete weekly service logs indicating the frequency logs are reviewed, and the status of the daily backup process. Create problem records for any abnormal condition and any repairs that have been made.	Offeror must describe proposed storage management Services. Offeror must identify tools it uses to support data backups including the following: • Processes and Procedures • Tools / Applications • End User Reports o Standard o Custom • Tiered Service/Support Levels • Escalation Procedures
2.	Provide appropriately trained staff that hold current manufacturer certifications for hardware and software technical support (where available). Staff will interact with vendor support Services as needed. Provide Commonwealth with a resume or CV for each operational staff member assigned to this engagement. A copy will be maintained on Offeror file including required background checks and clearances as required.	Offeror must submit a representative sample of staff resumes typically provided for these positions detailing their experience, education, and certifications.
3.	Provide platform level operational and technical support for the computing platform. Provide Level 2 and Level 3 Support to the Service Desk and/or Commonwealth Users. Provide a tiered level of support Services (e.g. Gold, Silver, Bronze)	Offeror must describe its approach to providing and maintaining different tiered levels of support. Offeror must provide a representative sample of available tiered service support Services.

4.	Monitor system backup processing on a daily basis. Review daily backup log for successful completion. Note failures, and correct the problem. Create problem record for any abnormal condition and any repairs that have been made. An automated software process will be utilized to report the completion status of backup processing, with electronic notification of failures sent to identified Commonwealth staff and Offeror technical support for follow up and corrective action.	Offeror must describe its approach to perform an initial review and audit of the backup policies, procedures and reports, to ensure the accuracy of the backup schedules, retention periods, target directories, and recovery point objectives. Offeror must describe its approach to identifying gaps and potential risks, and how those gaps and risks will be resolved.
5.	Ensure network connectivity, and consistent system response times. Identify automated system management tool(s) to ensure storage system availability and expected response times. Stop / Start time records will be a source of input for SLA measurements. Identify tool set(s).	Offeror must describe its real-time monitoring approach and toolset to provide and maintain network availability and performance. Offeror must identify tools it uses to support network availability and performance.
6.	Ensure storage device operating systems are maintained with the current system patch level, including firmware upgrades. Analyze monthly service patches and determine which patches need to be applied. Create a change record, log the update in the storage system log, and install based on maintenance schedule. Notify impacted Commonwealth users immediately of any unscheduled service interruptions via email/web.	Offeror must describe its approach to patch management. Offeror must identify tools used to manage system patches. Offeror must describe its approach for testing and validating updates to the OS and 3rd Party software that it supports. Offeror must describe its approach to communicating unscheduled and scheduled outages, including escalation process.

	The Offeror must document normal work hours and holiday schedules with each agency to determine the contact method and escalation process of each Commonwealth agency. Coordinate at an agency level and account for any required patching as technology upgrades require.	
7.	Utilize data storage conservation techniques such as data de-duplication or other industry standards, to reduce the overall footprint of the data.	Offeror must describe approach and toolset to meet this requirement. Offeror must describe data retention options/Services to store data for extended periods.
8.	Propose options/solutions for self-provisioning or limited self-management of storage as a service.	Offeror must describe approach and toolset to meet this requirement.
Continual Service Improvement		
9.	Reduce service risks.	Offeror must provide methods to eliminate or mitigate service risks.
10.	Improve service quality.	On a quarterly basis, Offeror must also recommend to the Commonwealth team any system changes that would be appropriate to maintain or improve SLA commitments.
11.	Improve client satisfaction.	Offeror must provide examples of previous Offeror initiatives aimed at continually improving client satisfaction.
12.	Ensure service transparency.	Offeror must provide methods and practices to ensure service transparency, providing visibility into service execution.
13.	Improve/reduce cost of service.	Offeror must provide examples of Storage Management initiatives that have been implemented or can be utilized to achieve reduced costs of Services and to meet or

		exceeded ROI (Return on Investment) analysis projections.

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

Introduction

The Unisys solution provides Storage Management through both EMC and IBM storage tools as well as Mainframe-based tools for storage dedicated to the Mainframes. These tools provide Unisys with the means to monitor and manage storage to the Commonwealth's requirements.

The Unisys solution includes the introduction of a highly cost effective Backup software infrastructure from CommVault. CommVault also provides the Commonwealth with a means to integrate the movement of Backup data into Archive storage manageable by the Commonwealth's Records Managers in order to meet regulatory compliance for Records retention.

1 Storage Management Services

1.A Offeror must describe proposed storage management Services.

The Unisys solution provides Storage Management Services within the framework of the Infrastructure Architecture services described in Schedule F, Section 3.2.2.2 (Infrastructure Architecture). The storage tools and components within the Storage Management Services are integrated into the Unisys Nagios collectors. Events within these tools and components will create log events that the Nagios collectors continuously monitor. This integration provides the tight link between Storage Management tools and ITSM monitoring systems. The Nagios collectors will forward events to an event correlation engine that will try to determine the root event and then automatically open an incident ticket. These incidents are tracked and escalated until resolution occurs.

The Commonwealth has benefitted over the years from the innovations and tuning around backup and storage monitoring and managements. Unisys has delivered high availability and access to storage through its innovative methods of using common open source storage monitoring tools such as the SMI-S standard created by the Storage Networking Industry Association, for the Unisys Nagios collectors as well as with proprietary vendor management systems. Unisys is able to use these systems to create proactive alerts through the Unisys incident ticketing system. Unisys uses this method to review logs proactively for incidents and to respond to these before any outages occur. This process lowers the cost of storage management for the Commonwealth because Unisys monitoring systems are continuously tied to events in the system logs rather than relying on a weekly, perhaps perfunctory review of logs by staff. By automating the analysis of exception-based logs Unisys support staff is pulled in quickly as soon as a problem arises.

1.B Offeror must identify tools it uses to support data backups including the following:

Processes and Procedures,

Tools / Applications,

End User Reports (standard and custom), and

Tiered Service/Support Levels

The Unisys solution includes the CommVault Simpana tool to automate the data backup services. This tool is integrated into the Unisys Nagios collectors within the ITSM Services so that abnormal events and backup failures result in incident tickets which are managed to resolution.

The CommVault Simpana tool also produces detailed reporting metrics on data backup activity. This reporting mechanism is integrated to the Real-time Dashboard maintained and managed by ITSM Services. This integration provides deep-level backup reporting to the Services Portals available to Commonwealth service managers and staff who can access these dashboards for up-to-date reporting on the Service Level metrics that roll up into the Commonwealth SLAs for Backups and Restores.

The Unisys solution manages Backup services within the Infrastructure Architecture framework described in F.3.2.2.2 (Infrastructure Architecture).

The available ITSM Capacity, Tiered Service Levels, Tools, and End User Reports that are integrated into the Backup Service components are described in detail in Section 1 of Schedule F, Section 3.2.3.2 (Site Operations).

These are the additional tools provided in the Enterprise Services Catalog for replication services within and between data center locations.

[redacted]

The diagram below illustrates a feature available in the Enterprise Services Catalog that is alluded to in the Commonwealth's Disaster Recovery and Business Continuity requirements: the ability to have 3 copies of synchronized data across various data centers. The Unisys solution assumes that the platinum application availability is achieved by building upon application-based data replication that the application can manage to failover in clustered configurations.

The [redacted] product is proposed to manage the requirements for triple data copies. This configuration shown in **Figure 3.2.4.2-1** can be ordered from the Enterprise Services Catalog and then tested to the Commonwealth's most critical application's failover requirements.

The [redacted] can already provide seamless failovers at the server/host layer for Windows and Linux servers running on [redacted] As the Commonwealth might expect [redacted] puts a high priority on integration testing with all of the product lines from its subsidiary [redacted] and this strategic partnership remains part of the [redacted] long-term strategy of providing increased value in the server and application layers.

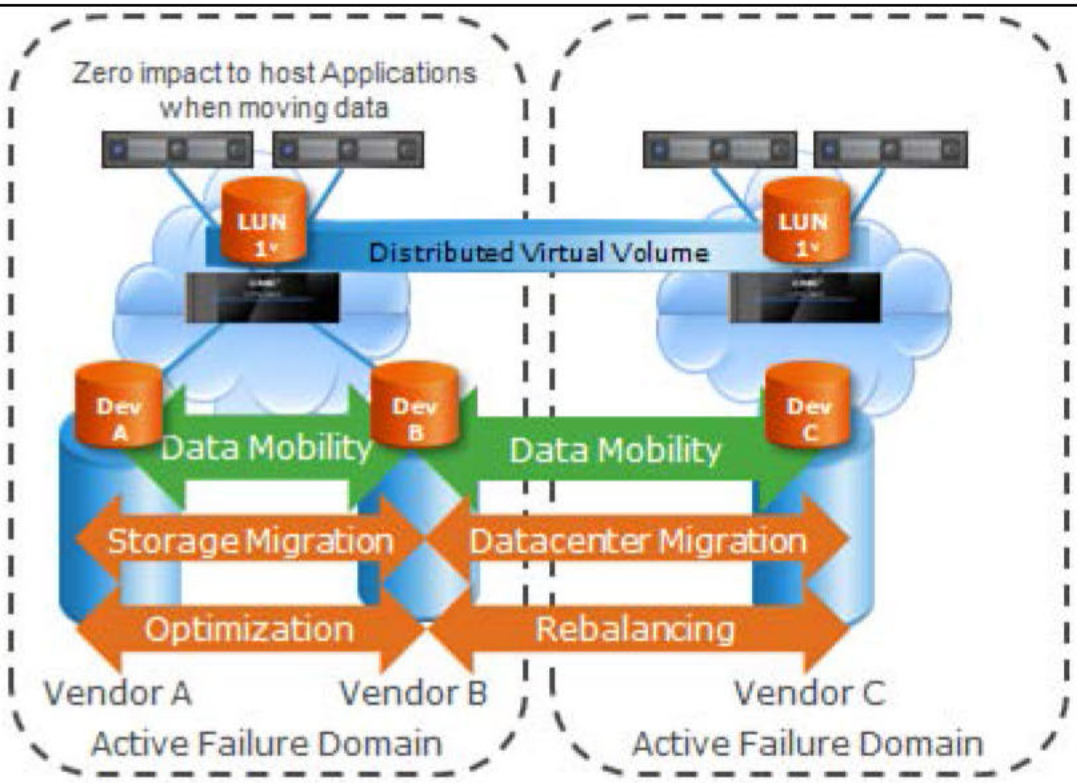


Figure 3.2.4.2-1 - [redacted] Triple Copy

[redacted]: Storage Virtualization and Data Protection

Figure 3.2.4.2-2 illustrates how the [redacted] product will allow the Unisys Team to provide value across heterogeneous storage environments. The Commonwealth can select the [redacted] solution in the Enterprise Services Catalog as well as the [redacted] solution so that Agencies can migrate data into the Unisys-managed data centers and leverage existing storage assets until the end of their service life.

The [redacted] configuration is also the means by which Unisys is able to offer the very fast Recover Time Objectives as well as Recovery Point Objectives that can offer near-zero data loss in the event of a disaster. These offerings are summarized below in Section 5.B as the Tier 5 and Tier 6 Disaster Recovery service offerings.

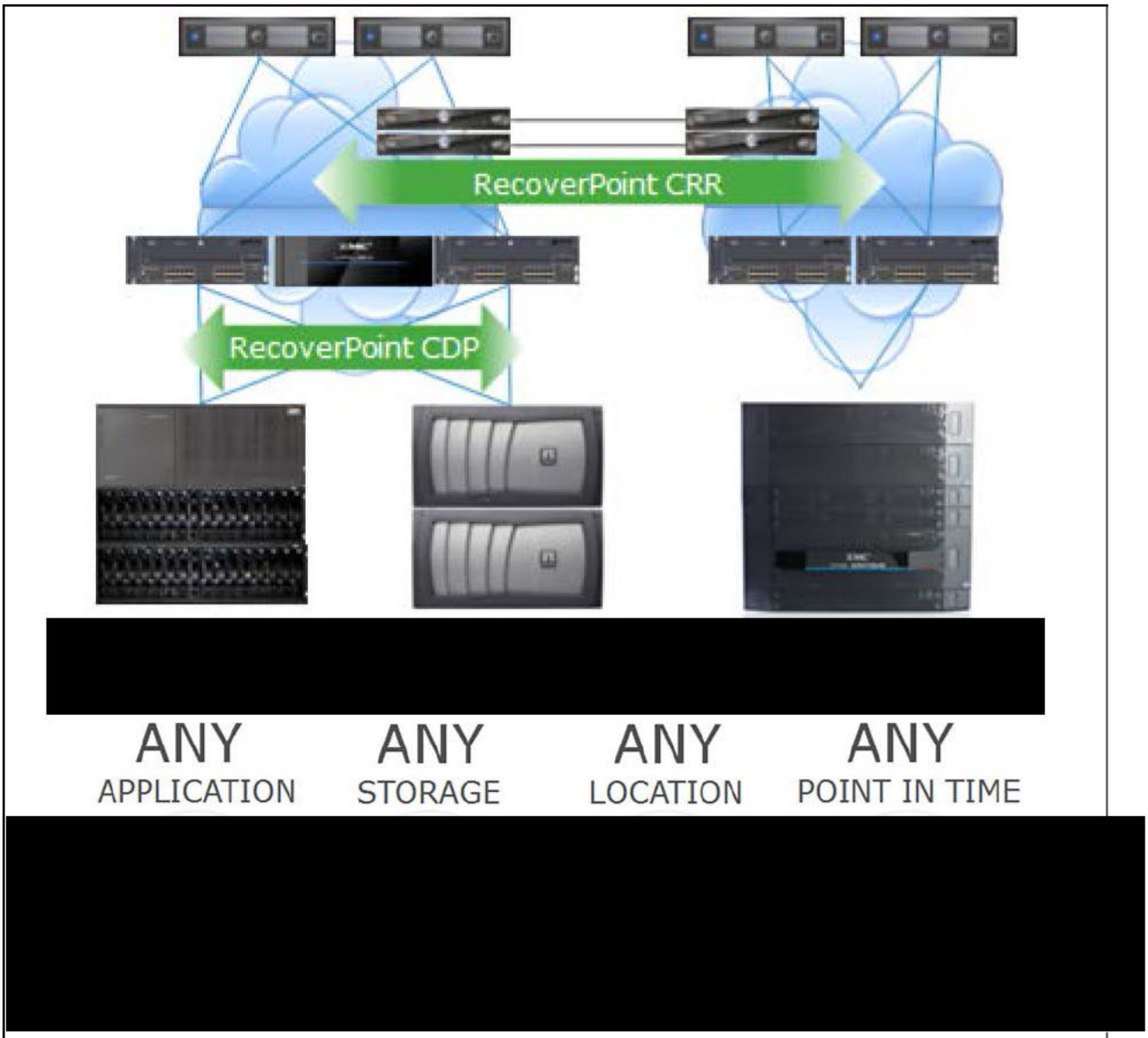


Figure 3.2.4.2-2 [redacted]

[redacted]

Figure 3.2.4.2-3 below shows the failover capabilities of the [redacted] storage platform in the Unisys solution. The modular frames in the Unisys N+1 architecture can be configured in pairs to further increase the reliability and resiliency of the underlying [redacted] infrastructure.

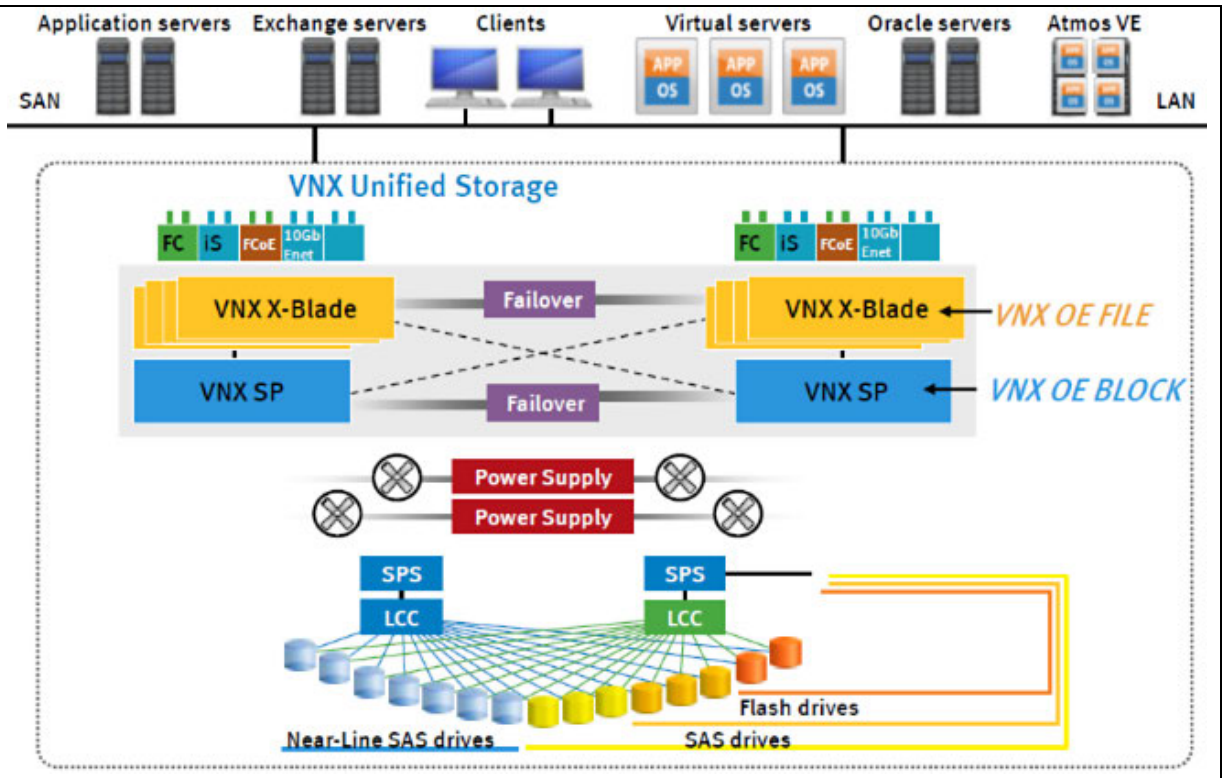


Figure 3.2.4.2-3 - [redacted]

The primary storage trends over the last two decades have reflected the increasing feature sets of mid-tier modular frames. Thus feature sets that customers paid a high premium for in Mainframe-class monolithic storage frames are, over time, refined and offered in the mid-tier frames. No company has been more successful in this storage trend than [redacted] and this accounts for its majority market share in the industry. The [redacted] product series takes advantage of the [redacted], offered within the Unisys solution, to manage communications between servers and storage. This replicates the process that occurs in the storage controllers of large storage frames and allows a pair of separate [redacted] storage frames to appear as a single entity to the servers through [redacted].

[redacted]

The [redacted] illustrated in **Figure 3.2.4.2-4** provides a cost-effective way of integrating diverse storage frames from different vendors and from different frame models from a single vendor and virtualize the storage in a manner that servers are unaware of the storage hardware beneath the [redacted] layer.

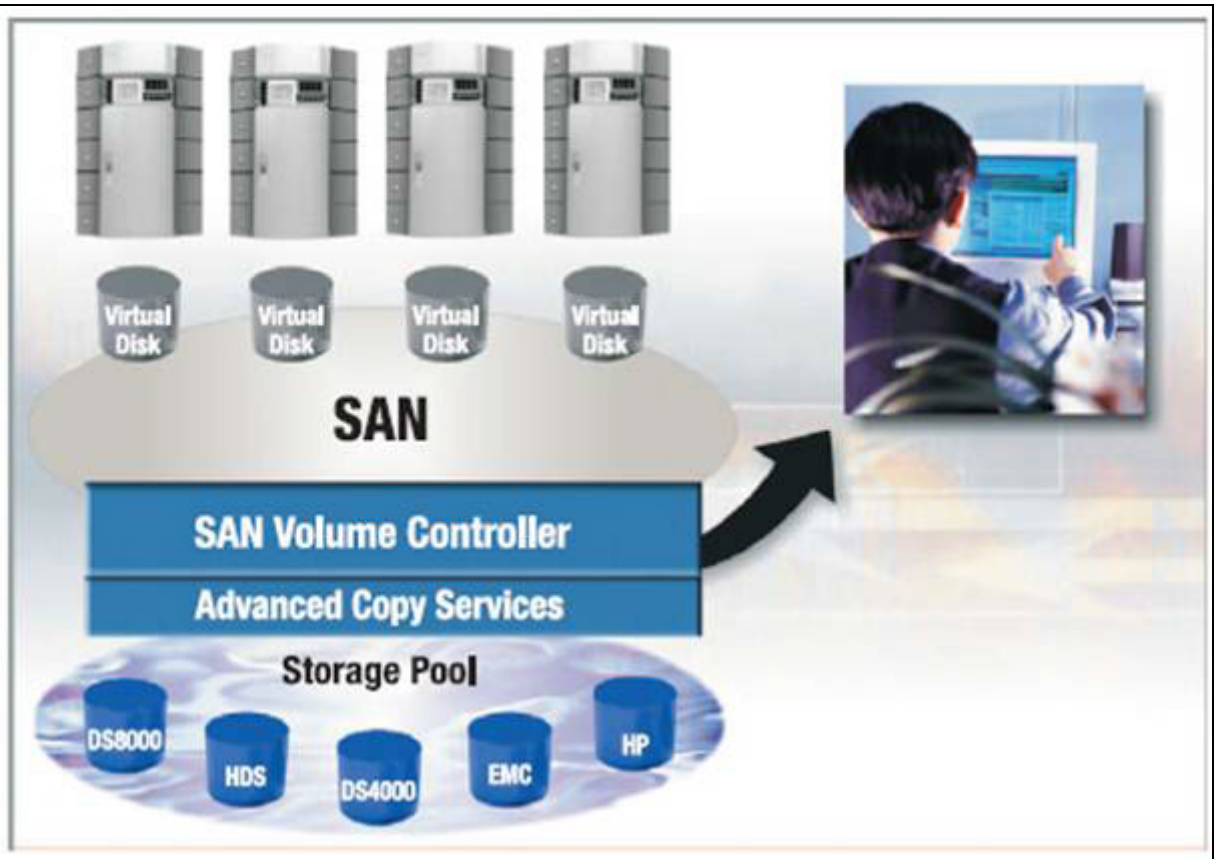


Figure 3.2.4.2-4 - [redacted]

SAN Volume Controller is designed to help increase the amount of storage capacity that is available to host applications. By pooling the capacity from multiple disk systems within the SAN, it helps enable storage administrators to reach beyond traditional islands of SAN storage and deploy storage in ways that can help best meet the needs of host applications.

Because the SVC hides the physical characteristics of storage from host systems, SAN Volume Controller is designed to help insulate host applications from physical changes to the storage pool. This ability can help applications continue to run without disruption as Unisys makes changes to the storage infrastructure. This will increase availability of Commonwealth services because a hardware refresh of storage frames can be conducted without disruption to the Commonwealth's servers providing access to data even when the replaced storage frame has been evacuated of data and unplugged.

End User Reports

- Standard Reports are summarized in 3.3.2.
- Custom Reports are offered by Unisys via the Enterprise Services Catalog

Tiered Service/Support Levels

The Commonwealth of Pennsylvania has indicated in Schedule J.2 - Datacenter Service Level Matrix the desired service tiers/support levels. In the design of the Services and the infrastructure needed to deliver those Service to the Commonwealth, the Unisys Team defined

the Service Tiers to align to those requirements. A fuller explanation and representative sample of all the Services provided in this structure can be found in the response to Section 3.2.1.5 sub-requirement 1.

1.C Escalation Procedures

Escalation procedures will be configured with the Unisys ITSM SLM toolset to support meeting SLA's proactively with automated escalations when incidents are approaching SLA violations. Also, there is a proactive escalation process for incident tickets supported by the Unisys service desk which manages all escalations for normal operations. The Unisys PMO will be involved with any critical escalations as a senior Account Manager will be managing the technical response team and Service Desk communications for critical Priority 1incidents. This includes well defined communications and notifications, status updates, and procedures to support restoring services effectively and efficiently. Escalation procedures are part of the Incident Management Process described in Schedule F, Section 3.2.1.4 Service Desk.

The overall approach for providing daily operations and monitoring including Processes and Procedures, Tools and Applications, End User Reports, Tiered Service/Support Levels and Escalation Procedures is described in Schedule F, Section 3.2.3.2.

1.D Monitor local operations, troubleshoot and resolve operational issues. Monitor system backup processing on a daily basis.

As described in the Facilities Management and Site Operations Schedule F, Sections 3.2.3.1 & 3.2.3.2, Unisys maintains sufficient onsite staff to manage local operations at Unisys-managed facilities. As described above, the backup monitoring is automated in the Unisys solution. In most cases simply re-starting a backup results in a successful backup because needed resources are tied up during peak times but become available a short time later. Unisys automates the restart process automatically. If the restarted backup fails then incident tickets are created to alert the team. Thus critical issues get right to Level 2 and Level 3 support as appropriate.

1.F Actively monitor the daily operations of all storage units.

The Unisys solution automates monitoring of storage units through the integration of ITSM incident ticketing and Nagios collectors which monitor SNMP and SMI-S interfaces on all storage units. Just as with Backup Services anomalies in the storage logs or alerts or warnings about component or service failures automatically created Incident Tickets that are tracked and escalated through the ITSM technical support structures.

1.G Maintain a log for each storage unit.

These logs are maintained on the storage units and a log of exceptions that require intervention are maintained in the Unisys ITSM ticket logging repositories.

1.H Complete weekly service logs indicating the frequency logs are reviewed, and the status of the daily backup process.

The Unisys solution is able to eschew weekly checks of service logs by automating near-instant ticket generations for failures and abnormal activities registered in the system logs.

1.I Create problem records for any abnormal condition and any repairs that have been made.

The Unisys solution creates incident tickets for abnormal conditions and required repairs. The resolution of these tickets provides a record of repairs.

2 Staff, Storage Management Staff Resumes

2.A Provide appropriately trained staff that hold current manufacturer certifications for hardware and software technical support (where available).

Unisys provides trained and certified storage and backup staff for the hardware and software proposed.

2.B Staff will interact with vendor support Services as needed.

Unisys provides the services as part of a standard Level2 and Level3 support services just as ITIL-based processes would stipulate.

2.C Provide Commonwealth with a resume or CV for each operational staff member assigned to this engagement.

Representative resumes for personnel providing Storage and Backup Services are located in the tab marked Rep-Resumes in Section 5.0 Personnel.

2.D A copy will be maintained on Offeror file including required background checks and clearances as required.

Unisys complies.

2.E Offeror must submit a representative sample of staff resumes typically provided for these positions detailing their experience, education, and certifications.

Representative resumes for personnel providing Storage and Backup Services are located in the tab marked Rep-Resumes in Section 5.0 Personnel.

3 Service Desk, Tiered Support

3.A Provide platform level operational and technical support for the computing platform.

Unisys complies.

3.B Provide Level 2 and Level 3 Support to the Service Desk and/or Commonwealth Users.

Offeror must describe its approach to providing and maintaining different tiered levels of support.

As described above, the Nagios collectors in the Unisys ITSM technical support architecture are tightly integrated into the service hardware and software componentry in order to automatically create incident tickets as needed that are tracked and escalated within the Unisys ITSM Service framework until incident resolution.

This process is described in much greater detail in Schedule F, Section 3.2.3.2 Site Operations.

3.C Provide a tiered level of support Services (e.g. Gold, Silver, Bronze)

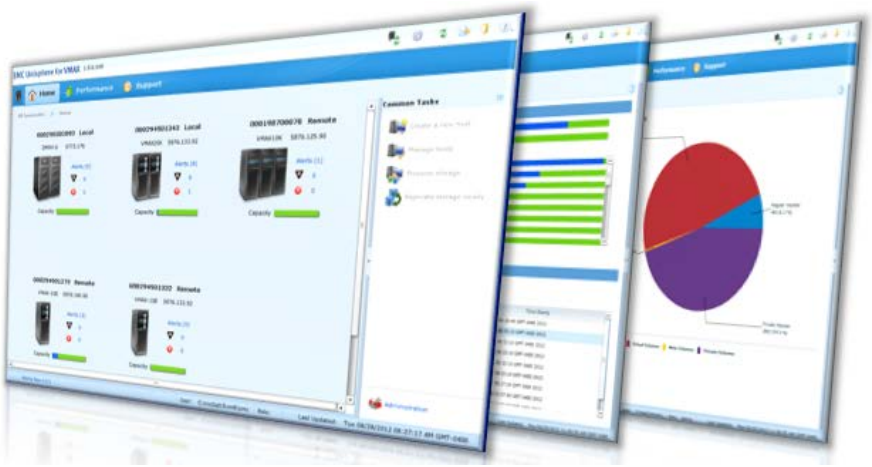
Offeror must provide a representative sample of available tiered service support Services.

The following table highlights the available tiers and associated capabilities.

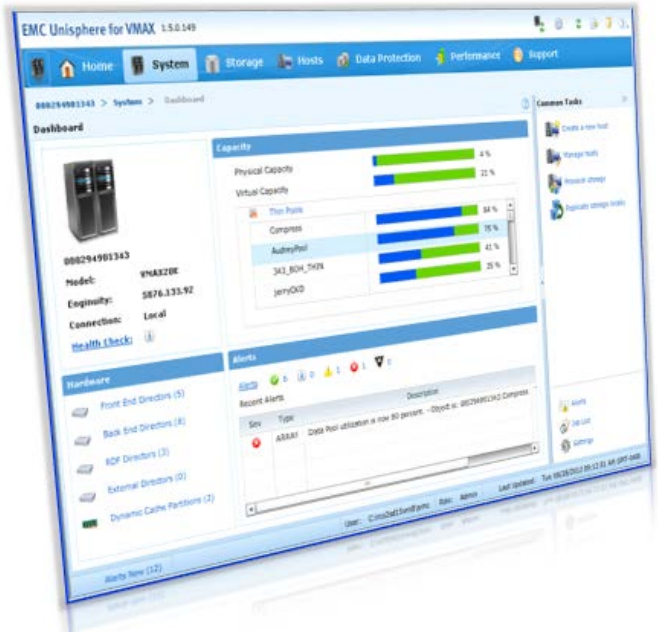
Tiered Support Level	Description
Platinum	• Provides 99.999% Application Infrastructure Availability • Storage frame is monitored via Nagios • Fully Managed Services • Asset Tracked In CMDB **with relationships** • Requires 3 storage frames load balanced and geographically dispersed
Gold	• Provides 99.99% Application Infrastructure Availability • Storage frame is monitoredvia Nagios • Fully Managed Services • Asset Tracked In CMDB **with relationships**
Silver	• Provides 99.9% Application Infrastructure Availability • Storage frame is monitoring via Nagios • Fully Managed Services • Asset Tracked In CMDB **with relationships**
Bronze	• Provides 99.4% Application Infrastructure Availability • Storage frame is monitored via Nagios • Fully Managed Services • Asset Tracked In CMDB **with relationships**
Basic	• Provides 98.5 % Application Infrastructure Availability • Storage frame is monitored via Nagios • Fully Managed Services • Asset Tracked In CMDB **with relationships**
IaaS	• Provides no Application Infrastructure Availability • No Monitoring

	• No Managed Services • Asset Tracked In CMDB **with relationships**

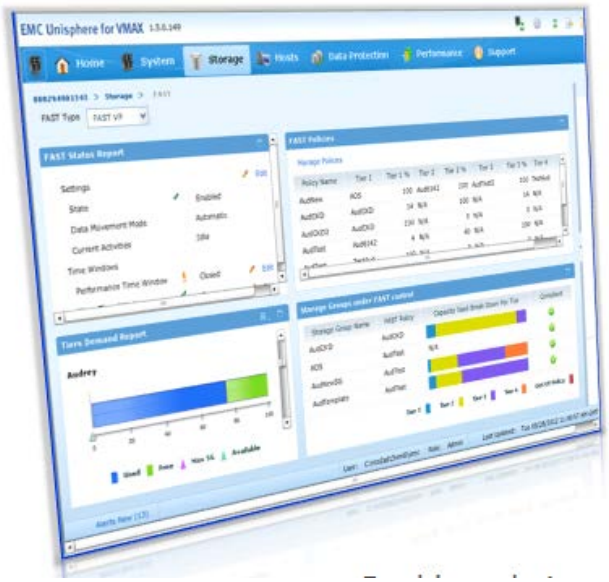
The Commonwealth's storage infrastructure will be managed by tightly integrated [redacted] management toolsets.



The [redacted] provides many feature sets. The array view, shown below, gives administrator quick access to a view of the underlying health of the hardware, capacity utilizations, and any infrastructure incidents.



The [redacted] tool integrates with the [redacted] of tools, as shown below, to provide easy management of storage policies, virtual storage pools, and the use of tiered storage by server groups.



The Unisys solution also provides storage services managed by the [redacted] which provides these services advantages for the Commonwealth:

- Unisys can manage heterogeneous storage from a single point of control
- Unisys technical teams can Move data among virtualized storage systems without disruptions to servers
- Optimize solid-state storage deployments automatically with [redacted]
- Allow for non-disruptive scalability from the smallest configuration to the largest
- Implement stretched configurations for high availability and data mobility between data centers

4 System Backup Review and Audit, Gap Assessment

4.A Offeror must describe its approach to perform an initial review and audit of the backup policies, procedures and reports, to ensure the accuracy of the backup schedules, retention periods, target directories, and recovery point objectives.

The Unisys Team will conduct an initial review and audit of the backup policies, procedures and reports, to confirm the accuracy of the backup schedules, retention periods, target directories, and recovery point objectives. The detailed process for conducting this audit, and how the audit findings will be communicated back to the Commonwealth can be found in Schedule F, Section 3.2.4.2, Subsection 4.

4.B Offeror must describe its approach to identifying gaps and potential risks, and how those gaps and risks will be resolved.

During transition and transformation, the Unisys solution includes an extended onsite presence of a CommVault technical manager who aids the Unisys Team in the search for existing gaps and

risks, along with potential improvements to the backup systems during the transition phase of the solution. This technical expert has extensive experience in implementations and in identifying value-add opportunities. The skills of this technical expert are married to the Unisys Team's extensive expertise around current backup operations. Jointly they lead the transition to the more cost effective CommVault backup infrastructure. The Unisys Team, also working with the CommVault technical manager, manages the review and audit of backup clients that move from the legacy system into the CommVault system. During transition a like-to-like set of backup policies, procedures, reports, schedules, retention periods, target directories, and recovery point objectives are built out. The Unisys Team can then present the Commonwealth for opportunities to further optimize the infrastructure to improve the quality of services or provide better cost efficiencies for the same services.

The Unisys Backup team is also able to compare the Backup inventory of clients and policies to the CMDB inventory to locate "negative" gaps in case a server or critical data set is introduced into the Fully Managed environment and, through unlikely process failures, was not also protected with sufficient backup resources. The Unisys governance processes and the processes generated by the Unisys solution's Enterprise Services Catalog are designed to remove such failures. Additionally, a compare of Backup infrastructure inventory from the backup tools perspective with the CMDB can locate a gap should one occur as an additional level of protection The activities to perform the gap analysis are described in F.3.2.4.2, Requirement 4.

4.C Monitor system backup processing on a daily basis.

As mentioned above, backup system processing is monitored automatically through the integration of Nagios collectors which generate incident tickets and automated runbook procedures upon backup abnormalities that would threaten data protection.

4.D Review daily backup log for successful completion.

4.E Note failures, and correct the problem.

The backup monitoring is automated in the Unisys solution. This reduces the cost of Backup services to the Commonwealth because staff is no longer needed to watch the nightly progress of backups and then intervene when the rare problem arises. In most cases simply re-starting a backup results in a successful backup because needed resources are tied up during peak times but become available a short time later. Unisys automates the restart process automatically. If the restarted backup fails then incident tickets are created to alert the team. Thus critical issues get right to Level 2 and Level 3 support as appropriate.

4.F Create problem record for any abnormal condition and any repairs that have been made.

Incident tickets are created automatically and create a record of abnormal conditions. Following ITIL V3 based processes Level2 and Level3 will review incidents for root causes that create multiple tickets. This identification of problems allows the team to establish workarounds and request architecture reviews as necessary. Repairs are also driven by incident tickets that are automatically generated by the Nagios collectors. Repairs are carried out as part of Incident ticket resolution and are logged following ITIL V3 Change

Management processes.

4.G An automated software process will be utilized to report the completion status of backup processing, with electronic notification of failures sent to identified Commonwealth staff and Offeror technical support for follow up and corrective action.

This is included as part of the CommVault tools as described above in Section 4.D/E.

5 Monitor Network Connectivity, Toolset

5.A Offeror must describe its real-time monitoring approach and toolset to provide and maintain network availability and performance.

Unisys provides event management solutions to help verify network connectivity and consistent system response times. Unisys will utilize automated system management tool(s) to provide real- time monitoring and notification of storage availability and response times including the stop and start times to support SLA availability measurements.

For a complete understanding of how this subset of Event Management Tools supports enterprise Event Management please refer to 3.2.3.2 Site Operations.

5.B Ensure network connectivity, and consistent system response times.

Unisys monitors for continuous network connectivity via network and SAN ports. As is typical with network architecture bandwidth is provided at amounts that generally exceed a normally operating device's ability to put data across the port.

5.C Identify automated system management tool(s) to ensure storage system availability and expected response times. Stop / Start time records will be a source of input for SLA measurements.

The Unisys Nagios collectors interrogate the SAN switch interfaces and create incident tickets upon failures that interrupt access to storage systems and threaten SLAs for availability and response times. These tickets along with the time of resolution provide the input for SLA measurements.

5.D Identify tool set(s).

Offeror must identify tools it uses to support network availability and performance.

The following tools are the major toolsets to support network and system event management and monitoring.

Monitoring Software	Managed Configuration	Monitoring and Management

	Items (CI's)	Functionality
[redacted]	LAN Devices including: • Switches • Routers • Load Balancers • Firewalls	Provides deep network device availability and performance monitoring, DNS, IP address management, network configuration management, and network traffic bandwidth throughput monitoring
[redacted]	Microsoft servers, databases, network devices, and storage hardware.	Provides a standard set of availability, performance and critical service monitors developed by Unisys for monitoring across infrastructure items including: • Servers • Network devices (switches, routers, load balancers) • Storage devices • Middleware • Applications (Exchange, Citrix XenApp, etc.)

6 Patch Management

6.A Ensure storage device operating systems are maintained with the current system patch level, including firmware upgrades.

Offeror must describe its approach to patch management.

Offeror must identify tools used to manage system patches.

The Unisys technical support team will work with the Commonwealth agencies to verify that the storage devices are maintained with the current patch levels including firmware upgrades

Unisys will follow the Change Management Process for applying patches and upgrades. This process will maintain the change record in the Unisys ITSM platform provided by BMC and also update the CMDB configuration management file upon deployment for windows server environment Configuration Items (CI's). The Change Record will be related to the CI's in the CMDB as an audit trail for changes to Windows CI's upon the completion of the Release and Deployment Process for changes.

Due to the criticality of storage components Unisys does not use automation tools for patch updates but relies on the careful attention of trained storage staff to manage each upgrade and reserves the option to require vendors to complete patch upgrades under the supervision of Unisys storage staff.

6.B Offeror must describe its approach for testing and validating updates to the OS and 3rd Party software that it supports.

Unisys approach to testing and validating updates to the OS and 3rd party software is to follow the Release Process for all changes into all production environments. The Release Process includes:

- Change ticket approvals
- Test planning and accepted test results

- Release and deployment planning including release back-out plans
- Release testing for risky deployments
- Early life cycle support to help deliver a successful deployment
- Release back-out for failed releases

The Unisys Team has partner access to the comprehensive battery of tests completed by EMC and IBM for all storage infrastructure components and will use this access to weigh the relative merits and risks associated with version releases. Although quite rare if a security patch for a storage component were released Unisys would propose a revised and potentially accelerated upgrade schedule through the normal change governance schedule so that the Commonwealth holds final approval for such changes.

6.C Offeror must describe its approach to communicating unscheduled and scheduled outages, including escalation process.

Unisys follows the standard ITIL V3 based Change Management governance for all scheduled changes and the ITIL V3 based Incident and Unisys Escalation processes for all unscheduled activity.

6.D Analyze monthly service patches and determine which patches need to be applied.

Monthly services patches rarely occur for storage hardware but Unisys pays close attention to vendor service announcements and will alert the Commonwealth with recommendations for a course of action should these arise.

6.E Create a change record, log the update in the storage system log, and install based on maintenance schedule.

The Unisys ITILV3 based processes for Change Management are strictly followed and include the steps listed above.

6.F Notify impacted Commonwealth users immediately of any unscheduled service interruptions via email/web.

Unisys approach to communicating unscheduled outages is to send notifications to key stakeholders for the Commonwealth/Agencies/Unisys/Third Parties depending on the outage. This will be through email, voice, Services Portal and Remedy broadcast capabilities. The same communications will be used for scheduled outages with additional communications in forward schedules of change reports.

Escalations for unscheduled outages are handled through the standard processes for managing incidents. Unisys service desk will manage all incidents and provide that proper escalation communications to key Commonwealth/Unisys/Third Parties personnel are managed. The BMC [redacted] will also be configured to escalate incident tickets based on incident priorities and SLAs to confirm that incidents tickets are being managed to SLA times for incident response and resolution.

To support the operational and technical support needs of the Commonwealth, the Unisys Team will deploy incident, problem and change management processes that define the flow of support from the Help Desk up through Level 3 support. These processes are closely aligned to the common IT Service Delivery platform. For more detailed information on these processes, please refer to Schedule F, Section 3.2.3.2.

6.G The Offeror must document normal work hours and holiday schedules with each agency to determine the contact method and escalation process of each Commonwealth agency.

Unisys will document and update yearly normal work hours and holiday schedules for each agency. This documentation will be used as a data feed into the operational documentation listing escalation processes and contact methods Unisys is to use when contacting agency personnel.

6.H Coordinate at an agency level and account for any required patching as technology upgrades require.

Unisys complies with the requirement to provide required patching for Fully-Managed components.

7 Data Storage Approach and Toolset

7.A Utilize data storage conservation techniques such as data de-duplication or other industry standards, to reduce the overall footprint of the data.

Offeror must describe approach and toolset to meet this requirement.

Offeror must describe data retention options/Services to store data for extended periods.

Unisys offers the Commonwealth the [redacted] platform and the CommVault suite of backup and archiving software to achieve data de-duplication. In addition Unisys offers the Commonwealth the means to transfer backup data sets from backup-based tape and disk to archive-based disk storage for long term retention and assured deletion at the expiration of the retention cycle. Like the EMC Avamar platform, a proprietary hardware solution, the CommVault offers the Commonwealth a means to utilize de-duplication not only at the target backup media to reduce capacity but also de-duplication at the source of the data the Commonwealth server that is backed up. This latter capacity reduces network load due to backups and speeds up the backup process by using hashed handshakes between backed-up server and the backup server.

Figure 3.2.4.2-5 below shows the basic concepts of CommVault's client and target based deduplication. The client to be backed up tracks all of the blocks that have changed within any file that needs to be backed up. Before sending the backup data it compares these blocks to a hashtable representing blocks that the media agent (aka Backup Server) already has stored. As a result of this source-based deduplication process the client only sends the backup server blocks that it has never seen before from any other client. Thus is five servers store a copy of a company policy document it is only sent to the backup server once, greatly reducing network bandwidth required for backups and also speeding up backups significantly: the faster transfer rates occur for the duplicated blocks that do not have to be sent at all. The Backup Server, with very low CPU processing costs when compared to disk-based controller CPUs does the de-

duplication processing for data that is sent to the backup target media, represented in the illustration as the magnetic library but this could be either a tape-based or disk-based backup media target.

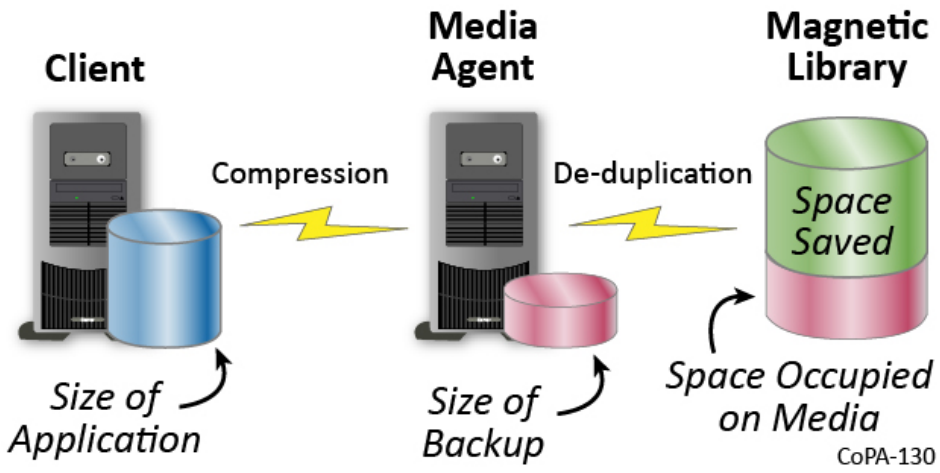


Figure 3.2.4.2-5 – CommVault Data Deduplication

Unisys also considered the option of implementing Thin Provisioning for the Commonwealth because this is an industry-standard tool used to reduce storage foot print although it is not widely used. Thin Provisioning would allow a vendor to report that 2 TBs of storage had been allocated to a server but the server would only be provided with a stub or an IOU that would be filled only as the server began to fill up the space with actual data. However Thin Provisioning also brings with it significant risk of performance impacts. Basically if a vendor has "thin provisioned" 1,000 TBs but has only provided 100TBs of actual disk to meet data requests then the I/O demand on the actual disk provisioned is 10 times greater than if the 100TBs had actually landed on 1,000 TBs of actual disk. Unisys would like to caution the Commonwealth to consider both the billing and performance implications of any solutions that represent "Thin Provisioning" as a significant cost saver: That savings comes with a high I/O performance penalty and removes transparency by disconnecting billing statements based on Thin Provisioned storage from the actual storage hardware and software that provide capacity-based performance.

8 Storage Self Management Service, Toolset

8.A Propose options/solutions for self-provisioning or limited self-management of storage as a service.

Offeror must describe approach and toolset to meet this requirement.

The Services Portal provided in the proposal offers a means for Commonwealth users to submit the most common storage management requests to create new storage, expand or contract existing storage, and tear down no longer needed storage assets. This also applies to requests to insert, modify, add, create or remove backup services at a server by server granularity.

The request and provisioning process for each of the anticipated platforms are as follows:

1. The Commonwealth User (user) will log onto the Services Portal, and select the Enterprise Services Catalog.

2. The Enterprise Services Catalog tool will authenticate and authorize the user
3. Based on what the user is authorized to do, they will be able to select the following:
   a. Storage Quantity
   b. Service Tier – Platinum, Gold, Silver, Bronze, Basic
   c. Storage Services
4. The Enterprise Services Catalog tool's workflow engine will then handle all authorizations for the provisioning.
5. Once approved, the Enterprise Services Catalog tool will open all change records needed to provision a the service request.
6. Once the change record is approved, the Enterprise Services Catalog Tool will run an automated run book for each platform that will provision the service request.
7. The Enterprise Services Catalog tool will then register the change in the following tools as appropriate:

[redacted]

8. Once all provisioning tasks have been performed, the Enterprise Services Catalog tool will notify the user that the storage has been provisioned and is ready for use.

9 CI Service Risk

9.A Reduce service risks.

Offeror must provide methods to eliminate or mitigate service risks.

Continual Service Improvement

Unisys recognizes the significant importance of Quality and Continuous Service Improvement to:

- Reduce service risk,
- Improve service quality,
- Improve client satisfaction,
- Provide service transparency, and
- Improve/reduce costs of service.

Through a continuous cycle of evaluation and improvement within an IT infrastructure, Unisys views quality and continuous service improvement as a critical success factor in driving customer satisfaction for the Commonwealth IT infrastructure. Each of the continuous service improvement areas identified above are driven through the tight integration of the following organizations, industry tools, proven processes and quality deliverables:

- Service Excellence Office,
- Quality Plans: transition and steady state service delivery

- Industry standard frameworks and methodologies: ITIL, ISO, SSL
- Industry accepted measurement tools
- Continuous Service Improvement & Innovation Processes (CSIIP)
- Risk management, audits and business continuity management
- Client Satisfaction Surveys and Knowledge Management Portal

Collectively this represents Unisys Integrated Quality Plan for the Commonwealth of Pennsylvania.

Specifics on each of these areas are outlined in Schedule F, Section 3.2.1.1.6 Continuous Service Improvement. Highlights from this section are outlined below and requested service examples are provided at the end of this section.

9 CI Service Risk

9.A Reduce service risks.

Offeror must provide methods to eliminate or mitigate service risks.

Risk management, independent quality audits, and business continuity management are integral quality management processes. Unisys is committed to managing risks and facilitating the achievement of business objectives the adherence to quality processes. We mitigate risk through the implementation of tight quality controls: standard policies, procedures, roles, risk assumptions, issues, and definitions, etc.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

10.A Improve service quality.

On a quarterly basis, Offeror must also recommend to the Commonwealth team any system changes that would be appropriate to maintain or improve SLA commitments.

The quality approach begins with the Service Excellence Office who provides definition and oversight of all ITIL process management and analysis functions. Process managers and analysts working in the Service Excellence Office are responsible for auditing process effectiveness, ensuring that service delivery teams comply with proper execution of processes, and analyzing process trends for anomalies. Continuous service improvement programs in collaboration with Commonwealth agencies are managed by the Service Excellence Office.

Through our Continuous Service Improvement and Innovation Process (CSIIP), the SEO reviews, analyzes and makes recommendations on improvement opportunities in each ITIL lifecycle phase. Unisys will leverage Six Sigma Lean tools and methodologies as well as ISO Certified internal audits to measure and maintain the highest quality services to the Commonwealth.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional

details in this area.

11 CI Client Satisfaction

11.A Improve client satisfaction.

Offeror must provide examples of previous Offeror initiatives aimed at continually improving client satisfaction.

Client satisfaction is extremely important to Unisys and a key focus in our IT solution. The SEO will integrate new agencies, customers and services into our multi-pronged client satisfaction approach that includes Service Desk surveys on the caller's experience, an overall agency satisfaction survey, and quarterly surveys with the Office of Administration. Data collection will be gathered across multiple levels to gain a clear understanding of the Commonwealth's satisfaction with the IT Services being provided.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

12 CI Service Transparency

12.A Ensure service transparency.

Offeror must provide methods and practices to ensure service transparency, providing visibility into service execution.

The service organizations will use standardized ITSM services processes, IT monitoring and automation tools. ITSM processes will be documented in the Commonwealth Computing Procedures Manual (CCPM). The CCPM will be available to Commonwealth approved staff on the Knowledge Management Portal (KMP) providing desired transparency into service execution processes. Through the Real-time Dashboard, the Commonwealth will have access to current operational performance of their application infrastructure.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

13 CI Reduce Cost of Service

13.A Improve/reduce cost of service.

Offeror must provide examples of Storage Management initiatives that have been implemented or can be utilized to achieve reduced costs of Services and to meet or exceeded ROI (Return on Investment) analysis projections.

The Service Excellence Office will proactively manages quality, continuous service improvement, ITIL process management, and customer satisfaction through a comprehensive quality plan that specifically addresses all of these areas. We believe this is a key differentiator in our partnership with the Commonwealth. Through this new organization and these quality plans, Unisys will drive best in class services and the highest customer satisfaction experience, while reducing overall costs to the Commonwealth.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

A few examples of Storage Management Continuous Service Improvement that have been implemented or can be utilized to achieve reduced costs of Services and to meet or exceeded ROI (Return on Investment) analysis projections are outlined below:

Storage Management

The DPH has implemented Distributed File Systems (DFS) to replicate our DPH File Server down to [redacted] In the event of a true disaster, files to perform our duties during and after the DR will be available. Data replication occurs in real time and is de-duplicated over the wire thus saving bandwidth on the WAN link. This confirms that our documentation, recovery scripts and procedures are current and accessible at all times to support Commonwealth agencies during disaster recovery drill and in the event of an actual disaster. By avoiding having to ship tapes containing this information to [redacted] and having to restore them, Unisys has improved the recovery time objective for disaster drills and disaster events.

Storage Management

As part of the DPH's continuing improvements in its backup infrastructure, the DPH has improved the successful recovery an 8TB database archive for IES from 10.7 hours down to nearly 4 hours by improving the bandwidth from .75Tb/hour to 2TB/hour. The DPH accomplished this by bypassing the AIX VIO Shared Ethernet Adapter (SEA) built in restrictions and optimizing throughput between the media servers and the data domain.

Storage Reporting - Service Level and Other Reports:

Throughout the contact, Unisys has provided a vast amount of contractual reporting to the Commonwealth. The reports include, but are not limited to Monthly Performance Reporting for each supported agency/bureau, Major reporting improvements include, Quarterly Vulnerability Reporting, Monthly XIV Storage Reporting for IES and DOR physical hosts, Monthly Storage Reports for PLCB, Monthly VMAX Storage Reports for DPW.

Storage SAN Advances:

Through advanced configuration and deployment of an Avamar grid the DPH is capable of replicating deployments of virtual servers between data centers. This capability is also leveraged for several disaster recovery scenarios including initial DR deployments and annual disaster recovery drills.

Storage Replication for DR:

Storage replication solutions have been implemented for several agencies using the latest disk to disk replication technology. These solutions have enabled a reduced dependency on tape media and drives for backup while providing a disk to disk update to offsite data supporting both data backup as well as disaster recovery requirements. Ongoing research and trials are conducted in conjunction with product support organizations to provide proper configuration and optimal performance for the technology supporting this critical managed service.

Disk-based Backup Strategy:

The Unisys solution leverages Data Domain products to facilitate disk-based backups and data

replication to an offsite location. This eliminates cost and unreliability associated with tape media and significantly expedites recovery time in the event of a disaster. The implementation of a disk to disk with data de-duplication strategy for IES resulted in a significant reduction in backup and restore times for the extremely large, rapidly growing SAP data store. At the time that IES migrated to the DPH, the data store in SAP was 5 TB. This data store had previously been backed up across 32 tape drives taking close to five hours to back up. This left IES exposed to issues with tape media that would prevent the ability to restore effectively. Since their implementation, the size of the SAP data store peaked at 9 TB with performance on the disk-based backup solution enabling completion of backups in less than four hours.

Unisys Team Experience

The Unisys Team experience is outlined in the above section.

Benefits to the Commonwealth

The Unisys Backup Service provides significant costs savings over those offered by competitors. Unisys has teamed with CommVault which is quickly displacing its competitors in market share due the high value provided by their solution at cost competitive rates. The Commonwealth also benefits from CommVault's strategic decision to expand its customer base within the state government market.

The Unisys solution for Storage Management provides interoperable, innovative automation and integration between the Unisys ITSM monitoring and management and the standard management tool suites offered by EMC, IBM, and CommVault. This innovation allows the Unisys ITSM technical support staff to remove costly labor-based monitoring and escalation and provide the Commonwealth with more cost effective solutions.

The Unisys integration of ITSM monitoring and management tools with logging and alert features provided by EMC, IBM, and CommVault also provides a higher quality of services for the Commonwealth by automating incident ticket creations to engage technical staff proactively. The ITSM monitoring of event logs within Infrastructure components can create incident tickets on an initial logged event before the event cascades into a service disruption.

3.2.4.3 ERP Hosting – SAP / Oracle

ERP Hosting – SAP service will provide hosting and operational support Services for two SAP-ERP systems that are currently located at the DPH. One system Services the General Accounting System application, and the other Services the Integrated Tax System application for the Department of Revenue. Each application has associated development and testing environments support on segregated equipment. Offeror must support various production and non-production versions of the applications and the associated hardware. The roles and the number of staff members required to perform the below listed tasks will be determined by the Offeror.

Due to the critical and complex nature of these SAP environments, the Commonwealth requires an experienced SAP hosting provider. The Offeror's proposed target infrastructure design for the Commonwealth's SAP environments must include a certified SAP sizing report prior to migration of the systems.

The ERP Hosting – Oracle service will provide hosting and operational support Services for the current Oracle Enterprise system utilized by the Pennsylvania Liquor Control Board (PLCB). The application has associated development and testing environments support on segregated equipment. Offeror must support various production and non-production versions of the applications and the associated hardware.

Reference Documentation

Exhibit H.4 - DOR - SAP TRM System

Exhibit I.1 - IES - DPH Commonwealth Owned IT Assets

Exhibit I.2 - IES - Application Inventory

Exhibit I.3 - IES - DPH Commonwealth Software Asset Unisys

Exhibit I.4 - IES - DPH September 2012 Measurement Report

Exhibit B.2 - Commonwealth Owned DPH IT Assets (see PLCB Oracle systems)

Requirements		Describe Compliance
1.	Provide ERP Hosting Services for SAP and Oracle based applications.	Offeror must describe its approach to providing ERP Hosting Services for both SAP and Oracle ERP systems. Offeror must provide a minimum of 3 verifiable Customer References of customers that use its SAP Hosting Services. Offeror must provide a minimum of 3 verifiable Customer References of

		customers that use its Oracle Hosting Services.
2.	Monitor local system operations, troubleshoot and resolve operational issues. Actively monitor the daily operations of all ERP systems. Maintain a log for each server detailing hardware / software configuration and critical service operations. Document review of the system logs on a weekly basis to ensure critical system Services are processing without errors. Complete weekly server log indicating which logs were reviewed, date and initial the log.	Offeror must describe its approach to monitoring and maintaining SAP and Oracle ERP systems including the following: • Processes and Procedures • Tools / Applications • End User Reports o Standard o Custom • Tiered Service/Support Levels • Escalation Procedures
3.	Monitor system backup processing on a daily basis. Review daily backup log for successful completion. Note failures, and correct the problem. Create problem record for any abnormal condition and any repairs that have been made. An automated software process will be utilized to report the completion status of backup processing, with electronic notification of failures sent to Offeror technical support, and identified Commonwealth staff for follow up and corrective action.	Offeror must describe its approach to perform an initial review and audit of the backup policies, procedures and reports, to ensure the accuracy of the backup schedules, retention periods, target directories, and recovery point objectives. Offeror must describe its approach to identify gaps and potential risks, and how those gaps and risks will be resolved.
4.	Provide IBM, SAP, and Oracle trained staff holding current manufacturer certifications for hardware and software technical support. Staff will interact with vendor support Services when	Offeror must submit a representative sample of staff resumes typically provided for these positions detailing their experience, education, and certifications.

	needed. Provide Commonwealth with a resume or CV for each operational staff member assigned to this engagement. A copy will be maintained on Offeror file including required background checks and clearances as required.	
5.	Provide cost effective operational and technical support for the computing platform. Provide Level 2 and Level 3 Support to the Service Desk and/or Commonwealth Users. Provide a tiered level of support Services (e.g. Gold, Silver, and Bronze).	Offeror must describe its approach to providing and maintaining different tiered levels of ERP (SAP & Oracle) support.
6.	Ensure network connectivity, and consistent system response times. Utilize automated system management tool(s) to ensure real-time monitoring and notification of server availability and response times. Stop / Start times of servers will be a source of input for SLA measurements. Identify tool set(s).	Offeror must describe its real-time monitoring approach and toolset to provide and maintain network availability and performance. Offeror must identify tools it uses to support network availability and performance.
7.	Ensure server operating systems are maintained with the current system patch level, based on the Services provided by the server. Analyze monthly service patches and determine which patches need to be applied, by server type. Create a change record, log the update in the server log, and install based on server maintenance schedule. Implement a Patch Management Program to ensure the timely	Offeror must describe its approach to patch management including analysis, communications, schedule (change records) and installation process. Offeror must describe its approach for testing and validating updates to the OS and 3rd Party software that it supports. Offeror must describe its approach to communicating unscheduled and scheduled outages, including its escalation process.

	application of updates on all infrastructure platforms in accordance with Commonwealth IT policy guidelines.	
8.	User Account Management Provide certified system administration staff to create and maintain the registration of profiles, associated groups, and the security permissions required to service the approved client base of the system and application.	Offeror must describe its administration/support approach and provide representative resumes.
9.	Procurement Planning Provide program and process to refresh the hardware at asset end-of-life, and when upgrades are needed to meet anticipated growth in utilization.	Offeror must describe its program and processes for upgrading systems.
10.	SLA Reporting Collect actual system availability, utilization and response time data. On a monthly basis, Offeror must create a SLA report for the Commonwealth and Vendor Management teams.	Offeror must describe its processes and toolset for monitoring and maintaining service levels. Offeror must provide a representative sample of its SLA reports for ERP hosting Services.
Continual Service Improvement		
11.	Reduce service risks.	Offeror must provide methods to eliminate or mitigate service risks.
12.	Improve service quality.	On a quarterly basis, Offeror must also recommend to the Commonwealth team any system changes that would be appropriate to maintain or improve SLA commitments.
13.	Improve client satisfaction.	Offeror must provide examples of

		previous Offeror initiatives aimed at continually improving client satisfaction.
14.	Ensure service transparency.	Offeror must provide methods and practices to ensure service transparency, providing visibility into service execution.
15.	Improve/reduce cost of service.	Offeror must provide examples of ERP Hosting initiatives that have been implemented or can be utilized to achieve reduced costs of Services and to meet or exceeded ROI (Return on Investment) analysis projections.

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

Introduction

Many of the Commonwealth's Agencies use ERP systems from SAP and Oracle to provide critical services within the Commonwealth or to their constituents. The Unisys Team will provide an ERP hosting service based upon the infrastructure support services provided for the Windows, Linux, AIX, Storage and Backup hosting services. Due to the unique application requirements for each ERP implementation, Unisys will work with each agency to confirm that the design and implementation of the infrastructure to support each ERP system meets the agency and application requirements.

As part of the ERP Hosting service, the Commonwealth benefits from data center compute services supporting multiple production and non-production application environments. These environments used for production, development, and test will use segregated hardware for each of the following ERP services leveraging the compute services' flexible and cost effective architecture.

- IES – SAP - General Account System
- DOR – SAP Treasury and Risk Management – Integrated Tax System
- PLCB – Oracle Enterprise

The Unisys Team includes support staff with experience managing complex infrastructure deployments for both SAP and Oracle environments. The support team maintains certifications with ongoing training for infrastructure support including Microsoft Windows, [redacted] storage products, and IBM AIX. In addition, the support team has access to the vendor's support organizations for SAP, Microsoft, [redacted] Oracle IBM, and [redacted]

During the transition planning activities for the migration of the SAP environments from the DPH, Unisys will work with the hardware vendors to provide an SAP sizing report. This report

will be used to validate that the server infrastructure planned in the new facility will meet the current requirements of the existing implementation.

1 ERP hosting Service Approach

1.A Provide ERP Hosting Services for SAP and Oracle based applications.

Offeror must describe its approach to providing ERP Hosting Services for both SAP and Oracle ERP systems.

For the Commonwealth ERP Hosting Service for SAP and Oracle, Unisys will use similar technologies and services provided for the Windows, Linux, AIX, Security and Storage services. By using similar technologies and services, the Unisys Team can provide access to a broad set of capabilities and flexibility to support the ERP infrastructure. Unisys also recognizes that ERP systems have unique requirements and will structure the ERP services to meet those requirements, such as using SAP and Oracle authorized patches, segregated infrastructure and recommended designs by SAP or Oracle.

1.B Offeror must provide a minimum of 3 verifiable Customer References of customers that use its SAP Hosting Services.

The Unisys Team provides SAP Hosting services for the following customers:

- IES SAP Enterprise System
  The Commonwealth was one of the first states to fully-integrated business processes in a SAP Enterprise Resource Planning (ERP) system across all state agencies. First implemented in 2002, the SAP ERP system efficiently and securely supports more than 53 state agencies and processes millions of finance, budget, procurement, supplier relationship, plant maintenance, payroll, travel, human resource and employee self-service transactions monthly. The Commonwealth's Bureau of Integrated Enterprise System (IES) migrated the SAP ERP system to the DPH in 2010 and has entrusted Unisys with the care of its supporting infrastructure since that time
- DOR SAP Integrated Tax System
  In 2011, the Department of Revenue (DOR) began a project to implement an Integrated Tax System to replace, update, and augment many of the current tax management systems used by the agency. DOR selected SAP's Treasury and Risk Management platform as the basis for the platform and had the system deployed within the DPH to have its infrastructure supported by Unisys. Unisys continues to work with DOR to add additional infrastructure as DOR implements additional functions and services as part of the agency's migration to an integrated platform.
- World Leading Brewery Company
  In 2007, a world's leading brewery company engaged Unisys as a partner to implement a common SAP HCM ECC 6.0 deployment across 30+ countries over a 5 year period and provide ongoing support. The program included the design and standardization of global employee HR Processes and integration with other corporate tools. The result of the program was a 20% reduction in the cost of maintenance by the IT organization through the use of an approach of one platform, and one framework using uniform processes and data across the enterprise.

1.C Offeror must provide a minimum of 3 verifiable Customer References of customers that use its Oracle Hosting Services.

The Unisys Team provides Oracle Hosting services for the following customers:

Pennsylvania Liquor Control Board (PLCB) Enterprise Resource Planning (ERP)

The Commonwealth of Pennsylvania supports and monitors all the retail and wholesale operations of State liquor sales. The PLCB ERP Phase I environment initially deployed 15 AIX LPARS into the DPH on IBM P6 570 servers in 2009. The effort continued through a Phase II deployment which brought in an additional 40 LPARS along with management servers and a storage device into the DPH. All statistical and financial data for PLCB are processed on the environment at the DPH.

In addition, the PLCB deployed a new point-of-sale application – SkillNet in 2011. This deployment brought all of the cash register processing into the DPH via SUSE Linux on virtual machines. The PLCB operates over 620+ Wine and Spirit stores and contributes over $500 million dollars per year to the PA General Fund.

During 2012, the ERP suite was rebranded to Integrated Business Management System (IBMS). The DPH assisted in the application deployment of this major upgrade to the PLCB in February of 2013. This upgrade also brought the introduction of Linux virtual machines into the DPH which captures the retail data warehouse (RDW) transactions, retail demand forecasting (planning), Oracle internet directory, Hyperion (statistical information) and an Oracle WebCenter.

California State University

Since 2001, California State University (CSU) has entrusted their Oracle PeopleSoft Higher Education environment's infrastructure support to Unisys. Unisys provides infrastructure hosting services from our Salt Lake [redacted] data center. As part of the 2011 renewal, Unisys added flexibility to scale the services with consumption based model to support CSU's business needs and activities as well as provides test, development and disaster recovery infrastructure from Unisys [redacted] Data Center.

United Kingdom Ministry of Justice

Since 1998, Unisys provides Oracle Financials hosting and application support for the United Kingdom Ministry of Justice as part of business process outsourcing program with Liberata. Unisys provides 2nd and 3rd level support for the compute services as well as the Oracle applications and related services. Unisys maintains the platforms to current levels, implements additional functionality such as Hyperion Reporting, and tests the latest releases with the Ministry's stake holders.

2.A Offeror must describe its approach to monitoring and maintaining SAP and Oracle ERP systems including the following:

Processes and Procedures,

Tools / Applications,

End User Reports (Standard and Custom),

Tiered Service/Support Levels, and

Escalation Procedures

Monitor local system operations, troubleshoot and resolve operational issues.

Actively monitor the daily operations of all ERP systems.

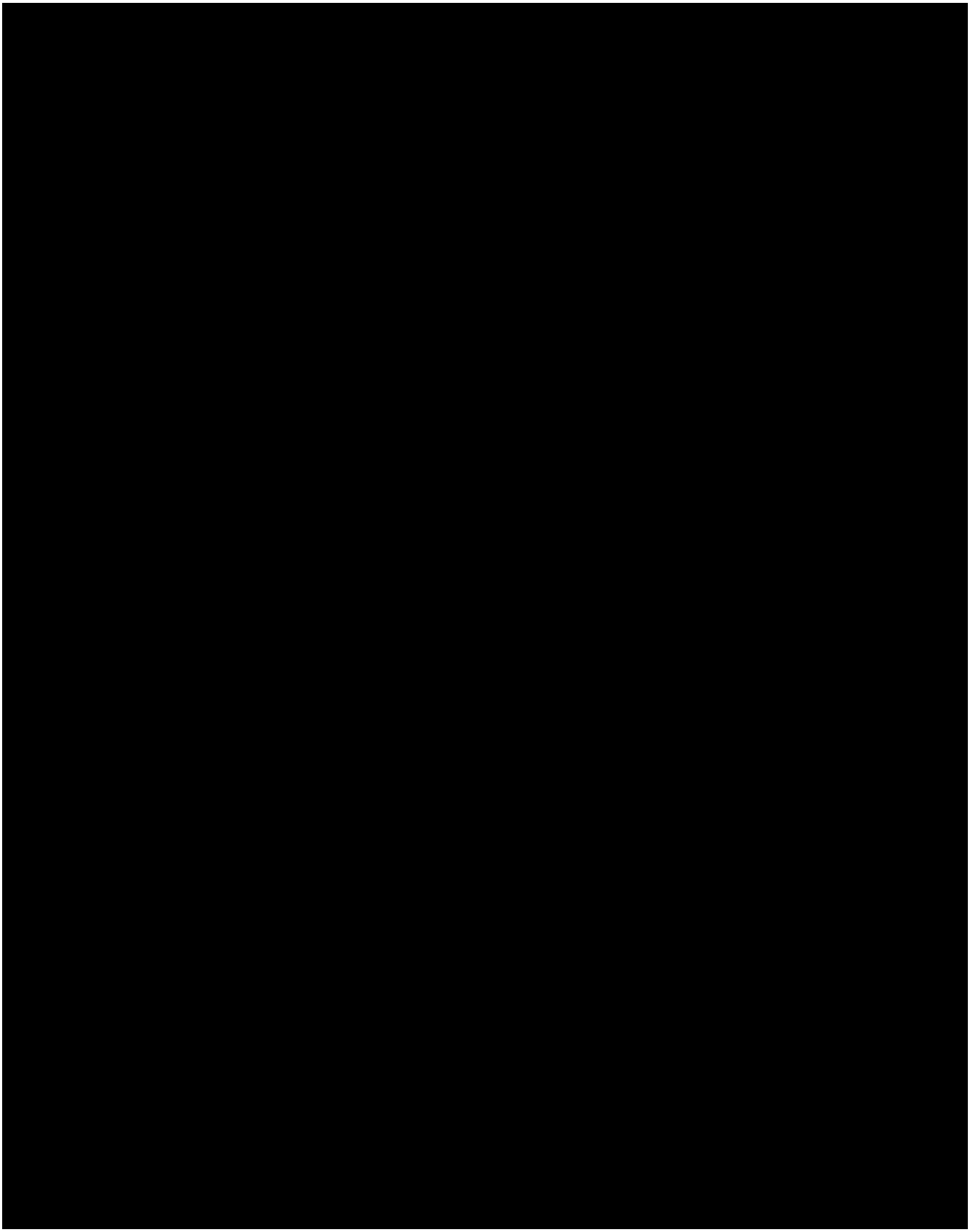
Unisys will provide hosting and operation support services to the Commonwealth of Pennsylvania for SAP and Oracle ERP systems operating on required versions of AIX, Linux, and Windows systems at the Commonwealth's [redacted] and Unisys data centers. Staffing required to perform the operational tasks listed below will be US based Unisys Team personnel both on-site and remote to the data centers.

a. ***Processes and Procedures.*** The processes and procedures for providing SAP and Oracle ERP system managed Compute Services will be documented in the CCPM which will be reviewed and approved by the Commonwealth. The scope of these processes and procedures will be based on the ITIL framework as well as technology best practices for support of Windows, AIX, Linux, Storage, Backup, and Network platforms, including infrastructure support best practices recommended by SAP and Oracle.

b. ***Tools/Applications.*** Unisys has outlined the complete approach to monitoring operations and supporting automated remediation over time from a common enterprise infrastructure platform across all technical towers for the Commonwealth in F3.2.3.2 Site Operations. The following is an overview of how all platforms, including the SAP and Oracle ERP Compute Services environments, will be monitored and managed.

The Integrated Unisys ITSM Management Platform software tools are summarized in **Figure 3.2.4.3-1.**

[redacted]



[redacted]

Figure 3.2.4.3-1 - Unisys ITSM Tools

c. *End User Reports*

The Unisys Team will provide common End User Reports for the ERP systems. The overall approach for end user reports is described in Schedule F, Section 3.2.3.2. Custom Reports are offered by Unisys via the Enterprise Services Catalog

d. Tiered Service/Support Levels

The Commonwealth of Pennsylvania has indicated in Schedule J.2 - Datacenter Service Level Matrix the desired service tiers/support levels. In the design of the Services and the infrastructure needed to deliver this Service to the Commonwealth, Unisys defined the Service Tiers to align to those requirements. A detailed explanation and representative sample of all the Services provided in this structure can be found in the response to Schedule F, Section 3.2.1.5 sub-requirement 1.

Tiered Support Level	Description
Platinum	• Provides 99.999% Application Infrastructure Availability • Server is monitoring via Nagios • Fully Managed Services • Asset Tracked In CMDB • Requires 3 servers load balanced and geographically dispersed
Gold	• Provides 99.99% Application Infrastructure Availability • Server is monitoring via Nagios • Fully Managed Services • Asset Tracked In CMDB • Requires 2 servers load balanced
Silver	• Provides 99.9% Application Infrastructure Availability • Server is monitoring via Nagios • Fully Managed Services • Asset Tracked In CMDB
Bronze	• Provides 99.4% Application Infrastructure Availability • Server is monitoring via Nagios • Fully Managed Services • Asset Tracked In CMDB

Basic	• Provides 98.5 % Application Infrastructure Availability • Server is monitoring via Nagios • Fully Managed Services • Asset Tracked In CMDB

e. Escalation Procedures.

Escalation procedures will be configured with the Unisys ITSM toolset to support meeting SLA's proactively with automated escalations when incidents are approaching SLA violations. Also, there is a proactive escalation process for incident tickets supported by the Unisys service desk which manages all escalations for normal operations. The Unisys PMO will be involved with any critical escalations as a senior Account Manager will be managing the technical response team and Service Desk communications for critical Priority 1incidents. This includes well defined communications and notifications, status updates, and procedures to support restoring services effectively and efficiently. Escalation procedures are part of the Incident Management Process described in F3.2.1.4 Service Desk.

The overall approach for providing daily operations and monitoring including Processes and Procedures, Tools and Applications, End User Reports, Tiered Service / Support Levels and Escalation Procedures is described in Schedule F, Section 3.2.3.2.

2.B Maintain a log for each server detailing hardware / software configuration and critical service operations.

Each server supported by the Unisys Team, including the SAP and Oracle ERP servers, will have their hardware and software configurations tracked within the Configuration Management Database (CMDB) and discovered with Atrium Discovery and Dependency Mapping (ADDM). By using an online CMDB with discovery, the Commonwealth benefits from having consistent data on the configurations which can be reported on an as needed basis versus maintaining a manual configuration log.

2.C Document review of the system logs on a weekly basis to ensure critical system Services are processing without errors.

The Unisys Team will collect each server's system logs and using the log management tool's report management functions, validate that critical system services are operating correctly on a weekly basis. In addition to the weekly review, the log management tool is integrated with the Enterprise System Management (ESM) toolset to automate notification of errors and events identified within the logs. As part of the notification, for system services operating with errors, an incident ticket will be created.

2.D Complete weekly server log indicating which logs were reviewed, date and initial the log.

The Unisys Service Delivery Manager will complete a weekly server log indicating which logs were reviewed, date and initial the log. A copy of this log will be made available to the Commonwealth on the Real-time Dashboard for review. These logs will be retained for one

year.

3 System Backup Systems Review and Audit

3.A Monitor system backup processing on a daily basis.

During Steady State operations for Fully Managed servers, the CommVault backup system processing is monitored automatically through the integration of Nagios collectors which generate incident tickets and automated run book procedures upon backup abnormalities that would threaten data protection. This provides reliability in the daily backup processes by addressing run-time issues.

3.B Review daily backup log for successful completion.

Note failures, and correct the problem.

Create problem record for any abnormal condition and any repairs that have been made.

The Unisys Team's solution automates the monitoring of backup logs. Appropriate support personnel are notified to address failures through the ITSM system and corrective actions are taken. Successful backups are reported daily.

Unisys support staff are trained to identify patterns of failure that result in incidents and, following ITIL V3 processes, escalate these to the status of a problem with applicable workarounds and final resolutions. Repairs are carried out as part of Incident ticket resolution and are logged following ITIL V3 Change Management processes.

3.C An automated software process will be utilized to report the completion status of backup processing, with electronic notification of failures sent to Offeror technical support, and identified Commonwealth staff for follow up and corrective action.

The Commonwealth benefits from the new Unisys approach to monitoring backup success rates. In most cases simply re-starting a backup results in a successful backup because needed resources are tied up during peak times but become available a short time later. Unisys automates the restart process. If the restarted backup fails then incident tickets are created to alert the Backup support team. Thus critical issues get right to Level 2 and Level 3 support personnel without even involving Level 1 support staff.

This automation of incident ticketing provides the Commonwealth with another advantage. During service delivery reviews the Commonwealth can also review response times to failures that might put critical applications at greater risk. Through the incident severity rating processes Unisys has the ability to adjust severity levels so that incidents that are closer to critical applications can receive prioritized support responses.

The full details for the innovative backup service provided to meet the Commonwealth's data protection needs are included in the F.3.2.4.2 Storage Management.

3.D Offeror must describe its approach to perform an initial review and audit of the backup policies, procedures and reports, to ensure the accuracy of the backup schedules, retention periods, target directories, and recovery point objectives.

As part the Transition data gathering activities, the Unisys Team will meet with the Commonwealth to review and audit backup policies, procedures and reports. The activities to perform this review are described in F.3.2.4.2, Requirement 4.

3.E Offeror must describe its approach to identify gaps and potential risks, and how those gaps and risks will be resolved.

During transition and transformation, the Unisys solution includes an extended onsite presence of a CommVault technical manager who aids the Unisys Team in the search for existing gaps and risks, along with potential improvements to the backup systems solution. This technical expert has extensive experience in implementations and in identifying value-add opportunities. The skills of this technical expert are married to the Unisys Team's extensive expertise around current backup operations. Jointly they lead the transition to the more cost effective CommVault backup infrastructure. The Unisys Team, also working with the CommVault technical manager, manages the review and audit of backup clients that move from the legacy system into the CommVault system. During transition a like-to-like set of backup policies, procedures, reports, schedules, retention periods, target directories, and recovery point objectives are built out. The Unisys Team can then present the Commonwealth with opportunities to further optimize the infrastructure to improve the quality of services or provide better cost efficiencies for the same services.

The Unisys Backup team is also able to compare the Backup inventory of clients and policies to the CMDB inventory to locate "negative" gaps in case a server or critical data set is introduced into the Fully Managed environment and, through unlikely process failures, was not also protected with sufficient backup resources. The Unisys governance processes and the processes generated by the Unisys solution's Enterprise Services Catalog are designed to remove such failures. Additionally, a compare of Backup infrastructure inventory from the backup tools perspective with the CMDB can locate a gap should one occur as an additional level of protection

The activities to perform the gap analysis are described in F.3.2.4.2, Requirement 4.

4 Staff, IBM systems, Oracle, and SAP Staff Resumes

4.A Offeror must submit a representative sample of staff resumes typically provided for these positions detailing their experience, education, and certifications.

Provide IBM, SAP, and Oracle trained staff holding current manufacturer certifications for hardware and software technical support.

The Unisys support team is composed of personnel who maintain education and certifications in a variety of infrastructure platforms including AIX, Windows, [redacted] and EMC and IBM Storage. Section 5.0 provides resumes for key personnel and representative personnel who have IBM, SAP, and Oracle training or certifications.

4.B Staff will interact with vendor support Services when needed.

As part of ongoing operations, the Unisys support team will have access to SAP, Oracle, IBM, and other vendor support services to assist with resolution of major incidents and problems. The Unisys Team maintains partnerships with Oracle, SAP, IBM and EMC and will use these partnerships as needed to provide a high quality service for the Commonwealth ERP infrastructure.

4.C Provide Commonwealth with a resume or CV for each operational staff member assigned to this engagement.

Representative resumes for support staff responsible for ERP hosting services can be found in Section 5.0 Personnel.

4.D A copy will be maintained on Offeror file including required background checks and clearances as required.

A copy of the resumes as well as the results of the background checks will be maintained by the Unisys Team as part of the management service. The approach for managing resumes and background checks is described in Section 5.0 Personnel.

5 Service Desk, Tiered Support

5.A Offeror must describe its approach to providing and maintaining different tiered levels of ERP (SAP & Oracle) support.

Provide cost effective operational and technical support for the computing platform.

By using a combination of services based upon the Windows, Linux, AIX, Security and Storage services proposed for the Commonwealth's environment and flexible options for the ERP systems, the Unisys Team will provided a cost effective service for both the infrastructure components and the operational and technical support.

The tiers of support for ERP services are described in requirement 2.A above.

5.B Provide Level 2 and Level 3 Support to the Service Desk and/or Commonwealth Users.

The ERP hosting services support will be available and accessible to Service Desk and authorized Commonwealth personnel. The service management processes for Service Request, Incident and Change Management will be the primary methods for requesting Level 2 or 3 support for the ERP systems, Agencies however will also have access to the support teams through the Agency Account Manager.

The activities and interactions between the Service Desk and Level 2 and 3 support are described in Schedule F, Section 3.2.3.2.

5.C Provide a tiered level of support Services (e.g. Gold, Silver, and Bronze).

As part of the overall infrastructure support model, the ERP hosting service will support the multiple tiers of support requested for the Fully Managed and Managed Only services, including Platinum, Gold, Silver, Bronze, and Basic.

The tiers of support for ERP services are described in requirement 2.A above.

6 Monitor Network Connectivity, Toolset

6.A Ensure network connectivity, and consistent system response times.

Offeror must describe its real-time monitoring approach and toolset to provide and maintain network availability and performance.

Utilize automated system management tool(s) to ensure real-time monitoring and notification of server availability and response times. Stop / Start times of servers will be a source of input for SLA measurements.

Identify tool set(s).

Offeror must identify tools it uses to support network availability and performance.

Unisys will provide event management solutions to provide network connectivity and consistent system response times. Unisys will utilize automated system management tool(s) to provide real- time monitoring and notification of server availability and response times including the stop and start times of servers to support SLA availability measurements.

The tools are indicated below and the enterprise Event Management's overall approach is described in Schedule F, Section 3.2.3.2 Site Operations.

The following tools are the major toolsets to support network and system event management and monitoring.

Monitoring Software	Managed Configuration Items (CI's)	Monitoring and Management Functionality
SolarWinds	LAN Devices including: • Switches • Routers • Load Balancers • Firewalls	Provides deep network device availability and performance monitoring, DNS, IP address management, network configuration management, and network traffic bandwidth throughput monitoring
Nagios	Microsoft servers, databases, network devices, and storage hardware. [redacted] unisys.com	Provides a standard set of availability, performance and critical service monitors developed by Unisys for monitoring across infrastructure items including: • Servers • Network devices (switches, routers, load balancers)

		• Storage devices • Middleware • Applications (Exchange, Citrix XenApp, etc.)

7 Patch Management

7.A Ensure server operating systems are maintained with the current system patch level, based on the Services provided by the server.

Offeror must describe its approach to patch management including analysis, communications, schedule (change records) and installation process.

Implement a Patch Management Program to ensure the timely application of updates on all infrastructure platforms in accordance with Commonwealth IT policy guidelines.

The Unisys technical support team will work with the Commonwealth agencies to determine patch policies, such as the Commonwealth ITBs, that should be applied to the ERP environments. As ERP application have unique requirements for some operating system and other software patches, the updates and advisements provided by SAP and Oracle will be included as part of the overall approach for patch management for the systems supporting the ERP environment.

The overall approach to patch management including analysis, communications, scheduling via change management and installation processes is described in Schedule F, Section 3.2.3.2 Site Operations.

7.B Offeror must describe its approach for testing and validating updates to the OS and 3rd Party software that it supports.

Unisys approach to testing and validating updates to the compute system' OS and 3rd party software in the SAP and Oracle ERP environments follows the Release Process for changes into ERP environments. The Release Process includes:

- Change ticket approvals
- Test planning and accepted test results
- Release and deployment planning including release back-out plans
- Release testing for risky deployments
- Early life cycle support to help provide a successful deployment
- Release back-out for failed release

The overall approach for testing, as part of patch management, various OS and 3rd Party software, when necessary, is described in Schedule F, Section 3.2.3.2 Site Operations.

7.C Offeror must describe its approach to communicating unscheduled and scheduled outages, including its escalation process.

The Unisys Team communicates unscheduled outages by sending notifications to key stakeholders for the Commonwealth, individual Agencies, Unisys Team, and Third Parties depending on the outage. This will be through email, voice, Services Portal and Remedy broadcast capabilities. The same communications will be used for scheduled outages with additional communications in forward schedules of change reports. The communications procedures will be documented within the CCPM.

Escalations for unscheduled outages are handled through the standard processes for managing incidents. Unisys service desk will manage all incidents and manage escalation communications to key Commonwealth/Unisys/Third Parties personnel. The Unisys ITSM application will also be configured to escalate incident tickets based on incident priorities and SLAs for response and resolution.

The overall escalation communications approach is described in Schedule F, Section 3.2.3.2 Site Operations.

7.D Analyze monthly service patches and determine which patches need to be applied, by server type.

As server OS patches are released from the respective manufacturers, the Unisys Team will validate the patches monthly with the ERP application team and check the SAP and Oracle support sites. As the ERP manufacturers require additional time to validate if a patch can impact the application, additional time before installing the patches may be required. Patches will be recommended based on the servers function. The testing and planning for rollout of the patches will follow the release process as defined in requirement 7.C.

The overall approach to analyzing patches is part of the patch management process described in Schedule F, Section 3.2.3.2 Site Operations.

7.E Create a change record, log the update in the server log, and install based on server maintenance schedule.

Each patch window will be processed through change management and performed during the approved change schedule. After the patch has successfully been applied, the CMDB will be updated.

The overall patch management process including the use of change management is described in Schedule F, Section 3.2.3.2 Site Operations.

8 User Account Management

8.A Provide certified system administration staff to create and maintain the registration of profiles, associated groups, and the security permissions required to service the approved client base of the system and application.

Offeror must describe its administration/support approach and provide representative resumes.

The Unisys Team's Windows, Linux and AIX support teams will provide user, profile, group, and security permission management on individual Windows, Linux and AIX servers. For Windows servers operating on an Active Directory domain, Unisys will work with Commonwealth Active

Directory support team to request changes in the Active Directory environment to support user, profile, group or security permissions changes.

Unisys recommends that the Commonwealth agency user account teams submit requests to have OS level user account changes made by the Unisys Team. However, the Commonwealth's authorized personnel performing agency user account management for the ERP application and require OS level user account changes can be provided with the appropriate privileges to make the associated user account changes.

All changes for user account management will be initiated through the service request and change management process and require an approved change record for implementation. The process for user account management will be documented within the CCPM.

User Account Management support will be provided by personnel with similar skills and experience indicated by the resumes located within Section 5.0 Personnel.

9 Plan, Procurement Planning

9.A Provide program and process to refresh the hardware at asset end-of-life, and when upgrades are needed to meet anticipated growth in utilization.

Offeror must describe its program and processes for upgrading systems.

Technology Refresh Plan

As part of the overall architecture support, the Commonwealth's environment will be reviewed on a quarterly basis to identify technology, services or components which require replacement to maintain the Commonwealth's business needs and associated service levels. The overall technology refresh plan will be documented in Key Deliverable D-03. This plan will be used for all Unisys supported environments including the Commonwealth ERP systems.

The overall Technology Refresh approach is described in Schedule F, Section 3.2.1.5.1 .

Capacity Management and Forecasting

The Commonwealth ERP systems will be monitored and reported from the Event Management Platform [redacted] and from the [redacted] t to support the ERP systems Capacity Management requirements. As part of the Capacity and Performance Management processes, , the performance and capacity reports will be generated and reviewed with the Commonwealth on a regular basis.

During transition the SAP and Oracle compute environments' capacity requirements will be assessed as part of the establishment of the Performance and Capacity Management Processes described in Schedule F, Sections 3.2.2.6 and 3.2.2.2.

10 SLA Reporting

10.A Collect actual system availability, utilization and response time data.

Offeror must describe its processes and toolset for monitoring and maintaining service levels.

Unisys will provide a SLA data collection and reporting process to support ERP Application

SLA's that will be established when Commonwealth agencies request services in the Enterprise Services Catalog to map infrastructure to ERP applications. Upon completion of the requested services, SLA's can be established for each ERP application's supporting infrastructure, based on requested :

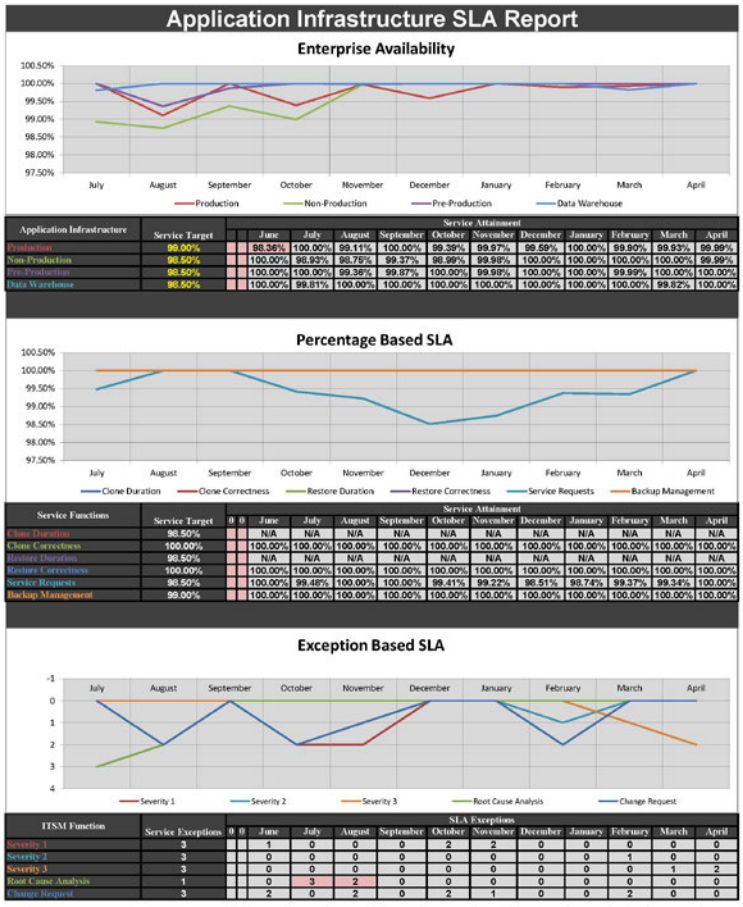
- System Availability
- Utilization
- Response Time

The SLA data will be tracked using the Service Level Management tool. The SLA Reporting solution is described in Schedule F, Section 3.2.1.2.

10.B On a monthly basis, Offeror must create a SLA report for the Commonwealth and Vendor Management teams.

Offeror must provide a representative sample of its SLA reports for ERP hosting Services.

Service Level reports will be generated on a monthly basis. These reports will be made available through the Services Portal via the dashboard and reviewed with the Commonwealth. An example of the monthly report is shown in the figure below. In addition to the monthly report, the Unisys Team is implementing an online operational dashboard via the Services Portal. An example of the dashboard is located in Schedule F, Section 3.2.3.2.



Application Infrastructure	Service Target	Service Attainment										
		June	July	August	September	October	November	December	January	February	March	April
Production	99.00%	98.36%	100.00%	99.11%	100.00%	99.39%	99.97%	99.59%	100.00%	99.90%	99.93%	99.99%
Non-Production	98.50%	100.00%	98.93%	98.75%	99.37%	98.99%	99.98%	100.00%	100.00%	100.00%	100.00%	99.99%
Pre-Production	98.50%	100.00%	100.00%	99.36%	99.87%	100.00%	99.98%	100.00%	100.00%	99.99%	100.00%	100.00%
Data Warehouse	98.50%	100.00%	99.81%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	99.82%	100.00%

Service Functions	Service Target	Service Attainment										
		June	July	August	September	October	November	December	January	February	March	April
Clone Duration	98.50%	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Clone Correctness	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
Restore Duration	98.50%	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Restore Correctness	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
Service Requests	98.50%	100.00%	99.48%	100.00%	100.00%	99.41%	99.22%	98.51%	98.74%	99.37%	99.34%	100.00%
Backup Management	99.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%

ITSM Function	Service Exceptions	SLA Exceptions										
		June	July	August	September	October	November	December	January	February	March	April
Severity 1	3	1	0	0	0	2	2	0	0	0	0	0
Severity 2	3	0	0	0	0	0	0	0	0	1	0	0
Severity 3	3	0	0	0	0	0	0	0	0	0	1	2
Root Cause Analysis	1	0	3	2	0	0	0	0	0	0	0	0
Change Request	3	2	0	2	0	2	1	0	0	2	0	0

Figure Application Infrastructure SLA Report

Continual Service Improvement

Unisys recognizes the significant importance of Quality and Continuous Service Improvement to:

- Reduce service risk,
- Improve service quality,
- Improve client satisfaction,
- Provide service transparency, and
- Improve/reduce costs of service.

Through a continuous cycle of evaluation and improvement within an IT infrastructure, Unisys views quality and continuous service improvement as a critical success factor in driving customer satisfaction for the Commonwealth IT infrastructure. Each of the continuous service improvement areas identified above are driven through the tight integration of the following organizations, industry tools, proven processes and quality deliverables:

- Service Excellence Office,

- Quality Plans: transition and steady state service delivery
- Industry standard frameworks and methodologies: ITIL, ISO, SSL
- Industry accepted measurement tools
- Continuous Service Improvement & Innovation Processes (CSIIP)
- Risk management, audits and business continuity management
- Client Satisfaction Surveys and Knowledge Management Portal

Collectively this represents Unisys Integrated Quality Plan for the Commonwealth of Pennsylvania.

Specifics on each of these areas are outlined in Schedule F, Section 3.2.1.1.6 Continuous Service Improvement. Highlights from this section are outlined below and requested service examples are provided at the end of this section.

11 CI Service Risk

11.A Reduce service risks.

Offeror must provide methods to eliminate or mitigate service risks.

Risk management, independent quality audits, and business continuity management are integral quality management processes. Unisys is committed to managing risks and facilitating the achievement of business objectives the adherence to quality processes. We mitigate risk through the implementation of tight quality controls: standard policies, procedures, roles, risk assumptions, issues, and definitions, etc.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

12 CI Service Quality

12.A Improve service quality.

On a quarterly basis, Offeror must also recommend to the Commonwealth team any system changes that would be appropriate to maintain or improve SLA commitments.

The quality approach begins with the Service Excellence Office who provides definition and oversight of all ITIL process management and analysis functions. Process managers and analysts working in the Service Excellence Office are responsible for auditing process effectiveness, ensuring that service delivery teams comply with proper execution of processes, and analyzing process trends for anomalies. Continuous service improvement programs in collaboration with Commonwealth agencies are managed by the Service Excellence Office.

Through our Continuous Service Improvement and Innovation Process (CSIIP), the SEO reviews, analyzes and makes recommendations on improvement opportunities in each ITIL lifecycle phase. Unisys will leverage Six Sigma Lean tools and methodologies as well as ISO Certified internal audits to measure and maintain the highest quality services to the Commonwealth.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

13 CI Client Satisfaction

13.A Improve client satisfaction.

Offeror must provide examples of previous Offeror initiatives aimed at continually improving client satisfaction.

Client satisfaction is extremely important to Unisys and a key focus in our IT solution. The SEO will integrate new agencies, customers and services into our multi-pronged client satisfaction approach that includes Service Desk surveys on the caller's experience, an overall agency satisfaction survey, and quarterly surveys with the Office of Administration. Data collection will be gathered across multiple levels to gain a clear understanding of the Commonwealth's satisfaction with the IT Services being provided.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

14 CI Service Transparency

14.A Ensure service transparency.

Offeror must provide methods and practices to ensure service transparency, providing visibility into service execution.

The service organizations will use standardized ITSM services processes, IT monitoring and automation tools. ITSM processes will be documented in the Commonwealth Computing Procedures Manual (CCPM). The CCPM will be available to Commonwealth approved staff on the Knowledge Management Portal (KMP) providing desired transparency into service execution processes. Through the Real-time Dashboard, the Commonwealth will have access to current operational performance of their application infrastructure.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

15 CI Reduce Cost of Service

15.A Improve/reduce cost of service.

Offeror must provide examples of ERP Hosting initiatives that have been implemented or can be utilized to achieve reduced costs of Services and to meet or exceeded ROI (Return on Investment) analysis projections.

The Service Excellence Office will proactively manage quality, continuous service improvement, ITIL process management, and customer satisfaction through a comprehensive quality plan that specifically addresses all of these areas. We believe this is a key differentiator in our partnership with the Commonwealth. Through this new organization and these quality plans, Unisys will drive best in class services and the highest customer satisfaction experience, while reducing overall costs to the Commonwealth.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

A few examples of ERP Hosting – SAP/Oracle support and initiatives that have been implemented or can be utilized to achieve reduced costs of Services and to meet or exceeded ROI (Return on Investment) analysis projections are outlined below:

Disk-based Backup Strategy:
Unisys leverages EMC's Avamar and Data Domain products to facilitate disk-based backups and data replication to an offsite location. This eliminates cost and unreliability associated with tape media and significantly expedites recovery time in the event of a disaster. The implementation of a disk to disk with data de-duplication strategy for IES resulted in a significant reduction in backup and restore times for the extremely large, rapidly growing SAP data store. At the time that IES migrated to the DPH, the data store in SAP was 5 TB. This data store had previously been backed up across 32 tape drives taking close to five hours to back up. This left IES exposed to issues with tape media that would prevent the ability to restore effectively with the implementation of disk-based backup, the SAP data store has completed backup in less than four hours, even with peaks of 9 TB size.

Flexible Capacity
As part of the migration to virtual infrastructure and a services based model, the California State University Higher Education PeopleSoft environment added the capability to use and adjust their compute services to meet the fluctuations in demands during key periods during the year, such as, class enrollment, application cycles and other peak usage while also reducing the overall physical footprint of the system.

Unisys Team Experience

Unisys Team Experience is located above in Requirements 1.B and 1.C.

Benefits to the Commonwealth

By providing an integrated service management approach for all compute services, the Unisys Team will enable the Commonwealth with common processes and tools to maintain the ERP environments consistently and cost-effectively. In addition, the Unisys Team will work with the Commonwealth's ERP teams to optimize their use of the new Infrastructure as a Service to support the fluctuations with peak load which occur during the year. This will support the Commonwealth's need to support the business while also managing the environment's overall capacity.

The Commonwealth can leverage additional technical services including SAP, Oracle and other technical skills via the Enterprise Services Catalog to support ongoing operations or unique projects. The Enterprise Services Catalog also includes the option for application monitoring services for additional monitoring capability.

3.2.4.4 UNIX Support – AIX / Linux

The Unix Support – AIX / Linux service will provide hosting and operational support Services for AIX and Linux server systems. The systems will be located in the Offeror's datacenters. Offeror must support various versions of the AIX and Linux operating systems. The number of staff members required to perform the operational tasks listed below will be determined by the Offeror.

Reference Documentation

Exhibit E.1 - DLI - Datacenter Inventory Template

Exhibit H.1 - DOR - Datacenter Inventory

Exhibit H.2 - DOR - DPH Asset List

Exhibit H.4 - DOR - SAP TRM System

Exhibit I.1 - IES - DPH Commonwealth Owned IT Assets

Exhibit I.2 - IES - Application Inventory

Exhibit I.3 - IES - DPH Commonwealth Software Asset Unisys

Exhibit B.2 - Commonwealth Owned DPH IT Assets (see PLCB Oracle systems)

Requirements		Describe Compliance

1.	Monitor local operations, troubleshoot and resolve operational issues.
	
	Actively monitor the daily operations of all AIX / Linux systems. Assume responsibility for all master and subordinate console functions. Issue operator commands to control all In-Scope platforms. Assume the responsibility for and perform all console operations. Monitor the performance of online interactive traffic and take appropriate action to resolve online-system-related incidents and/or problems, including escalating (as appropriate) the incident and/or problem to the proper Level 2 Support group. Monitor the transmission of files between the
		Offeror must describe its UNIX/Linux monitoring, operations and troubleshooting approach Commonwealth including the following:
		
		• Processes and Procedures
		• Tools / Applications
		• End User Reports
		  o Standard
		  o Custom
		• Support Levels
		• Escalation Procedures

	Commonwealth and any other parties as designated by Commonwealth. Provide operational support for data transmission (send/receive), consistent with commercial or agency standards. Manage, maintain, monitor, and control online and batch process, both scheduled and unscheduled (including on-request processing). Maintain a log for each server detailing hardware / software configuration and critical service operations. Review the system logs on a weekly basis to ensure critical system Services are processing without errors. Document review of the system logs on a weekly basis to ensure critical system Services are processing without errors. Complete weekly server log indicating which logs were reviewed, date and initial the log. Maintain and update the operational documentation for all operations procedures and Services.	
2.	Provide a review and analysis of UNIX system performance/capacity to determine if current performance/capacities are sufficient to support the needs of the UNIX stakeholders.	Offeror must perform an initial review and audit of the current UNIX usage, procedures and reports and provide an analysis of the current UNIX usage, processes and reports currently being supported. Offeror must document its review and audit findings and recommendations.
3.	Production Control and Scheduling (including batch processing) Describe the process of scheduling batch jobs within Commonwealth agency defined windows to achieve maximum performance as long as	Offeror must describe its approach to supporting the batch processing needs of the Commonwealth including the following: • Processes and Procedures • Tools / Applications

	required batch completion times are met. A cross platform (e.g. Window, Unix, and Mainframe) system will be required. Where practicable, provide for automated scheduling of batch work and processes including backups. Commonwealth agencies have a number of applications that require scheduling software / batch processing software (i.e. $Universe, SAP certified, etc.), this software is heavily integrated into many of these systems. Develop, maintain, and utilize an emergency contact list and escalation procedures to resolve abnormally ended jobs. Resolve abnormally ended jobs caused by conditions external to production programs. Repair abnormally ended jobs when possible and perform job restarts in accordance with the Service Management Manual. Check job outputs and print queues, and change job priorities. Notify Commonwealth agencies in accordance with the Offeror's proposed notification procedures in the event that applications do not execute properly.	• End User Reports o Standard o Custom • Tiered Service & Support Levels • Escalation Procedures Offeror must describe how it will operate and maintain current scheduling/batch software tools.
4.	Monitor system backup processing on a daily basis. Review daily backup logs for successful completion. Note failures, and correct the problem. Create	Offeror must describe its approach to performing an initial review and audit of the backup policies, procedures and reports, to ensure the accuracy of the backup schedules, retention periods, target directories, and recovery point objectives.

	problem record for any abnormal condition and any repairs that have been made. An automated software process will be utilized to report the completion status of backup processing, with electronic notification of failures sent to Offeror technical support, and identified Commonwealth staff for follow up and corrective action.	Offeror must describe its approach to identifying gaps and potential risks, and how those gaps and risks will be resolved.
5.	Provide AIX and Linux trained staff that hold current manufacturer certifications for hardware and software technical support. Provide technical advice and support to the Application Development and Maintenance (ADM) and Database Administration (DBA) staffs, as required. Post award; provide Commonwealth with a resume or CV for each operational staff member assigned to this engagement. A copy will be maintained on Offeror file.	Offeror must submit a representative sample of staff resumes typically provided for these positions detailing their experience, education, and certifications.
6.	Provide cost effective operational and technical support for the computing platform. Provide platform level operational and technical support for the computing platform. List the service levels for the various service tiers that can be provided. See Schedule J.1 Datacenter Service Level Management for the definitions of the expected options. Provide Level 2 and Level 3 Support to the Service Desk and/or Commonwealth Users.	Offeror must describe its approach to supporting the operational and technical support needs of the Commonwealth.

7.	Ensure network connectivity to COPANET, and consistent system response times. Utilize automated system management tool(s) to ensure real-time monitoring and notification of server availability and response times. Stop / Start times of servers will be a source of input for SLA measurements.	Offeror must describe its real-time monitoring approach and toolset to provide and maintain network availability and performance. Offeror must identify tools it uses to support network availability and performance.
8.	Ensure server operating systems are maintained with the current system patch level, based on the Services provided by the server. Analyze monthly service patches and determine which patches need to be applied, by server type. Create a change record, log the update in the server log, and install based on server availability schedule. Change requests will be approved and authorized using the change management process. Notify the Commonwealth of any scheduled or unscheduled service interruptions. Implement a Patch Management Program to ensure the timely application of updates on all infrastructure platforms in accordance with Commonwealth IT policy guidelines.	Offeror must describe its approach to supporting the software patch needs of the Commonwealth. Offeror must describe its approach to testing and validating updates to the OS and 3rd Party software that it supports. Offeror must describe its approach to communicating unscheduled and scheduled outages, including escalation process.
9.	User Account Management Provide certified system administration staff to create and maintain the registration of profiles, associated groups, and the security permissions required to service the	Offeror must describe its approach to supporting the needs of the Commonwealth.

	approved client base of the system and application.	
10.	Procurement Planning Provide program and processes to refresh the hardware at asset end-of-life, and when upgrades are needed to meet anticipated growth in utilization.	Offeror must describe its approach to supporting the needs of the Commonwealth.
11.	SLA Reporting Collect actual system availability, utilization and response time data. On a monthly basis, create a Service Level Agreement report for the Commonwealth and Vendor Management teams.	Offeror must describe its approach to supporting the needs of the Commonwealth.
12.	The Offeror must provide Software License Management.	Offeror must describe solution and approach to meet this requirement.
Continual Process Improvement		
13.	Reduce service risks.	Offer to identify methods and approaches to eliminate or mitigate service risks.
14.	Improve service quality.	On a quarterly basis, Offeror must also recommend to the Commonwealth team any system changes that would be appropriate to maintain or improve SLA commitments.
15.	Improve client satisfaction.	Offeror must provide examples of previous Offeror initiatives aimed at continually improving client satisfaction.
16.	Ensure service transparency.	Offeror must identify methods and practice to ensure service transparency, providing visibility into service execution.
17.	Improve/reduce cost of service.	Offeror will provide examples of UNIX Support initiatives that have been implemented or can be utilized to achieve reduced costs of Services and to meet or

		exceeded ROI (Return on Investment) analysis projections.

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

Introduction

The Commonwealth has a large investment in the development of mission critical applications on the IBM AIX platform across multiple agencies. These applications often require the performance, reliability and stability inherent to the Unix platform. Unisys and its partner, IBM, recognizes the strategic importance of this platform, and of the services needed to confirm this platform is available. To this end, the Unisys Team will perform all services around the AIX operating system, and underlying Flex Systems pSeries hardware platform. The Unisys team management of the AIX platform provides the Commonwealth with numerable advantages that other vendors can't match. Amongst these advantages are the reduction of risk. The Unisys team manages hundreds of thousands of AIX systems globally for customers across our portfolio. A large percentage of these AIX systems house mission critical applications. Leveraging the expertise of the Unisys team with the proposed hardware and software platform is a natural fit that reduces risk at every level, from infrastructure through the operating system to the application layer.

Linux is an important platform, increasingly becoming the platform of choice for database servers, internet and intranet servers, and infrastructure servers. Its influence and importance in the data center is growing yearly, and we expect this to become an even more important strategic platform for the Commonwealth. Unisys will provide support for the Linux platform across the Commonwealth, and will apply the processes, procedures and experience gained on other accounts maintain the platform. Additionally, through a unified framework of common IT Service Management tools and ITIL V3 aligned processes, Unisys will bring unique and innovative approaches to enterprise management to gain efficiency and increase reliability of this strategic platform.

1 AIX and Linux Operations Approach

1.A Offeror must describe its UNIX/Linux monitoring, operations and troubleshooting approach Commonwealth including the following:

The Unisys Team will provide hosting and operation support services to the Commonwealth of Pennsylvania for required versions of AIX and Linux systems at the Commonwealth [redacted] and Unisys data centers. Staffing required to perform the operational tasks listed below will be US based Unisys Team personnel both on-site and remote to the data centers.

Processes and Procedures

The processes and procedures for providing AIX/Linux infrastructure managed services will be documented in the CCPM which will be reviewed and approved by the Commonwealth. The scope of these processes and procedures will be based on the ITIL framework as well as technology best practices for support of AIX/Linux platforms.

Processes and procedures will be developed for the following areas:

- Server technology support – build and maintain for hardware, software, connectivity
- Vendor management – technical support, maintenance coverage, and remote access capability
- Platform specific procedures – customer notification, technical support escalations patching process/schedule, security monitoring, and log reviews

Tools / Applications

The Unisys Team has outlined the approach to monitoring operations and supporting automated remediation over time from a common enterprise infrastructure platform across all technical towers for the Commonwealth in F3.2.3.2 Site Operations.

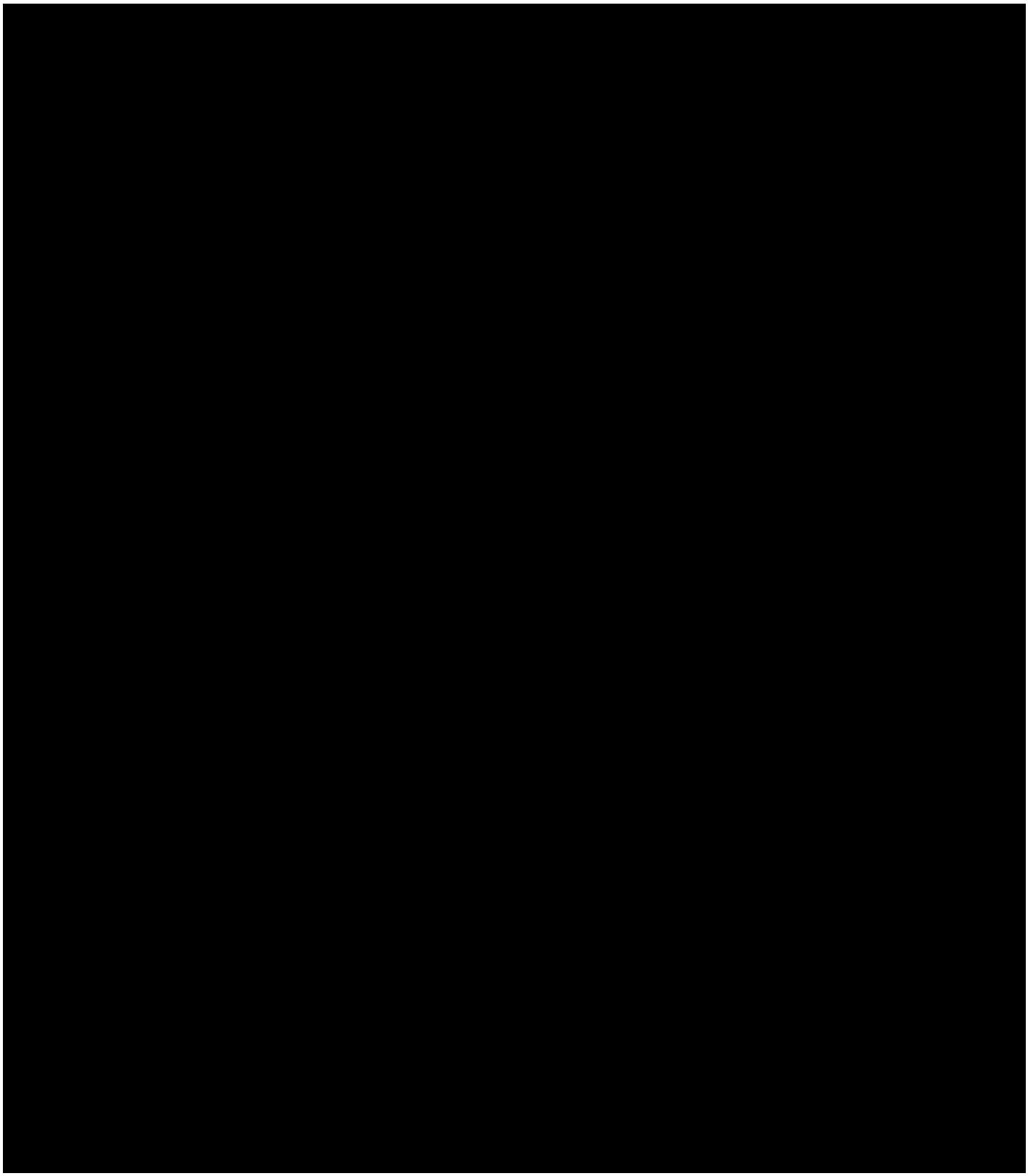
The Unisys Team will also implement, support, and operate a comprehensive and integrated Information Technology Service Management (ITSM) Architecture dedicated to the cross functional process support for all services provided to the Commonwealth for this contract. The proposed ITSM Architecture, shown in **Figure 3.2.4.4-1**, will provide an effective and efficient operational platform to support the Commonwealth's agencies application infrastructure for the following ITIL V3 (Information Technology Infrastructure Library) Service Management Processes.

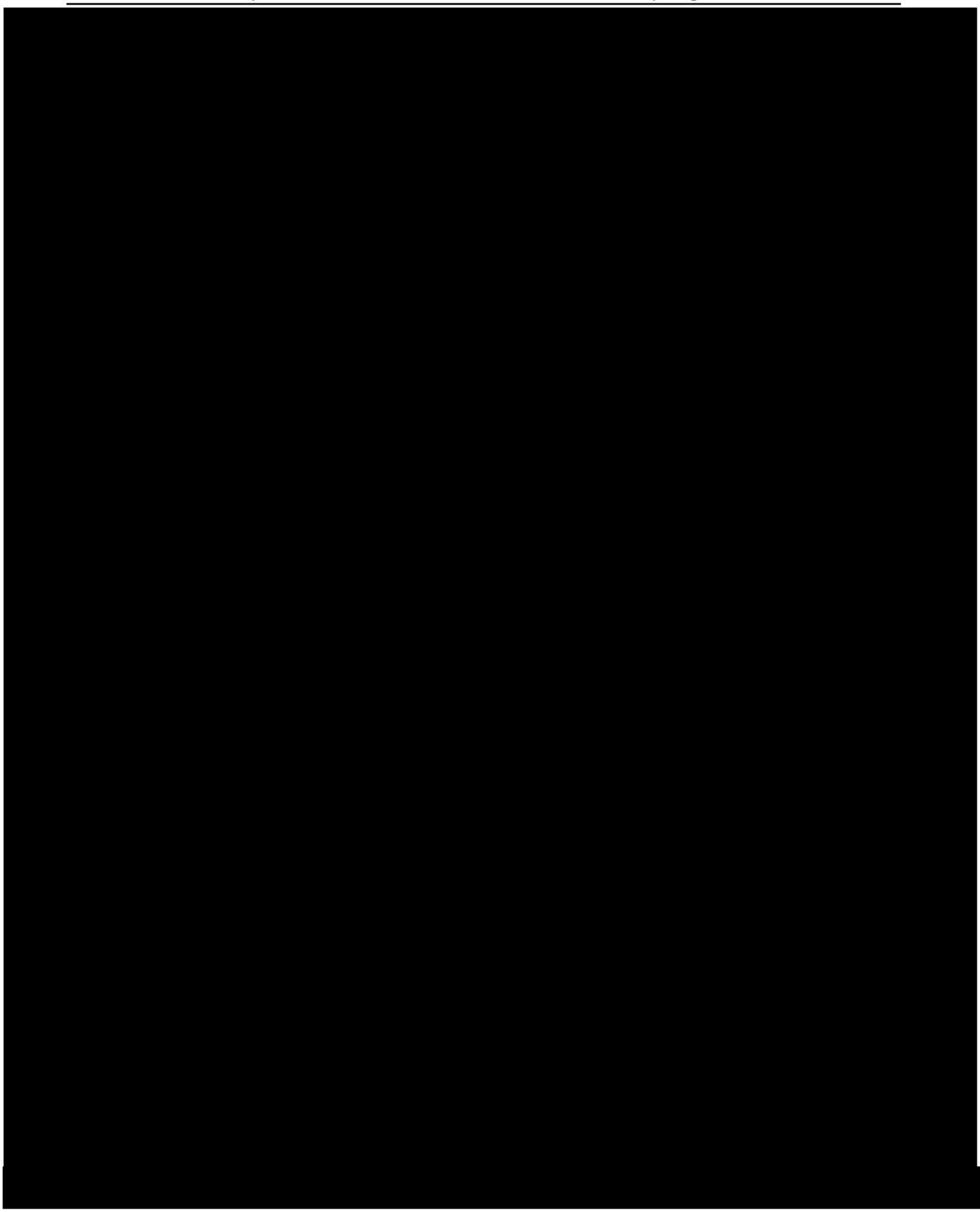
[redacted]

Figure 3.2.4.4-1 - Proposed Unisys ITSM Integrated Architecture.

The Integrated ITSM Management Platform software tools are summarized in the **Figure 3.2.4.4-2**.

[redacted]





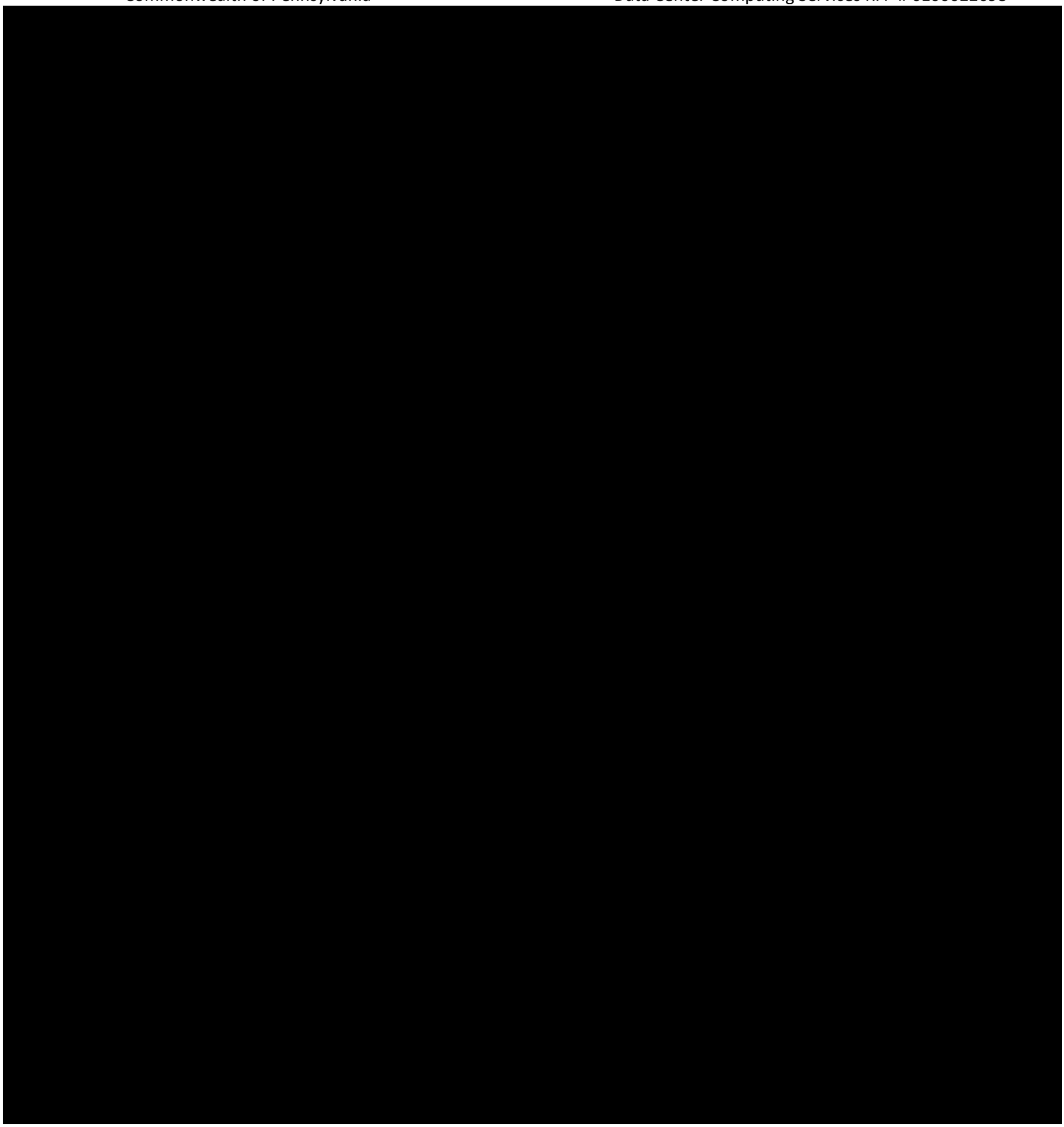


Figure 3.2.4.4-2 - The Unisys Team's ITSM Tools

The Unisys Team will assess the Commonwealth's current ITSM toolsets during transition. Assessment results determine which tools will be supported within this overall target ITSM proposed architecture, replaced, or eventually migrated to the target environment ITSM tools shown in **Figure 3.2.4.4-2**. Some of the tools that will be evaluated and assessed during transition include:

- NIMS
- IBM Systems Director

The resulting architectural decisions will be reviewed and approved by the Commonwealth's agencies. Some identified tools will continue to offer the functionality they currently providing, but will be integrated into the overall ITSM proposed architecture.

End User Reports (Standard and Custom)

Standard Reports are summarized in Schedule F, Section 3.3.2. Examples of standard IT Service Management (ITSM) status reports for critical processes include:

- Change Management
- Incident Management
- Problem Management

Custom Reports are offered by Unisys via the Enterprise Services Catalog.

Support Levels

In order to provide customization and flexibility to Commonwealth agencies, the Unisys Team offers tiered levels of managed services for AIX and Linux servers. These tiers offer various levels of administrator experience, on-site coverage and responsiveness SLA's. The tiers are designed to allow for flexibility to manage mission critical as well as development or

demonstration environments.

The following table highlights the available tiers and associated capabilities.

Tiered Support Level	Description
Platinum	• Provides 99.999% Application Infrastructure Availability • Server is monitoring via Nagios • Fully Managed Services • Asset Tracked In CMDB **with relationships** • Requires 3 servers load balanced and geographically dispersed
Gold	• Provides 99.99% Application Infrastructure Availability • Server is monitoring via Nagios • Fully Managed Services • Asset Tracked In CMDB **with relationships** • Requires 2 servers load balanced
Silver	• Provides 99.9% Application Infrastructure Availability • Server is monitoring via Nagios • Fully Managed Services • Asset Tracked In CMDB **with relationships**
Bronze	• Provides 99.4% Application Infrastructure Availability • Server is monitoring via Nagios • Fully Managed Services • Asset Tracked In CMDB
Basic	• Provides 98.5 % Application Infrastructure Availability • Server is monitoring via Nagios • Fully Managed Services • Asset Tracked In CMDB **with relationships**

Escalation Procedures

As part of the communication management plan, the Unisys Team will work closely with the Commonwealth of Pennsylvania to structure effective escalation procedures. These procedures will be developed to provide guidance for escalation activities in a number of categories including incident management service response, management notification, and service quality.

For incident management service response, escalation procedures will define the schedule, criteria, methods, and participants for the escalation of issues or incidents impacting computing services to the Commonwealth. The primary objective of this escalation is to assign appropriate vendor resources with the necessary skills to the incident process to restore service. The procedure will include steps to contact approved agency stakeholders to provide initial notification and to engage in joint problem determination/resolution activity as appropriate.

Escalation procedures will also include provisions to notify Commonwealth and Vendor

management staff of major service impacting events as well as to provide continuous updates are provided until the incident is resolved. In order to provide an easy method for the Commonwealth to notify the vendor of service quality concerns, the escalation procedures include the process and contacts to register the service quality issues for review and action.

For more details, including the specifics of the escalation process, please see Schedule F, Section 3.2.3.2 Site Operations.

Monitor local operations, troubleshoot and resolve operational issues.

Actively monitor the daily operations of all AIX / Linux systems.

The Unisys Team will provide hosting and operation support services to the Commonwealth of Pennsylvania for required versions of AIX and Linux systems. We will monitor the daily and local operations through the common IT Service Management platform. For details about tools and processes, please see Schedule F, Section 3.2.3.2 Site Operations.

1.B Assume responsibility for all master and subordinate console functions.

The Unisys Team will assume responsibility for all master and subordinate console functions. The Unisys Team is committed to improving service while reducing costs. To achieve this, the Unisys Team will utilize automation techniques whenever possible to enhance all master and subordinate console operations and to proactively monitor the mainframe and server environments. These automation techniques have been used and proven in delivery of our services to the Commonwealth and other clients.

1.C Issue operator commands to control all In-Scope platforms.

The Unisys Team issues console operations commands within the current contract. This will continue under the new contract. The Single Point Operations (SPO) workstation consoles and Accessory Manager sessions are used for the responding to or issuance of commands to the AIX and Linux systems.

1.E Assume the responsibility for and perform all console operations.

The Unisys Team will assume the responsibility for the console and perform all console operations for AIX and Linux utilizing the tools as detailed above.

1.F Monitor the performance of online interactive traffic and take appropriate action to resolve online-system-related incidents and/or problems, including escalating (as appropriate) the incident and/or problem to the proper Level 2 Support group.

The Unisys Team will monitor online interactive traffic and provide necessary troubleshooting support.

To support the operational and technical needs of the Commonwealth, the Unisys Team will

deploy incident, problem and change management processes that define the flow of support from the Service Desk up through Level 2 and Level 3 support. These processes are closely aligned to the common IT Service Delivery platform. For more detailed information on these processes, please refer to Schedule F, Section 3.2.3.2.

1.G Monitor the transmission of files between the Commonwealth and any other parties as designated by Commonwealth.

Provide operational support for data transmission (send/receive), consistent with commercial or agency standards.

The AIX and Linux platforms perform a high number of transmission files between the Commonwealth and other parties. Tools are provided to perform the file transfers using Commonwealth standards. The monitoring of file transfers has been established with the agencies and is effective to support the requirements to date. During Data Gathering Unisys will review with the Commonwealth which of the file transfers should be monitored by the Unisys Team.

Using monitoring of the scheduling tools through the tool consoles and operating system console messages, the Unisys Team will provide operational support. Should a transfer fail the Unisys Team will respond to messages or escalate to the appropriate support organization.

1.H Manage, maintain, monitor, and control online and batch process, both scheduled and unscheduled (including on-request processing).

The Unisys Team will provide batch monitoring activities using a combination of on-site and remotely located personnel (batch operators) and tools. The Unisys Team monitors the batch processing environment and provides alerts to the agencies via established processes of success and failure. The Unisys Team today provides monitoring and alerting functions. Additional services to procure the Unisys Team resources for full batch creation, scheduling and troubleshooting are available via the Enterprise Services Catalog.

1.I Maintain a log for each server detailing hardware / software configuration and critical service operations.

The Unisys Team will maintain a log for each server detailing hardware/software configuration and critical service operations using the Configuration Management Database (CMDB) and automated discovery and dependency tool. By maintaining the log for each server as an entry within the CMDB, the Commonwealth and the Unisys Team's Systems Administrators have access detailing all pertinent server information, including but not limited to hardware/software configuration, critical service operations, past errors that impact critical system Services, and major outage information. Reports from the CMDB are available to the Commonwealth via the online Services Portal.

1.J Review the system logs on a weekly basis to ensure critical system Services are processing without errors.

Document review of the system logs on a weekly basis to ensure critical system Services are processing without errors.

The Unisys Team actively monitors the system logs for processing errors. For system services operating with errors, an incident ticket will be created to track until the error is corrected. Tickets are driven through the Incident Management system described in Schedule F 3.2.1.4 "Service Desk". Additionally the Unisys Team reviews the system logs on a weekly basis and will document the reviews. The Unisys Team will collect AIX and Linux system logs and output from the OpCon and BL/Sched scheduling tools and using the report management functions within these tools, validate that critical system services are operating correctly.

1.K Complete weekly server log indicating which logs were reviewed, date and initial the log.

The Unisys Service Delivery Manager will complete a weekly server log indicating which logs were reviewed, date and initial the log. A copy of this log will be made available to the Commonwealth on the Services Portal for review. These logs will be retained for one year.

1.L Maintain and update the operational documentation for all operations procedures and Services.

The processes and procedures for providing AIX and Linux infrastructure operational support will be documented in the CCPM which will be reviewed and approved by the Commonwealth.

2 Systems, Review and Audit UNIX

2.1 Provide a review and analysis of UNIX system performance/capacity to determine if current performance/capacities are sufficient to support the needs of the UNIX stakeholders.

Offeror must perform an initial review and audit of the current UNIX usage, procedures and reports and provide an analysis of the current UNIX usage, processes and reports currently being supported.

Offeror must document its review and audit findings and recommendations.

The Unisys Team will provide a review and analysis of UNIX system performance/capacity, usage, procedures and reports and provide an analysis to the Commonwealth.

AIX:

For AIX systems, during the transition phase, the Unisys Team will bring in subject matter experts to perform an analysis of the AIX servers and their interaction with other servers in the infrastructure using a tool call [redacted]). This group will also conduct application affinity studies for the applications that reside on the AIX servers' as part of their base infrastructure. After TADDM is run and the data gathered, the Unisys Team will conduct a series of meetings with the Commonwealth to discuss the AIX servers, how they support the applications, where they may be concerns and make recommendation for the migration of the AIX data and possible consolidation. This is done before the Unisys Team takes control of the AIX environment.

Once the Unisys Team has control of the AIX environment, managing performance

necessary to achieve the Service Level requirements, we will provide monitoring, measuring, analyzing, and reporting systems performance and will work with the Commonwealth to recommend changes when performance levels threaten to fall short of the desired Service Levels.

Capacity Management includes developing and maintaining tactical and strategic plans to accommodate the Commonwealth's changing business needs. Capacity Management services include measuring system performance and providing the information to more accurately partition the resources according to meaningful workload statistics. It also provides a robust automated forecast system and an application model to forecast Service Levels and resource usage requirements for the most resource-intensive services.

The Unisys Team proposes to provide the following performance and Capacity Management Services:

1) Maintaining the tools, based upon a web portal interface, to gather monitoring information and to define the performance indicators and thresholds being monitored, including DASD, CPU, and memory.
2) Recommending and implementing, when approved, changes to resolve performance issues, address capacity problems, and optimize utilization.
3) Analyzing and reporting on performance, capacity trends, and peak period utilization using data gathered to work with the Commonwealth to determine future requirements on a quarterly basis.

Linux:

The initial review and audit of the current usage of the Commonwealth's compute infrastructure will be performed in two phases:

1) The first phase will be accomplished as the Unisys Team prepares to migrate the existing workload from each of the existing Commonwealth data centers into the new data centers. During this time, the Unisys team will deploy tools to collect and analyze all aspects of the Commonwealths current compute usage. Analysis of these workloads will be used to determine the optimal method for migrating these servers. This analysis will also serve as a baseline against which future capacity planning can be compared.
2) The second phase will occur when the Unisys Team deploys the new Capacity Planning process and tools into the Commonwealth compute environment. This phase will perform two functions, it will cover those servers not covered in phase one, and will perform a new audit once the workloads have been deployed in the new data centers.

3 Production Control and Scheduling Approach, Toolset including batch processing

3.A Offeror must describe its approach to supporting the batch processing needs of the Commonwealth including the following:

Reading the RFP documentation, it is clear that the Commonwealth considers production control and scheduling a core function of system operations. This function builds, tests, and monitors production loads and reports results to the Commonwealth and the Unisys Team. Production control executes defined processes and procedures related to the Commonwealth's

production workload, including scheduled maintenance, job control, data library levels, problem management, and change tracking. The production control activity coordinates all tasks in daily production operations. The Unisys Team will be responsible for the timely notification of each application owner for events defined by those application owners, whether they be Commonwealth of Pennsylvania agents, or other third party vendors.

The first step in providing production control and scheduling services is to work closely with the Commonwealth to get a clear understanding of requirements and dependency during Due Diligence. The Unisys Team will then incorporate these requirements into its production control process to develop a true cross platform, cross data center, unified production control and scheduling process. The objective is to achieve batch service level commitments through an efficient use of resources and technologies. For example, data will be gathered to develop statistics for the number of jobs executed per day/week/month, show the number of abends per day/week/month, etc., and provide these details to the Commonwealth via the Unisys Services Portal. This information will be used internally for problem trending and analysis, to verify that batch cycles complete in a timely manner and service level agreements are met.

The production control and scheduling function will use the Unisys Team's automated tools to open problem tickets for issues that impact production processing. The Unisys Team will track problem tickets and work with the Commonwealth for problem resolution in order to verify that production processing executes with as few interruptions as possible.

Promotions from test to production are subject to the production change management procedure that includes demonstration of successful system integration testing, as well as the Commonwealth's feedback and acceptance testing. This production change management procedure needs to be an integrated process across IT functions. The Unisys Team will work with the Commonwealth to integrate your requirements into our established, controlled production and change management procedures.

The Unisys Team will work with each the Commonwealth business unit to schedule changes into their respective production environments, following the same global production change management procedure.

Before applications are put into production, the following criteria need to be met:

- Identifying the Commonwealth operations point-of-contact.
- Determining the production change management procedure and tool to be used.
- Obtaining access to the production change management procedure and tool for project managers, project team leaders, and key project personnel who may become involved in creating production change management records.
- Establishing the timeframe requirements for entering a production change management record notifying the Commonwealth operations organization of the Unisys Team plans for introducing application changes into production.

The application maintenance organization documents the established production change approval process, including required communications and the method of obtaining authorization for promotion into the production environment.

The project manager or project team leader is responsible for communicating the plans for

introducing application changes into production to the Commonwealth operations point-of-contact. This communication is generally performed by the creation of a change management record, using the production change management tool. The project manager, project team leader, or selected project key personnel function in the role of change requester by communicating project plans to the Commonwealth operations organization. The data that must be provided to the Commonwealth operations organization includes:

- Planned date of code promotion into production.
- Backup plans should promotion fail.
- The Unisys Team application maintenance contact for the promotion.
- Listing of applications and modules involved in the promotion.
- Library location of the modules planned for promotion.

Processes and Procedures

The processes and procedures for providing Production Control and Scheduling, including batch management processing services will be developed in cooperation with the Commonwealth, its application support organizations and the Commonwealth's application owners. After completion, these processes and procedures will be documented in the CCPM which will be reviewed and approved by the Commonwealth. The scope of these processes and procedures will be based on the ITIL V3 framework as well as technology best practices for support of production control and scheduling.

Tools / Applications

The [redacted] will be used as the primary enterprise wide tool to support production control and scheduling. After an assessment during contract transition it will be determined how to transition current Unisys and IBM Mainframe batch processing from current tools and Commonwealth run production control and scheduling to Unisys operated production control and scheduling. Currently, the Unisys Team is offering a Catalog Service to migrate individual batch jobs to Unisys Team maintained and operated production control and scheduling.

The Unisys Team remote US batch operators will manage, maintain, monitor, and control online and batch process, both scheduled and unscheduled (including on-request processing), and in addition the system administrators will maintain a log for each server detailing hardware / software configuration and critical service operations. The Unisys Team will update the operational documentation.

End User Reports (Standard and Custom)

Standard Reports are summarized in Schedule F, Section 3.3.2. Examples of standard IT Service Management (ITSM) status reports for critical processes include:

- Change Management
- Incident Management

➢ Problem Management

Custom Reports are offered by Unisys via the Enterprise Services Catalog.

Tiered Service & Support Levels

The Unisys Team has provided the below tiered support level in alignment with Exhibit J.

Tiered Support Level	Description
Platinum	• Provides 99.9% Batch Processing Completed Successfully.

Escalation Procedures

Escalation procedures are part of the Incident Management Process described in F3.2.1.4 Service Desk. Escalation procedures will be configured with the [redacted] to support meeting Service Levels proactively with automated escalations when incidents are approaching SLA violations. Also, there is a proactive escalation process for incident tickets supported by the Unisys service desk which manages all escalations for normal operations. The Unisys PMO will be involved with any critical escalations as a senior Account Manager will be managing the technical response team and Service Desk communications for critical Priority 1incidents. This includes well defined communications and notifications, status updates, and procedures to support restoring services effectively and efficiently.

For additional details please see Schedule F, Section 3.2.3.2 Site Operations.

Offeror must describe how it will operate and maintain current scheduling/batch software tools.

The Unisys Team will operate and maintain current scheduling/batch software tools. The Unisys Team will maintain current scheduling/batch software tools ([redacted] and tools supporting the Unisys and IBM Mainframe environments such as [redacted] until an assessment and plan are completed during transition to either maintain current approach or migrate existing batch production control programs into one enterprise tool (i.e. [redacted]) as the Commonwealth desires for efficiency and effectiveness. Unisys will provide transition services for individual batch jobs to [redacted] as a Catalog Service.

3.B Describe the process of scheduling batch jobs within Commonwealth agency defined windows to achieve maximum performance as long as required batch completion times are met.

A cross platform (e.g. Window, Unix, and Mainframe) system will be required.

Where practicable, provide for automated scheduling of batch work and processes including

backups.

Commonwealth agencies have a number of applications that require scheduling software / batch processing software (i.e. $Universe, SAP certified, etc.), this software is heavily integrated into many of these systems.

The [redacted] application will be used for production control and monitoring and will send abnormal events to the BMC Event Management platform to automatically open incident tickets based on predefined batch monitoring events. Within the [redacted] SLA's will be managed proactively for batch production control and monitoring, and reporting with automated escalations when incidents are approaching SLA violations. Also, there is a proactive escalation process for incident tickets supported by the Unisys service desk which manages all escalations for normal operations. This includes well defined escalation, communication and status updates, and procedures to support restoring services effectively and efficiently.

The Unisys Team will operate and maintain current scheduling/batch software tools. The Unisys Team will maintain current scheduling/batch software tools ([redacted] and tools supporting the Unisys and IBM Mainframe environments such as [redacted] until an assessment and plan are completed during transition to either maintain current approach or migrate existing batch production control programs into one enterprise tool (i.e. [redacted] as the Commonwealth desires for efficiency and effectiveness. Unisys will provide transition services for individual batch jobs to [redacted] via the Enterprise Services Catalog.

3.C Develop, maintain, and utilize an emergency contact list and escalation procedures to resolve abnormally ended jobs.

The Unisys Team will develop, maintain, and utilize an emergency contact list and escalation procedures to resolve abnormally ended jobs.

3.D Resolve abnormally ended jobs caused by conditions external to production programs.

The Unisys Team will resolve abnormally ended jobs caused by conditions external to production programs. The Unisys Team will analyze exit codes in log files, and work with the job owners to correct the issue if it is code related. If the issue is an external system or external process failure, the Unisys Team will open an Incident ticket.

3.E Repair abnormally ended jobs when possible and perform job restarts in accordance with the Service Management Manual.

The Unisys Team will repair abnormally ended jobs when possible and perform job restarts in accordance with the Service Management Manual.

3.F Check job outputs and print queues, and change job priorities.

The Unisys Team will check job outputs and print queues, and change job priorities under the following conditions:

- A job or print failure is detected
- An Incident is raised by the Commonwealth end user

Any change initiated via Incident management will be made through change control. Changes will be tested in a test/development environment before being promoted to production. Additionally, Unisys will perform daily random spot checks on job and print queue logs to confirm proper completion.

3.G Notify Commonwealth agencies in accordance with the Offeror's proposed notification procedures in the event that applications do not execute properly.

The Unisys Team will notify Commonwealth agencies in accordance with our proposed notification procedures in the event that applications do not execute properly.

4 System Backup Review and Audit

4.A Offeror must describe its approach to performing an initial review and audit of the backup policies, procedures and reports, to ensure the accuracy of the backup schedules, retention periods, target directories, and recovery point objectives.

Offeror must describe its approach to identifying gaps and potential risks, and how those gaps and risks will be resolved.

The Unisys Team will conduct an initial review and audit of the backup policies, procedures and reports, to verify the accuracy of the backup schedules, retention periods, target directories, and recovery point objectives. The detailed process for conducting this audit, and how the audit findings will be communicated back to the Commonwealth can be found in Schedule F, Section 3.2.4.2, Subsection 4.

4.B Monitor system backup processing on a daily basis.

The Commonwealth benefits from the Unisys Team's approach to monitoring backup success rates. Unisys does not need to maintain staff to watch the nightly progress of backups and then intervene when the rare problem arises. In most cases simply re-starting a backup results in a successful backup because needed resources are tied up during peak times but become available a short time later. The Unisys Team automates this restart process. If the restarted backup fails then incident tickets are created to alert the team. Thus critical issues get right to Level 2 and Level 3 support personnel without even involving Level 1 support staff. On a daily basis Unisys also produces reports on backup successes.

4.C Review daily backup logs for successful completion.

The Commonwealth benefits from the Unisys Team's automated approach to monitoring backup success rates.

This automation of incident ticketing provides the Commonwealth with another advantage. During service delivery reviews the Commonwealth can review response times to failures that might put critical applications at greater risk. Through the incident severity rating processes

Unisys has the ability to adjust severity levels so that incidents that are closer to critical applications can receive prioritized support responses.

The Commonwealth can also designate application owners who require read access to the backup management console so that these individuals have ready access to monitor both the success and failure rates for backups as well as the backup content. As often happens some applications require specific bundles of directory backups and this access provides application owners a means of validating that customized backups have been implemented properly and are running correctly.

4.D Note failures, and correct the problem.

Failed backups automatically create incident tickets which are escalated from Level 1 through Level 3 support groups as necessary until resolved.

4.E Create problem record for any abnormal condition and any repairs that have been made.

Incident tickets are created automatically and create a record of abnormal conditions. Following ITIL-based processes Level 2 and Level 3 will review incidents for root causes that create multiple tickets. This identification of problems allows the team to establish workarounds and request architecture reviews as necessary. Repairs are also driven by incident tickets that are automatically generated by the Nagios collectors which review system logs for hardware. Failed backups will be automatically re-started upon a first failure because a second run of the backup is, more often than not, successful.

4.F An automated software process will be utilized to report the completion status of backup processing, with electronic notification of failures sent to Offeror technical support, and identified Commonwealth staff for follow up and corrective action.

The backup software produces daily, weekly, and monthly reports like the one shown below in **Figure 3.2.4.4-3**. The Nagios collectors in the ITSM infrastructure will create tickets automatically upon a failure of a backup for action by Level 1, Level 2, and Level 3 support as necessary. The Commonwealth can designate authorized personnel to receive notifications of these incident tickets, their status, and their resolution.

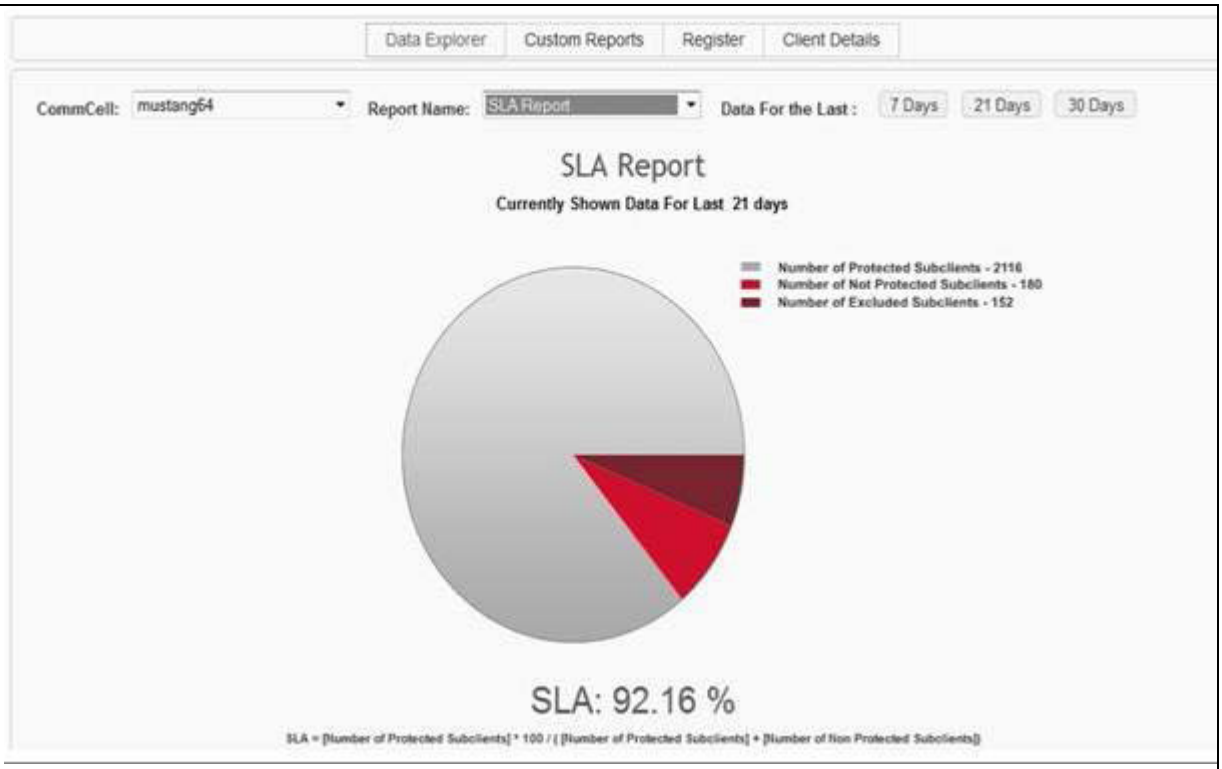


Figure 3.2.4.4-3 – Sample Backup Report

5 Staff, AIX and Linux Staff Resumes

5.A Offeror must submit a representative sample of staff resumes typically provided for these positions detailing their experience, education, and certifications.

Provide AIX and Linux trained staff that hold current manufacturer certifications for hardware and software technical support.

The Unisys Team will include qualified and certified staff to support AIX and Linux platforms. Representative resumes for personnel providing Linux and AIX Services are located in the tab marked Rep-Resumes in Section 5.0 Personnel.

5.B Provide technical advice and support to the Application Development and Maintenance (ADM) and Database Administration (DBA) staffs, as required.

The Unisys Team will provide technical advice and support to the Application Development and Maintenance (ADM) and Database Administration (DBA) staffs, as required. The first point of contact for this will be the Unisys Team's architecture office, which will be staffed with architects dedicated to the Commonwealth and its agencies. These architects can then reach back into the greater Unisys and IBM organizations to engage specific expertise as needed.

5.C Post award; provide Commonwealth with a resume or CV for each operational staff member assigned to this engagement.

Post award the Unisys Team will provide the Commonwealth with a resume for each operational staff member assigned to this engagement. Representative resumes for personnel providing Linux and AIX Services are located in the tab marked Rep-Resumes in Section 5.0 Personnel.

5.D A copy will be maintained on Offeror file.

The Unisys Team will maintain a copy of all resumes for staff assigned to the Commonwealth.

6 Service Desk, Tiered Support

6.A Offeror must describe its approach to supporting the operational and technical support needs of the Commonwealth.

To support the operational and technical support needs of the Commonwealth, the Unisys Team will deploy incident, problem and change management processes that define the flow of support from the Service Desk up through Level 3 support. These processes are closely aligned to the common IT Service Delivery platform. For more detailed information on these processes, please refer to Schedule F, Section 3.2.3.2.

Provide cost effective operational and technical support for the computing platform.

The Commonwealth of Pennsylvania has included in this RFP all the elements needed to achieve measurable and ongoing cost effective operational and technical support for the UNIX platform. Unisys will realize these cost efficiencies by properly integrating these pieces into a unified Enterprise Service Management solution. Included in the response to this RFP are tool sets that align to ITIL V3 processes. The Unisys Team will also deploy additional automation that will serve to realize further efficiencies. Finally, Unisys unique Continual Service Improvement Implementation Program will drive efficiency into the enterprise by continually reviewing outages, incidents, and other operational data to make specific recommendations to the Commonwealth to enable further efficiency.

The Unisys Team has included the cost efficiencies gained through adoption of the IT Service Management platform, ITIL V3 aligned processes utilization of a common server platform and through the deployment of automation into the solution. The efficiencies in the Unisys Team's solution are built in and reflected in the price of a resource unit.

6.B Provide platform level operational and technical support for the computing platform.

List the service levels for the various service tiers that can be provided.

In order to provide customization and flexibility to Commonwealth agencies, the Unisys Team offers tiered levels of managed services for Capacity on Demand servers. These tiers offer various levels of administrator experience, on-site coverage and responsiveness SLA's. The tiers are designed to allow for flexibility to manage mission critical as well as development or demonstration environments.

The following table highlights the available tiers and associated descriptions.

Tiered Support Level	Description
Platinum	• Provides 99.999% Application Infrastructure Availability • Server is monitoring via [redacted] • Fully Managed Services • Asset Tracked In CMDB **with relationships** • Requires 3 active servers load balanced and geographically dispersed
Gold	• Provides 99.99% Application Infrastructure Availability • Server is monitoring via [redacted] • Fully Managed Services • Asset Tracked In CMDB **with relationships** • Requires 2 active servers load balanced and geographically dispersed
Silver	• Provides 99.9% Application Infrastructure Availability • Server is monitoring via [redacted] • Fully Managed Services • Asset Tracked In CMDB **with relationships**
Bronze	• Provides 99.4% Application Infrastructure Availability • Server is monitoring via [redacted] • Fully Managed Services • Asset Tracked In CMDB **with relationships**
Basic	• Provides 98.5 % Application Infrastructure Availability • Server is monitoring via [redacted] • Fully Managed Services • Asset Tracked In CMDB **with relationships**

Based on the tired Service Levels, the Unisys Team will provide the Commonwealth a tiered approach to the UNIX environment. For the Platinum (99.999%) support level the Unisys Team will enlist all three Unisys data centers to provide an active-active-active solution with all components being fully redundant and each site supporting 50% of the peak load. Clustering will not be required for this support since the three sites will provide redundancy and will allow for planned outages in one site at a time. For the Gold (99.99%) level support, the Unisys Team will enlist two of the Unisys data centers and provide an active-active solution with all components being fully redundant with automatic failover and clustering is required. For Silver (99.9%) the Unisys Team will require only one of the Unisys data centers for production, but clustering is required. For Bronze (99.5%) and Basic support IBM a single data center is sufficient and clustering is not required. The Unisys Team will provide initial Level 2 Primary support for the Commonwealth's AIX infrastructure. If a problem should arise requiring

additional support the Unisys Team can leverage support from additional Global Delivery Center personnel as well as other resources within Unisys and its partner's organization for problem resolution.

Provide Level 2 and Level 3 Support to the Service Desk and/or Commonwealth Users.

The proposed solution includes a robust technical support staff with the necessary skills to provide the managed services requested by the Commonwealth of Pennsylvania in this RFP. The staffing levels are determined based on key performance indicators which specify the expected number of devices to be supported by each member of the technical team. The team will be staffed with junior and senior positions to provide coverage for Level 2 and Level 3 technical support requirements. Human resource actions including writing position descriptions, development plans, and funding for certifications are all targeted to verify that the technical support resources are prepared to support the managed services.

To support the operational and technical support needs of the Commonwealth, the Unisys Team will deploy incident, problem and change management processes that define the flow of support from the Help Desk up through Level 3 support. These processes are closely aligned to the common IT Service Delivery platform. For more detailed information on these processes, please refer to Schedule F, Section 3.2.3.2.

7 Monitor Network Connectivity, Toolset

7.A Ensure network connectivity to COPANET, and consistent system response times.

Offeror must describe its real-time monitoring approach and toolset to provide and maintain network availability and performance.

Unisys will provide event management solutions to help deliver network connectivity and consistent AIX and Linux systems response times. Unisys will utilize [redacted] applications to record incidents tickets that are generated from Linux server monitoring tools to provide real- time monitoring and notification of server availability and response times including the stop and start times of servers to support SLA availability measurements. SLA availability measurements are measured in [redacted] and displayed in the Real-time Dashboard SLA Portal Applications available to Commonwealth agency personnel. The following tools are the major toolsets to support network and system event management and monitoring

Monitoring Software	Managed Configuration Items (CI's)	Monitoring and Management Functionality
[redacted]	LAN Devices including: • Switches • Routers • Load Balancers • Firewalls	Provides deep network device availability and performance monitoring, DNS, IP address management, network configuration management, and network traffic bandwidth throughput monitoring

[redacted]	Microsoft and Linux servers, databases, network devices, and storage hardware.	Provides a standard set of availability, performance and critical service monitors developed by Unisys for monitoring across distributed architecture infrastructure items including: □□ Servers □□ Network devices (switches, routers, load balancers) □□ Storage devices □□ Middleware □□ Applications (Exchange, Citrix XenApp, etc.)
[redacted]	AIX servers	Provides a standard set of availability, performance and critical service monitors developed by IBM for monitoring across infrastructure items including: □□ AIX, IBM Mainframes

For a complete understanding of how this subset of Event Management Tools supports enterprise Event Management please refer to 3.2.3.2 Site Operations.

7.B Utilize automated system management tool(s) to ensure real-time monitoring and notification of server availability and response times. Stop / Start times of servers will be a source of input for SLA measurements.

Offeror must identify tools it uses to support network availability and performance.

The table above, in the answer to 7A, shows details for [redacted] the tool the Unisys Team will deploy to monitor Commonwealth connectivity. The balance of the table details the ancillary tools that will work with [redacted] to create an automated system for real-time monitoring of the Commonwealth compute environment.

For a complete understanding of how this subset of Event Management Tools supports enterprise Event Management please refer to 3.2.3.2 Site Operations.

8 Patch Management

8.A Ensure server operating systems are maintained with the current system patch level, based on the Services provided by the server.

Offeror must describe its approach to supporting the software patch needs of the Commonwealth.

Offeror must describe its approach to testing and validating updates to the OS and 3rd Party software that it supports.

The Unisys Team will follow the Commonwealth of Pennsylvania's ITB for patch policy, "ITB-SYM006 - Desktop and Server Software Patching Policy" for patching of UNIX servers.

AIX:

Software patching, validation of OS updates and outage communication is a bit different for AIX systems from other traditional platforms. An AIX system can be removed for planned hardware or software reconfiguration, maintenance, or upgrade by being dynamically redistributed across the remaining set of active systems. Once the system is ready to be brought back on line, it can be reintroduced in a non-disruptive manner and participate in dynamic workload balancing. The Commonwealth will be notified on a regular basis of scheduled or unscheduled service interruptions.

The performance of platform system administration covers the following services:

- Installation/maintenance of OS/OS patches/OS utilities.
- Problem determination/resolution for OS/OS patches/OS utilities.
- Review/recommend new OS/OS patches/OS utilities versions/patches.
- Install/upgrade OS/OS patches/OS utilities.
- Physical and logical storage management.
- Security configuration (IBM has exclusive security access control to the physical hardware, O/S and system tools, with the Commonwealth retaining responsibility for application security).
- Monitoring / support / reporting configuration setups.
- Performance monitoring and Capacity planning.
- Install and maintenance of backup software and applications.
- The Unisys team will setup and perform backup/recovery of OS and OS utility files. Unisys will provide Backup/ Recovery of files.
- Assist with automation efforts for system administration labor tasks.
- Report on related Service Levels.
- Provide technical support for application developers and the Commonwealth management.
- Participate in the Change Management and Problem Management processes.
- Provide [redacted] support.

Linux:

The toolset to support the automation of patch release and deployment is [redacted] Unisys will maintain in this toolset the appropriate patch policies for determining patch deployment and compliance. The [redacted] will be maintained with all the current patches supplied by the OEM's and will be used to manage the production state of patch deployment in the Linux environment. The following table shows all tools utilized in the management of Linux system patches.

Tool	Functionality

[redacted]	1. Maintains all current patches for the Linux operating systems 2. Performs the patching of systems.
[redacted]	Provides the following functionality related to patching: • Incident management • Change management
[redacted]	Configuration Items (CI) are automatically updated as needed post patching.
[redacted]	Updates the CMDB with needed additions to the CI

Unisys approach to testing and validating updates to the OS and 3rd party software is to follow the Release Process for all changes into all production environments. The Release Process includes:

- Change ticket approvals
- Test planning and accepted test results
- Release and deployment planning including release back out plans
- Release testing for risky deployments
- Early life cycle support to deliver a successful deployment
- Release back out for failed releases

8.B Analyze monthly service patches and determine which patches need to be applied, by server type.

The Unisys System Administration will analyze monthly service patches and determine which patches need to be applied, by server type. A recommended patch report will be reviewed with the Commonwealth. Upon Commonwealth approval, an implementation plan will be jointly developed. The implementation plan will list all activities to be performed in the patching of the server, contacts to call to test the server post-patch, test plans, and back out plans should the patch or testing fail.

8.C Create a change record, log the update in the server log, and install based on server availability schedule.

In accordance to the approved implementation plan, the Unisys System Administration team will create a change record in the Change Management System, log the update in the server log, and install the patch based on server availability schedule.

8.D Change requests will be approved and authorized using the change management process.

Before the patch is applied to the server, the Unisys team will confirm change requests are approved and authorized by the Commonwealth Change Authorization Board, as well as each agency with an interest in the server being patched, using the change management

process.

8.E Notify the Commonwealth of any scheduled or unscheduled service interruptions.

Offeror must describe its approach to communicating unscheduled and scheduled outages, including escalation process.

Unisys approach to communicating unscheduled outages is to send notifications to key stakeholders for the Commonwealth/Agencies/Unisys/Third Parties depending on the outage. This will be through email, voice, Services Portal and Remedy broadcast capabilities. The same communications will be used for scheduled outages with additional communications in forward schedules of change reports.

Escalations for unscheduled outages are handled through the standard processes for managing incidents. Unisys service desk will manage all incidents and verify that proper escalation communications to key Commonwealth/Unisys/Third Parties personnel are managed. The [redacted] will also be configured to escalate incident tickets based on incident priorities and SLA's to verify that incidents tickets are being managed to SLA times for incident response and resolution.

8.F Implement a Patch Management Program to ensure the timely application of updates on all infrastructure platforms in accordance with Commonwealth IT policy guidelines.

The Unisys team will work with the Commonwealth to implement a patch management program that provides timely application of updates to all infrastructure platforms, in accordance with the Commonwealths IT policies and guidelines, and as described by the answers to the previous sub-requirement 8A.

9 User Account Management

9.A Provide certified system administration staff to create and maintain the registration of profiles, associated groups, and the security permissions required to service the approved client base of the system and application.

Offeror must describe its approach to supporting the needs of the Commonwealth.

The Unisys Team will provide user, profile, group, and security permission management on individual AIX or Linux servers. Unisys recommends that the Commonwealth agency user account teams submit requests to have OS level user account changes made by Unisys. However, the Commonwealth's authorized personnel performing agency user account management for the AIX or Linux systems which require OS user account changes can be provided with the appropriate privileges to make user account changes. All changes for user account management will be initiated through the service request and change management process and will require an approved change record for implementation. The process for user account management will be documented within the CCPM.

10 Procurement Management

10.A Provide program and processes to refresh the hardware at asset end-of-life, and when upgrades are needed to meet anticipated growth in utilization.

Offeror must describe its approach to supporting the needs of the Commonwealth.

Procurement management is defined by the Unisys as Technology Refresh and as Capacity

Management and Forecasting. These two are further defined as follows:

a) Technology Refresh Plan

i) As part of the overall architecture support, the Commonwealth's environment will be reviewed on a quarterly basis to identify technology, services or components which require replacement to maintain the Commonwealth's business needs and associated service levels. The review will include the following activities. The overall technology refresh plan will be documented in Key Deliverable D-03. This plan will be used for all Unisys supported environments including the Commonwealth UNIX systems.

ii) Using the data within the Asset Management and Configuration Management databases, identify the technical components within the UNIX system environment which require replacement within the next 18 month period based upon the a 60 month replacement cycle.

iii) Review End of Sales and Service Life notices from the Manufacturers to validate if a component has been discontinued or has available ongoing maintenance options.

iv) Review ongoing Capacity and Performance reports to identify components with a refresh requirement which have additional needs driving a requirement or opportunity to change the component's classification to a different component to maintain the functionality and service levels.

v) Identify replacement technical components based upon the current Enterprise Services Catalog offerings

vi) Validate replacement technical components meet the current requirements for the impacted Commonwealth applications.

vii) Identify risk and impact for the Commonwealth environment to replace existing technical components or services.

viii) Create technology refresh recommendations, impact statements, and high level implementation plan.

ix) Present the technology refresh plan to the Commonwealth using the solution architecture review process.

x) Upon approval of the refresh plan, open service requests for each migration group and develop the detailed project plan for the migration plans.

b) Capacity Management and Forecasting

i) The Commonwealth UNIX systems will be monitored and reported from the Event Management Platform ([redacted] and from the [redacted] to support the UNIX Capacity Management requirements. As part of the Capacity and

Performance Management processes, , the performance and capacity reports will be generated and reviewed with the Commonwealth on a regular basis.

ii) During transition the UNIX environment capacity requirements will be assessed as part of the establishment of the Performance and Capacity Management Processes described in Schedule F, Sections 3.2.2.6 and 3.2.2.2. The assessments will be used to generate capacity and performance management recommendations and plans. . The Unisys Capacity Manager and Performance Analyst will work with the Commonwealth/Agencies to forecast AIX/Linux workload requirements in order to support the current and forecasted workload, as well as establish the monitoring requirements to support the ongoing daily assessment of the workload performance on the windows platform in total and by agency. Any recommendations to increase, modify or decrease UNIX systems capacity will be processed through the Change Process after reviewing recommendations with Commonwealth Stakeholders in the Capacity and Performance regularly scheduled meetings where trends, issues and forecasts are discussed and reviewed.

iii) As part of the annual Capacity and Forecast planning activity, the Unisys Team will work with the Commonwealth to identify what changes in growth are expected and provide recommendations on additional upgrades.

iv) In addition to the Commonwealth's growth forecasting information, the Unisys Team will use the data within the Capacity Management, Asset Management and Configuration Management databases and identify the technical components within ERP system environment which require upgrades or additional infrastructure to support the forecasted growth requirements.

v) Identify replacement or upgrade technical components based upon the current Enterprise Services Catalog offerings and the vendor's available products.

vi) Validate that the identified upgrades or additional components meet the current and forecasted requirements for the impacted Commonwealth ERP system.

vii) Identify risk and impact for the Commonwealth UNIX systems to upgrade or add additional components.

viii) Create the capacity upgrade recommendations, impact statements, and high level implementation plan.

ix) Present the capacity upgrade plan to the Commonwealth using the solution architecture review process.

x) Upon approval of the capacity upgrade plan, open service requests for upgrade project and develop the detailed project plan.

11 SLA Reporting

11.A Collect actual system availability, utilization and response time data.

The purpose of establishing a strong SLA reporting framework is to provide transparency into

the Commonwealth's vendors in its various technical towers. This framework must consist of industry best tools and processes, and should be developed in cooperation between Unisys, Unisys partners, the Commonwealth, and other Commonwealth vendors. The end result of this cooperative effort should be an SLA reporting framework that delivers the following:

- The establishment and maintenance of open communications with the Commonwealth through the governance structure, which encompasses regular meetings and delivers regular reports, many of which are available for the Commonwealth to access online.
- A process to work collaboratively with the Commonwealth to update the Service Level Document when services or service levels are created or modified based on a mutually agreed to process.
- Monitors and reports adherence to Service Levels.
- Verify that service level commitments are met by regularly reviewing service level commitments, compared with actual service level attainment.
- Take corrective actions based on root cause analysis to reduce the impact of future service level failures.
- Define needed monitoring and service level reports.
- Review service operations through management and technical reviews to analyze service level related measurements and take action.
- Identify when changes are required to the Service Levels

The Unisys Team will establish an SLA process and technical architecture to support all SLA's for this contract. See the overview in F3.2.1.2 Availability/SLM. Level 1 of the SLM process is outlined below in **Figure 3.2.4.4-4**:

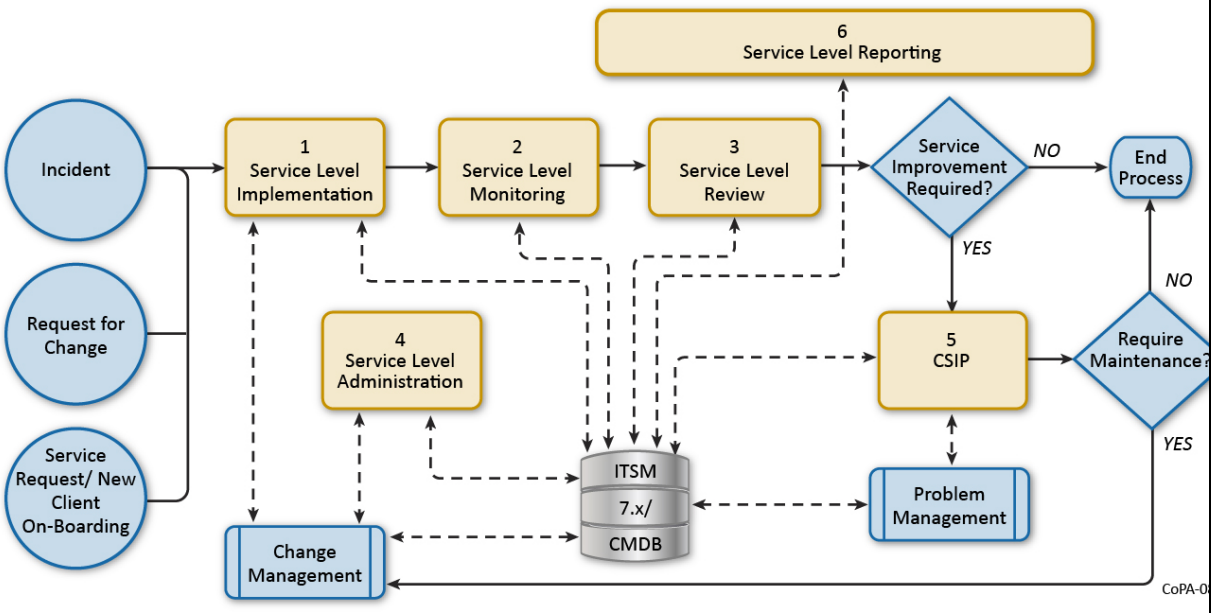


Figure 3.2.4.4-4 – SLM Process

Unisys will provide a detailed set of processes and procedures to support Service Level Management during transition of this contract. The process and procedures will support this

top level view of the process which includes:

1) Service Level Implementation
2) Service Level Monitoring
3) Service Level Review
4) Service Level Administration
5) Service Level Improvements (CSIP)
6) Service Level Reporting

The Unisys Team will provide the technical architecture and toolsets to support monitoring and maintaining service levels for the windows platform .The [redacted] will be used as the single unified platform to manage Service Level Agreements for Commonwealth agencies. [redacted] provides a continuous real-time platform for defining, measuring, monitoring, reporting, and reviewing the performance of SLA's to make sure that adequate levels of service are delivered in alignment with the Commonwealth's objectives for service delivery. The business contract will contain agreements in which the levels of service are specified. These agreements consist of individual service targets or goals that are used to evaluate whether the agreement is in compliance.

The [redacted] Application uses all the other [redacted] modules as inputs to determining if an SLA is in compliance. The [redacted] modules used for transaction inputs to determine if service level targets and goals are in compliance include:

- Incident Management
- Problem Management
- Change Management
- Asset/Configuration Management
- Performance/Capacity Management

11.B On a monthly basis, create a Service Level Agreement report for the Commonwealth and Vendor Management teams.

Offeror must describe its approach to supporting the needs of the Commonwealth.

The [redacted] and in some unique cases other tools as described in F3.2.1.2 will be used to push near real time SLA reporting data into the Real-time Dashboard reporting tool. The Agency Account Manager will review the monthly SLA report with the Commonwealth representatives.

See **Figure 3.2.4.4-5** for sample dashboard snapshot.

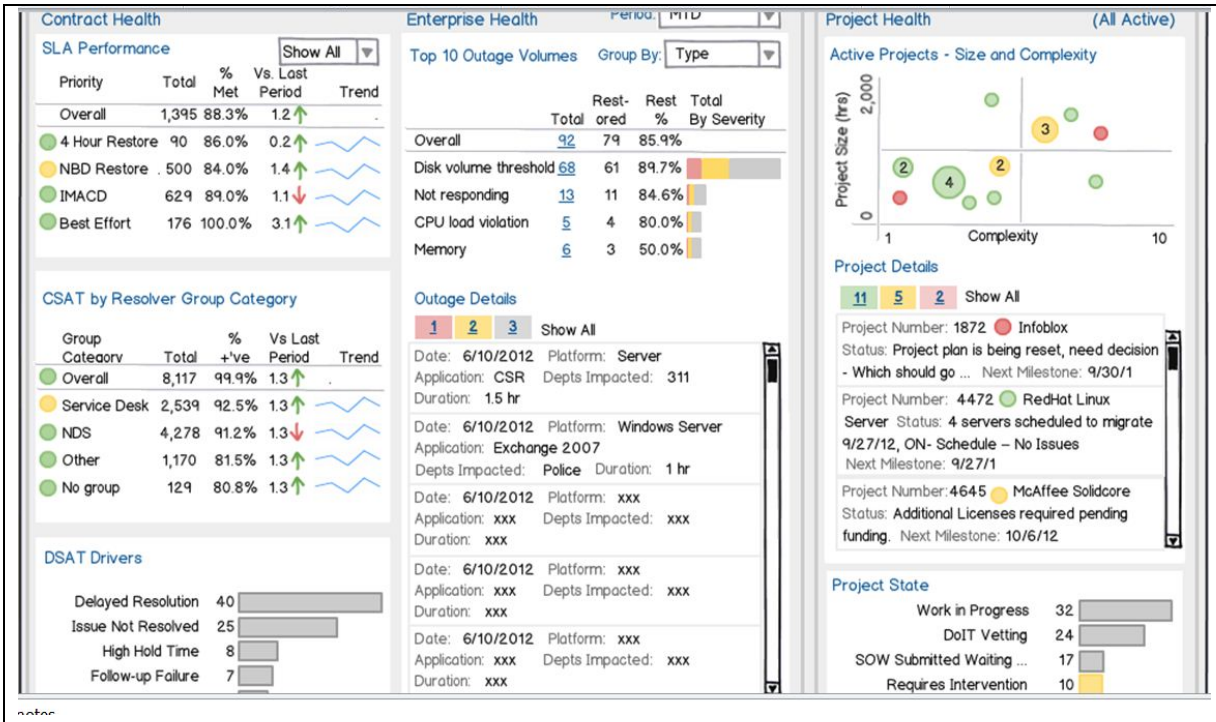


Figure 3.2.4.4-5– Sample Real-time Dashboard snapshot

12 Software License Management

12.A The Offeror must provide Software License Management.

Offeror must describe solution and approach to meet this requirement.

The Unisys Team will provide Software License Management for all infrastructure including UNIX platforms. The Unisys Team will provide 3rd Party License Management service for the Commonwealth and Unisys provided infrastructure software products. Unisys will be solely responsible for the management of all infrastructure software license products provided through this contract.

AIX:

For the AIX operating system, the Unisys Team uses a Definitive Software Library (DSL) to control the master copy of all production software, as well as related software licenses and controlled documentation for each release. We will also use a Definitive Hardware Store (DHS) to control spare components that are maintained at the production configuration level for use in recovery situations. Check-in and check-out of DSL and DHS components are strictly controlled by established release management procedures. Through our standardized process and version control, we validate that the software and hardware being rolled out are secure and traceable, such that only authorized versions are installed.

Linux:

The Unisys team will provide Software License Management for all infrastructure including Unix platforms. The Unisys team will provide 3rd Party License Management service for the Commonwealth and Unisys provided infrastructure software products. The goals of this service are to:

- Verify software contract compliance (to avoid non-compliance legal issues and expenses)
- Manage costs of software inventory by matching requirements for use to needs
- Confirm software maintenance contracts are maintained on schedule through early notifications

Unisys will coordinate with the Commonwealth to confirm compatibility between Commonwealth provided applications related software, and Unisys provided infrastructure software.

The following is the approach Unisys will execute during transition and as an ongoing process to provide 3rd party software license inventory and tracking per agency related infrastructure:

- Load all Unisys and Commonwealth software asset license contract information into the [redacted] application
- Load all software license certificate , license type, entitlements, manufacturer, and product information into the [redacted] e for the Software License Contract
- Run discovery through [redacted] to identify all software installations
- Run the [redacted] to build relationships between the discovered software CI's recorded in the [redacted] and the license certificates
- Run the [redacted] and [redacted] to identify noncompliant licenses and inventory for the Unisys and Commonwealth Asset Managers to audit the completeness and accuracy of the information
- Identify discrepancies in the information and make corrections
- Rerun Compliance Reports and 3Rd party software license inventory reports to get signoff from the Commonwealth and Unisys Asset managers that inventory is properly linked to license certificates in the production environment and the information is complete and accurate
- Provide notifications to Commonwealth/Agencies/Unisys and other Commonwealth service providers when there are software compliance issues or requirements for licenses to be purchased or retired from analysis of license inventory.

Continual Service Improvement

Unisys recognizes the significant importance of Quality and Continuous Service Improvement to:

- Reduce service risk,
- Improve service quality,

- Improve client satisfaction,
- Provide service transparency, and
- Improve/reduce costs of service.

Through a continuous cycle of evaluation and improvement within an IT infrastructure, Unisys views quality and continuous service improvement as a critical success factor in driving customer satisfaction for the Commonwealth IT infrastructure. Each of the continuous service improvement areas identified above are driven through the tight integration of the following organizations, industry tools, proven processes and quality deliverables:

- Service Excellence Office,
- Quality Plans: transition and steady state service delivery
- Industry standard frameworks and methodologies: ITIL, ISO, SSL
- Industry accepted measurement tools
- Continuous Service Improvement & Innovation Processes (CSIIP)
- Risk management, audits and business continuity management
- Client Satisfaction Surveys and Knowledge Management Portal

Collectively this represents Unisys Integrated Quality Plan for the Commonwealth of Pennsylvania.

Specifics on each of these areas are outlined in Schedule F, Section 3.2.1.1.6 Continuous Service Improvement. Highlights from this section are outlined below and requested service examples are provided at the end of this section.

13 CI Service Risk

13.A Reduce service risks.

Offeror must provide methods to eliminate or mitigate service risks.

Risk management, independent quality audits, and business continuity management are integral quality management processes. Unisys is committed to managing risks and facilitating the achievement of business objectives the adherence to quality processes. We mitigate risk through the implementation of tight quality controls: standard policies, procedures, roles, risk assumptions, issues, and definitions, etc.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

14 CI Service Quality

14.A Improve service quality.

On a quarterly basis, Offeror must also recommend to the Commonwealth team any system changes that would be appropriate to maintain or improve SLA commitments.

The quality approach begins with the Service Excellence Office who provides definition and oversight of all ITIL process management and analysis functions. Process managers and analysts working in the Service Excellence Office are responsible for auditing process effectiveness, ensuring that service delivery teams comply with proper execution of processes, and analyzing process trends for anomalies. Continuous service improvement programs in collaboration with Commonwealth agencies are managed by the Service Excellence Office.

Through our Continuous Service Improvement and Innovation Process (CSIIP), the SEO reviews, analyzes and makes recommendations on improvement opportunities in each ITIL lifecycle phase. Unisys will leverage Six Sigma Lean tools and methodologies as well as ISO Certified internal audits to measure and maintain the highest quality services to the Commonwealth.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

15 CI Client Satisfaction

15.A Improve client satisfaction.

Offeror must provide examples of previous Offeror initiatives aimed at continually improving client satisfaction.

Client satisfaction is extremely important to Unisys and a key focus in our IT solution. The SEO will integrate new agencies, customers and services into our multi-pronged client satisfaction approach that includes Service Desk surveys on the caller's experience, an overall agency satisfaction survey, and quarterly surveys with the Office of Administration. Data collection will be gathered across multiple levels to gain a clear understanding of the Commonwealth's satisfaction with the IT Services being provided.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

16 CI Service Transparency

16.A Ensure service transparency.

Offeror must provide methods and practices to ensure service transparency, providing visibility into service execution.

The service organizations will use standardized ITSM services processes, IT monitoring and automation tools. ITSM processes will be documented in the Commonwealth Computing Procedures Manual (CCPM). The CCPM will be available to Commonwealth approved staff on the Knowledge Management Portal (KMP) providing desired transparency into service execution processes. Through the Real-time Dashboard, the Commonwealth will have access to current operational performance of their application infrastructure.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

17 CI Reduce Cost of Service

17.A Improve/reduce cost of service.

Offeror must provide examples of Storage Management initiatives that have been implemented or can be utilized to achieve reduced costs of Services and to meet or exceeded ROI (Return on Investment) analysis projections.

The Service Excellence Office will proactively manage quality, continuous service improvement, ITIL process management, and customer satisfaction through a comprehensive quality plan that specifically addresses all of these areas. We believe this is a key differentiator in our partnership with the Commonwealth. Through this new organization and these quality plans, Unisys will drive best in class services and the highest customer satisfaction experience, while reducing overall costs to the Commonwealth.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

Unisys examples of continuous improvement

Examples of continuous service improvement have been included below under Unisys Team Experience.

Unisys Team Experience

A few examples of Server Management Continuous Service Improvement that have been implemented or can be utilized to achieve reduced costs of Services and to meet or exceeded ROI (Return on Investment) analysis projections are outlined below:

- American Red Cross
  Unisys hosts the client's mission-critical computing environment in the Unisys [redacted] data center which has been qualified to operate regulated biomedical systems. The data center is instrumented with the Unisys Enterprise Systems Management platform and fully integrated it into the ITSM infrastructure, giving the client an end-to-end solution that provides management and monitoring across the enterprise from a single command center. Included in this support are 160 IBM AIX systems. The standard monitoring platform runs on a Linux platform. Since the client went live in June 2012, they have experienced outstanding service delivered consistently across the enterprise and are achieving the value that was expected from their business case for the portions of the program that have been implemented to date. In the data center, we are achieving 99.9% uptime at a 40% lower cost than with their previous provider.

- City of Chicago
  Moving Linux virtual guests to Red Hat Enterprise Virtualization for the City of Chicago is saving many thousands of dollars in [redacted] licensing costs. Additionally, using Red Hat Enterprise Virtualization for Chicago Police Department decreased the startup costs for a virtual solution from $30,000 to $3,000.

- Live Partition Mobility Project – PLCB
  In July 2011 the DPH began the High Availability/LPM project which ran through September 2011. This project benefited PLCB by minimizing down time for any planned/unplanned outages. By Implementing LPM the DPH team is able to migrate

virtual machines (LPARS) from one physical frame to another, thus allowing maintenance to occur in a non-disruptive manner minimizing planned and unplanned outages. This improvement also enhanced the overall utilization of existing hardware and maximizing storage flexibility.

- Server Management:
  VM replication was implemented to improve the Recovery Point Objective of our Netbackup master servers from 24 hours down to approximately 6 hours. This change will also lower the time it takes to recover the Netbackup server in the DR environment from 2.5 hours to around 30 minutes expediting the start of DR database recovery efforts by almost 80%.

- AIX Server Recovery Improvements:
  To improve disaster recovery times, we converted AIX mksysb to iso images to facilitate a much faster server recovery time. Prior to this change, we used CD images or mksysb restores from tape. This resulted in an 85% improvement in recovery times.

- Server Virtualization Technologies:
  The DPH has deployed virtualization technologies that have improved troubleshooting and recovery efforts for several Commonwealth agencies. The DPH is able to create a test image from an existing production system through cloning. This live cloning capability allows the DPH to clone live running servers with near zero impact to the production system allowing diagnostics to occur on the cloned virtual machine as opposed to the production environment as was done in the past.

- Server Virtualization Technologies:
  The DPH has also provided the Commonwealth access to a [redacted] feature called Change Block Tracking that enables emergency restores of customer servers in as little as 15 minutes during monitored test windows. The agency puts in a change project request to take a snapshot of the existing system turning on Change Block Tracking allowing for expedited restoration of the server as needed. Most server restores prior to this capability were taking as long as 2 hours to restore/recover.

Benefits to the Commonwealth

The Unisys Team's UNIX infrastructure design was designed to deliver value to the Commonwealth through the following attributes:

- Standardization – by standardizing on IBM's Flex System platform for Windows, Linux, AIX and Capacity on Demand, the Unisys brings a powerful, cross platform capability to the Commonwealth.
- Efficiency – Utilizing IBM Flex System across multiple platforms drives efficiency into all process, from patch management to service delivery, resulting in year over year efficiency gains that benefits the Commonwealth throughout the length of the contract.
- Manageability – The common IT Service Management platform is leveraged across all hardware platforms, allowing for even more efficiency at the service delivery level. The capability to manage and maintain the full breath of the Commonwealth enterprise in a single, highly integrated toolset will allow the Unisys Team to offer new services in the future to meet changing demands.
- Optimization – Through a rigorous capacity management process and toolset, the Unisys

Team will aggressively optimize existing capacity, and allow us to make timely, specific virtualization and consolidation recommendations to the Commonwealth to meet its goal of increased virtualization and to prevent virtual sprawl.

- Automation – The Unisys Team will use the same Enterprise Services Catalog and automated run books to provision and manage Windows systems as the Commonwealth. The tools being deployed allow for increased automation across the enterprise in ways that will directly benefit the Commonwealth.
- Agility – With all the standardization being done, it would be very easy to lose sight of the need for an agile infrastructure. By utilizing Flex Systems for Windows and UNIX, the Commonwealth will have the ability to quickly reconfigure systems due to changing regulatory frameworks, even down to the ability to isolate workloads on AIX, Windows and Linux within the same chassis, a capability unique in the marketplace. In short, the server infrastructure can be rapidly changed as need to meet challenges in the future.

3.2.4.5 Mainframe Services

The Mainframe Services will provide hosting and operational support Services for both IBM and Unisys mainframe systems. These mainframe systems run several Logical Partitions (LPAR's) and Integrated Facility for Linux (IFL) partitions. Offeror must support the mainframe operating systems and the management of the associated partitions. The number of support staff members required to perform the tasks listed below will be determined by the Offeror.

Listed below are the basic Services required to manage the Mainframe systems required by the Commonwealth. Offeror must include these Services in addition to the base level of Services in this Offering.

Reference Documentation

Exhibit B.1 DPH - Asset List

Exhibit B.3 DPH - Commonwealth Software Asset Listing

Exhibit B.4 - DPH - Third Party Software

Exhibit B.5 DPH - Agency Disaster Recovery Matrix

Exhibit B.6 - DPH - COPA NETWORK

Requirements		Describe Compliance
1.	Provide Mainframe systems and operations (Unisys, IBM). Ability to purchase metered IBM &	Offeror must describe its approach to supporting the needs of the Commonwealth including the following:

	Unisys Million Instructions Per Second (MIPS). Monitor local operations, troubleshoot and resolve operational issues. Actively monitor the daily operations of all mainframe (current) systems. Assume responsibility for all master and subordinate console functions. Issue operator commands to control all In-Scope platforms throughout the organization. Provide all tools and apps that are currently being provided, for example MAPPER/APPMAP, browser based terminal emulation access, and middleware components (like OpenTI, IBM WBM & WMQ, etc.) that are critical to agency operations and application usage. Assume the responsibility for and perform all console operations. Monitor the performance of online interactive traffic and take appropriate action to resolve online-system-related incidents and/or problems, including escalating (as appropriate) the incident and/or problem to the proper Level 2 Support group. Monitor the transmission of files between the Commonwealth and any other parties as designated by the Commonwealth. Provide operational support for data transmission (send/receive), consistent with commercial or agency standards. Manage, maintain, monitor, and control online and batch process, both scheduled and unscheduled (including on-request processing).	• Processes and Procedures • Tools / Applications • End User Reports o Standard o Custom • Tiered Service/Support Levels • Escalation Procedures

	Maintain a log for each system detailing hardware / software configuration and critical service operations. Review the system logs on a weekly basis to ensure critical system Services are processing without errors. Maintain and update the operational documentation for all operations procedures and Services.	
2.	Provide a review and analysis of mainframe usage to determine if current usage is required to support the needs of the mainframe stakeholders. Offeror must perform an initial review and audit of the current mainframe usage, procedures and reports and provide an analysis of the current mainframe usage, processes and reports currently being supported. Offeror must document its review and audit findings and recommendations.	Offeror must describe solution and approach to meet this requirement.
3.	Production control and scheduling (including batch jobs) Provide a process of scheduling batch jobs within Commonwealth agency defined windows to achieve maximum performance as long as required batch completion times are met. Provide for automated scheduling of batch work and processes including backups. Provide the capability for agencies to schedule and monitor batch processing. Develop, maintain, and utilize an emergency contact list and escalation	Offeror must describe solution and approach to meet this requirement.

	procedures to resolve abnormally ended jobs. Resolve abnormally ended jobs caused by conditions external to production programs. Repair abnormally ended jobs when possible and perform job restarts in accordance with the Service Management Manual. Check job outputs and print queues, and change job priorities. Notify Commonwealth agency customers in accordance with the notification procedures in the event that applications and batch processing do not execute properly.	
4.	Batch Monitoring Actively monitor batch operations on all mainframe systems on a daily basis. Maintain a log for each batch system and review the system logs on a daily basis to ensure key batch Services are processing without errors. Document review of the system logs on a daily basis to ensure critical batch Services are processing without errors. Notify Commonwealth agencies in accordance with the notification procedures in the event that batch processing does not execute properly. Offeror must provide online monitoring of batch processing by the Commonwealth.	Offeror must describe its approach to supporting the needs of the Commonwealth. Offeror must describe its approach to allowing Commonwealth users to monitor the batch processing online.
5.	Monitor system backup processing on	Offeror must describe its approach to performing an initial review and audit of the backup policies, procedures and reports, to

	a daily basis. Process to review daily backup log for successful completion. Note any failures, initial and date the log, and correct the problem. Create problem record for any abnormal condition and any repairs that have been made. Automated software process will be utilized to report the completion status of backup processing, with electronic notification of failures sent to Offeror technical support, and identified Commonwealth staff for follow up and corrective action.	ensure the accuracy of the backup schedules, retention periods, target directories, and recovery point objectives. Offeror must describe its approach to identifying gaps and potential risks, and how those gaps and risks will be resolved.
6.	Provide cost effective, operational, and technical support for the computing platform. Provide platform level operational and technical support for computing platforms including Mainframe, Storage, AIX, LINUX, SAP, Oracle and Windows architects. Provide Level 2 and Level 3 Support to the Service Desk and/or Commonwealth Users. Provide technical advice and support to the Application Development and Maintenance (ADM) and Database Administration (DBA) staffs, as required. List the service levels for the various levels of service tiers that can be provided. See **Schedule J.1 Datacenter Service Level Management** for the definitions of the expected options.	Offeror must describe its approach to supporting the needs of the Commonwealth.
7.	Ensure network connectivity to	

	COPANET, and consistent system response times. Utilize automated system management tool(s) to ensure real time monitoring and notification of system availability and response times. Stop / Start times of servers will be a source of input for SLA measurements	Offeror must describe its real-time monitoring approach and toolset to provide and maintain network availability and performance. Offeror must identify tools it uses to support network availability and performance.
8.	Ensure operating systems are maintained with the current system patch level, based on the Services provided by the server. Analyze monthly service patches and determine which patches need to be applied. Create a change record, log the update in the system log, and install based on system availability schedule. Notify the Commonwealth of any scheduled or unscheduled service interruptions with consideration to Commonwealth scheduled holidays and standard workweek. Implement a Patch Management Program to ensure the timely application of updates on all infrastructure platforms in accordance with Commonwealth IT policy guidelines.	Offeror must describe its approach to supporting the needs of the Commonwealth. Offeror must describe its approach for testing and validating updates to the OS and 3rd Party software that it supports. Offeror must describe its approach to communicate unscheduled and scheduled outages, including escalation process.
9.	User Account Management Provide certified system administration staff to create and maintain the registration of profiles, associated groups, and the security permissions (including password management) required to service the approved client base of the system and	Offeror must describe its approach to supporting the needs of the Commonwealth.

	application.	
10.	Procurement Planning Provide a program and process to refresh the hardware at asset end-of-life, and when upgrades are needed to meet anticipated growth in utilization	Offeror must describe its approach to supporting the needs of the Commonwealth.
11.	SLA Reporting Collect actual system availability, utilization and response time data. Create a SLA report on a monthly basis, for the Commonwealth and Offeror.	Offeror must describe its approach to supporting the needs of the Commonwealth.
12.	The Offeror must provide Software License Management.	Offeror must describe solution and approach to meet this requirement.
13.	Coordinate at an agency level and account for any required patching as technology upgrades require.	Offeror must describe its approach to supporting the needs of the Commonwealth.
Continual Service Improvement		
14.	Reduce service risks. Methods to eliminate or mitigate service risks.	Offeror must describe its approach to supporting the needs of the Commonwealth
15.	Improve service quality. On a quarterly basis, make recommendations to the Commonwealth team any system changes that would be appropriate to maintain or improve SLA commitments.	Offeror must describe its approach to supporting the needs of the Commonwealth.
16.	Improve client satisfaction.	Offeror must provide examples of previous Offeror initiatives aimed at continually improving client satisfaction.
17.	Ensure service transparency. Methods and practice to ensure service	Offeror must describe its approach to supporting the needs of the

	transparency, providing visibility into service execution.	Commonwealth.
18.	Improve/reduce cost of service.	Offeror must provide examples of Mainframe Support initiatives that have been implemented or can be utilized to achieve reduced costs of Services and to meet or exceeded ROI (Return on Investment) analysis projections.

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

Introduction

The Unisys Team has evaluated the exhibits and schedules and the requirements stated in the Mainframe Services section of the RFP as a basis for the solution provided. The Unisys Team is uniquely positioned to provide Mainframe Services to the Commonwealth due to the fact the team is responsible for all manufacturing, support and innovation for the Commonwealth mainframe platforms. In addition the team has many years of experience not only supporting the requirements of the Commonwealth but all users of Unisys and IBM mainframe technologies worldwide.

Commonwealth has an over 30 year history of supporting mission critical applications using Unisys and IBM Mainframe technology. In support of the Commonwealth the Unisys Team has provided both platform and operational support for the mainframe platforms for over 13 years under the current Data Powerhouse contract with high levels of client satisfaction. The Commonwealth benefits from having the mainframe suppliers being its operational and technical support staff in that new features and functionality introduced within the mainframe environments have been introduced to the Commonwealth agencies during application deployment planning processes.

The Unisys Mainframe offering will continue to provide the Commonwealth with the hardware and software platforms, tools and mainframe operations and support staff required to support their mission critical application services.

The Unisys Team will deliver Mainframe services to the Commonwealth that include the following:

- New Mainframe platforms to replace the current technology on the floor
- New per MIP pricing for Mainframe Services
- Implementation and transition services to migrate the mainframe environments from the existing to the new data centers with reduced risk and minimal downtime to the agencies
- Existing tools and utilities utilized by the Commonwealth agencies to support their application processing requirements

- Ongoing support for the mainframe operating system software suites
- As needed, compiling, mapping, and linking programs
- Management of the operating environment ensuring optimal operating system performance
- Monitoring local operations, troubleshooting and resolving operational issues associated with the mainframe operating systems
- Maintaining a log for each partition detailing hardware and software configurations and critical service operations
- Monitoring system backup processing on a daily basis
- Providing trained staff holding manufacturer recognized certifications for hardware and software technical support
- Providing platform level operational and technical support for the computing platform based on service level selected
- Working in conjunction with other technical disciplines to provide advice and support as required
- Ensuring mainframe operating systems are maintained with the current patch level in accordance with services provided on that server
- Utilizing the change management process, preparing proper documentation to be used when changes are necessary in the environment
- Reviewing and analyzing system performance and capacity to determine if current performance and capacities are sufficient to support the needs of the Commonwealth
- Creating and maintaining the registration of profiles, associated groups, and the security permissions required to service the approved client base of the operating system
- Accountability for the mainframe platform availability
- Network connectivity into COPANET
- SLA and other reporting as detailed in the RFP requirements

Unisys mainframe services continue the long history of providing a mission critical processing environment for both the Unisys and IBM mainframes. In the sections that follow the Unisys Team describes in greater detail how the solution meets the Commonwealth's requirements. All Unisys and IBM mainframe services will be managed from the ITIL service reference model. Tools specific to both environments are employed where necessary but the operation is ultimately orchestrated and responsive to the common service management environment described in Unisys response to Schedule F's section 3.2 subsections.

In response to the requirements stated in the Mainframe Services Section the Unisys Team has separated responses into two technical towers. The first tower is around Unisys Mainframe Services and the second is the IBM Mainframe Services. While there are many similarities and commonality between functions such as ITSM, notification and reporting and support services, there are other areas which are unique to the platform that warrant separate responses.

Unisys Mainframe

1 Mainframe Operations Approach

1.A Offeror must describe its approach to supporting the needs of the Commonwealth including the following:

Processes and Procedures

Tools / Applications

End User Reports (Standard and Custom)

Tiered Service/Support Levels

Escalation Procedures

Provide Mainframe systems and operations (Unisys, IBM).

Processes and Procedures

The processes and procedures for providing Unisys Mainframe infrastructure managed services will be documented in the CCPM which will be reviewed and approved by the Commonwealth. The scope of these processes and procedures will be based on the ITIL framework as well as technology best practices for support of Unisys Mainframe platforms.

Processes and procedures will be developed for the following areas:

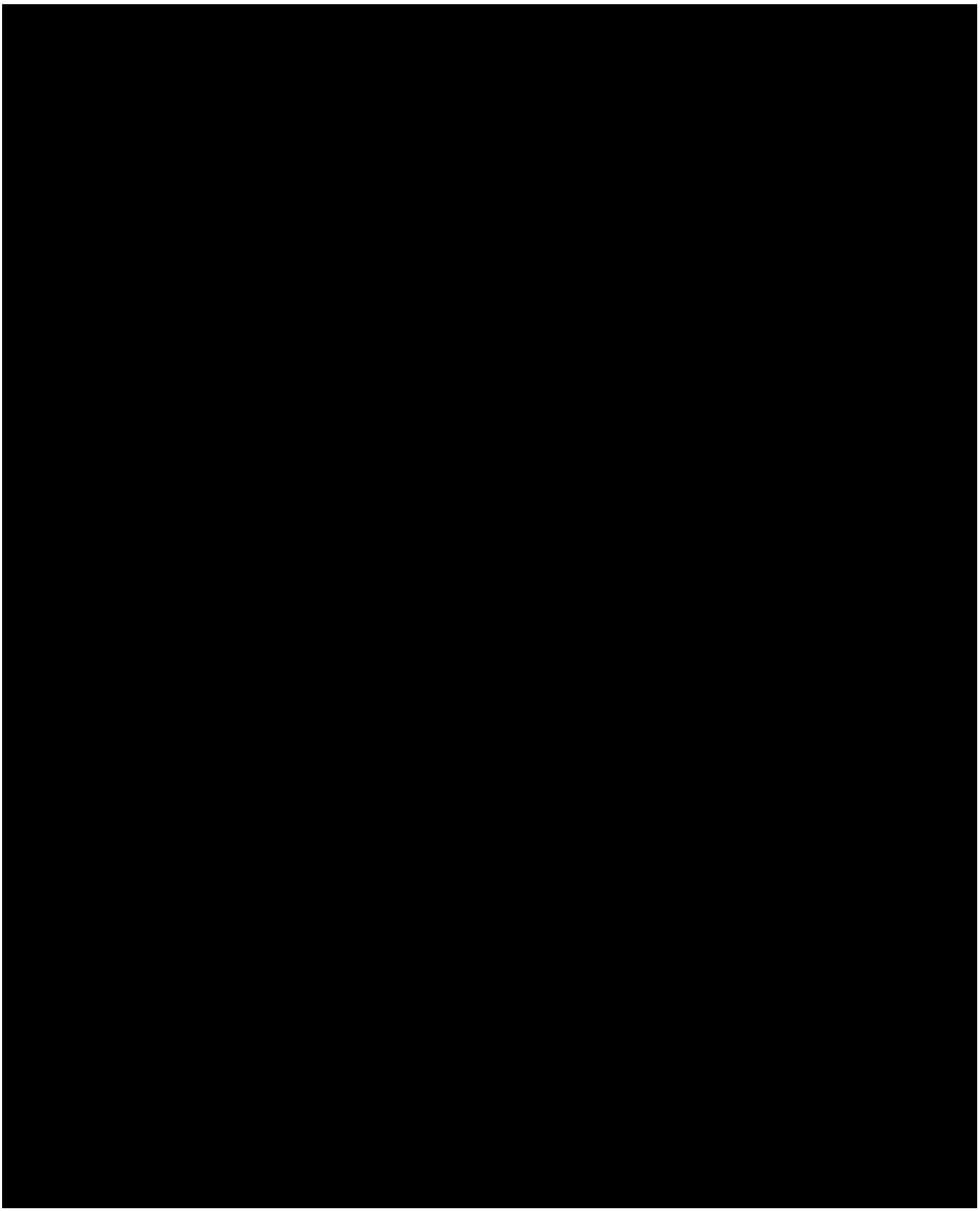
- Mainframe technology support – build and maintain for hardware, software, connectivity
- Vendor management – technical support, maintenance coverage, and remote access capability
- Platform specific procedures – customer notification, technical support escalations patching process/schedule, security monitoring, and log reviews
  - Tools/Applications

Unisys has outlined the complete approach to monitoring operations and supporting automated remediation over time from a common enterprise infrastructure platform across all technical towers for the Commonwealth in F3.2.3.2 Site Operations.

Unisys will implement, support, and operate a comprehensive and integrated Information Technology Service Management (ITSM) Architecture dedicated to the cross functional process support for all services provided to the Commonwealth for this contract. The proposed ITSM Architecture, shown in **Figure 3.2.4.5-1**, will provide an effective and efficient operational platform to support the Commonwealth's agencies application infrastructure for the following ITILV3 (Information Technology Infrastructure Library) Service Management Processes.

Figure 3.2.4.5-1 - Proposed Unisys ITSM Integrated Architecture

A full description of the tools used for the ITSM Management Platform is contained in the Schedule F, Section 3.2.3.2 "Site Operations". The specific tools as they pertain to the Unisys mainframe are summarized in the **Figure 3.2.4.5-2**.



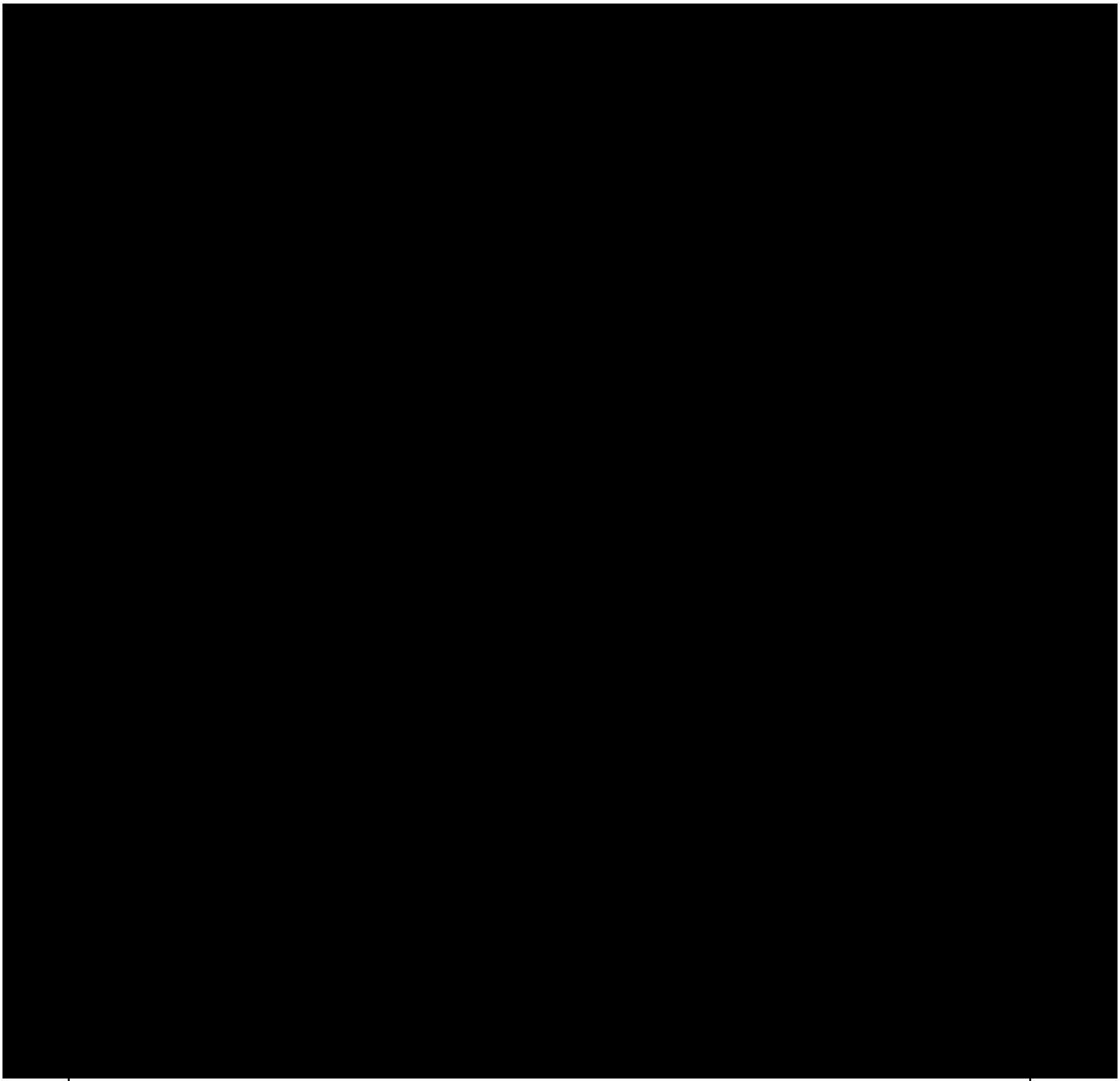


Figure 3.2.4.5-2 - Unisys Mainframe ITSM Tools

Unisys will assess the Commonwealth's current ITSM toolsets during transition. Assessment results determine which tools will be supported within this overall target ITSM proposed architecture, replaced, or eventually migrated to the target environment ITSM tools shown in **Figure 3.2.4.5-2**. The resulting architectural decisions will be reviewed and approved by the Commonwealth's agencies. Some identified tools will continue to offer the functionality they are currently providing, but will be integrated into the overall ITSM proposed architecture.

- End User Reports
  - Standard Reports are summarized in 3.3.2.
  - Custom Reports are offered by Unisys via the Enterprise Services Catalog
- Tiered Service/Support Levels

The Commonwealth of Pennsylvania has indicated in Schedule J.2 - Datacenter Service Level Matrix the desired service tiers/support levels. In the design of the Services and the infrastructure needed to deliver those Service to the Commonwealth, Unisys defined the Service Tiers to align to those requirements. A fuller explanation and representative sample of all the Services provided in this structure can be found in the response to Schedule F, Section 3.2.1.5, sub-requirement 1. The service tiers in the Unisys solution are as follows:

Tiered Support Level	Description This Service Level measures the percentage of time the Applications are Available during the applicable Measurement Window
Platinum	• 99.999% Application Infrastructure Availability SLA • Measurement Window – Monthly • Hours of Measurement – 24x7 • Days of Measurement – 365
Gold	• 99.99% Application Infrastructure Availability SLA • Measurement Window – Monthly • Hours of Measurement – 24x7 • Days of Measurement – 365
Silver	• 99.9% Application Infrastructure Availability SLA • Measurement Window – Monthly • Hours of Measurement – 24x7 • Days of Measurement – 365
Bronze	• 99.4% Application Infrastructure Availability SLA • Measurement Window – Monthly • Hours of Measurement – 24x7 • Days of Measurement – 365
Basic	• 98.5% Application Infrastructure Availability SLA • Measurement Window – Monthly • Hours of Measurement – 24x7 • Days of Measurement – 365

Escalation Procedures

As part of the communication management plan, Unisys will work closely with the Commonwealth of PA to structure effective escalation procedures. These procedures will be developed to provide guidance for escalation activities in a number of categories including

incident management service response, management notification, and service quality.

For incident management service response, escalation procedures will define the schedule, criteria, methods, and participants for the escalation of issues or incidents impacting computing services to the Commonwealth. The primary objective of this escalation is to assign appropriate vendor resources with the necessary skills to the incident process to restore service. The procedure will include steps to contact approved agency stakeholders to provide initial notification and to engage in joint problem determination/resolution activity as appropriate.

Escalation procedures will also include provisions to notify Commonwealth and Vendor management staff of major service impacting events as well as to confirm continuous updates are provided until the incident is resolved. In order to provide an easy method for the Commonwealth to notify the vendor of service quality concerns, the escalation procedures will include the process and contacts to register the service quality issues for review and action.

Provide Mainframe systems and operations (Unisys)

To support the requirements of the Commonwealth under the new contract Unisys will continue to offer Mainframe technology and operational support staff aligned with the Commonwealth tools and processes. Unisys will offer ClearPath Mainframe MIPS to support the application processing requirements. Details of the Unisys Mainframe offering are contained in Schedule F, Section 3.1.3.

The Unisys Mainframe environment includes both operational and support staff. This staff has many years supporting the needs of the Commonwealth and will be utilized under the new contract.

1.B Ability to purchase metered Unisys Million Instructions Per Second (MIPS).

Through the Catalog of Services the Commonwealth can procure MIPS based on an allocation model where the agencies will request the MIPS they require within the Catalog and can utilize the allocated MIPS to the total requested.

1.C Monitor local operations, troubleshoot and resolve operational issues.

Unisys is providing staff in the operation center which will be monitoring the batch processing and console messages. This staff provides monitoring of mainframe operations and provides troubleshooting to resolve operational issues. There are well established and tested escalation processes in place to address system related incidents. Escalation processes are described in Schedule F, Section 3.2.1.4 “Service Desk”. Notification of incidents to the appropriate Level 2 support group is part of the in place process today and will continue in the future.

1.D Actively monitor the daily operations of all mainframe (current) systems.

Unisys is providing staff in the operation center which will be monitoring the daily operations of the mainframe systems. This staff provides monitoring of mainframe operations within the current contract. This will continue under the new contract in support of the Commonwealth

processing requirements. Unisys utilizes tools such as OpCon and BL/Sched for Mainframe scheduling and Enterprise Output Manager for print. The scheduling tools and console messages are actively monitored for response requests and error conditions. The console logs are stored on the Commonwealth SPO Server for review and archive. These logs are maintained for approximately 90 days.

Unisys will drive cost reduction and efficiencies through leveraging our local and remote resources and deploying proven tools and capabilities into the environment. Unisys is committed to improving service while reducing costs. To achieve this, Unisys will utilize automation techniques whenever possible to enhance console operations and to proactively monitor the mainframe and server environments. These automation techniques have been used and proven in delivery of our services to other clients.

Mainframe operations will include monitoring ongoing operations and responding to events, alerts, or incidents. Activities performed include online and batch monitoring, recovery and restart, root cause analysis, incident and change management, and resource availability balancing.

Unisys will work with the Commonwealth to develop a comprehensive Policies and Procedures Job Scheduling Manual for the Unisys mainframe that will include specific instructions on what, when, and how to schedule and recover. Unisys will provide local staff to support the scheduling needs. Job scheduling also includes library management, the process of making sure the correct version of application code is promoted to production.

1.E Assume responsibility for all master and subordinate console functions.

The Unisys staff provides console operations functions within the current contract. This will continue under the new contract.

Dorado – Monitoring of the overall system consoles is done via the Single Point Operations (SPO) workstation consoles. Utilizing the Automated Message System (AMS) tool, many of the repetitive messages or conditions are automatically responded to by the system. For each organization (agency) an Operational Procedures Manual is maintained to address specific operational processes used in their environments. In the event that an undocumented alert is received escalation is made to the appropriate agency contact. These contacts are maintained in the Operations procedures Manuals. Monitoring of the BATCH processing is done through a combination of the SPO console and OpCon.

Libra – Monitoring of the overall systems consoles is done via an Accessory Manager sessions. Utilizing the Automated Message System (AMS) tool, many of the repetitive messages or conditions are automatically responded to by the system. An Operational Procedures Manual is maintained to address specific operational processes used in these environments. In the event that an undocumented alert is received escalation is made to the appropriate agency contact. These contacts are maintained in the Operations procedures Manuals. Monitoring of the BATCH processing is done through Web Console.

1.F Issue operator commands to control all In-Scope platforms throughout the organization.

The Unisys staff issue console operations commands within the current contract. This will

continue under the new contract. The Single Point Operations (SPO) workstation consoles and Accessory Manager sessions are used for the responding to or issuance of commands to the Dorado and Libra systems.

1.G Provide all tools and apps that are currently being provided, for example MAPPER/APPMAP, browser based terminal emulation access, and middleware components (like OpenTI, IBM WBM & WMQ, etc.) that are critical to agency operations and application usage.

Unisys has reviewed all Unisys and third party provided tools in use by the Commonwealth as contained in Exhibits B.4 and B.10 – Third Party Software Assets . Unisys has provided third-party license management for the various mainframe tools identified in the exhibits provided. This will continue under the new contract and the ability to procure the required tools will be provided by the Catalog of Services.

1.H Assume the responsibility for and perform all console operations.

The Unisys staff has console operations responsibility within the current contract. This will continue under the new contract. Refer to response 1.E above for a description of console operation functions.

1.I Monitor the performance of online interactive traffic and take appropriate action to resolve online-system-related incidents and/or problems, including escalating (as appropriate) the incident and/or problem to the proper Level 2 Support group.

The Unisys staff provides monitoring of online interactive traffic and provides troubleshooting to resolve operational issues. There are well established and tested escalation processes in place to address system related incidents. Notification of incidents to the appropriate Level 2 support group is part of the in place process today and will continue in the future. . Escalation processes are described in Schedule F, Section 3.2.1.4 “Service Desk”.

1.J Monitor the transmission of files between the Commonwealth and any other parties as designated by the Commonwealth.

The Mainframe platforms perform a high number of file transmissions between the Commonwealth and any other parties. Tools are provided on the Mainframes to perform the file transfers using Commonwealth standards. The monitoring of file transfers has been established with the agencies and is effective to support the requirements to date. During Data Gathering Unisys will review with the Commonwealth which of the file transfers should be monitored by Unisys staff.

1.K Provide operational support for data transmission (send/receive), consistent with commercial or agency standards.

Using monitoring of the scheduling tools through the tool consoles and operating system console messages, the staff will provide operational support. Should a transfer fail the staff will respond to any messages or escalate to the appropriate support organization.

1.L Manage, maintain, monitor, and control online and batch process, both scheduled and unscheduled (including on-request processing).

Unisys will provide batch monitoring activities using a combination of on-site and remotely located personnel (batch operators) and tools. For the Unisys mainframes OpCon and BL/Sched are used to manage and monitor the batching process. Unisys monitors the batch processing environment and provides alerts to the agencies via established processes of success and failure. Unisys today provides monitoring and alerting functions. Additional services to procure Unisys resources for full batch creation, scheduling and troubleshooting are available via the Catalog of Services.

1.M Maintain a log for each system detailing hardware / software configuration and critical service operations.

Within the services provided today by Unisys the hardware and software configurations are documented and reviewed with the Commonwealth agencies. Sources of data include the Exhibits from the contract as well as data extractions from the mainframe partitions. Hardware/Software configurations are currently maintained in the ODB and in COMUS The ODB operations database (ODB) is a database populated with information from the Site Configuration Management System (SCMS) database. The ODB contains configuration information that the Exec needs to operate component hardware. COMUS is an OS 2200 software tool that provides standard procedures for managing the installation and maintenance of certain OS 2200 software products. As part of the services provided under the new contract Unisys will integrate the mainframe configuration elements into the CMDB to have one master record of configuration data improving accuracy of information. Configuration information is updated on a cyclical basis based on changes in the environment and a multi-year record of configuration information is maintained for review by the Commonwealth. [redacted] in **Figure 3.2.4.5-3** below shows for mainframe discovery, normalization, and reconciliation process before pushing configuration management updates into the production CMDB.

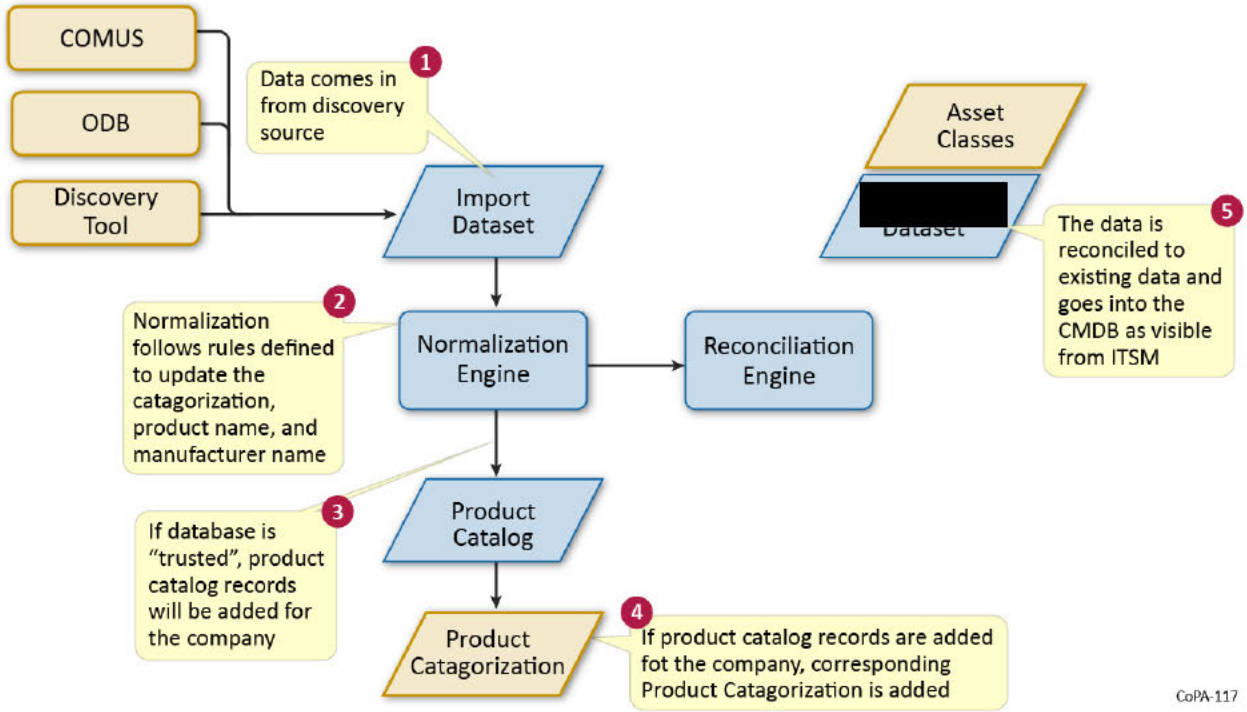


Figure 3.2.4.5-3 - [redacted]

1.N Review the system logs on a weekly basis to ensure critical system Services are processing without errors.

Unisys actively monitors the system logs for processing errors. For any system services operating with errors, an incident ticket will be created to track until the error is corrected. Tickets are driven through the Incident Management system described in Schedule F 3.2.1.4 "Service Desk". Additionally Unisys reviews the system logs on a weekly basis. The Unisys Team will collect each mainframe's system logs and output from the OpCon and BL/Sched scheduling tools and using the report management functions within these tools, validate that critical system services are operating correctly.

Daily Status Reports (Overview of Last 24 Hours) are produced and e-mailed to a specific distribution list for each of the supported state agencies. They are posted to the Services Portal for archive. Incident Ticket Reports are generated automatically from ITSM and posted to the Services Portal.

1.O Maintain and update the operational documentation for all operations procedures and Services.

Unisys will update and maintain operational documentation and processes within the CCPM and these will be reviewed with the Commonwealth on a periodic basis. Changes to the CCPM are subject to the Change Management Process. Please refer to Schedule F 3.2.1.3 "Change and Release Management" for a full description of the Unisys Change and Release Management process.

Unisys utilizes a Change Project to perform functions such as updated to operation manuals, processes and procedures. A variety of templates have been created for this to update

documentation. A sample screen shot of the current template screen is shown below in **Figure 3.2.4.5-4**:

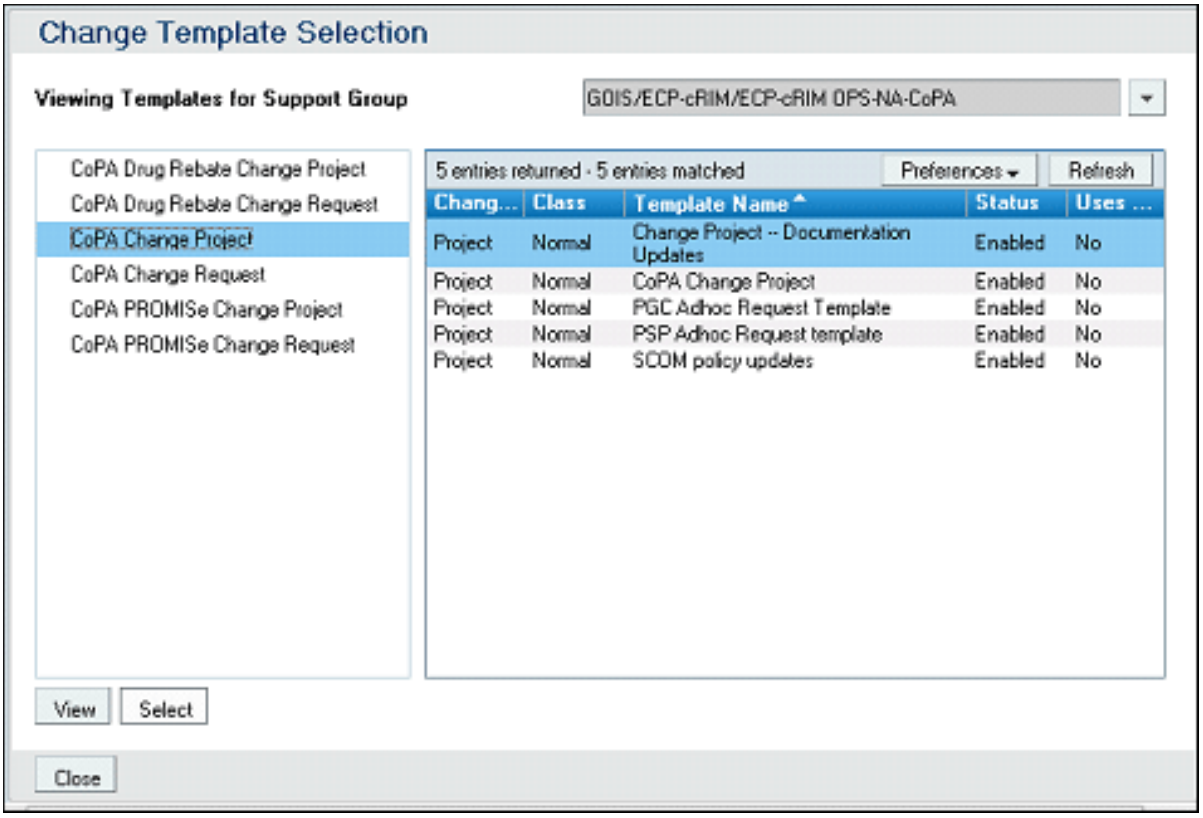


Figure 3.2.4.5-4 – Change Template screen

Once the appropriate selection is made the user is prompted for various input data to complete the documentation change. Once the user input is complete the process of notification and approval takes place until the technical writing and approval process is undertaken and completed.

2 Mainframe Usage Review and Audit

2.A Provide a review and analysis of mainframe usage to determine if current usage is required to support the needs of the mainframe stakeholders.

Offeror must describe solution and approach to meet this requirement.

The RFP requirements state that an initial review of mainframe utilization, processes and reports and to document the findings for the Commonwealth. The Mainframe usage is monitored constantly today using the Sightline tool identified in the Exhibits. Usage data is available for review by the Commonwealth agencies.

Upon contract initiation Unisys will perform a current state audit of mainframe performance. Current processes and reports will be reviewed with the Commonwealth to determine if any additions or changes are required.

2.B Offeror must perform an initial review and audit of the current mainframe usage, procedures and reports and provide an analysis of the current mainframe usage, processes and reports currently being supported.

The initial review and audit of the current usage of the Commonwealth's compute infrastructure will be accomplished as Unisys prepares to migrate the existing workload from each of the existing Commonwealth data centers into the new data centers. During this time, Unisys will deploy tools to collect and analyze all aspects of the Commonwealths current compute usage. Analysis of these workloads will be used to determine the optimal method for migrating these servers. This analysis will also serve as a baseline against which future capacity planning can be compared.

Unisys provides Monthly Performance Reports and Annual Capacity Planning Reports to the Commonwealth. These reports will be utilized to get baseline performance statistics as part of the audit process. In the new contract the mainframe usage reports will be generated using the current tool set and will be available to authorized Commonwealth users via the user portal. Sample Monthly Performance Report in **Figure 3.2.4.5-5** shows an example of a report produced for the Unisys mainframe environment.

System	System Availability		Online Transaction Processing Subsystem								Batch Completion (SLA=0)	DASD (Gigabytes)			CPU Utilization	
System A/B	SLA	Current Month	SLA	Current Month	SLA	Current Month	SLA	Current Month	SLA	Current Month	Current Month	Configured	Actual	%	Peak	Average
			Server A													
Agency A Web	99.90%	100.00%	99.70%	100.00%							0	151.5	55.6	37%	78.1%	12%
			Server B													
Agency A EDI	99.70%	100.00%	99.70%	100.00%							0	204.0	75.9	37%	0.0%	0%
			Server C		Web Server 1		Web Server 2		OLTP							
Agency B System A	99.90%	100.00%	99.90%	100.00%	99.70%	100.00%	99.70%	100.00%	99.90%	100.00%	0	2,465.0	2,651.3	104%	84.4%	58%
			Server D		MAPPER		APPMAP		OLTP							
Agency B System C	99.90%	100.00%	99.90%	100.00%	99.90%	100.00%	99.70%	100.00%	99.90%	100.00%	0	2,465.0	2,651.3	104%	100.0%	99%
			Server E													
Agency B System F	99.90%	100.00%	99.90%	100.00%							0	1,504.2	981.7	65%	99.4%	49%
Agency B Open Systems												49,595.9	40,894.3	82%		CoPA-231

Figure 3.2.4.5-5 - Sample Mainframe Monthly Performance Report

For Unisys Mainframe systems, During the transition phase Unisys will bring in subject matter experts to perform an analysis of the Unisys Mainframe systems and their interaction with other servers in the infrastructure using a tool called Atrium Discovery and Dependency Mapping (ADDM). This group will also conduct application affinity studies for the applications that reside on the Unisys Mainframe systems' as part of their base infrastructure. After ADDM is run and the data gather Unisys will conduct a series of meetings with the Commonwealth to discuss the Unisys Mainframe systems, how they support application, where they maybe concerns and make recommendation for the migration of the Unisys Mainframe systems to the new data centers.

As part of the audit process the Unisys Team will review processes and reports used by the Commonwealth and Unisys Team for applicability in the new environment. The output of this

review process will be utilized to create the audit report.

2.C Offeror must document its review and audit findings and recommendations.

An audit report of findings and recommendations will be provided to the Commonwealth. The key deliverables and reports to be address during this audit include; D-02.57, D-02.58, D-02.59, D-02.79 and D-02.80 found in Schedule K "Key Program Deliverables".

3 Production Control and Scheduling Approach, Toolset including batch jobs

3.A Offeror must describe solution and approach to meet this requirement.

Provide a process of scheduling batch jobs within Commonwealth agency defined windows to achieve maximum performance as long as required batch completion times are met.

Provide for automated scheduling of batch work and processes including backups.

Provide the capability for agencies to schedule and monitor batch processing.

Production Control and Scheduling

Unisys will provide production control and scheduling via the Enterprise Services Catalog. The Service will assess batch job(s) that are currently the Commonwealth's responsibility or are new jobs for production control and scheduling. This Catalog service will assess the requirements of the Commonwealth/Agency requesting this service. The Service will meet the following requirements:

- Provide a process for scheduling batch jobs within Commonwealth agency defined windows to achieve required batch completion times. Provide for automated scheduling of batch work and processes including backups.
- Provide the capability for agencies to schedule and monitor batch processing.
- Resolve abnormally ended jobs caused by conditions external to production programs.
- Repair abnormally ended jobs when possible and perform job restarts in accordance with the Service Management Manual.
- Check job outputs and print queues, and change job priorities.

The first step in providing production control and scheduling services is to work closely with the Commonwealth to get a clear understanding requirements and dependency during Due Diligence. Unisys will then incorporate these requirements into its production control process to develop a true cross platform, cross data center, unified production control and scheduling process. The objective is to achieve batch service level commitments through an efficient use of resources and technologies. For example, data will be gathered to develop statistics for the number of jobs executed per day/week/month, show the number of abends per day/week/month, etc., and provide these details to the Commonwealth via the Unisys Services Portal. This information will be used internally for problem trending and analysis, to verify that batch cycles complete in a timely manner and service level agreements are met.

The production control and scheduling function will use Unisys automated tools to open problem tickets for issues that impact production processing. Unisys will track problem tickets and work with the Commonwealth for problem resolution in order to verify that production

processing executes with as few interruptions as possible.

Unisys will work with the Commonwealth/Agencies to determine if current batch jobs should be converted to [redacted] or if existing tools should continue to be utilized. Unisys intends to standardize per the Commonwealth's requirement to have one enterprise platform for batch job production control and scheduling.

To allow the Commonwealth to schedule and monitor batch and backup jobs Unisys has provided the following tools for the mainframe systems as Enterprise Services Catalog items:

- Batch Scheduling and Monitoring
  - [redacted])
  - [redacted])
- Backup Scheduling and Monitoring
  - [redacted])
  - [redacted]

Authorized Commonwealth staff will have access to these tools to schedule and monitor the batch and backup jobs.

3.B Develop, maintain, and utilize an emergency contact list and escalation procedures to resolve abnormally ended jobs.

Unisys will notify Commonwealth agency customers (an emergency contact list) in accordance with the notification procedures in the event that applications and batch processing do not execute properly. Emergency contact lists and escalation processes are contained in the ITSM system. For full description of the Unisys ITSM system please refer to Schedule F 3.2.3.2 "Site Operations".

3.C Resolve abnormally ended jobs caused by conditions external to production programs.

Unisys will work with the Commonwealth agency customers to resolve abnormally terminated jobs in accordance with the established procedures in the event that applications and batch processing do not execute properly.

The Restart/Recovery Procedures vary by agency under the current contract. For those agencies that have documented Restart/Recovery Procedures which do not require change, these procedures will be followed. For any which require change Unisys will work with the Commonwealth agencies to add/modify the procedures. In the event of an undocumented abnormal termination, the appropriate agency contact will be notified.

Critical services (programs) are monitored daily and through automations will alert in the event of failures/errors. All failures/errors are documented in the specific agency Daily Status Reports as well as via ITSM.

3.D Repair abnormally ended jobs when possible and perform job restarts in accordance with the Service Management Manual.

Unisys will repair abnormally ended jobs and perform job restarts in accordance with the Service Management Manual in the event that applications and batch processing do not execute properly.

Processes to repair abnormally ended jobs are described in Schedule F 3.2.3.2 “Site Operations”.

3.E Check job outputs and print queues, and change job priorities.

For print output the Commonwealth uses Enterprise Output Manager (EOM) for mainframe print jobs. This tool will be utilized to check job outputs and print queues and change job priorities. Unisys or authorized Commonwealth staff can access the EOM console and check print status or change priorities.

3.F Notify Commonwealth agency customers in accordance with the notification procedures in the event that applications and batch processing do not execute properly.

For problem resolution and repair the following process will be utilized used:

- Note failures using scheduling tools
- Open Incident ticket to record issues and corrective activity
- Provide automated notification of batch failures
- Resolution of batch failure
- Close of Incident ticket

Incident Ticket Reports are generated automatically from ITSM and posted to the Commonwealth Services Portal.

Full description of the notification procedures are contained in Schedule F 3.2.3.2 “Site Operations”.

4 Monitor Batch operations

4.A Offeror must describe its approach to supporting the needs of the Commonwealth.

Actively monitor batch operations on all mainframe systems on a daily basis.

Unisys will provide Batch Monitoring as a Catalog Service. The Service will monitor batch job(s) that are currently the Commonwealth’s responsibility or are new jobs for monitoring. This Catalog service will assess the monitoring requirements of the Commonwealth/Agency requesting this service. The Service will meet the following requirements:

- Actively monitor batch operations on all mainframe systems on a daily basis.
- Maintain a log for each batch system and review the system logs on a daily basis to verify key batch Services are processing without errors.

- Document review of the system logs on a daily basis to confirm critical batch Services are processing without errors.
- Notify Commonwealth agencies in accordance with the notification procedures in the event that batch processing do not execute properly.

4.B Maintain a log for each batch system and review the system logs on a daily basis to ensure key batch Services are processing without errors

Batch operations are accomplished through OpCon on the OS 2200 platform and BL/Sched on the MCP platform. The Unisys staff monitors these logs and reports to the Commonwealth agencies any exceptions that occur. The tools produce daily logs of batch completion and failure and the Unisys Team reviews these logs on a daily basis and produces reports which are shared with the Commonwealth agencies.

Daily Status Reports (Overview of Last 24 Hours) are produced and e-mailed to a specific distribution list for each of the supported Commonwealth agencies. It is also posted to the Services Portal for archive.

4.C Document review of the system logs on a daily basis to ensure critical batch Services are processing without errors.

Unisys actively monitors the system logs for processing errors. For any system services operating with errors, an incident ticket will be created to track until the error is corrected. Tickets are driven through the Incident Management system described in Schedule F 3.2.1.4 “Service Desk”. Additionally, Daily Status Reports are generated to document batch failures as well as the OpCon Console alerting to Batch failures.

4.D Notify Commonwealth agencies in accordance with the notification procedures in the event that batch processing does not execute properly.

Daily Status Reports are provided to the specific agency for review as well as being posted to the Services Portal for internal review. Review of the System Log constitutes analysis of the Console messages for batch processing. These messages are analyzed live visually by Operations as well as the Autoaction Message System (AMS), for Unisys Dorado Mainframe processing errors. AMS highlights and holds on the console, all batch processing errors, to provide they are further documented and reviewed in detail. This is a well-established process and will continue under the new contract. Full description of the notification procedures are contained in Schedule F 3.2.3.2 “Site Operations”.

4.E Offeror must provide online monitoring of batch processing by the Commonwealth.

Offeror must describe its approach to allowing Commonwealth users to monitor the batch processing online.

Authorized users from the Commonwealth agencies have access to the scheduling tools and have console access to the Unisys Mainframe environments allowing them the ability to monitor and correct any batch execution incidents. Sample Batch Monitoring Screen in **Figure 3.2.4.5-6** shows an example of a monitoring screen from the OpCon tool.

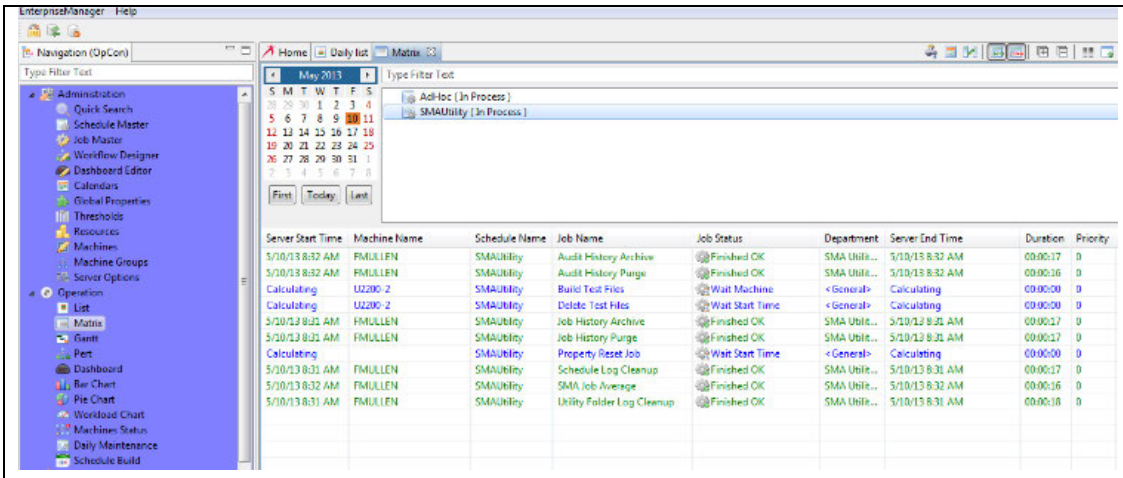


Figure 3.2.4.5-6 - Sample Batch Monitoring Screen

5 System Backup review and Audit

5.A Offeror must describe its approach to performing an initial review and audit of the backup policies, procedures and reports, to ensure the accuracy of the backup schedules, retention periods, target directories, and recovery point objectives.

Offeror must describe its approach to identifying gaps and potential risks, and how those gaps and risks will be resolved.

During the Due Diligence phase after contract initiation Unisys will review the current backup environment against backup windows, retention policies and recovery point objectives and will produce an audit report of their findings. As part of that audit report Unisys will include potential risks and gaps they have identified and will review them with the Commonwealth with potential mitigation strategies and costs. Offerings available from the Enterprise Services Catalog will be reviewed with the Commonwealth and passed through the Architectural Review Board for final approval. Key deliverables and due dates to be addressed with this process include the following; D-02.42, D-02-43 and D-02.44 as contained in Schedule K “Key Program Deliverables”.

5.B Monitor system backup processing on a daily basis.

5.C Process to review daily backup log for successful completion.

Unisys mainframe backup operations system backups are performed through BL/Lib on the Libra mainframes and SMA OpCon on the Dorado platforms. Both Unisys and Authorized Commonwealth staff will have access to these tools. Should errors occur in the backup processing, an incident ticket will be created to track until the error is corrected. Tickets are driven through the Incident Management system described in Schedule F 3.2.1.4 “Service Desk”.

The Backup Administration Console is monitored on a 7x24 basis to report backup initiation, progress and failures and also to report completions. Failures are responded to by automatic restart procedures or operational procedures.

A Daily Status Report is generated and e-mailed to a specific distribution list for each of the supported state agencies. It is also posted to the Services Portal for archive.

An example of a sample backup report is shown in the **Figure 3.2.4.5-7** below.

OPERATIONS DAILY STATUS REPORT

Commonwealth Agency			
Current Boot/Copy Tape		System ID	
Fall Back Boot Tape	NA	Fixed Disk	DRS:
Last Tape Boot		Current AMS Database	
Last Disk Boot		AMS Date Installed	

Task	Completed

	Completed	Task	Completed

Task	Completed

Commonwealth Agency OPCONS Server batch errors

Commonwealth Agency System 1			
Current Boot/Copy Tape		System ID	
Fall Back Boot Tape	NA	Fixed Disk	DRS:
Last Tape Boot		Current AMS Database	
Last Disk Boot		AMS Date Installed	

Task	Started	Completed

Task	Started	Completed

Task	Started	Completed

Task	Completed

Figure 3.2.4.5-7 - Sample Backup Report

5.D Note any failures, initial and date the log, and correct the problem.

The Commonwealth has benefited from the long standing process used by Unisys to monitor Mainframe backup success rates. Using the OpCon and BL/Lib software tools Unisys monitors the nightly progress of backups and then intervene when the rare problem arises. In most cases simply re-starting a backup results in a successful backup because needed resources are tied up during peak times but become available a short time later. Unisys automates the restart process automatically. If the restarted backup fails then incident tickets are created to alert the Backup support team. Thus critical issues get right to Level 2 and Level 3 support personnel without even involving Level 1 support staff. Escalation processes are described in Schedule F 3.2.1.4 " Service Desk".

This automation of incident ticketing provides the Commonwealth with another advantage. During service delivery reviews the Commonwealth can review response times to failures that might put critical applications at greater risk.

Incident Ticket Reports are generated automatically and logs are created with the date time and

assigned resources are from ITSM system and posted to the Services Portal.

Through the incident severity rating processes Unisys has the ability to adjust severity levels so that incidents that are closer to critical applications can receive prioritized support responses.

5.E Create problem record for any abnormal condition and any repairs that have been made.

For problem resolution and repair the following process will be utilized used:

- Note failures using scheduling tools
- Open Incident ticket to record issues and corrective activity
- Provide automated notification of batch failures
- Resolution of batch failure
- Close of Incident ticket

Tickets are driven through the Problem Management system described in Schedule F 3.2.1.4 "Service Desk."

5.F Automated software process will be utilized to report the completion status of backup processing, with electronic notification of failures sent to Offeror technical support, and identified Commonwealth staff for follow up and corrective action.

Unisys has a proven automated approach to monitoring daily backups. On a daily basis Unisys also produces reports on backup successes. The Daily Status Reports are provided to the specific agency for review as well as being posted to the Services Portal.

6 Technical Support

6.A Offeror must describe its approach to supporting the needs of the Commonwealth.

Provide cost effective, operational, and technical support for the computing platform.

The Unisys mainframe systems are a key component of the overall application environment within the Commonwealth. For over 25 total years and 13 years under the current contract Unisys has been providing high levels of operational and technical support to the Commonwealth with high client satisfaction ratings. The Commonwealth wants to continue to receive this high level of support with the lowest cost.

6.B Provide platform level operational and technical support for computing platforms including Mainframe, Storage, AIX, LINUX, SAP, Oracle and Windows architects.

The Mainframe/Midrange Infrastructure function provides hosting and operational support services for both IBM and Unisys mainframe and midrange systems. The service supports all mainframe operating systems and management of the associated logical partitions on the platform. This combined team has provided the services predating the inception of the Data PowerHouse contract in 1999.

The Unisys Mainframe function will continue to be supported by senior level Unisys engineers with over 25 years supporting the Commonwealth's systems with specialty in the OS220 and MCP operating systems. For operational and technical support of non-mainframe platforms please refer to the following sections.

Storage	Schedule F, Section 3.2.4.2
AIX	Schedule F, Section 3.2.4.4
Linux	Schedule F, Section 3.2.4.4
SAP	Schedule F, Section 3.2.4.3
Oracle	Schedule F, Section 3.2.4.3
Windows	Schedule F, Section F 3.2.4.1

This team understands the business priorities associated with applications that run on that platform for the Department of Public Welfare, the Pennsylvania State Police, and the Pennsylvania Game Commission. For representative resumes please refer to Section 5 “Personnel”.

The proposed solution includes a robust technical support staff with the necessary skills to provide the managed services requested by the Commonwealth of Pennsylvania in this RFP. The staffing levels are determined based on key performance indicators which specify the expected number of devices to be supported by each member of the technical team. The team will be staffed with junior and senior positions to provide coverage for Level 2 and Level 3 technical support requirements. Human resource actions including writing position descriptions, development plans, and funding for certifications are all targeted to confirm that the technical support resources are prepared to support the managed services.

In addition to providing the required resources, Unisys will be focused on proper work allocation and skills development. The ITSM7 system will be the primary tool used to allocate work across the various service towers providing communications and control capabilities for delivering the services. Skills development will be provided with formalized training programs and peer mentoring assignments to allow for on the job training opportunities.

6.C Provide Level 2 and Level 3 Support to the Service Desk and/or Commonwealth Users.

As part of the proposed solution, Unisys will provide Level 2 and Level 3 support to the Commonwealth of Pennsylvania. The proposed solution includes a robust technical support staff with the necessary skills to provide the managed services requested by the Commonwealth of Pennsylvania in this RFP. The staffing levels are determined based on key performance indicators which specify the expected number of devices to be supported by each member of the technical team. The team will be staffed with junior and senior positions to provide coverage for Level 2 and Level 3 technical support requirements. Human resource actions including writing position descriptions, development plans, and funding for certifications are all targeted to confirm that the technical support resources are prepared to support the managed services.

Incident tickets are created automatically and create a record of abnormal conditions. Following ITIL-based processes Level2 and Level3 will review incidents for root causes that create multiple tickets. This identification of problems allows the team to establish workarounds and request architecture reviews as necessary. Tickets are driven through the Incident Management system described in Schedule F 3.2.1.4 "Service Desk".

6.D Provide technical advice and support to the Application Development and Maintenance (ADM) and Database Administration (DBA) staffs, as required.

Unisys is the provider of the Mainframe technology and our staff has direct access to Unisys engineering and support organization to make sure the Commonwealth has the best level of service possible. The staff provides 7x24 operational and technical support through both onsite and remote staff which reduces the overall cost to the Commonwealth without introducing risk. This staff also provides Level 2 and 3 support to the Service desk. Under the new contract Unisys will provide the same level of technical and operational support that is done today. A Services Catalog item has been added to enable the Commonwealth to procure any additional ADM and DBA technical advice and support outside what is being delivered today.

As part of the weekly change meetings Unisys participates and provides advice to the application and database staff as part of the application review process. Based upon new application or database requirements and solution knowledge available through Unisys and our partners, the staff provides and will continue to provide technical support to these staffs.

6.E List the service levels for the various levels of service tiers that can be provided. See Schedule J.1 Datacenter Service Level Management for the definitions of the expected options.

The Commonwealth of Pennsylvania has indicated in Schedule J.2 - Datacenter Service Level Matrix the desired service tiers/support levels. In the design of the Services and the infrastructure needed to deliver those Service to the Commonwealth, Unisys defined the Service Tiers to align to those requirements. A fuller explanation and representative sample of all the Services provided in this structure can be found in the response to Schedule F, Section 3.2.1.5, sub-requirement 1. The service tiers in the Unisys solution are as follows:

Tiered Support Level	Description This Service Level measures the percentage of time the Applications are Available during the applicable Measurement Window
Platinum	• 99.999% Application Infrastructure Availability SLA • Measurement Window – Monthly • Hours of Measurement – 24x7 • Days of Measurement – 365
Gold	• 99.99% Application Infrastructure Availability SLA • Measurement Window – Monthly • Hours of Measurement – 24x7 • Days of Measurement – 365

Silver	99.9% Application Infrastructure Availability SLA Measurement Window – Monthly Hours of Measurement – 24x7 Days of Measurement – 365
Bronze	99.4% Application Infrastructure Availability SLA Measurement Window – Monthly Hours of Measurement – 24x7 Days of Measurement – 365
Basic	98.5% Application Infrastructure Availability SLA Measurement Window – Monthly Hours of Measurement – 24x7 Days of Measurement – 365

7 Monitor Network Connectivity, Toolset

7.A Ensure network connectivity to COPANET, and consistent system response times.

Offeror must describe its real-time monitoring approach and toolset to provide and maintain network availability and performance.

As part of the overall application environment which includes Mainframe, Open Systems and end user devices the mainframes require a high degree of network connectivity and performance. Many of mainframe centric applications have migrated off the traditional “green screen” usage to more server to server or web based access and the reliance on the network and performance requirements have increased.

Included in the Mainframe technical design is the review of the current network utilization and network connectivity to meet performance requirements and the results have been designed into the mainframe configurations. The Mainframe configurations provided in the Enterprise Services Catalog have the network connectivity included to meet the current and projected future network requirements. These designs also include full redundancy to provide for network connections should a card or switches fail.

From a monitoring and notification view Unisys provides a holistic approach in which availability and response times are viewed from a mainframe centric (looking out) and user centric (looking in) perspective. From the mainframe view the operating software provides notification of disconnects should an error occur. From an application performance view Sightline provides performance monitoring across the mainframe and open platforms and provides automated alerts of performance issues. Refer to Schedule F 3.2.1 “Network and Security Architecture” for a full description of the Unisys network solution.

7.B Utilize automated system management tool(s) to ensure real time monitoring and notification of system availability and response times. Stop / Start times of servers will be a source of input for SLA measurements

Offeror must identify tools it uses to support network availability and performance.

Unisys will provide event management solutions to help provide network connectivity and consistent windows systems response times. Unisys will utilize [redacted] applications to record incidents tickets that are generated from mainframe monitoring tools to provide real-time monitoring and notification of mainframe availability and response times including the stop and start times of mainframes to support SLA availability measurements. SLA availability measurements are measured in [redacted] and displayed in the Real-time Dashboard available to Commonwealth/Agency personnel. The following tools are the major toolsets to support network and system event management and monitoring.

Monitoring Software	Managed Configuration Items (CI's)	Monitoring and Management Functionality
[redacted]	LAN Devices including: • Switches • Routers • Load Balancers • Firewalls	Provides deep network device availability and performance monitoring, DNS, IP address management, network configuration management, and network traffic bandwidth throughput monitoring
[redacted]	Microsoft servers, databases, network devices, and storage hardware.	Provides a standard set of availability, performance and critical service monitors developed by Unisys for monitoring across infrastructure items including: • Servers • Network devices (switches, routers, load balancers) • Storage devices • Middleware • Applications (Exchange, Citrix XenApp, etc.)

For a complete understanding of how this subset of Event Management Tools supports enterprise Event Management please refer to 3.2.3.2 Site Operations. Refer to Schedule F 3.2.1 "Network and Security Architecture" for a full description of the Unisys network tools.

8 Patch Management

8.A Implement a Patch Management Program to ensure the timely application of updates on all infrastructure platforms in accordance with Commonwealth IT policy guidelines.

Offeror must describe its approach to supporting the needs of the Commonwealth.

Unlike Windows or other open systems operating environments the mainframes are typically not patched on a monthly basis. On mainframes the operating systems are patched based on new system release levels or to enable new features as requested by the Commonwealth. Unisys staff reviews new features and operating system levels and presents them to the Commonwealth during the change meetings to determine if any patching or upgrades are required. Based upon approval and scheduling with the Commonwealth Unisys applies the changes to the mainframe systems. Commonwealth Information Technology Bulletins (ITBs)

will be followed.

8.B Offeror must describe its approach for testing and validating updates to the OS and 3rd Party software that it supports.

Rather than deploying changes directly to the production environments, the development or Unisys test partitions are used to test and validate all new operating system patches and hardware components. Once fully tested and approved by the Commonwealth the patches are applied to the production partitions.

The Unisys technical support team will work with the Commonwealth agencies to determine patch policies that should be applied to the Mainframe environment.

Unisys will follow the Change Management Process for applying patches to the Mainframe environment. This process will maintain the change record in the [redacted] and also update the CMDB configuration management file upon deployment for the Mainframe environment Configuration Items (CI's). The Change Record will be related to the CI's in the CMDB as an audit trail for changes to server CI's upon the completion of the Release and Deployment Process for changes.

Unisys approach to testing and validating updates to the Mainframe OS and 3rd party software in the Mainframe environment is to follow the Release Process for all changes into all production environments. The Release Process includes:

- Change ticket approvals
- Test planning and accepted test results
- Release and deployment planning including release back-out plans
- Release testing for risky deployments
- Early life cycle support to help provide a successful deployment
- Release back-out for failed releases

Software patching, validation of OS updates and outage communication is specific to the Mainframe systems. A Mainframe partition (in the Dorado environment) or Development system (in the Libra environment) can be removed for planned hardware or software reconfiguration, maintenance, or upgrade. Once upgrades and patches are applied and validated by the Commonwealth and Unisys the systems are brought back on line. Upon approval by the Commonwealth the remaining Production environments will be updated and tested based on the same process which was utilized for the no-production environments.

8.C Ensure operating systems are maintained with the current system patch level, based on the Services provided by the server.

Unisys reviews the mainframe release levels and verifies the operating systems are maintained within the Unisys software support cycle. Unisys proactively reviews future operating system releases and documents any impacts the release may have on agency applications processing environments. This allows adequate preparation time for new operating system releases to be

applied when available.

8.D Analyze monthly service patches and determine which patches need to be applied.

Unisys staff members review the current operating system releases and the applicability of applying new software releases to the mainframe platforms. Based on new features or fixes in the operating system Unisys will present to the Commonwealth agencies any fixes or new releases that should be applied in the next update cycle.

8.E Create a change record, log the update in the system log, and install based on system availability schedule.

The implementation of the changes is part of the change management process in which the change ticket is created prior to the application of the patch. After the patching is complete the change ticket is closed. The mainframe system scan identifies the changes and updates are made to the CMDB.

Change reports are generated automatically from ITSM and posted to the Services Portal.

8.F Notify the Commonwealth of any scheduled or unscheduled service interruptions with consideration to Commonwealth scheduled holidays and standard workweek.

Offeror must describe its approach to communicate unscheduled and scheduled outages, including escalation process.

Unisys approach to communicating unscheduled outages is to send notifications to key stakeholders for the Commonwealth/Agencies/Unisys/Third Parties depending on the outage. This will be through email, voice, portal and Remedy broadcast capabilities. The same communications will be used for scheduled outages with additional communications in forward schedules of change reports.

Escalations for unscheduled outages are handled through the standard processes for managing incidents. Unisys service desk will manage all incidents and provide that proper escalation communications to key Commonwealth/Unisys/Third Parties personnel are managed. The [redacted] will also be configured to escalate incident tickets based on incident priorities and SLAs to verify that incidents tickets are being managed to SLA times for incident response and resolution.

Emergency contact lists and escalation processes are contained in the ITSM system. For full description of the Unisys ITSM system please refer to Schedule F 3.2.3.2 “Site Operations”.

9 User Account Management

9.A Provide certified system administration staff to create and maintain the registration of profiles, associated groups, and the security permissions (including password management) required to service the approved client base of the system and application.

Offeror must describe its approach to supporting the needs of the Commonwealth.

User account management including creation and maintenance of the registration of profiles, associated groups, and the security permissions (including password management) is a function which is done by Commonwealth staff under the current contract. An Enterprise Services Catalog item has been added to enable the Commonwealth to procure account management services. A full description of the Unisys Security Management offering is contained in Schedule F 3.2.2.5 "Security Management".

10 Procurement Management

10.A Provide a program and process to refresh the hardware at asset end-of-life, and when upgrades are needed to meet anticipated growth in utilization

Offeror must describe its approach to supporting the needs of the Commonwealth.

The Commonwealth requires a program and process to refresh the hardware at asset end-of-life, and when upgrades are needed to meet anticipated growth in utilization. The Unisys Team as part of the Service Delivery framework participates in capacity planning and procurement planning. Using this planning process end-of-life dates and new application requirements as well as ongoing capacity management are used to identify when upgrades or replacements are needed. As with the other technology areas the Mainframes will be part of the Technology Refresh Plan and Capacity Management process. On overview of these is shown below as related to Mainframe services

- Technology Refresh Plan
  - As part of the overall architecture support, the Commonwealth's environment will be reviewed on a quarterly basis to identify technology, services or components which require replacement to maintain the Commonwealth's business needs and associated service levels. The review will include the following activities. The overall technology refresh plan will be documented in Key Deliverable D-03. This plan will be used for all Unisys supported environments including the Commonwealth Mainframe systems.
  - Using the data within the Asset Management and Configuration Management databases, identify the technical components within the Mainframe system environment which require replacement within the next 18 month period based upon the a 60 month replacement cycle.
  - Review End of Sales and Service Life notices from the Manufacturers to validate if a component has been discontinued or has available ongoing maintenance options.
  - Review ongoing Capacity and Performance reports to identify any components with a refresh requirement which have additional needs driving a requirement or opportunity to change the component's classification to a different component to maintain the functionality and service levels.
  - Identify replacement technical components based upon the current Services Catalog offerings
  - Validate replacement technical components meet the current requirements for the impacted Commonwealth applications.

- Identify risk and impact for the Commonwealth environment to replace existing technical components or services.
- Create technology refresh recommendations, impact statements, and high level implementation plan.
- Present the technology refresh plan to the Commonwealth using the solution architecture review process.
- Upon approval of the refresh plan, open service requests for each migration group and develop the detailed project plan for the migration plans.

➢ Capacity Management and Forecasting

- The Commonwealth Mainframe systems will be monitored and reported from the Capacity Management system used as part of the Unisys management toolset. As part of the Capacity Management process, the capacity reports will be generated and reviewed with the Commonwealth on a regular basis.
- As part of the annual Capacity and Forecast planning activity, Unisys will work with the Commonwealth to identify what changes in growth are expected and provide recommendations on additional upgrades.
- In addition to the Commonwealth's growth forecasting information, Unisys will use the data within the Capacity Management, Asset Management and Configuration Management databases and identify the technical components within Mainframe system environment which require upgrades or additional infrastructure to support the forecasted growth requirements.
- Identify replacement or upgrade technical components based upon the current Services Catalog offerings and the vendor's available products.
- Validate that the identified upgrades or additional components meet the current and forecasted requirements for the impacted Commonwealth Mainframe system.
- Identify risk and impact for the Commonwealth Mainframe system to upgrade or add additional components.
- Create the capacity upgrade recommendations, impact statements, and high level implementation plan.
- Present the capacity upgrade plan to the Commonwealth using the solution architecture review process.
- Upon approval of the capacity upgrade plan, open service requests for upgrade project and develop the detailed project plan.

11 SLA Reporting

11.A Collect actual system availability, utilization and response time data.

Offeror must describe its approach to supporting the needs of the Commonwealth.

The purpose of establishing a strong SLA reporting framework is to provide transparency into the Commonwealth's vendors in its various technical towers. This framework must consist of industry best tools and processes, and should be developed in cooperation between Unisys, Unisys partners, the Commonwealth, and other Commonwealth vendors. The end result of this cooperative effort should be an SLA reporting framework that delivers the following:

- The establishment and maintenance of open communications with the Commonwealth through the governance structure, which encompasses regular meetings and delivers regular reports, many of which are available for the Commonwealth to access online.
- A process to work collaboratively with the Commonwealth to update the Service Level Document when services or service levels are created or modified based on a mutually agreed to process.
- Monitors and reports adherence to Service Levels.
- Verify that service level commitments are met by regularly reviewing service level commitments, compared with actual service level attainment.
- Take corrective actions based on root cause analysis to reduce the impact of future service level failures.
- Define needed monitoring and service level reports.
- Review service operations through management and technical reviews to analyze service level related measurements and take action.
- Identify when changes are required to the Service Levels

Unisys will establish an SLA process and technical architecture to support all SLA's for this contract. See the overview in Schedule F, Section 3.2.1.2 "Availability/SLM". Level 1 of the SLM process is shown in **Figure 3.2.4.5-8** below:

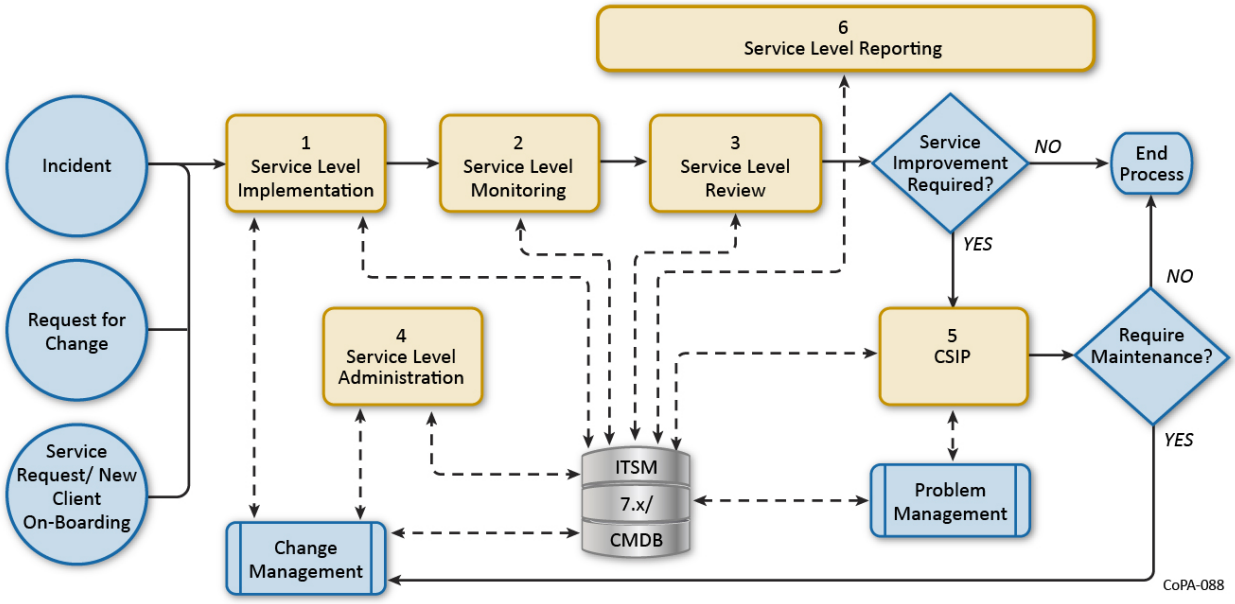


Figure 3.2.4.5-8 - SLM Reporting

Unisys will provide a detailed set of processes and procedures to support Service Level Management during transition of this contract. The process and procedures will support this top level view of the process which includes:

- Service Level Implementation
- Service Level Monitoring
- Service Level Review
- Service Level Administration
- Service Level Improvements (CSIP)
- Service Level Reporting

Unisys will provide the technical architecture and toolsets to support monitoring and maintaining service levels for the mainframe platforms .The [redacted] will be used as the single unified platform to manage Service Level Agreements for Commonwealth agencies. [redacted] provides a continuous real-time platform for defining, measuring, monitoring, reporting, and reviewing the performance of SLA's (per J1 – J3) for mainframe services to make sure that adequate levels of service are delivered in alignment with the Commonwealth's objectives for service delivery. The business contract will contain agreements in which the levels of service are specified. These agreements consist of individual service targets or goals that are used to evaluate whether the agreement is in compliance.

The [redacted] uses all the other [redacted] modules as inputs to determining if an SLA is in compliance. The [redacted] modules used for transaction inputs to determine if service level targets and goals are in compliance include:

- Incident Management
- Problem Management
- Change Management
- Asset/Configuration Management
- Performance/Capacity Management

The [redacted] and in some unique cases other tools as described in F3.2.1.2 will be used to push near real time SLA reporting into the SLA PureShare dashboard reporting tool.

11.B Create a SLA report on a monthly basis, for the Commonwealth and Offeror.

Unisys uses a combination of Sightline and mainframe data are used to report on availability, utilization and response time data. Unisys provides a variety of Monthly SLA reports to OA via the agency specific Monthly Performance Reports and the BES Monthly Report. These reports are generated and posted on a portal as well as e-mailed to key stakeholders.

Key deliverables and due dates to be addressed for SLAs include the following; D-02.04, D-02.05, D-02.06, D-02.07 AND D-02.08 as contained in Schedule K " Key Program Deliverables".

Figure 3.2.4.5-9 below is a snapshot of the Real-time Dashboard which will be available to authorized Commonwealth users.

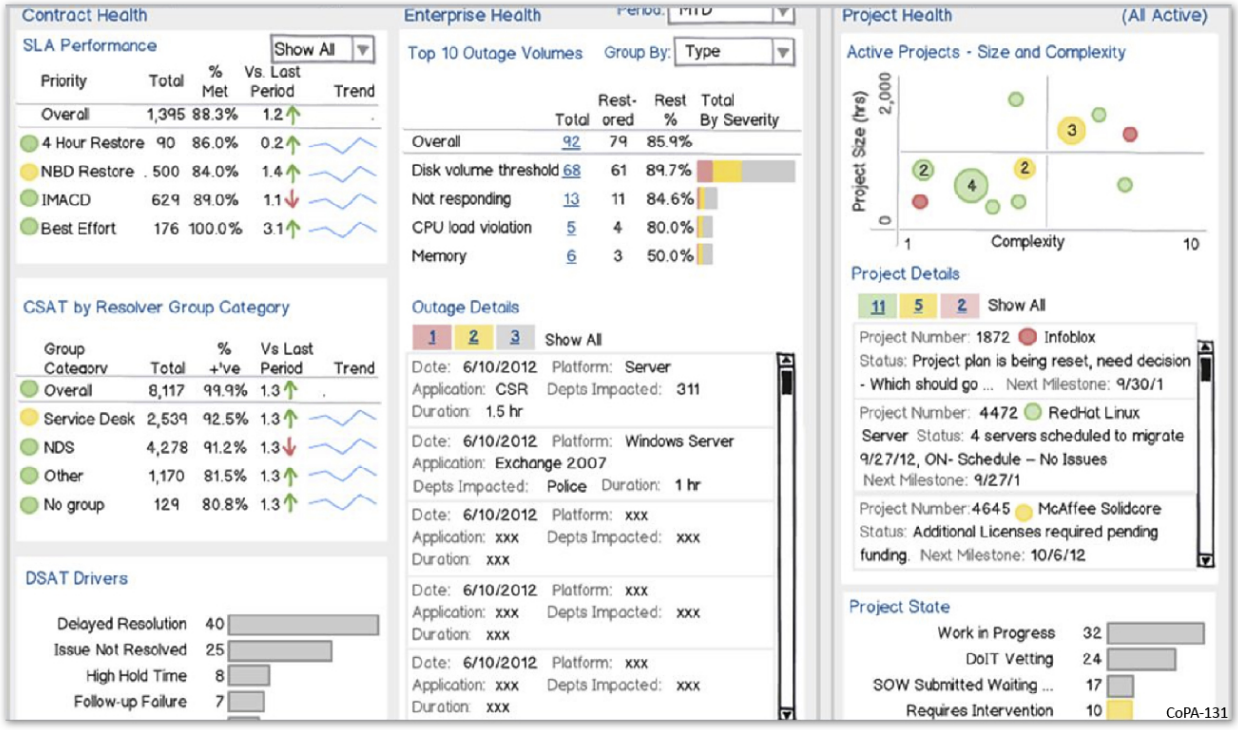


Figure 3.2.4.5-9 - Sample SLA Dashboard

12 Software License Management

12.A The Offeror must provide Software License Management.

Offeror must describe solution and approach to meet this requirement.

Unisys will provide Software License Management for all infrastructure including mainframe platforms. Unisys will provide 3rd Party License Management service for the Commonwealth and Unisys provided infrastructure software products. Unisys will be solely responsible for the management of all infrastructure software license products provided through this contract. The goals of this service are to:

- Confirm software contract compliance (to avoid non-compliance legal issues and expenses)
- Manage costs of software inventory by matching requirements for use to needs
- Verify software maintenance contracts are maintained on schedule through early notifications

Unisys will coordinate with the Commonwealth to verify compatibility between Commonwealth provided applications related software, and Unisys provided infrastructure software.

The following is the approach Unisys will execute during transition and as an ongoing process

to provide 3rd party software license inventory and tracking per agency related infrastructure.

- Load all Unisys and Commonwealth software asset license contract information into the [redacted]
- Load all software license certificate , license type, entitlements, manufacturer, and product information into the [redacted] for the Software License Contract
- Run discovery through [redacted] to identify all software installations Run the [redacted] to build relationships between the discovered software CI's recorded in the [redacted] and the license certificates
- Run the [redacted] to identify non-compliant licenses and inventory for the Unisys and Commonwealth Asset Managers to audit the completeness and accuracy of the information
- Identify any discrepancies in the information and make corrections
- Rerun Compliance Reports and 3Rd party software license inventory reports to get signoff from the Commonwealth and Unisys Asset managers that inventory is properly linked to license certificates in the production environment and the information is complete and accurate
- Provide notifications to Commonwealth/Agencies/Unisys and other Commonwealth service providers when there are software compliance issues or requirements for licenses to be purchased or retired from analysis of license inventory.

Unisys provides third-party software license management as part of the service today and this will continue with the new contract.

13 Mainframe Patching Approach

13.A Coordinate at an agency level and account for any required patching as technology upgrades require.

Offeror must describe its approach to supporting the needs of the Commonwealth.

The Unisys technical support team will work with the Commonwealth agencies to determine patch policies that should be applied to the Unisys Mainframe environment. Patching is part of the Change Management process. Patches are identified and discussed with the agencies. Patches are applied based upon an agreed upon schedule. Please refer to Schedule F, Section 3.2.1.3 Change and Release Management of this document for detail on the formal ITSM7 change management process.

Unisys will follow the Change Management Process for applying patches to the production Unisys Mainframe environment. This process will maintain the change record in the [redacted] platform and also update the CMDB configuration management file upon deployment for the mainframe environment Configuration Items (CI's). The Change Record will be related to the CI's in the CMDB as an audit trail for changes to Mainframe CI's upon the completion of the Release and Deployment Process for changes. Change Reports are generated automatically from ITSM and posted to the Commonwealth DPH SharePoint Portal.

IBM Mainframe

IBM Mainframe Operations Approach

1.A Offeror must describe its approach to supporting the needs of the Commonwealth including the following:

Processes and Procedures

Tools / Applications

End User Reports (Standard and Custom)

Tiered Service/Support Levels

Escalation Procedures

Provide Mainframe systems and operations (Unisys, IBM).

The Unisys Team will provide all mainframe systems and operations support for both the Unisys and IBM mainframe environments. This section will detail the Unisys Team's approach to supporting The Commonwealth's IBM mainframe operating systems.

The Unisys Team will actively monitor the daily operations of all mainframe systems using a combination of on-site and remotely located personnel and tools. The Team proposes to apply our experience, global expertise, and broad scope of proven tools and methodologies to enable the Commonwealth to achieve the required results. In implementing our mainframe services, we will take a collaborative approach in which we leverage the Commonwealth's best processes, transform any that do not work well, and integrate them with The Team's proven approaches. We will evaluate and blend these processes in a manner that will best meet the business needs of the Commonwealth.

Processes and Procedures

The processes and procedures for providing IBM Mainframe infrastructure managed services will be documented in the CCPM which will be reviewed and approved by the Commonwealth. The scope of these processes and procedures will be based on the ITIL framework as well as technology best practices for support of IBM Mainframe platforms.

Processes and procedures will be developed for the following areas:

- Mainframe technology support – build and maintain for hardware, software, connectivity
- Vendor management – technical support, maintenance coverage, and remote access capability
- Platform specific procedures – customer notification, technical support escalations patching process/schedule, security monitoring, and log reviews

Tools / Application

Unisys has outlined the complete approach to monitoring operations and supporting automated remediation over time from a common enterprise infrastructure platform across all technical towers for the Commonwealth in F3.2.3.2 Site Operations.

The Unisys Team will implement, support, and operate a comprehensive and integrated

Information Technology Service Management (ITSM) Architecture dedicated to the cross functional process support for all services provided to the Commonwealth for this contract. The proposed ITSM Architecture, shown in **Figure 3.2.4.5-10**, will provide an effective and efficient operational platform to support the Commonwealth's agencies application infrastructure for the following ITILV3 (Information Technology Infrastructure Library) Service Management Processes.

Figure 3.2.4.5-10 - Proposed Unisys ITSM Integrated Architecture.

The Unisys Team will provide all tools and applications that are currently provided by IBM. The Unisys Team will also provide browser based terminal emulation access and middleware components that are critical to agency operations and application usage.

The Integrated ITSM Management Platform software tools as they pertain to the IBM

mainframe are summarized in the **Figure 3.2.4.5-11**.

Listed below are additional tools utilized in the operational and technical support of the Commonwealth.

	[redacted]	[redacted]

Unisys will assess the Commonwealth's current ITSM toolsets during transition. Assessment results determine which tools will be supported within this overall target ITSM proposed architecture, replaced, or eventually migrated to the target environment ITSM tools. The resulting architectural decisions will be reviewed and approved by the Commonwealth's agencies. Some identified tools will continue to offer the functionality they currently providing, but will be integrated into the overall ITSM proposed architecture.

- End User Reports
  - Standard Reports are summarized in 3.3.2.
  - Custom Reports are offered by Unisys as a Catalog Service
- Tiered Service/Support Levels

The Commonwealth of Pennsylvania has indicated in Schedule J.2 - Datacenter Service Level Matrix the desired service tiers/support levels. In the design of the Services and the infrastructure needed to deliver those Service to the Commonwealth, Unisys defined the Service Tiers to align to those requirements . A fuller explanation and representative sample of all the Services provided in this structure can be found in the response to Schedule F, Section 3.2.1.5, sub-requirement 1. The service tiers in the Unisys solution are as follows:

Tiered Support Level	Description This Service Level measures the percentage of time the Applications are Available during the applicable Measurement Window
Platinum	• 99.999% Application Infrastructure Availability SLA • Measurement Window – Monthly • Hours of Measurement – 24x7 • Days of Measurement – 365
Gold	• 99.99% Application Infrastructure Availability SLA • Measurement Window – Monthly • Hours of Measurement – 24x7 • Days of Measurement – 365
Silver	• 99.9% Application Infrastructure Availability SLA • Measurement Window – Monthly • Hours of Measurement – 24x7 • Days of Measurement – 365
Bronze	• 99.4% Application Infrastructure Availability SLA • Measurement Window – Monthly • Hours of Measurement – 24x7 • Days of Measurement – 365

Basic	98.5% Application Infrastructure Availability SLA Measurement Window – Monthly Hours of Measurement – 24x7 Days of Measurement – 365

Escalation Procedures

As part of the communication management plan, the Unisys Team will work closely with the Commonwealth of PA to structure effective escalation procedures. These procedures will be developed to provide guidance for escalation activities in a number of categories including incident management service response, management notification, and service quality.

For incident management service response, escalation procedures will define the schedule, criteria, methods, and participants for the escalation of issues or incidents impacting computing services to the Commonwealth. The primary objective of this escalation is to assign appropriate vendor resources with the necessary skills to the incident process to restore service. The procedure will include steps to contact approved agency stakeholders to provide initial notification and to engage in joint problem determination/resolution activity as appropriate.

Escalation procedures will also include provisions to notify Commonwealth and Vendor management staff of major service impacting events as well as to provide continuous updates are provided until the incident is resolved. In order to provide an easy method for the Commonwealth to notify the vendor of service quality concerns, the escalation procedures will include the process and contacts to register the service quality issues for review and action.

Provide Mainframe systems and operations (IBM)

To support the requirements of the Commonwealth under the new contract the Unisys Team will continue to offer IBM Mainframe technology and operational support staff aligned with the Commonwealth tools and processes. The Unisys Team will offer IBM mainframe MIPS and CPWS to support the application processing requirements. Details of the IBM Mainframe offering are contained in Schedule F, Section 3.1.3.

The IBM mainframe environment includes both operational and support staff. This staff has many years supporting the needs of the Commonwealth and will be utilized under the new contract.

1.B Ability to purchase metered IBM & Unisys Million Instructions Per Second (MIPS).

Through the Catalog of Services the Commonwealth can procure MIPS or CPWS based on an allocation model where the agencies will request the MIPS or CPWS they require within the Catalog and can utilize the allocated MIPS or CPWS to the total requested.

1.C Monitor local operations, troubleshoot and resolve operational issues.

The Unisys Team, which includes IBM resources familiar with the Commonwealth's

environment and requirements, is providing staff in the operation center that will be monitoring the batch processing and console messages. The staff provides monitoring of mainframe operations and provides troubleshooting to resolve operational issues. There are well established and tested escalation processes in place to address system related incidents. Escalation processes are described in Schedule F, Section 3.2.1.4 "Service Desk". Notification of incidents to the appropriate Level 2 support group is part of the in place process today and will continue in the future.

1.D Actively monitor the daily operations of all mainframe (current) systems.

The Unisys Team staff provides monitoring the daily operations of the IBM mainframe operations within the current contract. The Unisys Team will actively monitor the daily operations of all IBM mainframe systems using a combination of on-site and remotely located personnel and IBM tools. The Unisys Team proposes to apply our experience, global expertise, and broad scope of proven tools and methodologies to enable the Commonwealth to achieve the required results. This will continue under the new contract in support of the Commonwealth processing requirements.

This includes delivery of mainframe services to the Commonwealth as the Unisys Team utilizes a formal, integrated methodology. Each process in our methodology rigorously follows a pattern of planning, testing, coordinating, implementing, monitoring, and reporting on delivery in its specific area.

The Unisys Team will drive cost reduction and efficiencies through leveraging our local and remote resources and deploying proven tools and capabilities into the environment. The Unisys Team is committed to improving service while reducing costs. To achieve this, the Unisys Team will utilize automation techniques whenever possible to enhance console operations and to proactively monitor the mainframe and server environments. These automation techniques have been used and proven in delivery of our services to other clients.

Mainframe operations will include monitoring ongoing operations and responding to events, alerts, or incidents. Activities performed include online and batch monitoring, recovery and restart, root cause analysis, incident and change management, and resource availability balancing.

The Unisys Team will work with the Commonwealth to develop a comprehensive Policies and Procedures Job Scheduling Manual for the IBM mainframe that will include specific instructions on what, when, and how to schedule and recover. The Unisys Team will provide local staff to support the scheduling needs. Job scheduling also includes library management, the process of making sure the correct version of application code is promoted to production.

1.E Assume responsibility for all master and subordinate console functions.

The Unisys Team will assume responsibility for all master and subordinate console functions. The Unisys Team is committed to improving service while reducing costs. To achieve this, the Unisys Team will utilize automation techniques whenever possible to enhance all master and subordinate console operations and to proactively monitor the mainframe and server environments. These automation techniques have been used and proven in delivery of our

services to the Commonwealth and other clients.

1.F Issue operator commands to control all In-Scope platforms throughout the organization.

The Unisys Team staff issue console operations commands within the current contract. This will continue under the new contract. The Mainframe consoles are used for the responding to or issuance of commands to the zLinux and iSeries systems.

1.G Provide all tools and apps that are currently being provided, for example MAPPER/APPMAP, browser based terminal emulation access, and middleware components (like OpenTI, IBM WBM & WMQ, etc.) that are critical to agency operations and application usage.

The Unisys Team has reviewed all IBM and third party provided tools in use by the Commonwealth as contained in Exhibits B.4 and B.10 – Third Party Software Assets. IBM has provided third party license management for the various mainframe tools identified in the exhibits provided. This will continue under the new contract and the ability to procure the required tools will be provided by the Catalog of Services.

Tools and applications currently being provided, that are critical to the agency operations and/or application usage, will continue to be provided by IBM. During the data gathering process, comparable replacement tools or applications may be proposed if in the best interest of the Commonwealth.

1.H Assume the responsibility for and perform all console operations.

The Unisys Team staff has console operations responsibility within the current contract. This will continue under the new contract. Refer to response 1.E above for a description of console operation functions.

1.I Monitor the performance of online interactive traffic and take appropriate action to resolve online-system-related incidents and/or problems, including escalating (as appropriate) the incident and/or problem to the proper Level 2 Support group.

The Unisys Team staff provides monitoring of online interactive traffic and provides troubleshooting to resolve operational issues. There are well established and tested escalation processes in place to address system related incidents. Notification of incidents to the appropriate Level 2 support group is part of the in place process today and will continue in the future. . Escalation processes are described in Schedule F, Section 3.2.1.4 “Service Desk”.

1.J Monitor the transmission of files between the Commonwealth and any other parties as designated by the Commonwealth.

The Mainframe platforms perform a high number of transmission files between the Commonwealth and any other parties. Tools are provided on the Mainframes to perform the file transfers using Commonwealth standards. The monitoring of file transfers has been

established with the agencies and is effective to support the requirements to date. During Data Gathering Unisys will review with the Commonwealth which of the file transfers should be monitored by Unisys Team staff.

1.K Provide operational support for data transmission (send/receive), consistent with commercial or agency standards.

Using monitoring of the scheduling tools through the tool consoles and operating system console messages, the staff will provide operational support. Should a transfer fail the staff will respond to any messages or escalate to the appropriate support organization.

1.L Manage, maintain, monitor, and control online and batch process, both scheduled and unscheduled (including on-request processing).

IBM will provide all batch monitoring activities using a combination of on-site and remotely located personnel (batch operators) and tools. IBM will utilize [redacted] Workload Scheduler to manage and monitor the batching process. The following details the activities associated with mainframe batch monitoring, on-request processing and restart:

- Monitor scheduled batch jobs
- Resolve non-application batch scheduling conflicts for root cause analysis and change management purposes
- Monitor scheduler-related incidents, and develop and recommend changes to the scheduler database
- Perform required batch setup activities, such as ad hoc requests
- Schedule batch jobs that require immediate execution upon request
- Invoke resolution and restart procedures in case of batch job failure
- Recover customer's batch environment
- Log each batch job

The batch operator is responsible for the effective monitoring and recovery of the customer's batch environment. Additionally the batch operator oversees that of all production batch applications are performed, while verifying that problems are promptly detected and proper recovery and escalation procedures are followed. To perform these tasks, the batch operator must possess a solid understanding of batch related tools and processes:

- Provide monitoring of batch execution on a 24 hour x 7 day basis
- Provide failure documentation via the problem management process
- Provide recommendations to the recovery center to enhance and improve the automation platform to eliminate manual tasks, reduce opportunities for error, and improve quality of services

1.M Maintain a log for each system detailing hardware / software configuration and critical service operations.

Within the services provided today by IBM the hardware and software configurations are documented and reviewed with the Commonwealth agencies. Sources of data include the Exhibits from the contract as well as data extractions from the mainframe partitions. As part of the services provided under the new contract the Unisys team will integrate the mainframe configuration elements into the CMDB to have one master record of configuration data improving accuracy of information. Configuration information is updated on a cyclical basis based on changes in the environment and a multi-year record of configuration information is maintained for review by the Commonwealth.

1.N Review the system logs on a weekly basis to ensure critical system Services are processing without errors.

The Unisys Team actively monitors the system logs for processing errors. For any system services operating with errors, an incident ticket will be created to track until the error is corrected. Tickets are driven through the Incident Management system described in Schedule F 3.2.1.4 "Service Desk". Additionally the Unisys Team reviews the system logs on a weekly basis. The Unisys Team will collect each mainframe's system logs and output from the [redacted] Workload Scheduler tools and using the report management functions within these tools, validate that critical system services are operating correctly.

Daily Status Reports (Overview of Last 24 Hours) are produced and e-mailed to a specific distribution list for each of the supported state agencies. They are posted to the Services Portal for archive. Incident Ticket Reports are generated automatically from ITSM and posted to the Services Portal.

1.O Maintain and update the operational documentation for all operations procedures and Services.

The Unisys Team will update and maintain operational documentation and processes within CCPM and these will be reviewed with the Commonwealth on a periodic basis. Changes to the CCPM are subject to Change Management Process. Please refer to Schedule F 3.2.1.3 "Change and Release Management" for a full description of the Unisys Change and Release Management process.

The Unisys Team utilizes a Change Project to perform functions such as updated to operation manuals, processes and procedures. A variety of templates have been created for this to update documentation. A sample screen shot of the current template screen is shown below in **Figure 3.2.4.5-12**:

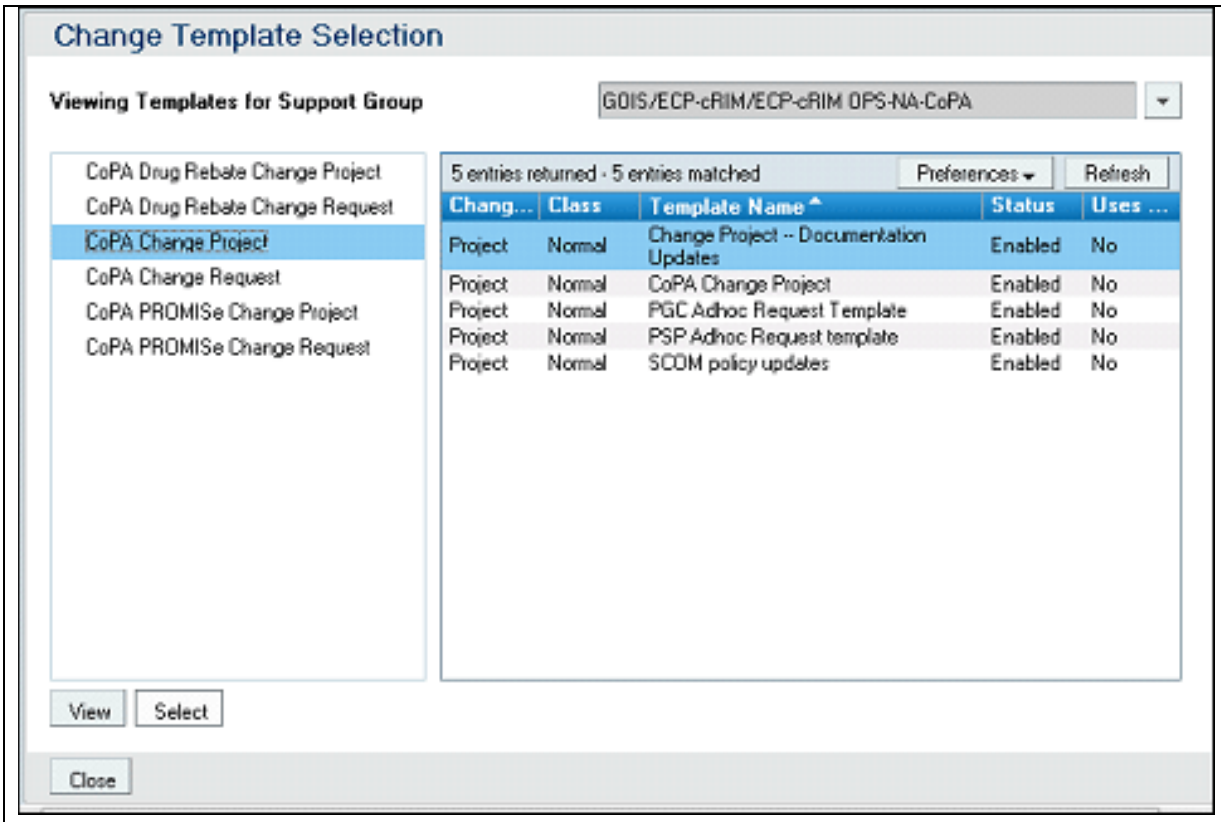


Figure 3.2.4.5-12 – Change Template screen

Once the appropriate selection is made the user is prompted for various input data to complete the documentation change. Once the user input is complete the process of notification and approval takes place until the technical writing and approval process is undertaken and completed.

2 IBM Mainframe Usage Review and Audit

2.A Provide a review and analysis of mainframe usage to determine if current usage is required to support the needs of the mainframe stakeholders.

The RFP requirements state that an initial review of mainframe utilization, processes and reports and to document the findings for the Commonwealth. The Mainframe usage is monitored constantly today using the SRM tool identified in the Exhibits. Usage data is available for review by the Commonwealth agencies.

Upon contract initiation, the Unisys Team will perform a current state audit of mainframe performance. Current processes and reports will be reviewed with the Commonwealth to determine if any additions or changes are required.

2.B Offeror must perform an initial review and audit of the current mainframe usage, procedures and reports and provide an analysis of the current mainframe usage, processes and reports currently being supported.

Offeror must describe solution and approach to meet this requirement.

The initial review and audit of the current usage of the Commonwealth's mainframe environment will be accomplished as the Unisys Team prepares to migrate the existing workload from each of the existing Commonwealth data centers into the new data centers. During this time, the Unisys Team will deploy tools to collect and analyze all aspects of the Commonwealths current compute usage. Analysis of these workloads will be used to determine the optimal method for migrating these servers. This analysis will also serve as a baseline against which future capacity planning can be compared.

The Unisys Team provide Monthly Performance Reports and Annual Capacity Planning Reports to the Commonwealth. These reports will be utilized to get baseline performance statistics as part of the audit process. In the new contract the mainframe usage reports will be generated using the current tool set and will be available to authorized Commonwealth users via the Services Portal.

For IBM Mainframe systems, during the transition phase the Unisys Team will bring in subject matter experts from IBM to perform an analysis of the IBM Mainframe systems and their interaction with other servers in the infrastructure using a tool called ADDM. This group will also conduct application affinity studies for the applications that reside on the IBM Mainframe systems' as part of their base infrastructure. After ADDM is run and the data gathered, The Unisys Team will conduct a series of meetings with the Commonwealth to discuss the IBM Mainframe systems, how they support applications, where they may be concerns and make recommendation for the migration of the IBM Mainframe systems to the new data centers.

As part of the audit process the Unisys Team will review processes and reports used by the Commonwealth for applicability in the new environment. The output of this review process will be utilized to create the audit report.

2.C Offeror must document its review and audit findings and recommendations.

An audit report of findings and recommendations will be provided to the Commonwealth. The key deliverables and reports to be address during this audit include; D-02.57, D-02.58, D-02.59, D-02.79 and D-02.80 found in Schedule K "Key Program Deliverables".

3 IBM Mainframe Production Control and Scheduling Approach, Toolset including batch jobs

3.A Offeror must describe solution and approach to meet this requirement.

Provide a process of scheduling batch jobs within Commonwealth agency defined windows to achieve maximum performance as long as required batch completion times are met.

Provide for automated scheduling of batch work and processes including backups.

Provide the capability for agencies to schedule and monitor batch processing.

Production Control and Scheduling

The Unisys Team will provide production control and scheduling as a Catalog Service. The Service will assess batch job(s) that are currently the Commonwealth's responsibility or are new jobs for production control and scheduling. This Catalog service will assess the

requirements of the Commonwealth/Agency requesting this service. The Service will meet the following requirements:

- Provide a process for scheduling batch jobs within Commonwealth agency defined windows to achieve required batch completion times. Provide for automated scheduling of batch work and processes including backups.
- Provide the capability for agencies to schedule and monitor batch processing.
- Resolve abnormally ended jobs caused by conditions external to production programs.
- Repair abnormally ended jobs when possible and perform job restarts in accordance with the Service Management Manual.
- Check job outputs and print queues, and change job priorities.

The first step in providing production control and scheduling services is to work closely with the Commonwealth to get a clear understanding requirements and dependency during Due Diligence. The Unisys Team will then incorporate these requirements into its production control process to develop a true cross platform, cross data center, unified production control and scheduling process. The objective is to achieve batch service level commitments through an efficient use of resources and technologies. For example, data will be gathered to develop statistics for the number of jobs executed per day/week/month, show the number of abends per day/week/month, etc., and provide these details to the Commonwealth via the Unisys Services Portal. This information will be used internally for problem trending and analysis, to verify that batch cycles complete in a timely manner and service level agreements are met.

The production control and scheduling function will use Unisys automated tools to open problem tickets for issues that impact production processing. The Unisys Team will track problem tickets and work with the Commonwealth for problem resolution in order to verify that production processing executes with as few interruptions as possible.

The Unisys Team will work with the Commonwealth/Agencies to determine if current batch jobs should be converted to [redacted] or if existing tools should continue to be utilized. The Unisys Team intends to standardize per the Commonwealth's requirement to have one enterprise platform for batch job production control and scheduling.

To allow the Commonwealth to schedule and monitor batch and backup jobs The Unisys Team have provided the following tools for the mainframe systems as Enterprise Services Catalog items:

- Batch Scheduling and Monitoring
  - SMA OpCon (Unisys Dorado)
  - BL/Sched (Unisys Libra)
- Backup Scheduling and Monitoring
  - SMA OpCon (Unisys Dorado)
  - BL/Sched (Unisys Libra)
- [redacted] Workload Scheduler

Authorized Commonwealth staff will have access to these tools to schedule and monitor the batch and backup jobs.

3.B Develop, maintain, and utilize an emergency contact list and escalation procedures to resolve abnormally ended jobs.

The Unisys Team will notify Commonwealth agency customers (an emergency contact list) in accordance with the notification procedures in the event that applications and batch processing do not execute properly. Emergency contact lists and escalation processes are contained in the ITSM system. For full description of the Unisys Team's ITSM system please refer to Schedule F 3.2.3.2 "Site Operations".

3.C Resolve abnormally ended jobs caused by conditions external to production programs.

The Unisys Team will work with the Commonwealth agency customers to resolve abnormally terminated jobs in accordance with the established procedures in the event that applications and batch processing do not execute properly.

The Restart/Recovery Procedures vary by agency under the current contract. For those agencies that have documented Restart/Recovery Procedures which do not require change, these procedures will be followed. For any which require change Unisys will work with the Commonwealth agencies to add/modify the procedures. In the event of an undocumented abnormal termination, the appropriate agency contact will be notified.

Critical services (programs) are monitored daily and through automations will alert in the event of failures/errors. All failures/errors are documented in the specific agency Daily Status Reports as well as via ITSM.

3.D Repair abnormally ended jobs when possible and perform job restarts in accordance with the Service Management Manual.

The Unisys Team will repair abnormally ended jobs and perform job restarts in accordance with the Service Management Manual in the event that applications and batch processing do not execute properly.

Processes to repair abnormally ended jobs are described in Schedule F 3.2.3.2 "Site Operations".

3.E Check job outputs and print queues, and change job priorities.

For print output on the IBM platform the Commonwealth uses Job Entry Subsystem 2 (JES2) for z/OS and Remote Spooling Communications Subsystem (RSCS) for z/VM and z/VSE. In addition, some of the commonwealth agencies utilize the VPS product suite. These tool will be utilized to check job outputs and print queues and change job priorities. Unisys Team or authorized Commonwealth staff can access the print consoles and check print status or

change priorities.

3.F Notify Commonwealth agency customers in accordance with the notification procedures in the event that applications and batch processing do not execute properly.

For problem resolution and repair the following process will be utilized used:

- Note failures using scheduling tools
- Open Incident ticket to record issues and corrective activity
- Provide automated notification of batch failures
- Resolution of batch failure
- Close of Incident ticket

Incident Ticket Reports are generated automatically from ITSM and posted to the Commonwealth Services Portal.

Full description of the notification procedures are contained in Schedule F 3.2.3.2 "Site Operations".

4 IBM Mainframe Monitor Batch Operations

4.A Offeror must describe its approach to supporting the needs of the Commonwealth.

Actively monitor batch operations on all mainframe systems on a daily basis.

The Unisys Team will provide all batch monitoring activities using a combination of on-site and remotely located personnel (batch operators) and tools. The Unisys Team will utilize [redacted] Workload Scheduler to manage and monitor the batching process. The following details the activities associated with mainframe batch monitoring and restart:

- Monitor scheduled batch jobs
- Resolve non-application batch scheduling conflicts for root cause analysis and change management purposes
- Monitor scheduler-related incidents, and develop and recommend changes to the scheduler database
- Perform required batch setup activities, such as ad hoc requests
- Schedule batch jobs that require immediate execution upon request
- Invoke resolution and restart procedures in case of batch job failure
- Recover customer's batch environment
- Log each batch job

The batch operator is responsible for the effective monitoring and recovery of the customer's batch environment. Additionally the batch operator oversees that of all production batch applications are performed, while verifying that problems are promptly detected and proper recovery and escalation procedures are followed. To perform these tasks, the batch operator

must possess a solid understanding of batch related tools and processes:

- Provide monitoring of batch execution on a 24 hour x 7 day basis
- Provide failure documentation via the problem management process
- Provide recommendations to the recovery center to enhance and improve the automation platform to eliminate manual tasks, reduce opportunities for error, and improve quality of services

4.B Maintain a log for each batch system and review the system logs on a daily basis to ensure key batch Services are processing without errors

Batch operations are accomplished through [redacted] Workload Scheduler on the IBM platforms. The Unisys Team staff monitors these logs and reports to the Commonwealth agencies any exceptions that occur. The tools produce daily logs of batch completion and failure and the Unisys Team reviews these logs on a daily basis and produces reports which are shared with the Commonwealth agencies.

Daily Status Reports (Overview of Last 24 Hours) are produced and e-mailed to a specific distribution list for each of the supported Commonwealth agencies. It is also posted to the Services Portal for archive

4.C Document review of the system logs on a daily basis to ensure critical batch Services are processing without errors.

The Unisys Team actively monitors the system logs for processing errors. For any system services operating with errors, an incident ticket will be created to track until the error is corrected. Tickets are driven through the Incident Management system described in Schedule F 3.2.1.4 “Service Desk”. Additionally Daily Status Reports are generated to document batch failures.

4.D Notify Commonwealth agencies in accordance with the notification procedures in the event that batch processing does not execute properly.

Daily Status Reports are provided to the specific agency for review as well as being posted to the Services Portal for internal review. Review of the System Log constitutes analysis of the Console messages for batch processing. These messages are analyzed live visually by Operations as well as detected by [redacted] Workload Scheduler and other console tools. The tools highlight and hold on the console, all batch processing errors, to provide they are further documented and reviewed in detail in accordance with the Service Management Manual. This is a well-established process and will continue under the new contract. Full description of the notification procedures are contained in Schedule F 3.2.3.2 “Site Operations”.

4.E Offeror must provide online monitoring of batch processing by the Commonwealth.

Offeror must describe its approach to allowing Commonwealth users to monitor the batch processing online.

Authorized users from the Commonwealth agencies have access to the scheduling tools and have console access to the IBM Mainframe environments allowing them the ability to monitor and correct any batch execution incidents.

5 IBM Mainframe System Backup review and Audit

5.A Offeror must describe its approach to performing an initial review and audit of the backup policies, procedures and reports, to ensure the accuracy of the backup schedules, retention periods, target directories, and recovery point objectives.

Offeror must describe its approach to identifying gaps and potential risks, and how those gaps and risks will be resolved.

During the Due Diligence phase after contract initiation the Unisys Team will review the current backup environment against backup windows, retention policies and recovery point objectives and will produce an audit report of their findings. As part of that audit report the Unisys Team will include potential risks and gaps they have identified and will review them with the Commonwealth with potential mitigation strategies and costs. Offerings available from the Enterprise Services Catalog will be reviewed with the Commonwealth and passed through the Architectural Review Board for final approval. Key deliverables and due dates to be addressed with this process include the following; D-02.42, D-02-43 and D-02.44 as contained in Schedule K "Key Program Deliverables".

5.B Monitor system backup processing on a daily basis.

The Unisys Team will actively monitor and manage system backup processing on a daily basis using a combination of on-site and remotely located personnel and tools. In addition the Team will perform the activities listed below. This will provide the Commonwealth a current, stable, compliant, and recoverable system. In the unlikely event of a serious error, the mainframe platforms and all its components will be at sufficiently current levels so support personal can effectively execute a diagnostic and recovery plan. In addition to stability, the Commonwealth can benefit from the latest provisions being made available through software products.

The Unisys Team will:

- Monitor system backup processing on a daily basis
- Define, support, and test diagnostic and recovery tools.
- Maintain a mounted, online backup to the operating system and its critical components and subsystems for rapid recovery in the event of a catastrophic error impacting the mainframe's ability to continue operating and/or fail to Initial Program Load (IPL) off the current operating system.
- Install, test, and support Standalone Recovery (SAR) tools in the event of a catastrophic error that affects both the current and backup operating systems.
- Develop the Backup Plan using a standard planning convention, including policies, procedures and reports
- Update the Backup Plan as necessary to support production changes

- Review the Backup Plan on an annual basis or as warranted by business or technical changes
- Activities associated with day-to-day recovery from non-disaster type failures or service outages that may occasionally occur, and often can be mitigated through fail-over to another server or logical partition (LPAR), are covered by Backup/Recovery, Problem Management, or Availability Management services.

5.C Process to review daily backup log for successful completion.

The Unisys Team will actively monitor and manage system backup processing on a daily basis using a combination of on-site and remotely located personnel and tools. This will provide the Commonwealth a current, stable, compliant, and recoverable system and serve as the process to review daily backup for successful completion.

Unisys Team will:

- Develop the Backup Plan using a standard planning convention, including policies, procedures and reports
- Update the Backup Plan as necessary to support production changes
- Review the Backup Plan on a daily basis to confirm successful completion
- Activities associated with day-to-day recovery from non-disaster type failures or service outages that may occasionally occur, and often can be mitigated through fail-over to another server or logical partition (LPAR), are covered by Backup/Recovery, Problem Management, or Availability Management services.

The Unisys Team will collect each mainframe's system logs and output from the [redacted] Workload Scheduler tools and using the report management functions within these tools, validate successful completion.

5.D Note any failures, initial and date the log, and correct the problem.

The Unisys Team actively monitors the system logs for processing errors. For any system services operating with errors, an incident ticket will be created to track until the error is corrected. Tickets are driven through the Incident Management system described in Schedule F 3.2.1.4 "Service Desk". Additionally the Unisys Team reviews the system logs on a weekly basis. The Unisys Team will collect each mainframe's system logs and output from the [redacted] Workload Scheduler tools and using the report management functions within these tools, validate that critical system services are operating correctly. The Unisys Team will note any failures, initial and date the log, and correct the problem.

The Commonwealth has benefited from the long standing process used by the Unisys Team to monitor Mainframe backup success rates. Using the [redacted] Workload Scheduler tools the Unisys Team monitors the nightly progress of backups and then intervene when the rare problem arises. In most cases simply re-starting a backup results in a successful backup because needed resources are tied up during peak times but become available a short time later. The Unisys Team automates the restart process automatically. If the restarted backup fails then incident tickets are created to alert the Backup support team. Thus critical issues get right to Level 2 and Level 3 support personnel without even involving Level 1 support

staff. Escalation processes are described in Schedule F 3.2.1.4 " Service Desk".

This automation of incident ticketing provides the Commonwealth with another advantage. During service delivery reviews the Commonwealth can review response times to failures that might put critical applications at greater risk.

Incident Ticket Report are generated automatically and logs are created with the date time and assigned resources are from ITSM system and posted to the Services Portal.

Through the incident severity rating processes Unisys has the ability to adjust severity levels so that incidents that are closer to critical applications can receive prioritized support responses.

5.E Create problem record for any abnormal condition and any repairs that have been made.

For problem resolution and repair the following process will be utilized used:

- Note failures using scheduling tools
- Open Incident ticket to record issues and corrective activity
- Provide automated notification of batch failures
- Resolution of batch failure
- Close of Incident ticket

Tickets are driven through the Problem Management system described in Schedule F 3.2.1.4 "Service Desk"

5.F Automated software process will be utilized to report the completion status of backup processing, with electronic notification of failures sent to Offeror technical support, and identified Commonwealth staff for follow up and corrective action.

The Unisys Team has a proven automated approach to monitoring daily backups. On a daily basis, the Unisys Team produces reports on backup successes. The Daily Status Reports are provided to the specific agency for review as well as being posted to the Services Portal.

6 IBM Mainframe Service Desk, Tiered Support

6.A Offeror must describe its approach to supporting the needs of the Commonwealth.

Provide cost effective, operational, and technical support for the computing platform.

In order to deliver value and a continuously improving service level, the Unisys Team recognizes a standard set of processes and tools are required to offer the scalability and rapid deployment that the Commonwealth business conditions mandate. The Unisys Team will use [redacted] as the strategic model for its operational processes and as the strategic framework for its delivery processes. [redacted] is directly aligned to Process Reference Model for IT (PRM-IT) and provides a sound base to take advantage of leading-edge workflow automation opportunities.

Because the processes are global standards which all of our employees and practitioners follow, new service additions or deletions can be rapidly absorbed or extracted in a repeatable fashion, with less set-up time and fewer errors, no matter where they are delivered from. Our close mapping to ITIL, generally accepted as a best practice, is a validation that we have standardized on a robust set of processes. The process templates are tool and organization independent and allow the Unisys Team to deliver services consistently and competently from anywhere in the world.

Element		Function
People		Access to skills: As the Commonwealth changes over time it can expect to have to integrate new IT operations (or technologies) with a diversity of platforms and tools. IBM's platform level operational and technical support resources are skilled in virtually all manufacturers' products and can readily access the right skills to make the integration successful. Knowledge Transfer: During transition IBM will bring across the Commonwealth skills in support of the Commonwealth account. During the transition period they transfer their account knowledge to IBM peers. Of course, IBM's current extensive knowledge of the Commonwealth's environment will be extensively leveraged.
Process	**Service Management Standards**	**Standardization:** Because the processes are global standards which all of our employees and practitioners follow, new service additions or deletions can be rapidly absorbed or extracted in a repeatable fashion, with less set-up time and fewer errors, no matter where they are delivered from. Our close mapping to ITIL, generally accepted as a best practice, is a validation that we have standardized on a robust set of processes. The process templates are tool and organization independent and allow IBM to deliver services consistently and competently from anywhere in the world. **Repeatability:** These standard processes are extremely well documented. Our employees are both trained in these processes as well as subject to ongoing audit with respect to their proper use of them. This permits our teams to execute rapidly when changes are made to the environment at the Commonwealth's request. Planning time can be reduced and IBM can move more rapidly to execution. **Repeatable, Scalable:** IBM has completed more than 220 complex transitions in the past three years alone. Our well documented, highly repeatable transition process will prove valuable to the Commonwealth in mitigating risk during the initial transition and speeding potential future acquisition

		integration. Some of the characteristics that make our transition repeatable, scalable and a vital asset when integrating acquisitions in the future are: ▪ Global transition and transformation architecture model (GTTA) – continuously improved by IBM to increase speed and seamlessness of transitions ▪ Specialized service teams with experienced technical, transition and transformation skills – experience that will be leveraged during acquisition integration ▪ Process, tools, and intellectual capital to remove risk, ease implementation, and to support continuous improvement – assets such as transition project control books and repositories of lessons learned and best practices ▪ Certified IBM Project Managers with breadth and depth of experience in transitions and transformations.
Technology	**Knowledge access**	IBM captures learning from its delivery operations around the world, meaning that we can use our knowledge base to find similar issues encountered elsewhere and apply appropriate solutions. We can also leverage our broad product and service portfolio to obtain solutions or shortcuts from our hardware, software and services groups to accelerate the deployment of new hardware and remedies to problems as they arise.
	Automation	IBM's ITIL conformant processes and process flows are implemented across an integrated set of highly automated tools that help verify that the Commonwealth receives consistent, predictable and proactive service.

6.B Provide platform level operational and technical support for computing platforms including Mainframe, Storage, AIX, LINUX, SAP, Oracle and Windows architects.

The Mainframe/Midrange Infrastructure function provides hosting and operational support services for both IBM and Unisys mainframe and midrange systems. The service supports all mainframe operating systems and management of the associated logical partitions on the platform. Theses combined teams have provided the services predating the inception of the Data PowerHouse contract in 1999.

The Unisys Team Mainframe function will continue to be supported by senior level engineers with over 25 years supporting the Commonwealth's systems. For operational and technical support of non-mainframe platforms please refer to the following sections.

Storage	Schedule F, Section 3.2.4.2
AIX	Schedule F, Section 3.2.4.4

Linux	Schedule F, Section 3.2.4.4
SAP	Schedule F, Section 3.2.4.3
Oracle	Schedule F, Section 3.2.4.3
Windows	Schedule F, Section 3.2.4.1

Our teams understand the business priorities associated with applications that run on that platform for the Departments of Public Welfare, Transportation, Labor and Industry Unemployment Compensation, Revenue, Corrections, the Pennsylvania State Police, and the Pennsylvania Game Commission. For representative resumes please refer to Section 5 "Personnel".

The proposed solution includes a robust technical support staff with the necessary skills to provide the managed services requested by the Commonwealth of Pennsylvania in this RFP. The staffing levels are determined based on key performance indicators which specify the expected number of devices to be supported by each member of the technical team. The team will be staffed with junior and senior positions to provide coverage for Level 2 and Level 3 technical support requirements. Human resource actions including writing position descriptions, development plans, and funding for certifications are all targeted to verify that the technical support resources are prepared to support the managed services.

In addition to providing the required resources, the Unisys Team will be focused on proper work allocation and skills development. The ITSM7 system will be the primary tool used to allocate work across the various service towers providing communications and control capabilities for delivering the services. Skills development will be provided with formalized training programs and peer mentoring assignments to allow for on the job training opportunities.

6.C Provide Level 2 and Level 3 Support to the Service Desk and/or Commonwealth Users.

As part of the proposed solution, IBM will provide Level 2 and Level 3 support to the Commonwealth of Pennsylvania for hardware and software within the IBM mainframe environment. The proposed solution includes a robust technical support staff with the necessary skills to provide the managed services requested by the Commonwealth of Pennsylvania in this RFP. The staffing levels are determined based on key performance indicators which specify the expected number of devices to be supported by each member of the technical team. The team will be staffed with junior and senior positions to provide coverage for Level 2 and Level 3 technical support requirements. Human resource actions including writing position descriptions, development plans, and funding for certifications are all targeted to confirm that the technical support resources are prepared to support the managed services.

Incident tickets are created automatically and create a record of abnormal conditions. Following ITIL-based processes Level2 and Level3 will review incidents for root causes that create multiple tickets. This identification of problems allows the team to establish workarounds and request architecture reviews as necessary. Tickets are driven through the Incident Management system described in Schedule F 3.2.1.4 "Service Desk"

6.D Provide technical advice and support to the Application Development and Maintenance (ADM) and Database Administration (DBA) staffs, as required.

IBM is the provider of the Mainframe technology and our staff has direct access to IBM engineering and support organization to make sure the Commonwealth has the best level of service possible. The staff provides 7x24 operational and technical support through both onsite and remote staff which reduces the overall cost to the Commonwealth without introducing risk. This staff also provides Level 2 and 3 support to the Service desk. Under the new contract, the Unisys Team will provide the same level of technical and operational support that is done today.

As part of the weekly change meetings the Unisys Team participates and provides advice to the application and database staff as part of the application review process. Based upon new application or database requirements and knowledge of solution available through the Unisys Team the staff provides and will continue to provide technical support to these staffs.

6.E List the service levels for the various levels of service tiers that can be provided. See Schedule J.1 Datacenter Service Level Management for the definitions of the expected options.

The Commonwealth of Pennsylvania has indicated in Schedule J.2 - Datacenter Service Level Matrix the desired service tiers/support levels. In the design of the Services and the infrastructure needed to deliver those Service to the Commonwealth, the Unisys Team defined the Service Tiers to align to those requirements. A fuller explanation, and representative same of all the Services provided in this structure can be found in the response to Schedule F, Section 3.2.1.5, sub-requirement 1. The service tiers in the Unisys solution are as follows:

Tiered Support Level	Description This Service Level measures the percentage of time the Applications are Available during the applicable Measurement Window
Platinum	• 99.999% Server Availability SLA • Measurement Window – Monthly • Hours of Measurement – 24x7 • Days of Measurement – 365
Gold	• 99.99% Server Availability SLA • Measurement Window – Monthly • Hours of Measurement – 24x7 • Days of Measurement – 365
Silver	• 99.9% Server Availability SLA • Measurement Window – Monthly • Hours of Measurement – 24x7

	◻◻ Days of Measurement – 365
Bronze	◻◻ 99.4% Server Availability SLA ◻◻ Measurement Window – Monthly ◻◻ Hours of Measurement – 24x7 ◻◻ Days of Measurement – 365
Basic	◻◻ 98.5% Server Availability SLA ◻◻ Measurement Window – Monthly ◻◻ Hours of Measurement – 24x7 ◻◻ Days of Measurement – 365

7 IBM Mainframe Monitor Network Connectivity, Toolset

7.A Ensure network connectivity to COPANET, and consistent system response times.

Offeror must describe its real-time monitoring approach and toolset to provide and maintain network availability and performance.

As part of the overall application environment which includes Mainframe, Open Systems and end user devices the mainframes require a high degree of network connectivity and performance. Many of mainframe centric applications have migrated off the traditional "green screen" usage to more server to server or web based access and the reliance on the network and performance requirements have increased.

Included in the Mainframe technical design is the review of the current network utilization and network connectivity to meet performance requirements and the results have been designed into the mainframe configurations. The Mainframe configurations provided in the Enterprise Services Catalog have the network connectivity included to meet the current and projected future network requirements. These designs also include full redundancy to provide for network connections should a port, card or switches fail.

From a monitoring and notification view Unisys provides a holistic approach in which availability and response times are viewed from a mainframe centric (looking out) and user centric (looking in) perspective. From the mainframe view the operating software provides notification of disconnects should an error occur. From an application performance view Sightline provides performance monitoring across the mainframe and open platforms and provides automated alerts of performance issues. Refer to Schedule F 3.2.1 "Network and Security Architecture" for a full description of the Unisys network solution.

7.B Utilize automated system management tool(s) to ensure real time monitoring and notification of system availability and response times. Stop / Start times of servers will be a source of input for SLA measurements

Offeror must identify tools it uses to support network availability and performance.

Unisys will provide event management solutions to help verify network connectivity and consistent windows systems response times. Unisys will utilize [redacted] applications to record incidents tickets that are generated from mainframe monitoring tools to provide real- time monitoring and notification of mainframe availability and response times including the stop and start times of mainframes to support SLA availability measurements. SLA availability measurements are measured in [redacted] and displayed in the online operational dashboard as part of the Services Portal available to Commonwealth/Agency personnel. The following tools are the major toolsets to support network and system event management and monitoring.

Monitoring Software	Managed Configuration Items (CI's)	Monitoring and Management Functionality
[redacted]	LAN Devices including: • Switches • Routers • Load Balancers • Firewalls	Provides deep network device availability and performance monitoring, DNS, IP address management, network configuration management, and network traffic bandwidth throughput monitoring
N[redacted]	Microsoft servers, databases, network devices, and storage hardware.	Provides a standard set of availability, performance and critical service monitors developed by Unisys for monitoring across infrastructure items including: • Servers • Network devices (switches, routers, load balancers) • Storage devices • Middleware • Applications (Exchange, Citrix XenApp, etc.)

For a complete understanding of how this subset of Event Management Tools supports enterprise Event Management please refer to 3.2.3.2 Site Operations. Refer to Schedule F 3.2.1 "Network and Security Architecture" for a full description of the Unisys network tools.

8 IBM Mainframe Patch Management

8.A Implement a Patch Management Program to ensure the timely application of updates on all infrastructure platforms in accordance with Commonwealth IT policy guidelines.

Offeror must describe its approach to supporting the needs of the Commonwealth.

The Unisys Team will implement a patch management program that effectively provides the Commonwealth testing and validation of updates to the OS and 3rd Party software that it supports. In addition we will communicate unscheduled and scheduled outages and provide a detailed escalation process for patch management.

The same availability characteristics associated with handling unscheduled outages are

applicable to planned outages as well. A system can be removed for planned hardware or software reconfiguration, maintenance, or upgrade. New work can be dynamically redistributed across the remaining set of active systems. Once the system is ready to be brought back on line, it can be reintroduced in a non-disruptive manner and participate in dynamic workload balancing. The Commonwealth will be notified on a regular basis of any scheduled or unscheduled service interruptions.

Platform system administration covers the following services:

- Install/maintain OS/OS patches/OS utilities.
- Problem determination/resolution for OS/OS patches/OS utilities.
- Review/recommend new OS/OS patches/OS utilities versions/patches.
- Install/upgrade OS/OS patches/OS utilities.
- Security configuration (IBM has exclusive security access control to the physical hardware, O/S and system tools, with the Commonwealth retaining responsibility for application security).
- Setup and perform backup/recovery of OS and OS utility files.
- Report on related SLAs.
- Provide technical support for application developers and the Commonwealth management

Commonwealth Information Technology Bulletins (ITBs) will be followed.

8.B Offeror must describe its approach for testing and validating updates to the OS and 3rd Party software that it supports.

The Unisys Team will first install update to the OS and third-party software updates in a test environment. At the conclusion of sufficient testing by the technical support team the updated environment will be made available to the Commonwealth users to run through their testing procedures in that environment. Upon completion of successful testing the upgraded environment will be cascaded up through the environments and into production upon approval of the Commonwealth.

8.C Ensure operating systems are maintained with the current system patch level, based on the Services provided by the server.

IBM reviews the mainframe release levels and verifies the operating systems are maintained within the IBM software support cycle. The Unisys Team proactively reviews future operating system releases and documents any impacts the release may have on agency applications processing environments. This allows adequate preparation time for new operating system releases to be applied when available.

8.D Analyze monthly service patches and determine which patches need to be applied.

Unisys Team staff members review the current operating system releases and the applicability of applying new software releases to the mainframe platforms. Based on new features or fixes in the operating system the Unisys Team will present to the Commonwealth agencies any fixes or new releases that should be applied in the next update cycle.

8.E Create a change record, log the update in the system log, and install based on system availability schedule.

The implementation of the changes is part of the change management process in which the change ticket is created prior to the application of the patch. After the patching is complete the change ticket is closed. The mainframe system scan identifies the changes and updates are made to the CMDB.

Change reports are generated automatically from ITSM and posted to the Services Portal.

8.F Notify the Commonwealth of any scheduled or unscheduled service interruptions with consideration to Commonwealth scheduled holidays and standard workweek.

Offeror must describe its approach to communicate unscheduled and scheduled outages, including escalation process.

The Unisys Team's approach to communicating unscheduled outages is to send notifications to key stakeholders for the Commonwealth/Agencies/Unisys/Third Parties depending on the outage. This will be through email, voice, portal and Remedy broadcast capabilities. The same communications will be used for scheduled outages with additional communications in forward schedules of change reports.

Escalations for unscheduled outages are handled through the standard processes for managing incidents. Unisys service desk will manage all incidents and verifies that proper escalation communications to key Commonwealth/Unisys/Third Parties personnel are managed. The [redacted] will also be configured to escalate incident tickets based on incident priorities and SLAs to confirm that incidents tickets are being managed to SLA times for incident response and resolution.

Emergency contact lists and escalation processes are contained in the ITSM system. For full description of the Unisys ITSM system please refer to Schedule F 3.2.3.2 "Site Operations".

9 IBM Mainframe User Account Management

9.A Provide certified system administration staff to create and maintain the registration of profiles, associated groups, and the security permissions (including password management) required to service the approved client base of the system and application.

Offeror must describe its approach to supporting the needs of the Commonwealth.

User account management including creation and maintenance of the registration of profiles, associated groups, and the security permissions (including password management) is a function which is done by Commonwealth staff under the current contract. An Enterprise Services Catalog item has been added to enable the Commonwealth to procure user account

management services. A full description of the Unisys Security Management offering is contained in Schedule F 3.2.2.5 "Security Management".

10 IBM Mainframe Procurement Management

10.A Provide a program and process to refresh the hardware at asset end-of-life, and when upgrades are needed to meet anticipated growth in utilization

Offeror must describe its approach to supporting the needs of the Commonwealth.

Refresh coordination begins once refresh planning with the Commonwealth is complete. It is initiated after the proposed schedule has been agreed upon. The refresh coordination process manages the execution of these agreements through refresh coordinators. A refresh coordinator will keep the Commonwealth informed throughout the process, allowing orchestration of all activities required to successfully refresh the in-scope equipment.

When the refresh schedule is agreed to and education materials have been provided, the refresh coordinator will open a management record in our (or the Commonwealth's) problem and change management database. This record will contain the Commonwealth/end user's contact information, location, system configuration, and schedule information and will be updated throughout the refresh process. It is this record that will initiate the perform team by providing the schedule, logistic, and configuration data to complete the end user equipment. As the perform team receives and configures the new equipment, validates the schedule with the end user, and finally completes the refresh, they will continue to update the change management system to provide status. Once the equipment is refreshed, the coordinator will verify that the asset management records are updated, make certain that the end user is able to use the new equipment, and finally close the change management record.

The Unisys Team will use criteria for determining when an asset is at End of Life (EOL), which centers on determining when the hardware vendor will no longer support the device. Typically, hardware support is critical for the Team to be able to meet our service levels and restore the system. Another criterion may be when a particular device has received multiple failures. In either case, the Team considers a device EOL when it is cost prohibitive to fix.

Refresh activities are normally performed in groups (often during off-shift hours) to minimize end-user disruption and reduce costs. The Team will work with the Commonwealth, based on the Commonwealth's changing business needs or the industry's changing market trends, to determine the most-effective refresh strategy. Internally, IBM uses a five-year refresh cycle for mainframes and a four-year refresh cycle for servers. With the Commonwealth's assistance, The Team would identify the equipment that requires refresh and then implement the approved strategy, which would include tracking the age and location of the devices and notifying the Commonwealth when a device is due for refresh.

The Unisys Team will also perform the following activities:

- Notify the Commonwealth when the device is not economical to repair.
- Install the approved devices.
- Provide disposal or redeployment of the replaced device.

The Commonwealth requires a program and process to refresh the hardware at asset end-of-

life, and when upgrades are needed to meet anticipated growth in utilization. The Unisys Team as part of the Service Delivery framework participates in capacity planning and procurement planning. Using this planning process end-of-life dates and new application requirements as well as ongoing capacity management are used to identify when upgrades or replacements are needed. As with the other technology areas the Mainframes will be part of the Technology Refresh Plan and Capacity Management process. An overview of these is shown below as related to Mainframe services

- Technology Refresh Plan
  - As part of the overall architecture support, the Commonwealth's environment will be reviewed on a quarterly basis to identify technology, services or components which require replacement to maintain the Commonwealth's business needs and associated service levels. The review will include the following activities. The overall technology refresh plan will be documented in Key Deliverable D-03. This plan will be used for all Unisys supported environments including the Commonwealth Mainframe systems.
  - Using the data within the Asset Management and Configuration Management databases, identify the technical components within the Mainframe system environment which require replacement within the next 18 month period based upon the a 60 month replacement cycle.
  - Review End of Sales and Service Life notices from the Manufacturers to validate if a component has been discontinued or has available ongoing maintenance options.
  - Review ongoing Capacity and Performance reports to identify any components with a refresh requirement which have additional needs driving a requirement or opportunity to change the component's classification to a different component to maintain the functionality and service levels.
  - Identify replacement technical components based upon the current Enterprise Services Catalog offerings
  - Validate replacement technical components meet the current requirements for the impacted Commonwealth applications.
  - Identify risk and impact for the Commonwealth environment to replace existing technical components or services.
  - Create technology refresh recommendations, impact statements, and high level implementation plan.
  - Present the technology refresh plan to the Commonwealth using the solution architecture review process.
  - Upon approval of the refresh plan, open service requests for each migration group and develop the detailed project plan for the migration plans.

- Capacity Management and Forecasting
  - The Commonwealth Mainframe systems will be monitored and reported from the Capacity Management system used as part of the Unisys management toolset. As part of the Capacity Management process, the capacity reports will be generated and reviewed with the Commonwealth on a regular basis.
  - As part of the annual Capacity and Forecast planning activity, Unisys will work with the Commonwealth to identify what changes in growth are expected and provide recommendations on additional upgrades.
  - In addition to the Commonwealth's growth forecasting information, Unisys will use the data within the Capacity Management, Asset Management and Configuration Management databases and identify the technical components within Mainframe system environment which require upgrades or additional infrastructure to support the forecasted growth requirements.
  - Identify replacement or upgrade technical components based upon the current Enterprise Services Catalog offerings and the vendor's available products.
  - Validate that the identified upgrades or additional components meet the current and forecasted requirements for the impacted Commonwealth Mainframe system.
  - Identify risk and impact for the Commonwealth Mainframe system to upgrade or add additional components.
  - Create the capacity upgrade recommendations, impact statements, and high level implementation plan.
  - Present the capacity upgrade plan to the Commonwealth using the solution architecture review process.
  - Upon approval of the capacity upgrade plan, open service requests for upgrade project and develop the detailed project plan.

11 IBM Mainframe SLA Reporting

11.A Collect actual system availability, utilization and response time data.

Offeror must describe its approach to supporting the needs of the Commonwealth.

The purpose of establishing a strong SLA reporting framework is to provide transparency into the Commonwealth's vendors in its various technical towers. This framework must consist of industry best tools and processes, and should be developed in cooperation between Unisys, Unisys partners, the Commonwealth, and other Commonwealth vendors. The end result of this cooperative effort should be an SLA reporting framework that delivers the following:

- The establishment and maintenance of open communications with the Commonwealth through the governance structure, which encompasses regular meetings and delivers regular reports, many of which are available for the

Commonwealth to access online.

- A process to work collaboratively with the Commonwealth to update the Service Level Document when services or service levels are created or modified based on a mutually agreed to process.
- Monitors and reports adherence to Service Levels.
- Verify that service level commitments are met by regularly reviewing service level commitments, compared with actual service level attainment.
- Take corrective actions based on root cause analysis to reduce the impact of future service level failures.
- Define needed monitoring and service level reports.
- Review service operations through management and technical reviews to analyze service level related measurements and take action.
- Identify when changes are required to the Service Levels

Unisys will establish an SLA process and technical architecture to support all SLA's for this contract. See the overview in Schedule F, Section 3.2.1.2 "Availability/SLM". Level 1 of the SLM process is shown in **Figure 3.2.4.5-13** below:

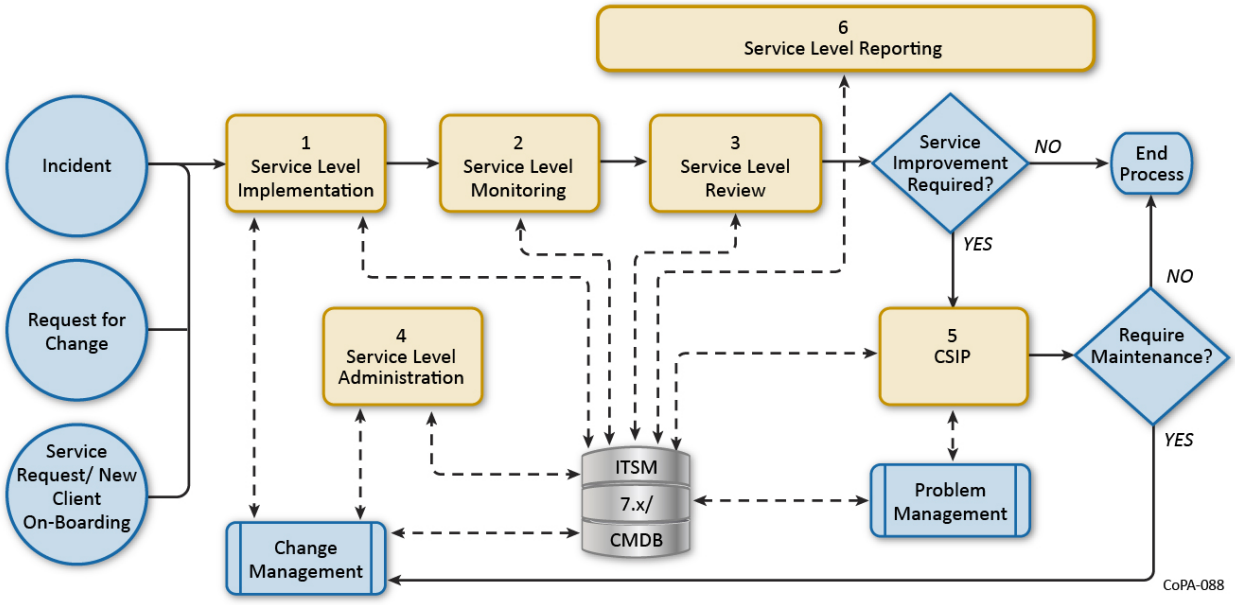


Figure 3.2.4.5-13 - SLM Reporting

Unisys will provide a detailed set of processes and procedures to support Service Level Management during transition of this contract. The process and procedures will support this top level view of the process which includes:

- Service Level Implementation
- Service Level Monitoring

- Service Level Review
- Service Level Administration
- Service Level Improvements (CSIP)
- Service Level Reporting

Unisys will provide the technical architecture and toolsets to support monitoring and maintaining service levels for the mainframe platforms .This includes the automated collection of data like availability and tracking when SLA thresholds are exceeded. The [redacted] ill be used as the single unified platform to manage Service Level Agreements for Commonwealth agencies. [redacted] provides a continuous real-time platform for defining, measuring, monitoring, reporting, and reviewing the performance of SLA's (per J1 – J3) for mainframe services to make sure that adequate levels of service are delivered in alignment with the Commonwealth's objectives for service delivery. The business contract will contain agreements in which the levels of service are specified. These agreements consist of individual service targets or goals that are used to evaluate whether the agreement is in compliance.

The [redacted] ion uses all the other [redacted] modules as inputs to determining if an SLA is in compliance. The [redacted] modules used for transaction inputs to determine if service level targets and goals are in compliance include:

- Incident Management
- Problem Management
- Change Management
- Asset/Configuration Management
- Performance / Capacity Management

The [redacted] and in some unique cases other tools as described in F3.2.1.2 will be used to push near real time SLA reporting into the online operational dashboard reporting tool.

11.B Create a SLA report on a monthly basis, for the Commonwealth and Offeror.

The Unisys Team uses a combination of Sightline and mainframe data are used to report on availability, utilization and response time data. Unisys provides a variety of Monthly SLA reports to OA via the agency specific Monthly Performance Reports and the BES Monthly Report. These reports are generated and posted on a portal as well as e-mailed to key stakeholders. Key deliverables and due dates to be addressed for SLAs include the following; D-02.04, D-02.05, D-02.06, D-02.07 AND D-02.08 as contained in Schedule K "Key Program Deliverables".

12 IBM Mainframe Software License Management

12.A The Offeror must provide Software License Management.

Offeror must describe solution and approach to meet this requirement.

Unisys will provide Software License Management for all infrastructure including mainframe platforms. Unisys will provide 3rd Party License Management service for the Commonwealth and The Unisys Team provided infrastructure software products. Unisys will be solely responsible for the management of all infrastructure software license products provided through this contract. The goals of this service are to:

- Verify software contract compliance (to avoid non-compliance legal issues and expenses)
- Manage costs of software inventory by matching requirements for use to needs
- Confirm software maintenance contracts are maintained on schedule through early notifications

Unisys will coordinate with the Commonwealth to verify compatibility between Commonwealth provided applications related software, and Unisys provided infrastructure software.

The following is the approach Unisys will execute during transition and as an ongoing process to provide 3rd party software license inventory and tracking per agency related infrastructure.

- Load all Unisys, IBM, and Commonwealth software asset license contract information into the [redacted] application
- Load all software license certificate , license type, entitlements, manufacturer, and product information into the [redacted] for the Software License Contract
- Run discovery through [redacted] to identify all software installations Run the BMC License Engine software to build relationships between the discovered software CI's recorded in the BMC Atrium CMDB and the license certificates
- Run the [redacted] and [redacted] to identify non-compliant licenses and inventory for the Unisys and Commonwealth Asset Managers to audit the completeness and accuracy of the information
- Identify any discrepancies in the information and make corrections
- Rerun Compliance Reports and 3Rd party software license inventory reports to get signoff from the Commonwealth and Unisys Asset managers that inventory is properly linked to license certificates in the production environment and the information is complete and accurate
- Provide notifications to Commonwealth/Agencies/Unisys and other Commonwealth service providers when there are software compliance issues or requirements for licenses to be purchased or retired from analysis of license inventory.

Unisys provides third-party software license management as part of the service today and this will continue with the new contract.

Where the Unisys Team can drive higher software cost savings we will provide that license for that tooling. In most cases there is rarely much difference between software tooling, third party license costs, and those of our customers. During due diligence the Unisys Team will research software tools costs and make a determination on which tools should stay licensed to the Commonwealth and which tools license should move over to the Team.

13 IBM Mainframe Upgrade and New Technology Approach

13.A Coordinate at an agency level and account for any required patching as technology upgrades require.

Offeror must describe its approach to supporting the needs of the Commonwealth.

The Unisys technical support teams will work with the Commonwealth agencies to determine patch policies that should be applied to the Unisys and IBM Mainframe environments. Patching is part of the Change Management process. Patches are identified and discussed with the agencies. Patches are applied based upon an agreed upon schedule. Please refer to Schedule F, Section 3.2.1.3 Change and Release Management of this document for detail on the formal ITSM7 change management process.

The Unisys Team will follow the Change Management Process for applying patches to the production Mainframe environment. This process will maintain the change record in the [redacted] and also update the CMDB configuration management file upon deployment for the mainframe environment Configuration Items (CI's). The Change Record will be related to the CI's in the CMDB as an audit trail for changes to Mainframe CI's upon the completion of the Release and Deployment Process for changes. Change Reports are generated automatically from ITSM and posted to the Commonwealth DPH SharePoint Portal.

Continual Service Improvement

Unisys recognizes the significant importance of Quality and Continuous Service Improvement to:

- Reduce service risk,
- Improve service quality,
- Improve client satisfaction,
- Provide service transparency, and
- Improve/reduce costs of service.

Through a continuous cycle of evaluation and improvement within an IT infrastructure, Unisys views quality and continuous service improvement as a critical success factor in driving customer satisfaction for the Commonwealth IT infrastructure. Each of the continuous service improvement areas identified above are driven through the tight integration of the following organizations, industry tools, proven processes and quality deliverables:

- Service Excellence Office,
- Quality Plans: transition and steady state service delivery

- Industry standard frameworks and methodologies: ITIL, ISO, SSL
- Industry accepted measurement tools
- Continuous Service Improvement & Innovation Processes (CSIIP)
- Risk management, audits and business continuity management
- Client Satisfaction Surveys and Knowledge Management Portal

Collectively this represents Unisys Integrated Quality Plan for the Commonwealth of Pennsylvania.

Specifics on each of these areas are outlined in Schedule F, Section 3.2.1.1.6 Continuous Service Improvement. Highlights from this section are outlined below and requested service examples are provided at the end of this section.

14 CI Service Risk

14.A Reduce service risks.

Offeror must describe its approach to supporting the needs of the Commonwealth

Methods to eliminate or mitigate service risks.

Risk management, independent quality audits, and business continuity management are integral quality management processes. Unisys is committed to managing risks and facilitating the achievement of business objectives the adherence to quality processes. We mitigate risk through the implementation of tight quality controls: standard policies, procedures, roles, risk assumptions, issues, and definitions, etc.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

15 CI Service Quality

15.A Improve service quality.

Offeror must describe its approach to supporting the needs of the Commonwealth

The quality approach begins with the Service Excellence Office who provides definition and oversight of all ITIL process management and analysis functions. Process managers and analysts working in the Service Excellence Office are responsible for auditing process effectiveness, ensuring that service delivery teams comply with proper execution of processes, and analyzing process trends for anomalies. Continuous service improvement programs in collaboration with Commonwealth agencies are managed by the Service Excellence Office.

Through our Continuous Service Improvement and Innovation Process (CSIIP), the SEO reviews, analyzes and makes recommendations on improvement opportunities in each ITIL lifecycle phase. Unisys will leverage Six Sigma Lean tools and methodologies as well as ISO Certified internal audits to measure and maintain the highest quality services to the Commonwealth.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional

details in this area.

15.B On a quarterly basis, Offeror must also recommend to the Commonwealth team any system changes that would be appropriate to maintain or improve SLA commitments.

Unisys will continually align and re-align IT services to the changing business needs of the Commonwealth Agencies by identifying and implementing improvements to IT services that support business processes. This will be accomplished through our Continuous Service Improvement and Innovation Process (CSIIP). SEO reviews, analyzes and makes recommendations on improvement opportunities in each ITIL lifecycle phase. Unisys will leverage Six Sigma Lean Tools and Methodologies as well as ISO Certified Internal Audits to measure and maintain the highest quality services to the Commonwealth. Unisys will meet with the Commonwealth Agencies monthly to review all the monthly SLA and utilization reporting. Unisys will meet quarterly with the Commonwealth to review the trending analysis and work together to determine the go forward IT Strategy for the Commonwealth. Unisys will make proactive recommendations for system changes to meet the ever changing business requirements of the Commonwealth.

16 CI Client Satisfaction

16.A Improve client satisfaction.

Offeror must provide examples of previous Offeror initiatives aimed at continually improving client satisfaction.

Client satisfaction is extremely important to Unisys and a key focus in our IT solution. The SEO will integrate new agencies, customers and services into our multi-pronged client satisfaction approach that includes Service Desk surveys on the caller's experience, an overall agency satisfaction survey, and quarterly surveys with the Office of Administration. Data collection will be gathered across multiple levels to gain a clear understanding of the Commonwealth's satisfaction with the IT Services being provided.

Please refer Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

17 CI Service Transparency

17.A Ensure service transparency.

Offeror must describe its approach to supporting the needs of the Commonwealth.

The service organizations will use standardized ITSM services processes, IT monitoring and automation tools. ITSM processes will be documented in the Commonwealth Computing Procedures Manual (CCPM). The CCPM will be available to Commonwealth approved staff on the Knowledge Management Portal (KMP) providing desired transparency into service execution processes. Through the Real-time Dashboard, the Commonwealth will have access to current operational performance of their application infrastructure.

Specific to the Mainframe environment Unisys will leverage the ITIL framework in delivering IT Service Management. Industry accepted Measurement Tools such as Dorado Systems –

OPCON, Libra Systems – BL/Sched and IBM Systems [redacted] Workload Scheduler to monitor and schedule production batch jobs. Sightline will be used on the Unisys Mainframes and SRM–Server Resource Manager on the IBM mainframes to monitor mainframe usage, application performance monitoring and provide information for SLA reporting. SolarWinds will monitor the network infrastructure. Hardware and Software configurations and licenses will be managed proactively through the CMDB. These tools will be the foundation for establishing baselines, performance, capacity, and availability management, and SLA/SLO reporting within the Mainframe environment. These tools and reports will also provide excellent visibility and services transparency to the Commonwealth.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

17.B Offeror must provide methods and practices to ensure service transparency, providing visibility into service execution.

The Unisys Data PowerHouse provides full visibility into mainframe service execution. Commonwealth agencies have full access to monitoring and scheduling tools which run against the mainframe platforms. Various SLA and performance reports are generated and the results posted on a portal. Key reports are e-mailed to Commonwealth stakeholders for their review.

18 CI Reduce Cost of Service

18.A Improve/reduce cost of service.

Offeror must provide examples of Mainframe Support initiatives that have been implemented or can be utilized to achieve reduced costs of Services and to meet or exceeded ROI (Return on Investment) analysis projections.

The Service Excellence Office will proactively manage quality, continuous service improvement, ITIL process management, and customer satisfaction through a comprehensive quality plan that specifically addresses all of these areas. We believe this is a key differentiator in our partnership with the Commonwealth. Through this new organization and these quality plans, Unisys will drive best in class services and the highest customer satisfaction experience, while reducing overall costs to the Commonwealth.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

A few examples of Mainframe Services Management Continuous Service Improvement that have been implemented or can be utilized to achieve reduced costs of Services and to meet or exceeded ROI (Return on Investment) analysis projections are outlined below:

Unisys Mainframe:

The DPH implemented a process to mirror Client data (86 disk packs using EMC time finder) between production mainframes and those at [redacted] Continual improvements remain underway to expand this process increasing the amount of data supported by time finder by and additional thirty percent. This mirroring technique has provided DPW with the ability to maintain 7 x 24-hour processing while replicating data necessary for disaster recovery down to [redacted] This process improvement has enhanced our ability to perform disaster recovery

data restoration faster than previously possible, from physical tape storage.

Unisys Mainframe:

For major mainframe Operating System Software releases, the DPH implemented a process to utilize Virtual Tape for storage of software to be installed. Previous process utilized physical tape and CD media. New process allowed for preload of software to virtual tape (disk) and eliminated delays due to mount time of physical media as well as improved data transfer rates. This process improvement shortened downtime by 75% for the installation of software and allowed Commonwealth agencies to resume processing faster and more efficiently.

IBM System z10 Migration to z196 Processor:

In 2011, the Department of Labor and Industry was planning to migrate off of the IBM mainframe, but due to unforeseen circumstances, an extension of services were required on the Data PowerHouse mainframe platform. The Unisys Team brought forth a solution to replace the z10 processor with a z196 processor. This offered a number of benefits to the Commonwealth including additional processor capacity, a boost in the integrated facility for Linux (IFL). The system also offered improved performance and increased processor speed with optimizations for DB2 and WebSphere. Since this processor offered more capacity leveraging fewer processors, many agencies realized reductions in software license and maintenance fees.

IBM System z Business Class Mainframe processor

Due to a number of situations including the increase in unemployment compensation benefit terms and skyrocketing unemployment rate coupled with delays experienced on mainframe application modernization efforts, processor utilization rates were projecting to exceed the capacity of the z10 mainframe within the year 2011. We located an IBM Business Class processor in our excess inventory. This machine was equipped with the capacity required to support the Department of Corrections. At no additional cost to the Commonwealth, we seamlessly migrated DOC workload from the z10 mainframe system to the business class processor, providing 180 MIPS of capacity relief on the z10.

Unisys Team Experience

The Unisys mainframe systems are a key component of the overall application environment within the Commonwealth. For over 25 total years and 13 years under the current contract Unisys has been providing high levels of operational and technical support to the Commonwealth with high client satisfaction ratings. The Unisys proposal provides the ability for the Commonwealth to procure mainframe services which meet their application processing requirements.

The Commonwealth has benefited from this teams daily working relationship and knowledge of the agencies that use the Unisys Mainframe technology including the Department of Public Welfare, Pennsylvania State Police and the Pennsylvania Game Commission. This team understands the criticality and business functions of the applications which are supported by the mainframes. The team has provided operational support services and upgrades for the Commonwealth for over two decades. This experience provides the Commonwealth with a unique opportunity to move forward into their new data center model with the lowest risk.

Outside of the Commonwealth team Unisys brings worldwide experience in the support and operations of our mainframe technologies. As the manufacturer of the hardware platforms and developer of the operating systems the team is best positioned to provide new and innovative

solutions to the Commonwealth. The team has direct access to engineering and support resources which are an extension of the direct team supporting the Commonwealth.

The Unisys Team understand the criticality of the applications which are supported on our platforms and will provide the Commonwealth with the lowest risk, least disruptive migration of the current platforms to the new environment.

Some examples of where the team has provided new and innovative solutions to our clients include:

Client	Challenge	Result
Prudential Global Data Services	Operating in a global economy, the ability to improve service levels and drive efficiencies is important. To achieve this, Prudential Global Data Services sought to both consolidate its globally distributed data centers into a centralized location and adopt shared-service IT delivery, without affecting the timeliness or reliability of vital financial services.	1-second completion time for 99% of daily transactions 85% reduction in the runtime of daily management tasks 90% reduction in the time required to restore a production workload
University of Washington	As a higher-education institution, the University of Washington must comply with all U.S. Department of Education (DOE) mandates, including those for information exchange. Recently, this called for updating its existing student loan processing solution to more tightly integrate with federal XML transmission standards, while improving performance, security, and manageability.	Achieved approximately 30-second elapsed time for first large production run Streamlined administration and support of the information exchange function by hosting the process within the ClearPath environment
GSA	The U.S. General Services Administration (GSA) wanted to improve the efficiency of key operations while enabling employees to work more productively. This called for	GSA avoided spending an estimated $9.9 million for new application development by web-enabling, and preserving the value in, existing applications. Through intuitive ClearPath ePortal

	moving from "green screens" to a user-friendly graphical user interface (GUI) for applications that support Federal Asset Management functions, without requiring extensive, time-consuming, and costly changes.	technology and only one week of training, the Agency delivered new capabilities well within deadlines. Thanks to modern front-end interfaces, users can now navigate quickly through newly enhanced applications to perform work faster.
EMC Insurance	EMC turned to Unisys for help in several areas. First, the insurer's portfolio of online services was growing – driving up demand for processing power. In addition, the 35-year-old power equipment in its downtown Des Moines location needed to be updated – causing EMC to consider a costly move of its production data center to a new location.	A robust IT infrastructure, featuring two physically separate data centers with ample capacity to back each other up in case of disaster, is further reinforced with such Tier 3 attributes as dual power and communication feeds and a backup generator at one location—enabling EMC to provide secure Internet services and achieve a quick recovery time objective in disaster situations. The company avoided a $4 million data center "build and relocation" expenditure. BIS and ICE development tools allowed the organization to quickly respond to market demands for new online services. A Pay-for-Use business model and metering technology help EMC put processing power where it's needed—instantly. Built-in power allows ClearPath servers to grow with EMC's business.
TravelSky Technology Limited	A leading provider of information technology solutions for China's air travel and tourism industries needed to provide expanded	Availability: Enabled real-time data delivery and secure, continuous business operations for smooth passenger reservations and

	capacity and secure operations in preparation for the 2008 Olympic Games in Beijing.	departure control Growth: Provides capacity needed to meet double-digit annual traffic growth Agility: Easily supported a 20% increase in peak processing requirements during the Olympics, compared to the average number of transactions per second handled during an active 3-month period in the previous year
State of Washington Automated Client Eligibility System (ACES)	Since the initial install, ACES has had many enhancements and innovations. Web-based development was introduced in phases. Migrating to a Web-based approach has become a priority, and projects are being defined that will move existing legacy-based functions to the web more quickly. A new client facing portal was installed in 2010.	The Team supports a dedicated Mainframe environment for the account. Capacity reports and trending are provided on a monthly basis and IBM works with the customer to define and recommend architecture changes to meet future needs and strategy. IBM manages the Mainframe which includes a z/OS and z/VM Linux platform. The legacy functions of the application run in z/OS and web based functions run in Linux. Services include currency of all system software, installation and configuration. The operation environment is monitored and problems are diagnosed and resolved.
State of Georgia – Georgia Technology Authority	In 2007, the State of Georgia conducted a third-party assessment of the state's IT operations and documented serious and chronic problems throughout state government which included aging infrastructure, the inability to meet minimum industry	IBM provides a scope of service to the State of Georgia that is very similar to that desired by the Commonwealth of Pennsylvania and includes-- Mainframe support Ongoing support: OS patching, hardware break/fix

	standards, the lack of processes and skills, little coordination of spending and deficiencies in disaster recovery. Georgia determined that their most efficient method for addressing their challenges was to partner with private-sector leaders in technology service delivery. The State awarded an 8-year contract for IT Infrastructure Services to IBM. The contract includes mainframes; distributed computing servers and associated storage; tape; network connectivity and security; print; service desk; end-user computing and disaster recovery. The end result meant saving money, staying current with modern technology and ensuring that confidential data remains safe and secure from outside threats.	Common ITIL-based systems management services including incident and problem management, performance management and capacity management Manage backup recovery, tape (on/off site) and disaster recovery. Implement standard monitoring tools and provide 24x7 monitoring. Upon transformation, systems consolidated into a State of Georgia data center supported by IBM

Benefits to the Commonwealth

As the Commonwealth is aware, the current services provided by the Unisys Mainframe team have provided technology and support services with a high level of client satisfaction. The proposed Unisys Mainframe Service solution contained in the response is designed to not only continue to supply the level of services expected but add additional value. The solution is based on the core services provided by the Unisys Team and adds the overall Unisys Enterprise Architecture Operating Model. This Operating model provides consistence in service delivery across all platforms including Enterprise IT Service Management and Managed Hosting services.

The solution provides the Commonwealth with a new hardware compute environment that is based on a consumptive utility model versus the previous fixed asset model available in the past. This new compute model reduces cost to the Commonwealth and provides an opportunity for continuous cost improvement over time as new technologies are released which can be leveraged by the agencies. As part of the Capacity Planning process the Unisys Team will work with the Commonwealth agencies to determine if new Mainframe Services are available which can be leveraged to further reduce costs.

The Unisys Team has been responsible for migration the Commonwealth through several technology upgrades in the past. By selecting the Unisys Team to provide Mainframe Services the Commonwealth avoids both the risk of a newcomer's initial learning curves as well as the

service cost to Agencies and Commonwealth citizens during the outages that often result from such learning curves.

The Unisys Mainframe Services are part of the overall Commonwealth IT Service Management Program. This program will provide additional efficiencies through common processes, increased automation and a centralized CMDB. The IT Service Management program will allow IT resources to focus on problem resolution versus daily operational tasks which will improve service delivery and reduce costs.

3.2.4.6 Security & Firewall

The Security & Firewall service will provide hosting and operational support Services for security products and firewalls located at the data centers. These security devices and Services protect the equipment and applications in the data centers from malicious attempts to penetrate the computing environment with worms, phishing, Trojan horse malware, and unlawful data access. Offeror must install and maintain mainstream security hardware and software utilizing current industry best practices sufficient to protect the enterprise class data center environments with a significant volume of sensitive class data (e.g. HIPAA, CJIS, CHRIA, PCI, PII, etc.). The number of support staff members required to perform the tasks listed below will be determined by the Offeror.

Listed below are the basic Services required to manage the security & firewall systems required by the Commonwealth. Offeror must include these Services in addition to the base level of Services in this Offering.

Reference Documentation

Exhibit A - Commonwealth Network Environment

Exhibit J.1 through J.3 - Commonwealth Security and Compliance Requirement

Exhibit G.6 - PSP - CJIS Security Policy

Exhibit G.9 - PSP - CCHRI

Exhibit G.7 - PSP - Summary of CJIS Requirements

Exhibit G.12 - PSP - CHRIA Handbook

	Requirements	Describe Compliance
1.	Monitor local security operations, troubleshoot and resolve operational issues. Actively (normal daily process) monitor the operations of all security,	Offeror must describe its approach to supporting the needs of the Commonwealth including the following: • Processes & Procedures

	firewall systems and security zones. Maintain a log for each server/appliance/system and review the system logs on a daily basis to ensure key system Services are processing without errors. Provide the ability to import data to agency SIEM or enterprise SIEM tool for correlation and reporting purposes. Provide the ability for Commonwealth agencies to request security modifications (firewall changes) as documented in the CCPM. Document review of the system security logs on a weekly basis to ensure critical system Services are processing without errors. Complete weekly server log indicating which logs were reviewed, date and initial the log.	• Tools / Applications • End User Reports o Standard o Custom • Tiered Service/Support Levels • Escalation Procedures Offeror must describe prior experience relative to providing datacenter management and support of CJIS, CCHRI, HIPAA and PCI compliant systems.
2.	Provide security training to Commonwealth personnel specific to the security Services being delivered. Provide the Commonwealth with a resume or CV for each operational staff member assigned to this engagement. Comply with agency background checks and clearances as defined in Appendix A - Terms and Conditions.	Offeror must describe its approach to supporting the needs of the Commonwealth. Offeror must submit a representative sample of staff resumes typically provided for these positions and describe the process to ensure compliance of background checks and clearances.
3.	Achieve cost effective 24/7 security operational coverage for this critical system. Provide dedicated security support staff onsite during scheduled business days, and automated log and notification systems to alert security team of possible intrusion events in real time	Offeror must describe its security operations coverage and how it will be applied.

	mode. Provide Level 2 and Level 3 Support to the Service Desk and/or Commonwealth Users. Security staff must be available to respond and evaluate the severity of the event 24/7/365.	
4.	Ensure network connectivity, and ensure consistent system response times. Utilize automated system management tool(s) to ensure real-time monitoring and notification of server availability and response times.	Offeror must describe its real-time monitoring approach and toolset to provide and maintain network availability and performance. Offeror must identify tools it uses to support network availability and performance.
5.	Ensure server/appliance operating systems are maintained with the current system patch level. Implement a Patch Management Program to ensure the timely application of security updates on all infrastructure platforms in accordance with Commonwealth IT policy guidelines. Ensure signature and threat analysis files are updated on a regular basis, and conform to industry best practices. Analyze monthly service patches and determine which patches need to be applied, by server type. Create a change record, log the update in the server log, and install based on server availability schedule. Notify the Commonwealth of any scheduled or unscheduled service interruptions.	Offeror must describe its approach to supporting the needs of the Commonwealth. Offeror must describe its approach for testing and validating updates to the OS and 3rd Party software that it supports. Offeror must describe its approach to communicating unscheduled and scheduled outages, including escalation process.
6.	Provide active security operations,	Offeror must describe its Security

	corrective action, and reporting by utilizing Offeror software to monitor inbound and outbound traffic for malicious patterns and content, and take appropriate protective measures. The ability to utilize security management software to detect threats and analyze firewall logs, to proactively detect and protect from malicious events. Comply with agency specific security requirements. Comply with all agency and OA/OIT security policies and ITBs. On a quarterly schedule, run appropriate penetration testing, and report results to Commonwealth and Offeror. Create monthly report on events, incidents and corrective activities. Report that indicates systems not in compliance with security standards. Real time reporting of security breaches.	Operations Process and how it will be applied.
7.	SLA Reporting including but not limited to collecting actual system availability, utilization and response time data. Create a Service Level Agreement report for the Commonwealth and Offeror on a monthly basis.	Offeror must describe its approach to supporting the needs of the Commonwealth.
8.	Software License Management	Refer to 3rd Party Software Management service.
Continual Process Improvement		
9.	Reduce service risks.	Offer methods to eliminate or mitigate

		service risks.
10.	Improve service quality. Make recommendations to the Commonwealth team any system changes that would be appropriate to maintain or improve SLA commitments on a quarterly basis.	Offeror must describe its approach to supporting the needs of the Commonwealth.
11.	Improve client satisfaction.	Offeror must provide examples of previous Offeror initiatives aimed at continually improving client satisfaction.
12.	Ensure service transparency using documentation methods to ensure service transparency, by providing visibility into service execution.	Offeror must describe its approach to supporting the needs of the Commonwealth.
13.	Improve/reduce cost of service.	Offeror must provide examples of Security and Firewall Support initiatives that have been implemented or can be utilized to achieve reduced costs of Services and to meet or exceeded ROI (Return on Investment) analysis projections.

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

Introduction

Unisys understands the importance of the critical need for the Commonwealth to protect its equipment, applications, and data such as HIPAA, PCI, PII, CJIS, and CHRIA, from malicious and unlawful attempts to cause harm to its computing infrastructure. Unisys will leverage its experience with industry leading security and firewall products to provide hosting and operational support services within the Commonwealth's data centers.

1 Security Operations Approach, Experience

1.A Offeror must describe its approach to supporting the needs of the Commonwealth including the following:

Processes & Procedures

Tools / Applications

End User Reports (Standard and Custom)

Tiered Service/Support Levels

Escalation Procedures

Monitor local security operations, troubleshoot and resolve operational issues.

Unisys will manage security operations in accordance with our standard model for site operations. Unisys will monitor security devices via a standardized logging platform that supports syslog, SNMP, and Windows event logging. The Unisys SIEM (Security Incident and Event Management) will support correlation of system logs in order to identify, report, and enable security staff to respond to potential security incidents. Schedule F, Sections 3.1.2, 3.2.3.2 and 3.2.2.5 contain additional details regarding the processes, procedures, tools, and applications for monitoring network and security operations as well as escalation procedures.

Unisys will work with Commonwealth security staff to provide periodic, standardized agency reports for security incident and management. The following are some of the significant reports that will be provided to the Commonwealth.

Report Category	Standard Reports
Change Management Standard Reporting	Forward Schedule of Change Emergency Changes Report Change Backlog Report Open Changes by Status Changes that Spawned Incidents Changes that Spawned other Changes Changes Requests Backed Out Change Lifecycle and Process Efficiency Open Changes by Phase Change Rejected by CAB Planned Unavailability by Change Change Lead Time Report Change Backlog Report Change Bypass Process Report Change Trend Report Change Reason Report
Incident Management Standard Reporting	Number of Incidents by Status Incident Volume Trend Report Open Incidents Aging Report Incident Resolution Time Analysis Number of Incidents by Impact Number of Incidents opened by Operations Percentage of Incidents reopened Backlog of Unresolved Incidents

	Top Requestor Departments Top Requestor Sites Number of Incidents by Reported Source Number of Incidents by Product Category Number of Incidents with Status of Pending SLA Performance Summary Response Time Metric Report Metrics Scorecard Incident Trend Report Top 10 Resolvers Group Report
Problem Management Standard Reporting	Number of Problems by Status Percent of Re-occurring Problems by Impact MTTR for a Problem Average Time lag for Problem Resolution and closure Percent of Problems with a RCA Number of Opened Problem by Investigation Drivers Aging of Open Problems Number of Problems by CI Ratio of Problems to Incidents Number of Problems with High Priority Incidents

Security changes and problems will be categorized within these comprehensive reports. The Unisys SIEM tool and Remedy Platform has the ability to provide ad-hoc, customized reporting and will follow prescribed security incident procedures (SIP) in accordance with the ISO27001 standard and associated proposed SIP document. Unisys has a Catalog Service for the Commonwealth to request customized reporting.

1.B Actively (normal daily process) monitor the operations of all security, firewall systems and security zones.

The Unisys SIEM platform integrated with the Remedy Incident platform will provide automated and customizable log reviews and incident escalation to dedicated, on-site security operations staff during the scheduled business day's review of critical system processes and components.

1.C Maintain a log for each server/appliance/system and review the system logs on a daily basis to ensure key system Services are processing without errors.

System logs, including all servers, appliances, and network/security devices will be maintained through a combination of individual server logging, the enterprise monitoring platform, and the

enterprise SIEM system. Data center operations staff will monitor servers, appliances, firewalls and security systems to confirm proper equipment operations. These activities will be documented in logs for each device and reviewed daily for proper operations. Please refer to Schedule F, Section 3.2.3.2 – Site Operations for more details.

1.D Provide the ability to import data to agency SIEM or enterprise SIEM tool for correlation and reporting purposes.

The Unisys SIEM can support exports of security incident data via syslog transfer or flat file export (CEF or CSV) into the Commonwealth's SIEM environment.

1.E Provide the ability for Commonwealth agencies to request security modifications (firewall changes) as documented in the CCPM.

The Commonwealth will be able to request security modifications through the Change Management Process documented in the CCPM.

1.F Document review of the system security logs on a weekly basis to ensure critical system Services are processing without errors.

Unisys will automate security event management using the Unisys SIEM platform with the [redacted]) platform for consolidated incident and event management. Security staff will periodically review system security logs to identify any unusual events.

1.G Complete weekly server log indicating which logs were reviewed, date and initial the log.

The Unisys security team will conduct a weekly server log review, indicating which logs were reviewed. Each entry will be dated and initialed.

1.H Offeror must describe prior experience relative to providing datacenter management and support of CJIS, CCHRI, HIPAA and PCI compliant systems.

Unisys recognizes that the Commonwealth's business needs and application are required to adhere to many federal and state regulations and statutes, including CJIS, CHRIA, IRS Federal Tax Information, PCI and HIPAA. Unisys will continue to work with the Commonwealth to maintain the Commonwealth's environments to meet the technical and audit requirements for these regulations.

Unisys currently supports agencies such as the Department of Public Welfare, Pennsylvania Liquor Control Board, Department of Revenue, the Department of Health, and the Pennsylvania State Police in the DPH required to adhere to and be audited on the security standards of CJIS, CCHRI, HIPAA, PCI, NIST, FISMA and IRS. As required, Unisys will support Commonwealth agencies in complying with these stated security requirements by ensuring the appropriate complement of network security devices are implemented for each agency.

The Unisys Team has provided data center management in support of other government agencies in support of CJIS, CCHRI, HIPAA, and PCI systems. As an example, Unisys designed a data and records management system for the Alabama Criminal Justice Information Center that was required to meet CJIS and CHRIA requirements. The Alabama Criminal Justice Information Center (ACJIC) is a state agency providing local, state, and federal criminal justice agencies with the information needed for citizen safety. ACJIC realized that gaps in its information technology were hindering communications and business continuity. It needed to more efficiently deliver critical information from its network and systems. ACJIC explored several solutions and solution providers before choosing Unisys to help establish an IT infrastructure specifically designed to address the agency's requirements.

2 Training Approach, Security

2.A Provide security training to Commonwealth personnel specific to the security Services being delivered. Offeror must describe its approach to supporting the needs of the Commonwealth.

Unisys will create and present annual training to Commonwealth personnel addressing the security requirements and features of the data center. Please see Schedule F, Section 3.3.2.2 – Security Transition for details on our formal security training program.

2.B Provide the Commonwealth with a resume or CV for each operational staff member assigned to this engagement.

Offeror must submit a representative sample of staff resumes typically provided for these positions and describe the process to ensure compliance of background checks and clearances.

Unisys will manage, as it currently does, background checks for all staff members. A representative sample of staff resumes for individuals who typically fill these positions are provided in the representative resume section of this proposal (see Section 5.0 Personnel).

2.C Comply with agency background checks and clearances as defined in Appendix A - Terms and Conditions.

In accordance with Appendix A section 44, the Unisys Team will perform fingerprint background checks consistent with ITB-SEC009 and CJIS policy on all Unisys Team personnel providing support or services for the Commonwealth. As part of our ISO27001 certification, we perform an annual 3rd party/subcontractor review as well. Unisys has been completing Commonwealth specific background checks since the beginning of the Data PowerHouse contract. Unisys will provide written confirmations to the Commonwealth when the background checks are conducted. Please refer to Schedule F, Section 3.2.1.1.3 Subcontractor Management for more details on our process for performing background checks.

3 Service Desk, Tiered Support, Operational Coverage

3.A Achieve cost effective 24/7 security operational coverage for this critical system.

Offeror must describe its security operations coverage and how it will be applied.

Provide dedicated security support staff onsite during scheduled business days, and automated log and notification systems to alert security team of possible intrusion events in real time mode.

Unisys will provide dedicated network/security support staff onsite during scheduled business days, coupled with automated tools that provide real time notification of suspected security intrusion events. Unisys Security Operations Center (SOC) is comprised of these security support staff and a suite of automated tools that provide comprehensive 24x7x365 monitoring, alerting, and response to security events. Personnel follow specific instructions to mitigate issues according to the Security Incident Procedure (SIP) policy.

3.B Provide Level 2 and Level 3 Support to the Service Desk and/or Commonwealth Users.

The Unisys security team will provide Level 2 and Level 3 Support to the Service Desk and/or Commonwealth users for security related incidents and requests. There are three levels of support in the Incident Management process. The first level of support is provided by service desk agents who have general expertise across many disciplines in order to restore a service. If first level service desk agents cannot restore the service, then a second level service desk agent – who has deeper expertise and more experience resolving incidents – is engaged. Third level escalations involve subject matter experts (e.g., vendors) who generally reside in external organizations (e.g., other IT disciplines or vendors) in order to restore a service. In the case of security related incident handling, the service desk agents will engage the Unisys security team to effectively resolve security matters. Please refer to Schedule F, Section 3.2.3.2 – Site Operations for more details.

3.C Security staff must be available to respond and evaluate the severity of the event 24/7/365.

The Unisys Service Desk (Level 1) will monitor the network/security team's response for security related incidents. The Service Desk will help to verify that the Unisys network/security team responds even during off hours depending upon the SLA requirements for incident priority response.

The [redacted] will collect, prioritize and forward all significant security events to the [redacted]. Network events will be correlated with other significant events and incident tickets will be auto-generated for identified significant security events. Notifications will be sent automatically to the Unisys network/security team (Level 2) and other Commonwealth stakeholders through email.

Events will be escalated to senior Unisys network/security support resources (Level 3) and/or the OEM as needed to verify availability SLAs are met.

4 Monitor network Connectivity, Toolset

4.A Ensure network connectivity, and ensure consistent system response times.

Unisys will provide event management solutions to help confirm network connectivity and consistent system response times. Proactive monitoring tools will be used that monitor excessive delay and latency in the network.

Offeror must describe its real-time monitoring approach and toolset to provide and maintain network availability and performance.

4.B Utilize automated system management tool(s) to ensure real-time monitoring and notification of server availability and response times.

Offeror must identify tools it uses to support network availability and performance.

Unisys will utilize automated system management tool(s) to provide real- time monitoring and notification of server availability and response times including the stop and start times of servers to support SLA availability measurements. The following tools are the major toolsets to support network and system event management and monitoring.

Monitoring Software	Managed Configuration Items (CI's)	Monitoring and Management Functionality
[redacted]	LAN Devices including: • Switches • Routers • Load Balancers • Firewalls	Provides deep network device availability and performance monitoring, DNS, IP address management, network configuration management, and network traffic bandwidth throughput monitoring
[redacted]	Microsoft servers, databases, network devices, and storage hardware.	Provides a standard set of availability, performance and critical service monitors developed by Unisys for monitoring across infrastructure items including: • Servers • Network devices (switches, routers, load balancers) • Storage devices • Middleware • Applications (Exchange, Citrix XenApp, etc.)

For a complete understanding of how this subset of Event Management Tools supports enterprise Event Management please refer to 3.2.3.2 Site Operations.

5 Patch Management

Ensure server/appliance operating systems are maintained with the current system patch level.

Offeror must describe its approach to supporting the needs of the Commonwealth.

Implement a Patch Management Program to ensure the timely application of security updates on all infrastructure platforms in accordance with Commonwealth IT policy guidelines.

Offeror must describe its approach for testing and validating updates to the OS and 3rd Party software that it supports.

Ensure signature and threat analysis files are updated on a regular basis, and conform to industry best practices.

Analyze monthly service patches and determine which patches need to be applied, by server type.

Create a change record, log the update in the server log, and install based on server availability schedule.

Notify the Commonwealth of any scheduled or unscheduled service interruptions.

Offeror must describe its approach to communicating unscheduled and scheduled outages, including escalation process.

The Unisys technical support team will patch based on Commonwealth /Agency policies as defined in the ITBs. The patch program will address policies, processes, procedures for the following:

- Sources of patches (how to obtain them from the OEM's)
- Toolsets that will be used to stage patches for possible deployment
- Change management procedures supporting the Change Management Process to identify, approve and manage deployment of patches
- Compliance procedures to include utilization of the toolsets to run compliance audits and identify out of compliance CI's with patch policies and approved changes
- Process and procedures to bring out of compliance CI's back into compliance

Unisys will follow the Change Management Process for applying patches to all IT infrastructure CI's. This process will maintain the change record in the [redacted] platform and also update the CMDB configuration management file after completion of the patch release and deployment process. The [redacted] change record will be related to the CI's in the CMDB as an audit trail for patch changes upon the completion of the Release and Deployment Process.

The distributed IT infrastructure toolset to support the automation of patch release and deployment is [redacted]. Unisys will maintain in this toolset the appropriate patch policies for determining patch deployment and compliance. The [redacted] Suite will be maintained with all the current patches supplied by the OEM's and will be used to manage the production state of patch deployment in the windows environment.

Unisys approach to testing and validating updates to the all CI's is to follow the release and deployment process for all changes into all production environments. The release process includes:

- Change ticket approvals
- Test planning and accepted test results
- Release and deployment planning including release back out plans
- Release testing for risky deployments
- Early life cycle support to help provide a successful deployment *
- Release back out for failed releases

The Unisys technical support team will work with the Commonwealth/Agencies to determine patch policies for which patches should be applied to the server/appliance environment.

Policies will be implemented to govern changes to the server/appliance environment as it pertains to HIPAA, SOX, CIS, etc. and to conform to the Commonwealth policies.

Unisys will follow the Change Management Process for applying patches to the production environment. This process will maintain the change record in the [redacted] and also update the CMDB configuration management file upon deployment for the server/appliance Configuration Item (CI). The Change Record will be related to the CI in the CMDB as an audit trail for changes to servers.

The toolset to support the automation of patch release and deployment is [redacted]. Unisys will maintain in this toolset the appropriate patch policies for determining patch deployment and compliance. The [redacted] will be updated with all the current patches supplied by the infrastructure OEM's and will be used to manage the production state of patch deployment in the infrastructure environment. Unisys will use BSA to support:

- Policies for the server/appliance environment
- Software distribution and server/appliance patching
- Compliance management of patches required for security policies

6 Security Operations

6A Provide active security operations, corrective action, and reporting by utilizing Offeror software to monitor inbound and outbound traffic for malicious patterns and content, and take appropriate protective measures.

Offeror must describe its Security Operations Process and how it will be applied.

The ability to utilize security management software to detect threats and analyze firewall logs, to proactively detect and protect from malicious events.

Unisys will use a combination of intrusion prevention and SIEM (Security Incident and Event Management) software to monitor all inbound and outbound traffic for malicious content in real-time. Unisys will follow the incident and problem management process to expeditiously report and act on all suspected security events, which may include network based blocking of traffic. Firewall logs will be analyzed by both a standardized syslog platform and a SIEM that will correlate with other device logs (e.g. IPS, server, etc.).

6.B Comply with agency specific security requirements.

Comply with all agency and OA/OIT security policies and ITBs.

A Unisys SOC will be created that will adhere to Commonwealth ITBs, OIT policies, audit/compliance requirements; log, analyze and report real-time on all inbound and outbound data center traffic; perform quarterly penetration tests, and report on all issues including breaches.

6.C On a quarterly schedule, run appropriate penetration testing, and report results to Commonwealth and Offeror.

The Unisys Team will perform a quarterly vulnerability assessment and penetration testing of the data center's IT infrastructure. We have illustrated our steps to conduct this assessment in Schedule F, Section 3.2.2.5 Security Management.:

6.D Report that indicates systems not in compliance with security standards.

Quarterly Cyber Threat Intelligence (CTI) diagnostic: Through the Enterprise Services Catalog, the Commonwealth will be able to obtain a Quarterly Cyber Threat Intelligence diagnostic. As part of this quarterly diagnostic, we will perform the following activities

- Intranet cyber compromise analysis: Identify potential Commonwealth data center servers that may be compromised and are attempting to communicate with known adversary controlled devices on the Internet. We will analyze Commonwealth's security audit logs (up to two TB) that contains data up to two weeks from domain name server (DNS) logs, firewall logs and remote access logs of devices supporting critical data center servers.
- Rogue device discovery diagnostic: Perform an analysis on devices currently found in the data center's network to determine if the devices exhibit rogue or stealth-like characteristics. We will analyze up to two weeks of Network Dynamic Host Configuration Protocol (DHCP) and Address Resolution Protocol (ARP)/Content Addressable Memory (CAM) data from the data center's core network switches supporting critical data center servers. We will perform the rogue device discovery will be performed on the data center network that supports up to 2,000 data center servers.

6.E Create monthly report on events, incidents and corrective activities.

Monthly CTI program diagnostic: A monthly CTI program diagnostic will also be available through the Catalog of Services. We will perform an analysis on up to 25 data center servers to identify presence of potentially unwanted programs, malicious files, and unknown binaries.

Details of the security vulnerability assessment are listed below:

- Vulnerability assessment and penetration testing does not include web application vulnerability testing and social engineering assessment
- The Commonwealth will identify a "Trusted Agent" to help facilitate the security vulnerability assessment. The Trusted Agent is responsible to:
  - Define scope, identify and prioritize the IT assets for the security assessment
  - Make decisions to proceed with applicable testing
  - Coordinate the testing activity with stakeholders like IT infrastructure, application and data center service providers
  - Coordinate with other commonwealth agencies (if applicable) during the testing activities
  - Review the vulnerability reports and owns limited "as needed" distribution of the reports. The sensitive nature of information contained in the reports requires a

specific stakeholder being responsible for managing the communication aspects

- Identify mission critical systems of the Commonwealth, business partners or affiliates, and third parties, as applicable
- Identify the time period for communication to the appropriate stakeholders for high severity security vulnerabilities identified in production environment
- Coordinate and authorize the vulnerability assessment team access to the Commonwealth data center's information technology components considered for vulnerability assessment. In order to avoid interruptions, we recommend running many of the assessment tasks during non-business hours. At the Trusted Agent's direction, we execute as many of these tasks as practical during non-business hours.

➢ The Commonwealth "Trusted Agent" and Unisys information security manager will select the servers for the security vulnerability assessment based on business and security criticality

➢ We will use the data center licensed vulnerability scanning tools for this assessment

➢ The Commonwealth will select the four systems to perform the security configuration risk review

➢ The Commonwealth will identify and provide the appropriate audit logs and data for performing the quarterly and monthly CTI diagnostic assessments.

6.F Real time reporting of security breaches.

Unisys will report all suspected security breaches as severity 1 incidents using the incident management process.

7 SLA Reporting

SLA Reporting including but not limited to collecting actual system availability, utilization and response time data.

Offeror must describe its approach to supporting the needs of the Commonwealth.

Create a Service Level Agreement report for the Commonwealth and Offeror on a monthly basis.

The [redacted] Application will be used as the primary platform to manage Service Level Agreements for Commonwealth agencies. The [redacted] provides a continuous real-time platform for collecting the information to monitor and report against Availability SLA's for the Commonwealth. System Availability measurements are based on incident tickets within the Remedy platform. See Schedule F, Section 3.2.1.2, Availability/SLA Management for complete description of SLA reporting and Availability Management.

Unisys will create a Service Level Agreement report for the Commonwealth on a monthly basis as described in Schedule F, Section 3.2.1.2.

8 Software License Management

Refer to 3rd Party Software Management service.

Unisys will be solely responsible for the management of all infrastructure software license products provided through this contract. The goals of this service are to:

- Verify software contract compliance (to avoid non-compliance legal issues and expenses)
- Manage costs of software inventory by matching requirements for use to needs
- Confirm software maintenance contracts are maintained on schedule through early notifications

Unisys will maintain the Software Licensing and associated Maintenance for the Security and Firewall infrastructure using the Software License Management process defined in Schedule F, Section 3.2.1.8 – 3rd Party License Management. Please refer to this section for a complete description of the entire Software License Management process using the [redacted] and [redacted].

Continual Service Improvement

Unisys recognizes the significant importance of Quality and Continuous Service Improvement to:

- Reduce service risk,
- Improve service quality,
- Improve client satisfaction,
- Provide service transparency, and
- Improve/reduce costs of service.

Through a continuous cycle of evaluation and improvement within an IT infrastructure, Unisys views quality and continuous service improvement as a critical success factor in driving customer satisfaction for the Commonwealth IT infrastructure. Each of the continuous service improvement areas identified above are driven through the tight integration of the following organizations, industry tools, proven processes and quality deliverables:

- Service Excellence Office,
- Quality Plans: transition and steady state service delivery
- Industry standard frameworks and methodologies: ITIL, ISO, SSL
- Industry accepted measurement tools
- Continuous Service Improvement & Innovation Processes (CSIIP)
- Risk management, audits and business continuity management
- Client Satisfaction Surveys and Knowledge Management Portal

Collectively this represents Unisys Integrated Quality Plan for the Commonwealth of Pennsylvania.

Specifics on each of these areas are outlined in Schedule F, Section 3.2.1.1.6 Continuous

Service Improvement. Highlights from this section are outlined below and requested service examples are provided at the end of this section.

9 CI Service Risk

9.A Offeror must provide examples of previous Offeror initiatives aimed at eliminating or mitigating service risks.

Risk management, independent quality audits, and business continuity management are integral quality management processes. Unisys is committed to managing risks and facilitating the achievement of business objectives the adherence to quality processes. We mitigate risk through the implementation of tight quality controls: standard policies, procedures, roles, risk assumptions, issues, and definitions, etc.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

10 CI Service Quality

10.A Offeror must provide examples of previous Offeror initiatives aimed at improving service quality.

The quality approach begins with the Service Excellence Office who provides definition and oversight of all ITIL process management and analysis functions. Process managers and analysts working in the Service Excellence Office are responsible for auditing process effectiveness, ensuring that service delivery teams comply with proper execution of processes, and analyzing process trends for anomalies. Continuous service improvement programs in collaboration with Commonwealth agencies are managed by the Service Excellence Office.

Through our Continuous Service Improvement and Innovation Process (CSIIP), the SEO reviews, analyzes and makes recommendations on improvement opportunities in each ITIL lifecycle phase. Unisys will leverage Six Sigma Lean tools and methodologies as well as ISO Certified internal audits to measure and maintain the highest quality services to the Commonwealth.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

11 CI Client Satisfaction

11.A Improve client satisfaction.

Offeror must describe methods to continually improve client satisfaction.

Client satisfaction is extremely important to Unisys and a key focus in our IT solution. The SEO will integrate new agencies, customers and services into our multi-pronged client satisfaction approach that includes Service Desk surveys on the caller's experience, an overall agency satisfaction survey, and quarterly surveys with the Office of Administration. Data collection will be gathered across multiple levels to gain a clear understanding of the Commonwealth's satisfaction with the IT Services being provided.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

12 CI Service Transparency

12.A Provide service transparency.

Offeror must provide examples of previous Offeror initiatives aimed at providing service transparency; in particular, visibility into the service execution process.

The service organizations will use standardized ITSM services processes, IT monitoring and automation tools. ITSM processes will be documented in the Commonwealth Computing Procedures Manual (CCPM). The CCPM will be available to Commonwealth approved staff on the Knowledge Management Portal (KMP) providing desired transparency into service execution processes. Through the Real-time Dashboard, the Commonwealth will have access to current operational performance of their application infrastructure.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

13 CI Reduce Cost of Service

13.A Improve/reduce cost of service.

Offeror must provide examples of previous capacity initiatives implemented that achieved reduced costs of Services and that met or exceeded ROI (Return on Investment) analysis projections. If costs of Services increased due to increased required capabilities, so identify.

The Service Excellence Office will proactively manage quality, continuous service improvement, ITIL process management, and customer satisfaction through a comprehensive quality plan that specifically addresses all of these areas. We believe this is a key differentiator in our partnership with the Commonwealth. Through this new organization and these quality plans, Unisys will drive best in class services and the highest customer satisfaction experience, while reducing overall costs to the Commonwealth.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

A few examples of Security & Firewall support and initiatives that have been implemented or can be utilized to achieve reduced costs of Services and to meet or exceeded ROI (Return on Investment) analysis projections are outlined below:

1. Reduce Service Risks

In order to proactively identify possible network security risks, the Data PowerHouse implemented intrusion detection services in 2010 for all COPANET/MAN connections. This technology, coupled with the [redacted] MARS logging analysis platform, allows Unisys to identify and correlate IDS, firewall, and network switch/router logs for additional protection against the growing number of network based security threats. Suspected events are investigated and reported to the OA CISO office, which allows the Commonwealth to gain even greater insight into potential risks of their hosted systems and eliminate or mitigate those service risks.

2. Improve Service Quality

In 2010 Unisys began to provide virtual private network (VPN) services to the PA Game Commission in order to provide sensitive data traversing the network from the Data PowerHouse was encrypted. In 2013 the Department of Revenue also plans to utilize these encryption services over COPANET to confirm their data is protected in transit from the DPH.

These are examples of the types of recommendations Unisys will make to the Commonwealth team regarding any system changes that would be appropriate to maintain or improve SLA commitments on a quarterly basis.

3. Improve Client Satisfaction

In late 2009 Unisys began offering vulnerability scanning for nearly all agencies in the Data PowerHouse to expose potential security vulnerabilities and verify that Commonwealth mission critical systems are patched accordingly. This incremental service provides scheduled reports on a quarterly basis that the DPH service delivery staff review with the agency to verify they are able to continuously improve their security posture and reduce overall risk.

4. Provide Service Transparency

The Unisys Data PowerHouse began offering self-service firewall log review to selected agencies that requested this feature in 2012. This allows hosted agencies such as IES and the PA State Police to review the firewall logs that pertain to their managed systems for dropped or accepted packets, reducing their troubleshooting times and expediting the overall firewall change process for them. Agencies with self service capability have praised Unisys for this ability to get a glimpse into their operational network security policy, ensuring that when they are troubleshooting application issues, or deploying new services, they are able to identify and/or anticipate what changes will need to be implemented on the DPH firewalls.

5. Improve/Reduce Cost of Service

As a part of the 2008 contract extension to the Data PowerHouse, Unisys began a firewall consolidation initiative tied to the increasing use of shared infrastructure components and firewall virtualization. Prior to this, agencies in the DPH used separate physical Check Point firewalls. These were consolidated onto a shared [redacted] firewall service module (FWSM) platform, with each agency retaining a logical firewall partition with distinct security policy and configurations. This allowed for a significantly less complex hardware environment and reduced maintenance and licensing costs.

Unisys Team Experience

Unisys has provided decades of mission-critical enterprise security experience with large-scale deployments including Federal agencies. For example, Unisys collaborated with the USDA Agriculture Security Operations Center, 14 product vendors, and 7 technology vendors to implement a forward-thinking security solution to enhance proactive identification and defensive response to cyber security threats at strategic USDA locations throughout the United States.

The implementation of the USDA Security Sensor Array (SSA) was achieved by integrating and incorporating a comprehensive, consolidated, top-down security toolset of seven COTS (Commercial Off-The-Shelf) products and several technologies—the first solution of its kind to be deployed throughout a cabinet-level department in the Federal Government. Within SSA site implementations, seven strategic security technologies were integrated to provide real-time security awareness and understanding of existing and future threats against the USDA assets.

Each SSA includes Security Information and Event Management (SIEM), Intrusion Detection/Prevention System (IDPS), Malware Detection/Prevention System (MDPS), Network Behavior Analysis (NBA), Secure Socket Layer (SSL) Decryption, Packet Analysis, and Data Loss

Prevention (DLP). In addition to enterprise visibility and control, the solution provides local visibility and the capability to resolve Inspector General, OMB, and other security audit findings. SSA delivers the needed protections for USDA. This solution protects 250,000 network nodes at 5,000 locations throughout the United States.

Benefits to the Commonwealth

The Unisys Team, through its extensive security operations expertise, will provide the Commonwealth with:

- Advanced cyber situational awareness and intelligence analysis capability
- Leveraged security strategic planning and design, integrating current tools and organizational structures.
- Operational efficiencies from streamlined incident management
- Accelerated system development, integration, and deployment, with decreased implementation and operational risks.
- Assurance of a secure operational cyber environment through an integrated approach to risk management.

3.2.4.7 Database Management Services

The Database Management Service will provide the Commonwealth with a "managed database" service offering. The service must include the database platform (Hardware/Software) and the ongoing database management administration Services. The Offeror must provide a multi-tiered level of service (e.g. Gold, Silver, and Bronze) across multiple database platforms. While the Commonwealth's application portfolio (over 2,000 applications) currently utilizes numerous database technologies, the majority of the applications that are utilizing database technologies are using Oracle, Microsoft SQL, IMS, Sybase, or DB2.

It is anticipated the Database Management Services will be an optional service that can be utilized by the Agencies beyond the basic infrastructure Services.

Reference Documentation

N/A

Requirements		Describe Compliance
1.	Design, manage, and administer database environments that support multiple business applications.	Offeror must describe proposed approach to designing and supporting enterprise level database platforms and Services that support multiple agency business applications.

2.	Provide Level 2 and Level 3 Support to the Service Desk and/or Commonwealth Users.	Offeror must describe its approach to supporting the needs of the Commonwealth including the following: • Processes & Procedures • Tiered Service/Support Levels • Tools / Applications • Escalation Procedures • End User Reports o Standard o Custom
3.	Monitor database backup and recovery processing on a daily basis. Review daily backup log for successful completion. Note any failures, initial and date the log, and correct the problem. Create problem record for any abnormal condition and any repairs that have been made. Automated software process will be utilized to report the completion status of backup processing, with electronic notification of failures sent to Offeror technical support and identified Commonwealth staff for follow up and corrective action.	Offeror must describe its approach to perform an initial review and audit of the backup and recovery policies, procedures and reports, to ensure the accuracy of the backup schedules, retention periods, target directories, and recovery point objectives. Offeror must describe its approach to identifying gaps and potential risks, and how those gaps and risks will be resolved.
4.	Provide a multi-tiered level of service (e.g. Platinum, Gold, Silver, Bronze, and Basic) for Oracle, Sybase, Microsoft SQL, IMS or DB2 database platforms. Provide Level 2 and Level 3 Support to the Service Desk and/or Commonwealth Users.	Offeror must describe its approach to providing multi-tiered Services level.
5.	Utilize the proposed service	Offeror must describe how its proposed

	management Services (e.g. Incident, Service Request, Change, Configuration) to manage database management Services with multiple agency customers.	database management Services will support multiple agency service requests.
6.	Provide a review and analysis of system performance/capacity to determine if current performance/capacities are sufficient to support the needs of the stakeholders.	Offeror must perform an initial review and audit of the current usage, procedures and reports and provide an analysis of the current usage, processes and reports currently being supported. Offeror must document its review and audit findings and recommendations.
7.	Monitor system backup processing on a daily basis. Review daily backup log for successful completion. Note failures, and correct the problem. Create problem record for any abnormal condition and any repairs that have been made. An automated software process will be utilized to report the completion status of backup processing, with electronic notification of failures sent to Offeror technical support, and identified Commonwealth staff for follow up and corrective action.	Offeror must describe it approach to performing an initial review and audit of the backup policies, procedures and reports, to ensure the accuracy of the backup schedules, retention periods, target directories, and recovery point objectives. Offeror must describe its approach to identifying gaps and potential risks, and how those gaps and risks will be resolved.
Continual Process Improvement		
8.	Reduce service risks.	Offeror must provide methods to eliminate or mitigate service risks.
9.	Improve service quality.	On a quarterly basis, Offeror must also recommend to the Commonwealth team any system changes that would be appropriate to maintain or improve SLA commitments.
10.	Improve client satisfaction.	Offeror must provide examples of previous Offeror initiatives aimed at continually

		improving client satisfaction.
11.	Ensure service transparency.	Offeror must provide methods and practices to ensure service transparency, providing visibility into service execution.
12.	Improve/reduce cost of service.	Offeror must provide examples of Database Management Support initiatives that have been implemented or can be utilized to achieve reduced costs of Services and to meet or exceeded ROI (Return on Investment) analysis projections.

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

Introduction

The Unisys Team understands that databases and the database infrastructure serve as a backbone to mission critical Commonwealth applications. The availability, performance and scalability of these databases is critical to meet the business, user and customer needs managed by these applications.

To support this, the Unisys Team will provide optional Database Management Services. These 'managed database' services will be provided on a wide array of hardware/software platforms to provide the Commonwealth architectural flexibility. These hardware platforms include Unisys, IBM, HP, Dell and many other leading vendors on a variety of operating systems including Windows, Linux, Unix, IBM/Unisys mainframe systems, etc. We understand the majority of Commonwealth applications leverage the Oracle, Microsoft SQL, IMS, Sybase or DB2 database management systems. Our team will provide resources proficient in these technologies.

In addition to architectural flexibility, the Unisys Team will also provide various levels of tiered support across the entire array of platforms to best meet your business and financial needs. These services include:

- Design, Manage and Administer Database Environments
- Provide Level 2/3 support to Service Desk and/or Commonwealth Users
- Daily Monitoring of Database Backup and Recovery Processing
- Multi-Tiered Levels of Service
- Service Request Management
- Performance/Capacity Analysis
- Continual Process Improvement

The Database Management Services provided by the Unisys Team are comprehensive in terms of planning, managing and executing database management. The team provides the Commonwealth access to highly skilled and specialized resources with substantial experience managing state government applications and databases, including many existing Pennsylvania solutions such as DPW, L&I, Insurance and more. In addition to our deep Pennsylvania based relationships, our team also maintains strong relationships with the technology vendor community to keep abreast of the latest developments and advances in database technology.

The Database Management team supports the optional managed database service that includes the database platforms hardware and software and the ongoing database management administration services. This team is comprised of a mixture of resources from Unisys, IBM, and Deloitte who are well-versed in Oracle, Microsoft SQL, IMS, Sybase and DB2 database technologies.

The Commonwealth has requested Database Administration Services to be provided as needed through an optional service to agencies that are seeking support in this area. Since the services are optional, and volumes were not provided in Schedule I Volumetrics, precise staffing numbers are not provided within this section. Our approach to providing Database Administration Services to the Commonwealth is to leverage our partners with the most expertise in supporting the database platforms requested.

In this section, we provide details on our database management capabilities, experience and services delivery against the requirements in the RFP.

1 Infrastructure, Database Environment

1.A Design, manage, and administer database environments that support multiple business applications.

Offeror must describe proposed approach to designing and supporting enterprise level database platforms and Services that support multiple agency business applications.

The Unisys Team provides services to effectively design, manage and administer database environments that support multiple business applications. Our team is uniquely positioned to provide the Commonwealth with the Database Management services as it brings highly specialized staff and deep experience in supporting a highly available and performing infrastructure.

The Unisys Team provides the Commonwealth with 24x7 support to manage database administration, operations and availability. The following represents the Enterprise Services Catalog of Database Management Services that highlights the available services to design, manage and administer your Enterprise database solution:

Database Management Service	Description
Database Design	• Design multiple agency business application database environments • Design the database server and storage platform

	topologies • Design high availability and scalable solutions
Database Creation / Management	• Install and patch database software • Create and maintain shell database instance sized appropriately based on supplied requirements • Create high availability/clustered configurations where requested
Backup Management	• Create and establish database backups integrated with the larger system backup strategy • Monitor and verify successful execution, retention and storage of backups
Database Recovery	• Configure and test database recovery solutions from backup or archive log • Support Disaster Recovery planning, rehearsal and execution
Application Release Management	• Support deployment management through various test environments per defined work plans • Execute physical deployment of application objects within the database
Data Management and Reporting	• Refresh data from backup/export periodically • Create and execute data alteration / extract solutions periodically via supplied requirements • Standard or custom reports as requested
Proactive Database Performance Analysis	• Proactively monitor and report on database health and performance • Provide periodic reports highlighting performance trends and consumption patterns
Proactive SQL Analysis / Tuning Recommendations	• Proactively monitor and report on database SQL performance in the production environment • Provide monthly reports highlighting performance trends and a list of SQL tuning opportunities • Development of tuning options for identified performance opportunities
Provide Level 2/3 Technical Help Desk Support	• Support triage and resolution of calls from the Level 1 Help Desk • Collect and report metrics, solutions and outcomes of said support

The Unisys Team currently supports multiple agencies and applications within the

Commonwealth. We have demonstrated experience successfully managing complex system topologies that support multiple applications within distinct program offices and departments. Our approach on delivering successful projects across multiple agencies requires mature project management disciplines, clearly defined service offerings and efficient and timely communication and partnership with our clients.

2 Service Desk, Tiered Support, Level 2/3 Approach

2.A Provide Level 2 and Level 3 Support to the Service Desk and/or Commonwealth Users.

Offeror must describe its approach to supporting the needs of the Commonwealth including the following:

Processes & Procedures

Tiered Service/Support Levels

Tools / Applications

Escalation Procedures

End User Reports (Standard and Custom)

The Unisys Team provides Level 2 and Level 3 Support to Service Desk and/or Commonwealth Users. The Unisys Team offers multiple levels of database support services to provide timely and efficient handling of service requests, streamlined communications and premium customer service. We provide resources with excellent communication and client service skills to effectively interact with the Service Desk as well as Commonwealth Users to manage database issues/requests.

Our Level 2 technical support provides assistance with basic functionality of the database product, such as availability confirmation, overall performance verification, credential management, authorization and authentication as well as data management services. It is anticipated that Level 2 requests are of limited complexity and usually require limited time to resolve.

The Unisys Team Level 3 technical support includes more specialized and complex services such as targeted performance tuning, database availability and recovery, liaison between application teams and product vendors, overall database configuration, high availability and redundancy management, etc. Level 3 support questions often take more than a single session to resolve, or longer than a single day of engineer time.

The following highlights our approach toward Service Desk and Commonwealth User service/problem requests:

- **Processes and Procedures** – As service requests are identified by clients, the support team logs, triages, investigates and responds to end-user problems or requests. Our team follows a documented problem and incident management process based on the ITIL methodology. Processes and procedures are documented for streamline staff integration as well as facilitating consistent service delivery and expectations. Lastly, our team will focus on timely, clear and targeted communications to effectively manage and close requests with mutual satisfaction.
- **Tiered Service and Support Levels** – The Unisys Team provides tiered services and support levels to provide Commonwealth agencies the ability to customize their support

needs. Services can be 'purchased' from the Enterprise Services Catalog in a tiered support structure highlighted below.

Tiered Support Level	Description
Platinum	• Full time resources proactively monitoring database backups. Available 24x7x365 (on-site coverage averages 96 hrs. / week) with responsiveness SLA's. • Resources are vendor certified (where applicable) with over 10 years of experience
Gold	• Full time resources proactively monitoring database backups. Available 24x7x365 (on-site coverage averages 80 hrs. / week) with responsiveness SLA's. • Resources are vendor certified (where applicable) with over 8 years of experience
Silver	• Full time resources proactively monitoring providing operational status. Available 24x7x365 on-site coverage averages 60 hrs. / week) with responsiveness SLA's. • Resources have over 6 years of qualified experience
Bronze	• Shared resources proactively monitoring providing operational status. Available 24x7x365 on-site coverage averages 40 hrs. / week) with responsiveness SLA's. • Resources are available from a pool of qualified DBA's with over 4 years of experience
Basic	• Shared resources available to support requested execution of listed services. Available 8x5x365 with responsiveness SLA's. • Resources are available from a pool of qualified DBA's with over 2 years of experience

- **Tools or Applications** – In addition to standard desktop software (Office, etc.) the Unisys Team will leverage enterprise class tools to manage database access, inquiry and management. Examples include TOAD, Erwin, Enterprise Manager, Microsoft Management Studio, etc. Licensing changes for these tools may apply and, if required, the tools can be added to the Enterprise Services Catalog. In addition to the database management tools, the Unisys Team will using the enterprise system management tools described in Schedule F, Section 3.2.3.2.
- **Escalation Procedures** –The Unisys Team follows a standard ITIL process flow for service request escalation procedures. The Escalation approach is described in Schedule F, Section 3.2.3.2.
- **End User Reports (Standard and Custom)** – The Unisys Team brings highly experienced

DBAs that provide not only the support in managing databases and resolving issues, but also assisting with the development of end user reports that help with the management of critical Commonwealth applications. Data Management and Reporting is a service included in our Enterprise Services Catalog and governed by the tiered support listed above.

The overall approach for providing daily operations including Processes and Procedures, Tools and Applications, End User Reports, Tiered Service / Support Levels and Escalation Procedures is described in Schedule F, Section 3.2.3.2.

3.A Monitor database backup and recovery processing on a daily basis.

During Steady State operations for Fully Managed servers, the CommVault backup system processing is monitored automatically through the integration of Nagios collectors which generate incident tickets and automated run book procedures upon backup abnormalities that would threaten data protection. This provides reliability in the daily backup processes by addressing run-time issues.

The Unisys Backup team is also able to compare the Backup inventory of clients and policies to the CMDB inventory to locate "negative" gaps in case a server or critical data set is introduced into the Fully Managed environment and, through unlikely process failures, was not also protected with sufficient backup resources. The Unisys governance processes and the processes generated by the Unisys solution's Enterprise Services Catalog are designed to remove such failures. However, following a belt-and-suspenders approach to safety, the compare of Backup infrastructure inventory from the backup tools perspective with the CMDB can locate a gap should one occur.

3.B Review daily backup log for successful completion.

Note any failures, initial and date the log, and correct the problem.

Create problem record for any abnormal condition and any repairs that have been made.

The Unisys solution automates the monitoring of backup logs. Appropriate support personnel are notified to address failures through the ITSM system. Successful backups are reported daily.

Unisys support staff is trained to identify patterns of failure that result in incidents and, following ITIL processes, escalate these to the status of a problem with applicable workarounds and final resolutions. Repairs are carried out as part of incident ticket resolution and are logged following ITIL Change Management processes.

3.C Automated software process will be utilized to report the completion status of backup processing, with electronic notification of failures sent to Offeror technical support and identified Commonwealth staff for follow up and corrective action.

The Commonwealth benefits from the Unisys approach to monitoring backup success rates. In most cases simply re-starting a backup results in a successful backup because needed resources are tied up during peak times but become available a short time later. Unisys automates the restart process. If the restarted backup fails then incident tickets are created to alert the Backup support team. Thus critical issues get right to Level 2 and Level 3 support personnel without

even involving Level 1 support staff.

This automation of incident ticketing provides the Commonwealth with another advantage. During service delivery reviews the Commonwealth can review response times to failures that might put critical applications at greater risk. Through the incident severity rating processes Unisys has the ability to adjust severity levels so that incidents that are closer to critical applications can receive prioritized support responses.

The Commonwealth can also designate application owners who require read access to the backup management console so that these individuals have ready access to monitor both the success and failure rates for backups as well as the backup content. As often happens some applications require specific bundles of directory backups and this access provides application owners a means of validating that any customized backups have been implemented properly and are running correctly.

The Unisys Level 1 DBA team also reviews the post script logs to determine the success or failure of the backup. In case of failures, the report is reviewed with a Level 2/3 DBA for an immediate resolution. A tracker report displaying a series of backups for a period identified are shared with the Commonwealth staff, if needed

A full explanation of our innovative backup service to meet the Commonwealth's data protection needs is provided in our response to the 3.2.4.2 Storage Management table.

3.D Offeror must describe its approach to perform an initial review and audit of the backup and recovery policies, procedures and reports, to ensure the accuracy of the backup schedules, retention periods, target directories, and recovery point objectives.

As part the Transition data gathering activities, the Unisys Team will meet with the Commonwealth to review and audit backup policies, procedures and reports. The activities to perform this review are described in F.3.2.4.2, Requirement 4.

3.E Offeror must describe its approach to identifying gaps and potential risks, and how those gaps and risks will be resolved.

During transition and transformation, the Unisys solution includes an extended onsite presence of a CommVault technical manager who aids the Unisys Team in the search for existing gaps and risks, along with potential improvements to the backup systems during the transition phase of the solution. This technical expert has extensive experience in implementations and in identifying value-add opportunities. The skills of this technical expert are combined with the Unisys Team's extensive expertise around current backup operations. Jointly they lead the transition to the more cost effective CommVault backup infrastructure. The Unisys Team, also working with the CommVault technical manager, manages the review and audit of backup clients that move from the legacy system into the CommVault system. During transition a like-to-like set of backup policies, procedures, reports, schedules, retention periods, target directories, and recovery point objectives are built out. The Unisys Team can then present the Commonwealth for opportunities to further optimize the infrastructure to improve the quality of services or provide better cost efficiencies for the same services.

The activities to perform the gap analysis are described in F.3.2.4.2, Requirement 4.

4 Service Desk, Tiered Support, Multi-Tiered Approach

4.A Provide a multi-tiered level of service (e.g. Platinum, Gold, Silver, Bronze, and Basic) for Oracle, Sybase, Microsoft SQL, IMS or DB2 database platforms.

Offeror must describe its approach to providing multi-tiered Services level.

In order to provide customization and flexibility to Commonwealth agencies, the Unisys Team offers tiered levels of Database Management Services for Oracle, Sybase, Microsoft SQL, IMS and DB2. These tiers offer various levels of administrator experience, on-site coverage and responsiveness SLA's. The tiers are designed to allow for flexibility to manage mission critical as well as development or demonstration environments.

The table above in Requirement 2.A highlights the available tiers and associated capabilities.

4.B Provide Level 2 and Level 3 Support to the Service Desk and/or Commonwealth Users.

The support team providing the database management service will be accessible to the Service Desk and authorized Commonwealth Users through incident tickets assigned to the team. The activities and interactions between the Service Desk and Level 2 and 3 support are described in Schedule F, Section 3.2.3.2.

5 Multi Agency Database Management Services

5.A Utilize the proposed service management Services (e.g. Incident, Service Request, Change, Configuration) to manage database management Services with multiple agency customers.

Offeror must describe how its proposed database management Services will support multiple agency service requests.

The database management services provided by the Unisys Team are customized to the needs of the individual Commonwealth agency via a ITIL centric services catalog. This catalog provides various functional database management support services offered through flexible tiered levels of support based on agency requirements. For example, with the flexible services catalog, the Commonwealth can decide to opt for a Premium Tier support for a critical application for an agency, and decide to choose a Silver Tier support for a less critical application, and another Basic Tier support for non-critical 8AM-5PM application support. This flexibility allows for Commonwealth to serve different agencies and programs in a customized way allowing for the right level of responsiveness and cost.

Our team will leverage ITIL compliant processes to manage Incident, Service Requests, Change and Configuration Modification requests within a multiple agency topology. Our team will leverage enterprise class tools to track the submission, status and disposition of requests with tools such as Remedy, etc. Service request management procedures will be documented to support rapid staff integration, consistent execution and delivery as well as efficient and timely resolution and communication with the requestor.

Our team will work closely with Agency stakeholders to help plan, prioritize and then implement service requests. Requested changes that result in changes to the overall database

configuration are integrated into the Configuration Management Database (CMDB) for architectural documentation, automated monitoring and impact assessment support. Incidents will also be reported, tracked, managed and disposed through our integrated toolset. The toolset will serve as a knowledge repository to help mitigate and avoid reoccurrence of similar issues in the future.

Our integrated team and toolsets will allow us to leverage process best practices, lessons learned and consistent reusable solutions across multiple agencies. This will provide for improved service delivery, more responsive incident management and resolution as well as strategic vision, insight and recommendations to support Agency growth. Lastly, as Commonwealth agencies are working more closely together than ever before, our team will be best positioned to provide efficient, integrated services to support joint, multi-agency initiatives.

The Unisys Team has the technical depth and ITIL based methodology expertise to deliver seasoned level database management support services that will support the continued growth of Commonwealth Agencies. Our team has expertise across a variety of Enterprise class database platforms to support future business growth as well as the integration of new technology across the full spectrum of Commonwealth Agencies. Our efficient, ITIL based Incident, Service Request, Change and Configuration Management processes will provide for efficient and accurate service delivery with effective and timely communication.

6 System Performance Review and Audit

6.A Provide a review and analysis of system performance/capacity to determine if current performance/capacities are sufficient to support the needs of the stakeholders.

Offeror must perform an initial review and audit of the current usage, procedures and reports and provide an analysis of the current usage, processes and reports currently being supported.

Offeror must document its review and audit findings and recommendations.

As the backbone of mission critical applications, database performance, scalability and availability are paramount in delivering strategic business solutions. The Unisys Team has vast experience proactively planning and managing the capacity, configuration and system topology needed to support business processes. Our team will work closely with agency stakeholders to understand the business cycles and translate that into system capacity needs.

Review and analysis of system performance and capacity

Initially, our team will work closely with Commonwealth agencies to perform an analysis of system performance capacity to help verify agencies are positioned to have access to the capacity they need to manage business operations.

The analysis of system performance will cover a wide array of database solutions, including:

- Online Transactional System – A review of business process cycles, batch processing that access transactional repositories, transactional reporting processes and requirements and associated information lifecycle management practices.
- Data Warehouse – A review of the extract, transformation and load (ETL) processes, business analytics processes, cubes and reports that are generated and associated information lifecycle management practices.

- Operational Data Store – Review of ODS ETL processes, reporting and associated information lifecycle management practices.
- Unstructured Data Repositories – Review of any unstructured data (correspondence, images, etc.) solutions and associated capacity needs moving forward.
- Data Recovery – Review of existing data recovery solutions and how that may impact capacity planning.

Verify Current capacity is sufficient

As part of the capacity analysis, the Unisys Team will review the current baseline capacity plan with the Commonwealth to help assess the sufficiency of existing hardware and software resources. As the Commonwealth learns about the application growth from their clients, the Unisys Team develops an average and peak levels of load for estimation against the baseline. This analysis forms the basis for the expected capacity need/growth. Both the expected application usage and the data storage requirements will be used as input to the sizing effort. For the hardware components, this information includes considerations for memory, CPU, network, I/O and disk space. This data will be used to calculate the number of required servers and associated configuration, storage solutions, network accessing solutions and data protection strategies (firewalls, encryption, etc.).

Perform Initial Review and Audit

Current Usage, Procedures and Reports

In addition to the capacity analysis described above, the team will also perform a review of the usage, procedures and reports leveraged against the database. Usage, as discussed, includes the business cycles, ad-hoc reporting, operational reporting, batch processes and other business activities that exercise the database.

Our procedural review will focus on the processes around how the database is governed, including how individual credentials and authorities, service accounts, and data alterations are managed. The analysis will also review the current backup and retention policy and any other Information Lifecycle Management (Purge, Archive) solutions that are in place. Lastly, the review will include a high level review of the procedures around data at rest/in motion encryption and protection.

A high level analysis of reporting processes will be included that focuses on both business reporting as well as database health reports. These reports include generated statistics from the database and the output to identify tuning opportunities, performance anomalies and usage patterns.

Findings will be documented, shared and reviewed with individual agencies to define and verify the 'database lifecycle' baseline. This document will be used moving forward to help govern change validity and impact assessment to the database.

Document Review and Findings

The Unisys Team will prepare, submit and review the findings with the individual agency. The findings will include recommendations to better improve overall operations, decrease costs or increase the maintainability over the current database configuration.

7 System Backup Processing Review and Audit

7.A Monitor system backup processing on a daily basis.

During Steady State operations for Fully Managed servers, the CommVault backup system processing is monitored automatically through the integration of Nagios collectors which generate incident tickets and automated run book procedures upon backup abnormalities that would threaten data protection. This provides reliability in the daily backup processes by addressing run-time issues.

7.B Review daily backup log for successful completion.

Note failures, and correct the problem.

Create problem record for any abnormal condition and any repairs that have been made.

The Unisys Team's backup solution automates the monitoring of system backup logs. Appropriate support personnel are notified to address failures through the ITSM system. Successful backups are reported daily.

Unisys support staff is trained to identify patterns of failure that result in incidents and, following ITIL processes, escalate these to the status of a problem with applicable workarounds and final resolutions. Repairs are carried out as part of Incident ticket resolution and are logged following ITIL Change Management processes.

7.C An automated software process will be utilized to report the completion status of backup processing, with electronic notification of failures sent to Offeror technical support, and identified Commonwealth staff for follow up and corrective action.

The Commonwealth benefits from the new Unisys approach to monitoring backup success rates. In most cases simply re-starting a backup results in a successful backup because needed resources are tied up during peak times but become available a short time later. Unisys automates the restart process automatically. If the restarted backup fails then incident tickets are created to alert the Backup support team. Thus critical issues get right to Level 2 and Level 3 support personnel without even involving Level 1 support staff.

This automation of incident ticketing provides the Commonwealth with another advantage. During service delivery reviews the Commonwealth can review response times to failures that might put critical applications at greater risk. Through the incident severity rating processes Unisys has the ability to adjust severity levels so that incidents that are closer to critical applications can receive prioritized support responses.

The full details for the innovative backup service provided to meet the Commonwealth's data protection needs are included in the F.3.2.4.2 Storage Management.

7.D Offeror must describe it approach to performing an initial review and audit of the backup policies, procedures and reports, to ensure the accuracy of the backup schedules, retention periods, target directories, and recovery point objectives.

Offeror must describe its approach to identifying gaps and potential risks, and how those gaps and risks will be resolved.

The Unisys Team maintains a common set of processes for review, audit and gap analysis for system and database backups. The approach for system backup review, audit, and gap analysis is described in Schedule F, Section 3.2.4.2, Requirement 4.

Continual Service Improvement

Unisys recognizes the significant importance of Quality and Continuous Service Improvement to:

6. Reduce service risk,
7. Improve service quality,
8. Improve client satisfaction,
9. Provide service transparency, and
10. Improve/reduce costs of service.

Through a continuous cycle of evaluation and improvement within an IT infrastructure, Unisys views quality and continuous service improvement as a critical success factor in driving customer satisfaction for the Commonwealth IT infrastructure. Each of the continuous service improvement areas identified above are driven through the tight integration of the following organizations, industry tools, proven processes and quality deliverables:

8. Service Excellence Office,
9. Quality Plans: transition and steady state service delivery
10. Industry standard frameworks and methodologies: ITIL, ISO, SSL
11. Industry accepted measurement tools
12. Continuous Service Improvement & Innovation Processes (CSIIP)
13. Risk management, audits and business continuity management
14. Client Satisfaction Surveys and Knowledge Management Portal

Collectively this represents Unisys Integrated Quality Plan for the Commonwealth of Pennsylvania.

Specifics on each of these areas are outlined in Schedule F, Section 3.2.1.1.6 Continuous Service Improvement. Highlights from this section are outlined below and requested service examples are provided at the end of this section.

8 CI Service Risk

8.A Reduce service risks.

Offeror must provide methods to eliminate or mitigate service risks.

Risk management, independent quality audits, and business continuity management are integral quality management processes. Unisys is committed to managing risks and facilitating the achievement of business objectives the adherence to quality processes. We mitigate risk through the implementation of tight quality controls: standard policies, procedures, roles, risk assumptions, issues, and definitions, etc.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

9 CI Service Quality

9.A Improve service quality.

On a quarterly basis, Offeror must also recommend to the Commonwealth team any system changes that would be appropriate to maintain or improve SLA commitments.

The quality approach begins with the Service Excellence Office who provides definition and oversight of all ITIL process management and analysis functions. Process managers and analysts working in the Service Excellence Office are responsible for auditing process effectiveness, ensuring that service delivery teams comply with proper execution of processes, and analyzing process trends for anomalies. Continuous service improvement programs in collaboration with Commonwealth agencies are managed by the Service Excellence Office.

Through our Continuous Service Improvement and Innovation Process (CSIIP), the SEO reviews, analyzes and makes recommendations on improvement opportunities in each ITIL lifecycle phase. Unisys will leverage Six Sigma Lean tools and methodologies as well as ISO Certified internal audits to measure and maintain the highest quality services to the Commonwealth.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

10 CI Client Satisfaction

10.A Improve client satisfaction.

Offeror must provide examples of previous Offeror initiatives aimed at continually improving client satisfaction.

Client satisfaction is extremely important to Unisys and a key focus in our IT solution. The SEO will integrate new agencies, customers and services into our multi-pronged client satisfaction approach that includes Service Desk surveys on the caller's experience, an overall agency satisfaction survey, and quarterly surveys with the Office of Administration. Data collection will be gathered across multiple levels to gain a clear understanding of the Commonwealth's satisfaction with the IT Services being provided.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

11 CI Service Transparency

11.A Ensure service transparency.

Offeror must provide methods and practices to ensure service transparency, providing visibility into service execution.

The service organizations will use standardized ITSM services processes, IT monitoring and automation tools. ITSM processes will be documented in the Commonwealth Computing Procedures Manual (CCPM). The CCPM will be available to Commonwealth approved staff on the Knowledge Management Portal (KMP) providing desired transparency into service execution processes. Through the Real-time Dashboard, the Commonwealth will have access to current operational performance of their application infrastructure.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

12 CI Improve or Reduce Cost

12.A Improve/reduce cost of service.

Offeror must provide examples of Database Management Support initiatives that have been implemented or can be utilized to achieve reduced costs of Services and to meet or exceeded ROI (Return on Investment) analysis projections.

The Service Excellence Office will proactively manage quality, continuous service improvement, ITIL process management, and customer satisfaction through a comprehensive quality plan that specifically addresses all of these areas. We believe this is a key differentiator in our partnership with the Commonwealth. Through this new organization and these quality plans, Unisys will drive best in class services and the highest customer satisfaction experience, while reducing overall costs to the Commonwealth.

We believe the industrialized manner in which the Unisys Team provides services to the Commonwealth results in efficient, timely and high quality delivery of database services. The efficient, disciplined and repeatable manner by which services are delivered result in reduced cost when compared to less industrialized process management. Additionally, the depth of skill and experience brought forth by our team helps in the prevention of issues, delays or decreased customer satisfaction. Our team is tasked to keep up with database technology changes outside of the standard work day to better understand and prepare for upgrades, new technology integration, and issue management. In addition to their vast, personal experience, our team has access to other practitioners of our global firm to help keep abreast of the latest developments and experiences outside the Commonwealth. Our team has experience with public sector clients at both the local and Federal level as well as all 50 states.

The flexible, Enterprise Services Catalog based, procurement option provided by the Unisys Team also provides for decreased service delivery costs. Our model allows an agency to procure the level of service that is needed to support the business as opposed to the fixed nature of full time employee management. As an example, our 'Basic' tier of service provides for roughly 80 hours of support per month. An agency not using our model would be forced to hire a full time employee to provide this service at roughly 160 hours per month. Our experience has shown that, in this case, the DBA is then given other, non-database responsibilities that dilutes his/her ability to become an expert at database administration – you're left with a resource who is average at two things instead of an expert at one. Our solution provides you access to the equivalent of a fractional resource who is deeply specialized in database technologies that can provide high levels of support at a fraction of the cost.

Unisys Team Experience

The Commonwealth of Pennsylvania leverages many Enterprise class databases to manage the delivery of services to citizens, providers and other stakeholders. Petabytes of data are processed in a variety of database technologies including Oracle, Microsoft SQL, IMS, Sybase and DB2. Our team has provided database management services to the Commonwealth across a variety of these platforms across the Commonwealth including the Departments of Public Welfare, Transportation, Insurance, and Labor and Industry for over 10 years.

In addition, our team has experience in many Federal, State and Local agencies supporting a variety of large scale, public sector lines of business (including almost half of the Affordable Care Act installations throughout the country). This support includes database installation, configuration and tuning services that align with the capacity objectives. Additionally, our team has the technical depth to configure solutions that enhance availability, performance and recoverability in the event of a disaster. Our deep history and familiarity with the database topologies as well as the business processes of these Departments uniquely position us to provide services that will maintain and support growth for years to come.

Benefits to the Commonwealth

The experience described above is also valuable in the introduction of new technologies, processes and solutions. Our team will work closely with you to understand your strategic direction and vision to make appropriate recommendations to further your business goals. One example currently progressing at a Commonwealth agency is the use of database analytics tools and 'Big Data'. The solutions allow for the integration of internal data (databases, correspondence, etc.) and external data (Federal agencies, social media, etc.) to aid in the discovery of trends, facts and opportunities to help a business entity target action to maximize results. Solutions such as these can have a tremendous business benefit with a substantial ROI by leveraging, if progressed by the Commonwealth, Enterprise sharing, licenses and solutions all managed and integrated by the Unisys Team.

3.2.4.8 Limited-Use Colocation Services

While the Commonwealth's goal is to move to a fully managed infrastructure Services model, it is anticipated that there will be a need for the Offeror to provide some limited co-location Services within its proposed data center Services solution. Some examples of where colocation Services may be required are:

- Support for existing systems in the [redacted] prior to transformation to a fully managed service.
- 3rd Party Vendor Equipment that requires co-location with the primary systems for performance and/or security reasons.

The Offeror must provide data center co-location Services with the following options:

- Co-location Service Option 1: Data center Only (Rackspace, power, network connectivity, basic infrastructure Services)
- Co-location Service Option 2: Data center with Managed Services Option (Bronze, Silver, Gold Tiers) – Technology owned maintained by 3rd Party or Commonwealth
- Co-location Service Option 3: Remote Hands Support

Currently there are 3 areas within the Commonwealth [redacted] that are supporting co-location Services. [redacted] facility summary is provided as **Exhibit D.7**. While many of these systems will be migrated to a fully managed service over time, the Offeror shall plan for co-location space in its Data center Architecture.

Reference Documentation

Exhibit D.1 through D.15 Series - Enterprise Datacenter ([redacted] Exhibits

	Requirements	Describe Compliance
1.	Provide colocation Services within each of the datacenters. One of those centers will be the Commonwealth [redacted]	Offeror must describe how each of the datacenters will support its co-location offering within its proposed datacenter architecture.
2.	Provide Colocation Service Option 1: Datacenter Only (Rackspace, power, network connectivity, basic infrastructure Services)	Offeror must describe how it will support this colocation service option.

3.□	Provide Co-location Service Option 2: Datacenter with Managed Services Option (Bronze, Silver, Gold Tiers) – Technology owned maintained by 3rd Party or Commonwealth	Offeror must describe how it will support this co-location service option.
4.□	Provide Co-location Service Option 3: Remote Hands Support	Offeror must describe how it will support this co-location service option.
Continual Process Improvement		
5.□	Reduce service risks.	Offeror must provide methods to eliminate or mitigate service risks.
6.□	Improve service quality.	On a quarterly basis, Offeror must also recommend to the Commonwealth team any system changes that would be appropriate to maintain or improve SLA commitments.
7.□	Improve client satisfaction.	Offeror must provide examples of previous Offeror initiatives aimed at continually improving client satisfaction.
8.□	Ensure service transparency.	Offeror must provide methods and practices to ensure service transparency, providing visibility into service execution.
Deliverables		
Deliverables are defined in **Schedule K – Key Program Deliverables**		
Offeror Response		

Introduction

Unisys colocation services provide for the Commonwealth's need to maintain its own equipment within the data centers when the selection from the Unisys Enterprise Services Catalog is not practical. This colocation service provide space, power, network and cabinetry on the data center floor.

The colocation service is designed to support rack-mounted equipment within secure colocation cabinets ranging from ¼ cabinet to ½ cabinet and to a full cabinet (reference Schedule C, part numbers "CCSU13330008-A", "CCSU13330009-A", and "CCSU13330010-A" for the colocation configurations) as show in **Figure 3.2.4.8-1**. Optional Enterprise Services Catalog items may combine to meet the unique needs of some agencies including security cages and secure network conduits (see Schedule C, part numbers "CCSU13370501-A" through

"CCSU13370326-A" for secure cages, conduits and other security options).

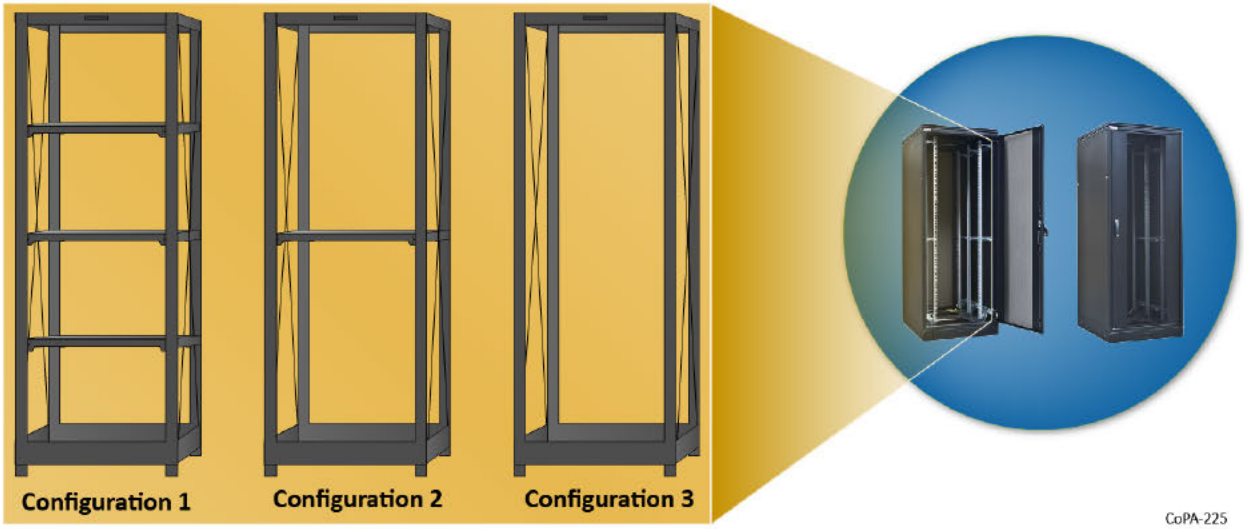


Figure 3.2.4.8-1 – Colocation Configurations

1 CoLocated Services Approach

1.A Provide colocation Services within each of the datacenters. One of those centers will be the Commonwealth [redacted]

Offeror must describe how each of the datacenters will support its co-location offering within its proposed datacenter architecture.

Unisys colocation services are available at [redacted] and the [redacted] The selection of colocation services from the Enterprise Services Catalog triggers a prompt for the choice of a preferred data center and then solicits comments from the requestor where any specifics such as location within the facilities including adjacency to other systems may be provided

The selection of the colocation service initiates the change management process with participation from the Unisys Facilities' Space Management team. This Commonwealth dedicated team advises the Commonwealth and Unisys service management on the best placement of the requested service in the facility as part of the change approval review process.

This placement may be in an area dedicated to colocation service, but specific requirements of the requestor are of key influence in the placement decision, especially related requests such as inclusion in a new or existing security cage.

2 CoLocated Services Option 1 Approach

2.A Provide Colocation Service Option 1: Datacenter Only (Rackspace, power, network connectivity, basic infrastructure Services)

Offeror must describe how it will support this colocation service option.

Colocation Option 1 includes rack space, dual power connection and network termination for a

rack or portion (¼ or ½) of a rack within a Unisys facility or the [redacted] Optionally, the Commonwealth may add a request for physical or logical segregation via caging, security treatments and secure network paths within the designated facilities.

This type of service does not include the addition of monitoring or management automation tools typical to the Fully Managed or Managed Only services. However, this service does benefit from the facilities' infrastructure and its support of the most basic reliability and availability architectures inherent in the Unisys facility and network designs.

This service does not include the services of system administrators or remote touch or other systems such as firewalls or load-balancers; each may be requested separately from the Enterprise Services Catalog. In addition, this colocation option does not include support from the backup and recovery infrastructure in the environment. Pricing for this service is provided in Schedule I's "Catalog of Services"; additional information is also provided in Schedule C. "Services Catalog".

3 CoLocated Services Option 2 Approach

3.A Provide Co-location Service Option 2: Datacenter with Managed Services Option (Bronze, Silver, Gold Tiers) – Technology owned maintained by 3rd Party or Commonwealth

Offeror must describe how it will support this co-location service option.

Colocation Service Option 2 gains many of the service characteristics of the Managed Only service offering with the exception of the standardization inherent in the highly prescriptive configuration of the Managed Only resource units.

This service builds upon Colocation Service Option 1 with the addition of the Unisys monitoring and service management tools. SLA support is provided once the proposed configuration passes SLA testing and when support for the requested SLA tier is demonstrated. In addition, complete application architectural definitions are required for the service level tools to be able to provide SLA monitoring and reporting of an application's infrastructure. Unisys additional Technical Services can be requested to assist in the process of application architecture definition if needed to support the application of SLAs to the requested equipment.

This service includes the support of monitoring and systems administration via the association of a Managed Services resource tier such as bronze, silver or gold during the selection of this service from the Enterprise Services Catalog. Backup and recovery becomes available via a related request of storage services from the Enterprise Services Catalog.

4 CoLocated Services Option 3 Approach

4.A Provide Co-location Service Option 3: Remote Hands Support

Offeror must describe how it will support this co-location service option.

Unisys offers remote hands support for any colocation configuration. This option is selected by combining Technical Services with one of the 3 colocation configuration configurations (full, ½ or ¼ rack) from the Enterprise Services Catalog.

Remote Hands Support offers the Commonwealth the option of designating a practical way of gaining continuous support for a co-located system using support hours occurring in the

cadence of care and maintenance for a system.

When this option is selected, the Commonwealth will be prompted to request a number of hours of support per month from the Unisys Team. This number of hours will be pre-allocated to the Commonwealth IT environment and available to staff to support the designated equipment with remote hands support such as media insertion/attachment, local console actions or other actions requiring physical touch. Build and support are limited only to that activity that requires local access.

Remote Hands Support offers the Commonwealth the option of gaining the support of Unisys server installation, administration and local hands support. Such an approach allows the Commonwealth to estimate both the amount of effort needed and a period within which that effort will occur.

Once selected, Unisys provides the needed Remote Hands Support with an eye to the limits established by the Commonwealth. If those limits are approached, Unisys notifies the requestor to confirm they are aware of that the limit is being reached so that the request can be adjusted if desired. This type of request allows for services.

Continual Service Improvement

Unisys recognizes the significant importance of Quality and Continuous Service Improvement to:

11. Reduce service risk,
12. Improve service quality,
13. Improve client satisfaction,
14. Provide service transparency, and
15. Improve/reduce costs of service.

Through a continuous cycle of evaluation and improvement within an IT infrastructure, Unisys views quality and continuous service improvement as a critical success factor in driving customer satisfaction for the Commonwealth IT infrastructure. Each of the continuous service improvement areas identified above are driven through the tight integration of the following organizations, industry tools, proven processes and quality deliverables:

15. Service Excellence Office,
16. Quality Plans: transition and steady state service delivery
17. Industry standard frameworks and methodologies: ITIL, ISO, SSL
18. Industry accepted measurement tools
19. Continuous Service Improvement & Innovation Processes (CSIIP)
20. Risk management, audits and business continuity management
21. Client Satisfaction Surveys and Knowledge Management Portal

Collectively this represents Unisys Integrated Quality Plan for the Commonwealth of Pennsylvania.

Specifics on each of these areas are outlined in Schedule F, Section 3.2.1.1.6 Continuous Service Improvement. Highlights from this section are outlined below and requested service examples are provided at the end of this section.

5 CI Service Risk

5.A Reduce service risks.

Offeror must provide methods to eliminate or mitigate service risks.

Risk management, independent quality audits, and business continuity management are integral quality management processes. Unisys is committed to managing risks and facilitating the achievement of business objectives the adherence to quality processes. We mitigate risk through the implementation of tight quality controls: standard policies, procedures, roles, risk assumptions, issues, and definitions, etc.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

6 CI Service Quality

6.A Improve service quality.

On a quarterly basis, Offeror must also recommend to the Commonwealth team any system changes that would be appropriate to maintain or improve SLA commitments.

The quality approach begins with the Service Excellence Office who provides definition and oversight of all ITIL process management and analysis functions. Process managers and analysts working in the Service Excellence Office are responsible for auditing process effectiveness, ensuring that service delivery teams comply with proper execution of processes, and analyzing process trends for anomalies. Continuous service improvement programs in collaboration with Commonwealth agencies are managed by the Service Excellence Office.

Through our Continuous Service Improvement and Innovation Process (CSIIP), the SEO reviews, analyzes and makes recommendations on improvement opportunities in each ITIL lifecycle phase. Unisys will leverage Six Sigma Lean tools and methodologies as well as ISO Certified internal audits to measure and maintain the highest quality services to the Commonwealth.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

7 CI Client Satisfaction

7.A Improve client satisfaction.

Offeror must provide examples of previous Offeror initiatives aimed at continually improving client satisfaction.

Client satisfaction is extremely important to Unisys and a key focus in our IT solution. The SEO will integrate new agencies, customers and services into our multi-pronged client satisfaction approach that includes Service Desk surveys on the caller's experience, an overall agency satisfaction survey, and quarterly surveys with the Office of Administration. Data collection will be gathered across multiple levels to gain a clear understanding of the Commonwealth's satisfaction with the IT Services being provided.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

8 CI Service Transparency

8.A Ensure service transparency.

Offeror must provide methods and practices to ensure service transparency, providing visibility into service execution.

The service organizations will use standardized ITSM services processes, IT monitoring and automation tools. ITSM processes will be documented in the Commonwealth Computing Procedures Manual (CCPM). The CCPM will be available to Commonwealth approved staff on the Knowledge Management Portal (KMP) providing desired transparency into service execution processes. Through the Real-time Dashboard, the Commonwealth will have access to current operational performance of their application infrastructure.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

Unisys Team Experience

The Unisys Team has supported each of these 3 options of colocation within the [redacted] for several years in a time and materials capacity.

In addition, Unisys currently offers colocation services from many of its other sites. In Latin America Unisys provides colocation for CETIP, a financial market company. They are using 161 square feet of dedicated space in our Rio de Janeiro Data Center as their disaster recovery location.

Unisys provides colocation services to a major telecommunications company. Our responsibilities within the space include media management in our secure tape storage facility, and ad-hoc smart hands and feet. Unisys also manages power to the racks, air conditioning and balancing, humidity and temperature control. The service is located in our Tier 3 facility in the UK. This site is configured with N+1UPS, generator, and twin power feeds from separate sources and diverse network provisioning. The client retains one of our 3 computer rooms for their exclusive use, occupying approximately 5,000 square feet.

Benefits to the Commonwealth

The Unisys colocation services provide opportunities for the Commonwealth to place equipment that needs to be placed within one of the data centers but cannot be sourced from Unisys. Equipment that must be provided by vendors with unique capability or in support of projects has a way to be placed in the service environment of professionally managed data centers with the facility's service capabilities and properties.

3.2.5 Capacity on Demand Services

3.2.5.1 Server Capacity on Demand

The Server Capacity On Demand is an Infrastructure as a Service (IaaS) offering that ensures the ready availability of server and mainframe capacity to accommodate cyclical, and seasonal, processing requirements, sudden or unplanned production demands, and short-term application development needs. Server capacity may be physical or virtual as requested by the Commonwealth.

The Server Capacity On Demand would include support for the following system platforms:

- X86
  - Windows
  - Linux
- I Series
  - i5/OS
- P Series
  - Linux
  - AIX
- Mainframe
  - IBM
  - Unisys

Reference Documentation

N/A

	Requirements	Describe Compliance
1.	Provide a provisioning capability to support on-demand requests for server resource capacity. The Commonwealth will require access to additional capacity on demand for the following platforms: X86 • Windows	Offeror must describe its request and provisioning process for each of the anticipated platform systems. Offeror must describe its approach to supporting the needs of the Commonwealth including the following: • Infrastructure/Capacity

	• Linux IBM I Series • i5/OS IBM P Series • Linux • AIX Mainframe • IBM • Unisys	• Tiered Service/Support Levels • Tools / Applications to manage and maintain capacity • End User Reports o Standard o Custom Offeror must describe its experience operating and managing mixed computing environments such as the Commonwealth.
2.	Maintain an adequate inventory of Windows/Linux, mid-range, and Mainframe server capacity that will be sufficient to satisfy forecasted informal, ad hoc, and cyclical Commonwealth requests.	Offeror must describe its approach to supporting the needs of the Commonwealth.
3.	As a function of ongoing account management, meet with the Commonwealth/Agencies to assess future server requirements.	Offeror must describe its approach to supporting the needs of the Commonwealth.
4.	Encourage Commonwealth server conservation via server virtualization when appropriate.	Offeror must describe its approach to supporting the needs of the Commonwealth.
5.	Provide expedited service, when requested, to satisfy urgent requirements.	Offeror must describe its approach to supporting the needs of the Commonwealth.
6.	Provide a self-provisioning tool to be used by the agencies to order and configure servers.	Offeror must describe its approach to supporting the needs of the Commonwealth.
Continual Process Improvement		
7.	Reduce service risks.	Offeror must describe its approach and provide examples of previous Offeror initiatives aimed at eliminating or mitigating service risks.

8.	Improve service quality.	Offeror must describe its approach and provide examples of previous Offeror initiatives aimed at improving service quality.
9.	Improve client satisfaction.	Offeror must provide examples of previous Offeror initiatives aimed at continually improving client satisfaction.
10.	Provide service transparency.	Offeror must describe its approach and provide examples of previous Offeror initiatives aimed at providing service transparency; in particular, visibility into the service execution process.
11.	Ensure service sustainability.	Offeror must describe its approach and provide examples of previous Offeror initiatives aimed at ensuring service sustainability; in particular, efforts targeted at cost containment and cost reductions.
12.	Improve/reduce cost of service.	Offeror must provide examples of On-Demand Server initiatives that have been implemented or can be utilized to achieve reduced costs of Services and to meet or exceeded ROI (Return on Investment) analysis projections.

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

Introduction

The Commonwealth of Pennsylvania is seeking a comprehensive strategy for dealing with the cyclical demands of capacity by utilizing a strategy of capacity on demand. The value to the Commonwealth in pursuing such a strategy is readily apparent, from both a technical and financial perspective. Financially, a capacity on demand strategy shifts the Commonwealth from a mixture of Capital Expense and Operational Expense, to a more predictable Operational Expense. This type of strategy obviates the need for large capital expenditures for the upgrade

and maintenance of compute power on disparate compute platforms, and smoothes the spikes in compute demand caused by cyclical and unforeseen events.

The Commonwealth has asked for a clear definition of the processes and tools that will be utilized in the capacity on demand environment. Unisys has developed a comprehensive strategy in the design of the Server Capacity on Demand infrastructure, by utilizing best of breed hardware and software components that will deliver to the Commonwealth of Pennsylvania a computing infrastructure that will meet the demands of the current workloads, as well as provide the flexibility to move the Commonwealth into the future of a consumption based compute model.

1 Server On Demand Approach

1.A Offeror must describe its request and provisioning process for each of the anticipated platform systems.

The request and provisioning process for each of the anticipated platforms are as follows:

1. The Commonwealth User (user) will log onto the Service Delivery Portal, and select the Enterprise Services Catalog.
2. The Enterprise Services Catalog tool will authenticate and authorize the user
3. Based on what the user is authorized to do, they will be able to select the following:
    a. Technology Platform:
        i. P Series (AIX/Linux)
        - X86 (Windows/Linux)
        - IBM I Series
        - IBM Mainframe
        - Unisys Mainframe
    b. Server Configuration – CPU, Memory, Disk space, etc.
    c. Service Tier – Platinum, Gold, Silver, Bronze, Basic
4. The Enterprise Services Catalog tool's workflow engine will then handle all authorizations for the provisioning.
5. Once approved, the Enterprise Services Catalog tool will open all change records needed to provision the service request.
6. Once the change record is approved, the Enterprise Services Catalog Tool will run an automated run book for each platform that will provision the service request.
7. Post provisioning, the Enterprise Services Catalog tool will call [redacted] as appropriate to perform system patching, security remediation and server conditioning (initial creation of accounts, permissions, etc.).
8. The Enterprise Services Catalog tool will then register the new service in the following tools:
    a. [redacted]

b. [redacted]

c. [redacted]

9. Once all provisioning tasks have been performed, the Enterprise Services Catalog tool will notify the user that the service request has been provisioned and is ready for use.

Offeror must describe its approach to supporting the needs of the Commonwealth including the following:

Infrastructure/Capacity

Inherent in the design of the infrastructure is the ability to utilize extremely small units of growth in all infrastructure components. By utilizing the [redacted] technology as the platform of choice for x86 and IBM pSeries servers, additional capacity in both network and compute can be ordered and brought online very quickly. All hardware platforms will follow a stringent capacity management and optimization process with well-defined triggers for adding capacity that provide future capacity demands are properly planned for and brought online before needed. This provides the Commonwealth an optimized, flexible and automated infrastructure that will smooth demand spikes and ease the last minute budgetary demands for compute power.

Tiered Service/Support Levels

In order to provide customization and flexibility to Commonwealth agencies, the Unisys Team offers tiered levels of managed services for Capacity on Demand servers. These tiers offer various levels of administrator experience, on-site coverage and responsiveness SLAs. The tiers are designed to allow for flexibility to manage mission critical as well as development or demonstration environments.

The following table highlights the available tiers and associated capabilities.

Tiered Support Level	Description
Platinum	• Provides 99.999% Application Infrastructure Availability • Server is monitoring via Nagios • Fully Managed Services • Asset Tracked In CMDB • Requires 3 servers load balanced and geographically dispersed
Gold	• Provides 99.99% Application Infrastructure Availability • Server is monitoring via Nagios • Fully Managed Services • Asset Tracked In CMDB

	• Requires 2 servers load balanced
Silver	• Provides 99.9% Application Infrastructure Availability • Server is monitoring via Nagios • Fully Managed Services • Asset Tracked In CMDB
Bronze	• Provides 99.4% Application Infrastructure Availability • Server is monitoring via Nagios • Fully Managed Services • Asset Tracked In CMDB
Basic	• Provides 98.5 % Application Infrastructure Availability • Server is monitoring via Nagios • Fully Managed Services • Asset Tracked In CMDB
IaaS	• Provides no Application Infrastructure Availability • No Monitoring • No Managed Services • Asset Tracked In CMDB

Tools / Applications to manage and maintain capacity

Utilizing the structure found in the Volumetrics tab of Schedule I, an enterprise services catalog will be developed that will enable the Commonwealth to order compute capacity online. The enterprise services catalog will serve two functions: the first as a central location from which the Commonwealth can order common services from Unisys. The second, more pertinent function is to serve as the central point from which compute capacity can be ordered. Capacity can be both provisioned and de-provisioned from this portion of the Enterprise Services Catalog.

The Enterprise Services Catalog includes the following components:

a. iCollaborate, a web-based front end that functions as the entry point into the Enterprise Services Catalog. iCollaborate performs all authentication, authorization and role adjudication functionality based on integration with the Commonwealths Active Directory service.

b. iRequest, the Enterprise Services Catalog component. For the Commonwealth, the Enterprise Services Catalog will allow the user to specify what type of compute platform is required, what size server or LPAR is needed, and lastly the support tier for the servers being ordered.

c. iDeliver, a complete workflow automation engine. The iDeliver component interfaces via API directly to the [redacted]. The iDeliver component will coordinate all change and request management processes, and where automated server provisioning is support, drive the build of the server environment.

This software suite also includes data for chargeback as well as online reporting for utilization, provisioning and de-provisioning.

The following tables lists the other components of the common IT service delivery platform that will be leveraged to deliver automated provisioning to the Commonwealth.

Tool	Function
[redacted]	• Services Catalog • Workflow automation
[redacted]	• Change Management • Incident Management
[redacted]	• Configuration Management Database
[redacted]	• Atrium Discovery and Dependency Mapping • Update of CMDB
[redacted]	• Enterprise Capacity Management across all servers, network and storage devices • Workload Management and visualization
[redacted]	• Provisioning Engine • Provides post provisioning server conditioning • Patch management and security compliance.
[redacted]	• Monitors Server Operation • Opens automated tickets in Incident management.

End User Reports (Standard and Custom)

Standard Reports are summarized in 3.3.2 Status Reports.

Custom Reports are offered by the Unisys Team as a Catalog Service.

Provide a provisioning capability to support on-demand requests for server resource capacity.

Please see the answer to 1.A above for the process that supports the capability of

Commonwealth users to provision server resource capacity. This process is delivered via the Enterprise Services Catalog tool detailed above in this section.

1.B The Commonwealth will require access to additional capacity on demand for the following platforms:

In addition to platform specific tools, [redacted], combined with the capacity management process, enables the Unisys Team to predict future capacity needs, as well quickly identify virtualization and consolidation opportunities across all platforms.

X86 (Windows, Linux)

Server capacity and on-demand environment requires a very vigorous capacity management regimen that must include future encyclical capacity needs calculations factors such as historical utilization, future growth plans as they are developed, as well as the velocity of changes to the environment. With these factors in mind, the environment was designed to be extremely flexible, allowing additional compute capacity that can be added by needed. By utilizing a common compute platform for Windows and Linux physical and virtual servers, decommissioned physical servers can be rapidly redeployed as needed to smooth unexpected surges in capacity. Additionally [redacted] and DRS can distribute and optimize loads to help smooth shorter term spikes.

IBM I Series, i5/OS

IBM System iSeries has double the utilized processing capacity (cores – CPW) available but held in reserve on the refreshed environment to be able to expand during spike periods. Additional costs will not be incurred unless these cores are activated and it won't require a new server to be procured and deployed in order to access that additional processing power.

The IBM System iSeries refreshed environment will have additional cores available for temporary spikes in utilization.

IBM pSeries (Linux, AIX)

For AIX Capacity on Demand, the Unisys Team will use the IBM Flex System hardware platform. With Flex System, capability is also added to share, or over commit, resources on a sliding basis if spikes are experienced by dynamic utilization of resources assigned to other processes, if available for use on a temporary basis. All such 'assignments' will need to be reviewed, confirmed, and approved prior to configuration. IBM System pSeries have additional capacity, cores and memory to meet short term requirements. Infrastructure has been provided, if required, to add more resource for longer term without major changes required. If longer term resources are required, additional costs will apply with requests being submitted via the Enterprise Services Catalog or Change Order.

Mainframe (IBM, Unisys)

Mainframe capacity for the Commonwealth has been highly measured and planned over the

lifecycle of the current contract. The Unisys Team has designed an architecture to support the application requirements with past capacity and processing environment knowledge which are different for agencies which utilize Mainframe MIPS. The Unisys Team will offer Mainframe MIPS capacity via the Enterprise Services Catalog that recognizes the unique processing requirements of the Commonwealth agencies. These include the ability to migrate production and development MIPS from one partition to the other based on current demand.

The Mainframe platforms will provide adequate capacity within the various environments to allow growth should demand require. Increases beyond the initial procured MIPS capacity will be reviewed during Change Management and capacity review meetings and appropriate changes to the environment will be recommended to the Commonwealth for their approval. As part of the service, the Unisys Team provides monthly performance reports and annual capacity planning reports to the Commonwealth which will be utilized to plan for adequate availability of Mainframe MIPS.

IBM Enterprise System zSeries (Mainframe) has 10 times the utilized processing capacity (engines - MIPS) available but held on the refreshed environment to be able to expand during spike periods. Additional costs will not be incurred unless these cores are activated and it won't require a new server to be procured and deployed in order to access that additional processing power.

1.C Offeror must describe its experience operating and managing mixed computing environments such as the Commonwealth.

The Unisys Team manages the infrastructure for several of the agencies in the Commonwealth today, providing mainframe, System I, Windows, Unix, Linux and storage capacity demands. Additionally, the Unisys Team has extensive experience operating and managing complex, mixed computing environments globally. This experience, combined with a common IT Service Management Platform and ITIL V3 aligned processes designed to maximize the capabilities of that platform, allow the Unisys Team to manage a complex environment such as the Commonwealths, while increasing efficiency and bring savings year over year to the Commonwealth.

2 Infrastructure Inventory Approach

2.A Maintain an adequate inventory of Windows/Linux, mid-range, and Mainframe server capacity that will be sufficient to satisfy forecasted informal, ad hoc, and cyclical Commonwealth requests.

Offeror must describe its approach to supporting the needs of the Commonwealth.

Please see the response above to requirement 1 for the Unisys Team's approach to supporting the needs of the Commonwealth.

3 Server Account Management

3.A As a function of ongoing account management, meet with the Commonwealth/Agencies to assess future server requirements.

Offeror must describe its approach to supporting the needs of the Commonwealth.

Unisys Agency Account Managers, Senior Enterprise Infrastructure Architect, and Agency

Infrastructure Architects will meet with the Commonwealth Agencies on a regular basis to understand ongoing business activities and requirements. As part of the quarterly Capacity Review activity, Unisys will use the information from these regular discussions and the Capacity and Performance reports to identify continued growth needs and future server requirements. As additional capacity or server deployments are identified, a service request will be submitted to support the solution development activity and the fulfillment of server deployments to support the Commonwealth's business activities.

For further information on account management and architectural governance, please refer to Schedule F, Section.3.2.1.1.2 and 3.2.1.6.

4 Server Conservation

4.A Encourage Commonwealth server conservation via server virtualization when appropriate. Offeror must describe its approach to supporting the needs of the Commonwealth.

The requirements of this RFP show that the Commonwealth of Pennsylvania is intent upon aggressively moving towards a virtual server landscape. Besides the obvious cost benefit in moving to a virtual environment, there are other tangential benefits for the Commonwealth. Shorter procurement and deployment cycles are such benefits. Another is the creation of an extremely flexible and agile infrastructure, which in itself creates new opportunities for cost reductions beyond what is in the scope of this RFP. However, the realization of these benefits depends on virtualization being adopted as the first choice in server procurement.

The Unisys Team will assist the Commonwealth with server conservation in 3 crucial ways:

1. Server virtualization recommendations
2. Server consolidation recommendations
3. Utilizing Capacity on demand as a tool to assist in capacity optimization

First, the Unisys Team will use the capacity management tools, such as [redacted], to make recommendations to the Commonwealth. As part of the quarterly capacity management reports, Unisys will make recommendations on servers that can quickly be virtualized.

As more servers become virtualized, the Commonwealth runs the risk of virtual server sprawl. To prevent this, the Unisys Team will also make recommendations, based on application information found in the CMDB, to contain the growth of the virtual infrastructure through server and application consolidation. Again, these recommendations will be a part of the quarterly capacity management report.

Last, the Unisys Team will work with the Commonwealth to better utilize Capacity on Demand as a way to conserve servers. The capacity on demand environment utilizes the same hardware platforms as other environments. Because of this, capacity on demand can be utilized as reserve capacity, allowing new applications to be sized to normal operations, and not sized to expected peaks. This same principal applies to unexpected compute demands from legislative mandate. Instead of purchasing new servers that may have a limited life, capacity on demand can be utilized to bring new capacity to applications during cyclical or unexpected peaks.

5 Server Support, expedited

5.A Provide expedited service, when requested, to satisfy urgent requirements.

Offeror must describe its approach to supporting the needs of the Commonwealth.

As stated in the answer above, the capacity on demand environment can be leveraged to bring compute capacity online very rapidly. By choosing specific support tiers when provisioning new compute capacity, the Commonwealth will also, in effect, be provisioning server support capacity on demand. By leveraging the capacity on demand environment as a strategic tool, the Commonwealth can ensure that cyclical or unexpected peaks in compute demand are no longer disruptive events.

6 Server Self Provisioning Tool

6.A Provide a self-provisioning tool to be used by the agencies to order and configure servers.

Offeror must describe its approach to supporting the needs of the Commonwealth.

As part of the solution that Unisys is proposing to the Commonwealth, the application suite mentioned in the answer to requirement 1 above will be made available to the Commonwealth. All server configurations and hardware platforms within schedule I will be available through the Enterprise Services Catalog for self-provisioning. Please refer to requirement 1 above for more details about the Enterprise Services Catalog tools, and the process used to provision compute capacity.

Continual Service Improvement

Unisys recognizes the significant importance of Quality and Continuous Service Improvement to:

16. Reduce service risk,
17. Improve service quality,
18. Improve client satisfaction,
19. Provide service transparency, and
20. Improve/reduce costs of service.

Through a continuous cycle of evaluation and improvement within an IT infrastructure, Unisys views quality and continuous service improvement as a critical success factor in driving customer satisfaction for the Commonwealth IT infrastructure. Each of the continuous service improvement areas identified above are driven through the tight integration of the following organizations, industry tools, proven processes and quality deliverables:

22. Service Excellence Office,
23. Quality Plans: transition and steady state service delivery
24. Industry standard frameworks and methodologies: ITIL, ISO, SSL

25. Industry accepted measurement tools
26. Continuous Service Improvement & Innovation Processes (CSIIP)
27. Risk management, audits and business continuity management
28. Client Satisfaction Surveys and Knowledge Management Portal

Collectively this represents Unisys Integrated Quality Plan for the Commonwealth of Pennsylvania.

Specifics on each of these areas are outlined in Schedule F, Section 3.2.1.1.6 Continuous Service Improvement. Highlights from this section are outlined below and requested service examples are provided at the end of this section.

7 CI Service Risk

7.A Reduce service risks.

Offeror must describe its approach and provide examples of previous Offeror initiatives aimed at eliminating or mitigating service risks.

Risk management, independent quality audits, and business continuity management are integral quality management processes. Unisys is committed to managing risks and facilitating the achievement of business objectives the adherence to quality processes. We mitigate risk through the implementation of tight quality controls: standard policies, procedures, roles, risk assumptions, issues, and definitions, etc.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

8 CI Service Quality

8.A Improve service quality.

Offeror must describe its approach and provide examples of previous Offeror initiatives aimed at improving service quality.

The quality approach begins with the Service Excellence Office who provides definition and oversight of all ITIL process management and analysis functions. Process managers and analysts working in the Service Excellence Office are responsible for auditing process effectiveness, ensuring that service delivery teams comply with proper execution of processes, and analyzing process trends for anomalies. Continuous service improvement programs in collaboration with Commonwealth agencies are managed by the Service Excellence Office.

Through our Continuous Service Improvement and Innovation Process (CSIIP), the SEO reviews, analyzes and makes recommendations on improvement opportunities in each ITIL lifecycle phase. Unisys will leverage Six Sigma Lean tools and methodologies as well as ISO Certified internal audits to measure and maintain the highest quality services to the Commonwealth.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

9 CI Client Satisfaction

9.A Improve client satisfaction.

Offeror must provide examples of previous Offeror initiatives aimed at continually improving client satisfaction.

Client satisfaction is extremely important to Unisys and a key focus in our IT solution. The SEO will integrate new agencies, customers and services into our multi-pronged client satisfaction approach that includes Service Desk surveys on the caller's experience, an overall agency satisfaction survey, and quarterly surveys with the Office of Administration. Data collection will be gathered across multiple levels to gain a clear understanding of the Commonwealth's satisfaction with the IT Services being provided.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

10 CI Service Transparency

10.A Provide service transparency.

Offeror must describe its approach and provide examples of previous Offeror initiatives aimed at providing service transparency; in particular, visibility into the service execution process.

The service organizations will use standardized ITSM services processes, IT monitoring and automation tools. ITSM processes will be documented in the Commonwealth Computing Procedures Manual (CCPM). The CCPM will be available to Commonwealth approved staff on the Knowledge Management Portal (KMP) providing desired transparency into service execution processes. Through the Real-time Dashboard, the Commonwealth will have access to current operational performance of their application infrastructure.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

11 CI Service Sustainability

11.A Ensure service sustainability.

Offeror must describe its approach and provide examples of previous Offeror initiatives aimed at ensuring service sustainability; in particular, efforts targeted at cost containment and cost reductions.

Service will be sustained by integrating any new agencies, customers, or services into our standard operational and quality processes and methodologies. We leverage ITIL processes, create quality project plans, utilize industry accepted measurement and monitoring tools, analyze trending reports and provide proactive continuous service improvement throughout the IT lifecycle. This enables new Commonwealth services to experience and sustain IT services and client satisfaction.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

12 CI Improve or Reduce Cost

12.A Improve/reduce cost of service.

Offeror must provide examples of On-Demand Server initiatives that have been implemented or can be utilized to achieve reduced costs of Services and to meet or exceeded ROI (Return on Investment) analysis projections.

The Service Excellence Office will proactively manage quality, continuous service improvement, ITIL process management, and customer satisfaction through a comprehensive quality plan that specifically addresses all of these areas. We believe this is a key differentiator in our partnership with the Commonwealth. Through this new organization and these quality plans, Unisys will drive best in class services and the highest customer satisfaction experience, while reducing overall costs to the Commonwealth.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

Unisys Team experience paragraph below details the example of On-Demand Server initiatives.

Unisys Team Experience

California State University was faced with the impact of the California Budget Crisis resulting in the need to reduce IT spend and yet, demonstrate continuous improvement in service delivery. This included reassessing IT support to use emerging technologies and ensuring their IT Infrastructure would support their aggressive software roadmap. The Unisys Team provided Cloud services (server/storage) across hardware platforms with flexibility to scale up/down to handle campus registration peaks, year –end processing cycles and Disaster Recovery. The result gave the California State University system the ability to handle the demand of academic semester/quarterly course scheduling peaks throughout the year with a flexible cost model. It also enabled improvement in Disaster Recovery through building images vs. servers, thus reducing RPO and RTO objectives.

The Unisys Team assigned to the Commonwealth account has also previously demonstrated its ability to deliver a capacity on demand infrastructure, including self-provisioning, to the Commonwealth. Post contract signing, the team that performed the previous work will be assigned to assist in the development and deployment of the new infrastructure on demand environment, to confirm that all lessons learned will be carried forward. This team is intimately familiar with the needs of the Commonwealth, and how to design and run a capacity on demand system in a multi-tenant, highly regulated governmental atmosphere. This represents a significant reduction of risk to the Commonwealth, both technically in design and speed to deployment, and from a regulatory perspective.

Benefits to the Commonwealth

The Unisys Team's capacity on demand solution delivers to the Commonwealth a powerful, agile and responsive tool that can be leveraged to address unexpected needs for compute resources due to unexpected or cyclical peaks in compute resource demand. It will allow the Commonwealth to right size compute resources for their application, provision for average load (not peak loads) and rely on capacity on demand to fill in the gap. In a disaster it's a tool that

can used to quickly spin up excess capacity and bring applications back online quickly.

3.2.5.2 Storage Capacity on Demand

The Storage Capacity On Demand service is an Infrastructure as a Service (IaaS) offering that ensures the ready availability of storage capacity to accommodate cyclical, or seasonal, storage requirements, sudden or unplanned production demands, short-term application development needs, and storage access for web enabled devices.

Reference Documentation

N/A

Requirements		Describe Compliance
1.	Maintain an adequate access to, or supply of storage area equipment, to satisfy forecasted informal, ad hoc, and cyclical Commonwealth requests.	Offeror must describe its approach to supporting the needs of the Commonwealth including the following: • Infrastructure/Capacity • Tiered Service/Support Levels • Tools / Applications to manage and maintain capacity • End User Reports o Standard o Custom
2.	Meet with the Commonwealth on an annual basis, or as requested, to assess future storage requirements.	Offeror must describe its approach to supporting the needs of the Commonwealth.
3.	Encourage data storage conservation via data de-duplication, compression, and other industry techniques.	Offeror must describe its approach to supporting the needs of the Commonwealth.
4.	Provide expedited data storage service to satisfy urgent requirements, as requested.	Offeror must describe its approach to supporting the needs of the Commonwealth.
5.	Provide online storage capabilities (Centralized Private Cloud Storage), which includes web service, browser, and mobile device accessibility, that	Offeror must describe its approach to supporting the needs of the Commonwealth.

	are fully secure, (compliant with ISO 27000, NIST 800-53, and Secure SDLC). This service must provide file-level encryption, multiple hierarchical permission levels, account level dynamic storage-sizing, and anti-virus capability.	
6.	Storage solution must include the capability to make quick copies of databases (SNAPS, Flash copies). Storage backup proposals must include disk-2-disk solutions.	Offeror must describe its approach to supporting the needs of the Commonwealth.
Continual Service Improvement		
7.	Reduce service risks.	Offeror must describe its approach and provide examples of previous Offeror initiatives aimed at eliminating or mitigating service risks.
8.	Improve service quality.	Offeror must describe its approach and provide examples of previous Offeror initiatives aimed at improving service quality.
9.	Improve client satisfaction.	Offeror must provide examples of previous Offeror initiatives aimed at continually improving client satisfaction.
10.	Provide service transparency.	Offeror must describe its approach and provide examples of previous Offeror initiatives aimed at providing service transparency; in particular, visibility into the service execution process.
11.	Ensure service sustainability.	Offeror must describe its approach and provide examples of previous Offeror initiatives aimed at ensuring service sustainability; in particular, efforts targeted at cost containment and cost reductions.

12.	Improve/reduce cost of service.	Offeror must provide examples of On-Demand Storage initiatives that have been implemented or can be utilized to achieve reduced costs of Services and to meet or exceeded ROI (Return on Investment) analysis projections.

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

Introduction

The Commonwealth seeks a comprehensive strategy for dealing with the cyclical demands of capacity by utilizing a strategy of capacity on demand. The value to the Commonwealth in pursuing such a strategy is readily apparent, from both a technical and financial perspective. Financially, a capacity on demand strategy shifts the Commonwealth from a mixture of Capital Expense\Operational Expense, to a more predictable Operational Expense. This type of strategy obviates the need for large capital expenditures for the upgrade and maintenance of compute power on disparate compute platforms, and smoothes the spikes in compute demand caused by cyclical and unforeseen events.

The Commonwealth has asked for a clear definition of how the processes and tools will be utilized in the capacity on demand environment. Unisys has developed a comprehensive strategy in the design of the Storage Capacity on Demand infrastructure, by utilizing best of breed hardware and software components that will deliver to the Commonwealth a storage infrastructure that will meet the demands of the current workloads, as well as provide the flexibility to move the Commonwealth into the future.

1 Data Storage Capacity Approach

1.A Maintain an adequate access to, or supply of storage area equipment, to satisfy forecasted informal, ad hoc, and cyclical Commonwealth requests.

The Unisys Team's strategy of providing Config1, Config2, and Config3 storage tiers within the same frame makes it easier to maintain an adequate supply of equipment to meet informal forecasts, ad hoc, and cyclical capacity needs.

The request and provisioning process for each of the anticipated platforms are as follows:

1. The Commonwealth User (user) will log onto the Service Delivery Portal, and select the Enterprise Services Catalog.
2. The Enterprise Services Catalog tool will authenticate and authorize the user
3. Based on what the user is authorized to do, they will be able to select the appropriate

Storage Tier from the following:

a. Technology Platform:

i. P Series (AIX/Linux)

- X86 (Windows/Linux)
- IBM I Series
- IBM Mainframe
- Unisys Mainframe

b. Server Configuration – CPU, Memory, Disk space, etc.

c. Service Tier – Platinum, Gold, Silver, Bronze, Basic

d. Storage Tier – Config1,Config2, and Config3

4. The Enterprise Services Catalog tool's workflow engine will then handle all authorizations for the provisioning.
5. Once approved, the Enterprise Services Catalog tool will open all change records needed to provision the requested storage.
6. Once the change record is approved, the Enterprise Services Catalog Tool will run an automated run book for each platform that will provision the storage.
7. Post provisioning, the Enterprise Services Catalog tool will call [redacted] to perform system patching, security remediation and server conditioning (initial creation of accounts, permissions, etc.)
8. The Enterprise Services Catalog tool will then register the new service in the following tools:
   a. [redacted]
   b. [redacted]
   c. [redacted]
9. Once all provisioning tasks have been performed, the Enterprise Services Catalog tool will notify the user that it's service request has been provisioned and is ready for use.

1.B Offeror must describe its approach to supporting the needs of the Commonwealth including the following:

Infrastructure/Capacity

Tiered Service/Support Levels

Tools / Applications to manage and maintain capacity

End User Reports (Standard and Custom)

Infrastructure/Capacity

Inherent in the design of the infrastructure is the ability to utilize extremely small units of growth in all infrastructure components. By utilizing the IBM and EMC storage products as the platforms of choice for storage, additional capacity in both network and compute can be ordered and brought online very quickly. All hardware platforms will follow a stringent

capacity management and optimization process with well-defined triggers for adding capacity to provide future capacity demands are properly planned for and brought online before needed. This provides the Commonwealth a highly optimized, flexible and highly automated infrastructure that will smooth demand spikes and ease the last minute budgetary demands for storage capacity.

Tiered Service/Support Levels

The storage capacity-on-demand will be broken out to show the 3 tiers of storage requested by the Commonwealth. These reports will also show the expected capacity provided by the backup to disk infrastructure and the snapshotting and ready-copy disk infrastructure.

Tools / Applications to manage and maintain capacity

Utilizing the structure found in the Volumetrics tab of Schedule I, an enterprise services catalog will be developed that will enable the Commonwealth to order compute capacity online. The enterprise services catalog will serve two functions: the first as a central location from which the Commonwealth can order common services from Unisys. The second, more pertinent function is to serve as the central point from which compute capacity can be ordered. Capacity can be both provisioned and de-provisioned from this portion of the Enterprise Services Catalog.

The Enterprise Services Catalog includes the following components:

a. iCollaborate, a web-based front end that functions as the entry point into the Enterprise Services Catalog. iCollaborate performs all authentication, authorization and role adjudication functionality based on integration with the Commonwealths Active Directory service.

b. iRequest, the Enterprise Services Catalog component. For the Commonwealth, the Enterprise Services Catalog will allow the user to specify what type of compute platform is required, what size server or LPAR is needed, and lastly the support tier for the servers being ordered.

c. iDeliver, a complete workflow automation engine. The iDeliver component interfaces via API directly to the [redacted], [redacted] [redacted] [redacted] v[redacted]. The iDeliver component will coordinate all change and request management processes, and where automated server provisioning is support, drive the build of the server environment.

The Enterprise Services Catalog also includes data for chargeback as well as online reporting for utilization, provisioning and de-provisioning.

The following tables lists the other components of the common IT service delivery platform that will be leveraged to deliver automated provisioning to the Commonwealth.

Tool	Function
[redacted]	• Services Catalog • Workflow automation

[redacted]	• Change Management • Incident Management
[redacted]	• Configuration Management Database
[redacted]	• Atrium Discovery and Dependency Mapping • Update of CMDB
[redacted]	• Enterprise Capacity Management across all servers, network and storage devices • Workload Management and visualization
[redacted]	• Provisioning Engine • Provides post provisioning storage conditioning • Patch management and security compliance.
[redacted]	• Monitors StorageOperation • Opens automated tickets in Incident management.

End User Reports

Standard

Standard Reports are summarized in 3.3.2.

Custom Reports are offered by the Unisys Team as a Catalog Service

Custom

Please see the answer to 1.A above for the process that supports the capability of Commonwealth users to provision server resource capacity. This process is delivered via the Enterprise Services Catalog tool detailed above in this section.

2 Data Storage, Annual Data Storage Requirement Meetings

2.A Meet with the Commonwealth on a annual basis, or as requested, to assess future storage requirements.

Offeror must describe its approach to supporting the needs of the Commonwealth.

The Commonwealth seeks at least annual meetings to review capacity and forecasts. The Unisys Program Management Office will establish regularly scheduled meetings to review these metrics. The Unisys Service Delivery Manager will also have ready access to detailed forecasts and will be prepared to meet monthly if this better suites the OA.

Storage capacity and on-demand environment requires a very vigorous capacity management regimen that must include future and cyclical capacity needs calculations factors such as historical utilization, future growth plans as they are developed, as well as the velocity of

changes to the environment. With these factors in mind, the environment is designed to be extremely flexible, allowing additional compute capacity can be added by needed. By utilizing a common pair of EMC and IBM storage platforms for physical and virtual servers, released storage capacity can be rapidly redeployed as needed to smooth unexpected surges in capacity.

The IBM and Unisys Mainframes are also provisioned to the IBM and EMC storage platforms and will benefit from flexible capacity provisioning although, traditionally, these platforms are less likely to have opportunities to take advantage of ad hoc storage provisioning.

3 Data Storage Conservation

3.A Encourage data storage conservation via data de-duplication, compression, and other industry techniques.

Offeror must describe its approach to supporting the needs of the Commonwealth.

The Commonwealth seeks industry-standard techniques to reduce storage costs. Unisys will provide disk deduplication as part of the Enterprise Services Catalog offering. Unisys proposes that in addition to the regular forecast meetings the Capacity Manager will review storage growth rates that exceed forecasts and report back on drivers for accelerated growth within agencies as well as review drivers for the growth with an eye toward landing less used data to more cost effective storage.

4 Data Storage Expedited

4.A Provide expedited data storage service to satisfy urgent requirements, as requested.

Offeror must describe its approach to supporting the needs of the Commonwealth.

As stated in the answer above, the capacity on demand environment can be leveraged to bring storage capacity online very rapidly. By choosing specific support tiers when provisioning new compute capacity, the Commonwealth will also, in effect, be provisioning storage support capacity on demand. By leveraging the capacity on demand environment as a strategic tool, the Commonwealth can confirm that cyclical or unexpected peaks in compute demand are no longer disruptive events.

5 Portal, Data Storage online Portal Capabilities Approach

5.A Provide online storage capabilities (Centralized Private Cloud Storage), which includes web service, browser, and mobile device accessibility, that are fully secure, (compliant with ISO 27000, NIST 800-53, and Secure SDLC). This service must provide file-level encryption, multiple hierarchical permission levels, account level dynamic storage-sizing, and anti-virus capability.

Offeror must describe its approach to supporting the needs of the Commonwealth.

The Commonwealth seeks Secure Centralized Private Cloud Services with server and mobile device accessibility. Unisys will provide these storage services. The complexity of the security features including hierarchy levels will be provided through server-based security systems. This will allow the Commonwealth to selectively choose where to invest higher costs to protect data according to just the applicable security policies rather than impose this cost on all data. Likewise anti-virus will be provided by host-based software but in the case of virus protection all data visible to servers, browsers and mobile devices will have virus protection.

Through the Catalog of Services the Commonwealth will also have access to the Unisys Stealth Solution™ which renders users, data, and infrastructure undetectable to cyber criminals. Built to meet requirements of the U.S. Department of Defense to help secure sensitive information, Unisys Stealth achieved the National Security Agency's National Information Assurance Partnership Common Criteria EAL-4+ certification, protecting data-in-motion across any network regardless if it is private or public.

Benefits of Unisys Stealth Solution

- Render data, users, and your data center dark to the outside world
- Securely protect the user, network, and data center
- Unprecedented security without an expensive reconfiguring of the network

6 Data Storage Copy Approach

6.A Offeror must describe its approach to supporting the needs of the Commonwealth.

Storage solution must include the capability to make quick copies of databases (SNAPS, Flash copies).

The snapshotting feature in the IBM and EMC toolsets creates point-in-time data copies that can be used for data backups, software development and testing, repurposing, data validation, and local rapid restores.

EMC VNX snapshots write new data to a new area within the storage pool without the need to read and write the old data block. This is accomplished with the "redirect on write" (ROW) technology so that a new snapshot does not require a read of the existing LUN.

The IBM SVC offers snapshotting as an interoperable feature that can work across all storage frames.

6.B Storage backup proposals must include disk-2-disk solutions.

The storage features sought by the Commonwealth will be provided by a variety of storage tools including frame-based copy tools such as the EMC RecoverPoint, the EMC VPLEX suite, and the IBM SVC tool suite. The Unisys Team, consisting of both EMC and IBM expert-level storage architects, already has experience within the Commonwealth, proposes this best-of-best interoperable solution.

In order to reduce overall costs, Snapshotting and copy features will be available for selection from the Enterprise Services Catalog rather than applied to all SAN-based storage volumes requested in the Schedule I Volumetrics.

Continual Service Improvement

The Quality Plan begins with the Service Excellence Office (SEO) within the Program Management Office. The SEO function provides definition and oversight of all ITIL process management and analysis functions including Change Management, Release Management, Incident Management, Problem Management, Asset Management, Configuration and CMDB Management, Availability Management, and Service Level Management. Process Managers and Analysts working in the Service Excellence Office are responsible for auditing process

effectiveness, ensuring that service delivery teams comply with proper execution of processes, and analyzing process trends for anomalies. Continuous Service Improvement programs in collaboration with Commonwealth agencies are managed by the Service Excellence Office.

The SEO manages and drives Quality across the Commonwealth's multi-dimensional, complex, and matrixed IT Service Delivery Organizations. The SEO standardizes Quality across COPA Agencies, Unisys, Partner Organizations, as well as across all ITIL IT Services Processes, IT Monitoring & Automation Tools, and Client Satisfaction surveys and processes. Unisys will leverage the ITIL Framework, ISO Certifications, Six Sigma Lean Tools, and our Continuous Service Improvement & Innovation Process (CSIIP) to proactively provide the highest quality IT services are being provided.

The SEO leverages the ITIL framework in delivering IT Service Management. Industry accepted Measurement Tools such as [redacted] The Unisys Capacity Management team can automatically identify under-utilized or over-utilized servers; accurately plan, implement, and manage the Commonwealth's virtualization and cloud computing initiatives; and continuously optimize supporting data center resources. Unisys can integrate performance metrics related to any IT resource (such as physical and virtual servers, databases, middleware, storage, networks, and facilities) or business service. These tools will be the foundation for establishing baselines, performance , capacity, trending, and SLA/SLO reporting for Capacity Management. These tools and reports will also provide excellent visibility and services transparency to the Commonwealth.

Continual Service Improvement

Unisys recognizes the significant importance of Quality and Continuous Service Improvement to:

21. Reduce service risk,
22. Improve service quality,
23. Improve client satisfaction,
24. Provide service transparency, and
25. Improve/reduce costs of service.

Through a continuous cycle of evaluation and improvement within an IT infrastructure, Unisys views quality and continuous service improvement as a critical success factor in driving customer satisfaction for the Commonwealth IT infrastructure. Each of the continuous service improvement areas identified above are driven through the tight integration of the following organizations, industry tools, proven processes and quality deliverables:

29. Service Excellence Office,
30. Quality Plans: transition and steady state service delivery
31. Industry standard frameworks and methodologies: ITIL, ISO, SSL
32. Industry accepted measurement tools

33. Continuous Service Improvement & Innovation Processes (CSIIP)
34. Risk management, audits and business continuity management
35. Client Satisfaction Surveys and Knowledge Management Portal

Collectively this represents Unisys Integrated Quality Plan for the Commonwealth of Pennsylvania.

Specifics on each of these areas are outlined in Schedule F, Section Continuous Service Improvement. Highlights from this section are outlined below and requested service examples are provided at the end of this section.

7 CI Service Risk

7.A Reduce service risks.

Offeror must describe its approach and provide examples of previous Offeror initiatives aimed at eliminating or mitigating service risks.

Risk management, independent quality audits, and business continuity management are integral quality management processes. Unisys is committed to managing risks and facilitating the achievement of business objectives the adherence to quality processes. We mitigate risk through the implementation of tight quality controls: standard policies, procedures, roles, risk assumptions, issues, and definitions, etc.

Please refer to Schedule F, Section Continuous Service Improvement for additional details in this area.

8 CI Service Quality

8.A Improve service quality.

Offeror must describe its approach and provide examples of previous Offeror initiatives aimed at improving service quality.

The quality approach begins with the Service Excellence Office who provides definition and oversight of all ITIL process management and analysis functions. Process managers and analysts working in the Service Excellence Office are responsible for auditing process effectiveness, ensuring that service delivery teams comply with proper execution of processes, and analyzing process trends for anomalies. Continuous service improvement programs in collaboration with Commonwealth agencies are managed by the Service Excellence Office.

Through our Continuous Service Improvement and Innovation Process (CSIIP), the SEO reviews, analyzes and makes recommendations on improvement opportunities in each ITIL lifecycle phase. Unisys will leverage Six Sigma Lean tools and methodologies as well as ISO Certified internal audits to measure and maintain the highest quality services to the Commonwealth.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

9 CI Client Satisfaction

9.A Improve client satisfaction.

Offeror must provide examples of previous Offeror initiatives aimed at continually improving client satisfaction.

Client satisfaction is extremely important to Unisys and a key focus in our IT solution. The SEO will integrate new agencies, customers and services into our multi-pronged client satisfaction approach that includes Service Desk surveys on the caller's experience, an overall agency satisfaction survey, and quarterly surveys with the Office of Administration. Data collection will be gathered across multiple levels to gain a clear understanding of the Commonwealth's satisfaction with the IT Services being provided.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

10 CI Service Transparancy

10.A Provide service transparency.

Offeror must describe its approach and provide examples of previous Offeror initiatives aimed at providing service transparency; in particular, visibility into the service execution process.

The service organizations will use standardized ITSM services processes, IT monitoring and automation tools. ITSM processes will be documented in the Commonwealth Computing Procedures Manual (CCPM). The CCPM will be available to Commonwealth approved staff on the Knowledge Management Portal (KMP) providing desired transparency into service execution processes. Through the Real-time Dashboard, the Commonwealth will have access to current operational performance of their application infrastructure.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

11 CI Service Sustainability

11.A Ensure service sustainability.

Offeror must describe its approach and provide examples of previous Offeror initiatives aimed at ensuring service sustainability; in particular, efforts targeted at cost containment and cost reductions.

Service will be sustained by integrating any new agencies, customers, or services into our standard operational and quality processes and methodologies. We leverage ITIL processes, create quality project plans, utilize industry accepted measurement and monitoring tools, analyze trending reports and provide proactive continuous service improvement throughout the IT lifecycle. This enables new Commonwealth services to experience and sustain IT services and client satisfaction.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

12 CI Improve or Reduce Cost

12.A Improve/reduce cost of service.

Offeror must provide examples of On-Demand Storage initiatives that have been implemented or can be utilized to achieve reduced costs of Services and to meet or exceeded ROI (Return on Investment) analysis projections.

The Service Excellence Office will proactively manage quality, continuous service improvement, ITIL process management, and customer satisfaction through a comprehensive quality plan that specifically addresses all of these areas. We believe this is a key differentiator in our partnership with the Commonwealth. Through this new organization and these quality plans, Unisys will drive best in class services and the highest customer satisfaction experience, while reducing overall costs to the Commonwealth.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

Unisys examples of continuous improvement

Examples of continuous service improvement have been included below under Unisys Team Experience.

Unisys Team Experience

Unisys Storage Resource Analysis (SRA) and Backup and Recovery Service (RBS) provide multiple ways to rein in storage and backup costs and are offered as a standard Unisys product in the market as well as to Unisys existing customers.

Federal IT managers know that analyzing and benchmarking storage and backup environments is a critical first step in deciding what to do about their agency's persistent data growth. But, the analysis has been difficult to execute in an accurate, unbiased and timely manner. For example:

- An in-house analysis often takes weeks of effort and involves cobbled solutions that rely upon spread sheets for reporting
- Vendors of storage solutions produce tools that analyze their hardware but not others
- Staff reports often sugar-coat deficiencies

The risk of not performing a storage analysis or back-up assessment is significant and results in:

- Operational instability
- Unreliable continuity of operations (COOP) plans
- Significant budgetary shortfalls
- Unplanned storage acquisitions

Knowing the importance of analyzing and benchmarking an agency's storage and back-up environment, Unisys created a suite of storage and back-up services. These services combine the tools and expert consulting required to deliver essential information to federal IT managers in an accurate, unbiased and timely manner.

Services Description

Unisys Storage Resource Analysis (SRA) and Backup and Recovery Service (RBS) provide multiple ways to rein in storage and backup costs:

- Optimize existing storage to improve utilization
- Save costs by retiring inefficient assets
- Reclaim orphaned storage
- Decrease complexity to improve reliability
- Expedite backups and recovery
- Identify points of failure

While the list of options to rein in costs are as different as each agency; the benefits are consistent:

- Transparency into your storage and backup environment
- Confidence to make changes knowing immediate and long-term impact
- Performance improvements of storage and backup
- Savings through well-planned storage acquisitions
- Ability to charge back users of storage
- Reduction in energy costs
- Operational stability

Benefits to the Commonwealth

The Commonwealth seeks cost-savings through a storage-as-a-service model. These are similar to the requirements put forward by the Internal Revenue Service.

The Internal Revenue Service was well-aware of Unisys expertise in storage management when, in 2012, it awarded the Enterprise Storage Acquisition task order to provide private cloud-based storage for the agency's information records.

This task order, awarded against GSA's Alliant Government-wide Acquisition Contract, has a one-year base period and nine one-year options and is potentially worth up to $139 million over 10 years, if all options are exercised. It includes pricing for each year based on the IRS's estimate of its storage requirements.

Under the task order, Unisys will initially acquire storage assets now owned and managed by IRS and will manage the more than 7.5 petabytes of storage space currently in multiple IRS data centers and facilities. Unisys will then plan, build, deploy and maintain a new IRS storage environment, transitioning those assets to a private cloud-based storage-as-a-service model in which the agency will pay for storage capacity as needed.

Under the task order, the IRS will pay only for the amount of storage it needs when it is needed, instead of purchasing storage equipment necessary to meet its peak demands.

"The IRS Enterprise Storage Acquisition program demonstrates how global best practices and

innovative approaches can bring significant cost savings to the US federal government and to taxpayers," says Ted Davies, president of Unisys Federal Systems. "As agencies look to achieve more within tightened budget constraints, we expect to see more agencies following the lead of the IRS."

3.2.5.3 DR Infrastructure on Demand

The DR Infrastructure On Demand service is an infrastructure as a service (IaaS) offering that ensures the ready availability of DR infrastructure; servers, storage systems, networking capabilities, etc. This infrastructure will enable Commonwealth datacenters to recover critical business applications and data in the event of a disaster.

Reference Documentation

N/A

Requirements		Describe Compliance
•	Maintain an adequate inventory of servers, storage systems, and networking capacity sufficient to satisfy forecasted informal, ad hoc, and cyclical Commonwealth requests.	Offeror must describe its approach to supporting the needs of the Commonwealth including the following: • Processes and procedures for developing and testing DR Plans • Capacity (servers, storage, etc.) • Tiered Service/Support Levels • Tools / Applications to manage and maintain capacity • End User Reports o Standard o Custom
•	Meet with the Commonwealth on a annual basis and as requested to assess its future DR requirements.	Offeror must describe its approach to supporting the needs of the Commonwealth.

•	Revise datacenter and disaster recovery plans, upon request of the Commonwealth.	Offeror must describe its approach to supporting the needs of the Commonwealth.
•	Provide support for the Commonwealth with identifying and establishing DR or Continuity of Government (CoG) capabilities and plans.	Offeror must describe its approach to supporting the needs of the Commonwealth.
Continual Process Improvement		
•	Reduce service risks.	Offeror must describe its process and provide examples of previous Offeror initiatives aimed at eliminating or mitigating service risks.
•	Improve service quality.	Offeror must describe its process and provide examples of previous Offeror initiatives aimed at improving service quality.
•	Improve client satisfaction.	Offeror must provide examples of previous Offeror initiatives aimed at continually improving client satisfaction.
•	Provide service transparency, in particular, visibility into the service execution process.	Offeror must describe its process and provide examples of previous Offeror initiatives aimed at providing service transparency.
•	Ensure service sustainability, in particular, efforts targeted at cost containment and cost reductions.	Offeror must describe its process and provide examples of previous Offeror initiatives aimed at ensuring service sustainability.
•	Improve/reduce cost of service.	Offeror must provide examples of On-Demand Infrastructure initiatives that have been implemented or can be utilized to achieve reduced costs of Services and to meet or exceeded ROI (Return on Investment) analysis projections.

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

Introduction

The Commonwealth seeks a comprehensive strategy for dealing with the cyclical demands of capacity by utilizing a strategy of capacity on demand. The value to the Commonwealth in pursuing such a strategy is readily apparent, from both a technical and financial perspective. Financially, a capacity on demand strategy shifts the Commonwealth from a mixture of Capital Expense and Operational Expense, to a more predictable Operational Expense. This type of strategy obviates the need for large capital expenditures for the upgrade and maintenance of compute power on disparate compute platforms, and smoothes the spikes in compute demand caused by cyclical and unforeseen events.

The Commonwealth has asked for a clear definition of the processes tools will be utilized in the capacity on demand environment. Unisys has developed a comprehensive strategy in the design of the Disaster Recovery on Demand infrastructure, by utilizing the same infrastructure options offered in the Storage on Demand and Server on Demand offerings. These best of breed hardware and software components will deliver to the Commonwealth a DR compute infrastructure that will meet the demands of the current workloads, as well as provide the flexibility to move the Commonwealth into the future.

The Unisys solution provides the Commonwealth with an Enterprise Services Catalog to provide DR Infrastructure on Demand and allows the Commonwealth to grow and expand the Disaster Recovery infrastructure to match the infrastructure capacity provided to critical production applications. The Enterprise Services Catalog is sufficiently granular to allow the Commonwealth to limit Disaster Recovery costs by, for instance, electing to provision only 80% of the Production compute capacity at the Disaster Recovery site. In this way the Commonwealth to purchase disaster compute capacity in appropriate quantities to meet but not exceed the risk threats.

1 DR Infrastructure on Demand

1.A Maintain an adequate inventory of servers, storage systems, and networking capacity sufficient to satisfy forecasted informal, ad hoc, and cyclical Commonwealth requests.

The incremental capacity is supported in the same fashion as the other Infrastructure on Demand components including servers, storage and network.

The details of this provisioning process are described in these Capacity on Demand Sections:

- Schedule F, Section 3.2.5 - Capacity on Demand Services
- Schedule F, Section 3.2.5.1 - Server Capacity on Demand Approach
- Schedule F, Section 3.2.5.2 - Storage Capacity on Demand

1.B Offeror must describe its approach to supporting the needs of the Commonwealth including the following:

Processes and procedures for developing and testing DR Plans

Capacity (servers, storage, etc.)

Tiered Service/Support Levels

Tools / Applications to manage and maintain capacity

End User Reports

The Unisys solution manages DR services within the Infrastructure Architecture framework described in F.3.2.2.2 (Infrastructure Architecture).

The DR Infrastructure on Demand is provided through the selection of required components and services in the Enterprise Services Catalog including granular services to improve DR services for specific data components.

Testing of DR plans is also provided in the Enterprise Services Catalog. The Unisys solution provides the means for Agencies to conduct tests 2 times per year as specified by the Commonwealth but Agencies can also elect to select tests for only once per year if they wish to manage costs for this effort.

The available Capacity, Tiered Service Levels, Tools, and End User Reports are described in detail in Schedule F, Section 1 of 3.2.3.2 (Site Operations)

2 DR, Annual Requirements Assessment Meetings

2.A Meet with the Commonwealth on a annual basis and as requested to assess its future DR requirements.

Offeror must describe its approach to supporting the needs of the Commonwealth.

The Unisys solution provides a IT Risk Manager who has responsibility for maintaining DR plans, and providing reviews and remediation recommendations for the Commonwealth Agencies on an annual basis. These meetings, following testing, provide the opportunity to assess current DR services to the changing needs of critical applications and related risks.

The Commonwealth benefits of reviews and planning for DR within DPH. Unisys has strived to meet and exceed the SLAs for Recovery Time Objectives with each test. The broadened scope of DR testing for agencies in the Unisys-managed data centers allows the Unisys DR team to increase opportunities to test and improve upon DR SLAs. The prior year's test provides the DR team with "lessons learned" even as it achieves existing SLAs. These become the basis for the revisions and improvements to the next test.

3 DR, Disaster Recovery Plan Updates

3.A Revise datacenter and disaster recovery plans, upon request of the Commonwealth.

Offeror must describe its approach to supporting the needs of the Commonwealth.

The Commonwealth will meet with the Unisys IT Risk Manager in the Program Management Office to review the progress of regular Agency-based meetings regularly scheduled by the CO to review and revise plans. The IT Risk Manager works with each Agency to incorporate their

existing DR plans into the online Living Disaster Recovery Planning System (LDRPS) tool set. The tool not only provides a means for accessing DR plans should a disaster actually occur, it also becomes a central repository for plan guides and artifacts which can be managed centrally.

Unisys uses this tool to provide the OA with a cross-Agency survey of plan offerings.

4 DR and CoG Planning Approach

4.A Provide support for the Commonwealth with identifying and establishing DR or Continuity of Government (CoG) capabilities and plans.

Offeror must describe its approach to supporting the needs of the Commonwealth.

The Unisys IT Risk Manager will support the Commonwealth with identifying and establishing DR and CoG capabilities and plans.

Continual Service Improvement

Unisys recognizes the significant importance of Quality and Continuous Service Improvement to:

1. Reduce service risk,
2. Improve service quality,
3. Improve client satisfaction,
4. Provide service transparency, and
5. Improve/reduce costs of service.

Through a continuous cycle of evaluation and improvement within an IT infrastructure, Unisys views quality and continuous service improvement as a critical success factor in driving customer satisfaction for the Commonwealth IT infrastructure. Each of the continuous service improvement areas identified above are driven through the tight integration of the following organizations, industry tools, proven processes and quality deliverables:

1. Service Excellence Office,
2. Quality Plans: transition and steady state service delivery
3. Industry standard frameworks and methodologies: ITIL, ISO, SSL
4. Industry accepted measurement tools
5. Continuous Service Improvement & Innovation Processes (CSIIP)
6. Risk management, audits and business continuity management
7. Client Satisfaction Surveys and Knowledge Management Portal

Collectively this represents Unisys Integrated Quality Plan for the Commonwealth of Pennsylvania.

Specifics on each of these areas are outlined in Schedule F, Section 3.2.1.1.6 Continuous Service

Improvement. Highlights from this section are outlined below and requested service examples are provided at the end of this section.

5 CI Service Risk

5.A Reduce service risks.

Offeror must describe its process and provide examples of previous Offeror initiatives aimed at eliminating or mitigating service risks.

Risk management, independent quality audits, and business continuity management are integral quality management processes. Unisys is committed to managing risks and facilitating the achievement of business objectives the adherence to quality processes. We mitigate risk through the implementation of tight quality controls: standard policies, procedures, roles, risk assumptions, issues, and definitions, etc.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

6 CI Service Quality

6.A Improve service quality.

Offeror must describe its process and provide examples of previous Offeror initiatives aimed at improving service quality.

The quality approach begins with the Service Excellence Office who provides definition and oversight of all ITIL process management and analysis functions. Process managers and analysts working in the Service Excellence Office are responsible for auditing process effectiveness, ensuring that service delivery teams comply with proper execution of processes, and analyzing process trends for anomalies. Continuous service improvement programs in collaboration with Commonwealth agencies are managed by the Service Excellence Office.

Through our Continuous Service Improvement and Innovation Process (CSIIP), the SEO reviews, analyzes and makes recommendations on improvement opportunities in each ITIL lifecycle phase. Unisys will leverage Six Sigma Lean tools and methodologies as well as ISO Certified internal audits to measure and maintain the highest quality services to the Commonwealth.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

7 CI Client Satisfaction

7.A Improve client satisfaction.

Offeror must provide examples of previous Offeror initiatives aimed at continually improving client satisfaction.

Client satisfaction is extremely important to Unisys and a key focus in our IT solution. The SEO will integrate new agencies, customers and services into our multi-pronged client satisfaction approach that includes Service Desk surveys on the caller's experience, an overall agency satisfaction survey, and quarterly surveys with the Office of Administration. Data collection will

be gathered across multiple levels to gain a clear understanding of the Commonwealth's satisfaction with the IT Services being provided.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

8 CI Service Transparency

8.A Provide service transparency, in particular, visibility into the service execution process.

Offeror must describe its process and provide examples of previous Offeror initiatives aimed at providing service transparency.

The service organizations will use standardized ITSM services processes, IT monitoring and automation tools. ITSM processes will be documented in the Commonwealth Computing Procedures Manual (CCPM). The CCPM will be available to Commonwealth approved staff on the Knowledge Management Portal (KMP) providing desired transparency into service execution processes. Through the Real-time Dashboard, the Commonwealth will have access to current operational performance of their application infrastructure.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

The contracting agency participates in planning, performance and post-testing reviews, thereby having visibility into the entire DR service execution process.

Included below is an example of a review of a successful DR testing that nonetheless included "Issues" and related "Actions" to use the transparency of the report to point to improvements to the service provided. The Unisys Team views "issues" as an opportunity to review services through the ITIL V3 Service Design process and continually improve services.

1. Database Restores
2. Objective
    a. Import backup catalog to Netbackup server at [redacted] and restore databases in time furnctional testing at 8 a.m. on day 3
3. Accomplishments
    a. Catalog import was finished before test began
    b. All AIX Oracle databases were restored by Noon on day 3
    c. Restored PW1 (4TB) and PC1 (10TB) databases
4. Issues
    a. Time to import larger databases was excessively long
    b. RMAN script issue was escalated to Unisys Oracle Tower and Symantec
    c. Some database restores needed to be restarted
    d. NBU log setting caused restart of DB restore on PW1
    e. PW1 restore extended into functional testing time
    f. PC1 database validation did not coplete within test timeframe
    g. PW1 index rebuild did not complete within test timeframe

5. Actions

   a. Retest RMAN scripts before next test

   b. Confirm indexing and validation are part of success criteria

9 CI Service Sustainability

9.A Ensure service sustainability, in particular, efforts targeted at cost containment and cost reductions.

Offeror must describe its process and provide examples of previous Offeror initiatives aimed at ensuring service sustainability.

Service will be sustained by integrating any new agencies, customers, or services into our standard operational and quality processes and methodologies. We leverage ITIL processes, create quality project plans, utilize industry accepted measurement and monitoring tools, analyze trending reports and provide proactive continuous service improvement throughout the IT lifecycle. This enables new Commonwealth services to experience and sustain IT services and client satisfaction.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

10 CI Improve or Reduce Cost

10.A Improve/reduce cost of service.

Offeror must provide examples of On-Demand Infrastructure initiatives that have been implemented or can be utilized to achieve reduced costs of Services and to meet or exceeded ROI (Return on Investment) analysis projections.

The Service Excellence Office will proactively manage quality, continuous service improvement, ITIL process management, and customer satisfaction through a comprehensive quality plan that specifically addresses all of these areas. We believe this is a key differentiator in our partnership with the Commonwealth. Through this new organization and these quality plans, Unisys will drive best in class services and the highest customer satisfaction experience, while reducing overall costs to the Commonwealth.

Please refer to Schedule F, Section 3.2.1.1.6 Continuous Service Improvement for additional details in this area.

The Catalog of Services approach to provisioning DR services provides the Commonwealth with significant opportunities for cost savings. Most organizations approach Disaster Recovery as a Like-to-Like issue and sometimes build out a DR site that is identical in computer power as the Production data center. With the Catalog of Services the Commonwealth could better manage the cost of Disaster Recovery to the likely risks of an actual disaster. For instance, when Unisys crafted the Disaster Recovery plan for the California State University system (CSU) they were reluctant to incur the cost of an identical compute power for a DR plan that they hoped never to use. Unisys presented two options to reduce cost:

3. For virtual servers the computer power was provisioned at a less than 100% of that available for production. CSU was willing to accept a diminished level of service

immediately following an actual data center disaster and Unisys was able to propose a reasonable delivery date to augment the DR facility if an actual disaster occurred. The difference between the current computer power in the DR site and that of the Production data center delivers a monthly savings for CSU.

4. Unisys also provided a means for CSU to utilize assets provisioned for their DR plan as Test and QA/Development servers under the agreement that if an actual disaster occurred then these services would be suspended so that these assets could be pulled into use as the Production infrastructure at the DR site. This allowed CSU to leverage the compute power of the DR site at relatively little risk.

The Agencies in the Commonwealth can, working with the Unisys IT Risk Manager, select servers and storage in the DR facility that would provide a diminished services in the event of an actual disaster. Given the very unlikely chance of an actual disaster this would allow the Agencies to better balance the full cost of a Like-to-Like DR solution against the risk of occurrence of an actual disaster.

Disaster Recovery – File Replication:

The DPH has implemented Distributed File Systems (DFS) to replicate our DPH File Server down to [redacted] In the event of a true disaster, files to perform our duties during and after the DR will be available. Data replication occurs in real time and is de-duplicated over the wire thus saving bandwidth on the WAN link. This provides that our documentation, recovery scripts and procedures are current and accessible at all times to support Commonwealth agencies during disaster recovery drill and in the event of an actual disaster. By avoiding having to ship tapes containing this information to [redacted] and having to restore them, Unisys has improved the recovery time objective for disaster drills and disaster events.

Disaster Recovery – NetBackup Recovery Improvement:

VM replication was implemented to improve the Recovery Point Objective of our NetBackup master servers from 24 hours down to approximately 6 hours. This change will also lower the time it takes to recover the NetBackup server in the DR environment from 2.5 hours to around 30 minutes expediting the start of DR database recovery efforts by almost 80%.

Disaster Recovery-Server Recovery Improvement:

To improve disaster recovery times, the DPH converted AIX mksysb to ISO images to facilitate a much faster server recovery time. Prior to this change, we used CD images or mksysb restores from tape. This resulted in an 85% improvement in recovery times.

Unisys Mainframe- Production Data Mirror Improvement:

The DPH implemented a process to mirror Client data (86 disk packs using EMC time finder) between production mainframes and those at [redacted] Continual improvements remain underway to expand this process increasing the amount of data supported by time finder by and additional thirty percent. This mirroring technique has provided DPW with the ability to maintain 7 x 24-hour processing while replicating data necessary for disaster recovery down to [redacted] This process improvement has enhanced our ability to perform disaster recovery data restoration faster than previously possible, from physical tape storage.

Storage Replication Improvement:

Storage replication solutions have been implemented for several agencies using the latest disk to disk replication technology. These solutions have enabled a reduced dependency on tape media and drives for backup while providing a disk to disk update to offsite data supporting both data backup as well as disaster recovery requirements. Ongoing research and trials are conducted in conjunction with product support organizations to provide proper configuration and optimal performance for the technology supporting this critical managed service.

PSP VDI Improvement:

The State Police was impacted when one of its barracks was closed down due to a mold infestation and they were unable to access computers and have staff in that location for weeks. They were interested in a business continuity plan that would enable them to have access to their files and applications from a remote location. We worked with them to establish a VDI proof of concept at the DPH. Using the Virtual Desktop Interface, they were able to access their information from iPads from any location.

Unisys Team Experience

The Continual Service Improvement sections above provide details of the Unisys Team's rich experience and the value that they have brought to the Commonwealth and its Agencies over the past many years. But the Commonwealth is likely unaware of the breadth of Unisys experience in providing reliable Disaster Recovery operations that provide significant value to customers.

Setting Customers on a course to DR

Unisys provides a service in the market called the Unisys Disaster Recovery Architecture Service. As part of this service the Unisys Team conduct a comprehensive 2-day seminar to provide customers with a solid foundation on which to build an end-to-end application and data disaster recovery capabilities. This service mirrors the embedded service provided to the Commonwealth in this proposal and managed by the Unisys IT Risk Manager on an agency-by-agency basis. For instance the Unisys Disaster Recovery Architecture Services provides:

- Reduction of costs through
  - The deployment of mature recovery services management
  - The collective disaster recovery architectures and processes financially rationalized against explicit, business-driven recovery targets
- Mitigated risk through
  - Knowledge transfer that allows each IT function to understand its specific role within the overall, end-to-end recovery process
  - Institution of proven and formalized recovery services management that yields reliable, disaster recovery capabilities
- Restored quality of service as shown by
  - Disaster recovery, service performance reviews that build confidence through "proof of delivery capability" reports

- Actual disaster recovery costs that become transparent to the business

(for more details see http://www.unisys.com/unisys/inc/pdf/brochures/Disaster_Recovery_Architecture_Service_datasheet.pdf)

Saving Money with efficient DR

Solution

JMC Steel Group worked with Unisys to design and execute a sizeable data center migration and modernization initiative, which standardized the SAP infrastructures at two key data centers on a common hardware platform – and provided the bullet-proof disaster recovery capabilities these critical environments demand.

Results

Carrying out its data center transformation strategy enabled JMC Steel to better support the operations of two major manufacturing facilities. Plus, by making a robust disaster recovery capability a key component of the project, the company greatly improved its ability to avoid the numerous harmful effects of both planned and unexpected downtime.

Metrics

- **Resiliency:** 15-minute recovery time objective (RTO) established and confirmed via testing of automated backup and failover capabilities.
- **Performance:** 300% increase in hardware performance and 50% reduction in response times.
- **Cost avoidance:** $250,000 in lost revenue per four hours of downtime avoided .

http://www.unisys.com/unisys/common/detail.jsp?id=1120000970009510096

Protecting Alabama State citizens through improved DR

The Alabama Criminal Justice Information Center (ACJIC) is a state agency providing local, state, and federal criminal justice agencies with the information needed to ensure citizen safety. ACJIC realized that gaps in its information technology were hindering communications and business continuity. It needed to more efficiently deliver critical information from its network and systems.

Unisys provided a real–time infrastructure with improved disaster recovery and business continuity through a turnkey solution comprising an ES7000/one enterprise server platform, Unisys SafeGuard 30m, and EMC SAN technology.

By implementing the system, ACJIC now has a dependable, cost–effective system that delivers real–time information to end users, supports future growth, and provides robust, reliable operations. It also provides system patches and updates with extreme ease and supports failover requirements. The result is enhanced officer and citizen safety while building trust among constituents.

Metrics

- **Better Security:** Reduced downtime and risk – 24x7 availability with failover in less than one minute from the primary site to the disaster recovery site
- **Reduced Costs:** Lowered costs while processing some 18 million transactions monthly
- **Improved Satisfaction:** Enhanced citizen and officer safety by ensuring a constant flow of real–time information
- **Better Productivity:** Enabled one–to–two–second searches for up to 40 million records in the Law Enforcement Tactical System

http://www.unisys.com/unisys/ri/cs/detail.jsp?id=9400019

Protecting Workers' Compensation through improved IT and DR

EMC Insurance Companies has grown from a provider of workers' compensation coverage to one of the Iowa's largest property and casualty insurance providers – with over 20 branch locations and assets in excess of $3 billion.

A key factor catalyzing nearly 100 years of steady expansion has been EMC's commitment to cultivating successful, lasting relationships with independent agency partners. Yet, as these partnerships grow, so too do the demands for speedy, personalized service that is available around the clock.

With Unisys technology driving its consolidation, virtualization, and business continuity processes, EMC has established an environment that promotes responsiveness and agility across the organization. As a result, the company is better equipped to deliver and support the services that its wide network of branch locations and independent agents demand 24x7.

Metrics

- **Cost:** Consolidated and virtualized 150 existing servers down to 50.
- **Efficiency**: Streamlined disaster recovery procedures, including an 80% reduction in documented processes
- **Service**: Implemented platforms that keep mission-critical systems and applications available at all times

http://www.unisys.com/unisys/ri/cs/detail.jsp?id=10020500013

De Beers UK Streamlines and Strengthens IT Processes and DR

De Beers UK contracted Unisys to outsource and manage the full scope of its IT data centre operations – from hosting critical applications to deploying business continuity measures to providing technical and end-user support services.

The fully managed data centre environment Unisys provided De Beers has enabled the company to improve the flexibility with which it can meet both current and future business and IT demands, eliminated the need to allocate in-house resources to routine IT management tasks, and provided the disaster recovery measures required to ensure the company's infrastructure remains resilient and resistant to failure. What's more, the end-user support capabilities extended the company's resiliency gains to its employees, helping them remain productive and make positive contributions to important initiatives.

Challenge

Minimize the risk of an interruption to global operations, and better support the efforts of end users – without adding complexity or increasing management burden.

Solution

De Beers UK contracted Unisys to outsource and manage the full scope of its IT data centre operations – from hosting critical applications to deploying business continuity measures to providing technical and end-user support services.

Results

The fully managed data centre environment Unisys provided De Beers has enabled the company to improve the flexibility with which it can meet both current and future business and IT demands, eliminated the need to allocate in-house resources to routine IT management tasks, and provided the disaster recovery measures required to ensure the company's infrastructure remains resilient and resistant to failure. What's more, the end-user support capabilities extended the company's resiliency gains to its employees, helping them remain productive and make positive contributions to important initiatives.

Metrics

- **Manageability:** Provisioned a new business intelligence application in four weeks
- **Recoverability:** Confirmed the resiliency of the new infrastructure via a full disaster recovery test

http://www.bookstore.unisys.com/unisys/ri/cs/detail.jsp?id=1120000970016610177

Benefits to the Commonwealth

The Unisys solution provides the Commonwealth with a means to control, manage, and save costs associated with DR services because of the fine granularity in the DR services listed in the Enterprise Services Catalog. Commonwealth Agencies may, for instance, adjust DR services to take on greater risk in times of austerity in order to reduce costs for services.

The Unisys solution provides the Commonwealth with the means to avoid excessive risks and improve the continuity of critical services by utilizing the DR services in the Enterprise Services Catalog to quickly increase DR protections of primary data whenever an Agency is able to identify an increased level of risk associated with critical applications.

As the Unisys Team Experience, Unisys has provided and will provide continual service improvement process that refine processes and services to provide service costs savings through the Unisys enhanced ITIL V3-based Service Design process that adds Continuous

Service Improvement and Innovation Process (CSIIP) Management to the standard ITIL V3 Service Design procedure.

3.2.5.4 Additional Technical Services

The Commonwealth may require additional technical support beyond the standard service level based infrastructure Services. The availability and access to skilled resources would complement the standard hosting offerings. The Offeror is expected to provide these additional resources for both short and longer-term engagements.

Reference Documentation

N/A

	Requirements	Describe Compliance
1.	Provide access to skilled technology resources. Additional technology support Services categories include but are not limited to: • Infrastructure (mainframe, mid-range and x86) Architects/Engineers • Performance Specialists • Database Architects • Database Analysts • Security Architects • Security Analysts • Unix (AIX, Linux) Administrators • Windows Server Administrators • Mainframe Systems Programmers • Batch Administrators • Microsoft Product Specialists (e.g. Exchange, SharePoint)	Offeror must describe its ability to support both short and long-term assignments for a variety of technology skill sets. Offeror must provide representative resumes within each skill category. Offeror must provide a rate card for each resource category in the Cost Matrix.

	• 3rd Party Software Product Specialists • Basis and SAP Oracle support	

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

Introduction

Using the Unisys Enterprise Services Catalog, the Commonwealth will have access to a wide array of additional technical support skills and services related to and on top of the managed compute services which can be used to support ongoing technical support activities, short term assistance requests or new projects. The technical resources and additional technical services are described within the Enterprise Services Catalog in Schedule C Enterprise Services Catalog.

1 Staff, Technical Services Resumes

1.A Offeror must describe its ability to support both short and long-term assignments for a variety of technology skill sets.

Offeror must provide representative resumes within each skill category.

Offeror must provide a rate card for each resource category in the Cost Matrix.

The Unisys Team comprising of Unisys, IBM, Deloitte and a number of Small Diverse Businesses, maintains a wide variety of skilled architects, analysts, technical support and consultants to draw upon to support individual Commonwealth requests for additional resources. The Commonwealth can request the use of additional technology resources through Service Requests via the Enterprise Services Catalog. These additional resources are listed within the Enterprise Services Catalog located in Schedule C. The rate card is available on Tab 5 of Schedule I in Section 10 Cost Submittal. Representative resumes for each type of additional resource are located within section 5 Personnel.

The Commonwealth has the flexibility to use additional technical support personnel and services to support short and long term assignments for projects and ongoing support activities. All requests for the additional skills or services will be recorded within the Enterprise Services Catalog and delivered after approval of the solution by the Commonwealth.

1.B Provide access to skilled technology resources. Additional technology support Services categories include but are not limited to:

Infrastructure (mainframe, mid-range and x86) Architects/Engineers

Performance Specialists

Database Architects

Database Analysts

Security Architects

Security Analysts

Unix (AIX, Linux) Administrators

Windows Server Administrators

Mainframe Systems Programmers

Batch Administrators

Microsoft Product Specialists (e.g. Exchange, SharePoint)

3rd Party Software Product Specialists

Basis and SAP Oracle support

Through the Enterprise Services Catalog, the Unisys Team will support the Commonwealth's request additional technology resources including, but are not limited to the above skilled resources. The Unisys Team maintains a wide variety of skilled architects, analysts, technical support and consultants to draw upon to support individual Commonwealth requests for additional resources. Depending on the skills and functions required and duration of the request, the timeframe to assign the resource may differ.

Unisys Team Experience

Commonwealth of Pennsylvania

As part of a Time and Materials contract, Unisys provides approximately 40 resources to support the Commonwealth of Pennsylvania Enterprise Data Center Unisys Team comprises of about 40 consultants with varied background like Project Managers, System Administrators, Exchange Administrators, Database Administrators, Network engineers, Technical Writers, Automation Engineers, SAN Administrators holding certifications including but not limited to PMP, ITIL, MCSE, MCTS, MCITP, MCDBA, MCSD, OCP, CCNP, CCDP, CISSP and CCSA.

New York State Office of Information Technology Services

As part of a long term relationship beginning in 1976 with the State of New York's Office of Information Technology Services (OITS), the Unisys Team provides skilled additional technical resources to augment OITS's technical team. New York State relies on these resources to manage the Unisys Dorado and Libra Mainframes, related server infrastructure and application development for the Office of Temporary and Disability Assistance, Department of Civil Service, State Education Department and New York State Division of State Police.

Benefits to the Commonwealth

As a part of the additional technical services offerings, the Commonwealth can use the Unisys Team's extensive technical skills to support the Commonwealth's time or complexity driven projects. In addition, the Enterprise Services Catalog offers many additional services, including technologies, assessments and technology management services to enable the Commonwealth

to meet your business needs which require activities above the base compute service offerings.

3.3 Transition Services

3.3.1 Transition Services – Guiding Principals

At present, the Commonwealth's information technology Services are hosted at a variety of Commonwealth data centers, including:

- Shared enterprise facilities - ([redacted] and DPH) and;
- Agency facilities, for example those managed and maintained by DPW, DOR, DOH, PSP and DLI.

The Commonwealth data center locations are identified in Exhibit S - Datacenter locations.

In an effort to reduce data center costs, simplify data center administration, and provide more robust and reliable information Services to the Commonwealth, the Commonwealth data center modernization initiative calls for the phased migration or transition of Commonwealth information Services to the newly-established Offeror managed multi data center environment.

The Guiding Principles associated with the transition to the new data center environment are:

- Transition approach must meet the milestone objectives as described in **Schedule D**.
  - Based on the Commonwealth's number of licenses, additional licenses may be needed for the transition of Services. The Offeror shall be responsible for any additional licenses needed for the transition of service.
  - The Commonwealth, at its sole discretion, may procure the software licenses through existing statewide contract.
- Initial transition approach of the Commonwealth's mainframe and SAP environments requires that the results be as close to the Commonwealth's current configuration as technically possible.
  - Any deviations from current environments must be approved by the Commonwealth.
- Customized approach developed to meet the needs of the Commonwealth
  - The selected Offeror's transition approach shall account for Commonwealth specific needs such as the Transition Considerations and Critical Configuration Considerations as described in Exhibits R and T.
  - The selected Offeror shall implement a discovery process during transition planning to acquire information required to develop a Detailed Transition Plan.
  - The selected Offeror shall include application level transformation models. Transformation models must take into account the initial transition approach that the Commonwealth's mainframe and SAP environments must be as close to the Commonwealth's current configuration as possible.

- Transformation project managers experienced in projects of similar size and complexity.
- Strong governance model, which includes:
  - Clearly defined roles and responsibilities
  - Jointly developed processes
  - Effective meetings and reporting framework to minimize resource requirements while achieving goals
  - Mechanisms in place to identify and address risks and issues
  - Compliance with applicable policies, standards, processes, and procedures
- Effective communication, which includes:
  - Consistent delivery of key messages through well-defined communication plans
  - Tailored communications to target audiences and stakeholders
  - Communications to meet the needs of the Commonwealth.
- Collaboration and teamwork, which includes:
  - Detailed upfront project planning and feedback
  - Agreement on status for reporting purposes
  - Plans scaled to address Commonwealth agency differences in size and complexity
  - Establishment and support for successful deliverable review process
  - Feedback on deliverables throughout the life of the project.

3.3.2 Transition Planning/Governance

The Offeror's Transition Program Management Office (TPMO) will contain a dedicated consolidation specific program team. The team will be responsible to jump-start the consolidation program by bringing respective stakeholders together for a series of transition workshops. The transition workshops will work to align the stakeholders, and produce the following deliverables:

- Overall transition approach and strategy for Server and Mainframe consolidation
- Transition and consolidation governance plan
- Transition risk assessment plan
- Consolidation cost/benefit analysis
- Consolidation stakeholder transition agreements
- Consolidation transition planning guidelines

The TPMO will provide program management Services to deliver architecture, transition plan integration, and organizational change management, as well as quality assurance, verification of testing, financial oversight, and operational readiness for the Mainframe and Server transition/consolidation program. The TPMO will exist under the overall Offeror's PMO office and will include a combination of resources dedicated to the effort full time, plus resources that participate in the program on an as needed basis. The program plan and architecture will be developed by the Offeror and approved by the Commonwealth. The Offeror must verify processes and tools are implemented to support Transition change control, schedule, quality, communications, risk and issues management.

Proposed Transition Plan

The Commonwealth anticipates the following high-level sequence of transition activities. The Offeror must develop an initial transition plan and present with its proposal. At minimum, the Offeror's proposed Transition Plan must reference these activities and project timeframes.

Transition Activities

The high level transition milestones and deliverables are described in **Schedule D - Transition Milestones** and **Schedule K - Key Program Deliverables**.

Target Datacenter Transitions

The following table includes the target datacenter facilities that are to be initially transitioned by the Offeror. The target datacenter facilities are defined as the physical Commonwealth facilities that are selected to be transitioned to the Offeror's control and/or facilities. The Offeror must coordinate with each Commonwealth agency or data center representative to create a *Facility Specific Transition Plan* for each targeted facility. The Offeror must include target datacenter transitions in its proposed Transition Timeline to be included in its proposal. The Offeror must include a "pilot" transition approach to verify successful transitions of Commonwealth applications and infrastructure. This approach will demonstrate to the agencies that Offeror's approach will be successful before moving forward with additional transition phases.

Offeror must establish a high-speed direct link (not via COPANet) with the current DPH location to enable "systems" connectivity that would facilitate the ability to effect smoother transition of data.

The selected Offeror shall not charge the Commonwealth for a transition milestone until the milestone has been accepted by the Commonwealth. Milestone acceptance criteria are described in Schedule D - Transition Milestones.

	Target Datacenter Facilities		Transition Requirement Notes
	Group1 Transitions		
1	**DPH** (All Agency Mainframe – Unisys, IBM; IES SAP, and all other Agency hosted environments)		• The DPH operation and all of its supported agency application workloads must be successfully migrated out of the current facility to the Offeror's Datacenter. • Operations support will be assumed by the Offeror once the workloads are successfully moved to the new provider's datacenter environment. • Key Transition Milestone(s): o Refer to **Schedule D - Transition Milestones**
1	[redacted]		• Offeror must assume operations support of the [redacted] datacenter

	Target Datacenter Facilities		Transition Requirement Notes
			• Key Transition Milestone(s): o Refer to **Schedule D - Transition Milestones**
Group 2 Transition			
2	**DLI**		• The DLI datacenter operations and all of its supported application workloads must be successfully migrated out of the DLI facility to the Offeror's Datacenter. • Key Transition Milestone(s): o Refer to **Schedule D - Transition Milestones**
Group 3 Transitions			
3	**DPW** – Rm. 105, 106 (Lower Environments, PACSES)		• The DPW Rooms 105, 106 datacenter operation and all supported application workloads must be successfully migrated out of the current DPW facility to the Offeror's Datacenter architecture. • Key Transition Milestone(s): Refer to **Schedule D - Transition Milestones**
3	**DOR**		• The DOR datacenter operation and all of its supported application workloads must be successfully migrated out of the current DOR facility to the Offeror's Datacenter architecture. • Key Transition Milestone(s): o Refer to **Schedule D - Transition Milestones**
3	**DOH**		• The DOH datacenter operation and all of its supported application workloads must be successfully migrated out of the current DOH facility to the Offeror's Datacenter architecture. • Key Transition Milestone(s): o Refer to **Schedule D - Transition Milestones**
3	**PSP**		• The PSP datacenter operation (Headquarters) and all of its supported application workloads must be successfully migrated out of the current PSP facilities to the Offeror's Datacenter architecture. • Key Transition Milestone(s): o Refer to **Schedule D - Transition Milestones**

3.3.2.1 Transition Program Management

The TPMO function confirms the non-disruptive migration of Commonwealth information Services from current Commonwealth host locations, to the Offeror provided multi datacenter environments.

The Offeror must establish a TPMO and develop the requisite transition plans.

A transition approach and detailed transition plan for each of the Commonwealth's existing Datacenters must be developed by the Offeror and approved by the Commonwealth. The Commonwealth has over 2,000 business applications with over 50% designated mission critical. The Offeror must work with each agency to determine its application environment within each facility. The Offeror's target datacenter environment must be configured and tested prior to migration of the application.

Reference Documentation

Schedule D - Transition Milestones

Exhibit D.7 - [redacted] - Facility Summary

Exhibit A - Commonwealth Network Environment

Exhibit(s) B.1 through B.6 - Data PowerHouse (DPH) Exhibits

Exhibit(s) C.1 through C.13 - Department of Public Welfare (DPW) Exhibits

Exhibit(s) D.1 through D.15 - Enterprise Datacenter ([redacted] Exhibits

Exhibit(s) E.1 through E.43 - Department of Labor & Industry (DLI) Exhibits

Exhibit(s) F.1 through F.4 - Department of Health (DOH) Exhibits

Exhibit(s) G.1 through G.16 - PA State Police (PSP) Exhibits

Exhibit(s) H.1 through H.8 - Department of Revenue (DOR) Exhibits

Exhibit(s) I.1 through I.13 - Commonwealth SAP Environment - Integrated Enterprise Services (IES) Exhibits

Exhibit L - Commonwealth Master Application Inventory

Exhibit(s) M.1 through M.7 Department of Corrections (DOC) and Pennsylvania Board of Probation and Parole (PBPP) Exhibits

Exhibit(s) N.1 through N.2 - PennDOT Exhibits

Requirements		Describe Compliance
1.	Establish a TPMO to manage all information service transition	Offeror must describe the proposed TPMO, and discuss the mission, goals and objectives, and the roles and responsibilities of the

	activities. The Office will be jointly administered by Offeror and Commonwealth staff. Provide a communication plan that will provide an information vehicle for all interested parties.	Offeror. Offeror must provide at least one sample where Offeror has successfully created an office similar to the required TPMO.
2.	Provide a functional organization chart for the TPMO, including an estimate of the type and number of full time Offeror resources that will be required to ensure the successful transition of Services from current multiple datacenters to the Offeror's datacenter Services.	Offeror must describe the TPMO structure including but not limited to the number of full time resources and the role of the TPMO in the transition.
3.	Analyze applications and design the required computing architecture to migrate Commonwealth datacenters to Offeror datacenter environments. Hardware, software, network, etc. Work with Commonwealth technical staff to ascertain the requirements to successfully migrate processing to Offeror datacenter environments	Offeror must describe solution and approach to meet this requirement. Offeror must provide at least one relevant example from a prior engagement, in which it was engaged, that is similar to the needs of the Commonwealth.
4.	Optimize Current Process and Procedures – Coordinate with Commonwealth agencies to review and plan for a transition of processes and procedures.	Offeror must describe its overall plan for optimization of the existing processes, procedures, tools, etc. to provide more efficient and effective Services. The description must include approach, plan, and methodologies.
5.	Revise datacenter DR plans on the occasion of major changes to the datacenter hardware, software, or network portfolio to reflect those major changes.	Offeror must describe solution and approach to meet this requirement.
6.	Establish an IT infrastructure that	Offeror must describe solution and approach

	meets all application processing requirements. The Offeror must confirm that the target IT infrastructure meets or exceeds current computing requirements. Work with Commonwealth technical staff to design and build the infrastructure required to support the applications being migrated to the Offeror multi datacenter environment.	to meet this requirement. Offeror must provide at least one relevant example from a prior engagement, in which it was engaged, that is similar to the needs of the Commonwealth.
7.	A multi-faceted Transition Strategy will be required: • Comprehensive; • Non-disruptive; and • Compliant with Commonwealth requirements. The Strategy will address the transition of: • Shared infrastructure elements, as appropriate; and • Specific information Services. • Disparate Agency application architectures and impacts to move to the new environment(s) The Strategy must also address the following: • Cost/Benefit for the Agency • Risks and Risk Mitigation Plan The migration order of the Commonwealth datacenters will be provided by the Commonwealth.	Offeror must describe the transition (interim and steady state strategies) and transition plans that it has employed during other similar size engagements.
8.	Identify mandatory requirements and critical success factors that will have	Offeror must describe the 3-5 characteristics, conditions, or variables it believes will have

	a direct impact on developing a successful transition plan	a direct and critical impact on the effectiveness, efficiency, and viability of the Offeror's solution. Offeror must describe its approach to mitigating risks and ensuring these critical factors are successfully addressed.
9.	Create a Transition Timeline that outlines the overall timeline starting at effective date and continues through delivering transition Services for each of the targeted datacenters.	Offeror must describe the overall timeline from the start of pre-Transition activities through the point at which the Offeror expects it will be delivering predictable, repeatable Managed Service Results that meet the requirements of the RFP. The schedule must include a description of the critical milestones related to Transition efforts for each targeted Commonwealth datacenter. Any critical milestones identified must be included in the Transition Project Plan.
10.	Create a generic Infrastructure Element Transition Plan that may be readily adapted to accommodate specific infrastructure element transitions. Create a prospective Infrastructure Element Transition Plan. Appropriate [redacted] DPH and other Agency Datacenter hardware elements may be re-purposed wherever possible.	Offeror must describe a realistic Transition Project Plan to transition the Commonwealth's datacenters to the proposed architecture.
11.	The [redacted] Managed Services datacenter assets must be managed and maintained by the Offeror until they are transitioned to the Offeror's managed Services. The current maintenance contract for the [redacted] servers is scheduled to expire on June 30, 2014.	Offeror must describe its transition approach to address the transition of operations and management of the [redacted] infrastructure from the Commonwealth to the Offeror's support Services and how it intends to address the server maintenance expiration issue.

12.	Create, manage and execute an application / infrastructure migration plan. The Offeror has the primary responsibility for planning and executing the transition of infrastructure elements, with support of Commonwealth technical and business support staff. The Offeror must provide adequate tools and techniques for moving and migrating Commonwealth data to the new target storage environment. The Offeror must ensure that critical applications are not decoupled from key infrastructure components causing system latency.	Offeror must describe solution and approach to meet this requirement. Offeror must provide at least one sample where it has successfully migrated application and hardware. Offeror must describe its proposed tools and techniques for moving and migrating Commonwealth data to the new target storage environment.
13.	Create a generic Information Service Transition Plan that may be readily adapted to accommodate specific information service transitions.	Offeror must outline a prospective Information Service Transition Plan to take over support of migrated Commonwealth systems and applications. Offeror must provide at least one sample where it has successfully completed application and hardware migrated.
14.	Meet with Commonwealth to produce and execute specific Information Service Transition Plans. Select cut over windows that minimize system unavailability and coordinate approval with the affected agency. Communicate to the Commonwealth cut over date and times. Setup a special call number and support staff to take calls concerning the migration, these Services must be made available to transitioned users until the transition is officially signed off as completed. .	Offeror must describe solution and approach to meet this requirement. Offeror must provide at least one relevant example from a prior engagement, in which it was engaged, that is similar to the needs of the Commonwealth.

15.	Work with Commonwealth to create testing, business acceptance and fallback plans.	Offeror must describe solution and approach to meet this requirement. Offeror must provide at least one relevant example from a prior engagement, in which it was engaged, that is similar to the needs of the Commonwealth.
16.	Service Management Systems – Offeror must transition all agency system management platforms currently in place to the Offeror, consolidating all system management responsibilities. The Offeror must make available all system management platforms and tools that are currently supporting the Commonwealth infrastructure.	Offeror must describe solution and approach to meet this requirement.
17.	CMDB – Work with the Commonwealth to acquire asset information to support the asset management system and configuration management system.	Offeror must describe its approach to capturing, validating and storing all configuration information required to perform the Services within 120 days of the Effective Date of the Contract. In particular, the Offeror must address how it will identify and relate critical associations (e.g. Application to Server, Server Tier to Application, Application to Disaster Recovery Time Objective, software to server, etc.) for the enterprise. Offeror must describe its approach to transitioning the data and related processes from the existing CMDB or equivalent system/database to the Offeror's solution and how the Offeror must ensure accuracy of data across Service Management areas to ensure accurate and timely invoicing and chargeback to the Commonwealth.
18.	Chargeback – Work with the Commonwealth to	Offeror must describe its transition approach to Chargeback Management.

	interface with the Commonwealth's billing processing and validation ITSM system to provide a chargeback system for new and existing Services available on the Offeror's Service Catalog.	Offeror must describe its approach to assisting the Commonwealth in transitioning Commonwealth customers from the existing Chargeback system. The description must include an expected analysis of the current billing system environment, expected termination assistance, communications plans, strategy for testing and major milestones.
19.	Identify Options and Costs – List the appropriate different options that will satisfy the requirements of the transition scope. Communicate options with the Commonwealth and obtain approval on selected option(s) to proceed.	Offeror must describe proposed approach.
20.	Expand/reconfigure datacenter facilities to accommodate growth in Commonwealth information and information systems.	Offeror must discuss its approach; the expansion/reconfiguration plans must include the [redacted]
21.	Produce weekly reports on the progress of the information service transition initiatives.	Offeror must describe its proposed approach to providing weekly transition progress reports.

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

Introduction

Strong communications between the Commonwealth and the Unisys Team is critical to the success of the program. The deliverables identified in Schedule K provide good insight to Unisys on the priorities for the program. Below you will find an extension of the Unisys response to each Key Program Deliverable that provides insight into the Unisys approach for each.

1 TPMO Approach

1.A Establish a TPMO to manage all information service transition activities.

Offeror must describe the proposed TPMO, and discuss the mission, goals and objectives, and the roles and responsibilities of the Offeror.

The Transition Program Management Office (TPMO) will provide standards, oversight and cross-functional support to the project within the initial Transition and any future transition activity that may occur during steady state. This organization takes advantage of the collective experiences of Unisys, IBM, and prior experience of the staff. **Figure 3.3.2.1-1** below depicts the functions within the TPMO and the teams that will leverage these functions. The TPMO will facilitate information sharing, provide guidance, and publish lessons learned to improve communications both vertically and horizontally.

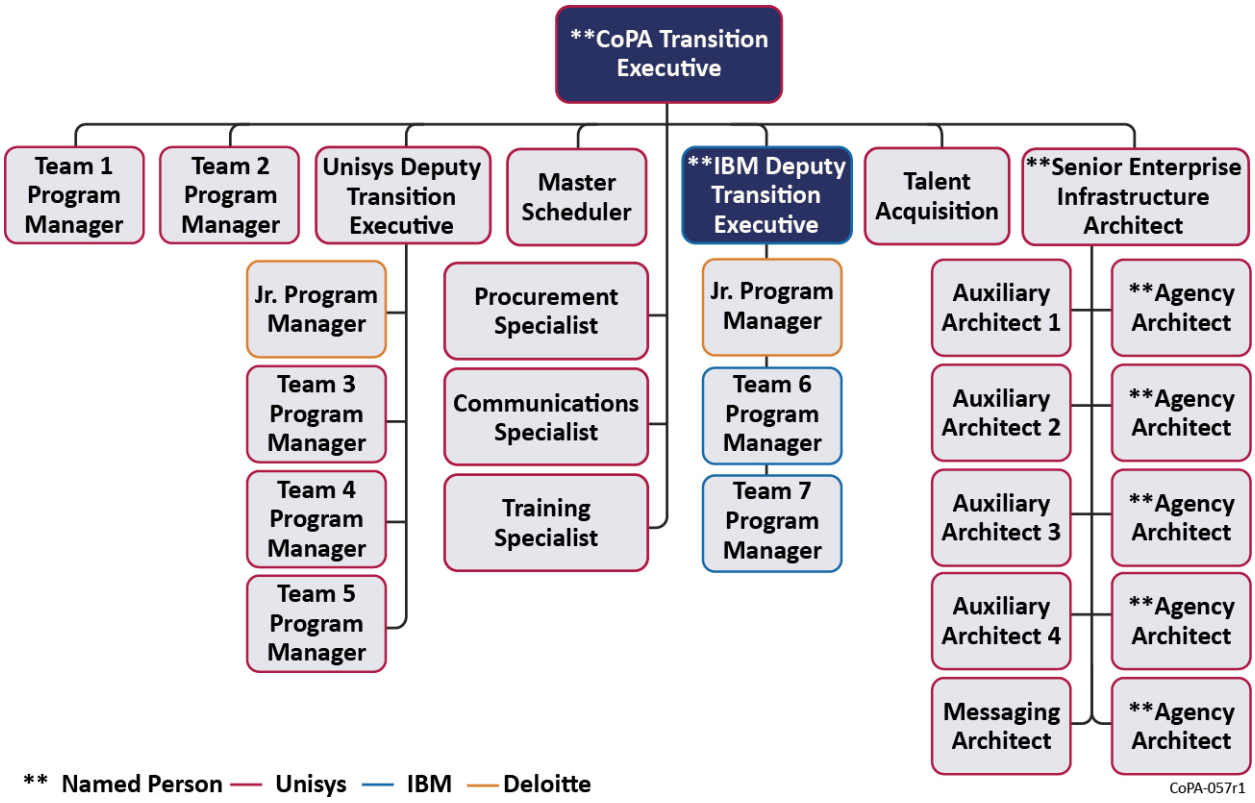


Figure 3.3.2.1-1 – TPMO Organization

The mission of the TPMO is to be the sole governance and program management organization responsible for the successful transition of all Commonwealth IT services from their internal Commonwealth IT organizations and Data PowerHouse (DPH) contract to this proposal's new contract services, organization, facilities, processes, deliverables and structure. As part of that mission, it is the TPMO's goal to accomplish this transition, as an application centric model, in accordance to the scope, requirements, deliverables and milestones set forth in Schedule D – Transition Milestones and Schedule K – Key Program Deliverables within the RFP.

The TPMO will nurture our existing working relationships with the Commonwealth to provide an efficient, coordinated, and insightful transition of services to the new contract with the objective to transition all of the Commonwealth's mainframe, midrange and SAP environments to be as close to the Commonwealth's current configuration as technically possible. Our TPMO will carefully control the changes to the current configuration through strong oversight of our teams and a close working relationship with the Commonwealth's technical and leadership teams. Our policy of open communication policy removes many of the pitfalls that disrupt transitions.

1.B Offeror must provide at least one sample where Offeror has successfully created an office similar to the required TPMO.

Key to this program's success is the strong organization and collaborating between the Commonwealth and the Unisys Team. A project of this size and complexity requires a deep level of understanding of the goals and current environment as well as diverse experiences. The Commonwealth of Pennsylvania Data Center Transition Program benefits from prior projects undertaken and led by the Unisys Team such as the American Red Cross, State of Georgia, as well as our existing Commonwealth of Pennsylvania Data PowerHouse contracts as referenced in Section 4.5 of this proposal.

1.C The Office will be jointly administered by Offeror and Commonwealth staff.

The TPMO while a standalone organization as it relates to transition will have joint administrative oversight through a Program Steering Committee. The Program Steering Committee will be comprised of senior leaders from both the Commonwealth and the Unisys Team. This committee will drive the strategic direction, tactical decisions, issue escalation, and communication with leaders within the Commonwealth Office of Administration, agencies, and bureaus.

Within each sub-project, a joint Commonwealth and Unisys oversight steering committee will be established The exact make-up and size of the steering committee will depend on the project but in general will be headed by one of the Deputy Transition Executives and include the Project Manager, Application Owners and as appropriate, an agency director's representative. These committees will be responsible for providing strategic direction to each project, decision making based on Commonwealth agency and customer requirements, resolution of project issues and communications within the agency/customer base.

1.D Provide a communication plan that will provide an information vehicle for all interested parties.

A program level Communications Plan, managed by the Transition Director, will provide overall governance and communication updates throughout the program. The Project Managers will leverage the common project level communications plan tailoring their communication plan from the common communication plan. **Figure 3.3.2.1-2** below depicts the proposed Program Level Communication Plan.

Title	Owner	Audience	Trigger	Purpose	Length (UOM)	Frequency	Format
Program Kickoff	Transition Director	Program Steering Committee and Program Sponsors	Contract Signature	To review and plan the program	4 hours	Once	Meeting
Program Steering	Transition	Program Steering	Program	Interactive review of	1 hour	Weekly	Meeting/Teleconference

Committee Reviews	Director	Committee and Program Sponsors	Kickoff	progress, risks and plans (tactical)			
Program Strategic Planning	Transition Director	Program Steering Committee and Program Sponsors	Calendar	Interactive Review of Progress, risks and plans (strategic)	4 hours	Quarterly	Meeting
Program Status Report	Transition Director	Unisys Leadership, Commonwealth Leadership	Program Kickoff	Informational Static report for wider dissemination (tactical)	2 Pages	Weekly	Report
Agency Kickoff	Transition Director	Agency Leadership, Commonwealth Sponsor, Unisys Leadership	Agency Kickoff	To review and plan agency participation	4 hours	Once	Meeting
Agency Status Review	Transition Director	Agency Leadership, Commonwealth Sponsor, Unisys Leadership	Agency Kickoff	Interactive Review Progress Risks and Plans (tactical)	2 hours	Monthly	Meeting
Milestone Signoff	Transition Director	Commonwealth Program Sponsor and Unisys Client Executive	Milestone Completion	To review results of the program; gain concurrence for successful completion of milestones	1 page	Periodic	Letter
Unisys Executive Reviews	Transition Director	Unisys: President of Global Managed Services, VP Outsourcing, VP Global Delivery, VP Commonwealth Account, VP Service Delivery, Global Director of Transitions, Commonwealth Program Manager	Contract Signature	Bi-lateral communications on issues, assistance with resolution, direction setting and course correction	1 hour	Weekly	Teleconference

Figure 3.3.2.1-2 - Sample Program Level Communication Plan

Figure 3.3.2.1-3 below depicts a sample Project Level Communication Plan.

Title	Owner	Audience	Trigger	Purpose	Length (UOM)	Frequency	Format
Project Kickoff	Project Manager	Application Owners, Agency Leader, Technical Project Team	Program Schedule	To review and plan the project	2 hours	Once	Meeting
Project Status Reviews	Project Manager	Application Owners, Technical Project Team	Project Kickoff	Interactive review of progress, risks and plans (tactical)	1 hour	Weekly	Meeting/Teleconference
Project Status Report	Project Manger	Unisys Leadership, Agency Leadership	Project Kickoff	Informational Static report for wider dissemination (tactical)	1 Page	Weekly	Report
Scope Signoff	Project Manager	Agency Leadership	Project Schedule	To document agreed upon scope and methods for project execution	1 or 2 Pages	Once	Report
30/7/2 day Notifications	Project Manager	Unisys Leadership, Agency Leadership, applications users	* 30/7/2 days prior to significant Events	To provide notification to affected parties of an event that may affect their business	1 Page	Once	Email/Letter
Event Completion Signoff	Project Manager	Commonwealth Application Owner or process owner	Completion of event + 3 days	To review the results of an event; gain concurrence for successful completion of the event / project	1 Page	Once/event	Letter

Figure 3.3.2.1-3 – Sample Project level Communications Plans

2 Transition Functional Organization Chart

2.A Provide a functional organization chart for the TPMO, including an estimate of the type and number of full time Offeror resources that will be required to ensure the successful transition of Services from current multiple datacenters to the Offeror's datacenter Services. Offeror must describe the TPMO structure including but not limited to the number of full time resources and the role of the TPMO in the transition.

Please see the response to requirement 1 in table F.3.3.2.1 for an overview of the TPMO and **Figure 3.3.2.1-1** above for the TPMO functional organization chart. Our response to Section 5.6, Staffing Plan provides additional staffing details such as the number of staff expected to participate. The TPMO structure including roles and responsibilities is described in detail below:

Transition Executive

Unisys has appointed [redacted] as the Transition Executive responsible for all aspects of delivering the transition, including milestones, communications, and the identification and assignment of transition resources. The Unisys Transition Executive will represent Unisys as the single point of contact (SPOC) during the transition, provide oversight and direction, and monitor the transition's overall status. The Unisys Transition Executive's role includes:

- Managing all aspects of the transition program, including planning, staffing, finance, and implementation of transition deliverables
- Maintaining overall business relationship with Unisys, Commonwealth and business partners as it relates to the Transition program
- Ensuring that all Transition communication is made according to the Communication Plan
- Confirming that resources participating in the transition program have a common understanding of needs of both businesses and the program's deliverables
- Agreeing on the scope, timelines, costs, and delivery timetables for each technology domain, confirming they are consistent and complementary with the transition program's objectives
- Establishing effective controls and procedures for the transition program
- Monitoring progress with all areas contributing to the program
- Reporting the transition's status to all program stakeholders
- Managing team performance to meet all transition objectives on time and within budget and quality
- Identifying and resolving conflicting transition priorities
- Managing internal and external relationships and expectations for a successful transition
- Conducting project and program implementation reviews to measure the transition's actual performance against the goals.

Deputy Transition Executive(s)

Unisys will appoint Deputy Transition Executive(s), who shall be responsible for aspects of delivering the projects within their portfolio, including milestones, communications, and the identification and assignment of transition resources. The Deputy Transition Executive(s) will

represent the Unisys Team as the single point of contact (SPOC) for their respective project portfolio during the transition, provide oversight and direction, and monitor their portfolio's overall status. The Deputy Transition Executive's role includes:

- Overseeing all aspects of the transition projects, including planning, staffing, finance, and implementation of transition deliverables
- Mentoring of Project Managers
- Providing an escalation point within each project
- Overseeing that all project portfolio communication is made according to the Communication Plan
- Confirming that resources participating in the transition project portfolio have a common understanding of needs of both businesses and the project's deliverables
- Establishing effective controls and procedures for the transition project
- Monitoring progress with all areas contributing to the project
- Facilitating reporting of their portfolio's status to the TPMO
- Identifying and resolving conflicting project priorities escalated from Project Managers
- Conducting project implementation reviews to measure the transition's actual performance against the goals and critical success factors.

Project Manager(s)

Project Managers, will be responsible for all aspects of delivering the projects, including milestones, communications, and the identification and assignment of project resources. The Project Manager(s) will represent the Unisys Team as the single point of contact (SPOC) at the individual project level, provide oversight and direction, and monitor the project's overall status. The Project Manager role includes:

- Managing all aspects of the project, including planning, staffing, finance, and implementation of deliverables
- Maintaining business relationship with Unisys, Commonwealth and business partners
- Facilitating all communication made according to the Communication Plan
- Confirming that resources participating in the project has a common understanding of needs of both businesses and the program's deliverables
- Agreeing on the scope, timelines, costs, and delivery timetables for each tower, confirming they are consistent and complementary with the transition program's objectives
- Monitoring progress with all areas contributing to the project
- Reporting the project's status to all project stakeholders
- Managing team performance to meet all project's objectives on time and within budget and quality
- Identifying and resolving conflicting project priorities.
- Managing internal and external relationships and expectations for a successful project

Project Coordinator(s) – a.k.a. Jr. Project Managers

Project Coordinators, will be appointed who shall be responsible for assisting the Project Manager in delivering a successful project. The Project Manager role includes:

- Scheduling Meetings
- Capturing, documenting and distributing meeting minutes
- Organizing project documentation
- Collecting schedule updates at the individual project level and provide those updates to the Master Scheduler

Master Scheduler

The Master Scheduler is responsible for all aspects of Project's Schedule(s). The Master Scheduler's role includes:

- Developing standards and guidelines, consistent with Unisys Project Management Best Practices, involving the Program's Master Schedule and all related schedules
- Facilitating weekly progress updates and tracking within Microsoft Project
- Detailed schedule development
- Schedule reporting as required
- Schedule issue escalation to the TPMO
- Consolidation of project schedules into the program schedule as needed.

Additional Transition Team Member Roles and Responsibilities

During the planning sessions, we will identify the Transition Subject Matter Experts (SME's). We will organize the SME's into teams to focus their work. Individually, each SME will have a role and specific responsibilities for the Transition. The team structure and functions are presented Team at the Transition Kickoff Meeting.

The following **Figure 3.3.2.1-4** provides an overview of the roles and responsibilities for each member of the Transition Team.

Team Member Role	Team Member Responsibilities
Technical Implementation Engineers	Responsible for various technical disciplines including Mainframe, AIX, x86 (Windows and Linux), Network, Security, ITSM, Storage, Backup and Monitoring. Will deliver technical knowledge of tools for implementation and processes.
Procurement Specialist	Responsible for ensuring all team members know and understand the procurement process, assist TIEs with securing BOMs, PO Approval, Order tracking, expediting and receiving. Will notify appropriate team members when orders are received.
Talent Acquisition Specialist	Responsible for ensuring all team members know and understand the staffing process, assist team members with staffing requisition tracking, expediting and receiving.
Training Specialist	Responsible for coordinating all training needs for the Commonwealth, Account PMO,

	Transition PMO and Technical Teams including use of facilities for training purposes, coordination of 3rd party training required for the transition and support in development of account specific training needs.	
Communications Specialist	Responsible to provide all communications to the Commonwealth and its Stakeholders is timely, accurate and professional.	
Senior Enterprise Infrastructure Architect	Responsible to provide overall Commonwealth Supported Architecture meets or exceeds requirements, is documented, and is implemented within quality standards.	
Agency and Auxiliary Architects	Responsible for agency and tower specific architectures as determined by the Account Lead Architect	

Figure 3.3.2.1-4 - Transition Roles and Responsibilities

3 Requirements Analysis Approach

3.A Analyze applications and design the required computing architecture to migrate Commonwealth datacenters to Offeror datacenter environments. Hardware, software, network, etc.

Offeror must describe solution and approach to meet this requirement.

The Commonwealth benefits from the 13+ years of experience the Unisys Team has supporting the Commonwealth of Pennsylvania and its key applications residing in the Data PowerHouse and Enterprise Data Center. The Transition and Data Center Methodology utilized by Unisys keeps the applications at the center of focus.

The first step in planning the Transition is to understand the applications supported within each data center. The Unisys Team will accomplish this during the Data Gathering phase leveraging [redacted] tool to understand all applications running in the environment and their relationship to each other and to the infrastructure. Additionally the Commonwealth may choose to request two additional tools from the Enterprise Services Catalog in situations where the application owners may need additional help to identify technical requirements. [redacted] the industry leading asset analytics tool, gathers detailed infrastructure information to provide the appropriate future-state infrastructure environment for each application/component. The application owners will also have at their disposal a process developed by Unisys Team members called Application Performance Impact Assessment that takes a top-down approach to identify those applications that are critical and require a deep dive. The process is supported by tools and software utilized for latency issue detection and validation.

Once the information gathering and documentation is complete, the Unisys Team will generate a draft move package grouping based on the application dependencies, the number of applications, and the number of servers. The move package groupings are reviewed at an application grouping level with representatives from the Commonwealth prior to creating the initial project schedules. The project team and application owners will provide a detailed review and input into the detailed project schedules. This input will include a review of the scope of each application, confirmation of related applications as well as input into the appropriate day, date and time of day that reduces the impact to the stakeholders who utilize the application(s).

During the project, additional attention is paid to each application to provide a smooth migration. These tasks include reviewing the applications for hard coded IP addresses, firewall rules, and other issues that may occur during the migration. Based on the information gathered

and the analysis of application requirements, the required computing architecture at the target data center environment will be reviewed and validated accordingly. Development and execution of detailed test plans both before and immediately after the migration is required to verify the application will execute as expected. Lastly, each migration project is not completed until the application owner has confirmed the application executes as expected.

3.B Offeror must provide at least one relevant example from a prior engagement, in which it was engaged, that is similar to the needs of the Commonwealth.

The Commonwealth of Pennsylvania Data Center Transition Program benefits from prior projects undertaken and led by the Unisys Team such as the American Red Cross, State of Georgia, as well as our existing Commonwealth of Pennsylvania Data PowerHouse contracts as referenced in Section 4.5 of this proposal.

3.C Work with Commonwealth technical staff to ascertain the requirements to successfully migrate processing to Offeror datacenter environments

The Unisys Team recognizes the need for and value the Commonwealth technology and application support staff participation in the transition program. In particular, the application owners will perform key roles in the program and projects. These stakeholders will be involved in the planning, execution and testing of migration packages. Prior to the kickoff of migration projects, the project manager will send a questionnaire to each application owner, requesting basic information for each application. The results will form the basis for the kickoff meetings content and will be updated throughout the project as additional information becomes available.

4 Process Optimization Plan

4.A Optimize Current Process and Procedures

Offeror must describe its overall plan for optimization of the existing processes, procedures, tools, etc. to provide more efficient and effective Services.

The description must include approach, plan, and methodologies.

The Transition of Services Project(s) will be dedicated to understanding and documenting the current state environment for the Commonwealth's data centers. When these tasks are completed, the team will turn its focus to identifying the gaps between current processes and the Unisys Team's best practices in order to develop a strong detailed plan for a seamless implementation and conversion to those appropriate best practices.

The Unisys Team will apply their experience and knowledge of the Commonwealth will enhance their ability to identify opportunities for transition improvements. For a more detailed explanation please see Section 3 Attachment 9 "Schedule M: Detailed Transition Plan". Additional information on the Unisys Team's approach to Continuous Improvement can be found in Schedule F, Section 3.2.1.1.6.

4.B Coordinate with Commonwealth agencies to review and plan for a transition of processes and procedures.

During the initial transition of services project, the Unisys Team will meet with the Commonwealth and key agency representatives to gain insight needed to create an effective

plan, and then to obtain concurrence on the plan.

5 DR, Data Recovery Plan Revisions

5.A Revise datacenter DR plans on the occasion of major changes to the datacenter hardware, software, or network portfolio to reflect those major changes.

Offeror must describe solution and approach to meet this requirement.

The Unisys IT Risk Manager in the Program Management Office will oversee an Agency-by-Agency review of each Disaster Recovery Plan during transition. As part of this review, each Agency plan will be entered into the new online DR planning tool requested by the Commonwealth. This transition process populates the online DR planning tool with the DR Runbooks and provides the initial capture of the Commonwealth's Disaster Recovery capacity required.

Following transition the IT Risk Manager in the Program Management Office will oversee the maintenance of the Commonwealth's online disaster recovery tool as part of this Unisys proposal. The IT Risk Manager and Disaster Recovery Coordinators have broad oversight at the Agency level and meets with Agency leaders regularly to review, update, and maintain Agency Disaster Recovery plans within the new online DR planning tool. The addition of new Customers or new Services will also initiate an action for the IT Risk Manager to schedule an oversight review with the appropriate Agency-level leader and validate they have been incorporated into Agency-level Disaster Recovery Plans.

The Unisys operations teams that maintain the Unisys-managed Disaster Recovery configurations across our data center locations will rely on review of changes to the online Disaster Recovery planning tool, regular Disaster Recovery trend reports and new Project roster reviews to gauge and maintain adequate supply and appropriate tiers of service in the Disaster Recovery sites.

Ultimately, the DR plan is tested for quality and completeness during the two annual tests that the Commonwealth stipulates. Upon completion of each test, the Disaster Recovery Testing team will review all DR test results as part of the regular remediation and improvement cycles that follow any DR testing.

The specifics of the Commonwealth's new DR Infrastructure on Demand are detailed in the Schedule F, Section 3.2.5.3 DR Infrastructure on Demand section.

6 Infrastructure Design, Example

6.A Establish an IT infrastructure that meets all application processing requirements. The Offeror must confirm that the target IT infrastructure meets or exceeds current computing requirements.

Offeror must describe solution and approach to meet this requirement.

Using the Commonwealth's requirements defined in Schedule F, Schedule J1-3, Schedule I, and the Exhibits, Unisys has developed a multi-tenant infrastructure architecture, including hardware, software, and services; which will support the Commonwealth's applications and services. Unisys is confident the solution provided meets or exceeds all processing requirements identified. For additional information on the infrastructure architecture, please see Schedule F, Section 3.2.2.2. Unisys will work with the Commonwealth and its Agencies to validate that the infrastructure meets or exceeds the current computing requirements during the transition of services to Unisys support and management. The transition program is

designed to migrate a "like for like" environment. If a new environment such as a test environment is required, the Commonwealth can choose from the options in the Enterprise Services Catalog.

As the Commonwealth migrates to the Unisys managed data centers, the Unisys Team will work the Commonwealth's technical staff to evaluate the application requirements and recommend the components of the infrastructure architecture and the services catalog to support the migration of the services to the managed data center environment. The Unisys Team will be implementing the infrastructure architecture to support a multi-agency environment to enable the Commonwealth to select the appropriate components and services in a manner that will be flexible for both cost and technical needs. Many elements of the infrastructure will be available as a shared service and also can be implemented as a separate dedicated component when a requirement for separation is provided. As part of the evaluation, Unisys will work with the Commonwealth to understand any regulatory requirements, recommend and implement additional services to meet the regulatory requirement.

6.B Offeror must provide at least one relevant example from a prior engagement, in which it was engaged, that is similar to the needs of the Commonwealth.

The Unisys Team has supported the Commonwealth's Data PowerHouse data center since 1999. This environment supports multiple agencies using both dedicated and shared technical components for many Commonwealth business critical applications. As part of the 2008 contract renewal, the Unisys Team added several technologies and services delivering flexibility to share technical resources between agencies to reduce cost and improve service for the Commonwealth.

Since 2001, the Unisys Team has provided data center hosting services to the California State University supporting the Chancellor's office and 23 campuses. The Hosting service provides infrastructure support for the University system's PeopleSoft Higher Education applications and Oracle databases using shared infrastructure and technologies while continuing to support the needs of the overall university system and individual campus operations.

6.C Work with Commonwealth technical staff to design and build the infrastructure required to support the applications being migrated to the Offeror multi datacenter environment.

Unisys will provide a network of data centers that supports relocation of Commonwealth applications. All Unisys data centers other than the [redacted] are Uptime Institute Tier 3 equivalent facilities.

The [redacted] will remain untouched except for provision of metering for the computer room. Updates to the facility infrastructure including BMS, UPS, generators, and air conditioning will be presented for Commonwealth approval. (NOTE: Because the facility is not Tier 3, configurations with SLA's requiring Tier 3 will be relocated to another facility.)

7 Multi Faceted Transition Strategy

7.A A multi-faceted Transition Strategy will be required: comprehensive, non-disruptive, and compliant with Commonwealth requirements

In general, the program will take a top-down approach to planning while each of the projects will be bottom-up. This allows the Program Steering Committee to provide strategic direction to the program to provide a successful migration while at the same time allowing the projects to focus on each agency, their applications and their stakeholder's unique requirements.

As project teams refine the application migration project plans, they will be engaging with application owners to incorporate in the plans not only blackout periods but in-flight projects and other schedule information as well. This type of information is critical to developing a plan that is least disruptive to the end user community as well as the application development and maintenance staff. For additional information, please see Section 3 Work Plan.

7.B The migration order of the Commonwealth datacenters will be provided by the Commonwealth.

The Migration Strategy will address the transition of: Shared infrastructure elements, as appropriate; and Specific information Services. Disparate Agency application architectures and impacts to move to the new environment(s)

Unisys proposes a phased and comprehensive approach in assessing and implementing data center migrations and consolidations. This approach focuses on several key areas. First, we identify risk and risk mitigation. Unisys treats these moves like a controlled disaster – every action is planned, tested, and validated with documented, rehearsed back-out and contingency plans. Second, is the business and application centric approach, we take the time to detail business requirements and understand application interdependencies disruption to the business. Finally, we use a thorough and comprehensive program management methodology to making the data center migration as smooth and non-disruptive as possible and will not short-cut planning activities.

Phase 1, Data Gathering and Analysis, will concentrate on developing a complete understanding of the current application and infrastructure inventory. Based on this information Unisys will be able to identify the requirements that will be used as inputs to the overall migration plan. A master migration plan will be negotiated with business stakeholders strives to minimize potential impacts to normal business operations. Phase 1 will concentrate on the following key areas:

- Project and resource planning
- Application inventory and physical asset inventory
- System and Application Mapping including dependencies and interdependencies
- Identification of either assets or application that will be retired, moved or consolidated
- Identification of requirements such as outage windows, change control process, validation needs, site availability and capacity constraints
- Aligning the applications and systems into move groups or migration bundles
- Selecting migration strategies and technical requirements for each application
  - Based upon Application RTO and RPO
  - Physical moves, data migrations to new "seed" equipment at the target site are two examples of migration strategies
- Building of a Master Migration Schedule

The overall goals of Phase 1 are to discover the assets to be moved and gain consensus on a migration schedule.

Phase 2 is the detailed site planning that establishes target site readiness to host the moved assets.

Design of the new storage assets, verification of network and facilities plans, and a rollout plan for new assets are completed at this time. Key goals for this period include:

- Validate that target site build-out plans will meet the time and infrastructure needs for the asset migration
- Validate that new storage infrastructure is designed appropriately and in order
- Validate that new server roll-outs are timed appropriately to meet migration schedule
- Finalize all scheduling for transportation and OEM re-certification of assets

At the conclusion of Phase 2, Unisys and the Commonwealth will agree to initiate migration activities.

Phase 3 is the execution of the move plans. For each of the move groups, Unisys creates detailed task level runbooks that choreograph every action during the move. These plans are tested via table top exercises; the actual moves are coordinated and tested by Unisys and Ingalls' resources. Key activities include:

- Finalizing detailed night of move project plans
- Completing migration workbooks containing detailed procedures for application shutdown, server power-off/power-on, and other key technical activities
- Testing and rehearsal of move activities
- Final site visits to confirm target site is ready for asset move
- Disassembly, packaging, transportation and re-assembly of all assets
- Verification of proper functionality at target site

Phase 3 concludes with the Commonwealths' acceptance of the Data Center migration.

Unisyss Data Center migration methodology has been successful in dozens of large data center moves. Key to our success is a disciplined quality assurance program. Unisys will assign a subject matter expert not directly involved in the engagement to review the project at pre-determined points in time known as "QA Gates." The QA reviewer will look for issues that create risk in several areas with an emphasis on those that may jeopardize the migration timelines or pose a threat to maintaining normal business operations. The QA reviewer will meet with a set of Client stakeholders and project sponsors to review how well Unisys is meeting expectations. Chart in **Figure 3.3.2.1-5** summarizes the steps in the methodology and the estimated QA Gate timing.

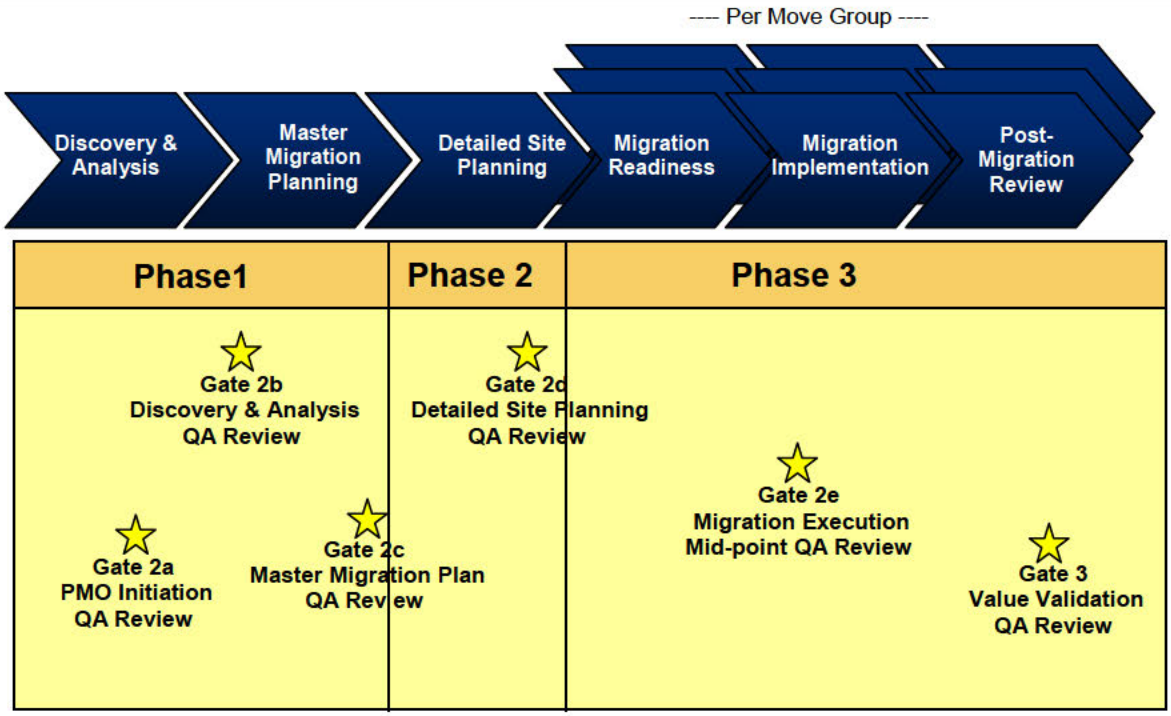


Figure 3.3.2.1-5 – Migration Phases

Once move groups are established the data center migrations will be accomplished using a variety of tools and techniques. The type of migration will be suggested by the Unisys Team but in all cases reviewed and agreed upon by the application owners.

The primary methods will be:

- Over-the-Wire – This is also known as P2P, V2V or Seed. This option will minimize the duration of the application outage required. For over-the-wire moves, seed hardware is first located in the receiving site and made production ready. A small application is placed on each server in the sending site to replicate the OS, application and application data onto the specific drives at the receiving site. Installation of the application is done during a monthly planned outage. An initial copy is executed soon after installation and sync copies are periodically executed leading up to the move event. During the move event, a final sync copy is taken after the application is shut down to verify all data and updates have been received in the new data center. Once the final sync is completed, the hardware in the sending data center is shut down and the application in the receiving data center is brought up. Once fully started, the application support team will execute the test plan created during the planning process. After a successful test, the test, the application owner will sign-off that it is ready for turnover to the end users. Using this option requires a shorter application outage. This method has low to moderate risk and a lower cost profile when utilized on assets with less than one year of expected life. As the age of the equipment increases so does the risk but the cost profile decreases due to the expectation of replacing the aging hardware.
- Lift and Shift –This option requires the applications to be shut down by the application support team, the supporting infrastructure will then be shut down and taken out of the racks, placed in shipping containers and transported to the new site via a dedicated professional moving partner. For applications that utilize shared storage, in most cases,

the data will be migrated over the wire using a data pre-application tool prior to the start of the event. In some cases, the project team may choose to ship data via tape. Once at the new site, the servers will be re-racked, cabled, and powered up according to the processes provided by the application support team. Once fully started, the application support team will be expected to execute the test plan created during the planning process. Once the team has successfully executed the test, the application owner will sign-off that it is ready for turnover to the end users. Using this option requires a longer application outage. This method has low to moderate risk and a low cost profile when utilized on assets with greater than one year of expected life. As the age of the equipment increases so does the risk and cost profile.

A third option exists which is a variation of the Over-the-Wire option.

- Seed with Greenfield – In this option, seed hardware is installed in the receiving data center, the operating system is installed directly on the hardware, the Application is installed and then the application's data is copied. Once fully started, the application support team will execute the test plan created during the planning process. Once the team has successfully executed the test, the application owner will sign-off that it is ready for turnover to the end users. Using this option requires a shorter application outage but presents a high risk profile and a higher cost profile.

In all cases, minimal changes are made to the environment to minimize the risk and expedite resolution of any incidents discovered during the migration events.

Early in the planning process, the Project Managers will work with the Application Owners to identify and agree on the migration method for each infrastructure device supporting an application being migrated. In most cases, shared services infrastructure devices such as Storage and Virtual Machines (VM) will be migrated over-the-wire to allow for flexibility in move package creation.

7.C The Migration Strategy must also address the following: Cost/Benefit for the Agency, Risks and Risk Mitigation Plan

Data Center Migrations employ three primary strategies: Over-the-Wire, Lift and Shift, and Seed with Greenfield. These strategies are defined in the previous section. Migrations may choose to employ one or all three or even combinations of the three depending on the application owner's priorities. A lift and shift strategy provides a low cost solution as no new hardware is required and labor expenses are reduced as compared to the other options. It does increase the risk due to the potential for damage during transport as well as the extended outage that would be required should a fallback need to be executed. Over-the-wire migrations increase the cost over lift and shift due to the requirement to purchase and install new hardware but are still less costly as compared to Seed with Greenfield. The risk level with Over-the-Wire is minimized by tools like [redacted] that will move bit-by-bit storage from the sending data center to the receiving data center including the operating system as configured and the application as configured.

The most risky and highest cost migration strategy is Seed with Greenfield however in some cases, this may be the best approach. For example, an application that requires an upgrade may choose this strategy if the application owner previously had planned an upgrade in place. See **Figure 3.3.2.1-6** below for cost and risk comparison for the options.

Migration Strategy	Risk Level	Cost Level
Over-the-Wire	Low	Medium
Lift and Shift	Medium	Low
Seed with Greenfield	High	High

Figure 3.3.2.1-6 – Migration Strategy Cost/Benefit and Risk Table

8 Critical Transition Plan Success Factors

8.A Identify mandatory requirements and critical success factors that will have a direct impact on developing a successful transition plan

Offeror must describe the 3-5 characteristics, conditions, or variables it believes will have a direct and critical impact on the effectiveness, efficiency, and viability of the Offeror's solution.

Critical to the success of any endeavor is the buy-in of participants. Large transition efforts such as the one the Commonwealth has initiated do not achieve the desired goals without cooperation from all levels of the organization. The list below are a few of the key characteristics and mitigation strategies:

- Resistance – Passive and Active resistance can both be roadblocks to success due to delays and misinformation.
  - Mitigation Strategies:
    - Include influential resources in the project. It will be important that we include not only resources who have specific technical skills but also a few who have influence over others in the organization. Make them a part of the solution.
    - Clear and directed communications
    - Gain buy-in from Commonwealth leaders via Steering Committees
- Clear scope and direction
  - Mitigation Strategies:
    - Include key thought leaders in planning process
    - Communicate in terms appropriate for the audience
    - Develop a strong, well thought project schedule and execute to it
    - Identify risks and plans to mitigate
- Appropriate Staffing
  - Mitigation Strategies:
    - Gain leadership's support for prioritization of project
    - Look across all organizations to find the right person for the right job at the right time

8.B Offeror must describe its approach to mitigating risks and ensuring these critical factors are successfully addressed.

Communications amongst stakeholders is the key to identifying and mitigating risk. A key component of the Program and Project plans will be maintenance of a risk register. Each project will maintain a risk register and actively work with stakeholders to identify potential risks and mitigation strategies. Within each weekly review meeting, the project managers will assess the current risk register with all team members for accuracy and input. It is the project manager's responsibility to assign mitigation task to team members and confirm progress.

9 Transition Timeline

9.A Create a Transition Timeline that outlines the overall timeline starting at effective date and continues through delivering transition Services for each of the targeted datacenters.

Any critical milestones identified must be included in the Transition Project Plan.

Figure 3.3.2.1-7 below shows a high level timeline of projects and activities as compared to the Commonwealth's Milestones. The Unisys Team is uniquely able to accomplish this accelerated timeline as a result of the close relationship our team has delivering current and prior projects with the Commonwealth. We save time on the DPH and [redacted] migrations by skipping over the major learning curve of a vendor that is not currently supporting Commonwealth environments.

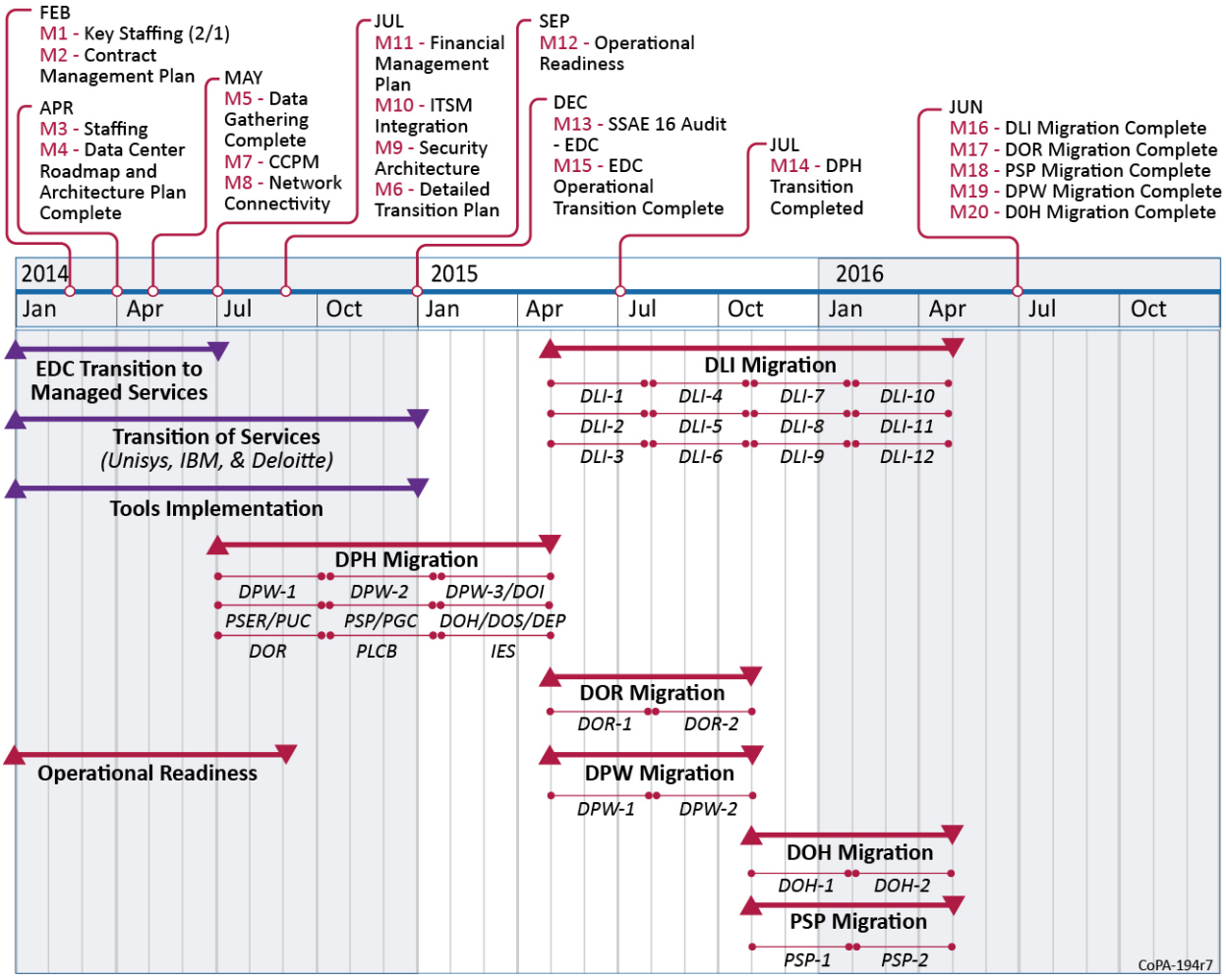


Figure 3.3.2.1-7 – Transition Program GANTT Chart

9.B Offeror must describe the overall timeline from the start of pre-Transition activities through the point at which the Offeror expects it will be delivering predictable, repeatable Managed Service Results that meet the requirements of the RFP.

The schedule must include a description of the critical milestones related to Transition efforts for each targeted Commonwealth datacenter.

The purpose of the Transition Program is to transform how the Unisys Team provides services to the Commonwealth today in order to broaden the scope and deliver high quality services in the future. Taking a top-down view of the program, it will be organized into three major categories of activity - Transition, Migration, and Program Management.

Transition activities center on the transformation and implementation of policies, processes, procedures, tools and people required to deliver services to the Commonwealth.

These activities are further broken into projects such as Account Team Set-up, Tools Implementation and Enterprise Data Center ([redacted] Transition to Managed Services. Very early in this process the Program Management Office will play a key role in establishing direction for tasks within each tower. Unisys has designed toolsets to support the implemented processes. This set of tools will greatly enable and facilitate high quality service delivery as well as facilitate improved sharing of information. Concurrent with the process and tools implementation, activities will occur to perform knowledge transfer from the existing [redacted] contract to the Managed Services agreement. In many cases, this knowledge transfer required for this transformation will occur by moving staff from the current team to the new team, providing a strong base of knowledge. Careful consideration will be given to which team members and how many will participate directly in the [redacted] Transition Activities and what positions will require backfill so as to continue to provide the high level of service the Commonwealth currently receives.

Migration. At Unisys we believe focus must always be on the application portfolio. Within the data center migration (DCM) activities, there are three major groupings.

- First, Operational Readiness provides application, infrastructure, and processes required to host the applications. Within these tasks, the Unisys Team will create detailed designs and implement the Wide Area Network (WAN), Local Area Network (LAN), Storage and Backup infrastructure, Monitoring, Tools, Server Management, Dashboard and Information Technology Service (ITSM) infrastructures.
- The second major grouping is Data Center Planning, which runs in parallel with Operational Readiness. Within the planning framework, the DCM team will be gathering and analyzing information gathered electronically as well as in meetings with the agencies and their application owners. Draft Move Packages created based on the information gathered and results of the analysis will show related applications which may have latency dependencies, schedule restrictions, size, complexity and number of applications. A typical Move Package will not exceed 100 servers and 6 applications.
- The last grouping is to execute the migration of the applications. The building of detailed plans will be a highly collaborative effort between the Commonwealth and the Unisys Team to build detailed plans. Each of these projects will have duration of approximately 3

months and will include development of test plans, detailed technology, and migration plans developed down to the minute by minute tasks required during the migration events.

Program Management drives the successful transition of all Commonwealth IT services from their internal Commonwealth IT organizations and Data PowerHouse (DPH) contract to this proposal's new contract services, organization, facilities, processes, deliverables and structure.

Figure 3.3.2.1-7 above shows the relationship of the Unisys Team's proposed project schedules to the Milestones provided by the Commonwealth. In every case the Unisys Team will meet or exceed the milestone delivery dates requested by the Commonwealth.

10 Infrastructure Element Transition Plan

10.A Create a generic Infrastructure Element Transition Plan that may be readily adapted to accommodate specific infrastructure element transitions.

Although all Transitions are similar, they are each unique. The Unisys approach to transition is based on grouping of business services, applications, and underlying infrastructure elements into logical Move Packages. **Figure 3.3.2.1-8** is a high level project schedule for a generic move package transition that needs to be executed in order to successfully transition and consolidate the Commonwealth's data centers. During the planning for each project, the project schedule will be further broken down to manageable tasks as suggested the Project Management Institutes' guidelines and scheduled specifically to the needs of each commonwealth project.

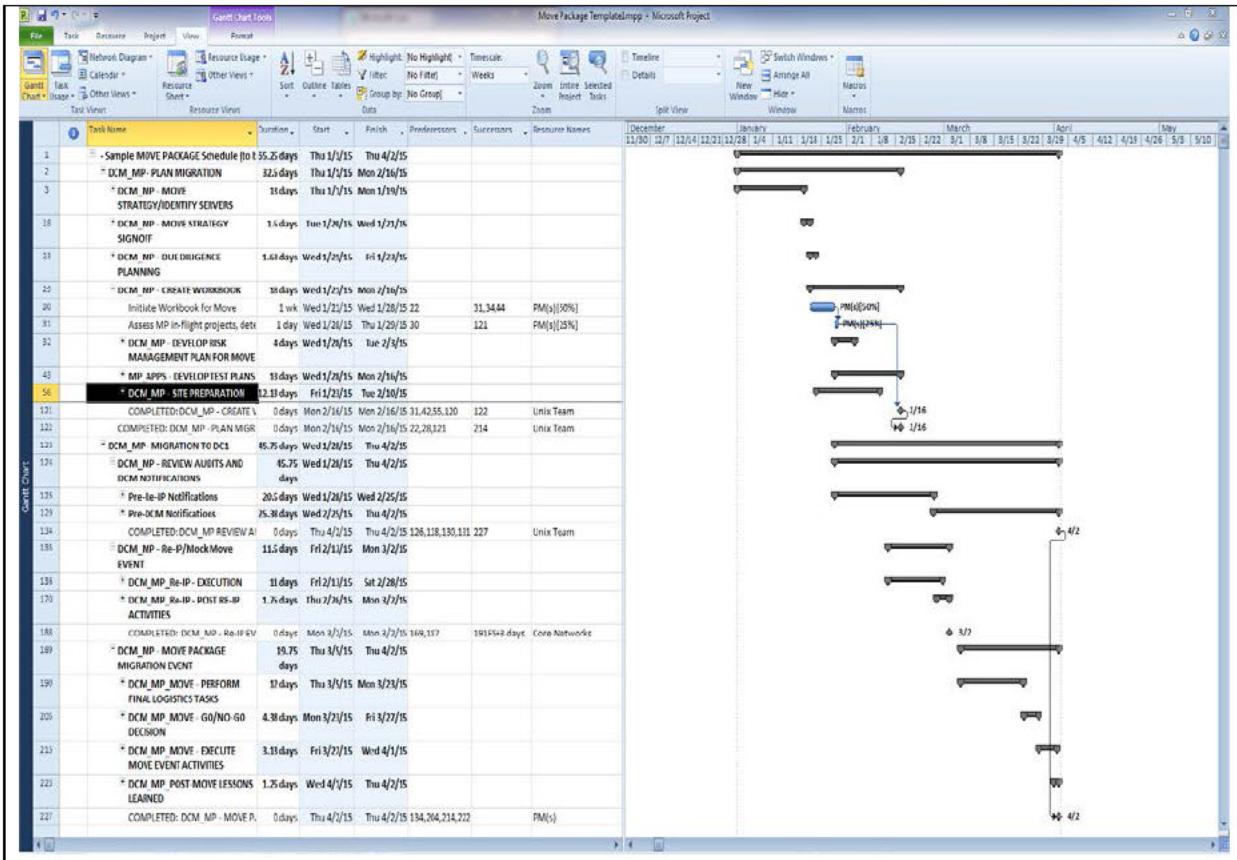


Figure 3.3.2.1-8 – Sample Application Migration Plan

10.B Create a prospective Infrastructure Element Transition Plan. Appropriate [redacted] DPH and other Agency Datacenter hardware elements may be re-purposed wherever possible.

Offeror must describe a realistic Transition Project Plan to transition the Commonwealth's datacenters to the proposed architecture.

As the Commonwealth and Unisys Team's work together developing and refining the detailed transition plans seen in **Figure 3.3.2.1-8**, hardware elements will be identified which will continue to have significant useful life remaining.

The Unisys team has proposed a realistic Transition Project Plan, as shown in **Figure 3.3.2.1-7** above, which accounts for the transition of Commonwealth's data centers and aligns with the milestones provided by the Commonwealth. See **Figure 3.3.2.1-7** – Transition Program GANTT Chart. This plan is described in detail in Schedule F, Section 3.1.2 "Work Plan Timeline" and Section 3 Attachment 9 "Schedule M: Detailed Transition Plan".

11 Infrastructure [redacted] Transition Plan

11.A The [redacted] Managed Services datacenter assets must be managed and maintained by the Offeror until they are transitioned to the Offeror's managed Services.

The current maintenance contract for the [redacted] servers is scheduled to expire on June 30, 2014.

Offeror must describe its transition approach to address the transition of operations and management of the [redacted] infrastructure from the Commonwealth to the Offeror's support Services and how it intends to address the server maintenance expiration issue.

Unisys is in a unique and strong position to execute the Transition for the Enterprise Data Center due to the current support provided by Unisys staff. This will minimize the turnover and mining of information required and eliminate much of the learning curve often associated with a Transition of Services. Transition services for the Enterprise Data Center will be the primary focus of two projects within the Commonwealth Transition Program.

The Transition of Service project will focus on gathering information and producing documentation on the current environment and processes at each data center, executing a Best Practices Assessment to identify gaps and developing a plan for each gap identified. An example of a gap during transition is the Best Practice of procuring maintenance on all devices. A complete physical and automated inventory identifies all devices in the [redacted] When the inventory is complete, the Unisys Team will analyze the information gathered along with other available information to develop a Technology Refresh Plan. As part of the Technology Refresh Plan, we will identify those infrastructure elements that will need maintenance until they are refreshed and develop an approach and estimated cost for each.

In addition, a second parallel and related project will focus on implementing a component based operating model to provide a high degree of timely and detailed support for the [redacted] environment.

12 Application and Infrastructure Migration, Example

12.A Create, manage and execute an application / infrastructure migration plan.

Offeror must describe solution and approach to meet this requirement. Offeror must provide at least one sample where it has successfully migrated application and hardware.

Attachment F-12 is an example of an Application Migration plan developed for the Commonwealth Consolidation Program, which shows a high level set of tasks that will be executed in order to migrate the Commonwealth's applications to the new data centers. The Unisys Team has planned, managed and executed many similar application migration projects including the American Red Cross and Nutreco.

12.B The Offeror has the primary responsibility for planning and executing the transition of infrastructure elements, with support of Commonwealth technical and business support staff.

The Unisys TPMO will be responsible for developing the project plans for all projects within the Transition Program. These project plans include input from the Commonwealth technical and business support staff and will be reviewed and approved by the Commonwealth. A detailed explanation of the Transition Program can be found in Section 3.1.2 and attachment 9 of Section 3.0 "Schedule M: Detailed Transition Plan".

12.C The Offeror must provide adequate tools and techniques for moving and migrating Commonwealth data to the new target storage environment. Offeror must describe its proposed tools and techniques for moving and migrating Commonwealth data to the new target storage environment.

Through a series of data gathering and analysis activities, the Unisys Team will partner with the Commonwealth to obtain asset data, locate utilization information, and map current to future state infrastructure to meet the Commonwealth's requirements. Below you will find

descriptions of analytic, planning, and risk reduction processes and tools for the transition activities.

Data Gathering and Analytics - Discovery

Data Gathering and analytics, or as they are sometimes called, discovery, activity provides the basis for verifying the current hardware and application inventories for the Commonwealth's current environment which provides the baseline data to be utilized to validate future state infrastructure and transition strategies. The data gathered during this process is crucial in developing the move groups and strategies for the transition phase. Move groups are logical groupings of business services, applications, and underlying technology that will be migrated from the current to future state. The data gathered will also provide the Commonwealth with additional knowledge of its environment, useful for planning future IT needs.

The Discovery phase starts with the collection of the currently available application and infrastructure inventory data. The Discovery activities are complete when all of the data necessary to develop a detailed plan for the migration is collected, reviewed and agreed upon with representatives of the Commonwealth and the agencies. The primary deliverable of the Discovery phase is a current and complete inventory. The inventory contains all of the components in the source data center, mapping to the applications that they support, and a list of stakeholders (application owners, support staff, and test staff).

Having a current complete hardware/software inventory is one of the prerequisites for successful migration planning and management. Validation consists of comparing the current Commonwealth supplied inventories to a list of inventories gathered during discovery and analyzing the gap.

Unisys will utilize a combination of automated discovery tools and questionnaires, interviews, and workshops to validate the hardware, software, and application inventories. The Unisys suite of data collection tools is built upon the data collection requirements. The tools use different access methods that consist of, WMI (Windows Management Instrumentation) access, secure log-on (SSH), SNMP, and network switch Span Port data. The toolsets will be reviewed with the Commonwealth; testing will be performed prior to general network deployment; the initial round of collected data will be reviewed with the Commonwealth and agency technical staff and validated for accuracy before approving the toolset.

Validation and Discovery of Current Applications Assessment – Atrium Discovery and Dependency Mapping (ADDM)

Unisys will utilize a combination of interviews, workshops, questionnaires, and automated discovery tools in the application discovery process to acquire data about applications and their dependencies. Unisys will conduct a review of the data provided with the RFP Exhibits to determine move strategies.

Application Discovery starts with the identification of the applications, underlying infrastructure and business requirements that the application supports. Using a combination of automated application dependency tools such as [redacted] and workshops Unisys will build a list of applications and dependencies to plan and support the migration activities. All of the application discovery information will be stored in the [redacted]. The CMDB will capture the assets for tracking and updating as they

migrate to the future state environment.

After the initial ADDM discovery, Unisys will capture the discovered information in an Application Questionnaire distributed to the agency application stakeholders in order to collect additional information. The information that will be validated and updated through the Application Questionnaires includes: business constraints, availability requirements (Service Level Agreements (SLAs)), maintenance windows, performance requirements, current functional baseline, upcoming releases, mapping to infrastructure, databases, internal / external users, application to application dependencies, SAN / database connections, and test plans. We will identify applications that could be decommissioned prior to the migration.

The ADDM tool allows for automated discovery of physical and virtual servers, applications, and network devices—and their interdependencies—to determine the move groups and strategies to be utilized in the transition activities. The output of the application discovery process is a clear and concise picture of how the IT infrastructure supports the applications and the overlying citizen services.

An essential step in providing low risk transition processes is the development of application maps that show the relationships among the applications and the underlying IT infrastructure components that support services. Some of the challenges in developing these maps include dealing with the complexity of multi-tiered applications and continuous change in the IT infrastructure. The use of ADDM will allow the Unisys Team to work with the Commonwealth application owners to map applications to their underlying infrastructure and define business services. Once input and validated in the CMDB, the team will add other information, such as users, policies, deployment blueprints, and service level key performance indicators (KPIs) to create a complete picture of the application dependencies which will be utilized during move planning.

Figure 3.3.2.1-9 below shows a sample Application Dependency Diagram provided by ADDM.

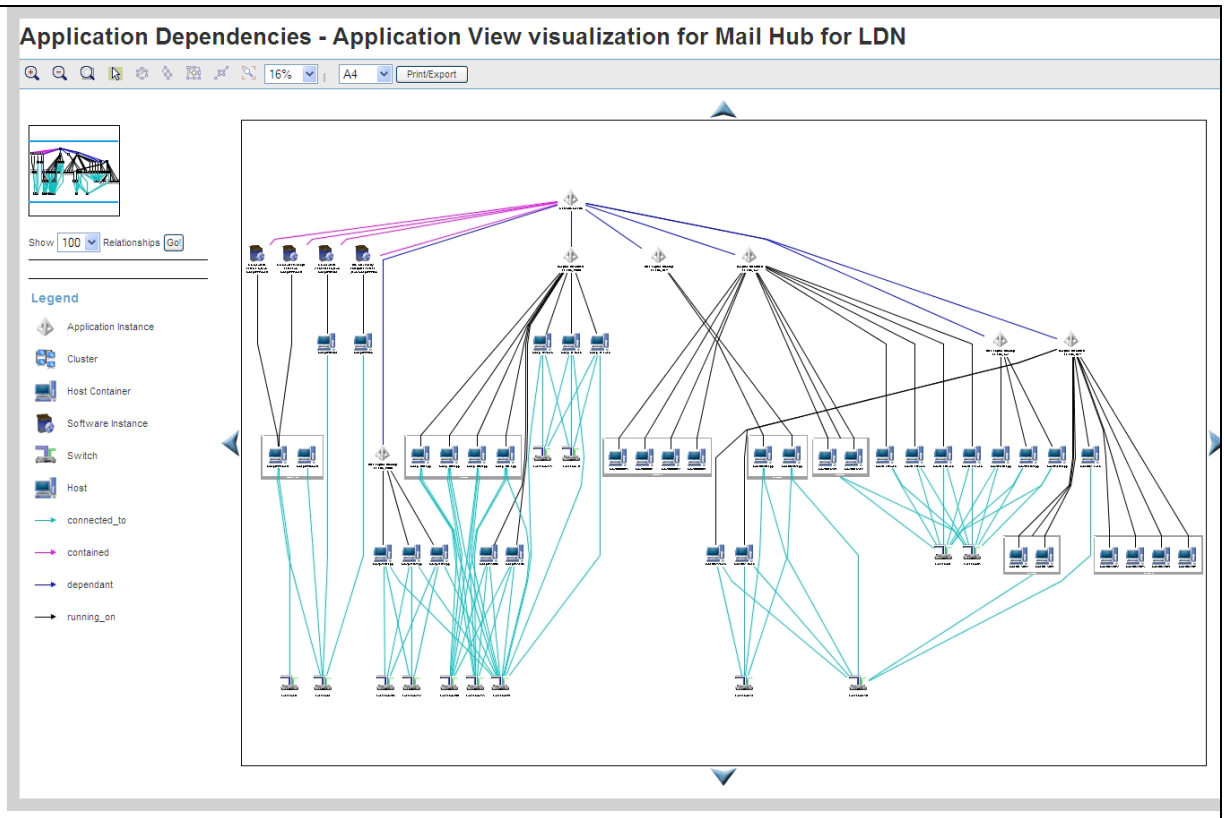


Figure 3.3.2.1-9 - Sample Application Map

The application dependency mapping for the Commonwealth will be based on the following steps:

1) Automatic discovery and dependency mapping

   a. An initial map of the dependencies and relationships of the applications is created. While providing an initial view of the application environment a complete picture is typically not possible without interaction with the application owners.

2) Analysis and reporting

   a. Reports are generated based on the initial application dependency map.

3) Collaboration

   a. The initial maps and reports are reviewed with the application owners and are validated as to the accuracy and completeness of the application map. Based on this review the maps are changed as appropriate.

4) Continual update

   a. As the IT infrastructure is constantly changing within the Commonwealth the

application maps are adjusted each time a change is made to the IT infrastructure.

The ADDM data collection tool is deployed within the [redacted] as part of their roll out of the [redacted] In **Figure 3.3.2.1-10** below you will see the ADDM Architectural diagram describing how these tools will work together.

Figure 3.3.2.1-10 – ADDM Architectural Diagram

After completion of the Discovery activities and creation of the Move Groups, the Unisys Team will utilize their proven solution to migrate the current workloads to the new environment. This solution has been proven in the Commonwealth and other clients and has reduced risk and minimized downtime. For both the physical to physical migrations (P2P) and virtual to Virtual (V2V), Unisys will utilize [redacted] provided by NetIQ corporation.

Physical to Physical and Virtual to Virtual Migrations – [redacted]

[redacted] is a workload mobility solution that automates the process of moving server workloads over the network between physical servers, virtual hosts and image archives. [redacted] decouples workloads from the underlying server hardware and streams them to and from physical or virtual hosts—all from a single point of control. Using [redacted] Unisys has been able to capture, test and migrate mission critical workloads from physical to virtual, physical to physical and virtual to virtual environments.

[redacted] provides the ability to migrate Windows and Linux workloads from and to disparate hardware platforms removing hardware dependent device drivers and utilities as part of the

migration process. Using a centralized migration control server migrations are tested and then scheduled for final cutover in an automated manner. [redacted] will automatically configure any server workload to operate on a new target environment making driver, kernel and other necessary changes as part of the process. [redacted] provides multiple replication types supporting both dynamic transactional workloads as well as more static environments using synchronization technologies.

Using [redacted], Unisys will establish physical to virtual, physical to physical and virtual to virtual transition environments that will allow multiple migrations to occur supporting the defined Move Groups within the Commonwealth. These environments will allow Unisys to capture the source environments within the [redacted] repository and to test the migrations. Once testing is complete automated workflows are created for each Move Group to ensure that the final migration process is completed against each move group. These workflows will accelerate workload migration activities and reduce manual errors using automation. Automation provides a process of configuring migration jobs and moving, copying and deploying workloads repeatable and reduces risks during migrations.

To reduce the downtime associated with workload relocation Unisys will utilize the Server Sync function within [redacted] Server Sync will allow the initial transfer to the target site or host, testing of the workload in the new location, and then perform a final sync before cutting over the workload—all while continuing to run the source. **Figure 3.3.2.1-11** below provides a view of the architecture that will be utilized in the implementation of [redacted]

Figure 3.3.2.1-11– [redacted] Architectural Diagram

12.D The Offeror must ensure that critical applications are not decoupled from key infrastructure components causing system latency.

The Unisys Team will collaborate with the Application Owners to identify applications affected by the latency. Using the tools described above in 12-C, efforts will be made to group closely

related applications in the same move packages. In the event application owners are unsure of relationships, The Unisys Team can offer an Application Performance Impact Assessment (APOC) which is intended to identify risks and mitigations.

13 Generic Information Service Transition Plan, Example

13. A Offeror must describe its proposed tools and techniques for moving and migrating Commonwealth data to the new target storage environment.

As described in Section 12.3 above, the Unisys Team will use a combination of tools and techniques to migrate data from the existing data centers to the new data centers. Please see response 12.C for an explanation.

Offeror must outline a prospective Information Service Transition Plan to take over support of migrated Commonwealth systems and applications. Offeror must provide at least one sample where it has successfully completed application and hardware migrated.

Unisys has created a generic Information Services Transition plan which can be viewed in its entirety in Section 3.0, Schedule M.

As referenced in Section 4.5, Unisys has recently executed similar application migrations including application and hardware migration at the American Red Cross.

14.A Meet with Commonwealth to produce and execute specific Information Service Transition Plans.

As described above in requirement 13 and Section 3.0 Work Plan; the Commonwealth Data Center Transition Program will have many touch points into the Commonwealth's IT Organizations. This includes the Transition and consolidation governance plan outlined in Schedule B Governance and depicted in **Figure 3.3.2.1-12** below, as well as active participation by Commonwealth subject matter experts who will be needed to providing technical, business and scheduling input for the various projects.

The Program Steering Committee will be comprised of senior leaders from both the Commonwealth and the Unisys Team. This committee will be responsible for approving strategic direction, decision approvals, significant issue escalation and communication with the senior leaders within the Commonwealth Agencies and Bureaus and the Unisys Team respectively.

Each project will have an oversight steering committee assigned as well. The exact make-up and size of the steering committee will depend on the project but in general will be headed by one of the Deputy Transition Executives and include the Project Manager, Application Owners and as appropriate, an agency director's representative. These committees will be responsible for providing strategic direction for each project, decision making based on agency and customer requirements, resolution of project issues and communications within the agency/customer set.

Figure 3.3.2.1-12 – Transition Governance Model

14.B Select cut over windows that minimize system unavailability and coordinate approval with the affected agency.

Unisys will work with the Commonwealth and Agency representatives to determine the appropriate timeframe within which an agency's applications will be migrated. Agency applications will be allocated to move packages based on information gathered during the Data Gathering portion of the transition and known blackout periods. As move package projects are initiated, the project managers will work with application owners to identify the best times of the day, week and month to execute testing and the migrations. If a particular application has unique requirements that do not fit the initial packages, Unisys will work with application owner's to identify another work package to which to move the application.

14.C Communicate to the Commonwealth cut over date and times.

Unisys will work with the Commonwealth and Agency representatives to identify the appropriate communications, method and timeframes. In general, these communications will occur approximately thirty, seven and two days prior to each major migration event such as a re-IP, mock move or actual migration event.

14.D Setup a special call number and support staff to take calls concerning the migration, these Services must be made available to transitioned users until the transition is officially signed off as completed. Offeror must describe solution and approach to meet this requirement.

During migration events, The Unisys Team will establish "war rooms" to monitor progress of the events and allow collaboration amongst team members. A "meet-me" or "bridge" line will be established and manned throughout the duration of the event. All critical members of the migration team will be present on the line until released by the project manager. The event is not complete until all application owners have provided a verbal signoff on the bridge.

14. E Offeror must provide at least one relevant example from a prior engagement, in which it was engaged, that is similar to the needs of the Commonwealth.

Recently Unisys executed a similar application migration project at the American Red Cross. For

more details on this effort, please see Section 4.5.

15 Testing, Business Acceptance, and Fallback Plans, Examples

Work with Commonwealth to create testing, business acceptance and fallback plans.

Offeror must describe solution and approach to meet this requirement.

Offeror must provide at least one relevant example from a prior engagement, in which it was engaged, that is similar to the needs of the Commonwealth.

One of the most important tasks of any transition plan is creating a full and robust test plan. The Commonwealth application owners will be expected to work with the application support teams to develop a test plan for each application as required by the Commonwealth. This test is executed prior to any significant activities to create a baseline of expected results and application performance. The results are compared to the test execution after each significant activity to validate acceptable results. The application owners confirm the plan is complete and executable. In addition the application owner is expected to use the results of the test to sign off on acceptance of the event.

The hour-by-hour (HxH) detailed plans that are developed for each application will include tasks required to fall back to the existing data center.

This level of planning and risk mitigation is standard in migration projects. Recently Unisys executed a similar application migration project at the American Red Cross. For more details on this effort, please see Section 4.5.

16 Service Management System Transition Approach

Offeror must transition all agency system management platforms currently in place to the Offeror, consolidating all system management responsibilities.

Offeror must describe solution and approach to meet this requirement.

The Offeror must make available all system management platforms and tools that are currently supporting the Commonwealth infrastructure.

The Unisys approach will be to transition existing system management platforms currently in place (e.g., SCOM in EDC and DPH) into the [redacted] event management and single pane of glass platform for system management to accelerate Agency Transition into the target data center platforms. The Unisys System Management Team will migrate these current systems management tools to the standards as outlined in the Site Operations Plan and toolsets and summarized below. By standardizing on these ITSM/ESM tools, the Commonwealth benefits from consistent standards and reduction in costs as toolsets that exist today in the agencies are consolidated onto one consistent and standard set of tools for systems management. If the Commonwealth does not desire to migrate systems management to the standard platform Unisys has proposed Enterprise Services Catalog options (e.g., SCOM) that will be available for the Commonwealth to select as alternatives to the standards.

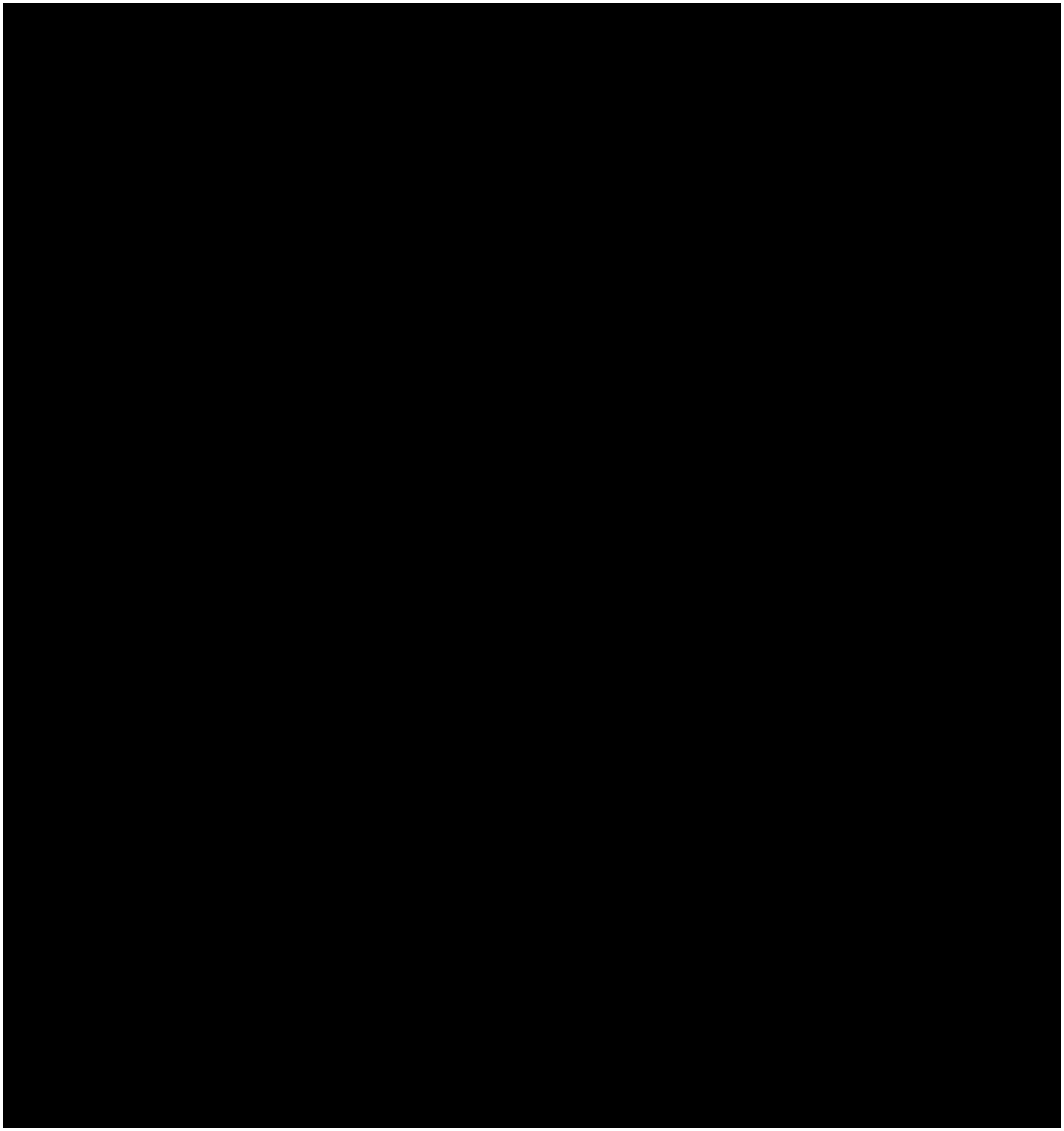
For applications outside of the DPH and EDC, the systems management tools will be migrated at the same time the agency's applications are migrated to the new data centers.

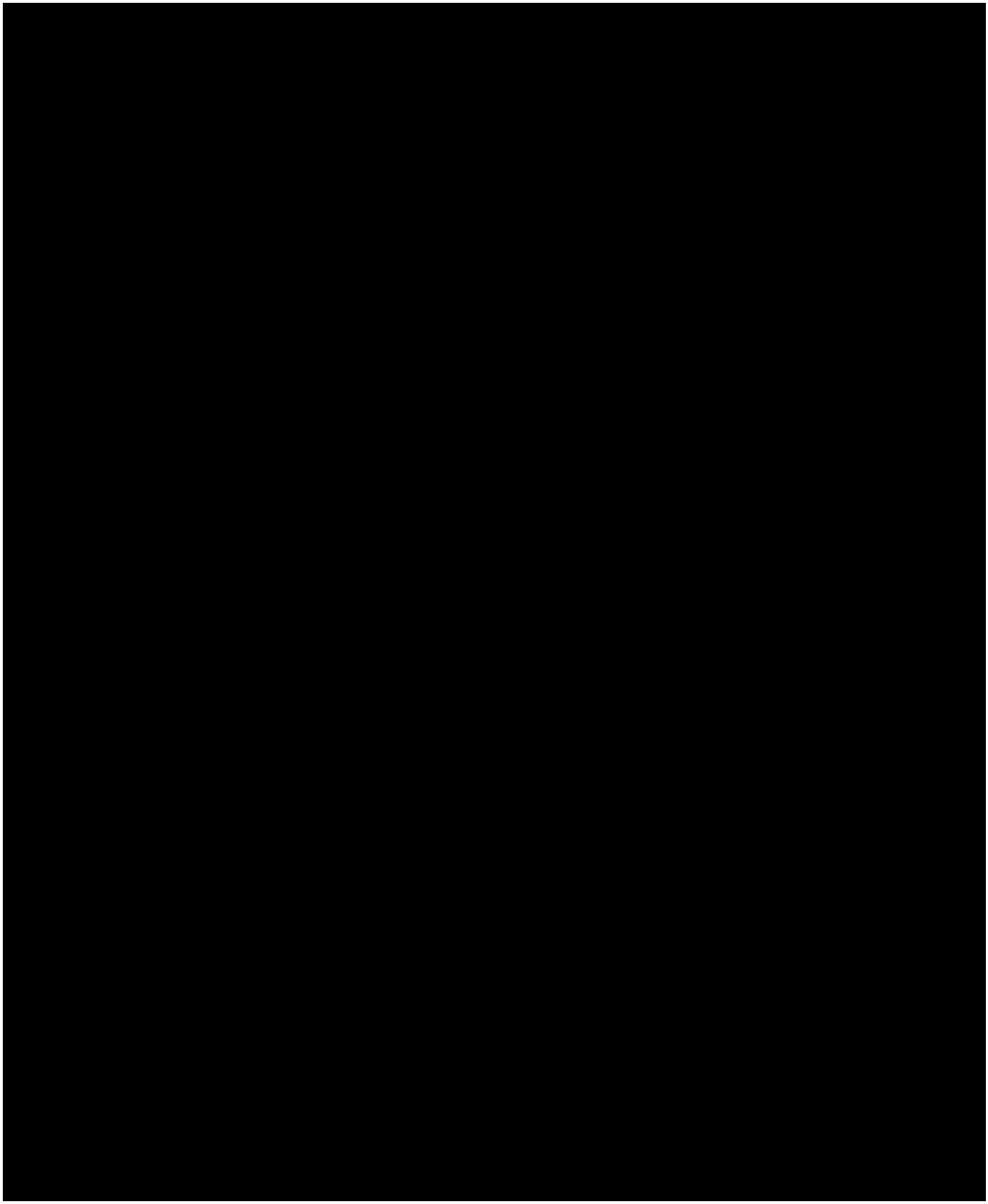
The following are the standards for ITSM/ESM systems management that Unisys intends to migrate to support lower costs and more consistent systems management after agencies are migrated.

Unisys will implement, support, and operate a comprehensive and integrated Information Technology Service Management (ITSM) architecture dedicated to the cross functional process support for all services provided to the Commonwealth for this contract. The proposed ITSM Architecture, shown in **Figure 3.3.2.1-13**, will provide an effective and efficient operational platform to support the Commonwealth's agencies application infrastructure for the following ITIL V3 (Information Technology Infrastructure Library) Service Management Processes.

Figure 3.3.2.1-13 - Proposed Unisys ITSM Integrated Architecture

The Integrated ITSM Management Platform software tools are summarized in the **Figure 3.3.2.1-14.**





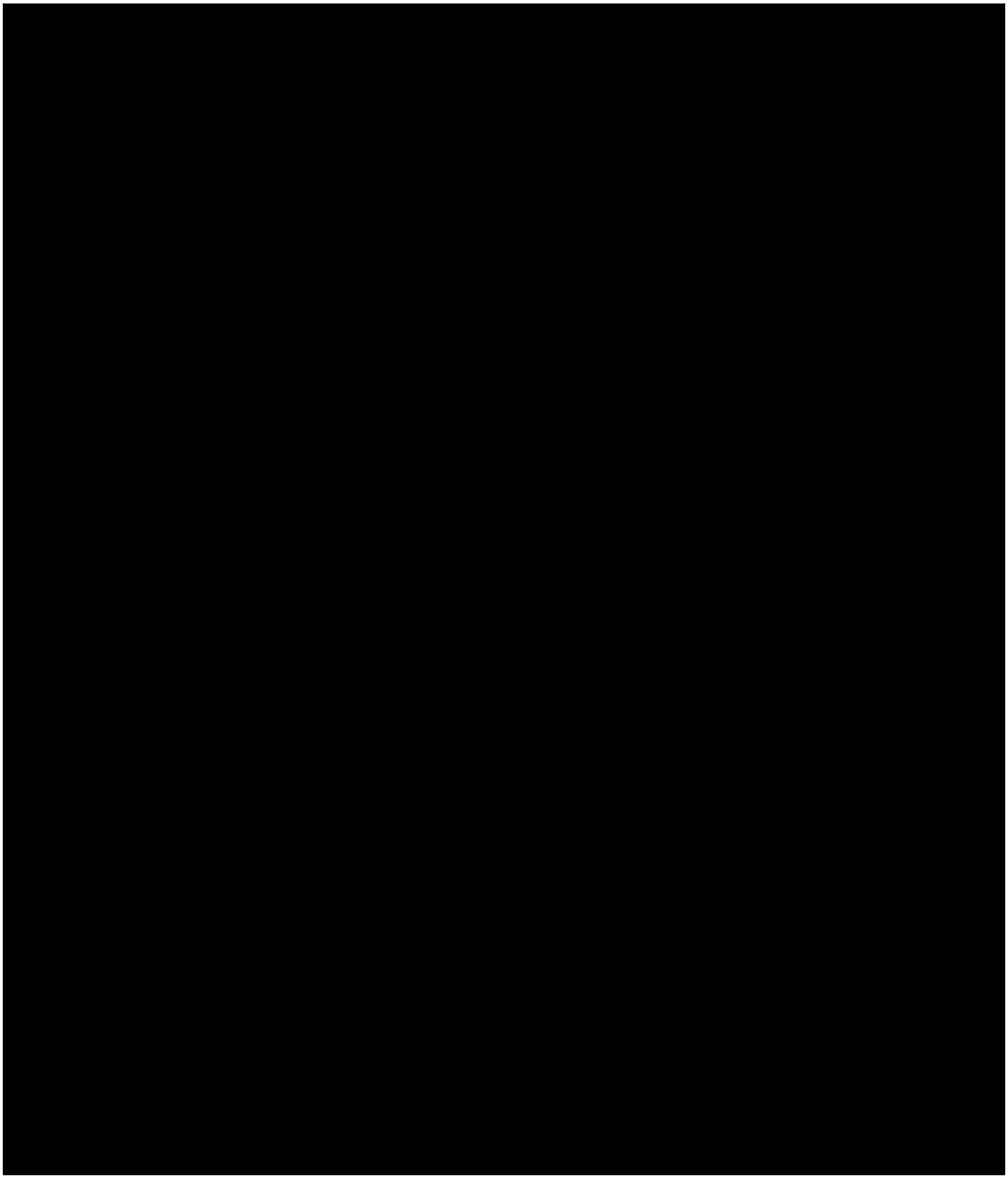
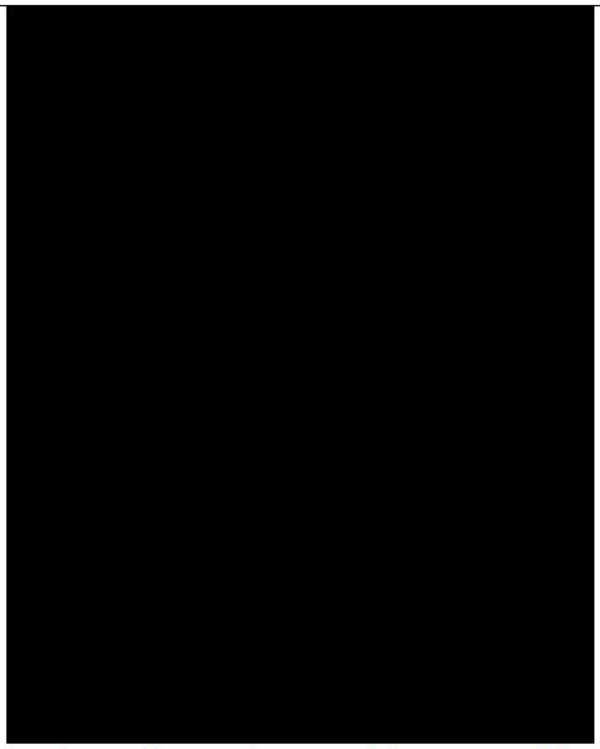


Figure 3.3.2.1-14 - Unisys ITSM Tools

Unisys will assess the Commonwealth's current ITSM toolsets during transition. Assessment results determine which tools will be supported within this overall target ITSM proposed architecture, replaced, or eventually migrated to the target environment ITSM tools shown in **Figure 3.3.2.1-14** above. Some of the tools that will be evaluated and assessed during transition include:

- [redacted]



The resulting architectural decisions will be reviewed and approved by the Commonwealth's agencies. Some identified tools will continue to offer the functionality they currently provide, but will be integrated into the overall ITSM proposed architecture.

ITSM Processes

Unisys is proposing an integrated set of ITSM processes to support the Commonwealth's requirements and goals for:

- ITIL V3
- ISO20000
- Integrated service processes in support of the Commonwealth Agencies and application teams from a service level driven perspective
- Efficiency and Effectiveness of service operations across the Commonwealth's agencies.

Service Operations

Service Operations involves the day-to-day operations management of Information Technology (IT) services. It includes guidance for achieving effectiveness and efficiency in the delivery and support of services that offer value for the customer and for the service provider. Service Operations provides a framework for maintaining stability in service operations that allow for changes in design, scale, scope, and service levels. Managers are provided with knowledge that facilitates making better decisions in areas such as managing the availability of services, controlling demand, optimizing capacity utilization, scheduling operations, and correcting problems.

Service Operations can be viewed as the factory of IT. This implies a close focus on the day-to-

day activities and infrastructure to deliver services. Management of infrastructure and operational activities supports Service Operations. Within the Commonwealth, this means satisfying service requests through the Request Fulfillment process, the handling of service interruptions through the Incident Management process, eliminating recurring incidents through the Problem Management process, and keeping a vigilant eye on the environment through the Event Management process. The processes are described below.

Management Portal

The Management Portal facilitates a common presentation across the Commonwealth's IT environment. The portal provides an integrated high-level dashboard for overall performance, Service Level Agreements (SLAs), and detailed metrics. Secure access is provided for content-based user-specific roles and permissions.

Because of the architecture's flexibility, information can be captured from any type of source such as reporting databases, monitoring tools, or even spreadsheets. The assembly layer of the solution allows data from multiple sources to be combined into an aggregated presentation to streamline information viewing.

The Management Portal is depicted in three diagrams – **Figures 3.3.2.1-15** Management Portal – Administrator Access, **Figure 3.3.2.1-16** Management Portal – User Access and **Figure 3.3.2.1-17** Management Portal – Service Dashboard.

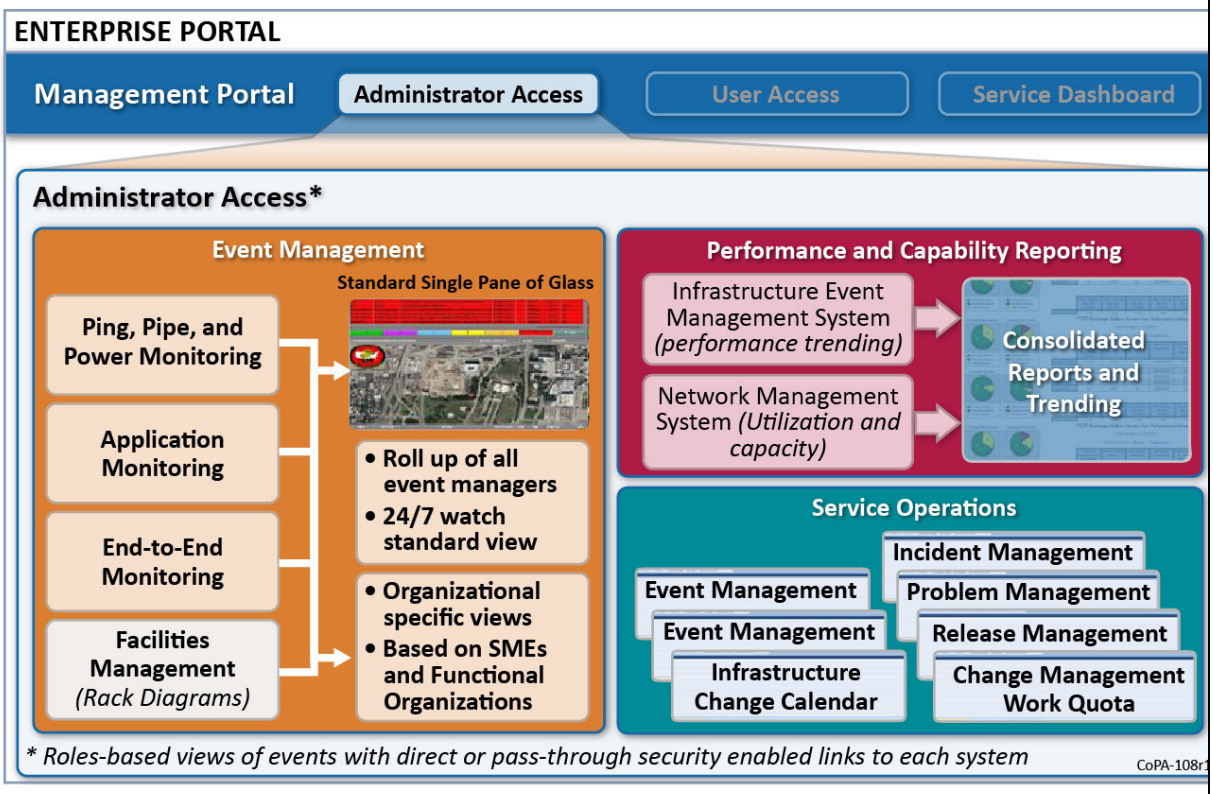


Figure 3.3.2.1-15 - Management Portal Example – Administrator Access

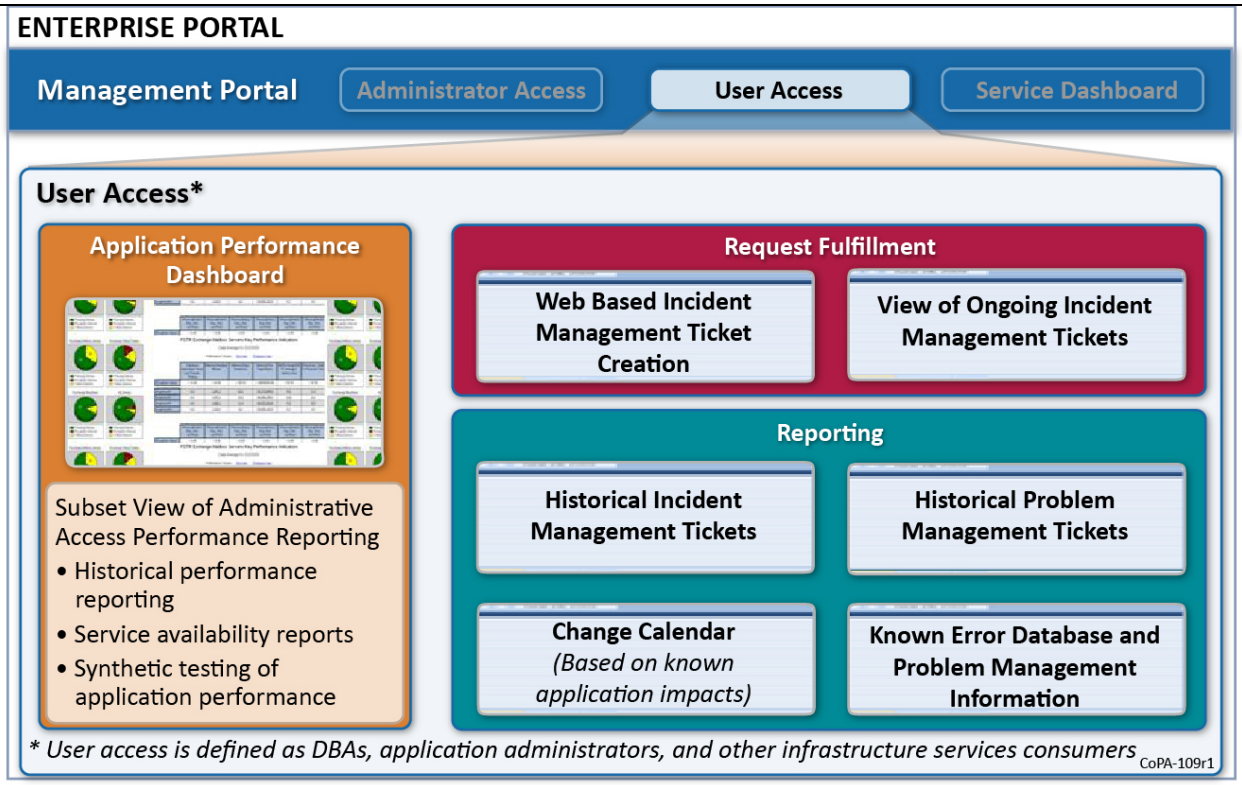


Figure 3.3.2.1-16 - Management Portal Example – User Access

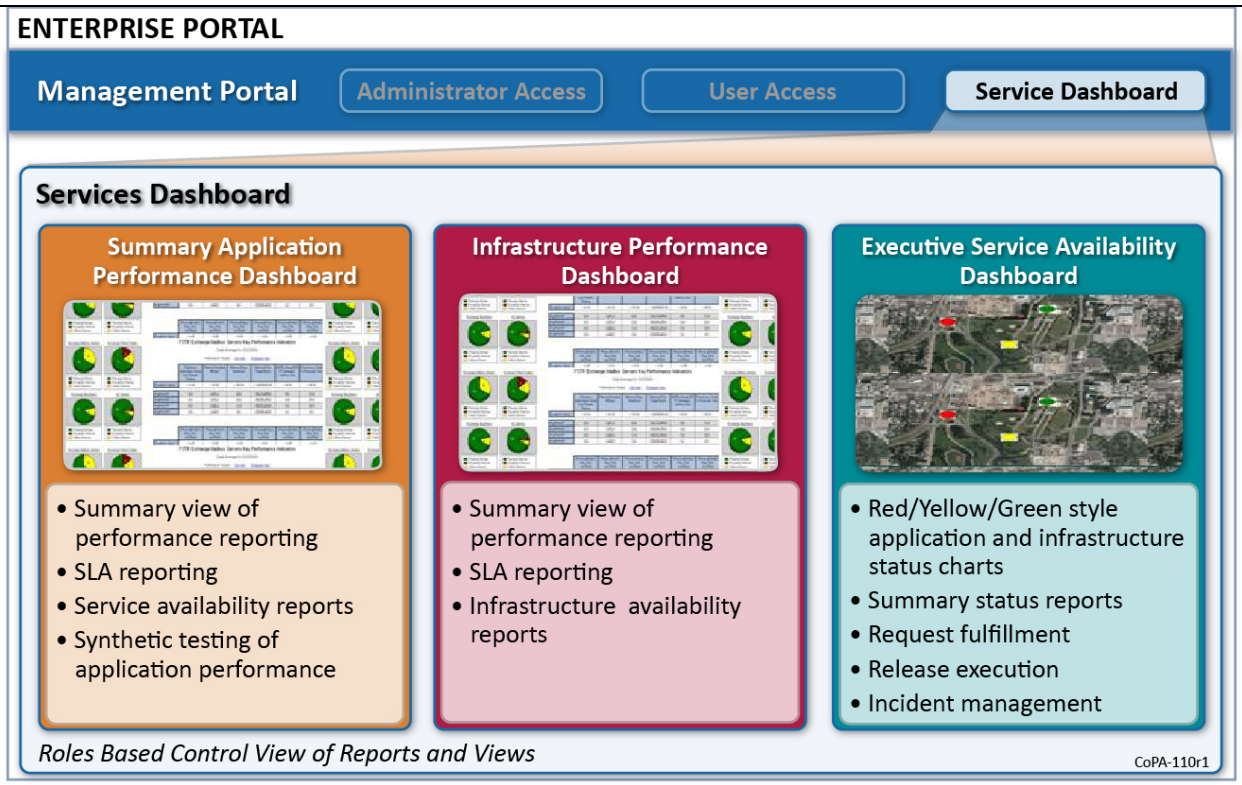


Figure 3.3.2.1-17 - Management Portal Example – Service Dashboard

Request Fulfillment

Description: Request Fulfillment is the process for handling and fulfilling service requests.

Activities:

Submit Service Request Using Self-Help – The requestor searches the Enterprise Services Catalog, selects the service needed, and submits the request.

Non-Catalog Request Fulfillment – Fulfills non-Enterprise Services Catalog item requests (e.g. Request for Information, Request for Administration, or an RFC submitted on behalf of a user).

Perform Service Item Request Approval –Approves Enterprise Services Catalog Requests.

Request Service Item Provisioning – Provisions requested service item.

Validate Service Deliverable – The requestor validates that the service request has been properly provisioned-- completing the fulfillment process when accepted.

Accept or Reject Service – Captures the requestor's acceptance or rejection of the provisioned service.

Inform Stakeholders About the Service – Communicates information to stakeholders about the service provisioned.

Event Management

Description: The Event Management process (refer to **Figure 3.3.2.1-18**), monitors the IT infrastructure for events that arise from servers, network components, and other devices, and provides event tracking, correlation, and disposition.

Events can be generated for Configured Items (CIs), environmental conditions, software, security, and standard operating activities.

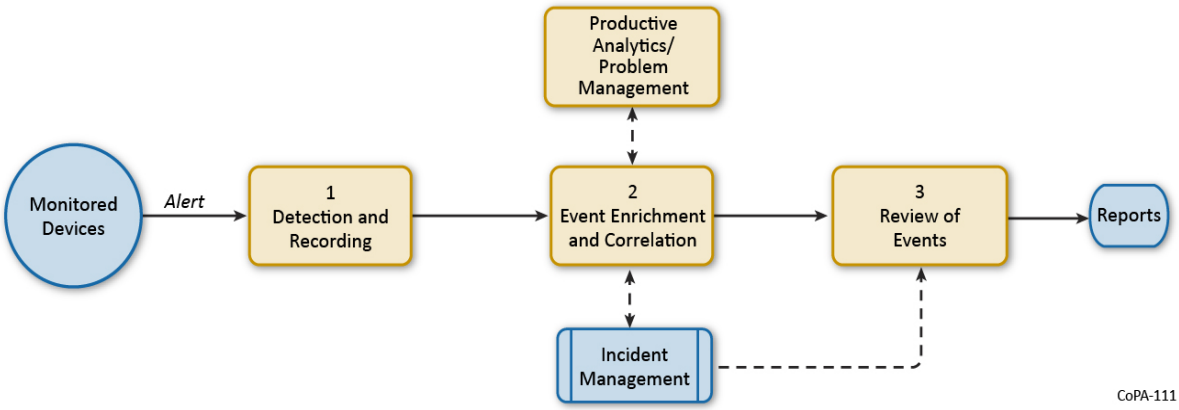


Figure 3.3.2.1-18 - Event Management Process Flow - Overview

Activities:

1. Event Detected and Recorded – Monitors the status of the various IT infrastructure items in the environment to detect when various thresholds are exceeded or events occur that should be reported.

2. Event Enrichment, Filtering & Correlation – Eliminates duplicates or suppresses events that are not significant in order to make event reporting more meaningful and manageable. Event correlation matches events that are related to root cause analysis.

   Auto Incident Ticketing – Created an automatic incident response based on the event detected.

3. Review of Events – Review events to determine if any action is required. It also reviews automated and manual actions taken to respond to events and to determine whether those actions were effective in improving the overall Event Management process.

   Reporting and Closing Event – Report and properly closes all events after appropriate review and action has been taken.

Incident Management

Description: Incident Management is the process (see **Figure 3.3.2.1-19**) of handling all incidents. This can include failures, issues or questions reported by users or by technical staff, or automatically detected events that automatically create incident records.

The purpose of Incident Management is to restore normal service as quickly as possible, to minimize any adverse impact on business operations. Incidents are categorized to identify who should work on them and for trend analysis. They are prioritized according to urgency and business impact.

There are three levels of support in the Incident Management process. Service desk agents provide the first level of support with general expertise across many disciplines in order to restore a service. If first level service desk agents cannot restore the service, then a second level service desk agent – who has deeper expertise and more experience resolving incidents – is engaged. Third level escalations involve subject matter experts (e.g., vendors) who generally reside in external organizations (e.g., other IT disciplines or vendors) in order to restore a service.

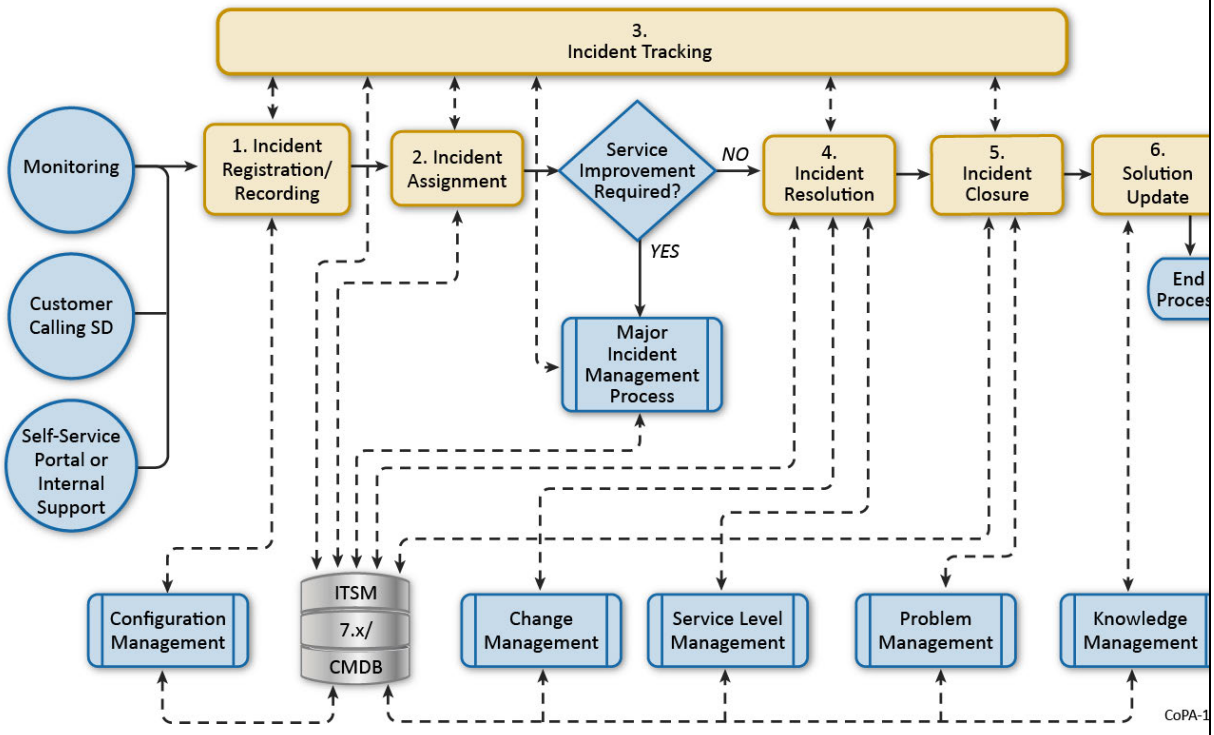


Figure 3.3.2.1-19 - Incident Management Process Flow

Activities:

1. Incident Registration and Recording – Verifies that all reported incidents and service calls are properly logged and validated.

2. Incident Assignment – Verifies that all incidents are assigned to the proper support team and level (e.g., 2nd/3rd level support)

3. Perform Escalation Management – Triggered when an incident has met the criteria for a valid escalation, such as:

   1) SLA commitments are breached (e.g., time to restore service)

   2) Priority of an incident has changed to a critical status

   3) A different support group is required to restore service

   This activity assigns ownership for an incident that has been identified as requiring escalation or transfer, validates the requirement, and facilitates the transfer to the identified support team after verifying that the incident priorities and requirements are understood, and that the identified support team accepts ownership for restoring service.

   Major Incident Process – Invoke the major incident process for Priority 1 (widespread) incident impacting enterprise wide service(s).

4. Incident Resolution – Resolver (team) determines how to restore service and completes restoration of service.

5. Incident Closure – Service Desk contacts impacted users to determine if service is restored satisfactorily and closes incident ticket.

6. Solution Update – Problem Manager determines if there is a solution, or temporary fix, to these types of incidents and then processes a problem and change ticket appropriately or adds a workaround to the knowledge management repository.

Problem Management

Description: The Problem Management process works to eliminate chronic incidents in the services infrastructure. It is a process focused on diagnostics and reconciliation of problems in the IT infrastructure to obtain stability in IT service delivery. It is focused on proactive and reactive IT infrastructure defect elimination to help reduce service impacting incidents.

The objective of Problem Management (refer to **Figure 3.3.2.1-20** Problem Management Process Flow) is to identify the root cause of an incident.

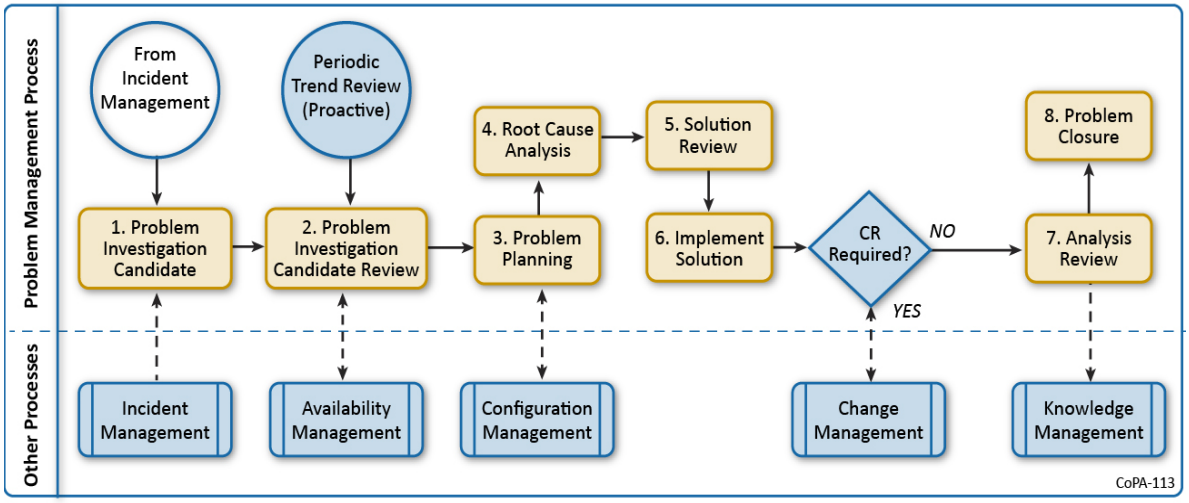


Figure 3.3.2.1-20 - Problem Management Process Flow

Activities:

1. Problem Investigation – Identifies a problem either proactively or reactively.

2. Problem Investigation Candidate Review – Records all relevant details of the problem so that an accurate problem record exists.

3. Problem Planning – Planning to support work around until the root cause if found and how to approach root cause analysis

4. Problem Root Cause Analysis –Performs a root cause analysis to determine the underlying cause of the problem. In order to restore service quickly in the future, workarounds may be developed and recorded to support the Incident Management process. Once the root cause is determined, a change request is submitted to eliminate the root cause of the problem.

5. Solution Review – The Problem Manager schedules a review of the proposed solution with key stakeholders to gain acceptance of the draft change request to eliminate the defect.

6. Implement Solution– Resolves the problem by approving and successfully testing and initiating the change request to eliminate the defect.

7. Problem Closure – Formally closes the problem record when any change has been completed and successfully reviewed, and the resolution has been applied. The status of any related known error record is updated to show that the resolution has been applied.

Service Transition

Service Transition provides guidance for the development and improvement of capabilities that are promoted into the production environment.

Service Transition processes are initiated as the result of a forthcoming change to the Commonwealth's production environment. Any change must first go through the Change Management (CM) process, which identifies valid changes through the review and approval of Request for Change (RFCs). RFCs can promote new or modified services, or modifications to the supporting software or hardware infrastructure. In many cases the change is categorized and prioritized for subsequent Service Transition processes.

As part of the acceptance of a change into the overall ITSM life cycle, the Service Asset and Configuration Management process is invoked. This process includes entering the service and all associated artifacts into the Configuration Management System (CMS) as an accepted CI. The artifacts associated with a service include software, documentation and test plans. Additionally, the artifacts are added to the Digital Media Library (DML) for initial archiving. The DML is used as the authoritative source of software, documentation and test plans for a baseline release. It can be used to restore the operational environment to the baseline or to assist in the release of software execution objects into the production environment following the Release and Deployment process.

Once the CIs are available in the DML, the Release and Deployment Management process and the Service Validation and Testing processes begin. Depending on the release strategy, objectives, risk assessment, etc., changes can, and most likely are, aggregated into a release – the defined unit of deployment for changes as they flow through the ITSM life cycle. Once a change is in the system, depending on the category and priority of the change, the change may go directly to the Service Validation and Testing process or be required to go through the more detailed Release and Deployment Management process. For example, if the change is minor and does not affect any other services, like a time setting, the change can go directly to the Service Validation and Testing process. If the change is more complicated and affects multiple services or platforms, it goes through the more detailed Release and Deployment Management process. Examples of more complicated changes include an application inclusion or an OS service pack change.

A release cannot be deployed into production without Change Management approval after review of the Service Validation and Testing results. The Service Validation and Testing process mitigates the risk of changes bundled in the release, and helps to verify that the release meets service utility (i.e., functionality to the user) and service (i.e. SLAs) requirements.

Change Management

Description: The Change Management process (see **Figure 3.3.2.1-21**) is responsible for controlling the life cycle of all changes. The goal is to respond to changing business requirements while maximizing value and reducing incidents, disruption, and rework. The objectives of this process are:

- To enable beneficial changes to be implemented with minimum disruption to IT service
- To verify that changes are recorded and evaluated, authorized, prioritized, scheduled, tested, implemented, documented, and reviewed in a controlled manner

The Change Management process drives service assets and CI planning, management, and reviews prior to their implementation and release.

The Change Management process and the Release and Deployment Management process closely govern the daily activities of the testing environment shared between Unisys and the

Commonwealth's agency application testing environments for testing, evaluating, and deploying applications and services to the production data centers. This forms the basis for establishing an operational capability and serves as the foundation for other ITSM processes that guide the day-to-day operation.

A *normal change* is a change that follows the normal Change Management process, requiring review and approval, etc. A *standard change* is a minor change with low risk that has been preapproved by the Change Manager because it follows a well-known and established procedure.

Refer to **Figure 3.3.2.1-21** for an overview of the Change Management Process Flow.

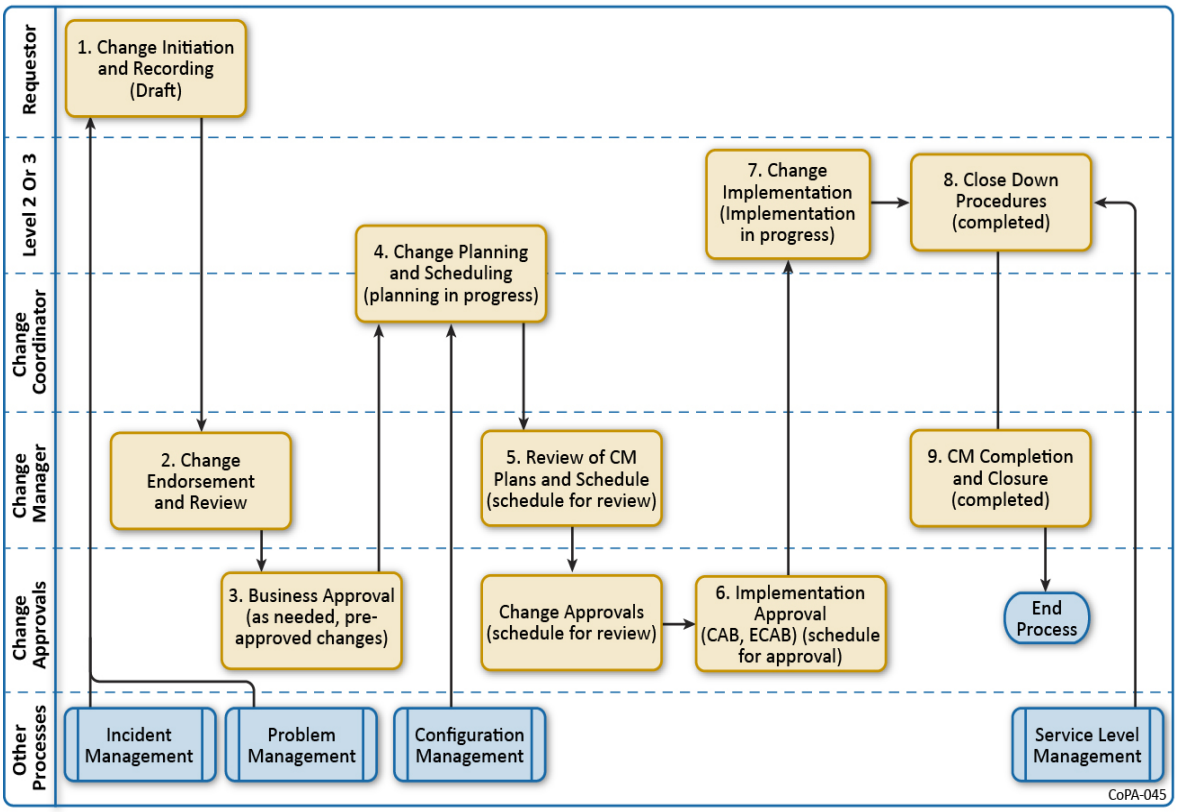


Figure 3.3.2.1-21 - Change Management Process Flow

Activities:

1. Change Initiation - Receives RFCs from requestors. In some cases RFCs are logged on the requestor's behalf.

2. Change Review - All RFCs are reviewed for completeness and accuracy.

3. Change Approvals – Changes are approved at the proper level and with appropriate personnel depending on whether the change requests types are standard, emergency, expedited, latent or normal, and their potential impact and priority.

4. Change Planning and Scheduling – Reviews the change to define planning and scheduling for implementation. A forward schedule of changes is maintained for stakeholder review and approval.

5. Emergency Change Management Approval – An emergency change requires Emergency (CAB) approval to implement changes to the production environment during an emergency due to a service outage. This expedited Change Management process proactively prevents an ongoing, serious service outage.

6. Change Implementation Approval – Reviews and approves the testing results and the release and deployment plans.

7. Change Implementation Review – Reviews the change implementation results including if it followed the release and deployment plan and was completed within the release window.

8. Change Closure - Reviews with the change stakeholders to determine satisfaction and success with the change implementation, lessons learned, and closure of the change.

Release and Deployment Management

Description:

The Release and Deployment Management process (see **Figure 3.3.2.1-22**) delivers significant business value by delivering changes at optimized speed, risk and cost, and offering a consistent, appropriate and auditable implementation of usable and useful business services.

The Release and Deployment Management process covers the whole assembly and implementation of new/changed services for operational use, from release planning through Early Life Support (ELS).

As previously stated, the Release and Deployment Management process and the Change Management process closely govern the daily activities of Unisys and the Commonwealth's agencies testing, evaluating, and deploying applications and services to the production data centers.

Refer to **Figure 3.3.2.1-22** for an overview of the Release Management Process Flow.

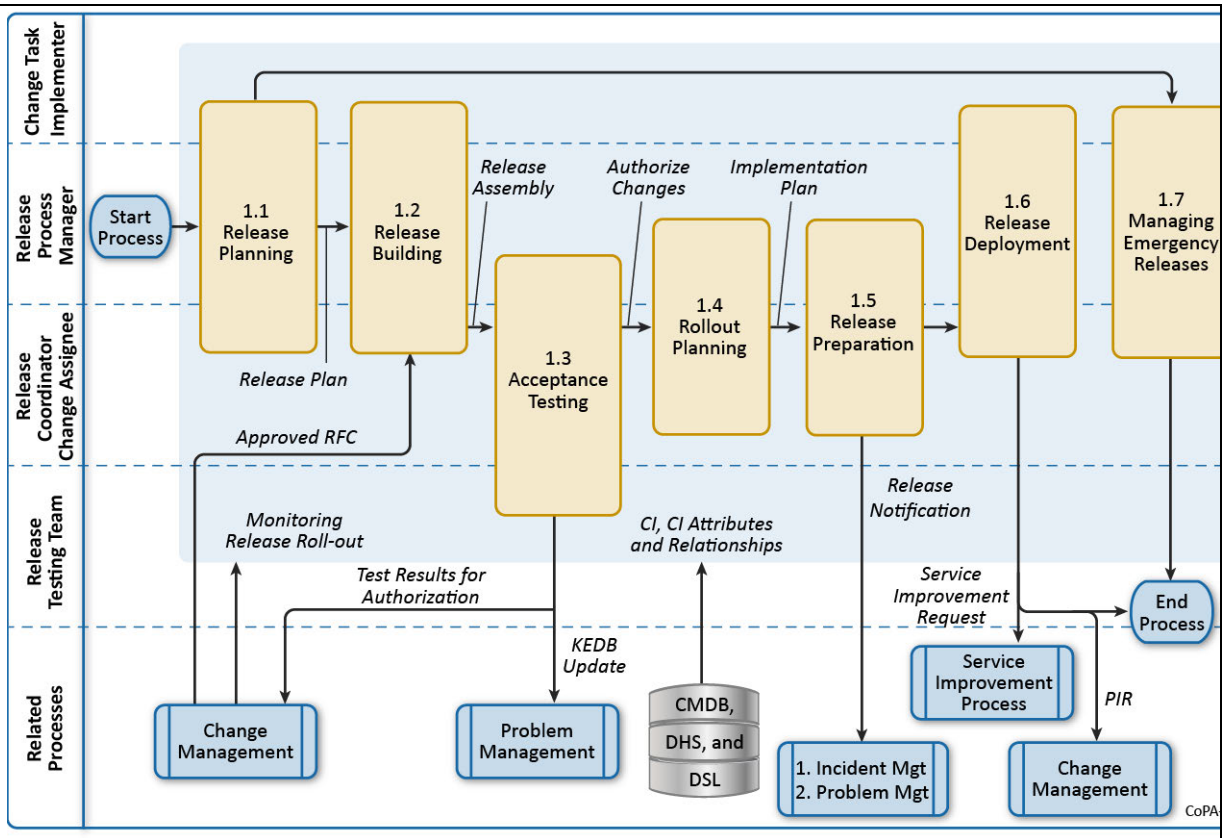


Figure 3.3.2.1-22 - Release and Deployment Management Process Flow

Activities:

1.1 - Release Planning – The Release and Deployment Manager and the planning and support teams work on the service transition package to establish, review, and periodically update the release policy document and schedule for releases.

1.2 - Release Building – After an RFC is validated and approved as part of the Change Management process, this activity begins the process of preparation for the release that includes supports one or several RFC's. This activity evaluates the service design baseline to verify the service release build and test begins with a stable, base-lined and approved design.

1.3 - Acceptance Testing – Coordinated through Test Management, which plans and controls the testing execution. Testing aims to build confidence in the service capability prior to final acceptance during the pilot or Early Life Service Support. Testing is based on the test strategy and model for the service being changed.

1.5 - Release Preparation – Prepares the organization and people for change, including the development of a detailed implementation plan that includes training, assigning individuals to specific process activities, etc.

1.6 - Release Deployment – Transfer assets, transfer/transition businesses and organizations, deploy processes and materials, deploy Service Management capabilities, transfer services, deploy services, decommission services, and retire services.

Provide Early Life Support (ELS) – Provides a smooth transition for the new or changed service to Service Operations in a controlled manner and establishes the new service capability and resources.

Verify Deployment – After the deployment and ELS activities are completed, this activity verifies that users, Service Operations and other staff and stakeholders are capable of using or operating the service.

Review and Close Deployment – Reviews the deployment against the requirement. Deployment is completed with a handover of the support for the deployment group or target environment to Service Operations.

Service Asset and Configuration Management

Description:

The Service Asset and Configuration Management Process addresses service assets throughout the entire service life cycle. It provides a complete inventory of assets, and identifies the individuals responsible for their control. It includes:

- Full life cycle management of IT and service assets, from the point of acquisition through disposal
- Maintenance of the asset inventory

The Service Asset and Configuration Management (SACM) process (**Figure 3.3.2.1-23**) provides a configuration model of the services, assets, and infrastructure that will contribute to meeting the ITSM objectives and assist in meeting service levels, by recording the relationships between service assets that will be managed as CIs. Assets are elevated to Configuration Items (CI's) for management purposes by augmenting asset data with configuration details that will support the management goals of ITSM and assist the Unisys Team in meeting SLA's.

The SACM process verifies the selected components of a complete service, system, or product (the configuration) are:

- Identified, baselined, and maintained
- Controlled through the Change Management process
- Released into controlled environments with operational use allowed only on the basis of formal approvals

SACM's may cover non-IT assets and work products that are used to develop services, and CIs required to support a service (e.g., documentation to support ongoing operations). The SACM covers interfaces to internal and external service providers where there are assets and CIs that need to be controlled, e.g., shared assets.

Refer to **Figure 3.3.2.1-23** for an overview of the SACM Process Flow.

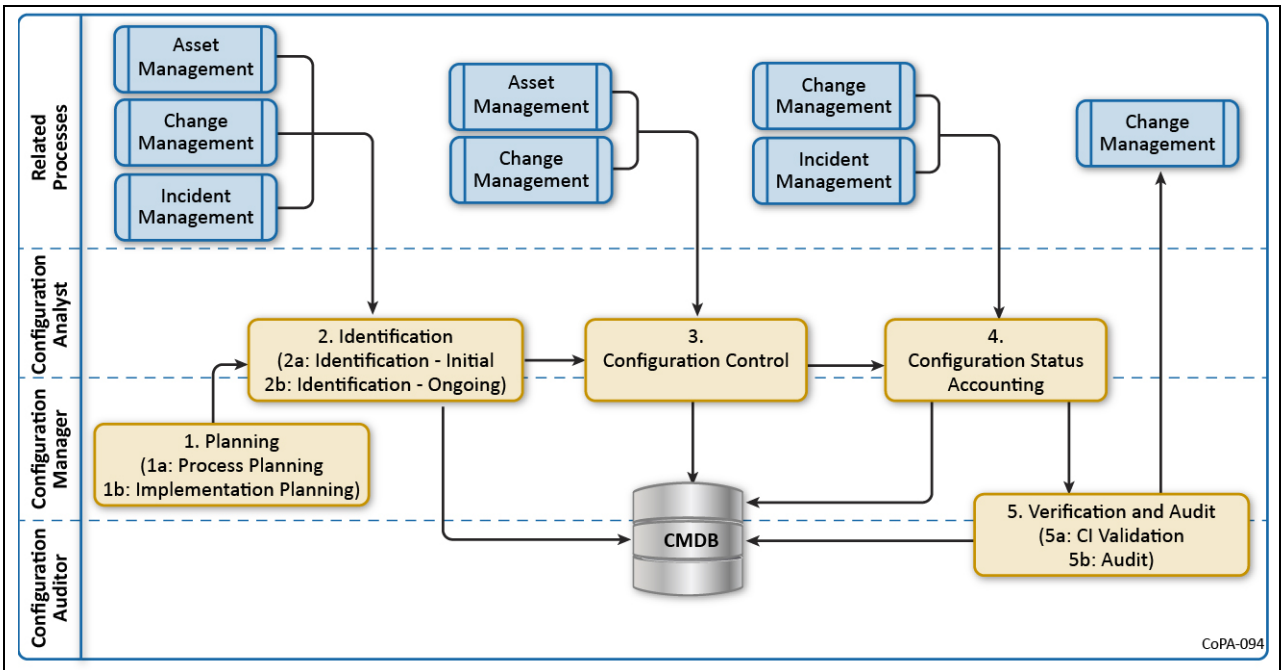


Figure 3.3.2.1-23 - Service Asset and Configuration Management Process Flow

Activities:

1. Management and Planning – This activity creates and delivers the Service Asset and Configuration Management plan.

2. Service Asset and Configuration Identification – This activity selects and identifies the configuration structures for all of the infrastructure's CIs, including identification of CI owners, CI interrelationships, and configuration documentation. This includes allocating identifiers and version numbers for CIs, labeling each item, and entering it into the Configuration Management Database (CMDB).

3. Configuration Control – This activity confirms authorized and identifiable CIs are accepted and recorded and confirms the existence of the appropriate controlling documentation (e.g., an approved RFC or an updated specification) to drive configuration changes. These activities happen throughout the CI life cycle.

4. Status Accounting and Reporting – This activity governs the reporting of all current and historical data regarding each CI throughout its life cycle. This information allows changes to CIs and their records to be traceable (e.g., tracking the status of a CI as it moves from one state to another).

5. Verification and Audit – This activity includes a series of reviews and audits that verify the physical existence of CIs and check that they are correctly recorded in the Configuration Management system.

Service Design. Service Design provides guidance for the design and development of services and Service Management practices. It covers design principles and methods for converting

strategic objectives into portfolios of services and service assets. Service Design is not limited to new services, but also includes the changes and improvements necessary to increase or maintain value to customers over the life cycle of services, the continuity of services, achievement of service levels, and conformance to standards and regulations. It provides guidance on how to develop design capabilities for Service Management.

The main purpose of Service Design is to design IT services, using governing IT practices, processes and policies, to facilitate the introduction of these services into the live environment while ensuring quality service delivery, customer satisfaction and cost-effective service provision. Service Design for the Commonwealth contract will focus on availability, capacity and service level management and is depicted in the following sections.

Enterprise Services Catalog Management

Maintaining the Enterprise Services Catalog includes:

- Managing the service definition and service component descriptions
- Updating the Enterprise Services Catalog
- Coordinating changes to the Configuration Management Database (CMDB) to reflect the Enterprise Services Catalog changes

Availability Management

Description: The Availability Management process (**Figure 3.3.2.1-24**) manages the availability of a service and plans, measures, monitors, and continuously strives to improve the availability of the IT infrastructure, services, and supporting organization and to confirm that service availability requirements are met consistently.

Availability Management helps to deliver a cost-effective and sustained level of availability that enables Commonwealth's agencies to satisfy its business objectives.

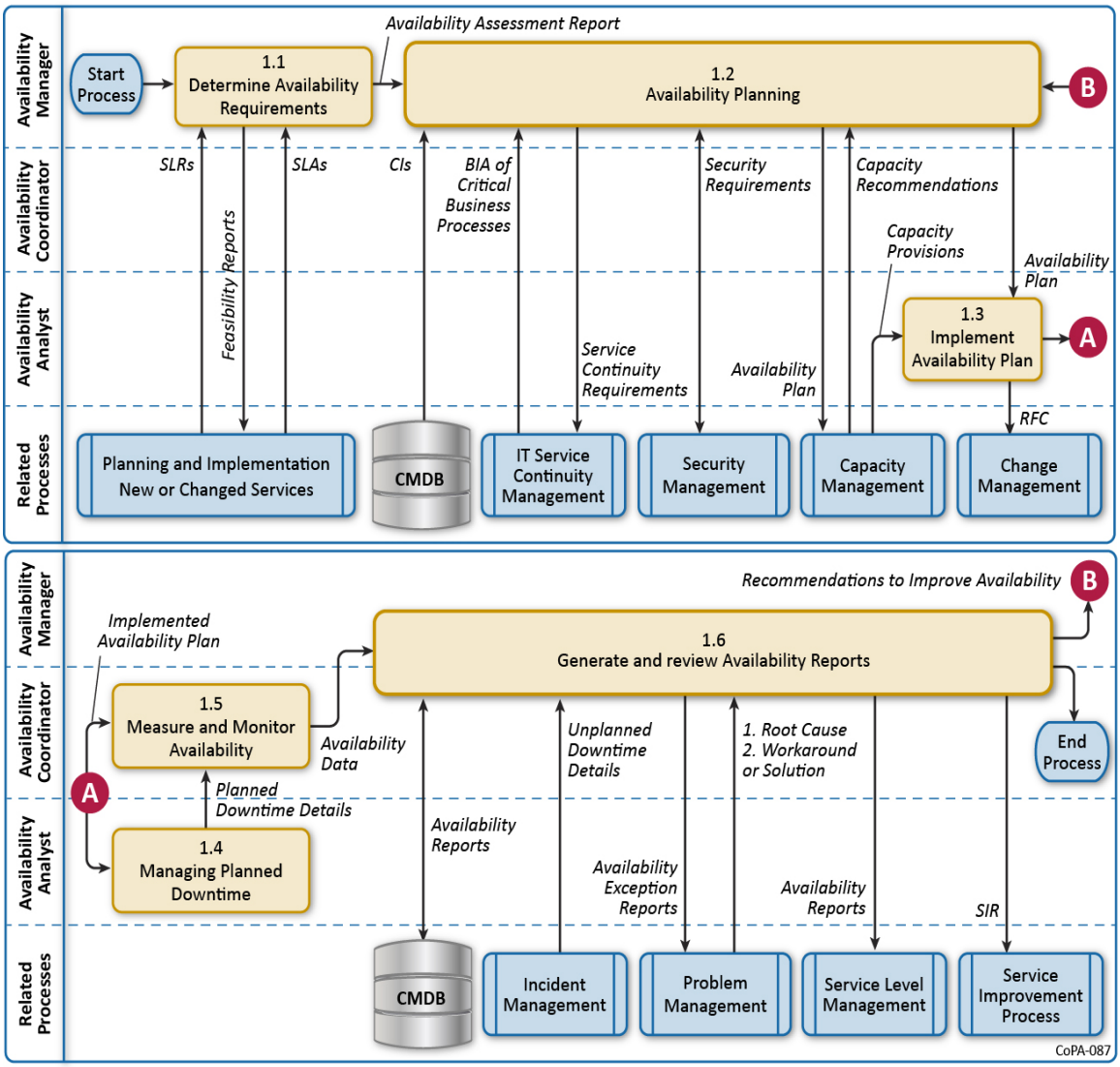


Figure 3.3.2.1-24 - Availability Management Process Flow

Activities:

1.1 - Determine Availability Requirements – This key activity confirms that the required level of availability for a new or changed IT service can be achieved, and is performed in conjunction with the Change Management process for a service being implemented or modified. It includes reviewing SLAs and availability requirements, availability incidents, and planning for meeting these requirements and addressing availability outages to determine how they can be avoided in the future.

1.2 - Availability Planning – Plans solutions to meet the availability requirements. This includes preparing cost effective solution, analyzing risks associated with the solutions, and obtaining approvals for the plans.

1.3 - Implement Availability Plan – Oversees the implementation of availability requirement solutions and tests those requirements against new or changed services.

1-4 - Manage Planned Downtime – Schedules and manages service downtime and the impact of availability and unavailability on services.

1.5 - Measure and Monitor Availability – Monitors, manages, measures, analyzes and reports on availability of services.

1.6 - Generate and Review Availability Reports – Preparation, review, and distribution of availability reports and actions for continuous improvement.

Capacity Management

Description: The Capacity Management process defines, tracks, and controls service capacities to meet forecasted demand at an agreed upon service level performance. It should be noted that considerations such as system capacity and network capacity are vital components that foster overall service capacity. **Figure 3.3.2.1-25** below shows the flow of information in the Capacity Management Process.

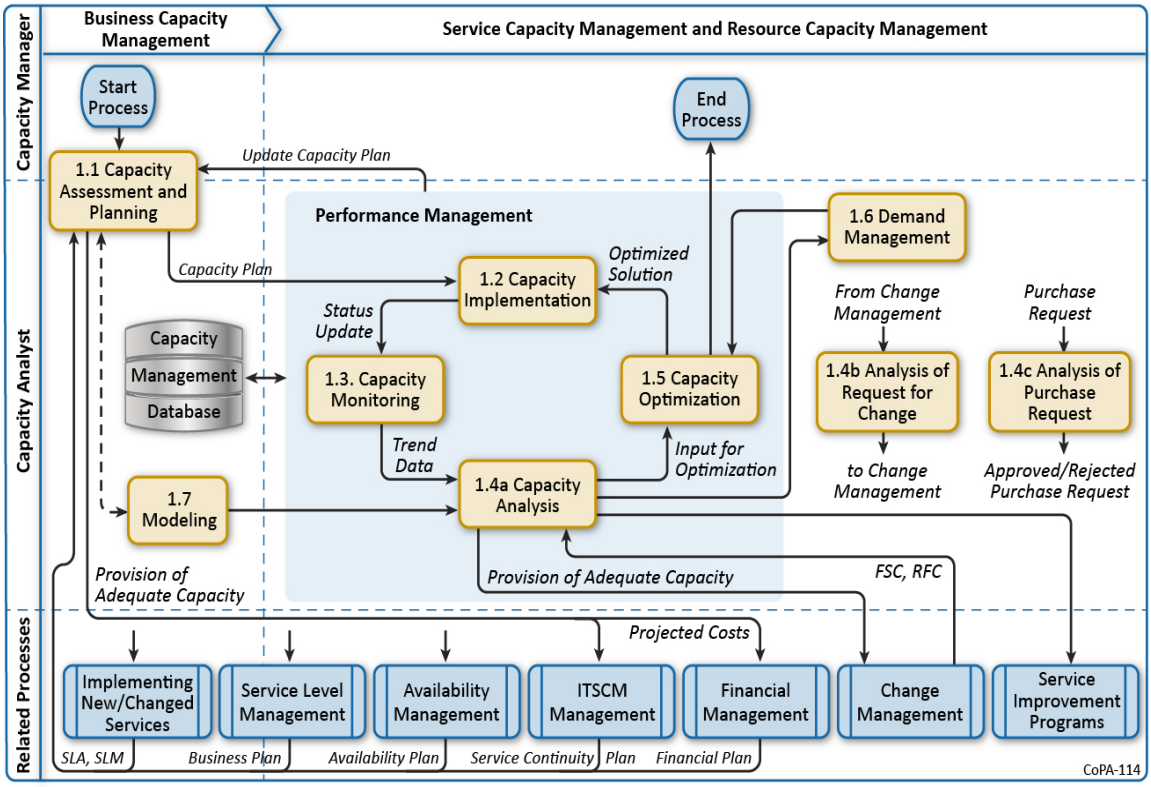


Figure 3.3.2.1-25 - Capacity Management Process Flow

Activities:

Capacity Assessment and Planning – This operational activity analyzes the current performance and capacity, reports obtained from the Service Level Reporting process, change requests, and current and future workload to identify requirements for capacity-related service availability and performance requirements.

Modeling – Models solutions to meet availability requirements and analyzes the advantages and disadvantages and costs of each alternative modeled solution. The Capacity Manager will present a recommended modeled solution for approval.

Performance Management – Implementation of the approved capacity plan, overseeing the implementation, monitoring and management of service availability and performance and recommending and implementing adjustments based on analysis and review.

Demand Management – Analysis of service consumption in the enterprise and recommending actions to shift demand for services, alter services, or eliminate services based on an overall enterprise view of services, demand, costs, and other factors.

Service Level Management

Description: The Service Level Management (SLM) process (**Figure 3.3.2.1-26**) is responsible for negotiating SLAs, and ensuring that SLAs are met. SLM is responsible for ensuring that all IT Service Management processes, Operational Level Agreements (OLAs), and Underpinning Contracts (UCs), are appropriate for the agreed service level targets. SLM monitors and reports on service levels and holds regular customer reviews.

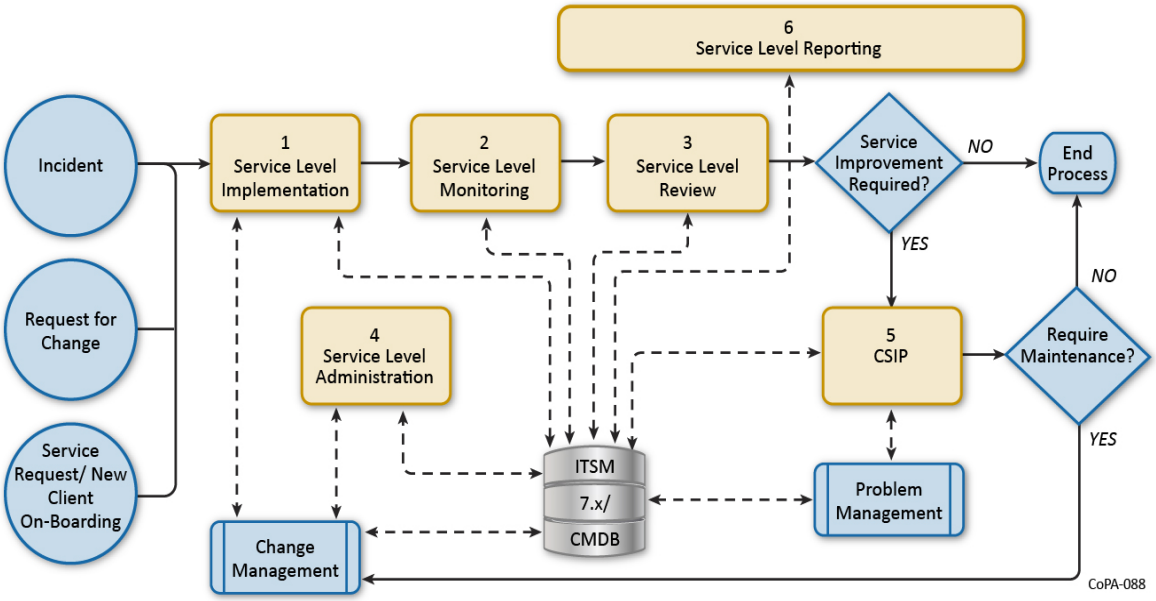


Figure 3.3.2.1-26 - Service Level Management Process Flow

Activities:

Service Level Implementation

Design SLA Framework – Use the Enterprise Services Catalog as an aid and designs the most appropriate SLA structure to confirm that all services and customers are covered in a

manner best suited to the organization's needs.

Determine, Document, and Agree to Requirements and Produce Service Level Requirements (SLRs) – Once the Enterprise Services Catalog has been produced and the SLA framework has been agreed to, this activity drafts the SLRs.

Review, Negotiate and Sign OLAs – Determines and negotiates the OLA requirements necessary for service delivery, and develops OLAs and obtains signatures for OLAs that support the SLA.

Review, Negotiate & Sign UCs – Reviews, negotiates, develops, and has signed the UCs that supports the SLAs and OLAs.

Create Service Level Agreement and Negotiate Terms – Drafts and negotiates the SLA that is needed to meet specified SLRs and objectives.

Activate the SLA – Oversees the signing and activating of the SLA.

Monitor Service Performance Against SLA and Produce Service Reports – Monitors performance in an ongoing manner and reports on specified service level measurement.

Perform Service Level Review – Performs periodic reviews of service level performance.

Service Level Administration – conduct periodic reviews of SLA's with stakeholders to review SLA's and determine if any changes are required to support existing or modified SLA's

Create a Service Improvement Plan – Creates a Service Improvement Plan (SIP) that is a formal plan to implement improvements to a process or IT service. A SIP is managed as part of the Continual Service Improvement (CSI) element of ITSM.

Service Level Reporting – produce SLA reports and make accessible to stakeholders with capabilities to drill down into details.

17 CM, CMDB Data collection and input

17.A Work with the Commonwealth to acquire asset information to support the asset management system and configuration management system.

Offeror must describe its approach to capturing, validating and storing all configuration information required to perform the Services within 120 days of the Effective Date of the Contract.

The Unisys Team recognizes that the Configuration Management Database (CMDB) is the key system of record for support of Services for the environment.

Unisys will take the following approach to capturing, validating and storing all configuration information required to perform Services within 120 days of the Effective Date of the Contract:

- Obtain all Configuration Information for infrastructure assets (this can be electronic, paper documents, etc.).
- Validate the configuration information through a Unisys/Commonwealth audit of the information.
- Unisys will store the configuration either in electronic or paper form to be stored in

appropriate electronic or paper form in order to perform required Services beginning on day 120 after effective date of contract.

- Billing will be reconciled to this captured, audited, and maintained store of configuration item before submitted to the Commonwealth.

Unisys plans to implement at 160 days a fully operational ITSM platform to support the Commonwealth agencies for transition as required in Schedule D. At the time the information gathered above will be loaded into the [redacted] for EDC and DPH Configuration Items with appropriate relationships. The ADDM tool will be fully operational and discovering CI's and relationships for infrastructure items. Unisys will have available an Application Mapping Catalog Service to map infrastructure items to the CMDB.

Figure 3.3.2.1-27 below represents how the maintenance of the [redacted] will be maintained through automated discovery of the transitioned environments in order to support Services.

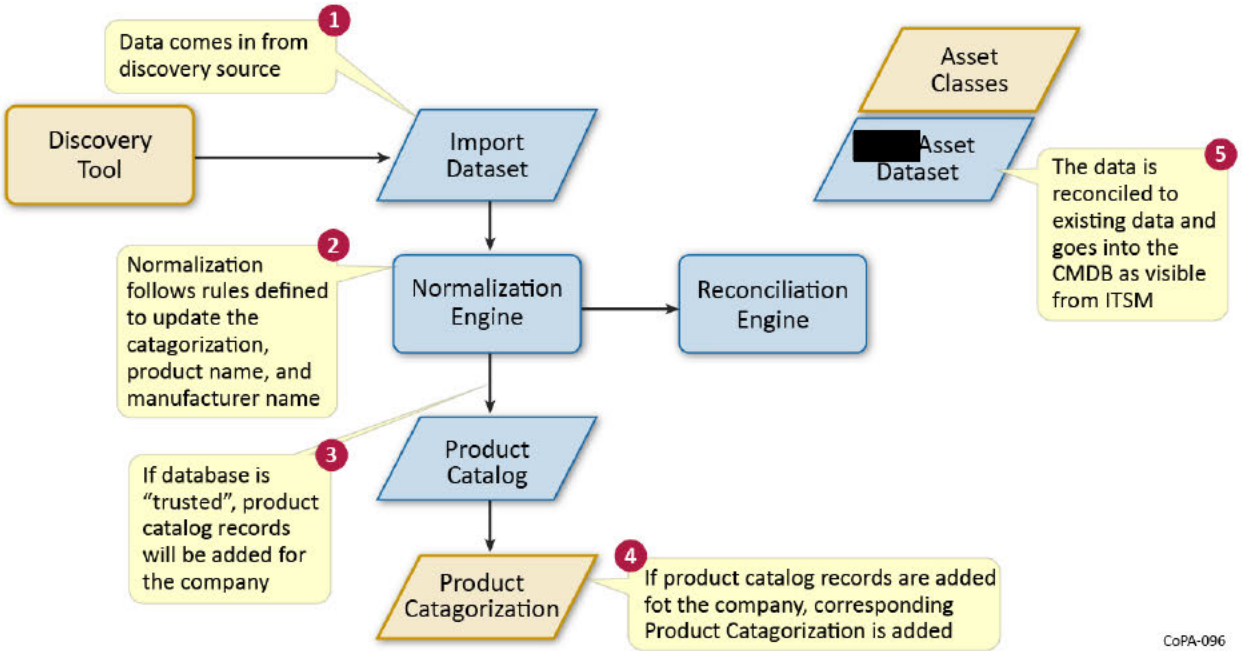


Figure 3.3.2.1-27 - [redacted]

The Unisys Configuration Management Team will have detailed processes and procedures to support and compliment the automated discovery, normalization and reconciliation processes outlined above. Refer to Schedule F, Section 3.2.1.7 Configuration Management for a complete description of the Configuration Management Process.

17.B In particular, the Offeror must address how it will identify and relate critical associations (e.g. Application to Server, Server Tier to Application, Application to Disaster Recovery Time Objective, software to server, etc.) for the enterprise.

Offeror must describe its approach to transitioning the data and related processes from the

existing CMDB or equivalent system/database to the Offeror's solution and how the Offeror must ensure accuracy of data across Service Management areas to ensure accurate and timely invoicing and chargeback to the Commonwealth.

Please refer to Configuration Management Schedule F, Section 3.2.1.7 for an overview of the CMDB processes and application infrastructure supporting relationships.

The approach to transition for the CMDB is as follows:

1. Determine requirements to support availability SLA's for each application transitioned using the Schedule J.3 definition for Infrastructure Availability

2. Determine the alternatives to establish the CMDB relationships to support these availability SLAs including:

    a. Utilizing the Commonwealth / Agency CMDB sources

    b. Discovery using [redacted]

    c. Using the [redacted] to finalize the mapping labels, relationships etc. to support the SLAs

    d. Obtaining the Commonwealth approval for the mapping during transition

Please Refer also the Financial Management Schedule F, Section 3.2.1.1.1 for an overview of how the Billing application uses the Enterprise Services Catalog and CMDB to provide accurate billing of provisioned services that are accurately reflected in the CMDB.

18 Chargeback Management

Work with the Commonwealth to interface with the Commonwealth's billing processing and validation ITSM system to provide a chargeback system for new and existing Services available on the Offeror's Service Catalog.

Offeror must describe its approach to assisting the Commonwealth in transitioning Commonwealth customers from the existing Chargeback system.

Offeror must describe its transition approach to Chargeback Management.

The description must include an expected analysis of the current billing system environment, expected termination assistance, communications plans, strategy for testing and major milestones.

Unisys has a good understanding and experience with billing by Agency. We will leverage the financial management component within the Enterprise Services Catalog ordering system to pull monthly data by agency for specific services ordered during that billing month. By utilizing the same tool for both Enterprise Services Catalog and invoicing, we will have the ability to manage the expenses at the level of the services. This solution will provide the Commonwealth with the ability to gain greater understanding of its IT costs through visibility into the usage details of the IT resources.

There are four facts needed to be known about a resource in order to charge for it; Who, What, When and How Much. This data will all be contained in the Enterprise Services Catalog system.

Once an Agency has ordered a service; the service is provisioned and verified through the Change Management process, then the units and Enterprise Services Catalog rates will be used to generate a monthly fee to the Agency. Invoicing is configured to provide various funding streams by general ledger accounts as identified by each agency during implementation. This system will provide reporting capabilities that will enable the agencies to manage both their IT utilization and costs at a level they define. The Unisys Team will work with the Commonwealth to develop the appropriate interface format for input into the Commonwealth Chargeback system. Refer to Schedule F, Section 3.2.1.1.1 for more detail on the Financial Management function.

During the transition period, Unisys will work with each agency to identify the various general ledger accounts they utilize in the Commonwealth system. A comparison to current billing will be done to provide consistency where it is needed. With the Agency's input, the system will then be set up per their requirements. Training will be provided to show the agency how the system will work from ordering of services through the billing process, and will be provided with available report formats.

Implementation of the Enterprise Services Catalog will be done as tasks within the Transition Project and will be managed in accordance with the standards establish for project management within the program including communications, testing, and schedule adherence.

During the transition described above, the Unisys Team will leverage the interim invoicing procedures defined in Schedule F, Section 3.2.1.1.1 Financial Management.

19 Options and Costs

List the appropriate different options that will satisfy the requirements of the transition scope.

Communicate options with the Commonwealth and obtain approval on selected option(s) to proceed.

Offeror must describe proposed approach

Throughout this document, the Unisys Team has provided options and suggested approaches to be discussed after contract award. Based on the options selected by the Commonwealth, costs and timelines may need to be altered. For additional details please see Section 3.0 Attachment 9 "Schedule M: Detailed Transition Plan".

20 EDC Expansion and Reconfiguration Options

20.A Expand/reconfigure datacenter facilities to accommodate growth in Commonwealth information and information systems.

Offeror must discuss its approach; the expansion/reconfiguration plans must include the EDC.

The Unisys Team's plan is to leave the [redacted] "as is" during transition/migration to mitigate risk and focus on transition activities. In addition to the [redacted] the Unisys Team is establishing infrastructure for the Commonwealth in [redacted] to provide the services outlined in this proposal and to accommodate existing applications as well as future growth. Unisys data center architecture is designed to flex with the Commonwealth's need for growth or reduction in data center hosted services. Refer to Section 3.1.1 "Multi Data Center Environment" for further details on the proposed Unisys Data Centers.

21 Transition Weekly Reports

21.A Produce weekly reports on the progress of the information service transition initiatives.

Offeror must describe its proposed approach to providing weekly transition progress reports.

The Commonwealth Transition Program will produce several weekly status reports during the life of the program. These reports will be tailored to the audience for whom they are intended including the program and project steering committees. Communications through these reports should have three facets.

1. Reviewing results from the past period
2. Expected results for the next period
3. Items for management attention. These items will be further categorized into those requiring action from the leadership team and those for information only. It is also expected this will not be the first leadership will be aware of these items' but rather is intended to keep these items in the forefront of leaders thoughts.

Status reports will be posted to a portal accessible to those recipients authorized to receive them. See response to 1-D "Communication Plan" above for further details.

Unisys Team Experience

Unisys, IBM and Deloitte are industry leaders in data center outsourcing. They have transitioned and migrated countless data centers into their support models and facilities. As an example, Unisys has recently provided similar services for the American Red Cross. Within the Commonwealth, the Unisys Team has successfully migrated multiple data centers into the Willow Oak data center. In addition, Unisys currently provides over half of the resources for the [redacted]

Section 4 will provide much more depth into several of these efforts.

Benefits to the Commonwealth

Unisys, IBM and Deloitte know the Commonwealth, know many of their environments and have strong relationships with the agencies. This knowledge and the relationships that have been forged over the years of working together give this team a significant advantage. We know what to expect from each other, we know how each other works and we have large, strong companies behind us with a strong understanding of the industry and technologies. Throughout the program you will no doubt see this team bringing in new team members who bring with them industry experience from other large companies. The synergies of combining the Commonwealth, Unisys, IBM, Deloitte and the diverse experience of the new team members will no doubt provide a world class solution for the Commonwealth which we believe can be achieved faster, with higher quality and a lower cost.

A Unisys Team transition provides a team already familiar with the Commonwealth and its organization, which can be more focused on the mechanics of a successful transition and meeting your needs without impact.

3.3.2.2 Security Transition Activities

To maintain continuity of Services, Offeror must provide training to Offeror's employees and subcontractors on security policies during initial phase of the Transition.

Reference Documentation

Schedule D - Transition Milestones

Exhibit D.7 - EDC Facility Summary

Exhibit A - Commonwealth Network Environment

Exhibit(s) B.1 through B.6 - Data PowerHouse (DPH) Exhibits

Exhibit(s) C.1 through C.13 - Department of Public Welfare (DPW) Exhibits

Exhibit(s) D.1 through D.15 - Enterprise Datacenter (EDC) Exhibits

Exhibit(s) E.1 through E.43 - Department of Labor & Industry (DLI) Exhibits

Exhibit(s) F.1 through F.4 - Department of Health (DOH) Exhibits

Exhibit(s) G.1 through G.16 - PA State Police (PSP) Exhibits

Exhibit(s) H.1 through H.8 - Department of Revenue (DOR) Exhibits

Exhibit(s) I.1 through I.13 - Commonwealth SAP Environment - Integrated Enterprise Services (IES) Exhibits

Exhibit L - Commonwealth Master Application Inventory

Exhibit(s) M.1 through M.7 Department of Corrections (DOC) and Pennsylvania Board of Probation and Parole (PBPP) Exhibits

Exhibit(s) N.1 through N.2 - PennDOT Exhibits

Requirements		Describe Compliance
1.	Baseline Security Risk and Vulnerability Assessment Conduct a security risk assessment, which includes a penetration test on the In-Scope systems, an architecture review, and a vulnerability assessment. This assessment must result in a report with recommendations for meeting the Commonwealth's baseline security standard.	Offeror must describe its proposed approach to conducting a security risk assessment including penetration test, which must result in a report with recommendations.

2.	Security Training The Offeror's security team will meet with the Commonwealth's Security teams (OA & Agency) to participate in creating a comprehensive Security Program strategy. The Offeror and the Commonwealth Security teams will develop security awareness training content consisting of the Offeror's Security Plan documentation, Commonwealth OA and agency security policy guidelines. Security training will be mandatory for employees, contractors and subcontractors assigned to work on the Commonwealth's Data Center project. Appropriate levels of training will be designated and tracked for compliance based on the specific area the employee will be working in. Both an individual's current training status and overall attainment of group training goals must be tracked and reported in the security clearance database. These levels will range from general security awareness that all employees will participate in to task-specific security and governance requirements targeted at operations, specialist, Commonwealth agency specific regulations, or working rules needed for compliance with Commonwealth or federal mandates unique to certain Commonwealth agencies and programs. This training will be delivered both during the new hire process, and on a regular schedule to be determined during Transition as new updates become necessary.	Offeror must describe its proposed approach to developing and implement a comprehensive Security Program.

3.	Initial Security Plan During the initial phase of the Transition the Offeror's security team will work with the Commonwealth's Security Team to create a Security Plan. Begin work on draft policy and procedure documents collectively known as the Security Plan during the start of the Transition Risk and Vulnerability Assessment, which will be completed one (1) month prior to Transition activities. Use best practice security standards (as outlined in the Requirements section of the RFP) along with past engagement experience to provide an outline that will address but will not be limited to the following: security strategy and technology roadmaps, security operations procedures, standard hardware and software security configurations, physical security policies and procedures, security incident management, private and protected data use standards, and audit procedures and reporting standards. This set of documents will be used as the foundation of the Offeror's master security plan for Datacenter operations which will be reviewed and updated on an annual basis.	Offeror must describe its proposed approach to performing the following: • Create a comprehensive Security Plan • Complete a Vulnerability Assessment (at the Offeror expense) • Document the agreed upon security strategy and roadmap • Document security procedures and standards • Document the security incident Management approach including o Standards o Processes o Reporting o Escalation
4.	On-boarding and off-boarding Conduct required background checks for its employees working on the Commonwealth Datacenter project. Where appropriate, use identity management tools to manage access to the systems requiring access by its	Offeror must describe its proposed approach to conducting required background checks for Offeror staff.

	employees. For systems where the Offeror is unable to use its identity management system, assign staff to manage the access. Train Offeror employees on his or her responsibilities within the contract. For logical and physical access to Commonwealth Co-location facilities and environments not managed by the Offeror, the Commonwealth's security access request process will be followed. For off-boarding, update security clearance database with the status of Offeror employee and concurrently update its identity management tool to ensure the access is revoked. Provide a monthly report describing personnel actions including but not limited to; new hires, terminations, any change in employee status/duties, etc.,	
5.	Complete DR Transition Activities Conduct knowledge transfer during the initial phase of the Transition, including review of Commonwealth DR plans and review of Third Party DR contracts. The Offeror must also update the DR plan contact information and any changes made in the first six (6) months of Transition.	Offeror must describe proposed approach to support the Tiered DR Services.

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

Introduction

The Unisys Team will conduct key security-related activities during the Transition phase to maintain continuity of Services. These services include a Baseline Security Risk and

Vulnerability Assessment, Security Training, development of an Initial Security Plan and On-boarding and Off-boarding procedures, and Disaster Recovery transition.

1 Security, Risk and Vulnerability Assessment

1.A Conduct a security risk assessment, which includes a penetration test on the In-Scope systems, an architecture review, and a vulnerability assessment. Offeror must describe its proposed approach to conducting a security risk assessment including penetration test, which must result in a report with recommendations.

The Unisys Team uses our demonstrated methodology and our deep experience in serving multiple agencies of Commonwealth and other public sector clients to perform the baseline security risk and vulnerability assessment. We use our experience in delivering security risk and vulnerability assessment projects for several public sector clients including the Commonwealth to deliver this assessment. Using state-of-the-art tools that are consistent with leading industry practices such as National Institute of Standards and Technology (NIST) standard, Open Web Application Security Project (OWASP) and System Administration, Audit, Network, Security (SANS) guidelines, we will tailor our assessment to meet the Commonwealth timelines and deliverable milestones.

In addition, the Unisys Team uses our public sector security risk framework to develop the data center security risk framework (during the initial security plan). A framework customized to the data center, helps integrate several relevant regulatory requirements and perform a one-time risk assessment to identify the data center security posture with relevant regulations and Commonwealth policies. The Unisys Team performs the following steps as part of the baseline security risk and vulnerability assessment:

- Step 1: Scope and Plan
- Step 2: Conduct vulnerability assessment
- Step 3: Perform penetration testing
- Step 4: Perform security risk assessment and architecture review
- Step 5: Perform security configuration risk review

We will work with the Commonwealth to perform the following activities described in the table below in **Figure 3.3.2.2-1.**

Steps	Unisys Team performs the following activities to identify potential security risks and vulnerabilities within the existing data center infrastructure
Step 1: Scope and Plan	Conduct two meetings with the data center stakeholders and the Commonwealth's "Trusted Agent" to • Document project requirements, scope and objectives • Identify Commonwealth's point of Contact ("Trusted Agent"). • Identify and document the time frame for conducting baseline security risk and vulnerability assessment.

Step 2: Conduct Vulnerability Assessment	• Identify the Commonwealth's target IT and application infrastructure using passive scanning (from public resources such as Search Engines) • Work with the Commonwealth's stakeholders to understand the architecture, business logic/functionality, external dependencies, user roles and privileges within the target IT infrastructure and application • Identify, using passive scanning techniques, the technology and infrastructure dependencies • Perform active reconnaissance and identify network protocols present on the target infrastructure and web applications using network discovery (SolarWinds, Ping and Xprobe2) • Identify well-known open TCP ports and services present on the target infrastructure using leading port scanning tools (Nmap and SuperScan) • Perform infrastructure vulnerability tests using automated vulnerability scanning tools (Tenable Nessus and Rapid7 Nexpose) on Commonwealth selected IT infrastructure. The tests will include performing vulnerability scans to meet the Payment Card Industry (PCI) Data Security Standard (DSS) vulnerability scanning requirements • Perform database vulnerability testing, using automated database vulnerability scanners (AppDetectivePro) on a total of Commonwealth selected standard database instances of Oracle, Microsoft SQL Server, MySQL and IBM DB2 • Conduct manual assimilation of the vulnerability scan results to identify false positives and manually verify the vulnerabilities identified by the vulnerability scanning tools.
Step 3: Perform Penetration Testing	• Analyze the vulnerabilities in order to identify the penetration testing steps that can be performed – based on the identified hosts with vulnerabilities • Research, develop and prepare custom penetration test scripts methods for system vulnerabilities • Communicate the penetration test activity with the trusted agent and obtain the confirmation before performing the tests on the target environment • Support the Commonwealth to select the IT infrastructure to perform the penetration testing. The selected IT infrastructure for further analysis will help provide a representative view of the data center IT environment (e.g., different server OS levels, HW vendors, and server functions). We will document and discuss the appropriate exploitation steps with the Commonwealth before performing the tests • Perform the controlled penetration testing on Commonwealth selected IT infrastructure to exploit the identified vulnerabilities. We will use Rapid7 Metasploit to perform the penetration tests Note: The Unisys Team performs the vulnerability assessment and penetration testing on Commonwealth selected data center's IT network infrastructure. The vulnerability assessment and penetration testing does not include web application vulnerability testing and social engineering assessment

Step 4: Perform Risk Assessment and Security Architecture Review	• Develop a data center security risk framework that includes an integration of relevant security regulations and commonwealth policies including, • Commonwealth Security Information Technology Bulletins (ITBs) • National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 revision 4 • Health Information Portability and Accountability Act (HIPAA) – Security and privacy rule • Internal Revenue Services (IRS) publication 1075 • Payment Card Industry (PCI) Data Security Standard (DSS) • Criminal Justice Information Services (CJIS) v5.1 • PA Criminal History Record Information Act (CHRIA),and • United States Social Security Administration (SSA). • Conduct a security risk assessment and IT architecture review of the existing seven data center IT infrastructures using the data center risk framework developed NIST SP800-53 rev4. The IT security architecture review includes specific components such as, • Trust Zone Architecture. • User Role Design. • Authentication and Authorization. • Data Protection. • Security Audit Logs and SIEM. • Data Privacy.
Step 5: Perform Security Configuration Risk Review	• Perform security configuration risk review using the IRS 1075 based Safeguard Computer Security Evaluation Matrix (SCSEM) on Commonwealth selected IT infrastructure handling Federal Taxpayer Information (FTI). We will work with the Commonwealth to select the IT infrastructure that includes a representative view of the information technology environment of the data center such as • Web servers • Application servers • Database instances • Standard operating systems (SCO UNIX,Tru64 UNIX, HP-UX, IBM AIX, Linux – Red Hat, SUSE, Microsoft Windows 2000, 2003 and 2008) • Boundary protection devices: perimeter firewalls, Intrusion Prevention System (IPS), routers and switches.

Figure 3.3.2.2-1 - Risk and Vulnerability Assessment Steps

1.B This assessment must result in a report with recommendations for meeting the Commonwealth's baseline security standard.

We document the results of the baseline security vulnerability and risk assessment as part of key deliverable D-09.01 – Baseline Security Risk and Vulnerability Assessment Report, and submit to the Commonwealth. In addition, we will work with data center stakeholders and the

Commonwealth stakeholders to develop a remediation plan.

We use the data center's defect tracking tool, to record the identified security vulnerabilities and risks. This enables the Commonwealth to monitor the vulnerability remediation status on a continuous basis. As part of this effort, we perform the reporting and remediation process through the following three steps:

- Step 1 – Prepare baseline security vulnerability assessment reports
- Step 2 – Assist infrastructure owners to determine infrastructure and business impacts
- Step 3 – Develop remediation plan

We describe the three steps of the remediation process below.

Step 1 – Prepare security risk and vulnerability assessment reports: We prepare and submit the report (Key Deliverable D-09.01) that includes the outline described in the table below in **Figure 3.3.2.2-2**:

Baseline Security Risk and Vulnerability Assessment Report Sections	Our Activities Addresses Baseline Security Risk and Vulnerability Assessment Details	Stakeholder	Tools/ Techniques
Security Vulnerability and Risk Description	• Describes the identified security vulnerability, vulnerability location(s), number of instances where identified and vulnerability severity (high, medium and low) • Provide the suggested vulnerability mitigation upon analyzing the root cause • Map each vulnerability identified to a system specific vulnerability ID, to track root cause and reemergence of vulnerabilities • Benchmarks the vulnerabilities identified with leading industry practices for network security and architecture.	• Unisys Team.	• Baseline security risk and vulnerability assessment
Vulnerability Categorization/ Business Impact	• Describes the infrastructure and business criticality of the security vulnerabilities identified and user groups impacted	• Commonwealth data center stakeholders /owners • Unisys Team	• IT Infrastructure Business Impact Analysis
Mitigation	• Provides the PCRs recorded for	• Commonwea	• Commonwealt

timeline	each vulnerability identified to monitor for mitigation during SAT phase of SDM • Tracks the mitigation status when submitted to the DPW CISO.	lth data center stakeholders /owners • Unisys Team	h data center standard defect tracking system

Figure 3.3.2.2-2 - Security Risk and Vulnerability Assessment report Outline

Figure **3.3.2.2-3** below illustrates a sample vulnerability assessment dashboard provided as part of the report. This dashboard provides a graphical representation of the vulnerability severity identified on the IT infrastructure.

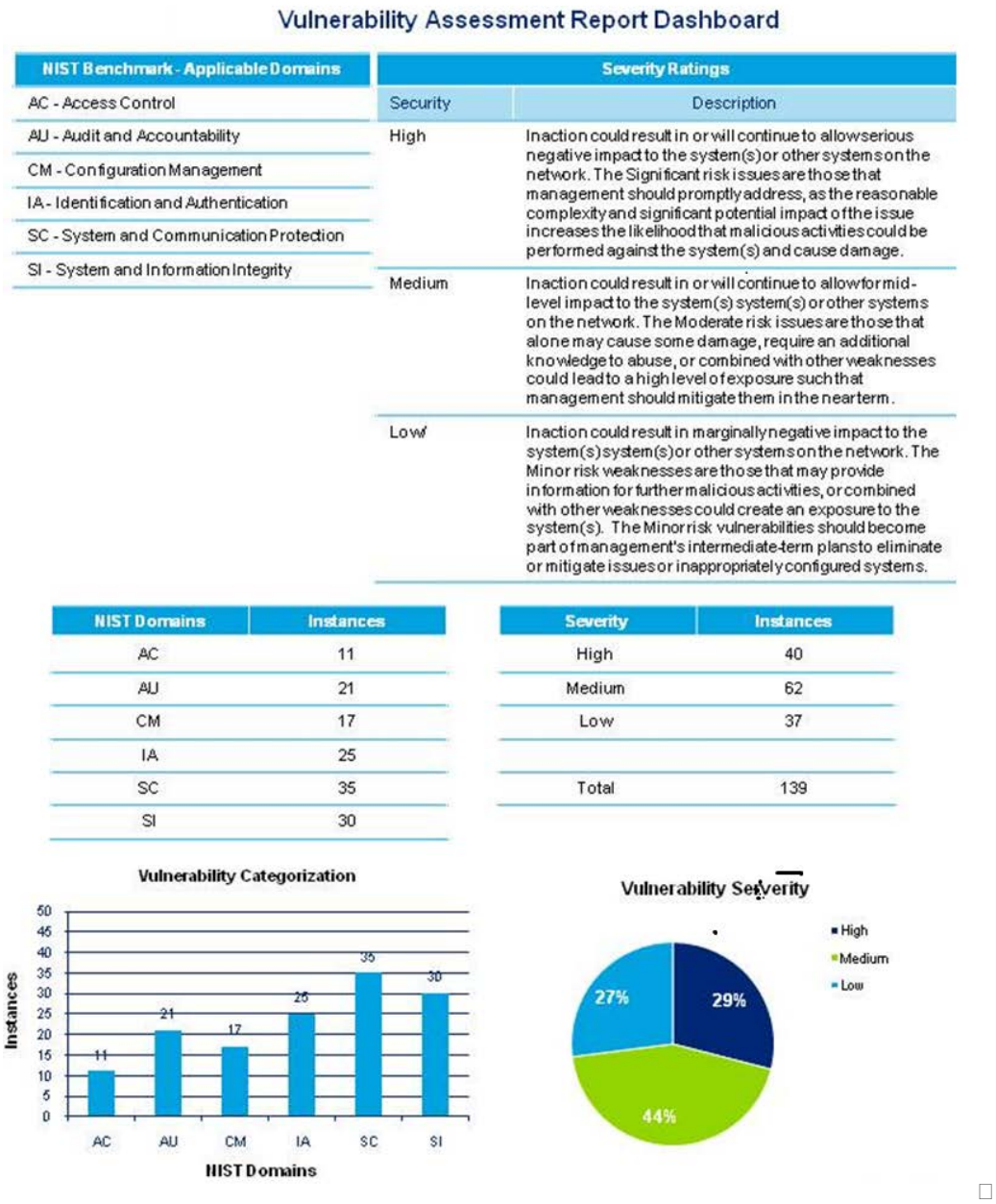


Figure 3.3.2.2-3 - Sample Vulnerability Assessment Dashboard

Step 2 –Identify potential business impacts from the identified security risks and vulnerabilities: We work with the Commonwealth and the data center stakeholders to identify the business impacts from the identified security risks and vulnerabilities including:

- Security risks for the identified vulnerabilities
- Infrastructure and business criticality for the vulnerable instances based on the risks identified
- Effort required to mitigate the vulnerability

- Remediation time frame.

Step 3 – Develop Remediation Plan: We work with the Commonwealth and the data center stakeholders to develop a remediation plan and help prioritize remediation efforts. We use the data center's standard defect tracking tool to record the identified vulnerabilities. This enables the Commonwealth to monitor the vulnerability remediation status on a continuous basis.

The Unisys Team's collaborative approach to work with the Commonwealth to perform baseline security risk and vulnerability assessment:

We work with the Commonwealth to identify a "Trusted Agent" to help facilitate the security risk and vulnerability assessment. The Trusted Agent is responsible to:

- Define scope, identify and prioritize the IT assets for the assessment
- Make decisions to proceed with applicable testing
- Coordinate the testing activity with stakeholders like IT infrastructure, application and data center service providers
- Coordinate with other commonwealth agencies (if applicable) during the testing activities
- Review the vulnerability reports and owns limited "as needed" distribution of the reports. The sensitive nature of information contained in the reports requires a specific stakeholder being responsible for managing the communication aspects
- Identify mission critical systems of the Commonwealth, business partners or affiliates, and third parties, as applicable
- Identify the time period for communication to the appropriate stakeholders for high severity security vulnerabilities identified in production environment
- Coordinate and authorize the vulnerability assessment team access to the Commonwealth data center's information technology components considered for vulnerability assessment. In order to avoid interruptions, we recommend running many of the assessment tasks during non-business hours. At the Trusted Agent's direction, we execute as many of these tasks as practical during non-business hours
- Select the servers for the baseline security risk and vulnerability assessment based on business and security criticality.

We will coordinate with the Commonwealth and the data center stakeholders to perform a backup of all data and servers for the environments, in addition to performing recovery procedures of systems, servers and applications.

In addition, we will use leading industry vulnerability scanning tools that supports PCI scanning – Tenable Nessus and Rapid 7 Nexpose in addition to using Rapid 7 Metasploit to perform penetration test. We use AppDetectivePro Pro to perform database security vulnerability assessment in addition to performing a security configuration review using leading industry standards such as IRS defined SCSEMs

2	***Training, Security***
2.A	***The Offeror's security team will meet with the Commonwealth's Security teams (OA & Agency) to***

participate in creating a comprehensive Security Program strategy. Offeror must describe its proposed approach to developing and implement a comprehensive Security Program.

We understand the importance and emphasis on security awareness training. We will work closely with the Commonwealth stakeholders to construct formal security training programs to help verify that data center personnel have a strong understanding of the Commonwealth and data center information security program, roles and responsibilities. **Figure 3.3.2.2-4** below illustrates our four phase approach (sample) to develop and deliver security training and awareness.

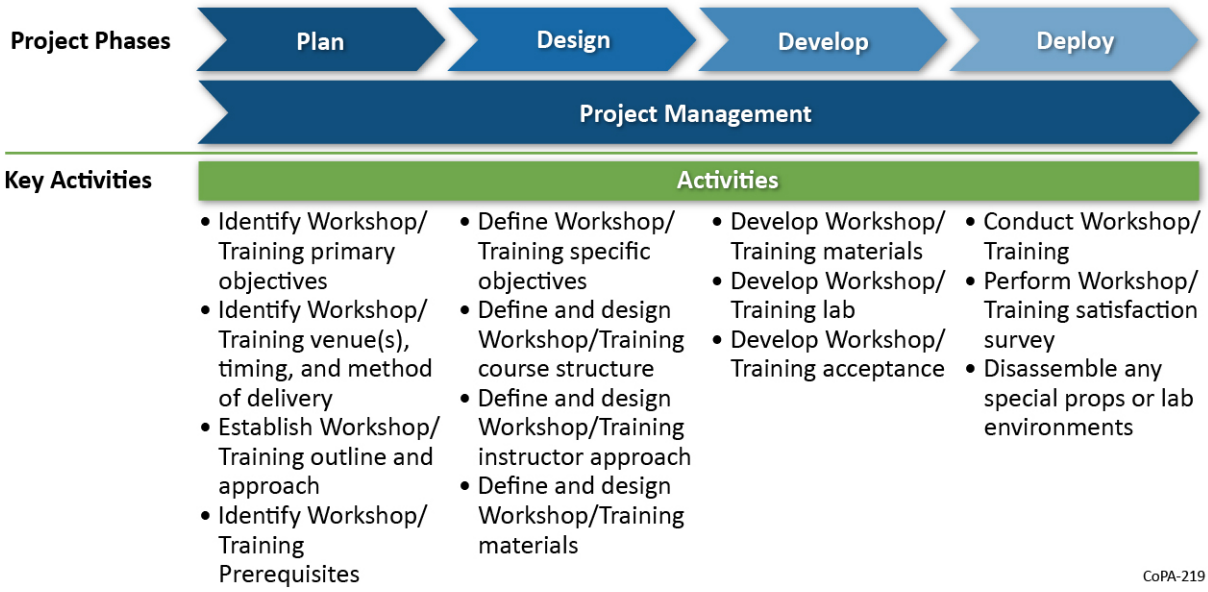


Figure 3.3.2.2-4 - Our Sample Approach to Conducting Security Training and Awareness

2.B The Offeror and the Commonwealth Security teams will develop security awareness training content consisting of the Offeror's Security Plan documentation, Commonwealth OA and agency security policy guidelines.

We will develop and deliver tailored security-related education and awareness workshops and specialized security training materials and instruction, that include:

- **"Train the trainer" program – Security Training for data center trainers –** design, develop, and conduct security training for the Commonwealth data center trainers. We will perform the following activities as part of this step:
  - Work with the Commonwealth to define the training requirements for the data center and create a comprehensive Security Program strategy
  - Identify the relevant security training requirements from the applicable regulations and standards such as IRS 1075, HIPAA and Commonwealth's Information Technology Bulletins (ITBs)

- Develop specialized security training material that describe the Commonwealth data center information security program and the individual's responsibility to protect Commonwealth data

- Work with the data center Information Security Manager, [redacted] to deliver a one-time security training session to the Unisys trainers who will train the other data center staff ("Train the Trainer" approach).

2.C Security training will be mandatory for employees, contractors and subcontractors assigned to work on the Commonwealth's Datacenter project.

Appropriate levels of training will be designated and tracked for compliance based on the specific area the employee will be working in.

Both an individual's current training status and overall attainment of group training goals must be tracked and reported in the security clearance database. These levels will range from general security awareness that all employees will participate in to task-specific security and governance requirements targeted at operations, specialist, Commonwealth agency specific regulations, or working rules needed for compliance with Commonwealth or federal mandates unique to certain Commonwealth agencies and programs. This training will be delivered both during the new hire process, and on a regular schedule to be determined during Transition as new updates become necessary.

- **Security Training for data center staff** – Conduct security training for Commonwealth data center staff. We will perform the following activities as part of this step:

  - Conduct mandatory training for all data center staff (i.e. employees, contractors and subcontractors) assigned to work on the Commonwealth's Data Center project on security awareness including Security Plan documentation and Commonwealth OA and agency security policy guidelines. Training will occur during the new hire process and at periodic intervals as deemed appropriate and necessary.

  - Designate and track appropriate levels of training for compliance per the individual staff member's role.

  - Track and report individual's current training status and overall attainment of group training goals in the security clearance database.

3 Initial Security Plan

Initial Security Plan, During the initial phase of the Transition the Offeror's security team will work with the Commonwealth's Security Team to create a Security Plan.

Begin work on draft policy and procedure documents collectively known as the Security Plan during the start of the Transition Risk and Vulnerability Assessment, which will be completed one (1) month prior to Transition activities.

Use best practice security standards (as outlined in the Requirements section of the RFP) along with past engagement experience to provide an outline that will address but will not be limited to the following: security strategy and technology roadmaps, security operations procedures, standard hardware and software security configurations, physical security policies and procedures, security incident management, private and protected data use standards, and audit procedures and reporting standards.

Offeror must describe its proposed approach to performing the following: Create a comprehensive Security Plan

Complete a Vulnerability Assessment (at the Offeror expense)

Document the agreed upon security strategy and roadmap

Document security procedures and standards

Document the security incident Management approach including (Standards, Processes, Reporting, and Escalation)

This set of documents will be used as the foundation of the Offeror's master security plan for Datacenter operations which will be reviewed and updated on an annual basis.

The Unisys Team understands that it is essential to establish the data center security plan during the initial phase of the transition. The table below in **Figure 3.3.2.2-5** illustrates how we have our custom approach to meet the appropriate RFP requirements:

Steps to develop initial security plan and related deliverables	Unisys Team's steps and activities are customized to meet the following RFP requirements
Step 1: Scope and Planning *Deliverable D-05.01: Transition Management Plan*	• Document the timelines and milestones to establish the data center initial security plan

Step 2: Create Commonwealth data center security plan *Deliverable D-07.01: Security Management Plan*	• Activity 1: Document security procedures and standards that includes o Security incident Management approach including ▪ Standards ▪ Processes ▪ Reporting ▪ Escalation o Draft policy and procedure documents collectively known as the Security Plan during the start of the Transition Risk and Vulnerability Assessment, which will be completed one (1) month prior to Transition activities. Use best practice security standards (as outlined in the Requirements section of the RFP) along with past engagement experience to provide an outline that will address but will not be limited to the following: ▪ Security strategy and technology roadmaps ▪ Security operations procedures ▪ Standard hardware and software security configurations ▪ Physical security policies and procedures ▪ Security incident management ▪ Private and protected data use standards, and ▪ Audit procedures and reporting standards. • Activity 2: Document the agreed upon security strategy and roadmap • Activity 3: Document the data center IT asset inventory • Activity 4: Define the data center security risk framework • Activity 5: Establish the initial security plan
Step 3: Perform vulnerability assessment *Deliverable D-09.01: Baseline Security Risk and Vulnerability Assessment Report*	Complete a Vulnerability Assessment
Step 4: Perform data discovery and classification to indicate level of sensitivity *Deliverable D-07.01: Security Management Plan*	Commonwealth responses to Q37 and Q46 of round 1 part 1 include data classification and identifying the data centers' data encryption requirements. The related activities include: • Activity 1: Data Classification and • Activity 2: Data Discovery.

Figure 3.3.2.2-5 - Customer Security Plan Approach

We have described our approach to perform the steps for establishing the initial security plan below:

Step 1 – Scope and Planning: During this first step, we will work with the Commonwealth to identify key data center stakeholders and document the security plan requirements, scope, objectives, milestones and timelines.

Step 2 – Create Commonwealth Data center Security Plan: As part of this step, we work with the Commonwealth to define and establish the data center's initial security plan that includes the following activities:

a. Activity 1: Establish the data center information security procedures and standards

b. Activity 2: Document the security strategy and roadmap

c. Activity 3: Document the data center IT asset inventory

d. Activity 4: Define data center security risk framework

e. Activity 5: Document and establish the data center initial security plan

Activity 1: Establish the data center information security procedures and standards

The Unisys Team will develop and establish the Commonwealth data center's information security policy framework that documents the appropriate security procedures and standards. The data center's information security policy framework will play an important role in the effective implementation of the data center information security programs and its security plan. Information security policy framework helps provide security risks are minimized and that security incidents are effectively responded to. This framework will assist the data center personnel to participate in the Commonwealth's efforts to secure its information assets and people. The effectiveness of the information security policy framework is dependent on the awareness within the data center personnel. As part of this project, we use the following leading industry practices to help establish an effective data center information policy framework:

Have you heard?

Unisys Teaming partner, Deloitte has established a Center for Cyber Innovation (CCI) that develops cyber solutions for clients in the public and private sectors who are seeking to improve information sharing, collaboration and performance by harnessing the power of increasingly interdependent networks.

- U.S. Department of the Interior's Information Technology Security Policy Handbook based on NIST SP 800-53 Recommended Information Security Controls for Federal Information Systems
- SANS Institute's Information Security Policy – A Development Guide for Large and Small Companies.

We use the Commonwealth's established security policy framework – Information

Technology Bulletins (ITBs) to help establish the data center's information policy framework. **Figure 3.3.2.2-6** below illustrates the high level information security policy framework.

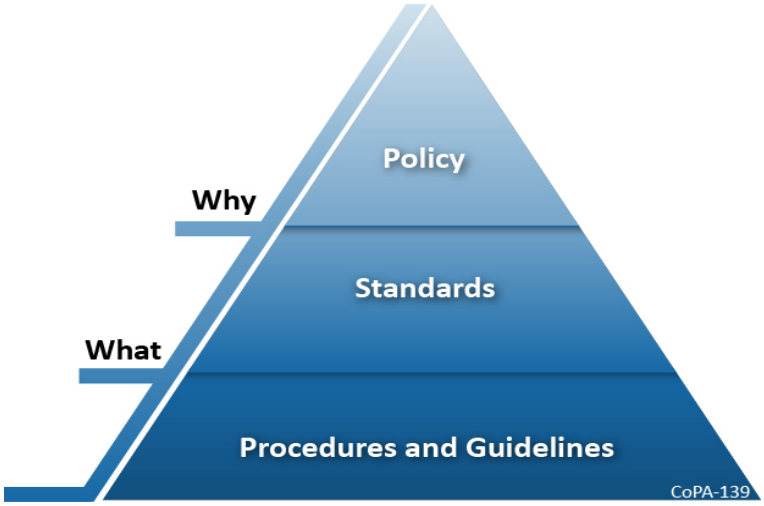


Figure 3.3.2.2-6 - Proposed data center Information Security Policy Framework

We have described the proposed structure of data center's information security policy framework in the table below along with sample policies, standards and procedures.

Information security policy framework	Definition	Sample policies, standards and procedures
"Policy" for identified and prioritized security domain	Policies are high-level statements regarding principles and requirements that set the tone and temperament of management's risk tolerance. A policy is a governing principle that provides the basis for standards and carries the highest authority in the organization.	• IT Risk Management • IT Compliance Management • Identity and Access Management (IAM) • Asset Management • Threat and Vulnerability Management
"Standards" for prioritized domain	Information Security Policy, Encryption Policy, Data Retention Policy, Privacy Policy	Sample IAM standards • Account provisioning • Role management • Entitlement review • Access management.

"Procedures and Guidelines"	Procedures are detailed step-by-step activities and tasks that personnel are to follow when performing certain aspects of their job responsibilities. They may include corporate, local and business unit specific procedures.	Sample Role management procedures • Role definition guidelines • Role decommissioning procedure

Key procedures and standards: The information security policy framework described above will include the following key policies, standards and procedures.

- Security operations procedures
- Standard hardware and software security configurations
- Physical security policies and procedures
- Security incident management
- Private and protected data use standards
- Audit procedures and reporting standards.

Security Incident Management Approach: As part of this activity, we will work with the Commonwealth to define the security incident management approach that includes establishing supporting standards, processes, reporting and escalation procedures. We will use guidance established by the leading industry standards and Commonwealth policy that includes and leading industry standards including

- Commonwealth Information Technology Bulletin (ITB)-SEC024 – IT Security Incident Reporting Policy
- NIST SP800-61 rev 2 – Computer Security Incident Handling Guide
- Internal Revenue Service (IRS) publication 1075
- US Social Security Administration (SSA)
- Criminal Justice Information System (CJIS) and
- Payment Card Industry (PCI) Data Security Standards (DSS).

Activity 2 – Develop the data center security strategy and roadmap

In addition to the information security policy framework, we will analyze the results of the baseline security risk and vulnerability assessment to help develop a security strategy and technology roadmap. A sample security and technology roadmap is illustrated in **Figure 3.3.2.2-7** below:

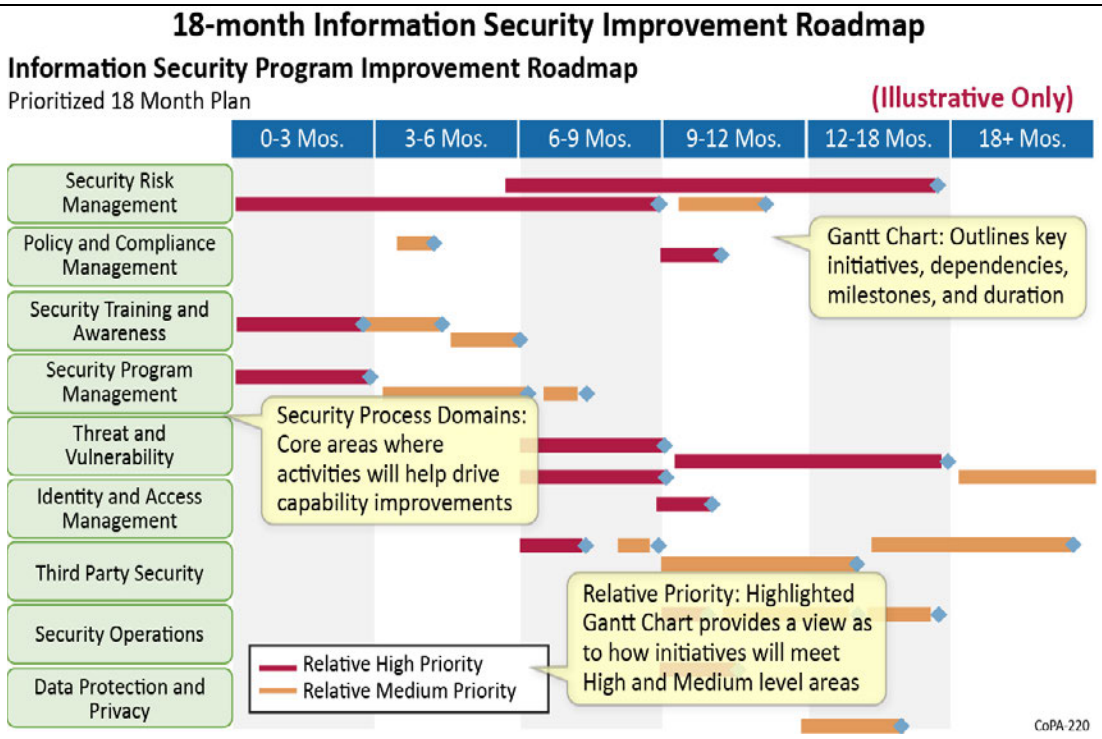


Figure 3.3.2.2-7 - Sample Information Security Improvement Roadmap

Activity 3: Document the data center IT asset inventory

We will document and establish the Commonwealth data center IT asset inventory that includes the current hardware and software security configuration. The Unisys Team will maintain IT asset current as part of ongoing data center operations and document it as part of the annual security management plan.

Activity 4: Define data center security risk framework by rationalizing individual security requirements from Commonwealth and Federal regulations, policies and standards.

From our experience of working with the Commonwealth, we understand that the data center needs to appropriately protect the citizen information using relevant regulations, policies and standards. The citizen information includes sensitive datasets such as social security numbers (SSNs), personal health information (PHI), child abuse data and criminal history records. Each of these sensitive datasets requires appropriate protection measures from several disparate regulations and standards as illustrated in **Figure 3.3.2.2-8** below.

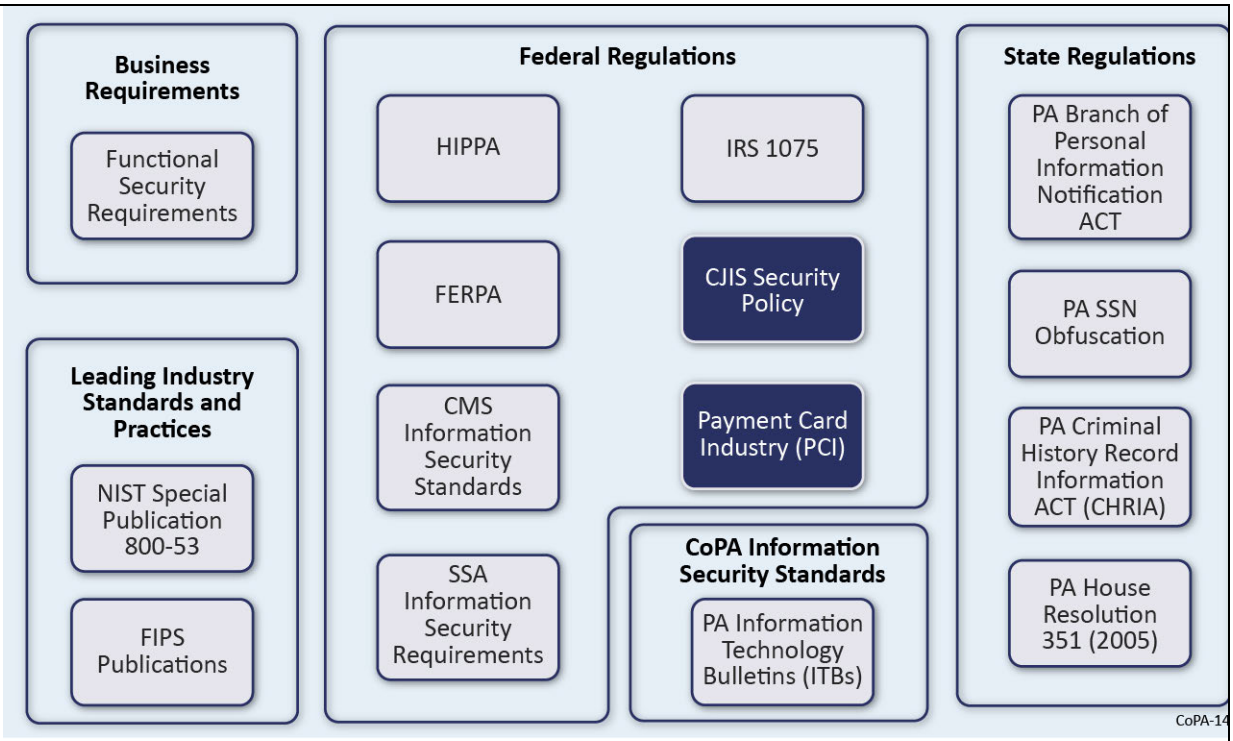


Figure 3.3.2.2-8 - Sample List of Applicable Regulations, Industry Standards and Leading Industry Practices

The Unisys Team will establish the data center's initial security risk framework based on the known security and privacy requirements. These requirements are integrated from the relevant Commonwealth policies, industry standards, and State and Federal regulations (illustrated in the above figure). During data center transition, we use this security risk framework to define the security plan and design data protection controls that meets the relevant regulations and business requirements.

We use our Unisys Teaming partner Deloitte's existing public sector security risk framework with the Commonwealth's specific regulations and standards. The use of such an accelerator allows us to "hit" the ground running. **Figure 3.3.2.2-9** below illustrates our approach to identify, correlate and integrate security regulatory requirements to define the data center security risk framework.

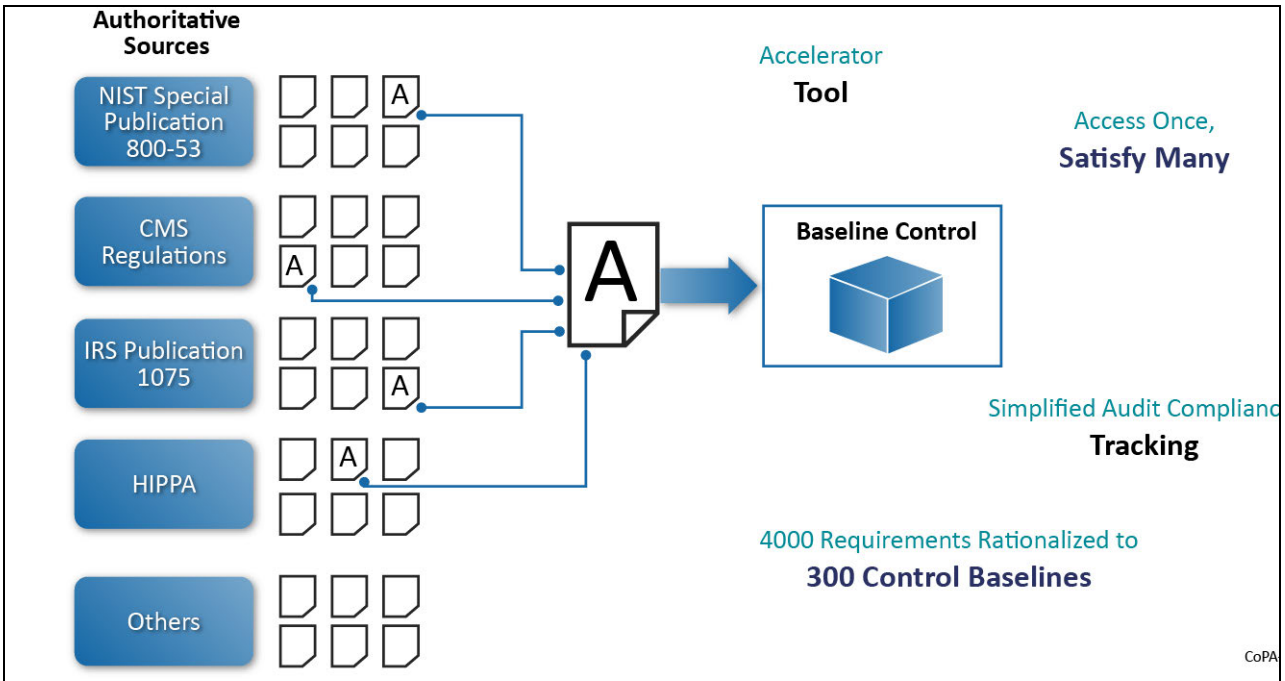


Figure 3.3.2.2-9 - Our approach to identify data protection requirements using the data center security risk framework

Activity 5: Document and establish the data center initial security plan

We will develop a data center security plan based on leading industry standards; NIST SP800-18 (a RFP requirement specified by Q50 of round 1 part 2) and NIST SP800-53 rev 4. We work with the Commonwealth to identify the applicable security domains that comprise the breadth of the data center's information security plan, based on the security domains listed by NIST SP800-53 rev 4. The data center security plan includes (but not limited to) the following information security domains illustrated in the **Figure 3.3.2.2-10**. In addition, we also use the Centers for Medicare and Medicaid Services (CMS) security plan template to define and maintain the appropriate security controls.

Figure 3.3.2.2-10 - Sample data center security plan domains

After identification of the information security domains, we work with the Commonwealth to determine individual security areas that drive corresponding information security domains. The maturity of information security domains and the program are dependent on the effectiveness of metrics established to monitor the security controls to address corresponding information security areas. As an example, the key individual security controls for three of the security domains include:

Information Security Domain	Information security controls	
Access Control	•□Access Control Policy and Procedures •□Account Management •□Access Enforcement •□Information Flow Enforcement •□Separation of Duties •□Least Privilege	•□Unsuccessful Login Attempts •□System Use Notification •□Concurrent Session Control •□Remote Access •□Wireless Access •□Access Control for Mobile Devices
Incident Response	•□Incident Response Policy and Procedures •□Incident Response Training	•□Incident Handling •□Incident Monitoring •□Incident Reporting

Physical and Environmental Protection	• Physical and Environmental Protection Policy and Procedures • Physical Access Authorizations • Physical Access Control • Monitoring Physical Access • Visitor Control	• Access Records • Emergency Lighting • Fire Protection • Temperature and Humidity Controls • Water Damage Protection • Delivery and Removal

Annual update of data center security plan: Using the initial security plan as base, we will perform an annual review of the data center security plan and update the security controls based on updates to regulations, policies, standards and leading industry practices.

Step 3 – Perform Vulnerability Assessment: We will conduct a one-time security vulnerability assessment on the data center's IT infrastructure to help identify potential security vulnerabilities and suggest mitigation controls, as part of baseline security risk and vulnerability assessment, described earlier in this section.

Step 4 – Perform data discovery and classification to indicate level of sensitivity: We perform data discovery and data classification assessment to indicate level of sensitivity of Commonwealth's PII and identify presence of PII data at rest. This step includes the following activities – Data classification and Data discovery, as illustrated below:

Activity 1 – Data Classification: We will conduct and facilitate five workshops with the Commonwealth stakeholders to define a data classification standard for the Commonwealth's Personally Identifiable Information (PII) based on sensitivity of PII. For example, some of the categories include

- Special handling PII (that contains SSN, driver license number, FEIN, and Medicare ID)
- Protected Health Information
- Individual information
- Sensitive PII (i.e. racial or ethnic origins, religious or philosophical beliefs, trade-union membership, and criminal convictions).

Activity 2 – Data Discovery: We perform a one-time assessment using the Symantec Data Loss Prevention (DLP) solution's data discovery tool on the Commonwealth selected data center IT infrastructure consisting of servers and databases to identify the PII data at rest. We perform the following tasks as part of this activity:

- Document the results of the data discovery assessment in the IT asset inventory
- Use the data center security risk framework to identify appropriate data encryption requirements to appropriately protect the PII data and meet the relevant regulations, policies and standards.

4 Staff Background Checks

4.A Conduct required background checks for its employees working on the Commonwealth Datacenter project.

Offeror must describe its proposed approach to conducting required background checks for Offeror staff.

In accordance with Appendix A section 44, the Unisys Team will perform fingerprint background checks consistent with ITB-SEC009 and CJIS policy on all Unisys Team personnel providing support or services for the Commonwealth. As part of our ISO27001 certification, we perform an annual 3rd party/subcontractor review as well. Unisys has been completing Commonwealth specific background checks since the beginning of the Data PowerHouse contract. The Unisys Team will provide written confirmations to the Commonwealth when the background checks are conducted. Please refer to Schedule F, Section 3.2.1.1.3 Subcontractor Management for more details on our process for performing background checks. The onboarding procedure described in this section details the background check process.

4.B Where appropriate, use identity management tools to manage access to the systems requiring access by its employees.

For systems where the Offeror is unable to use its identity management system, assign staff to manage the access.

Train Offeror employees on his or her responsibilities within the contract. For logical and physical access to Commonwealth Co-location facilities and environments not managed by the Offeror, the Commonwealth's security access request process will be followed.

The Unisys Team takes a layered approach to security. Each facility has both physical and logical security in place. Physical security prevents unauthorized personnel from gaining access to the systems. Perimeter security includes cameras and an active physical security presence. All facilities include guard-controlled access to interior spaces. Access control systems include access to and within the facilities in all data centers. Access control includes a combination of identity management tools, namely keycard, keypad and biometric devices. In addition, access control systems including keypad and biometric authentication capabilities are available.

The Unisys Team provides dedicated network/security support staff at its facilities 24x7x365, coupled with automated tools that provide real-time notification of suspected security intrusion events. Unisys Security Operations Center (SOC) is comprised of security support staff and a suite of automated tools that provide comprehensive 24x7x365 monitoring, alerting, and response to security events.

The Unisys Team will use innovative identity management tools, i.e. password vaults and remote administration, for system administrators. These tools allow Unisys to actively control and limit the number and use of system administrator passwords that exist for Commonwealth privileged access and easily monitor and block the actions of system administrators.

All employees and subcontractors are trained regarding proper physical and logical access to Commonwealth facilities, environments, and systems.

In support of the Commonwealth's security needs, Unisys will establish an On-boarding and Off-boarding procedure documented within the CCPM.

The Unisys Team On-boarding procedure will cover the following activities:

1) Conduct background checks for members of the program team in accordance with Appendix A Section 44 as defined within ITB-SEC009. Access will not be granted to new members until successful completion of the background check.

2) Provide the team member with the program's security training

3) Submit requests to add the user with the required privileges to the appropriate identity management system or, if not supported by an identity management system, individual systems.

4) Submit requests to permit user access to the Unisys Team and Commonwealth's facilities as required by the team member's responsibilities and tasks. For Commonwealth facilities, the Unisys Team will submit the request through the Commonwealth's security access request process.

4.C For off-boarding, update security clearance database with the status of Offeror employee and concurrently update its identity management tool to ensure the access is revoked.

Provide a monthly report describing personnel actions including but not limited to; new hires, terminations, any change in employee status/duties, etc.,

The Off-boarding procedure will include the following activities.

1) Notification of the team member's change of status and request updates to the security clearance database.

2) Submit user permission revocation change requests for all identity management tools and individual systems to remove the team member's access to the Commonwealth systems.

The Unisys Team will also provide a monthly report for the Commonwealth regarding onboard and off-boarding activities, including new team members, terminations, and changes in employee duties.

5 DR, Data Recovery Transition Activities

5.A Conduct knowledge transfer during the initial phase of the Transition, including review of Commonwealth DR plans and review of Third Party DR contracts.

Offeror must describe proposed approach to support the Tiered DR Services.

5.B The Offeror must also update the DR plan contact information and any changes made in the first six (6) months of Transition.

The Unisys Team will conduct knowledge transfer during the initial phase of the Transition, including review of Commonwealth DR plans and review of Third Party DR contracts.

1. Review Existing Agency DRPs. The Commonwealth seeks a regular reviews of the Agency DRPs. The Unisys IT Risk Manager will take charge of completing Agency-by-Agency reviews of existing DR plans and Third Party DR contracts as part of transition activities. Unisys expects the reviews will likely coalesce into a broadly comprehensive Disaster Recovery strategy that utilizes the Unisys-maintained Disaster Recovery site with Tiers of DR services. The DR

solution includes not only the same components available in the Production environment but also a rich diversity of DR Tiers which will allow the Commonwealth to build sufficient high availability through the Disaster Recovery offering to match the Production equivalent for any application. For more details on the Tiered DR solution, refer to Schedule F, Section 3.1.3 Data Center Architecture and Technology.

The Unisys IT Risk Manager expects that the Commonwealth is currently served by a wide variety of Disaster Recovery plans maintained by each Agency. On average Unisys expects that many agencies have adequate plans but within the variety Unisys expects to discover under-funded plans with significant gaps and over-funded plans that likely protect non-critical assets. Unisys has deep experience supporting current DPH disaster recovery plans. By choosing Unisys as a partner the Commonwealth benefits both from this experience as well as the Unisys-implemented [redacted]. Unisys seeks to bring all Agency DRPs within the proposed LDRPS framework so that Unisys can help the Commonwealth arrive at a standardized agency approach to DR.

2. Online Disaster Recovery Tool. The Commonwealth has appropriately identified a need for an easy-to-use Online Disaster Recovery Tool that will allow all agencies to maintain their diverse DRPs within a single tool. The Unisys IT Risk Manager will also coordinate the input of existing Agency DRPs into this single tool as part of transition activities.

The Commonwealth is familiar with the LDPRS tool which is currently in place to manage the DRP related to IBM Mainframe services at the [redacted] facility. The Unisys Team will exploit the full capabilities of the tool to build strong:

- Crisis management plans to fit each Agency's operational structure.
- Technology recovery plans to match a matrix management approach, including dependency mapping for the infrastructure supporting your applications.
- Critical application recovery plans to smoothly interface with your infrastructure recovery plans.
- Process or departmental recovery plans to support your planning decisions and strategies and to identify dependencies between critical business processes.
- Site event management plans to document how to deal with a specific incident at a particular business location.

Working with the Unisys Team, the LDRPS tool reduces the time needed to train users by providing step-by-step guidance to plan builders.

We will also update the DR plan contact information and any changes made in the first six (6) months of Transition. More detailed information about the DR Plan can be found in Schedule F, Section 3.2.2.4 DR Plan and Schedule F, Section 3.2.5.3 DR Infrastructure on Demand.

Unisys Team Experience

Unisys has managed and maintained the full data center operations of De Beers, the world's leading diamond company, since 2011. A De Beers executive stated, "We are pleased with the role Unisys has played in this effort. Unisys ability to fully manage our data center environment, and provide various levels of technical and end user support, will play an important role in

enabling business and IT strategies well into the future." As part of taking over data center operations for De Beers, Unisys conducted a risk assessment which identified that the company's current IT model contained a number of single points of failure – where the disruption of mission-critical components could significantly hinder operations. After conducting the risk assessment, Unisys transformed their IT infrastructure to be more available, resilient, and flexible and also provided proven disaster recovery capability."

Unisys has provided staff security training for countless clients including the Board of Airline Representatives New Zealand (BARNZ) which represents international airlines which fly into New Zealand, including Qantas, Cathay Pacific, Air Pacific, Emirates, Malaysian Airlines and Singapore.

Unisys has successfully supported the Department of Justice (DOJ) Asset Forfeiture Management System (AFMS) since our initial engagement in 1995, and we continue to provide the AFMS program's Consolidated Asset Tracking System (CATS) Program Management Office with comprehensive system security for INFOSEC applications support. Unisys tailored the Certification and Accreditation process to consider the specific mission, threat environment, and the development and/or implementation of necessary countermeasures to mitigate threats. We developed the System Security Plan, Security Test and Evaluation (ST&E) Plan, Rules of Behavior (RoB), IT Contingency Plan (ITCP), Security Awareness and Training Plan (SATP), Incident Response Plan (IRP), and Configuration Management Plan (CMP), as required to certify and accredit the system. Included was a risk assessment which required completion of a vulnerability scan and penetration test.

The Data PowerHouse complies with applicable INFOSEC requirements specified by the Commonwealth, DOJ, FBI, IRS, and the HIPAA, including secure configuration of Commonwealth operating systems, installation and maintenance of security management software, change management procedures, problem resolution and escalation procedures, and semi-annual background checks and security awareness training for Unisys employees assigned to support the Commonwealth. Unisys established a security management infrastructure to oversee the development and implementation of security policy, procedures, and guidelines. This infrastructure enables participation in security implementation at all levels within the project and serves a vital part in security risk mitigation.

Benefits to the Commonwealth

The deep, diverse security experience the Unisys Team has acquired over years supporting both federal and state governments and commercial partners will be leveraged, along with the extensive security experience of Deloitte, to provide comprehensive security transition support for the Commonwealth. Planning is a key for any successful transition; therefore the Unisys Team will follow its proven methodology for developing and implementing a security plan for the Commonwealth. The Unisys Team will draw upon the expertise it has gained from mitigating a wide gamut of security vulnerabilities in various environments to protect the Commonwealth and its assets. The Unisys Team's security experts will provide understandable, practical security training to properly train Commonwealth staff.

Attachments to Schedule F – CoPA Datacenter Statement of Work

The following attachments are referenced in Schedule F – Datacenter Statement of Work:

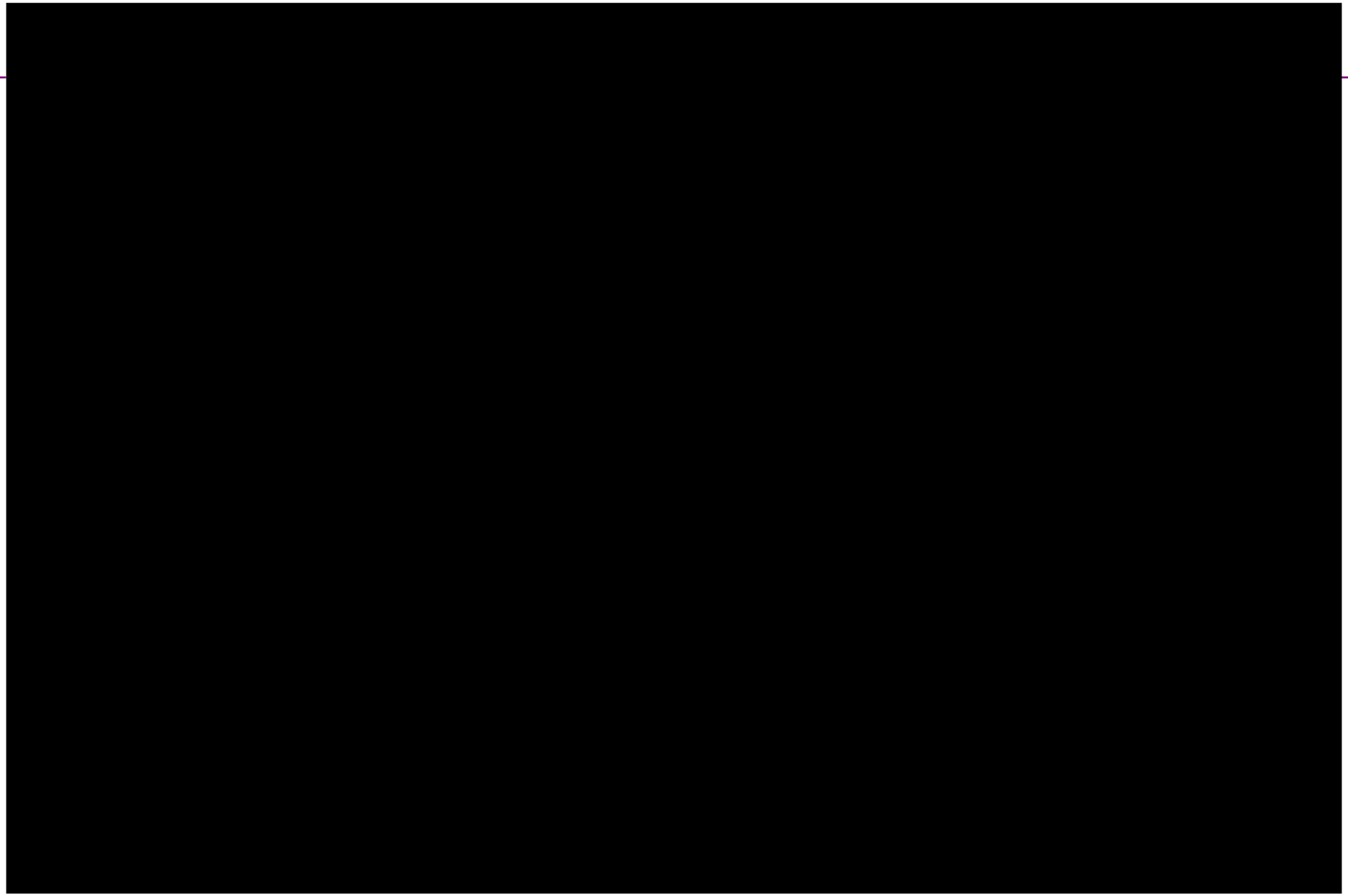
- Attachment F-1 – DPH Monthly Service Performance Management Meeting
- Attachment F-2 – Managed Services IES and Unisys – Measurement Report
- Attachment F-3 – AMOS Enterprise Architecture Project SOW
- Attachment F-4 – Technical Architecture Deliverable Guide
- Attachment F-5 – Sample SAP Sizing Estimate
- Attachment F-6 – Sample Capacity Management Plan
- Attachment F-7 – IES DPH Capacity Planning Report
- Attachment F-8 – Sample Monthly Server Capacity Report
- Attachment F-9 – Commonwealth of Pennsylvania – Office of Information Technology Enterprise Data Center Security Management Plan
- Attachment F-10 – Sample Security Assessment Report
- Attachment F-11 – Sample Performance Reports
- Attachment F-12 – Application Migration Plan.

This page intentionally left blank.

Attachment F-1 – DPH Monthly Service Performance Management Meeting

This attachment shows the monthly performance report delivered at an agency level.

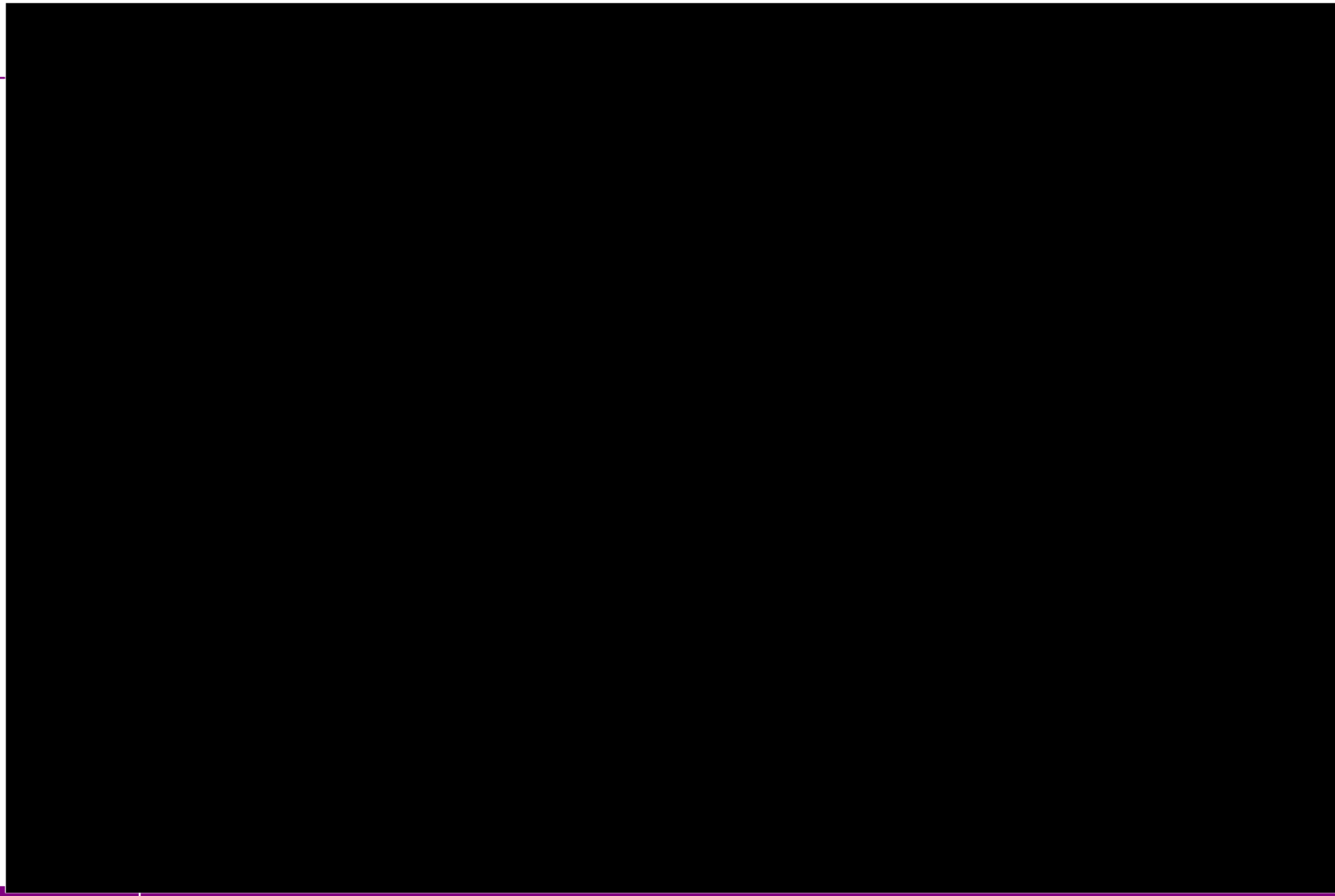
This page intentionally left blank.



DPH Confidential

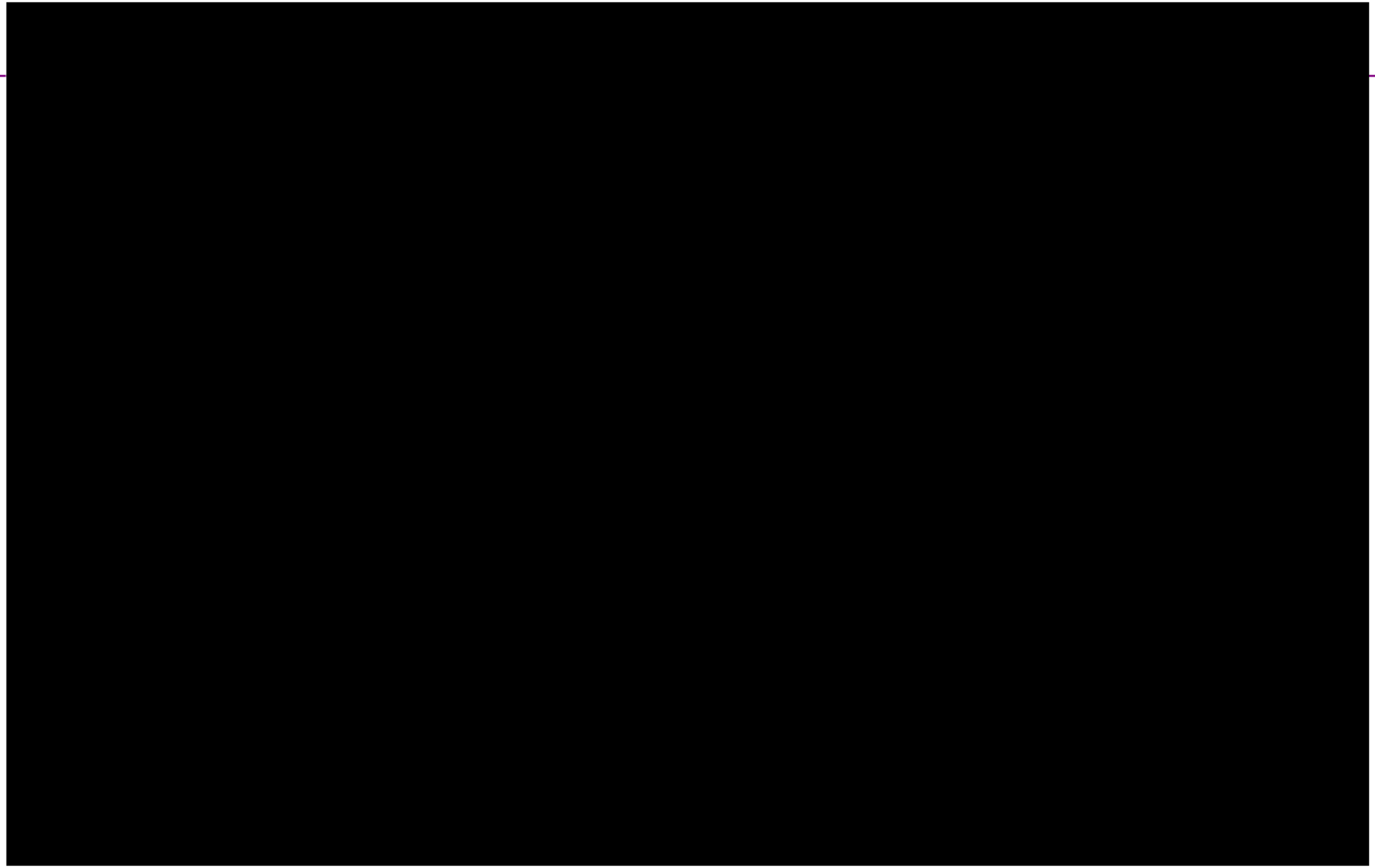
UNISYS

DPH Confidential



DPH Confidential

DPH Confidential



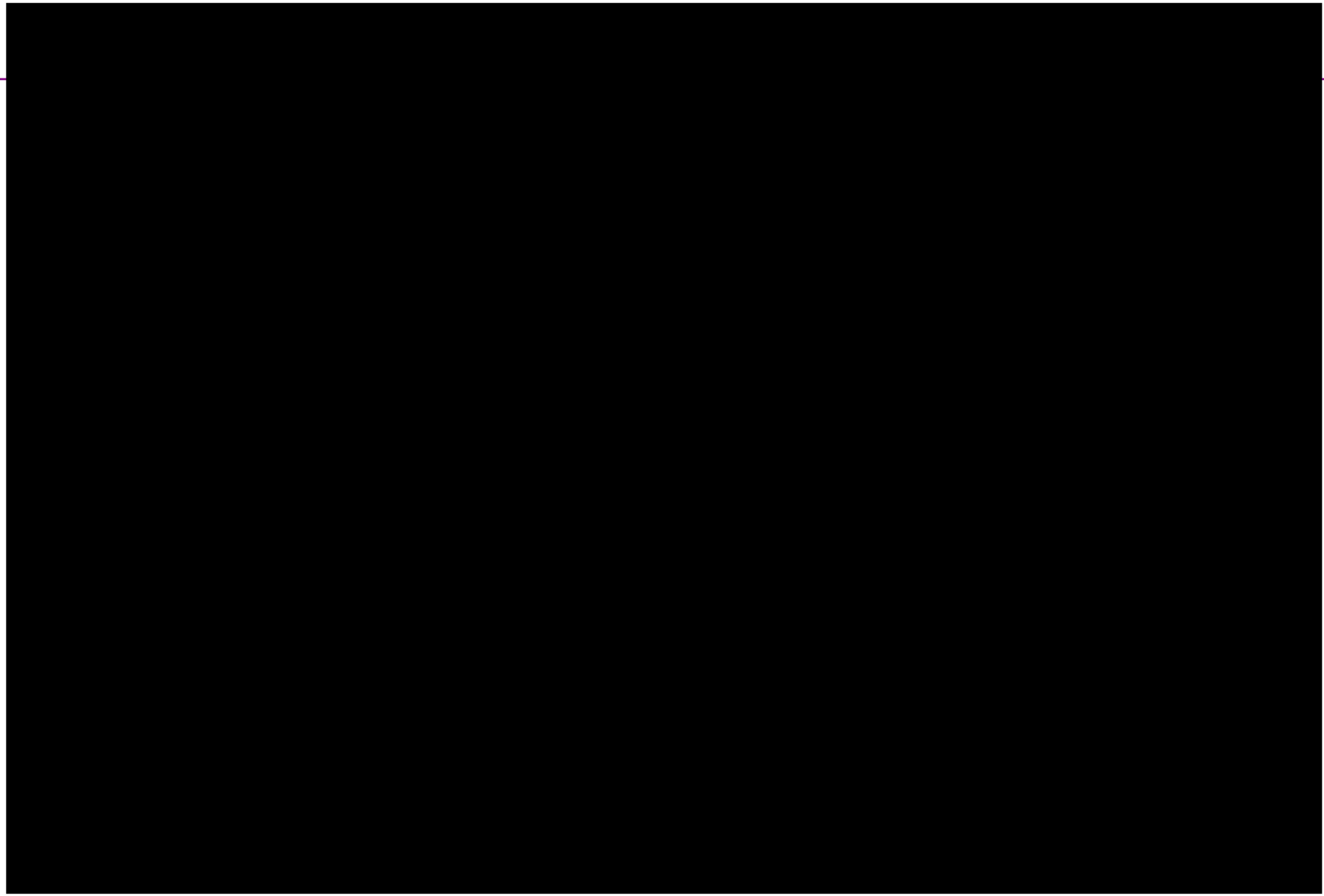
UNISYS

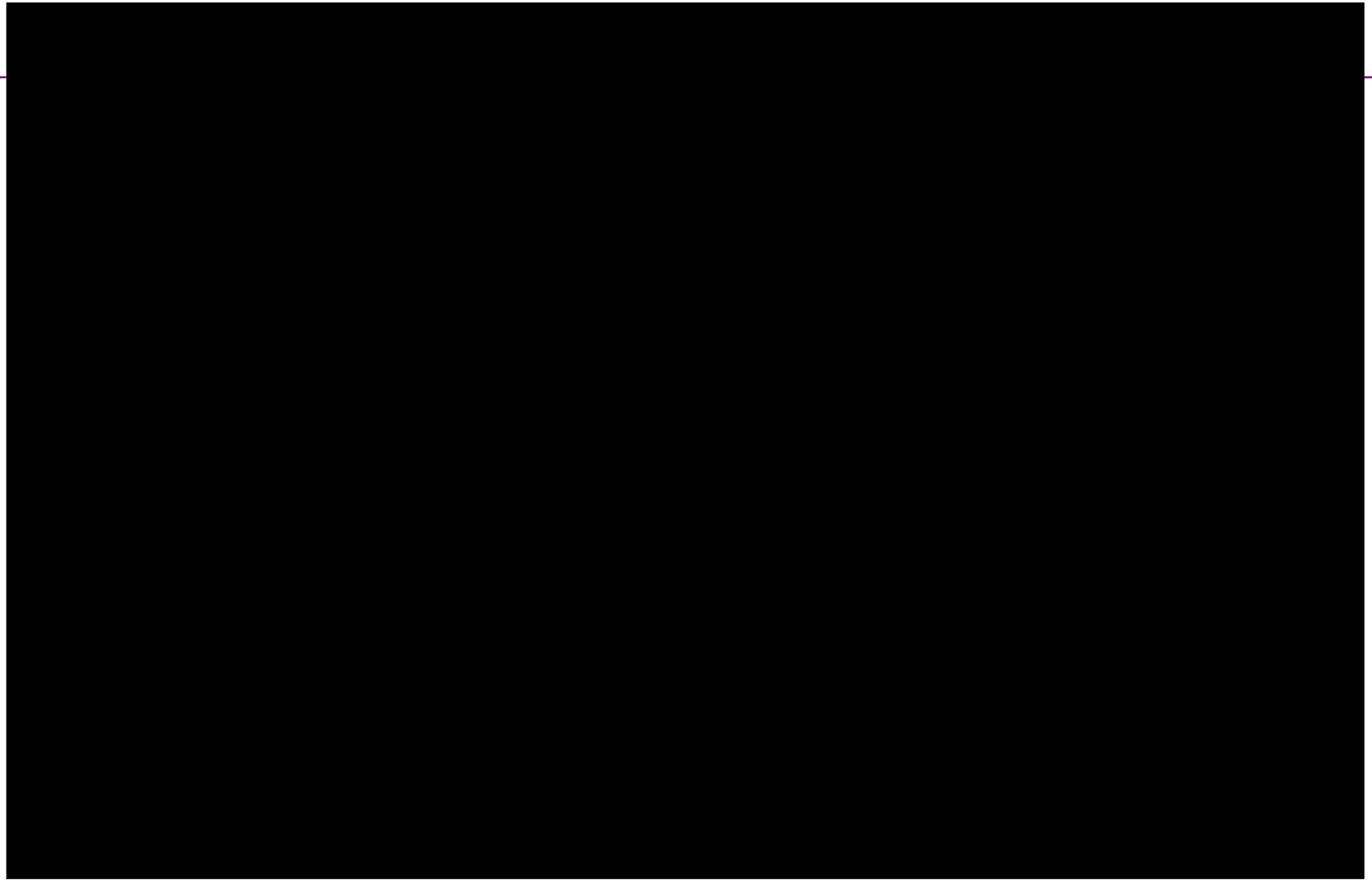
DPH Confidential

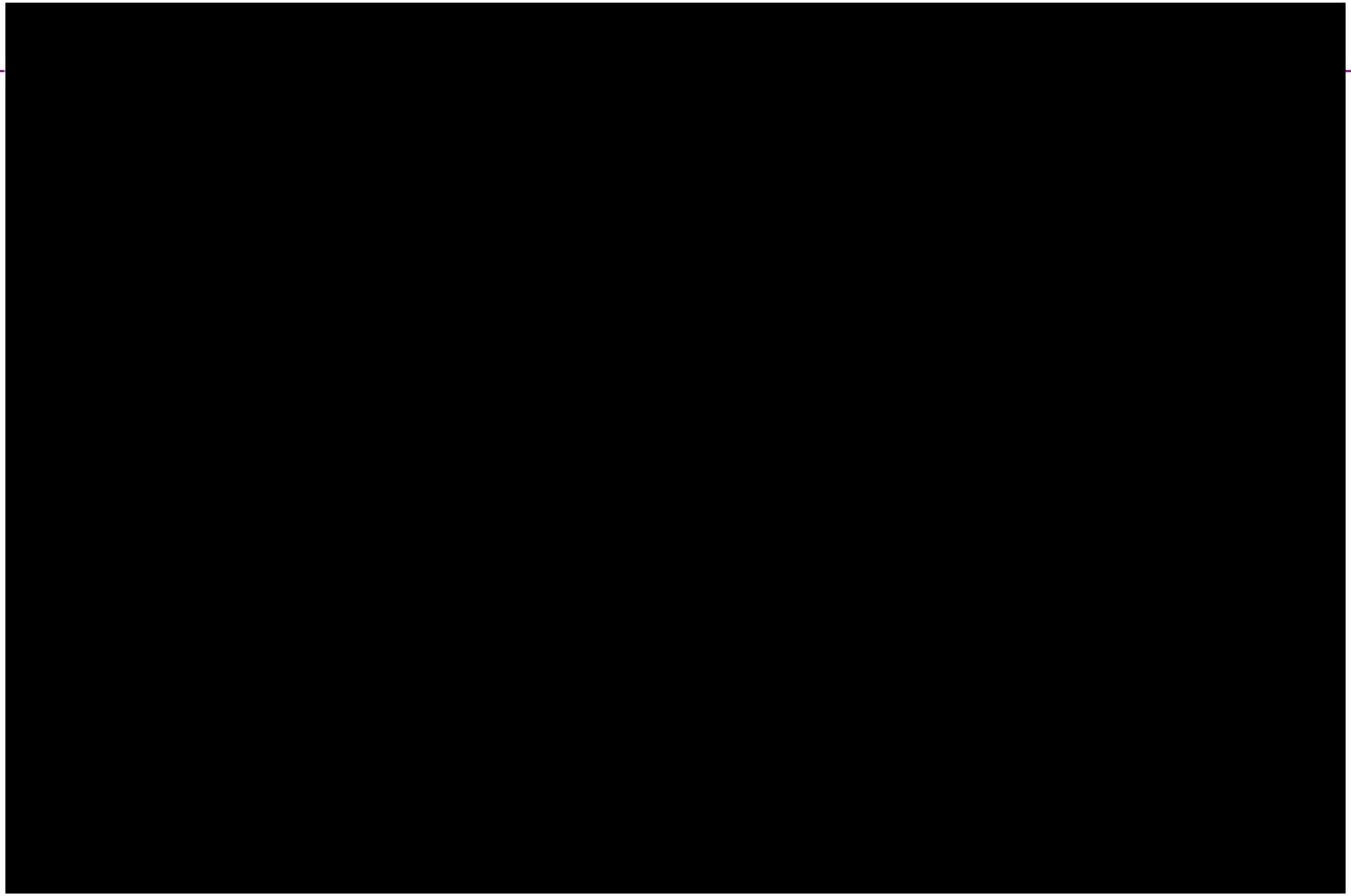
DPH Confidential

UNISYS

DPH Confidential





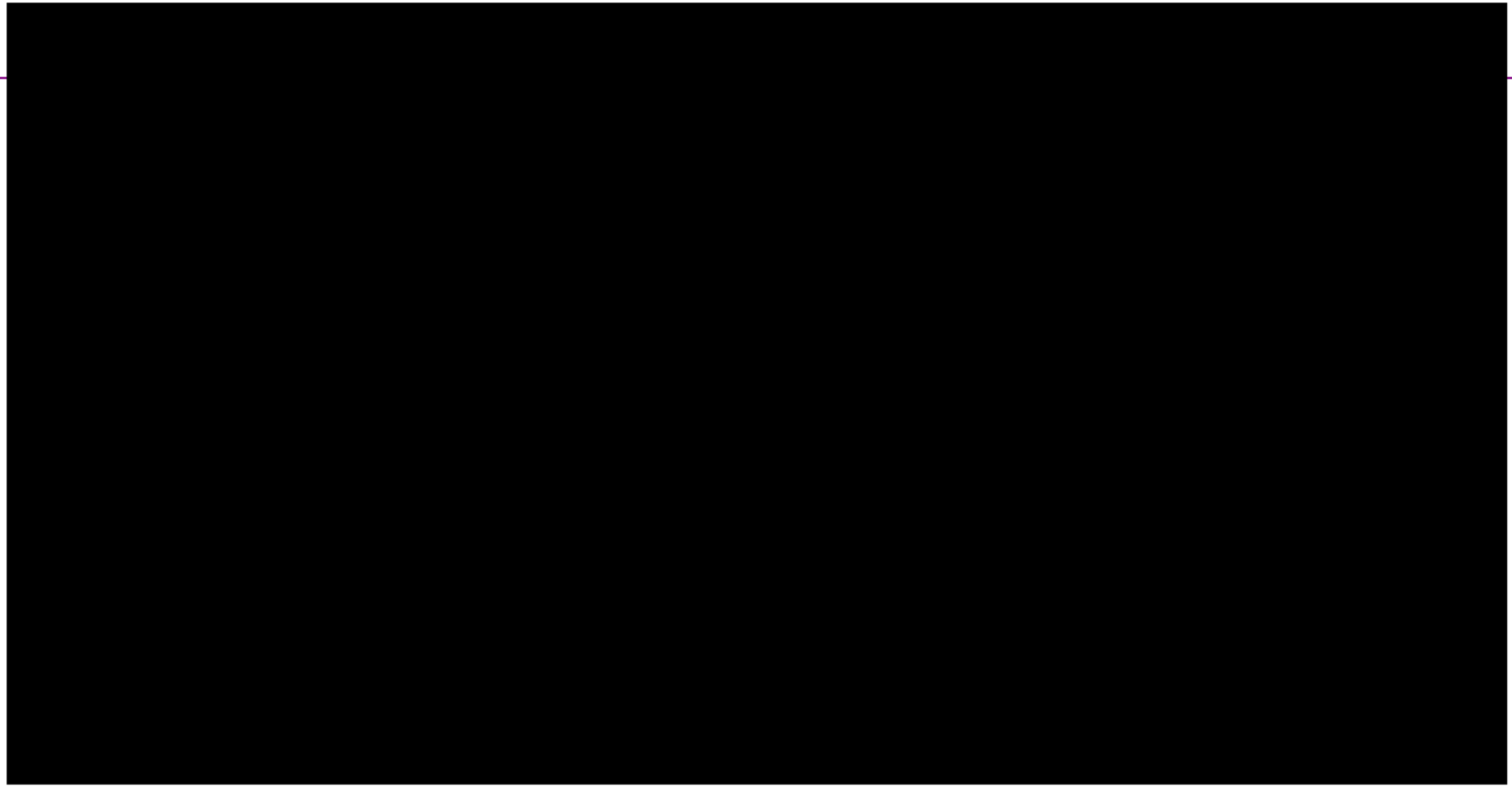


Data PowerHouse

UNISYS

DPH Confidential

DPH Confidential



DPH Confidential

UNISYS

DPH Confidential

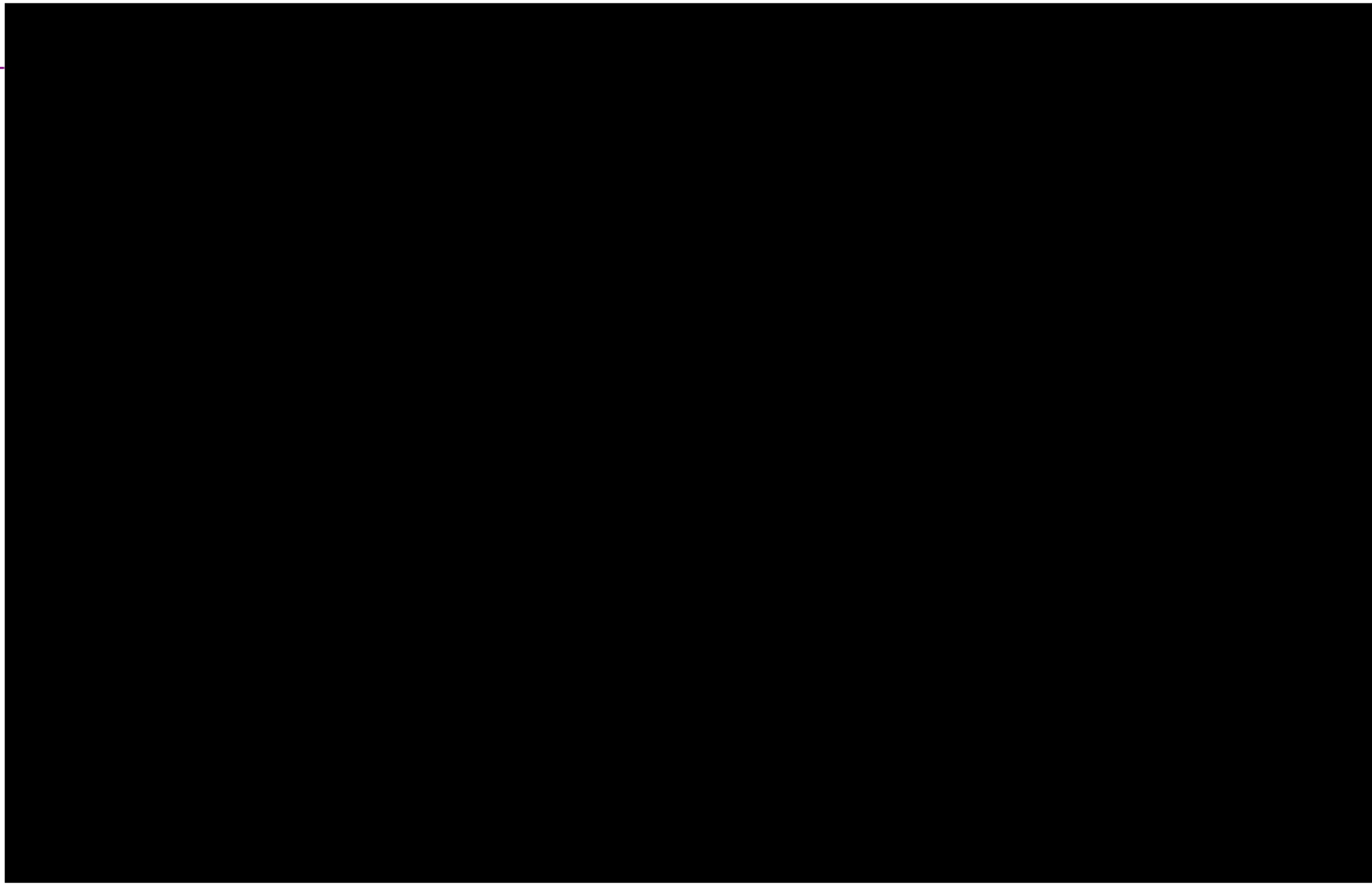
UNISYS

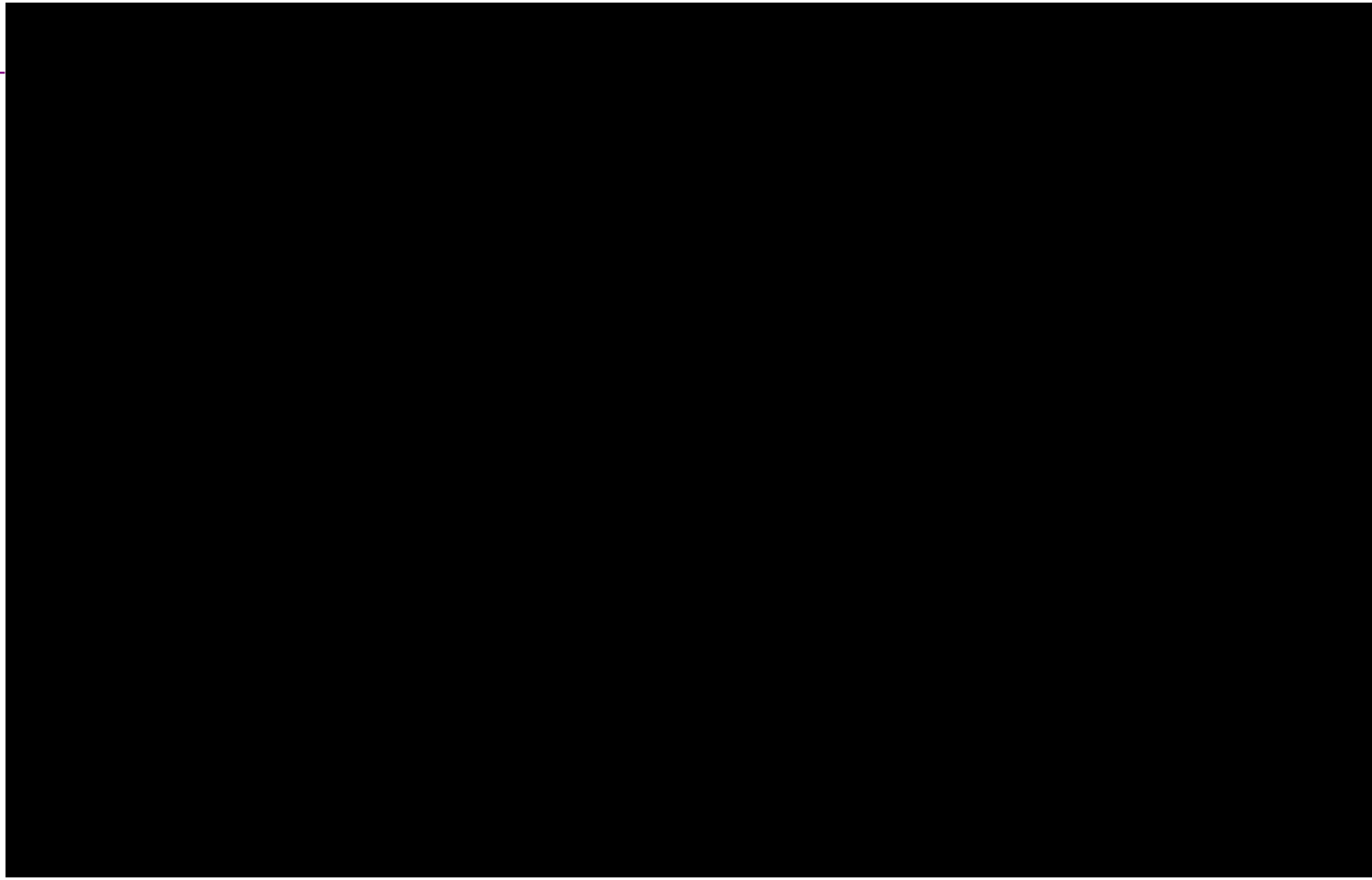
DPH Confidential

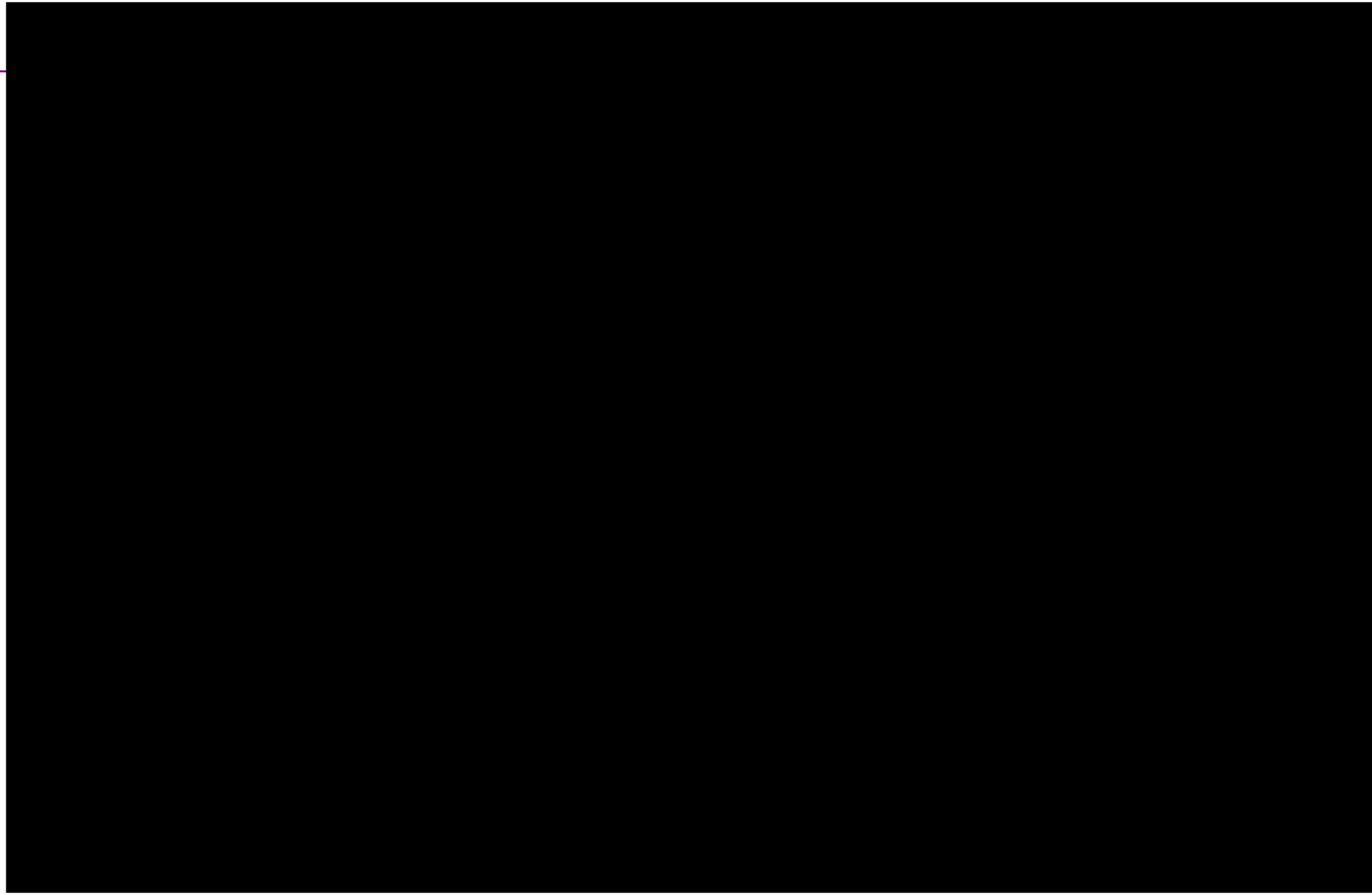
UNISYS

DPH Confidential

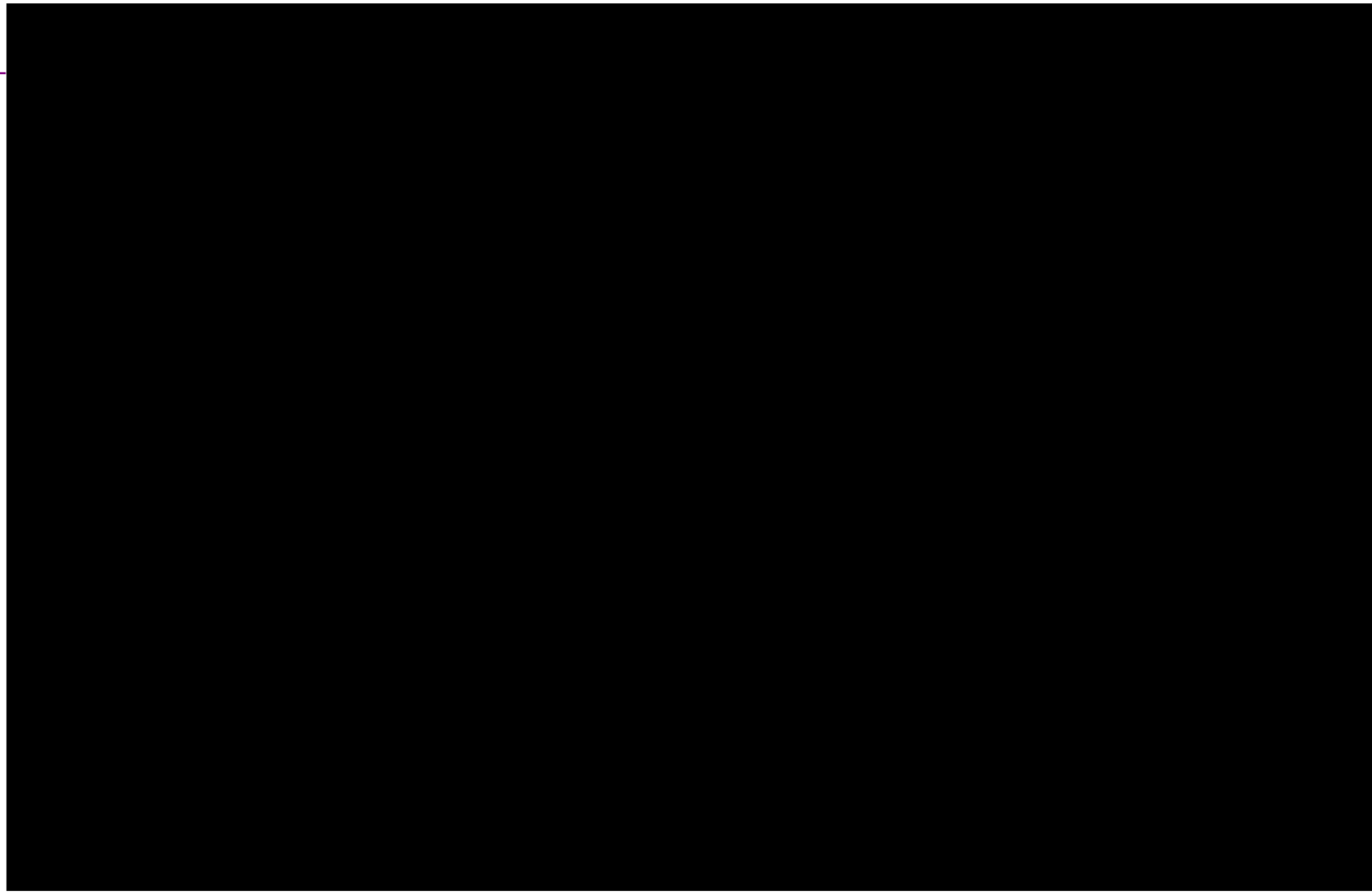
DPH Confidential

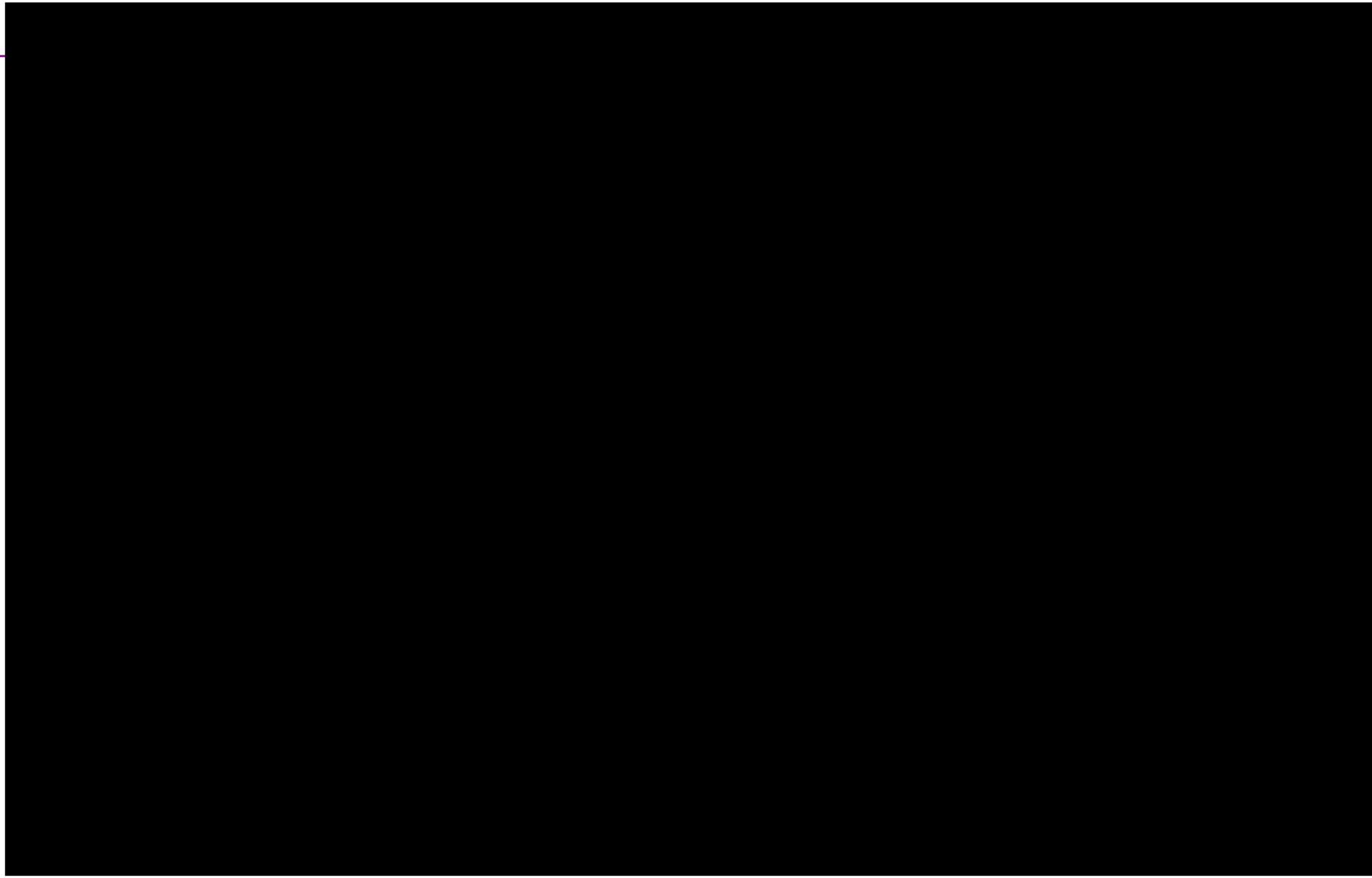


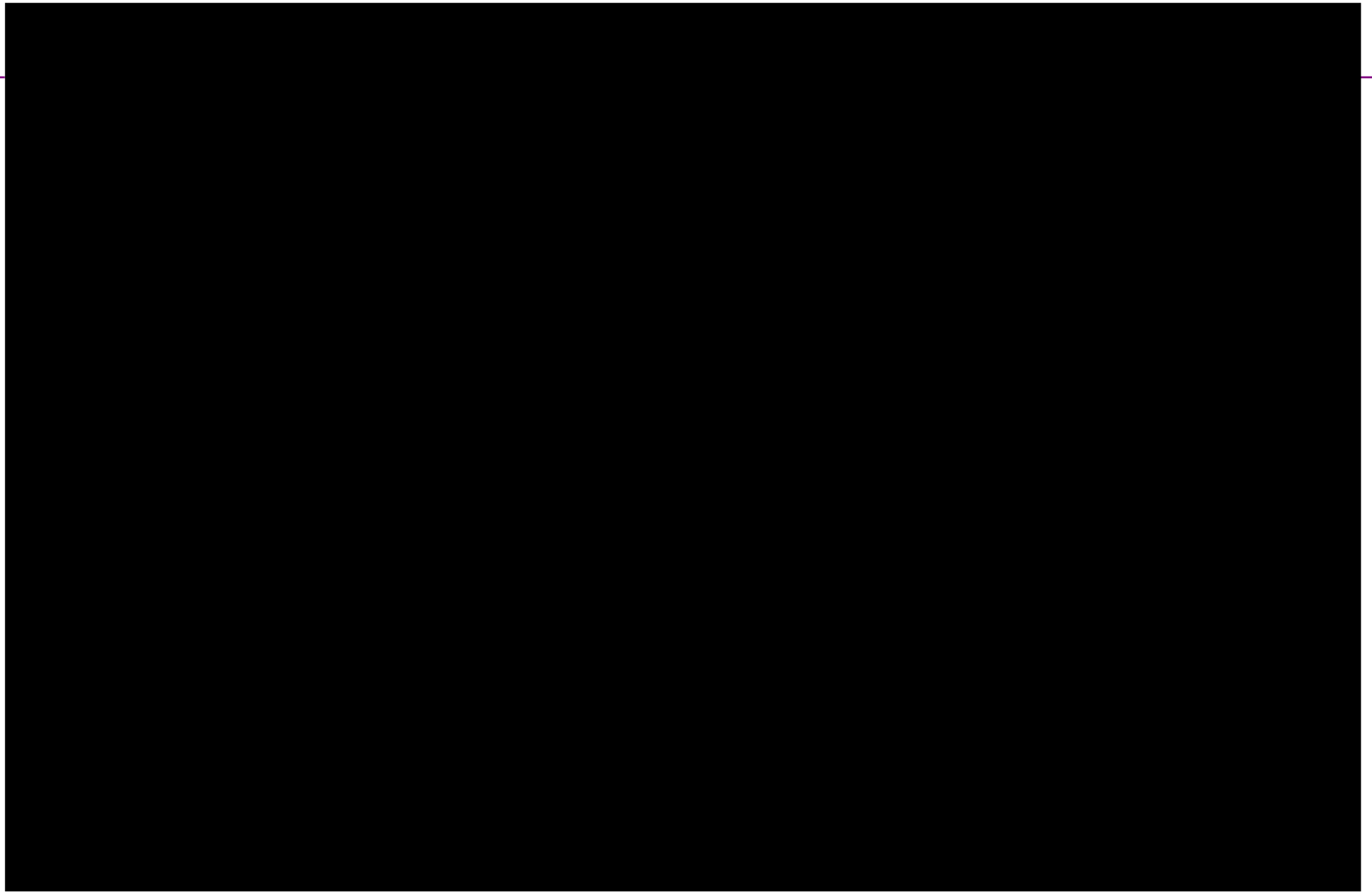


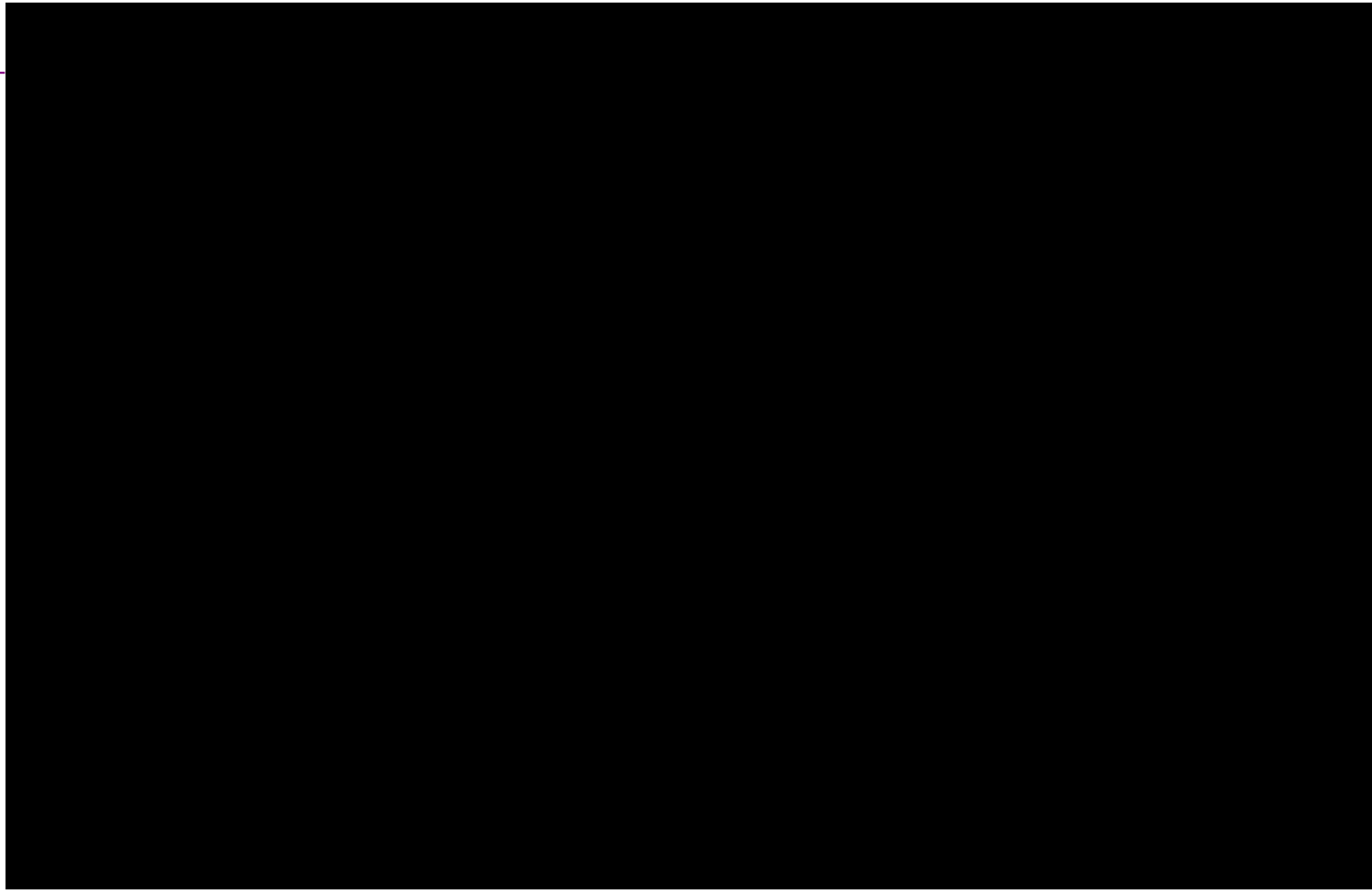


DPH Confidential

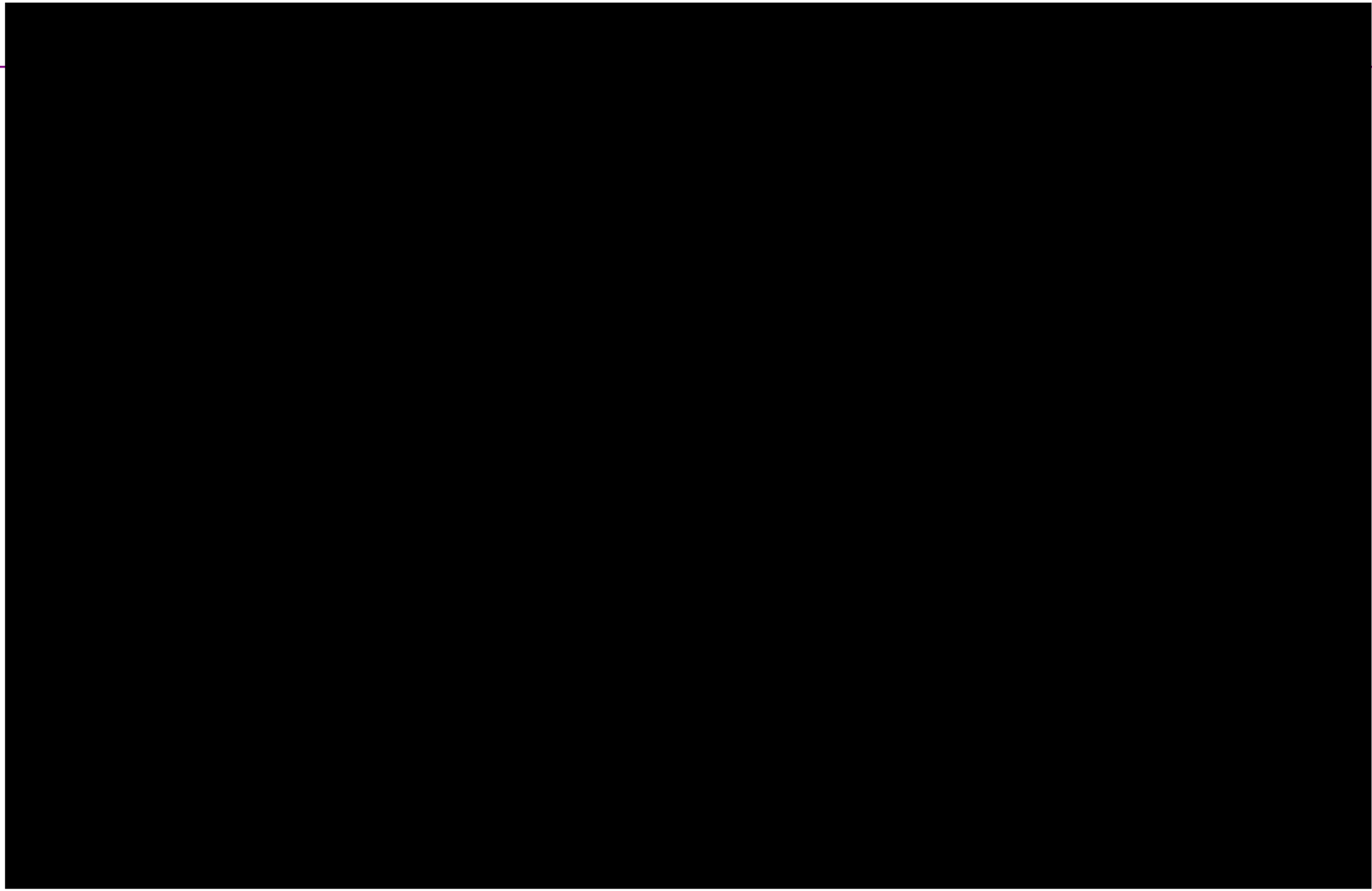


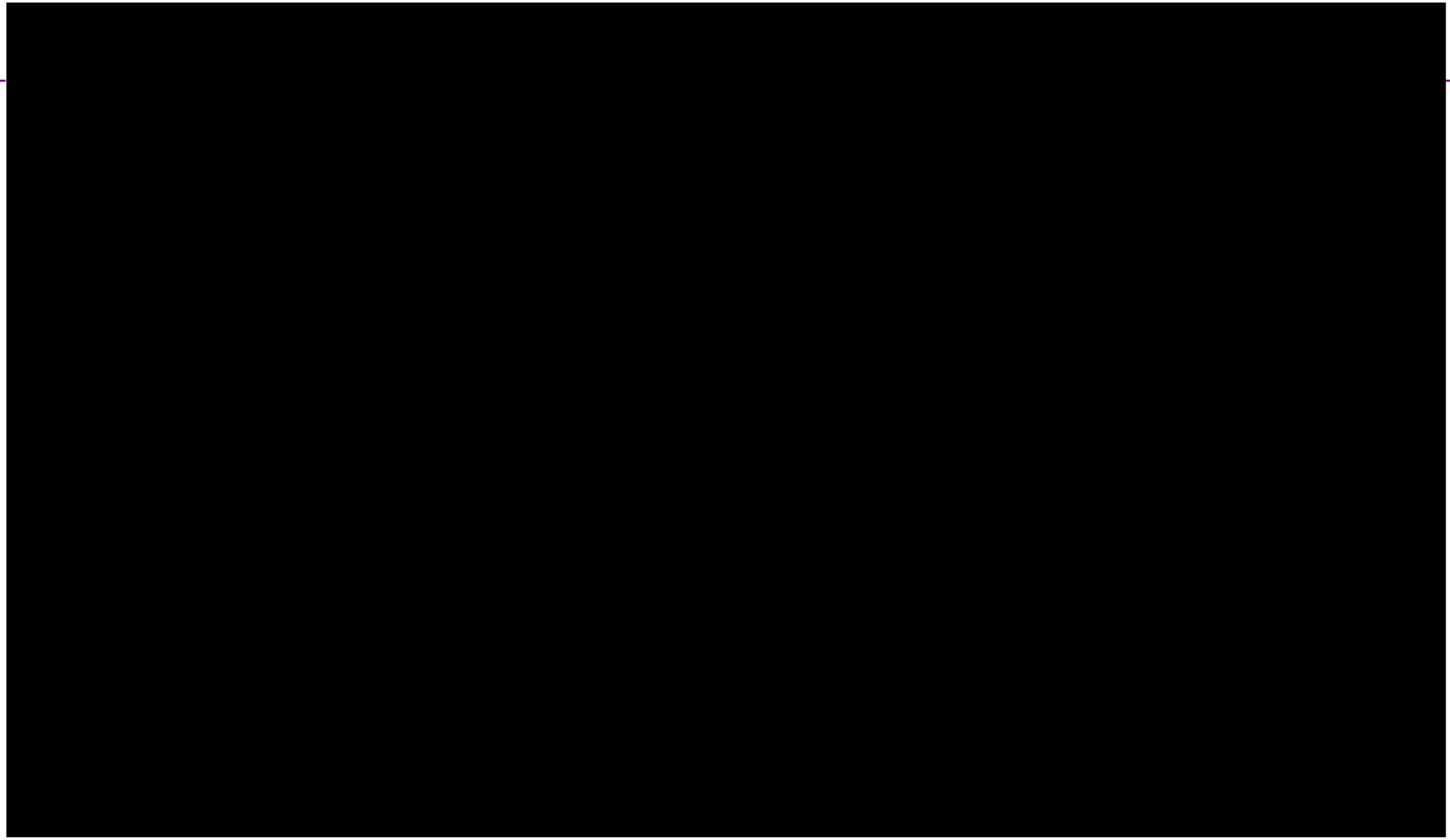


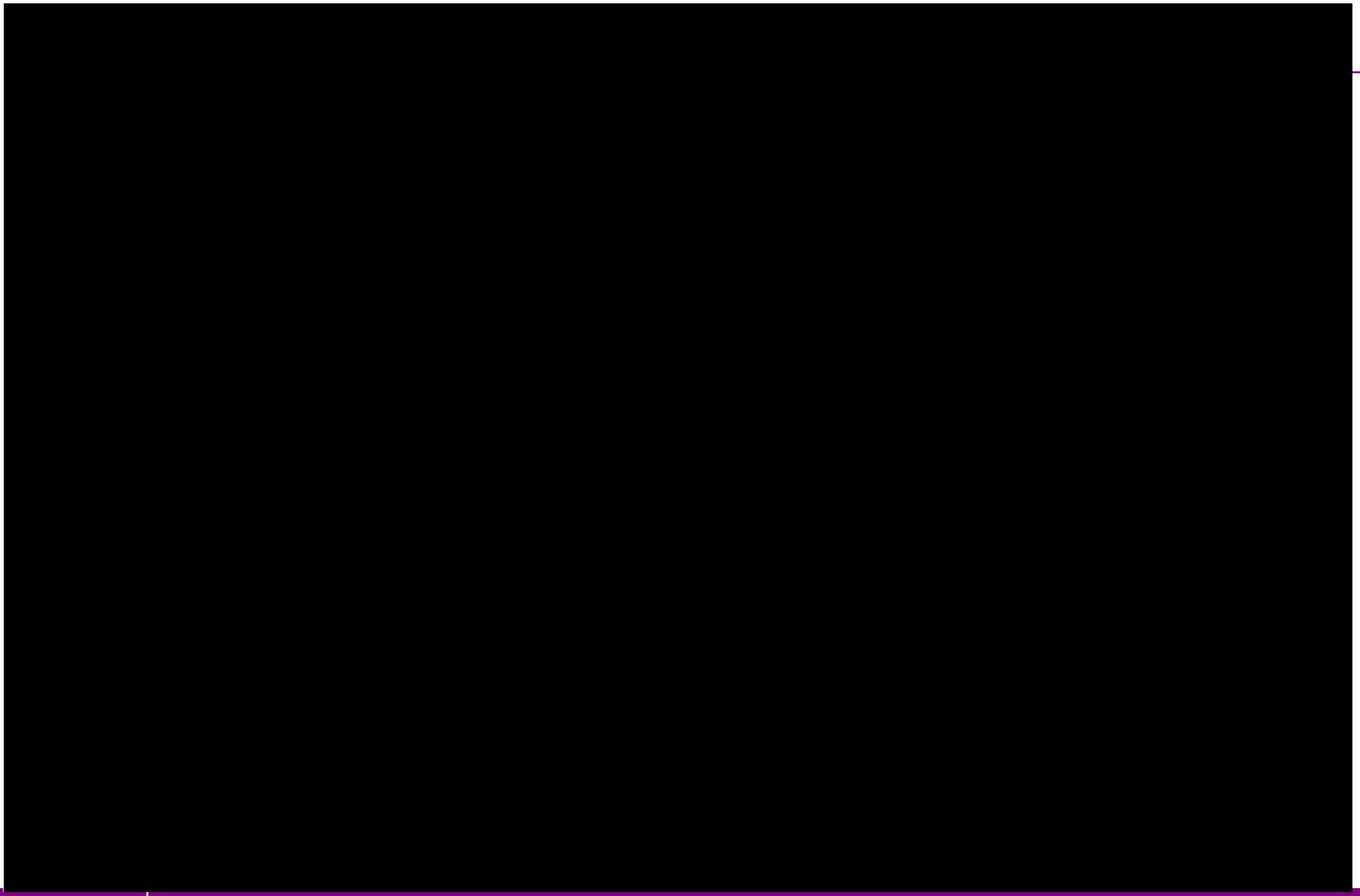


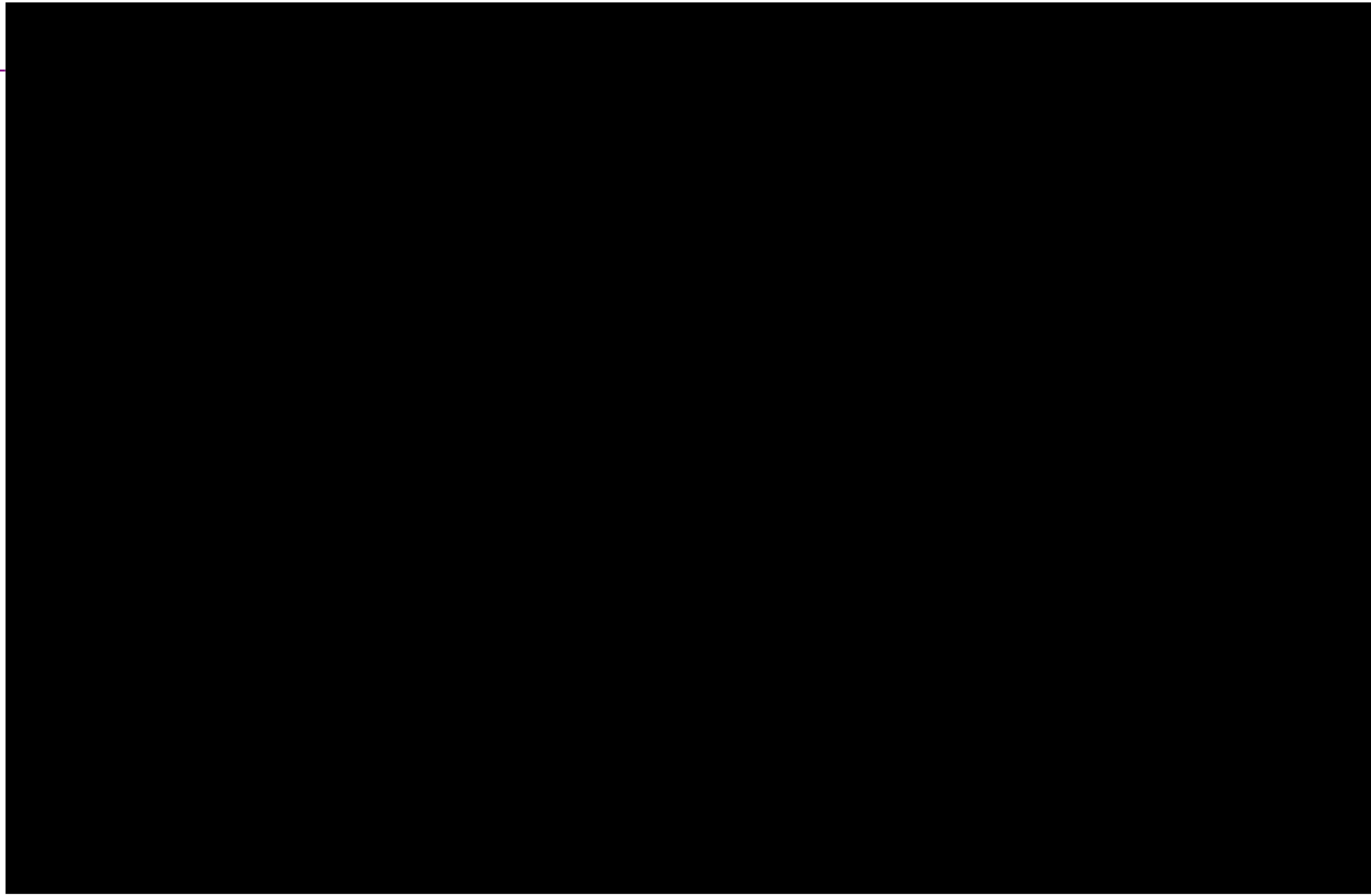


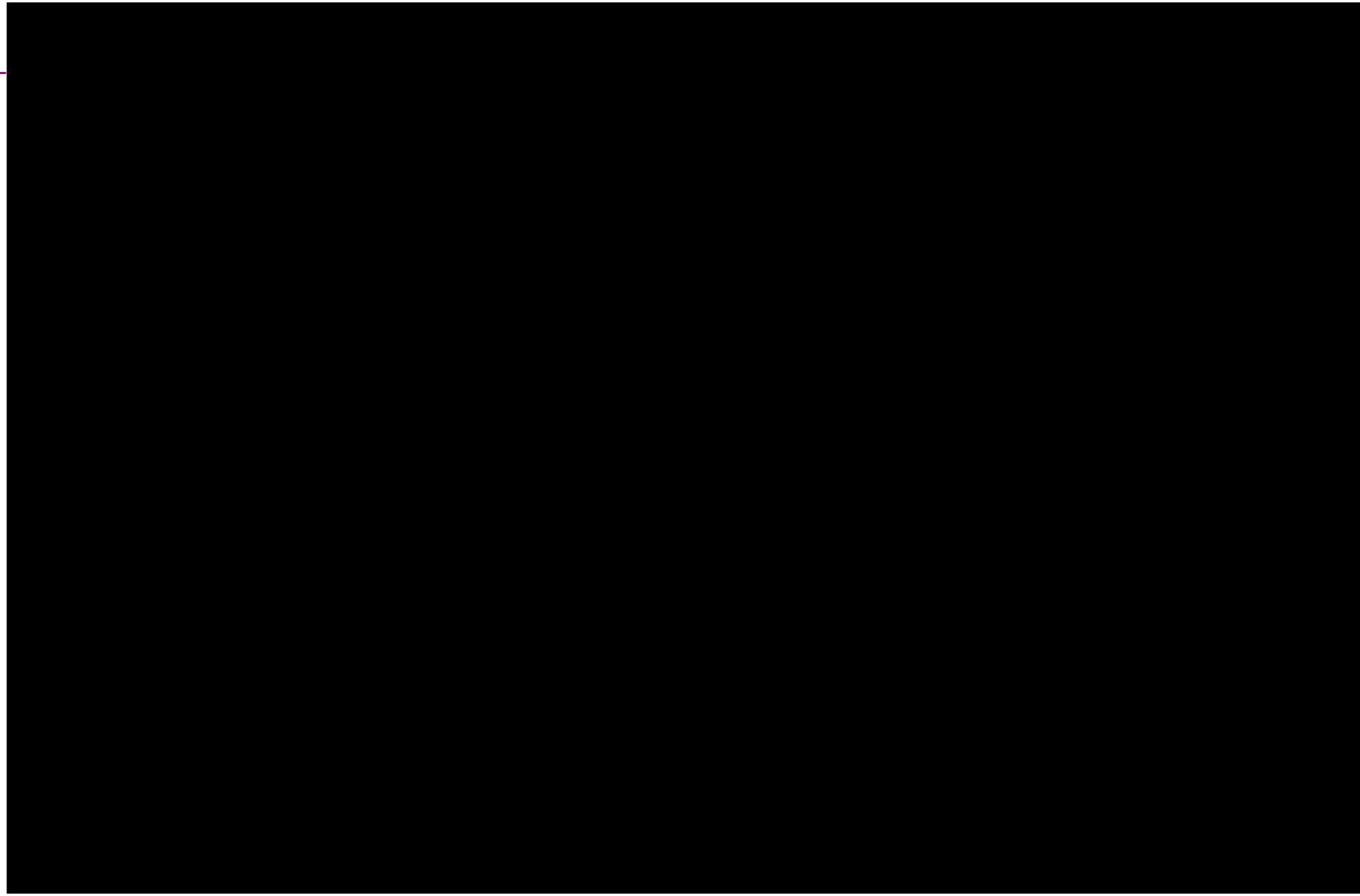
DPH Confidential

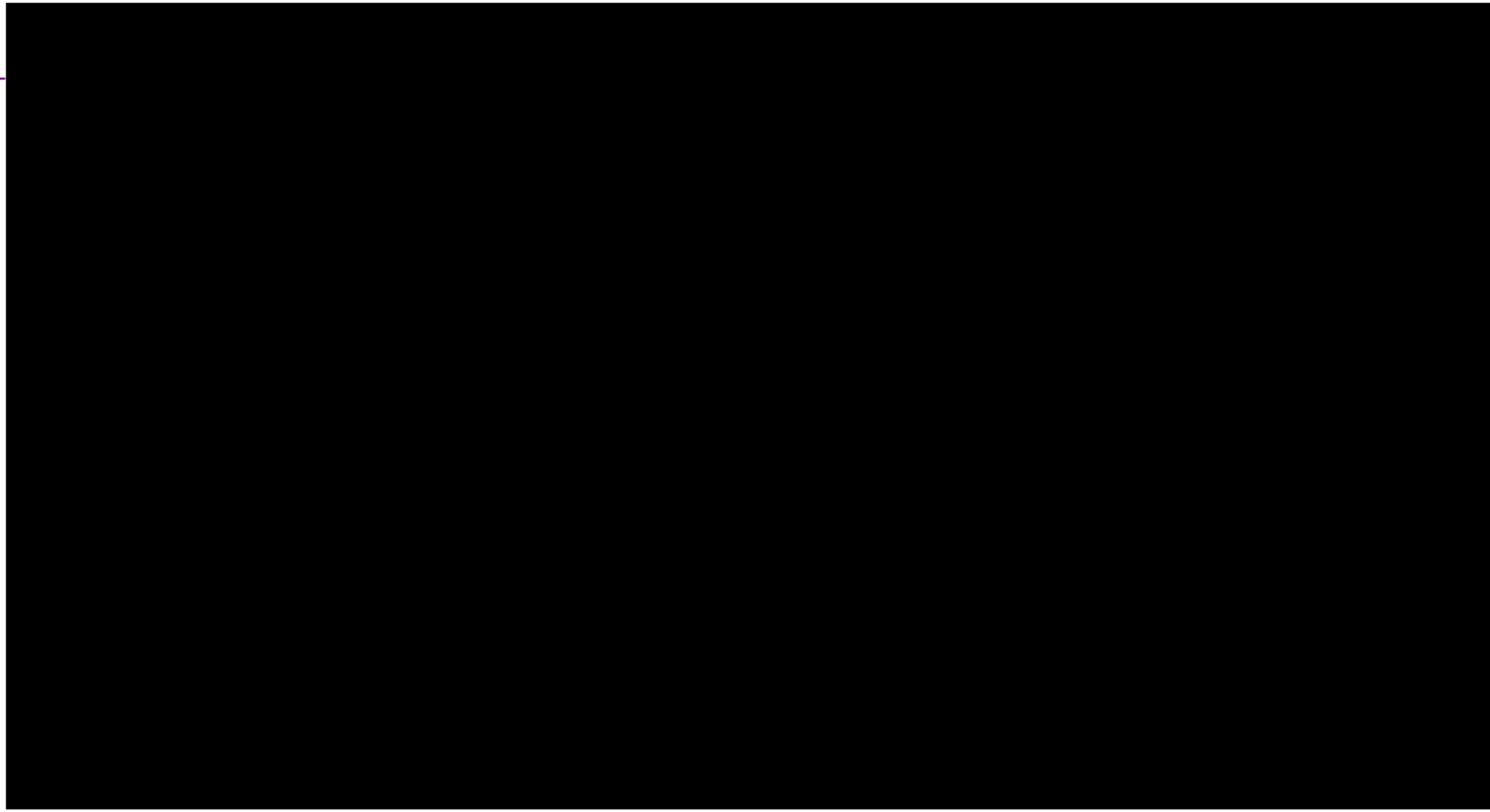












This page intentionally left blank.

Attachment F-2 – Managed Services IES and Unisys – Measurement Report

This attachment provides an example of the aggregated program view of a managed services measurement report.

This page intentionally left blank.

UNISYS

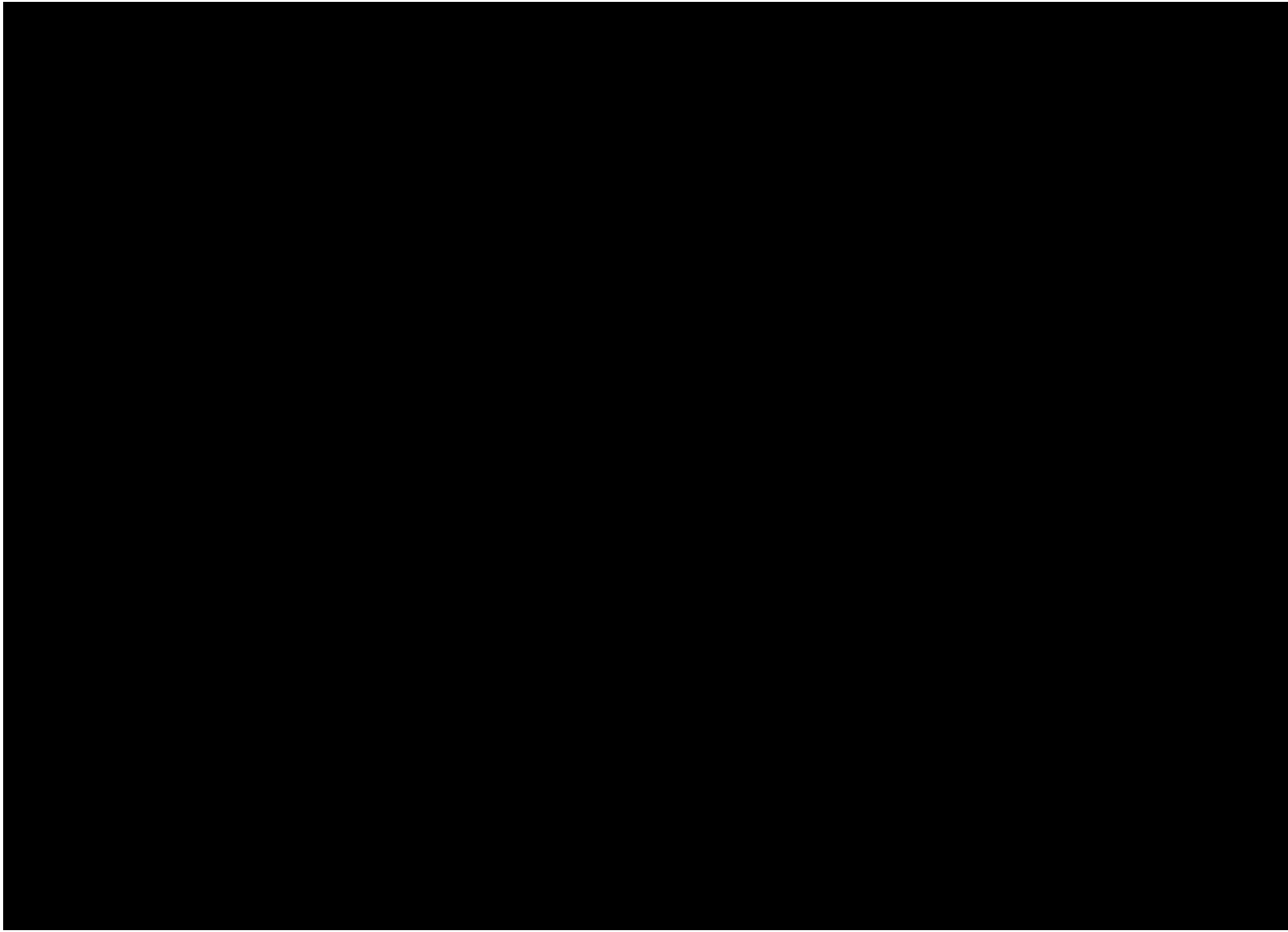
pennsylvania
OFFICE OF ADMINISTRATION

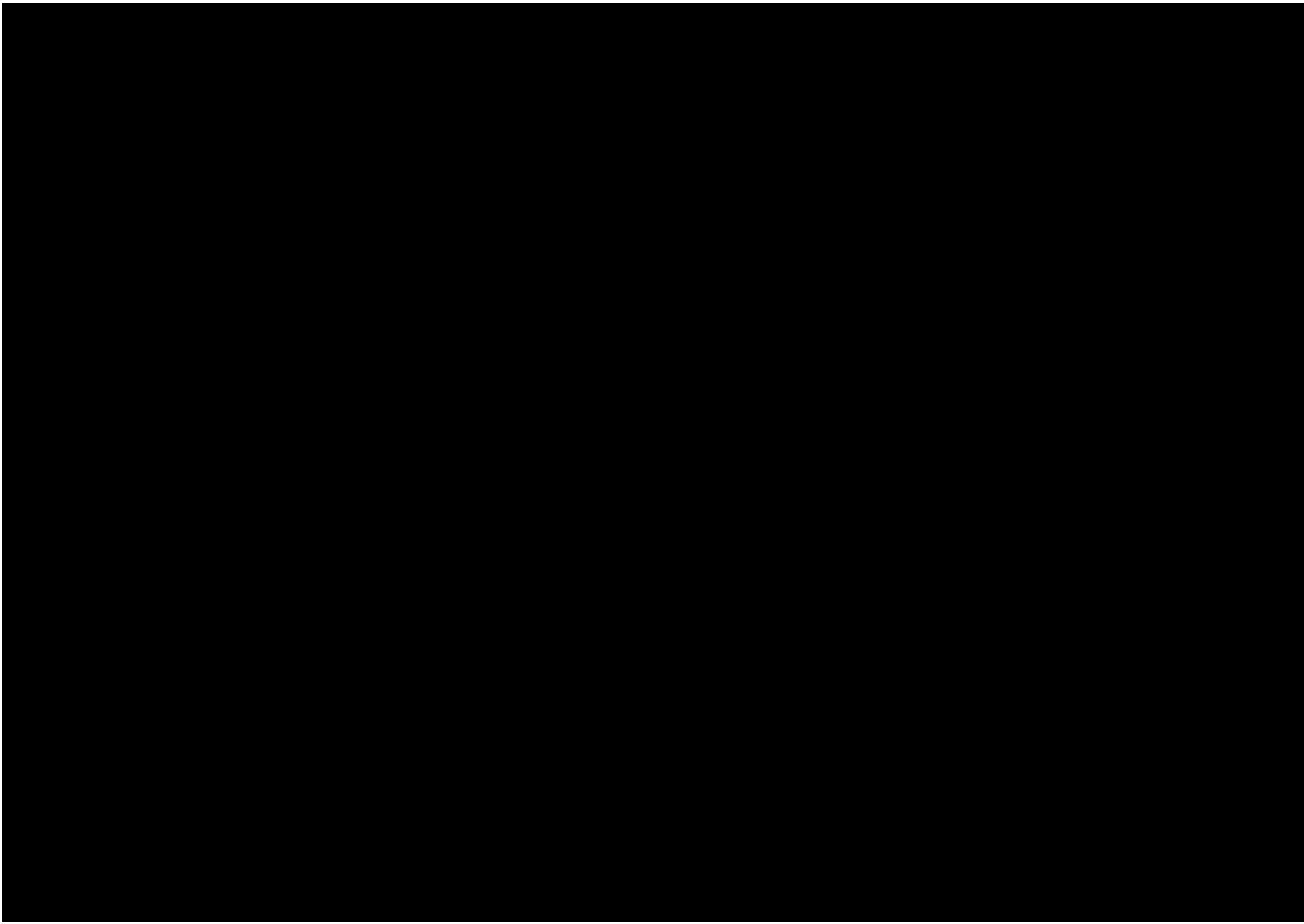
Managed Services IES and Unisys

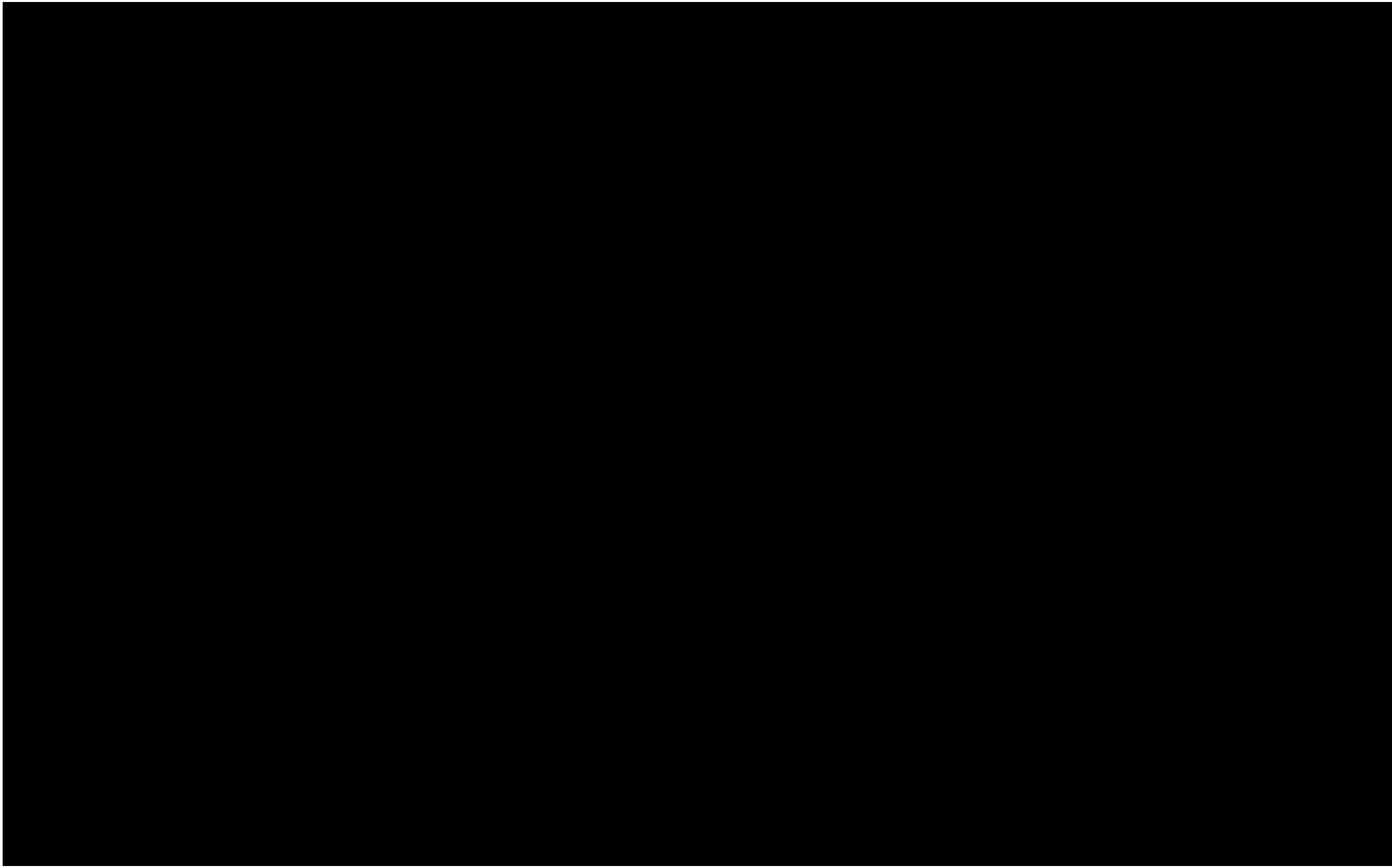
Measurement Report

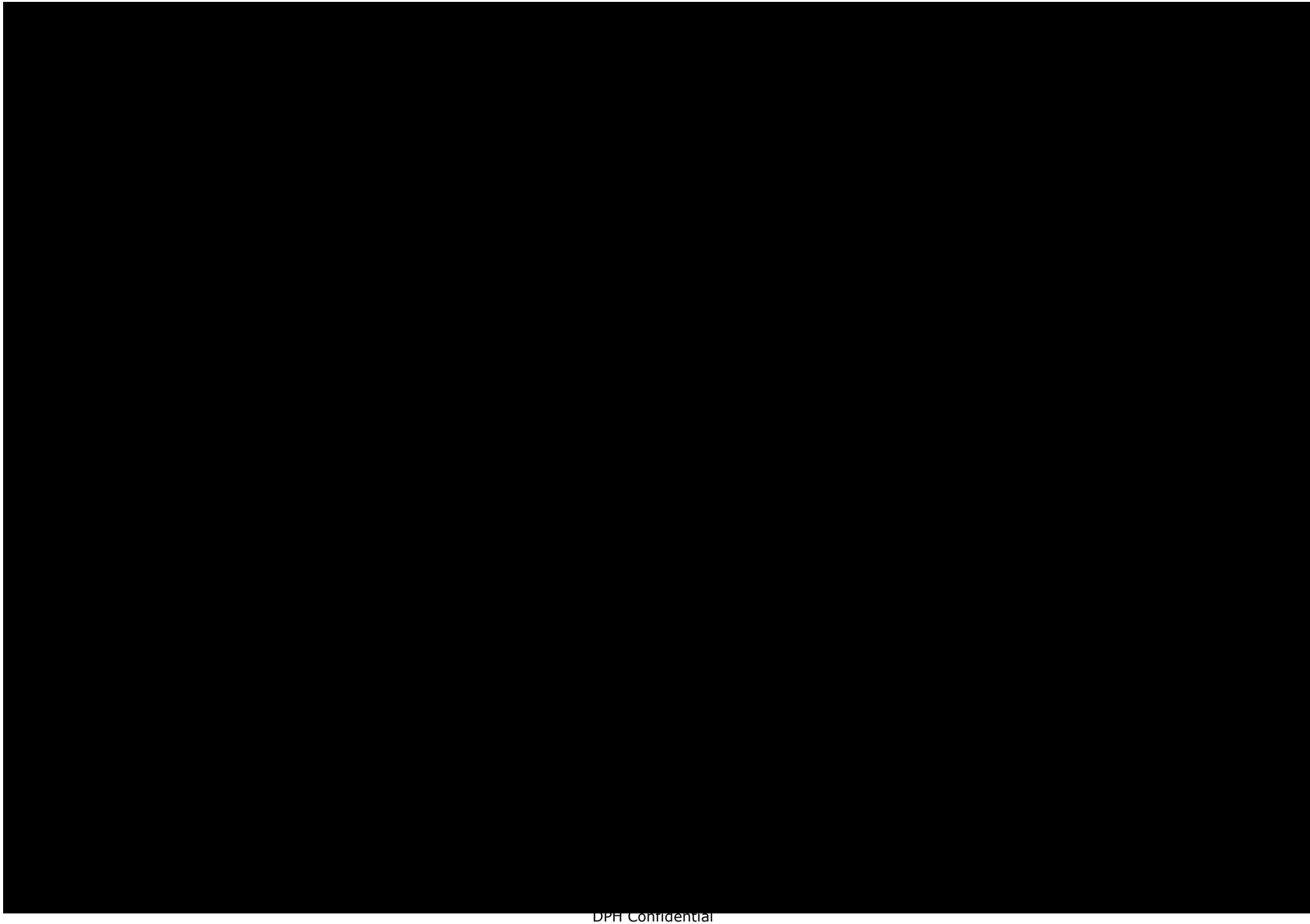
April 2013

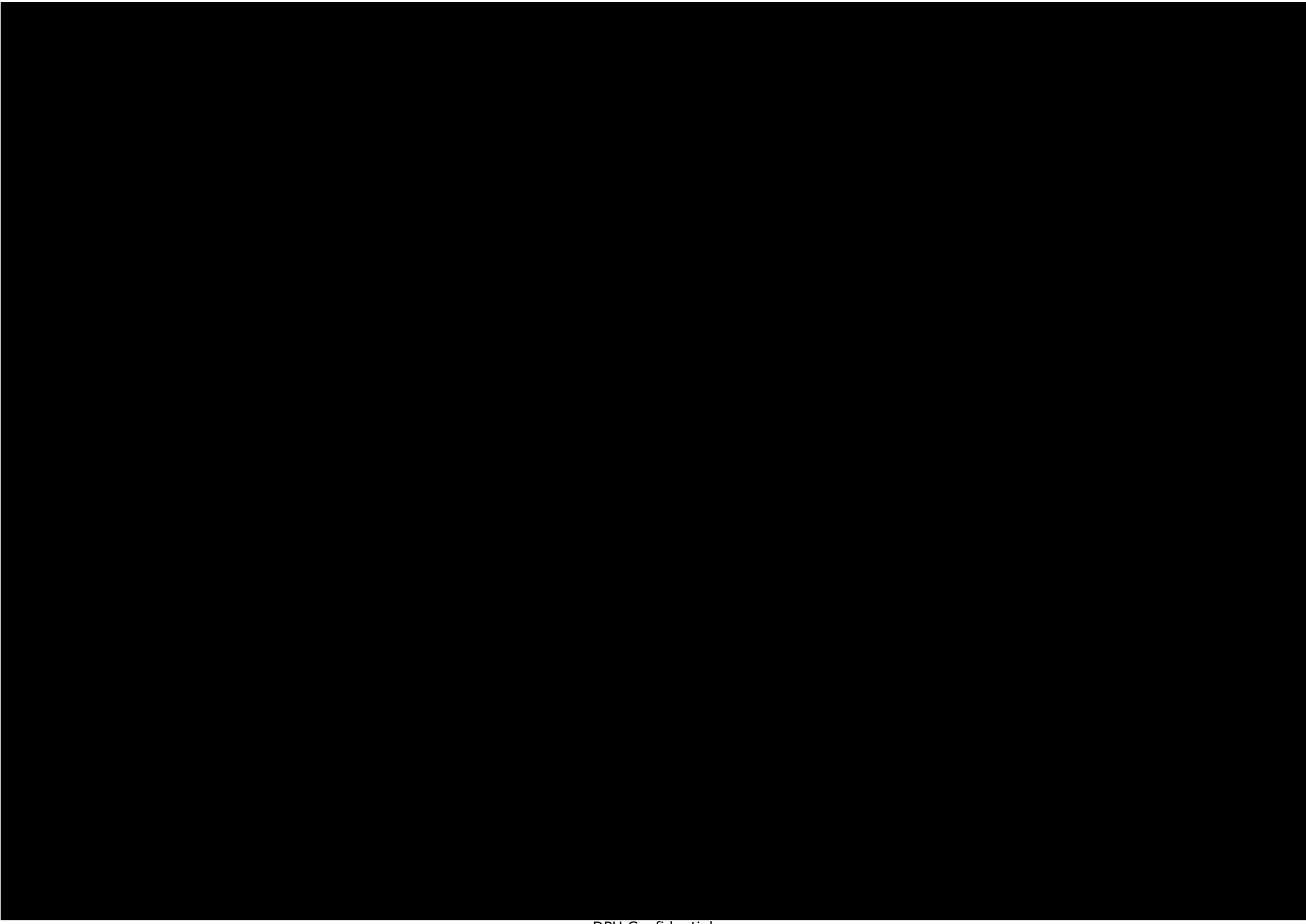
DPH Confidential
This document is for the sole purposes of managing and administering
the Data PowerHouse project for the Commonwealth of Pennsylvania

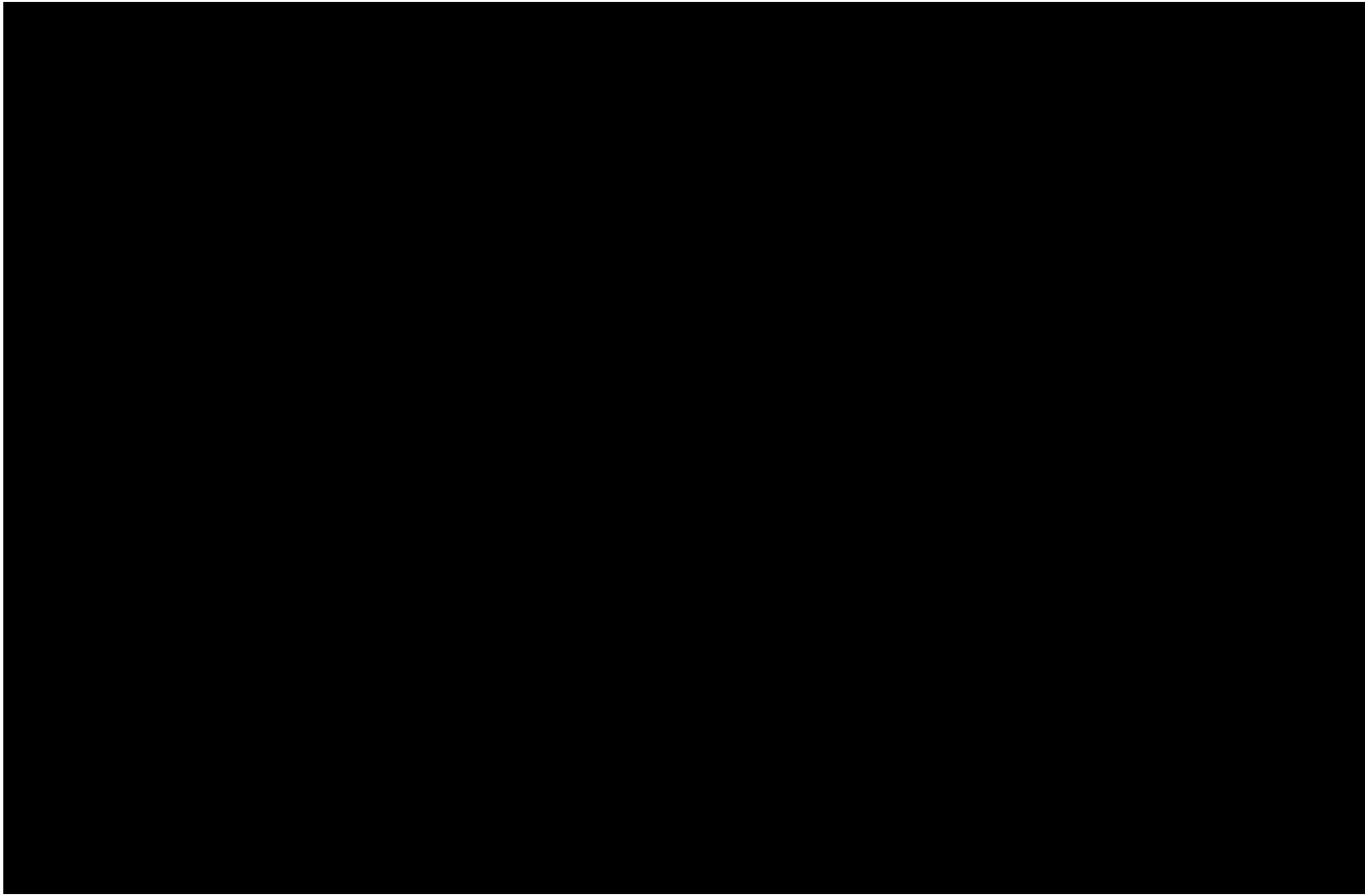


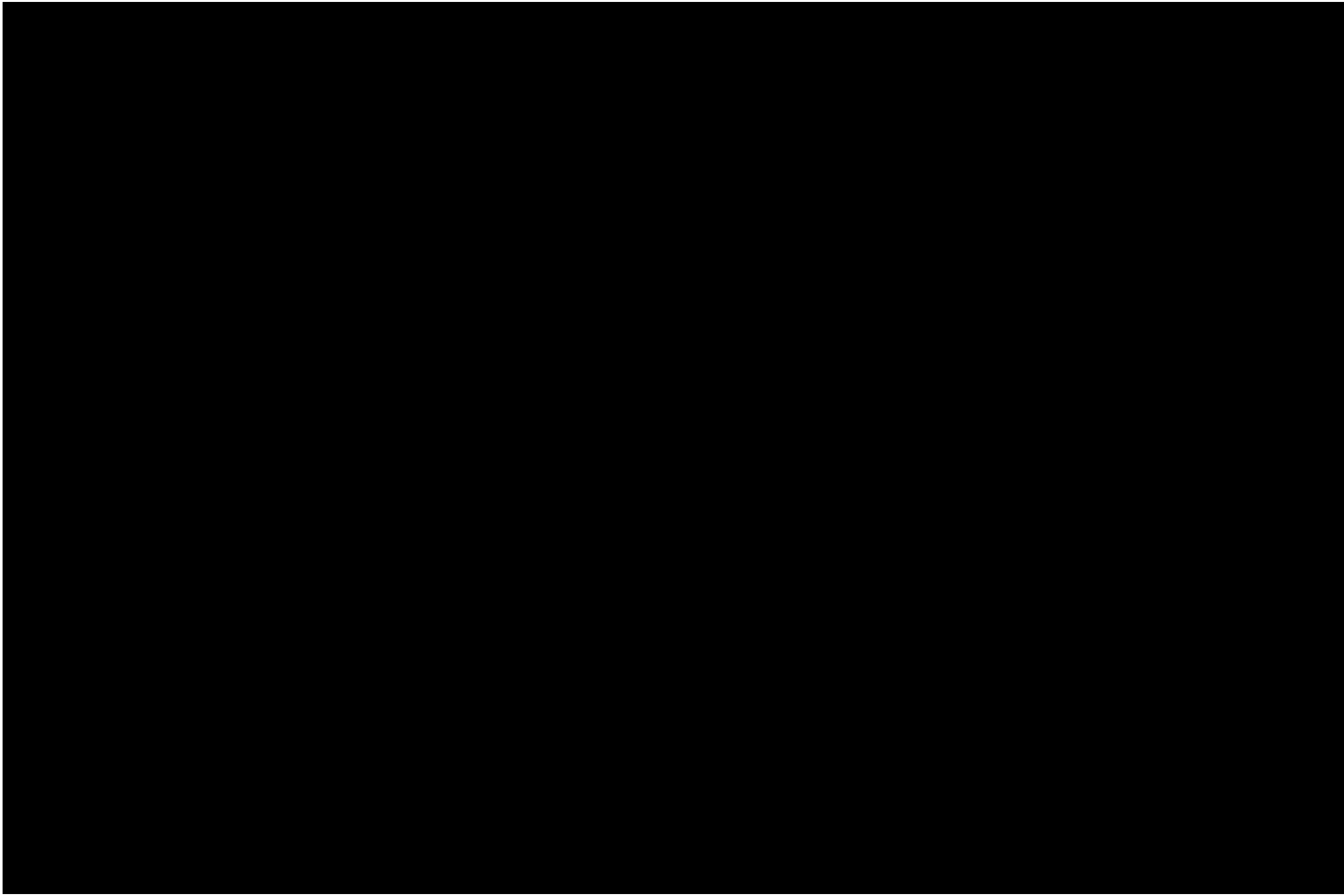


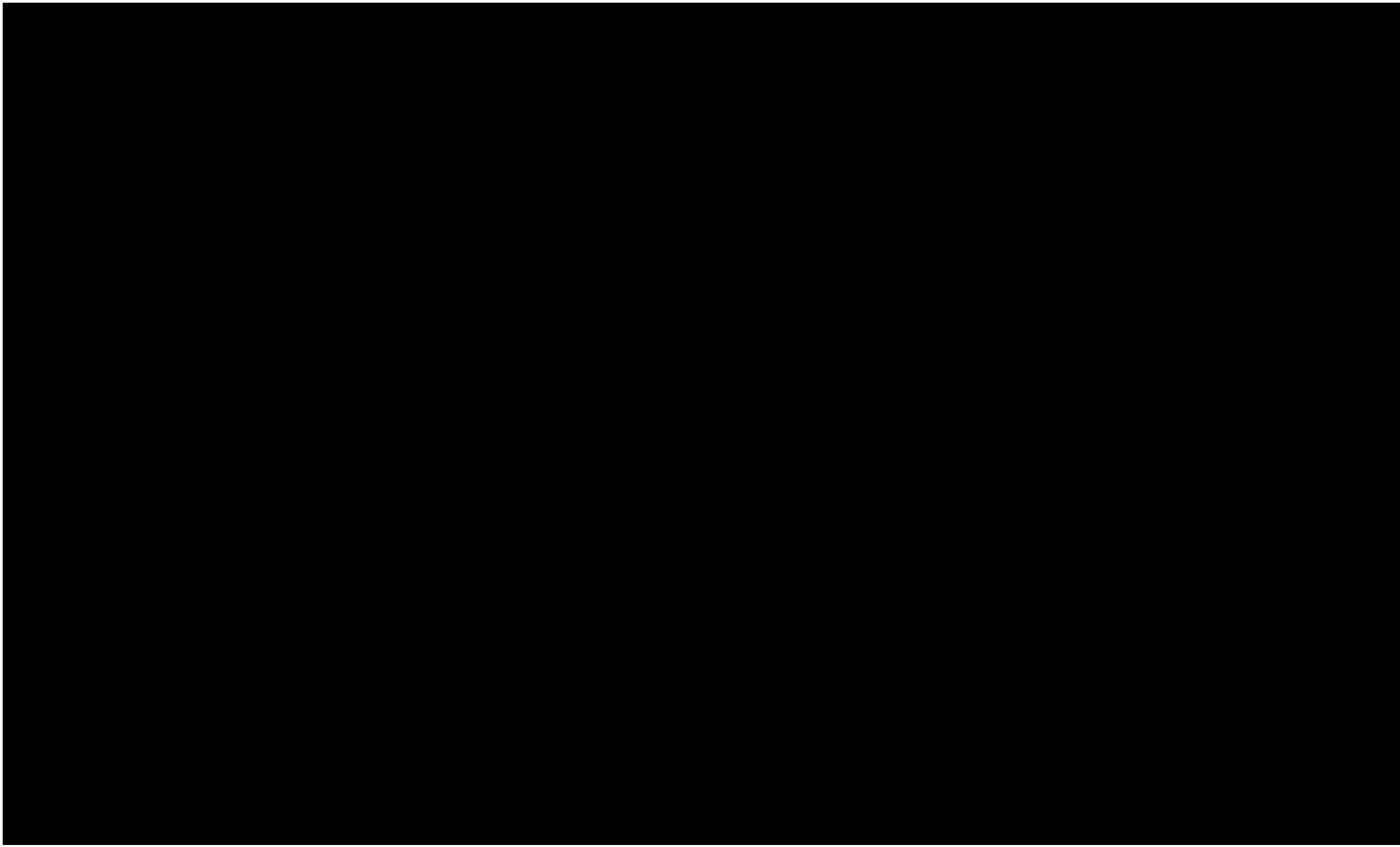


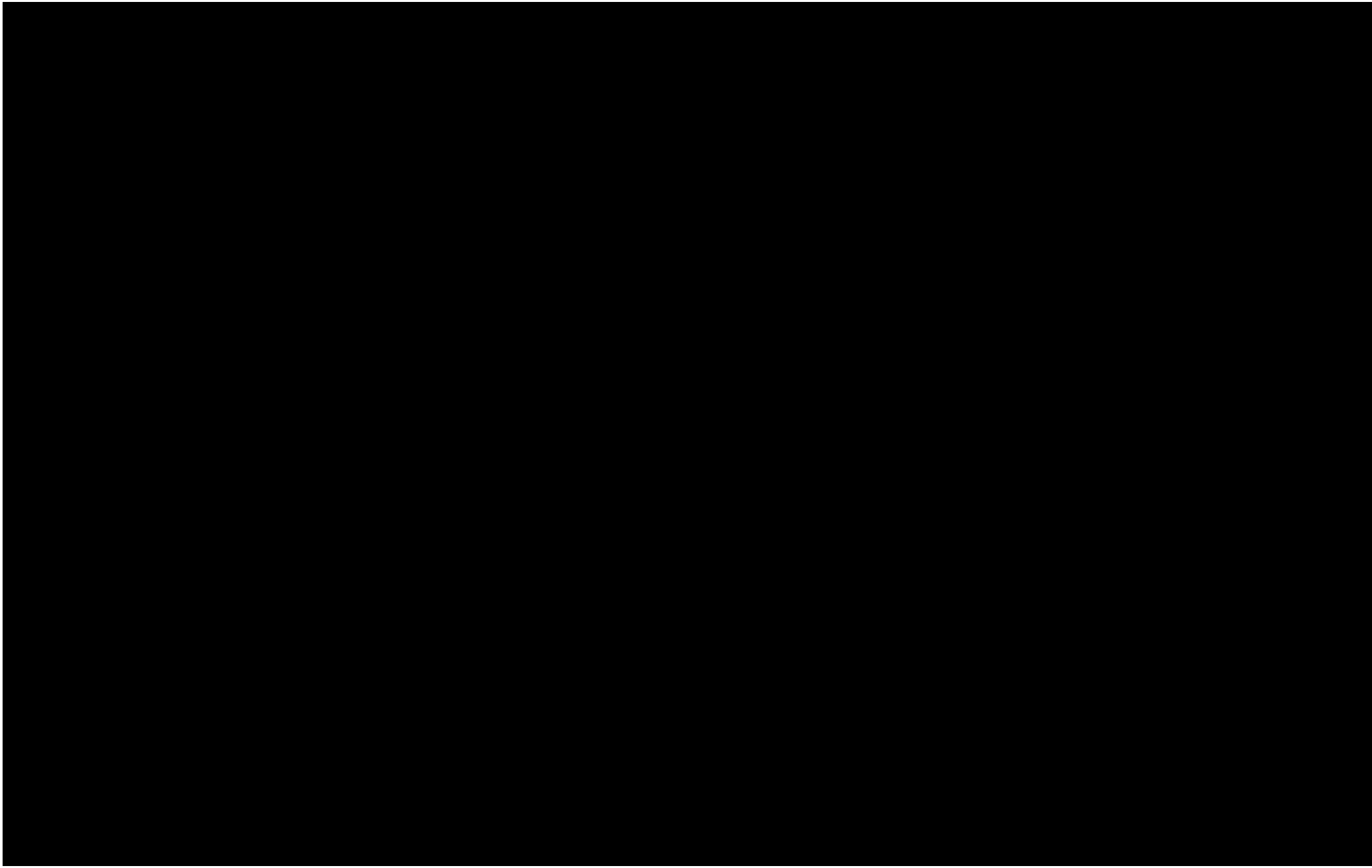


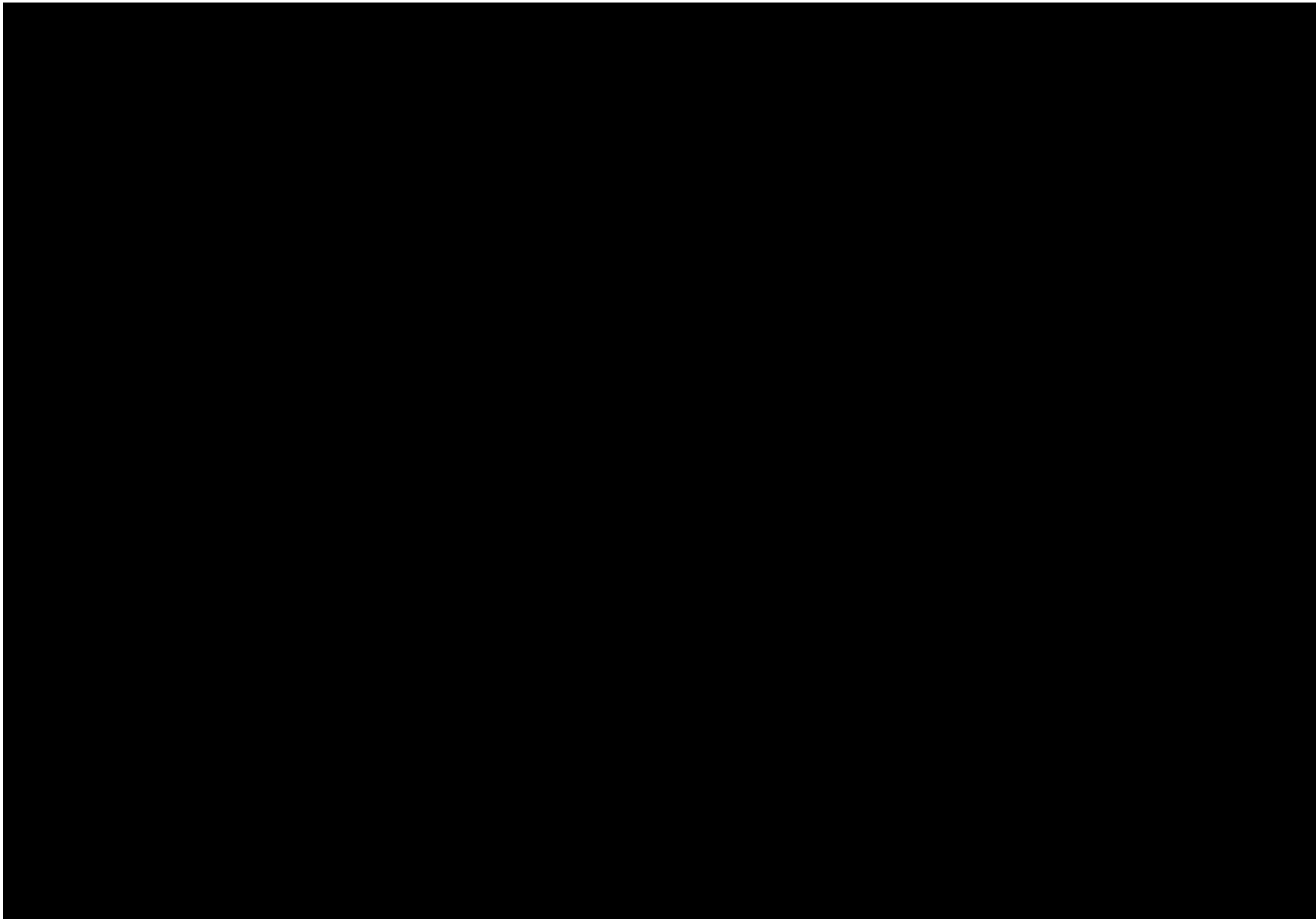


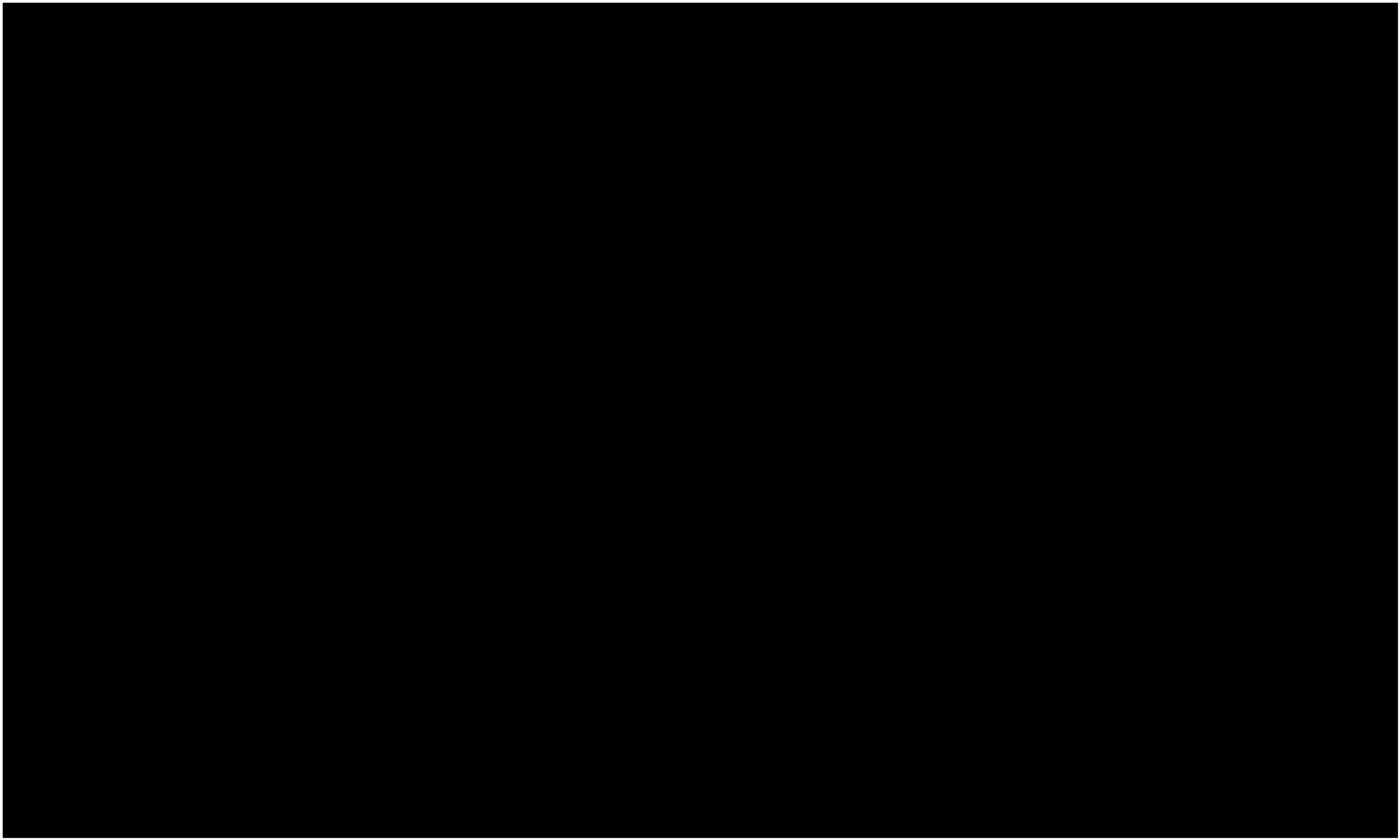


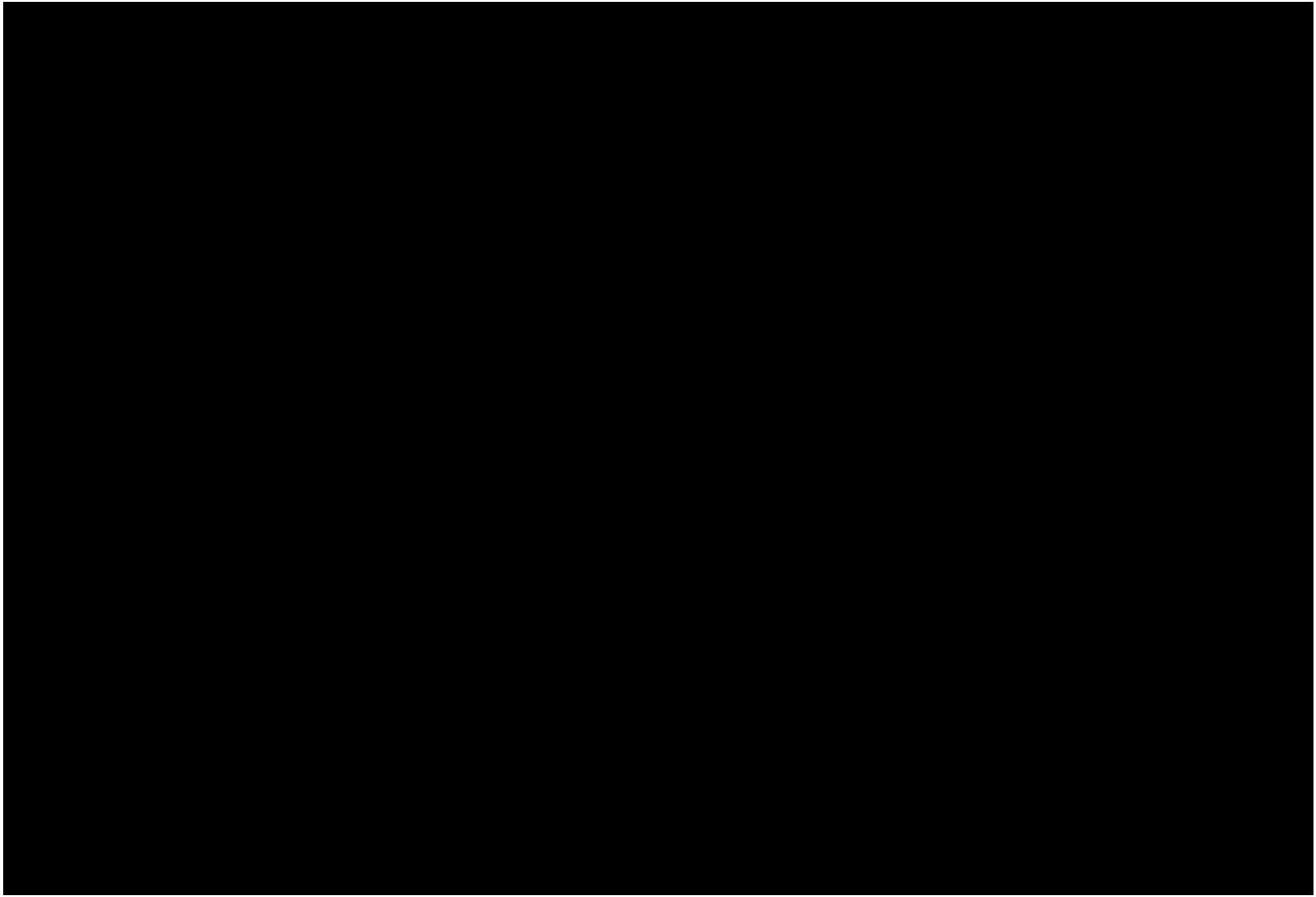


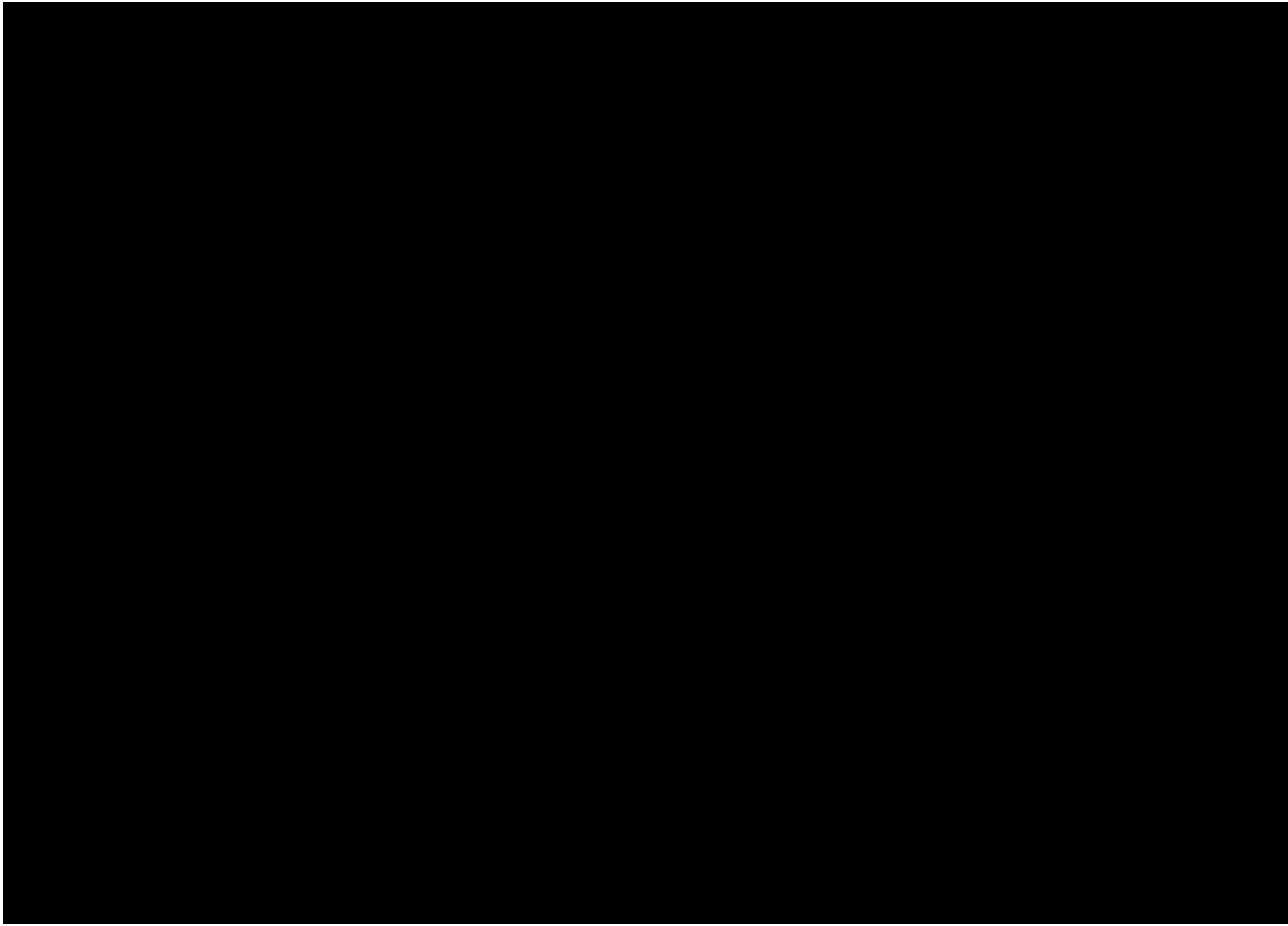


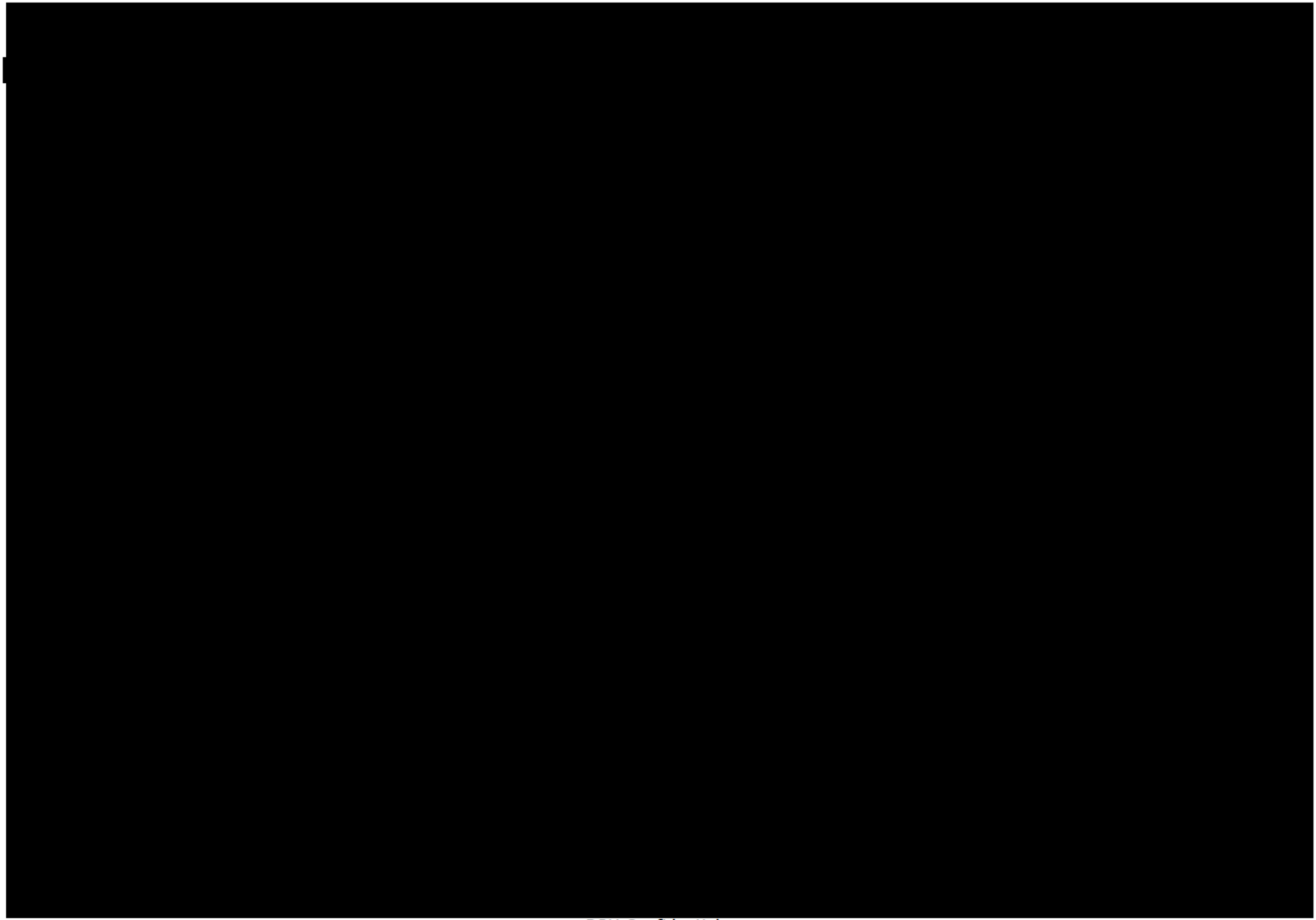


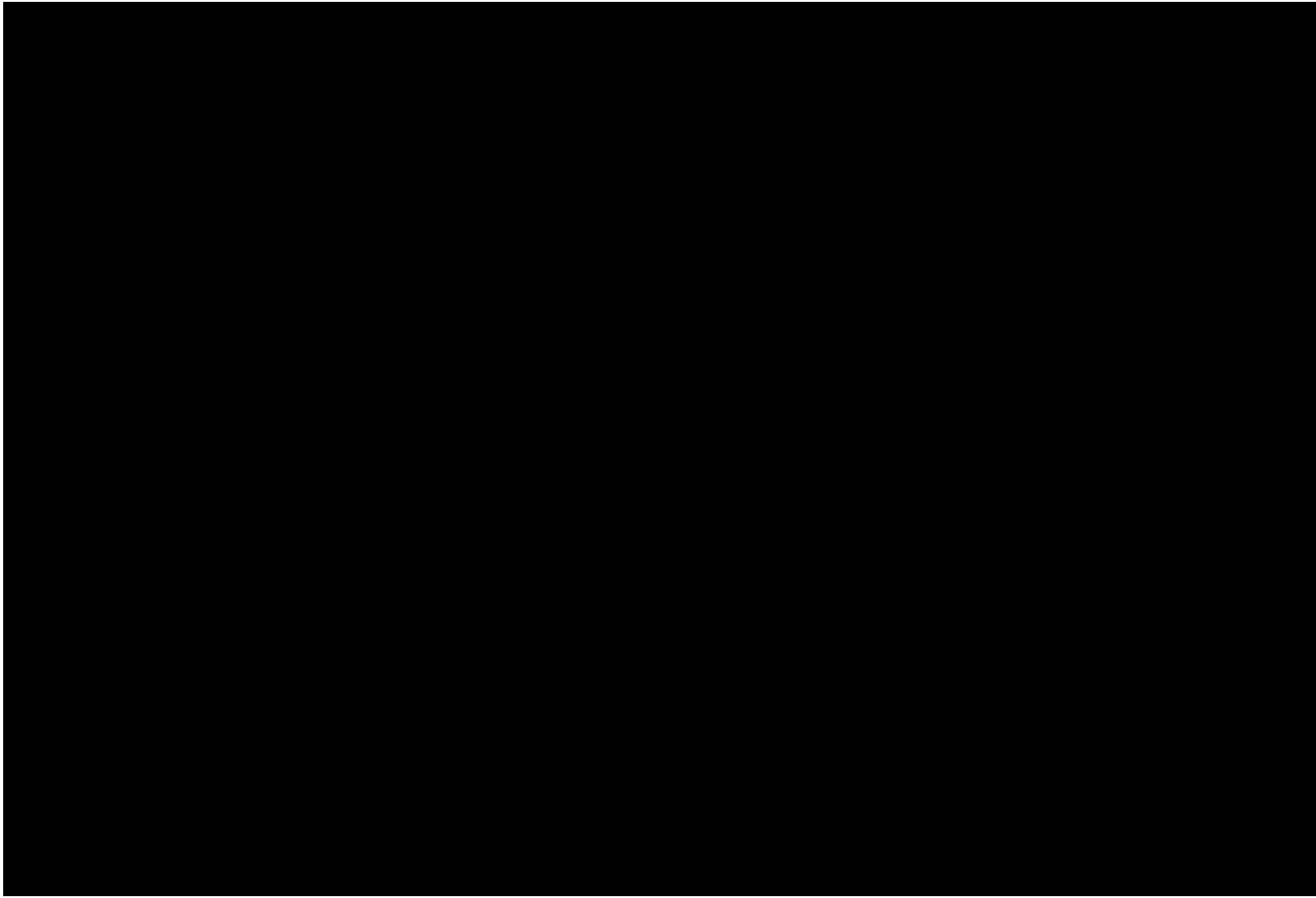


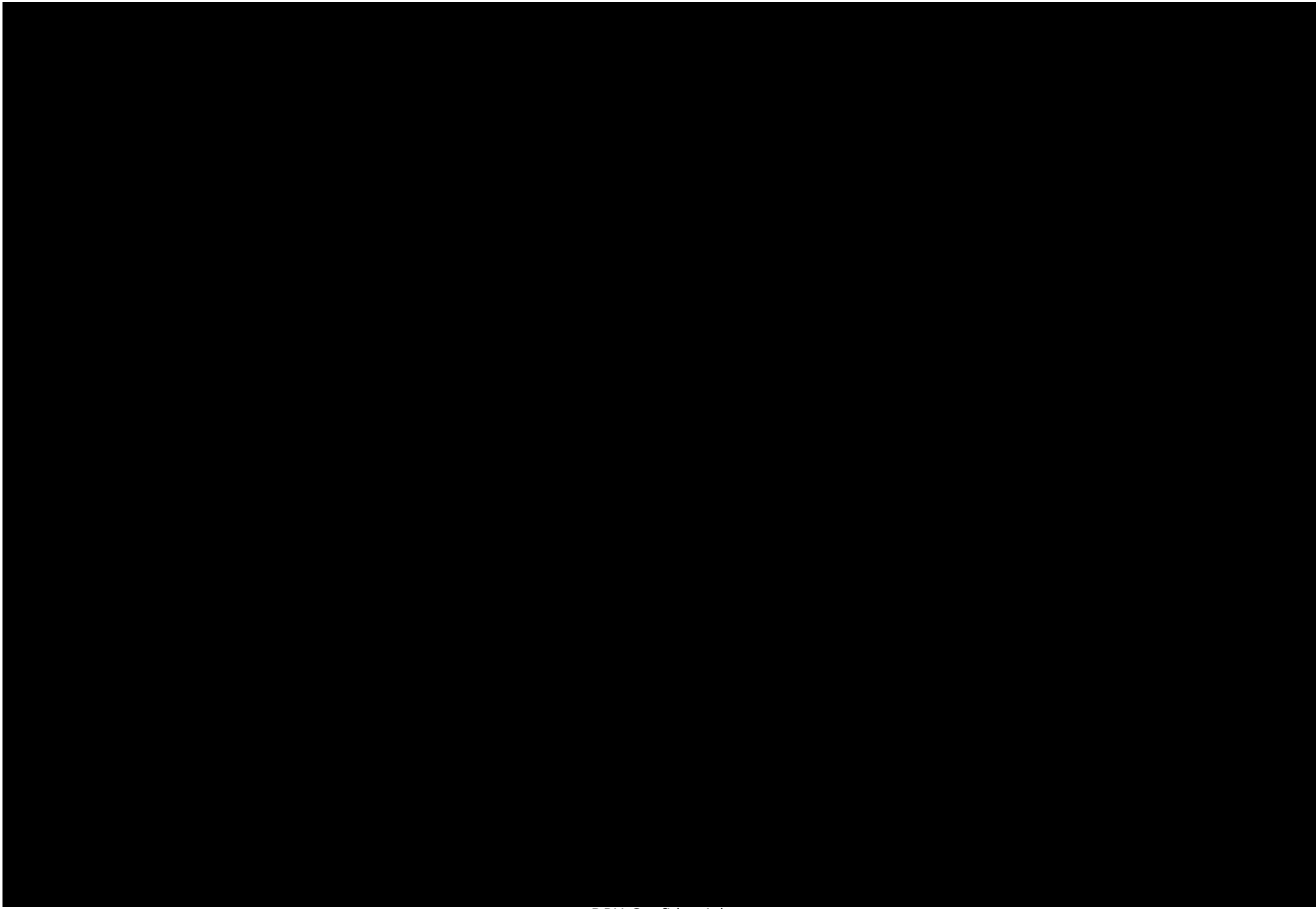


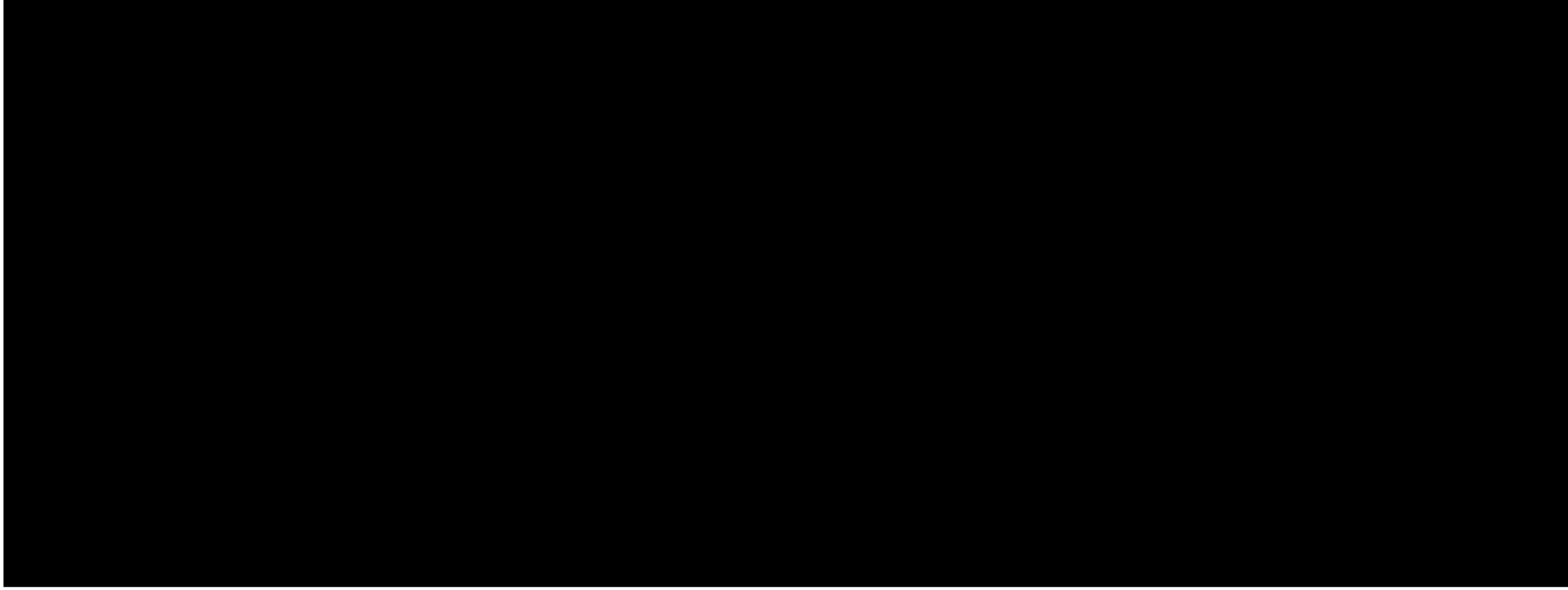


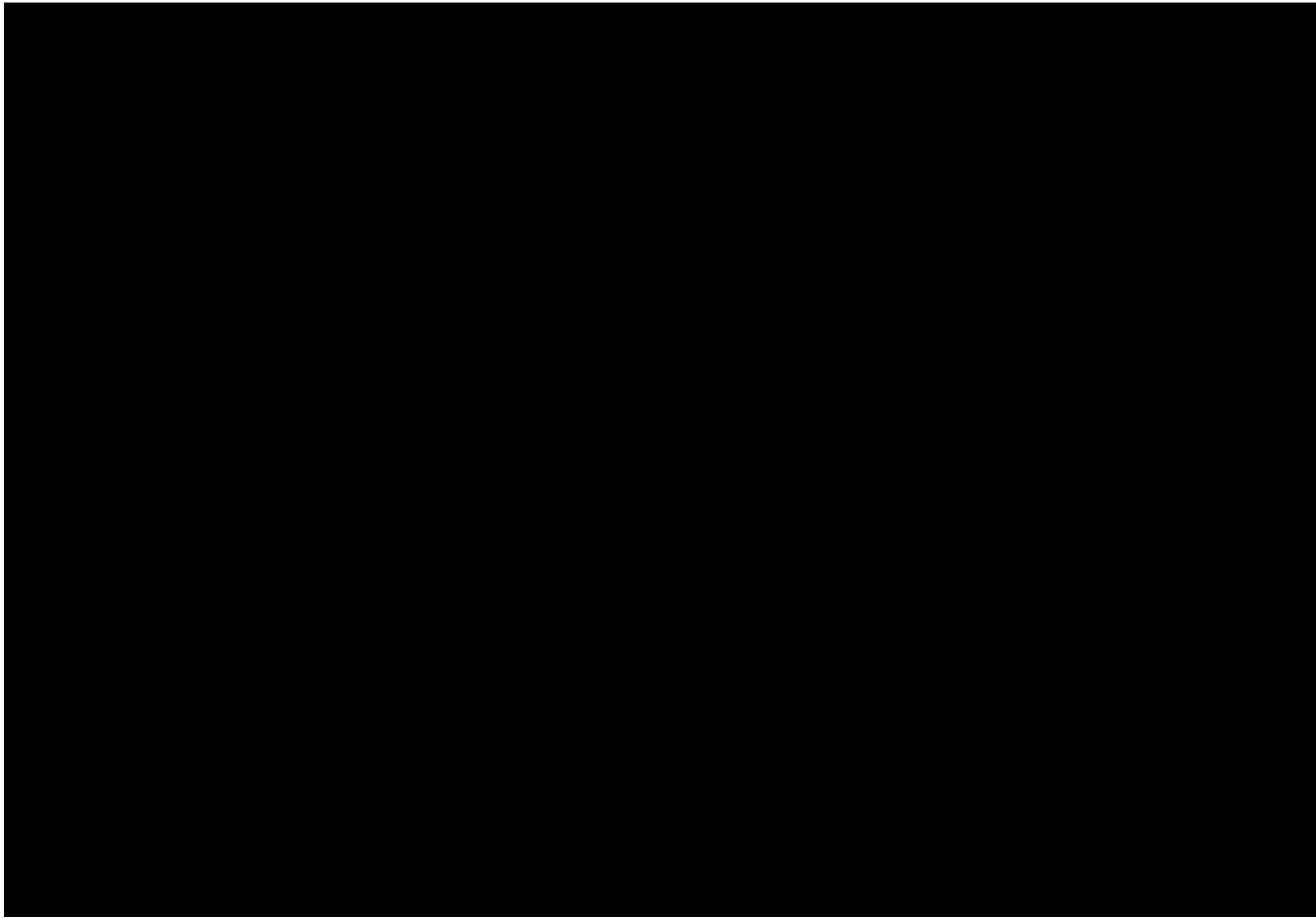


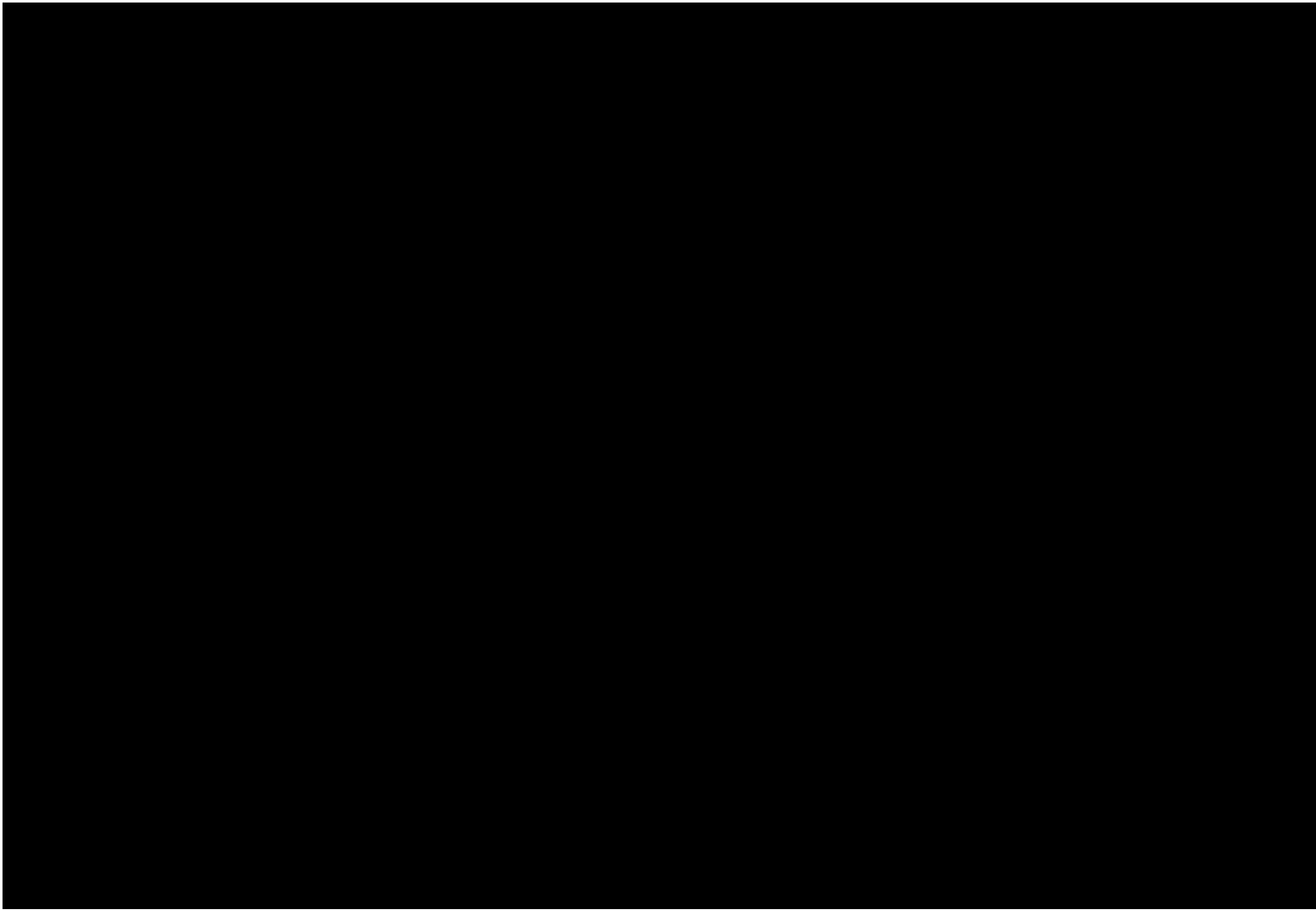


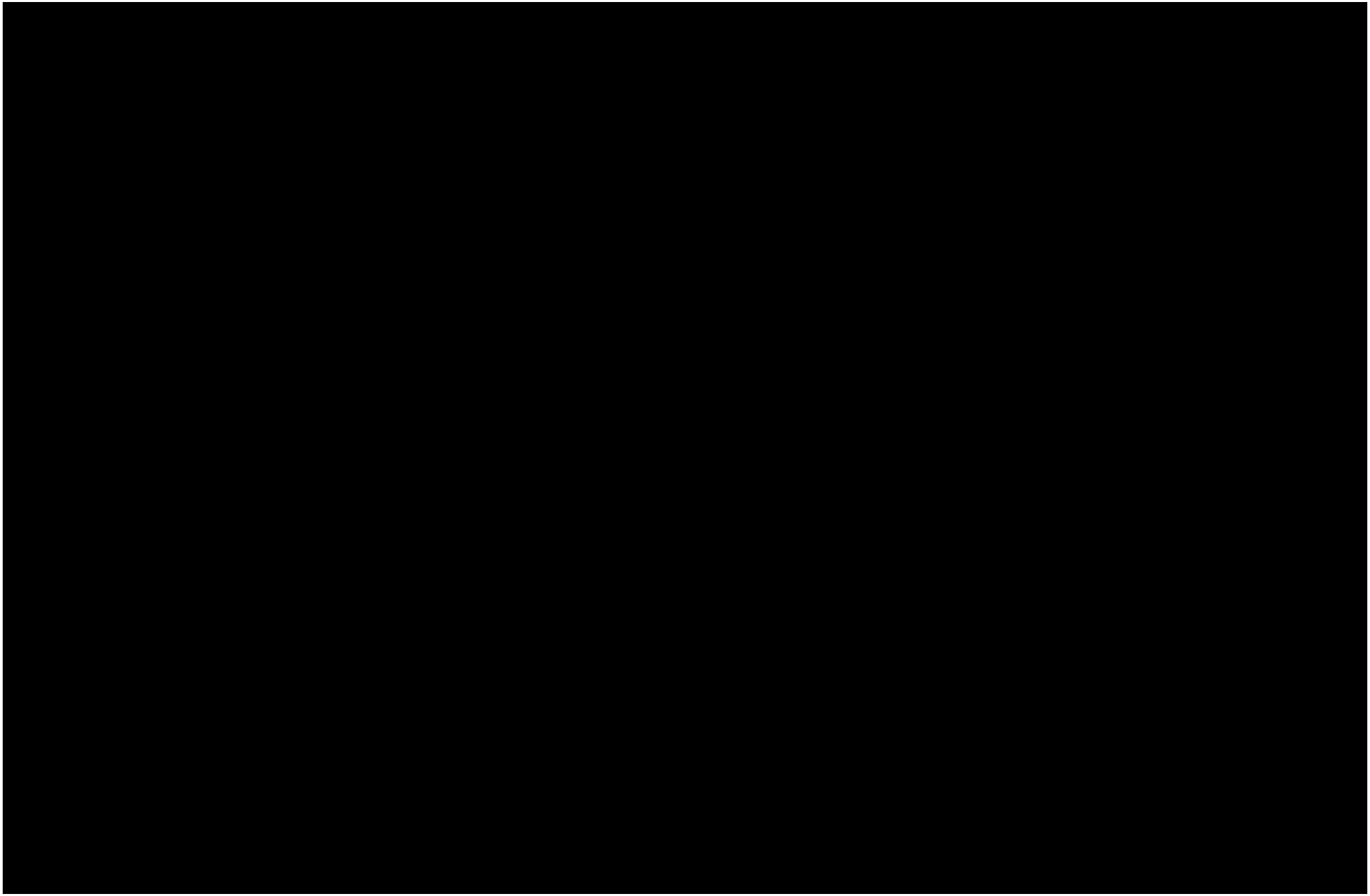


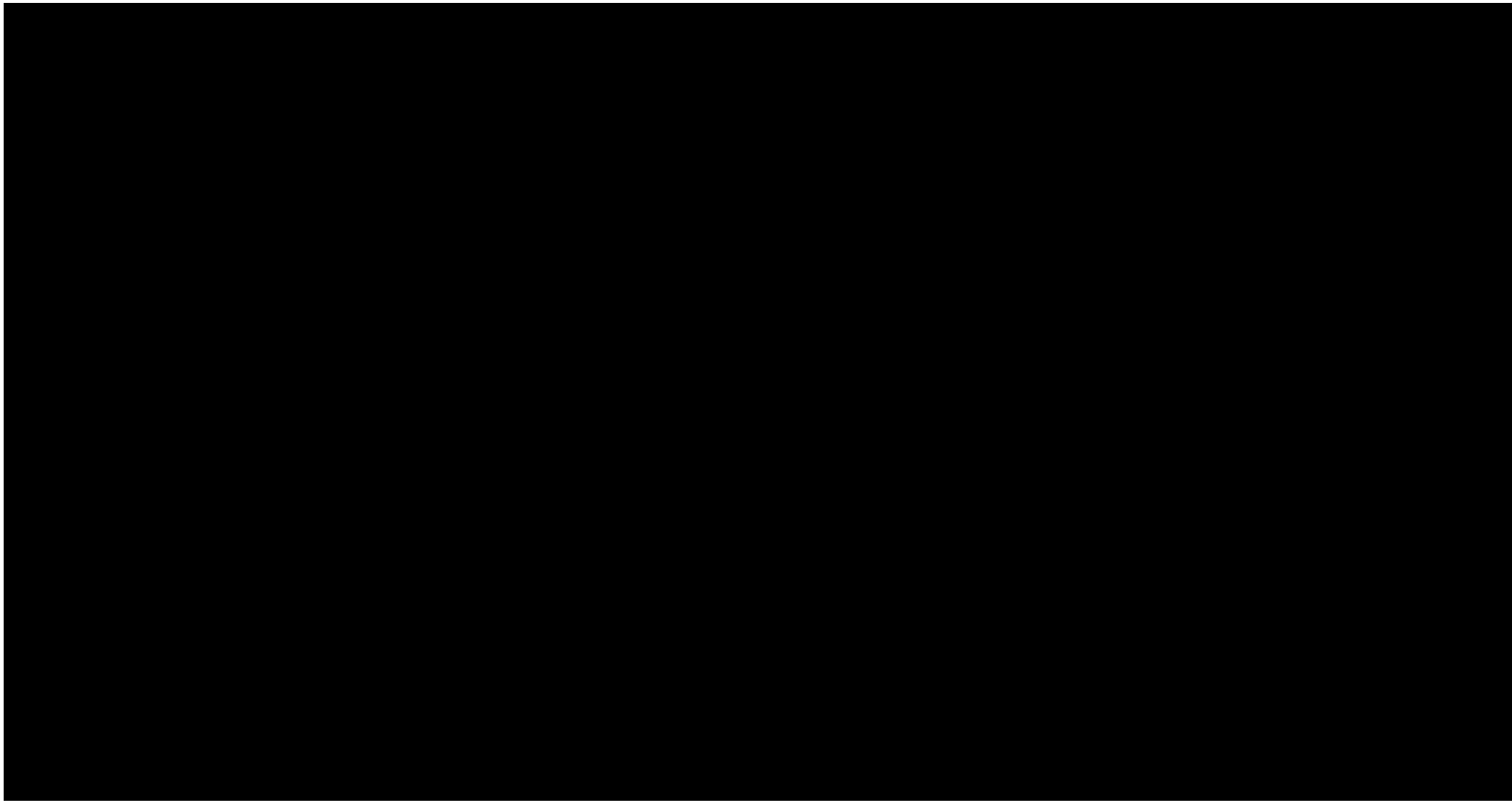


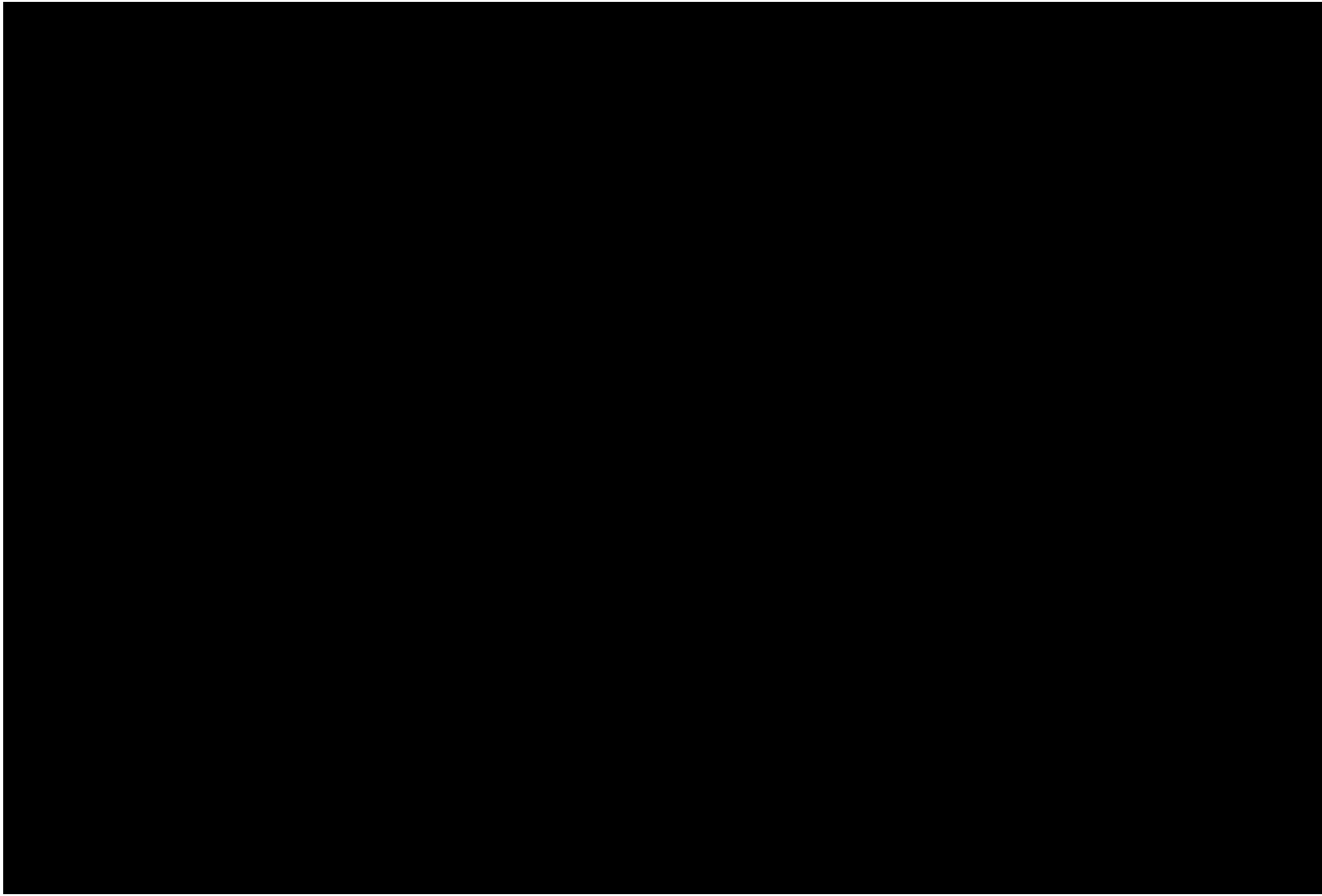


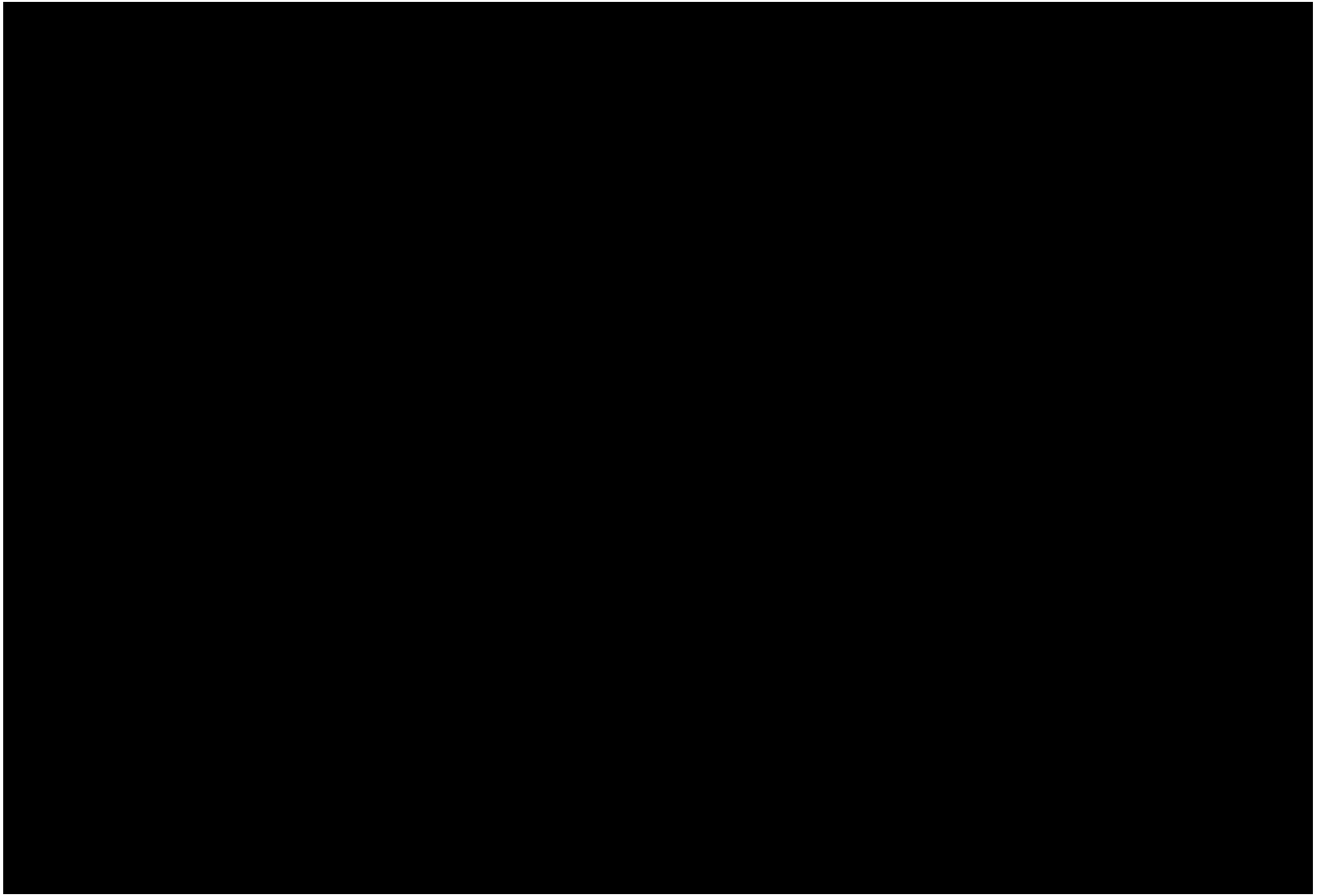


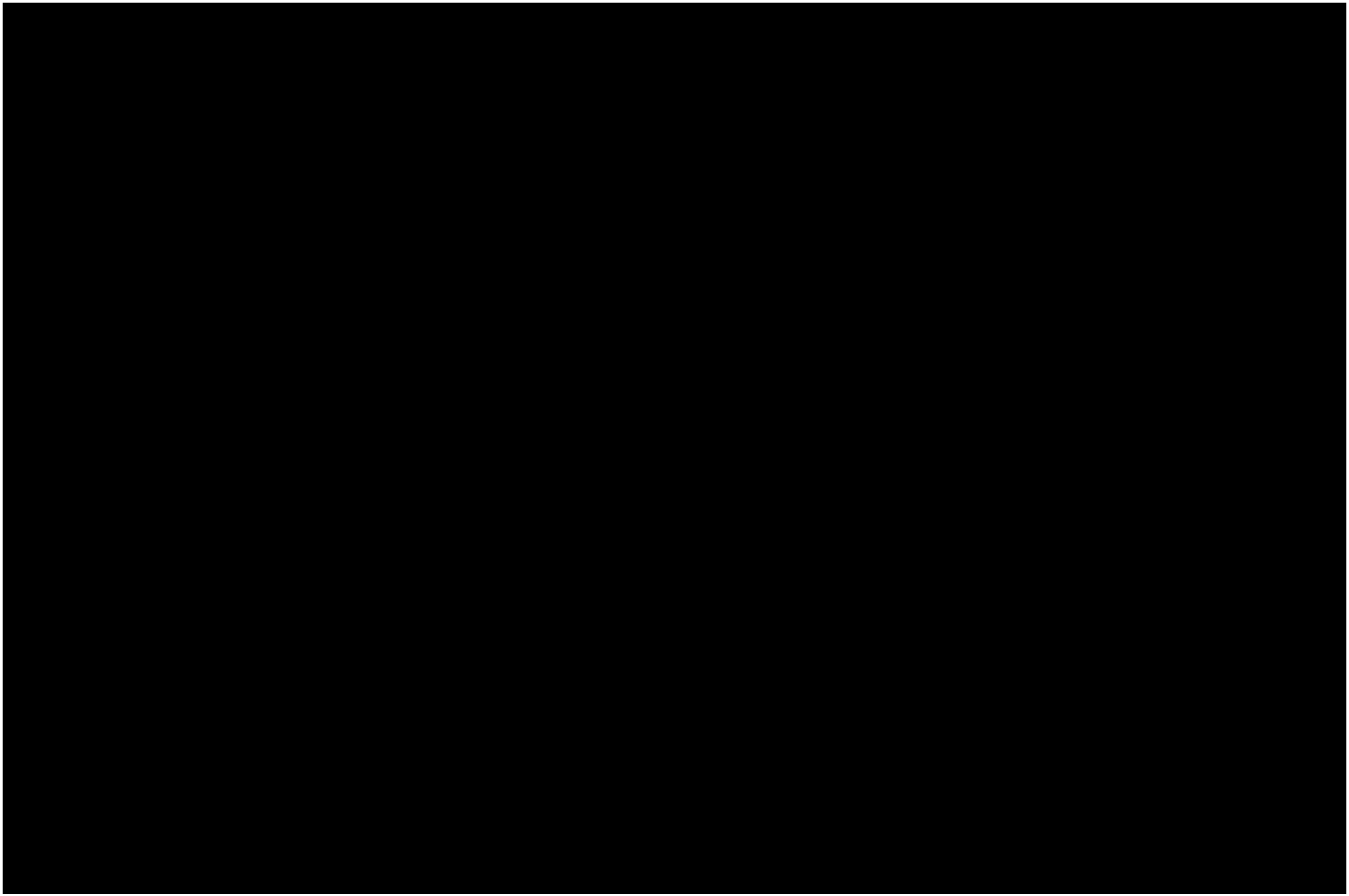


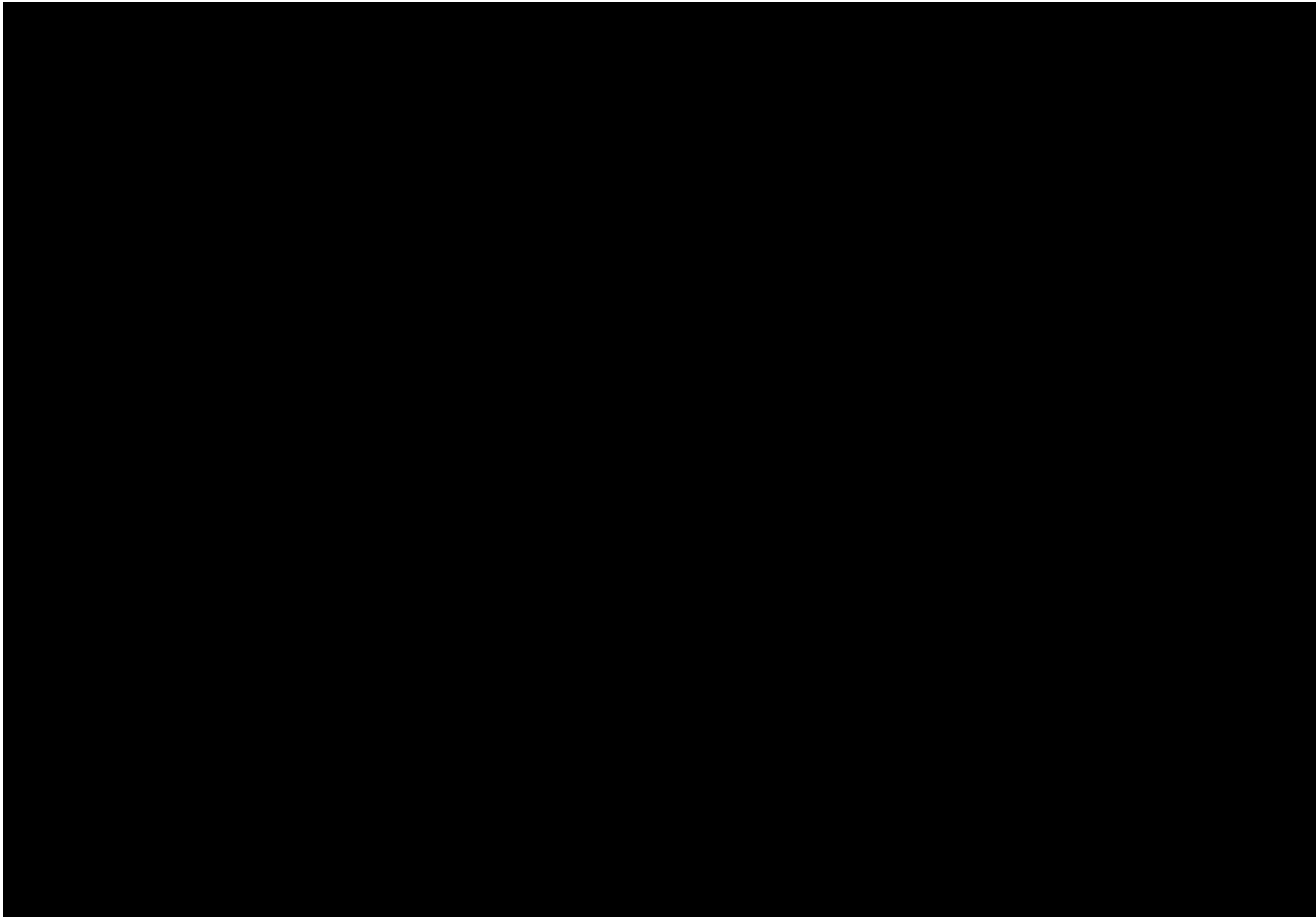


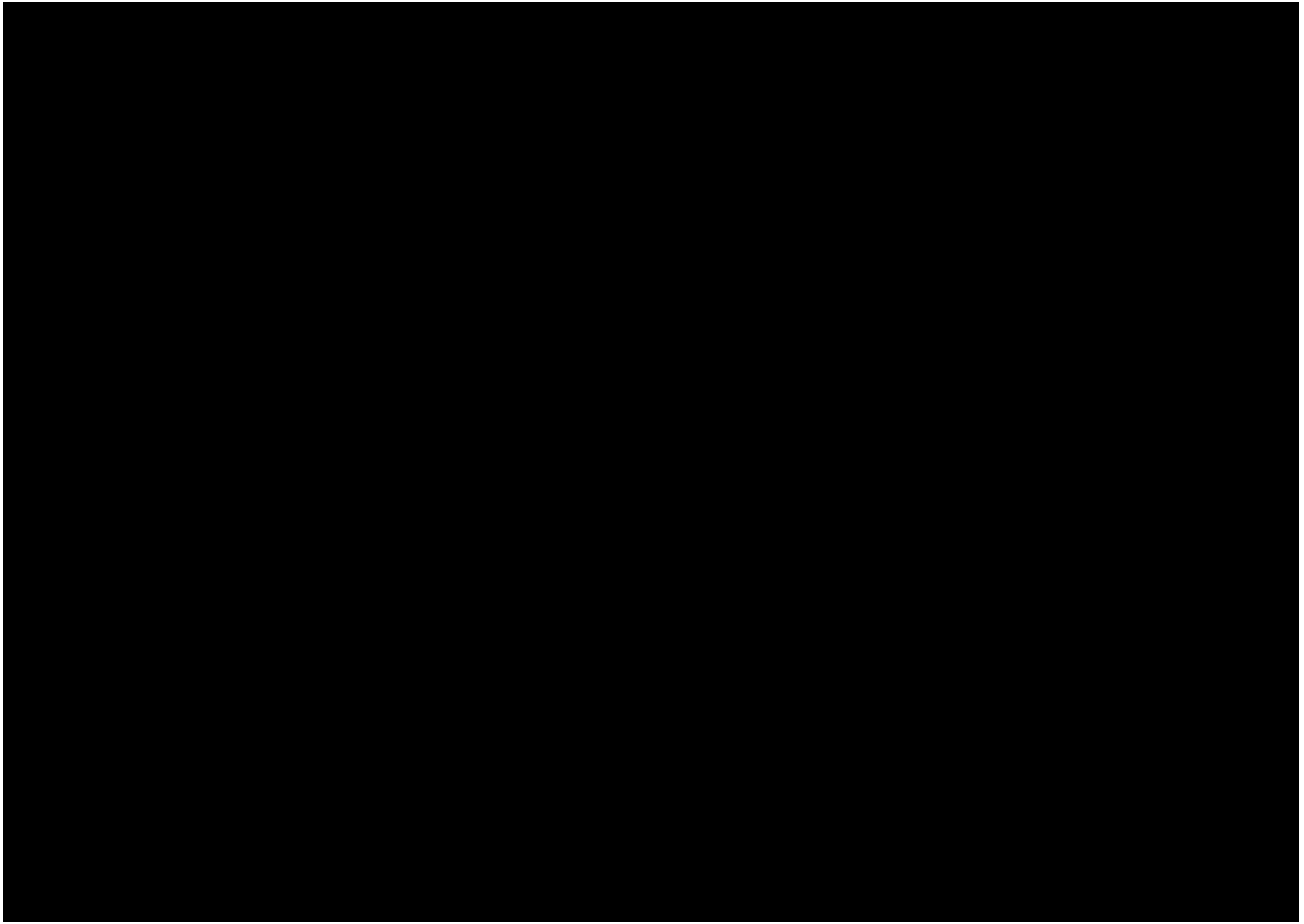


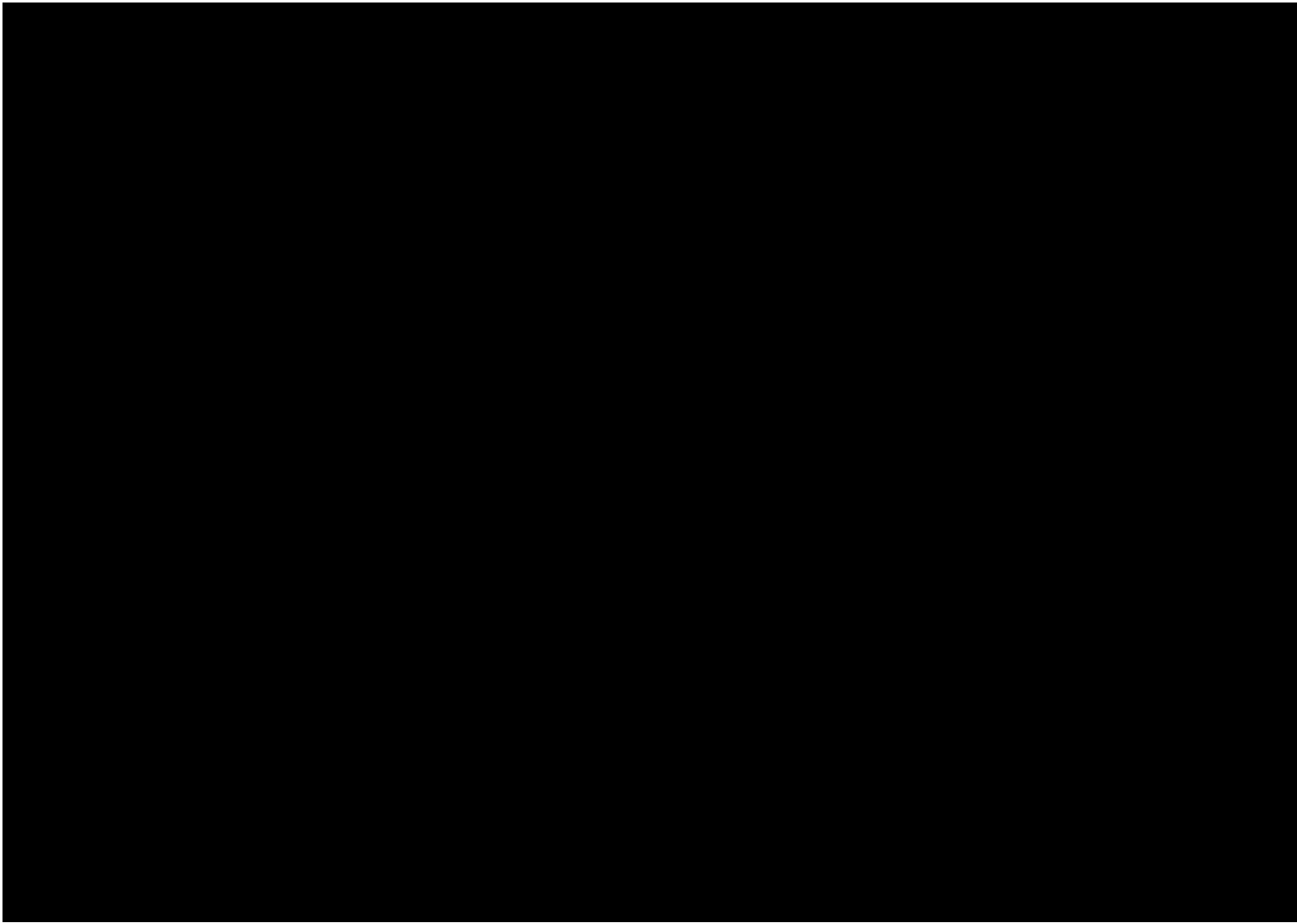


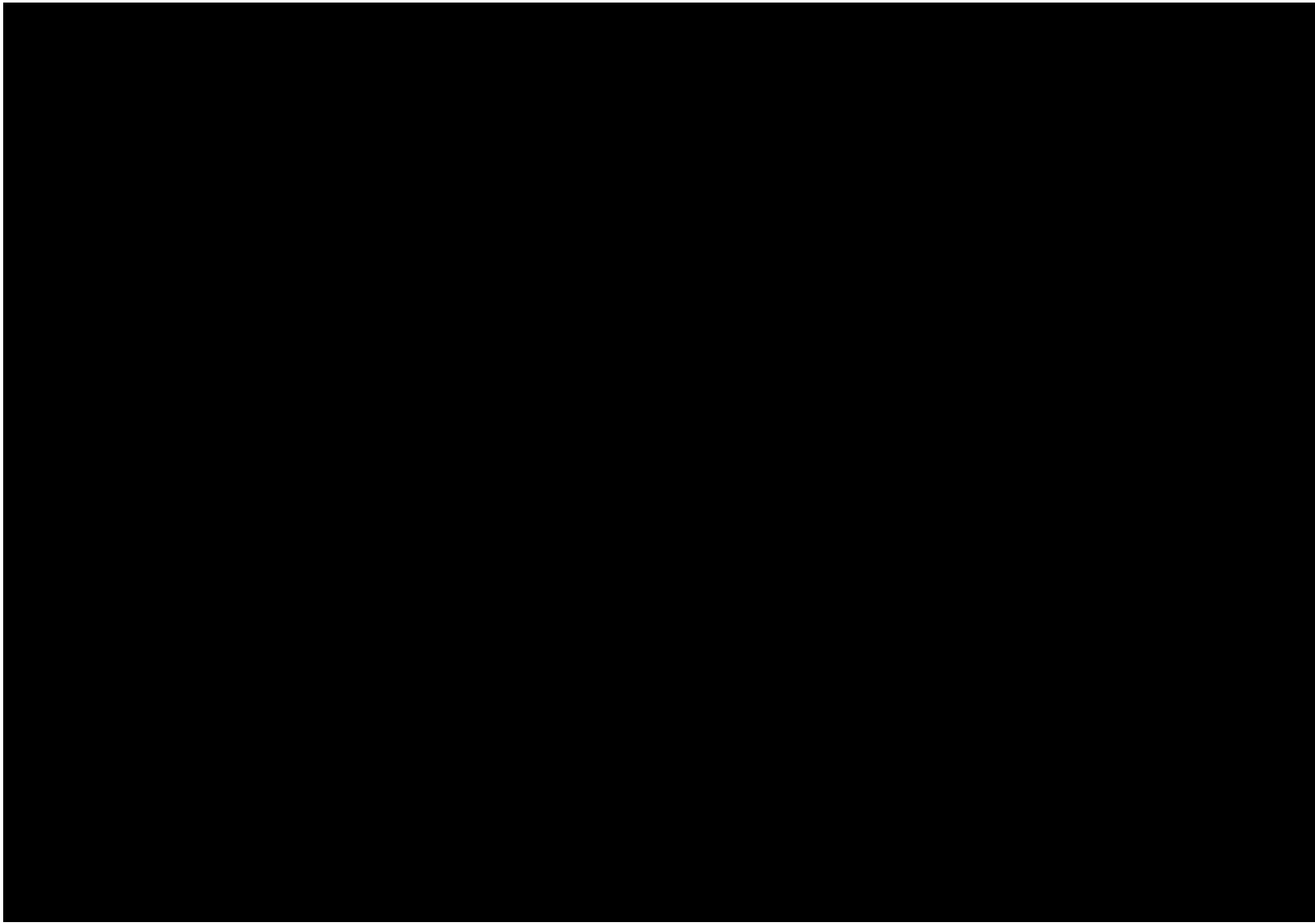


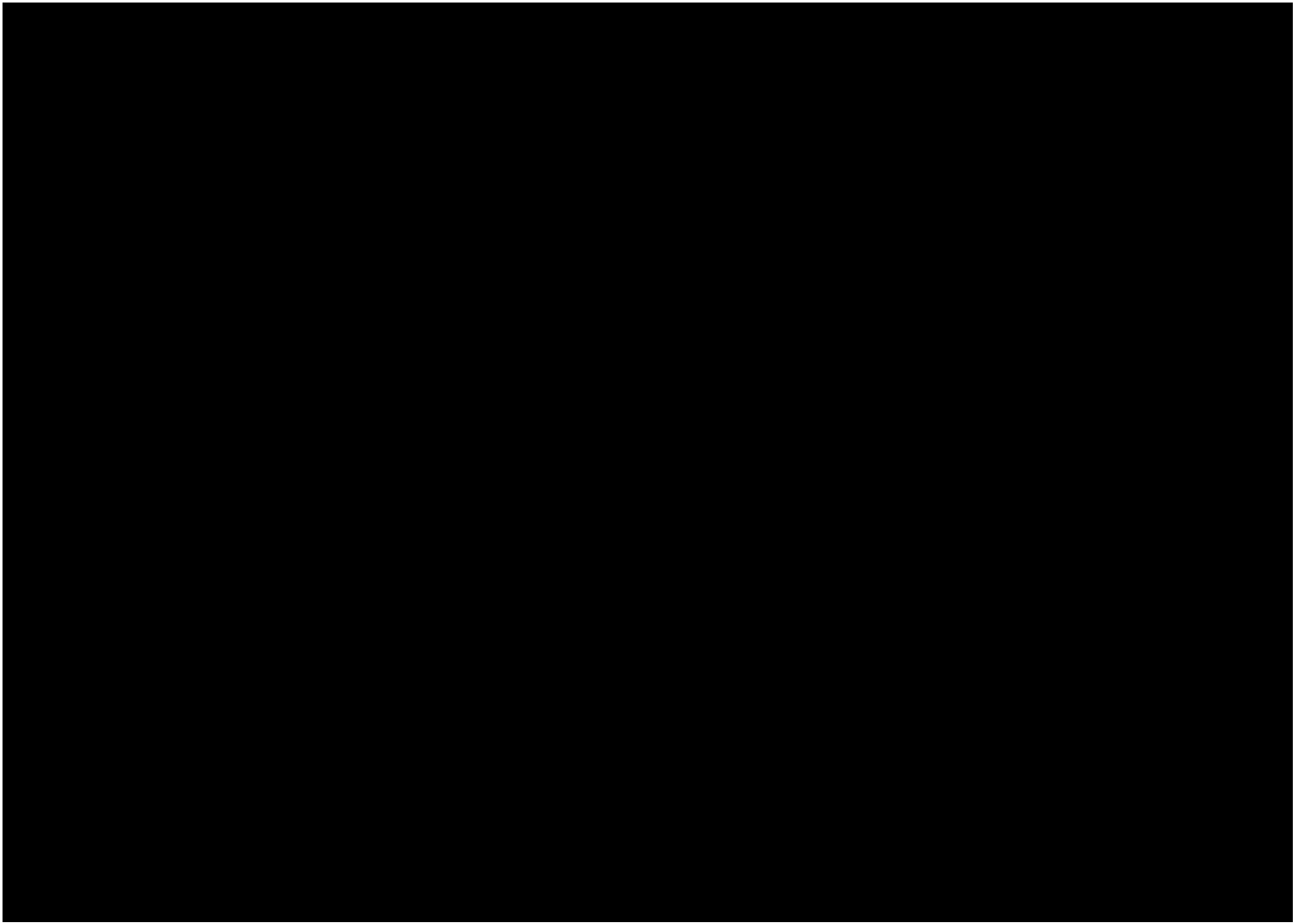


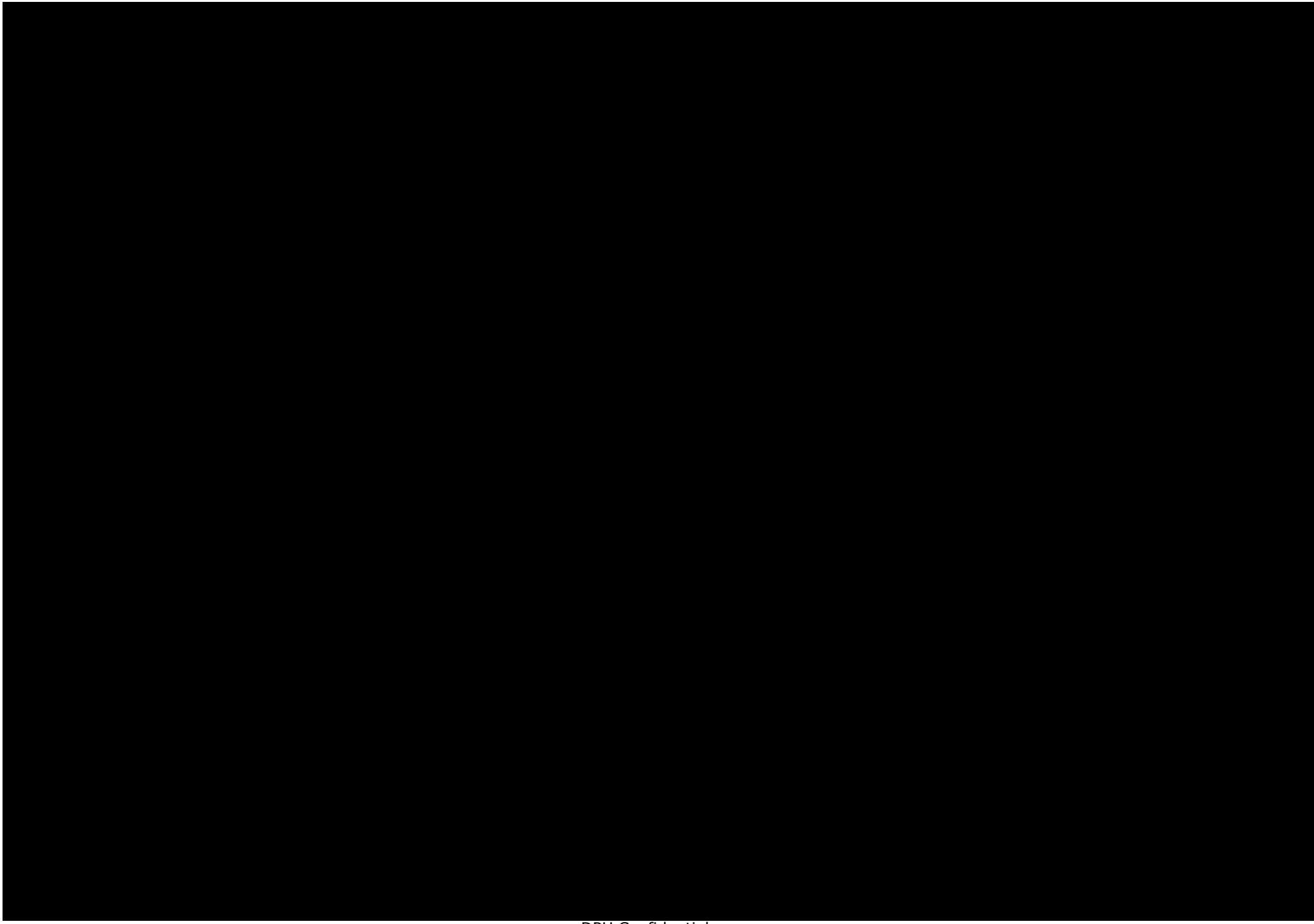


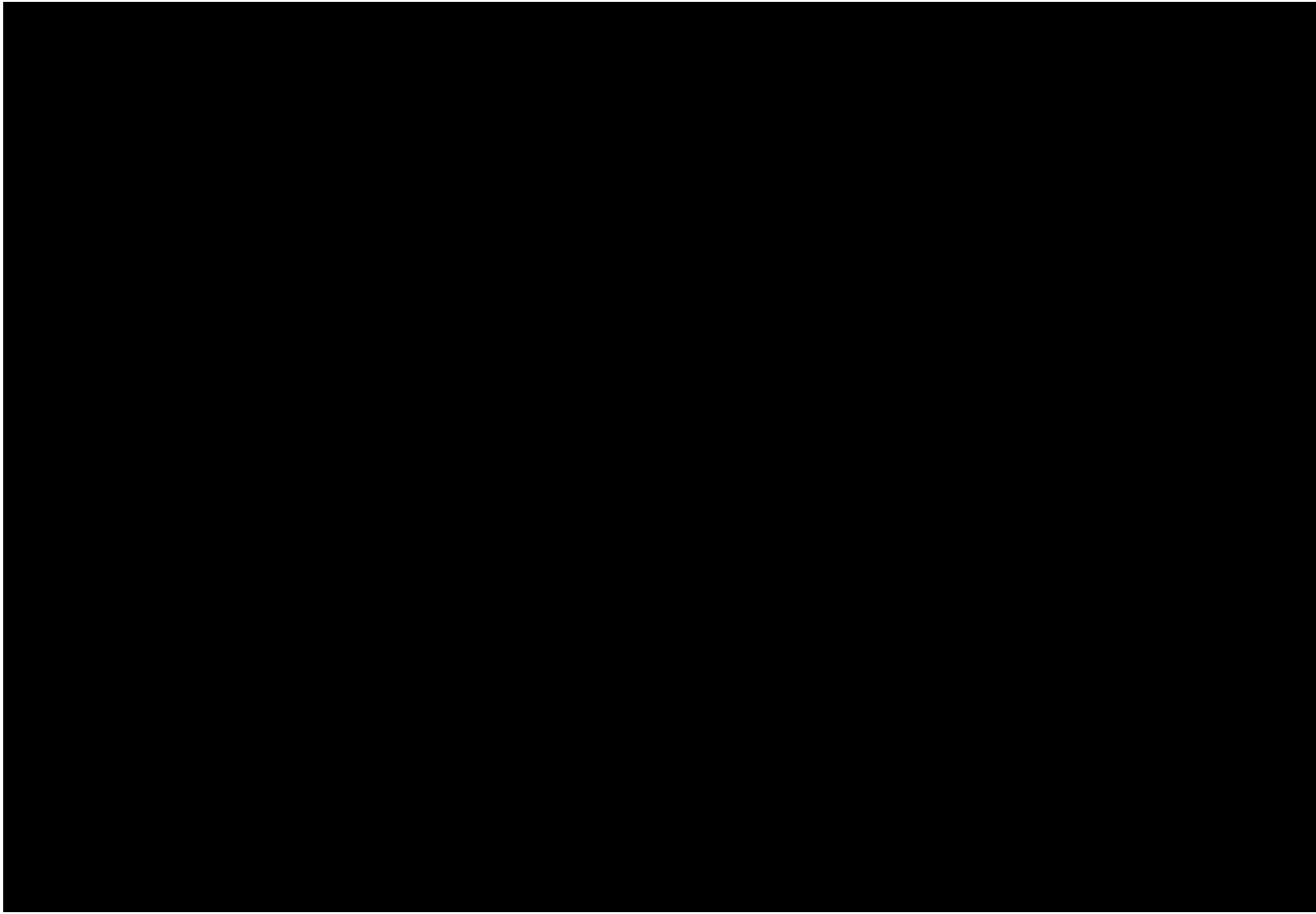


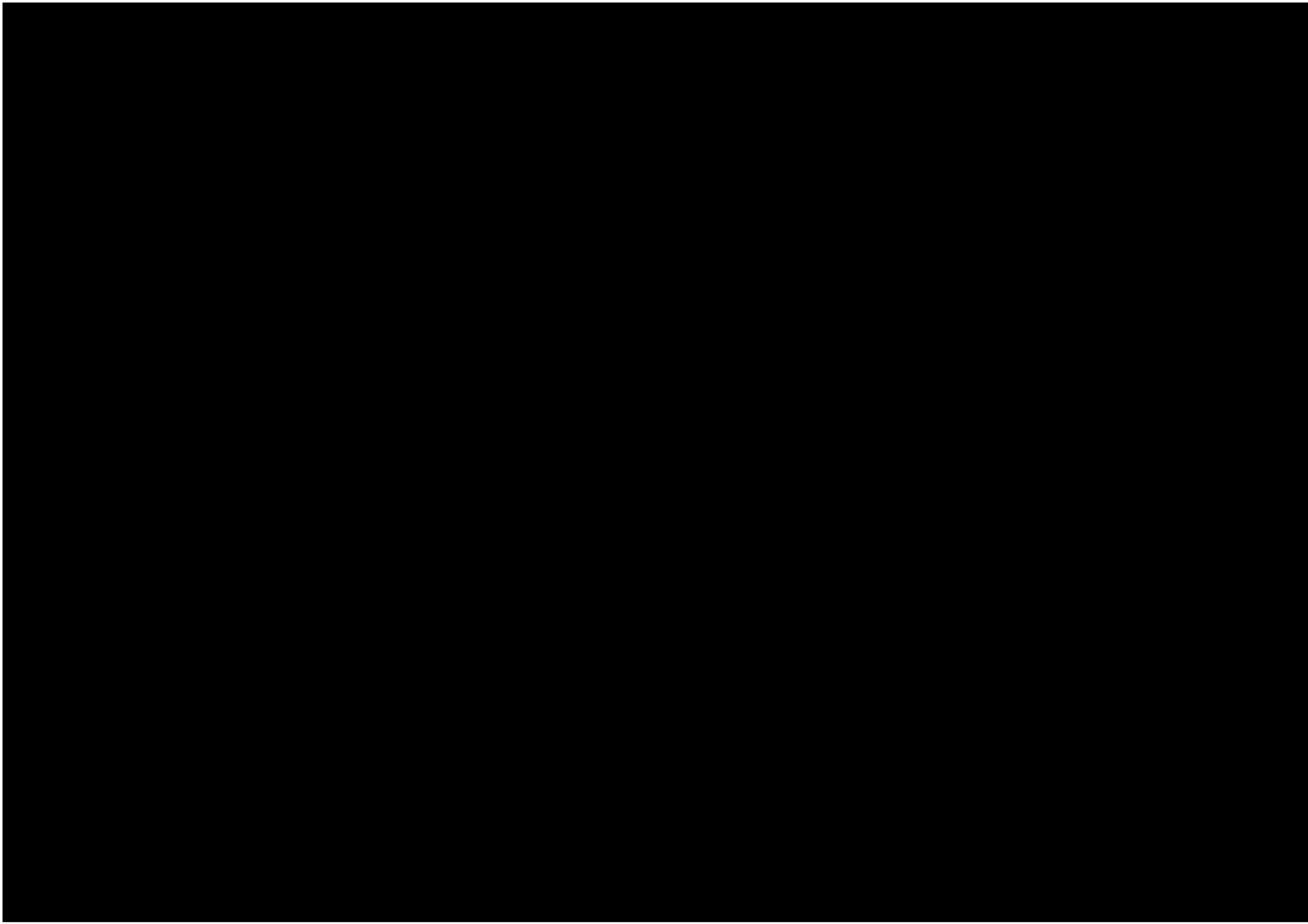


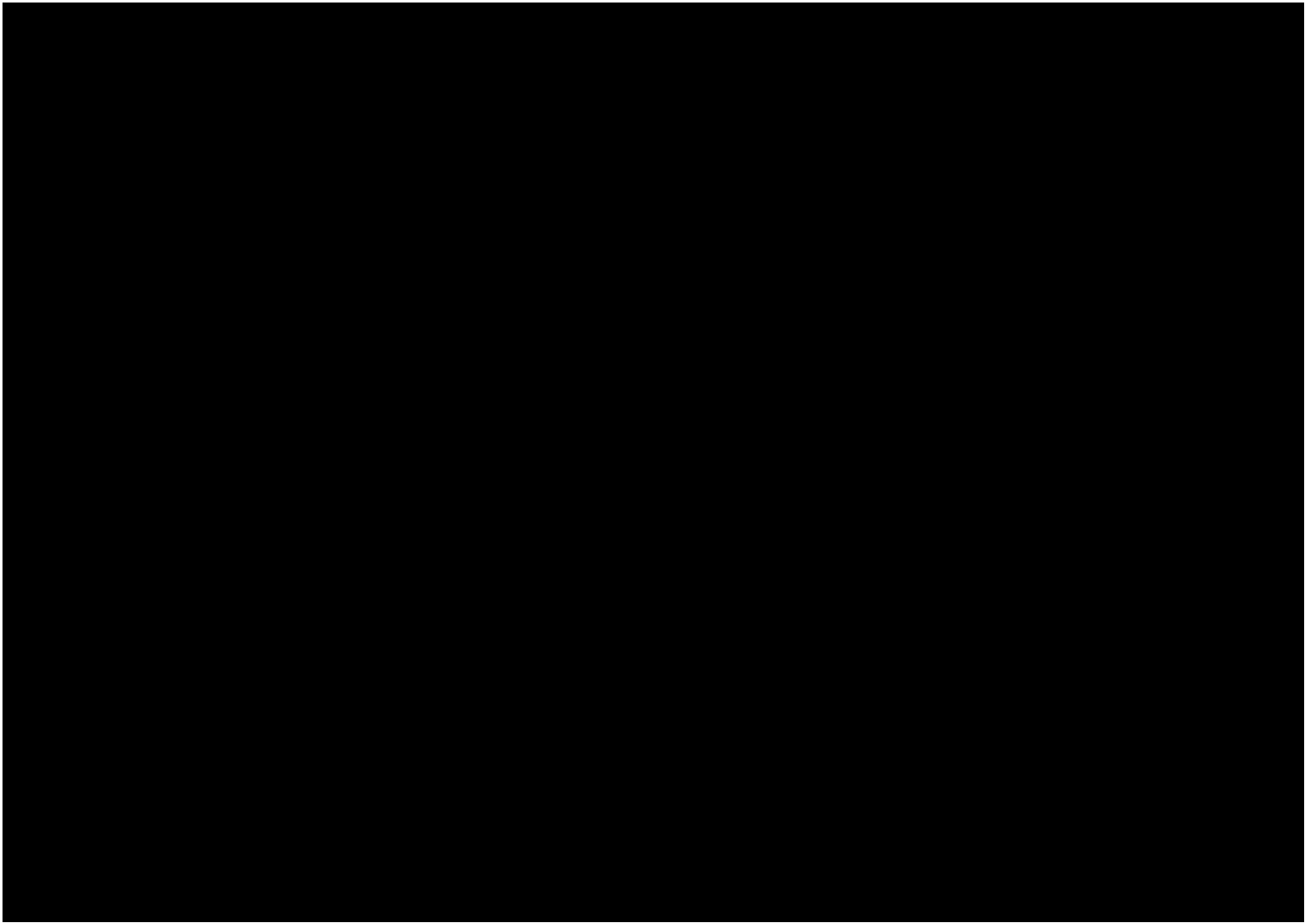


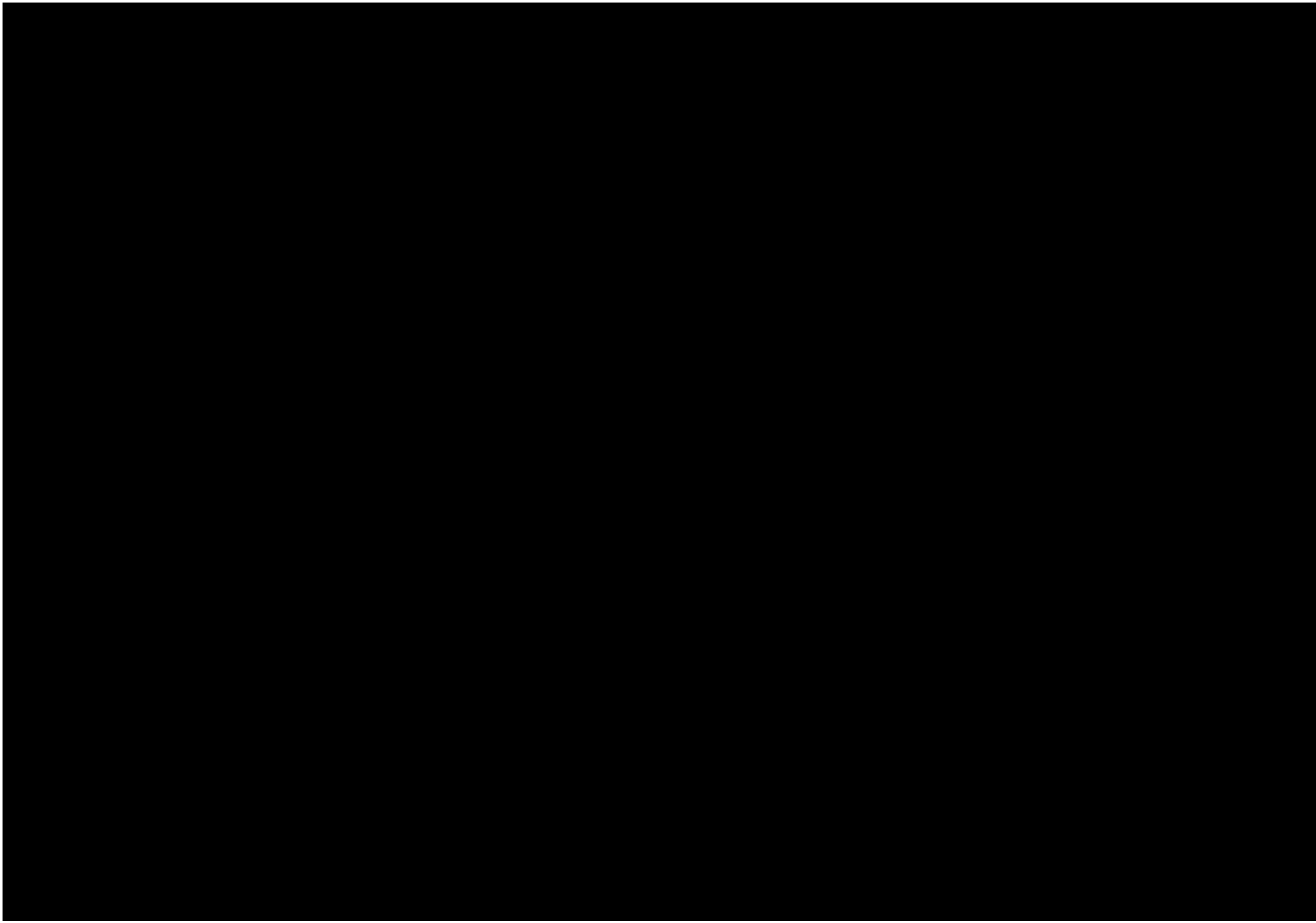


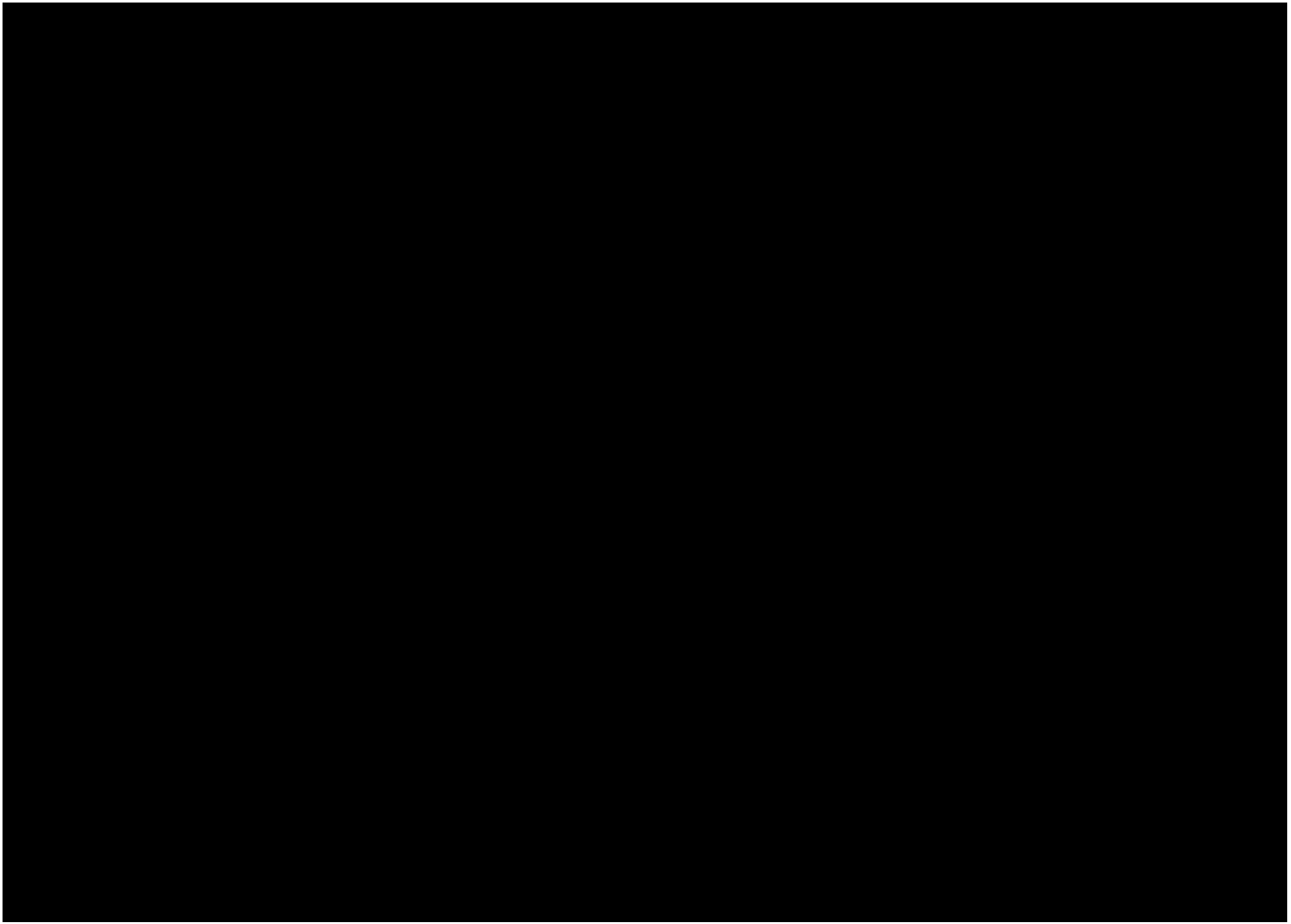


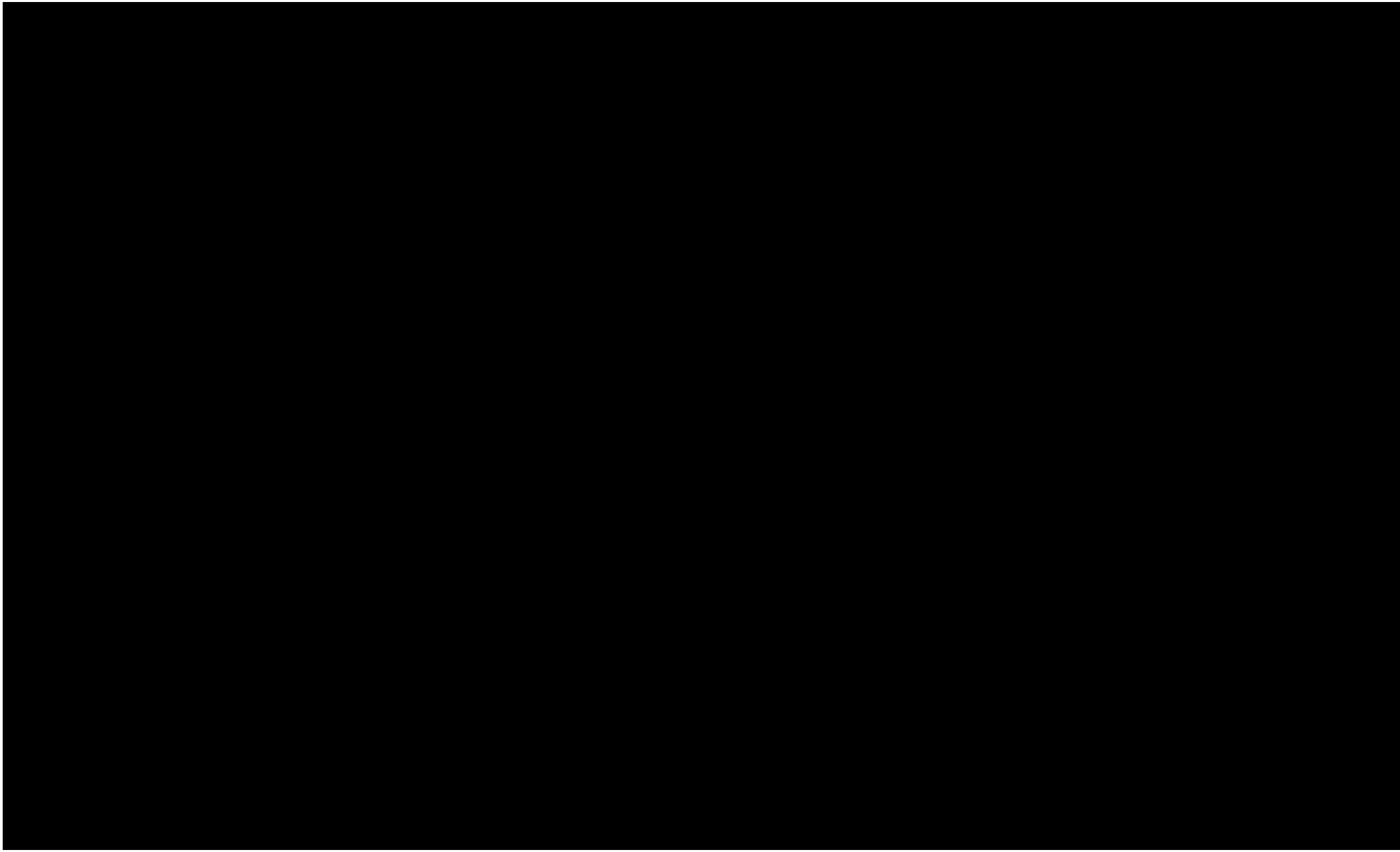


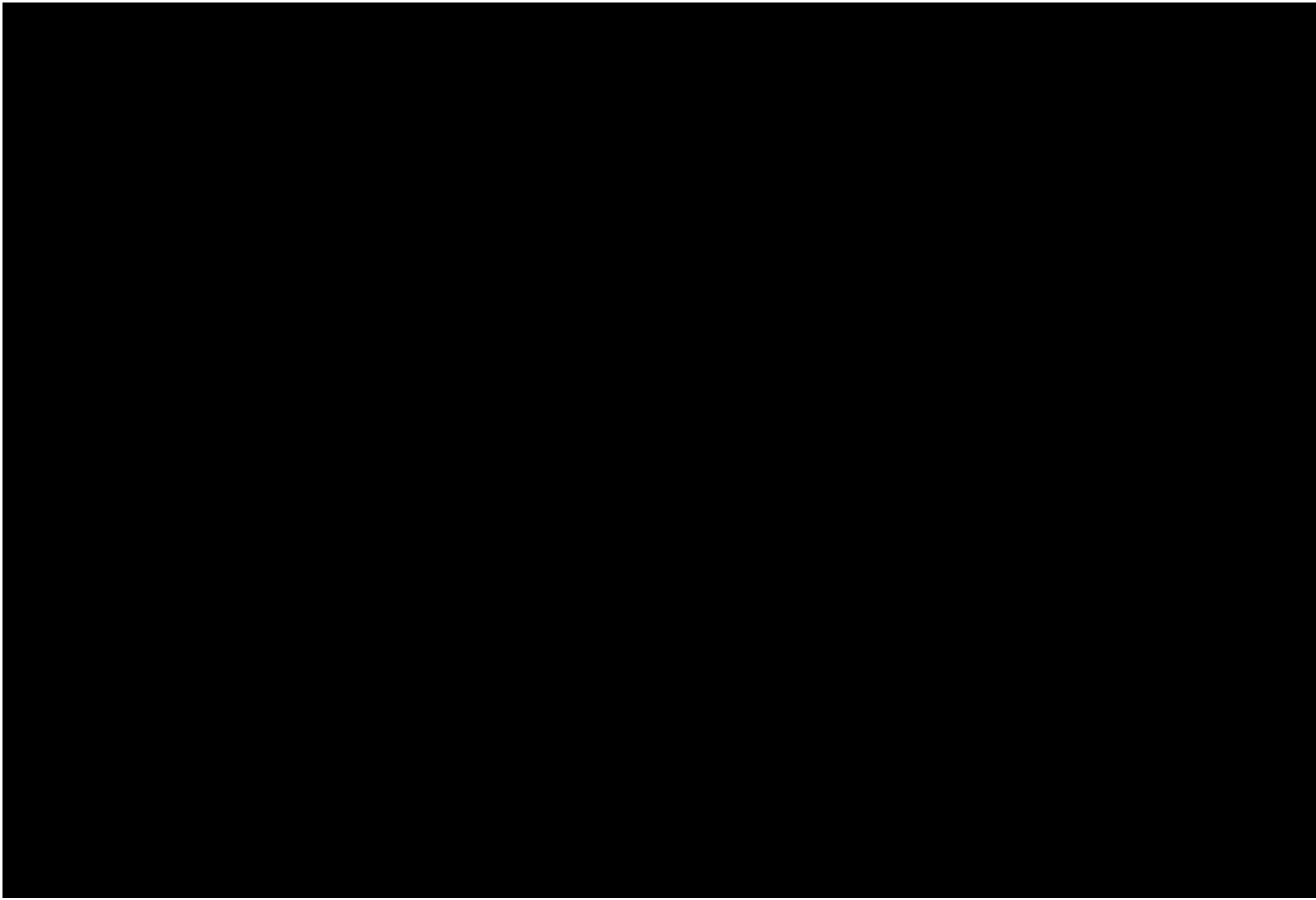


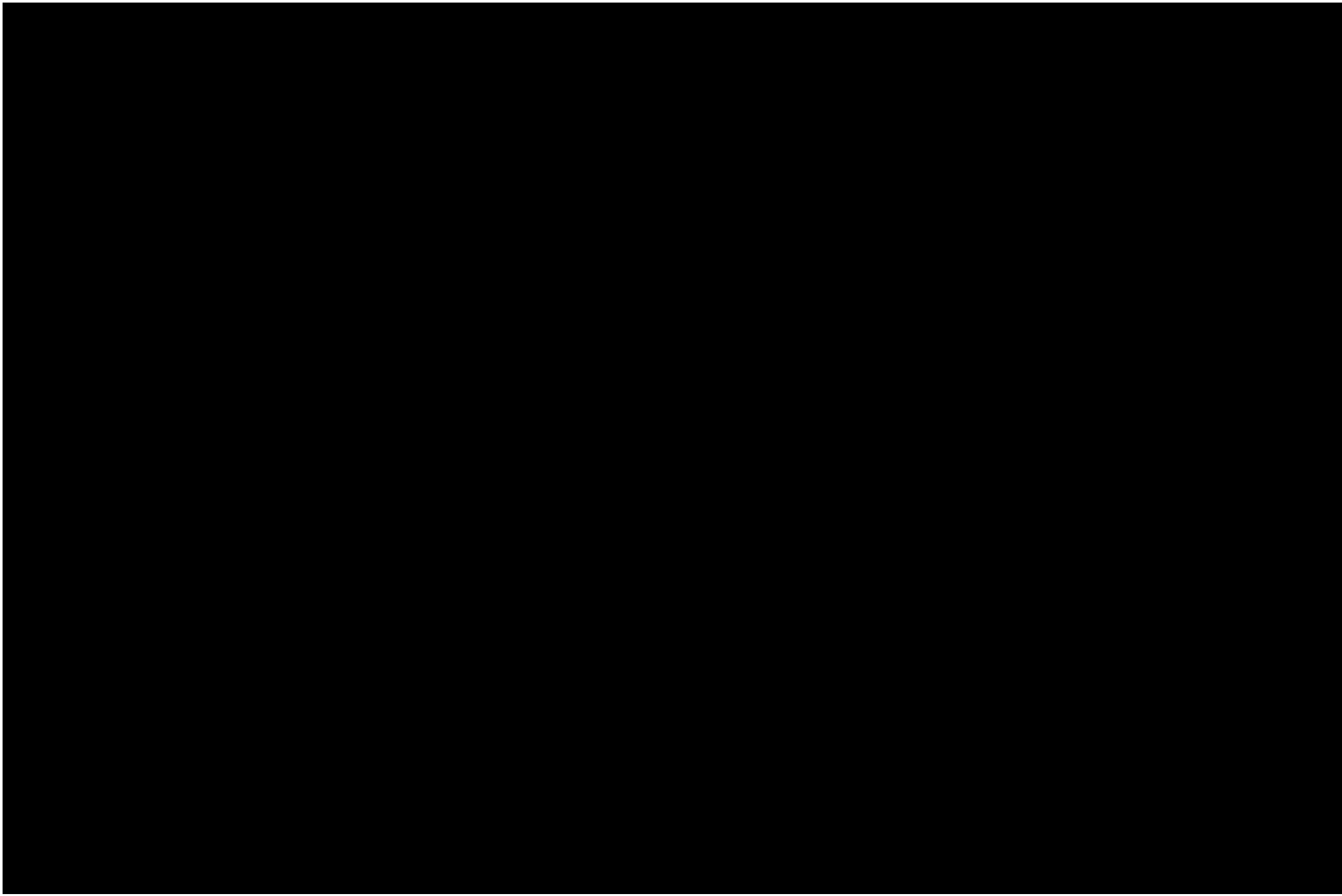


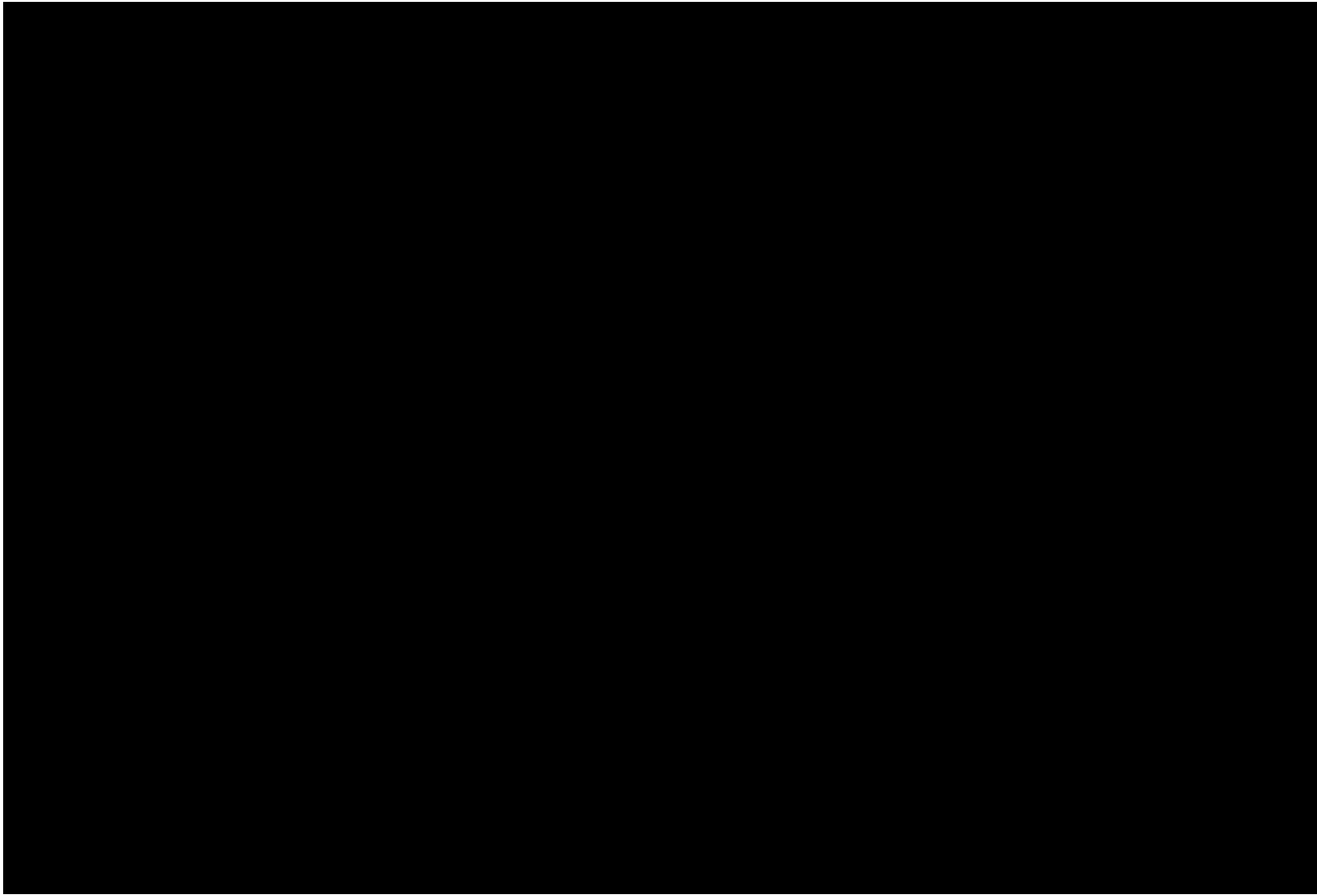


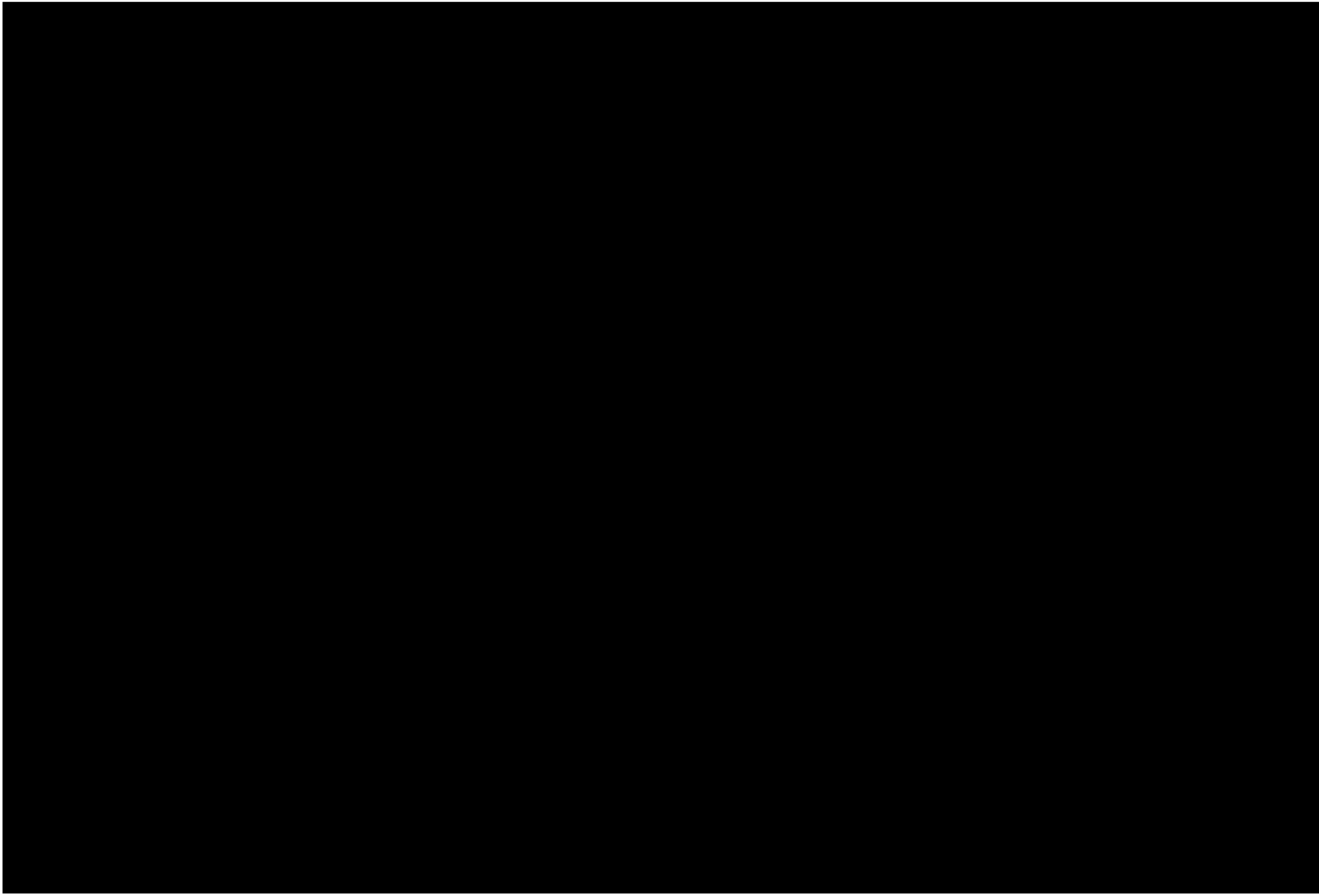


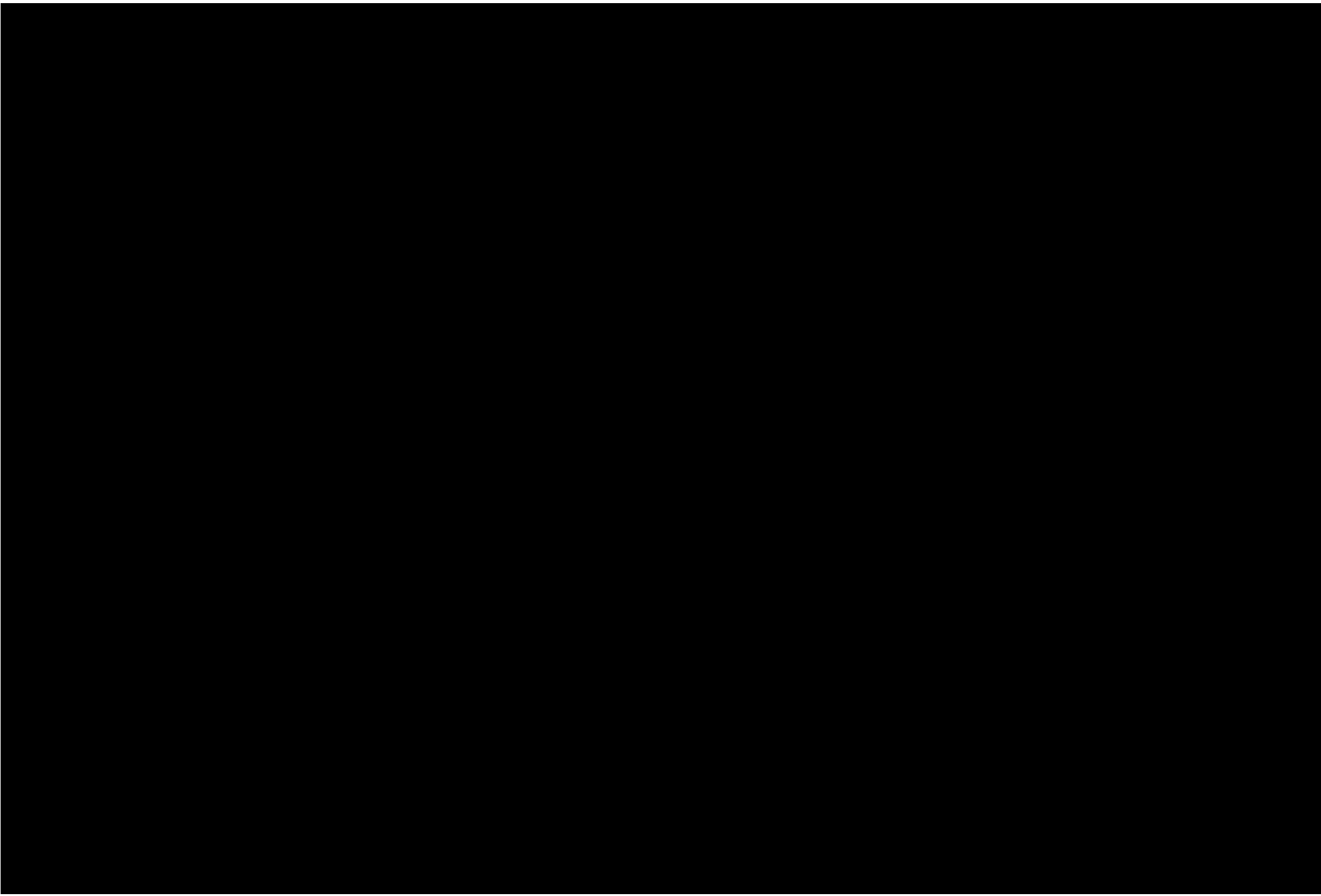


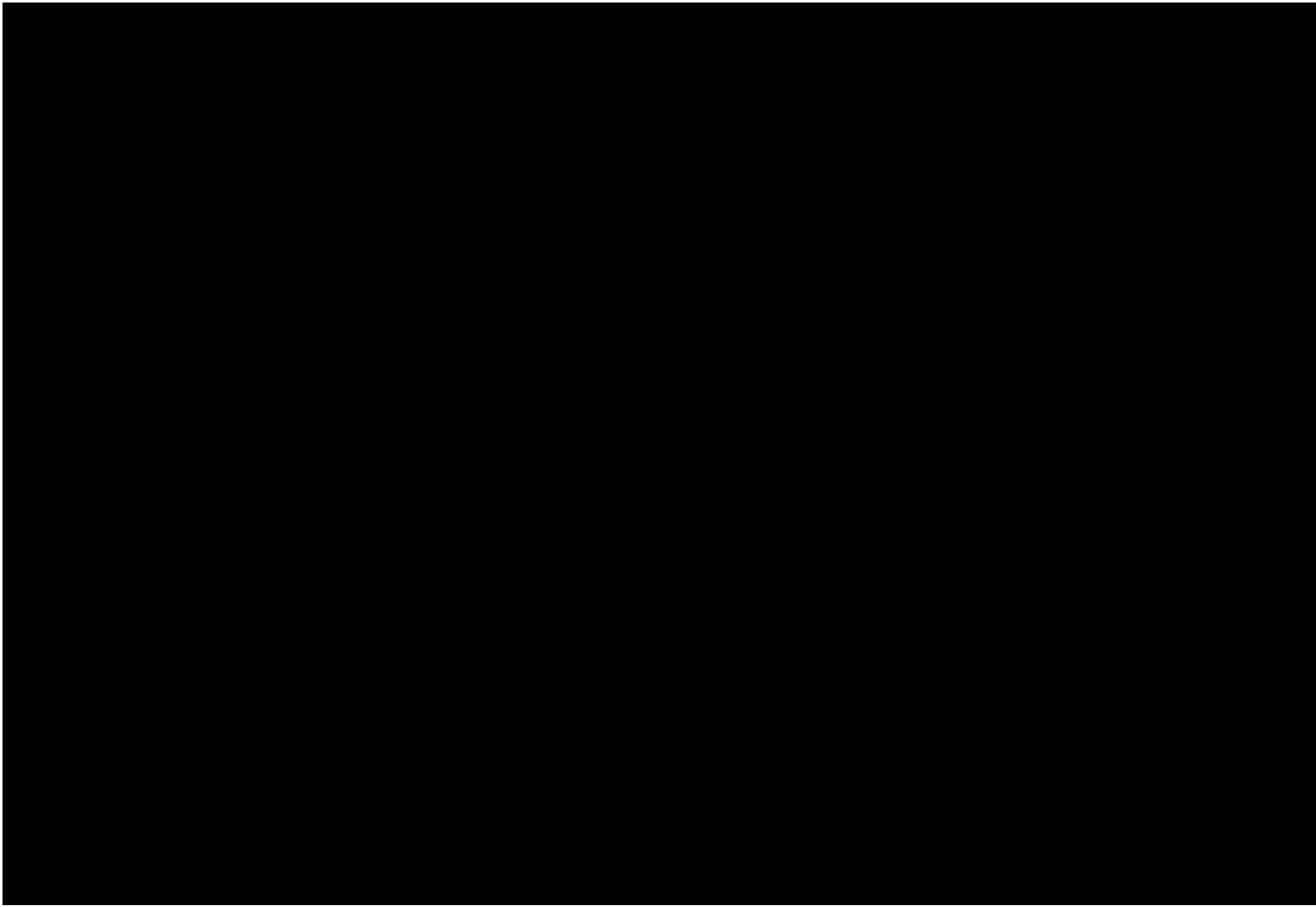


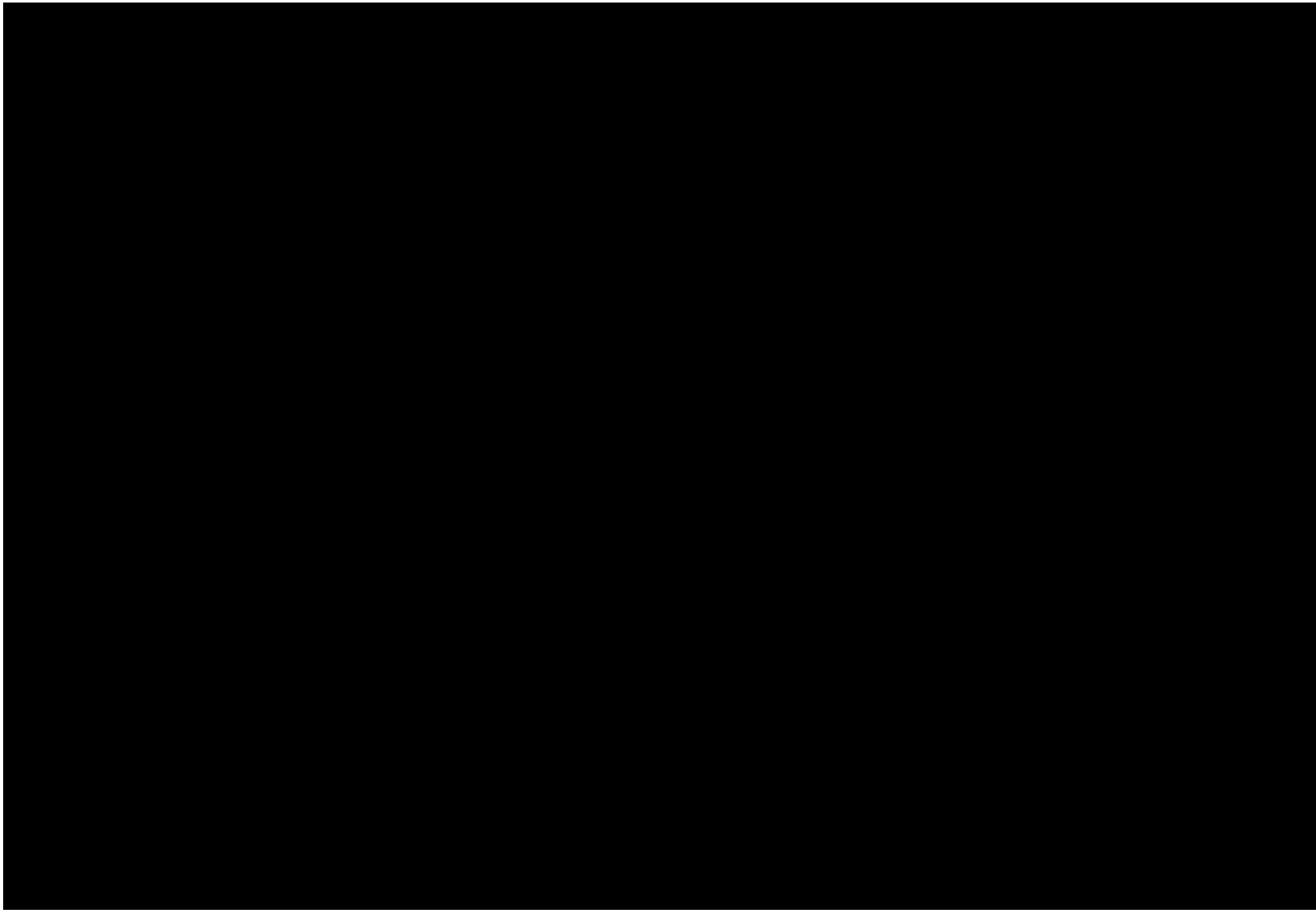


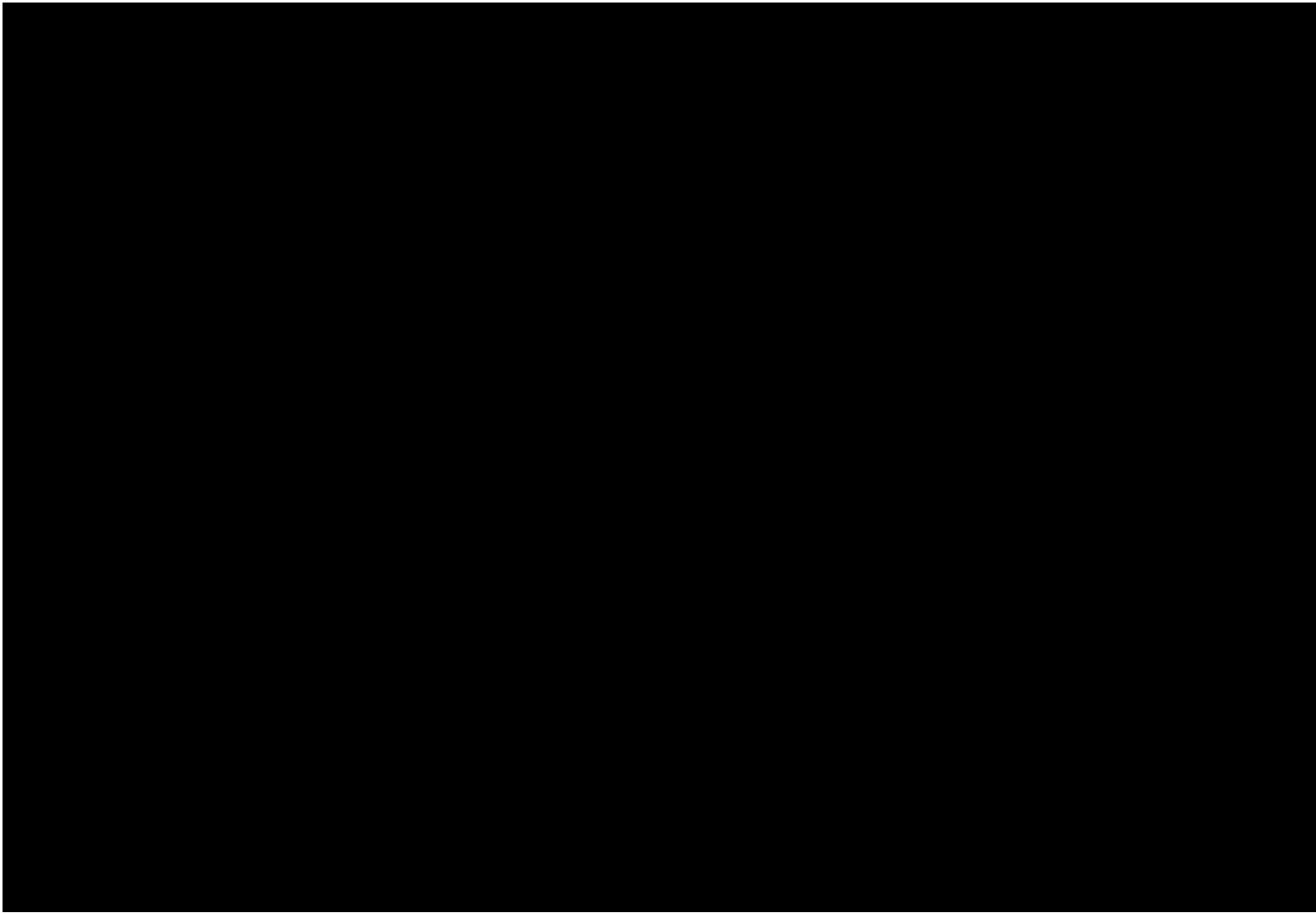


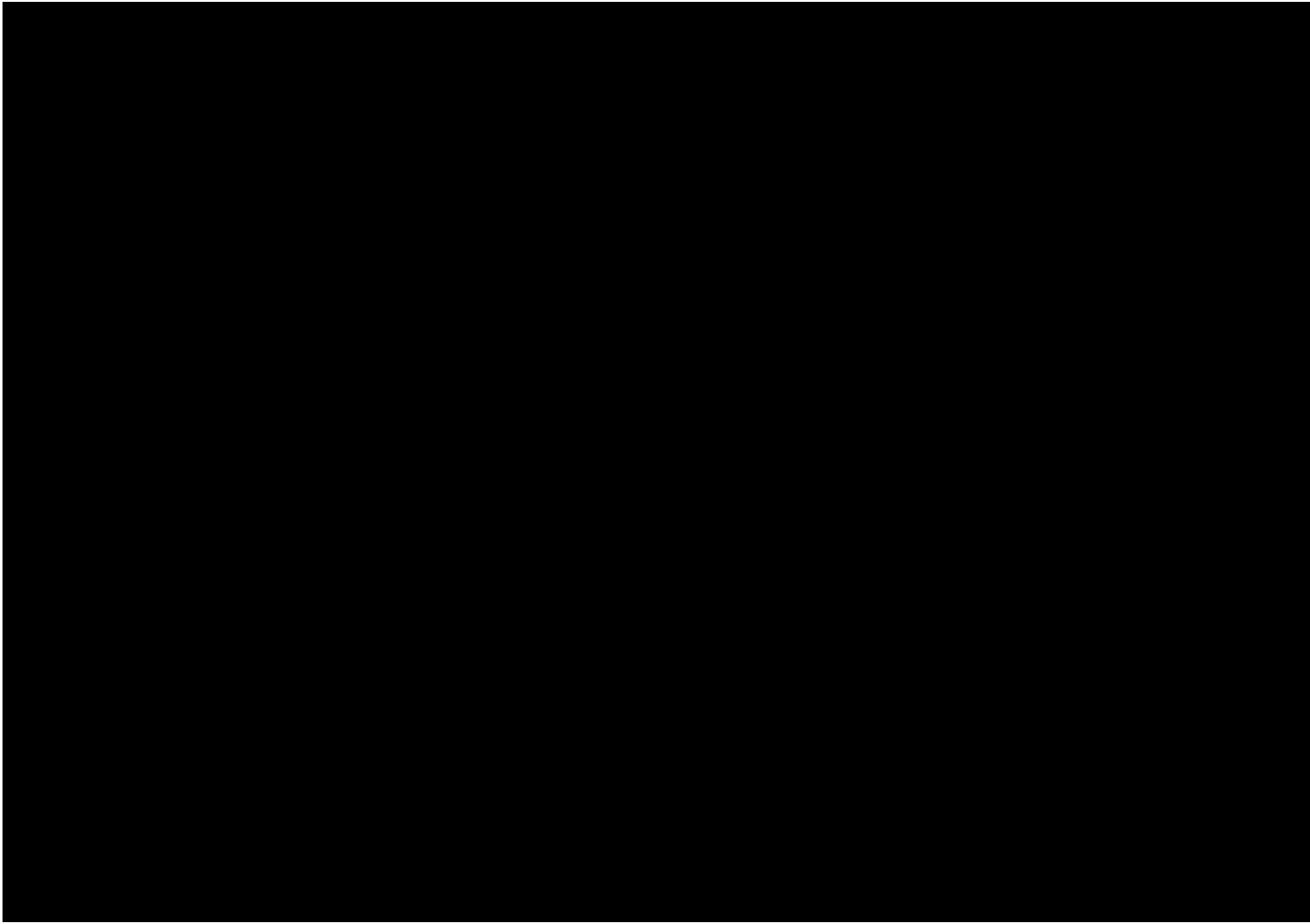


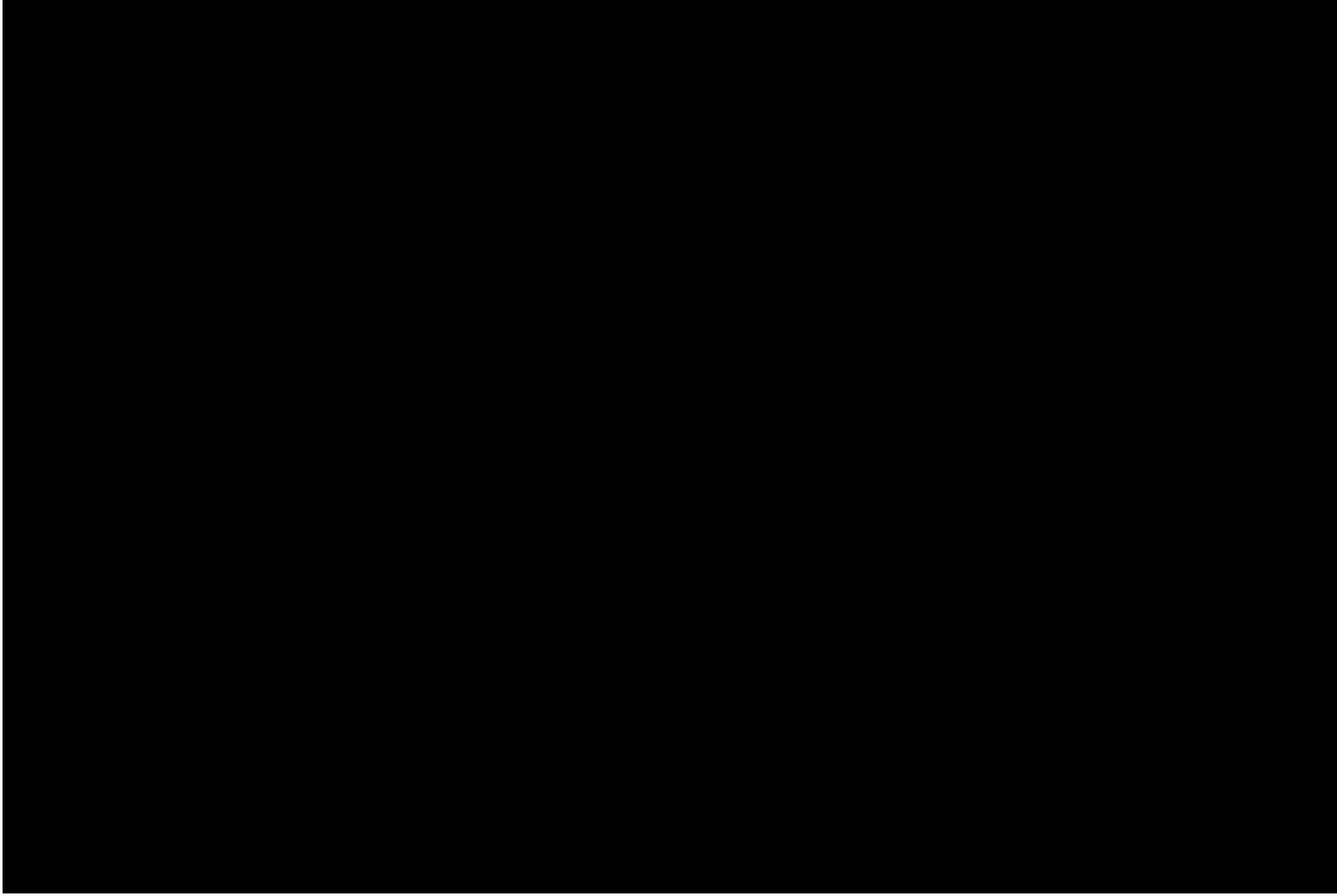


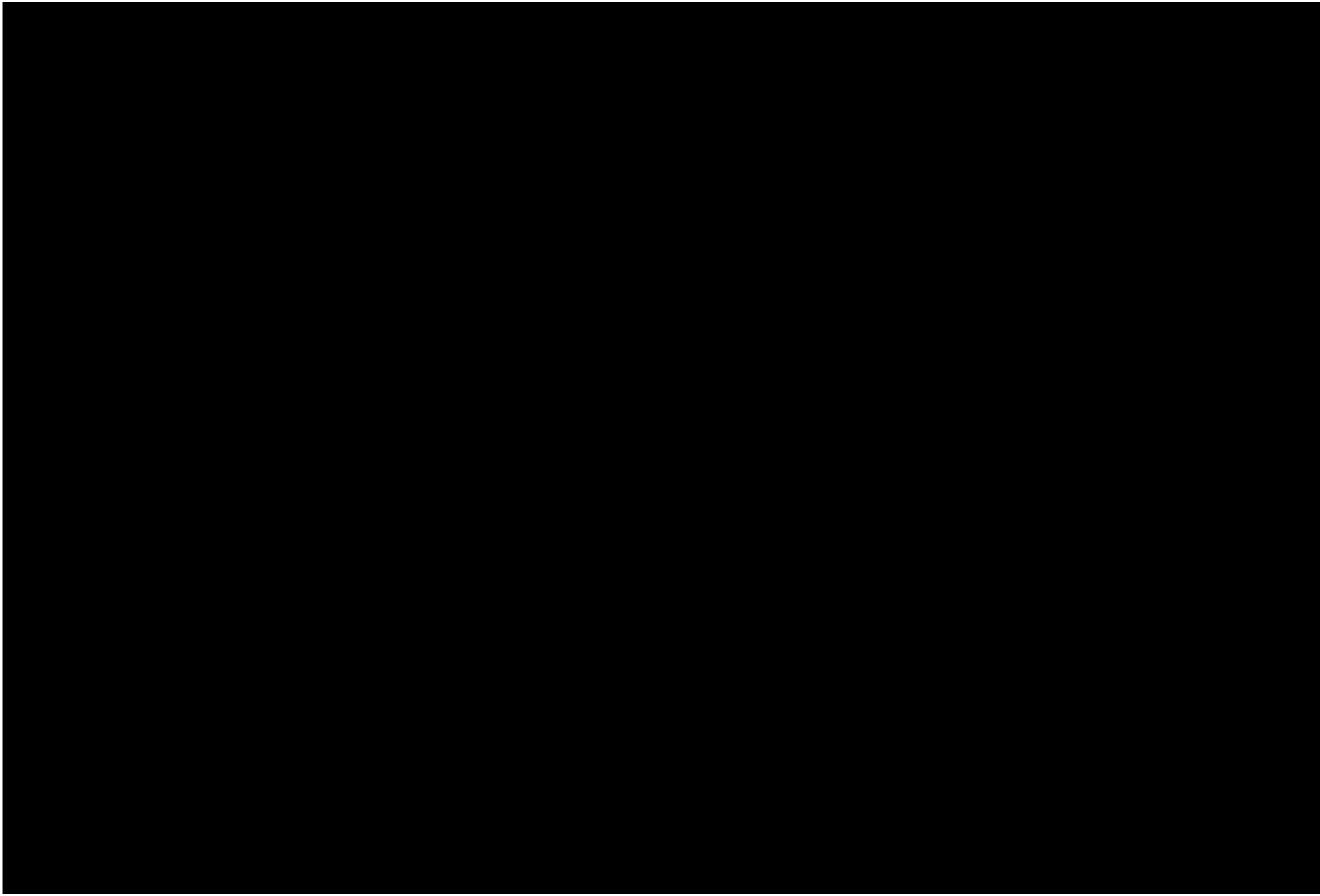


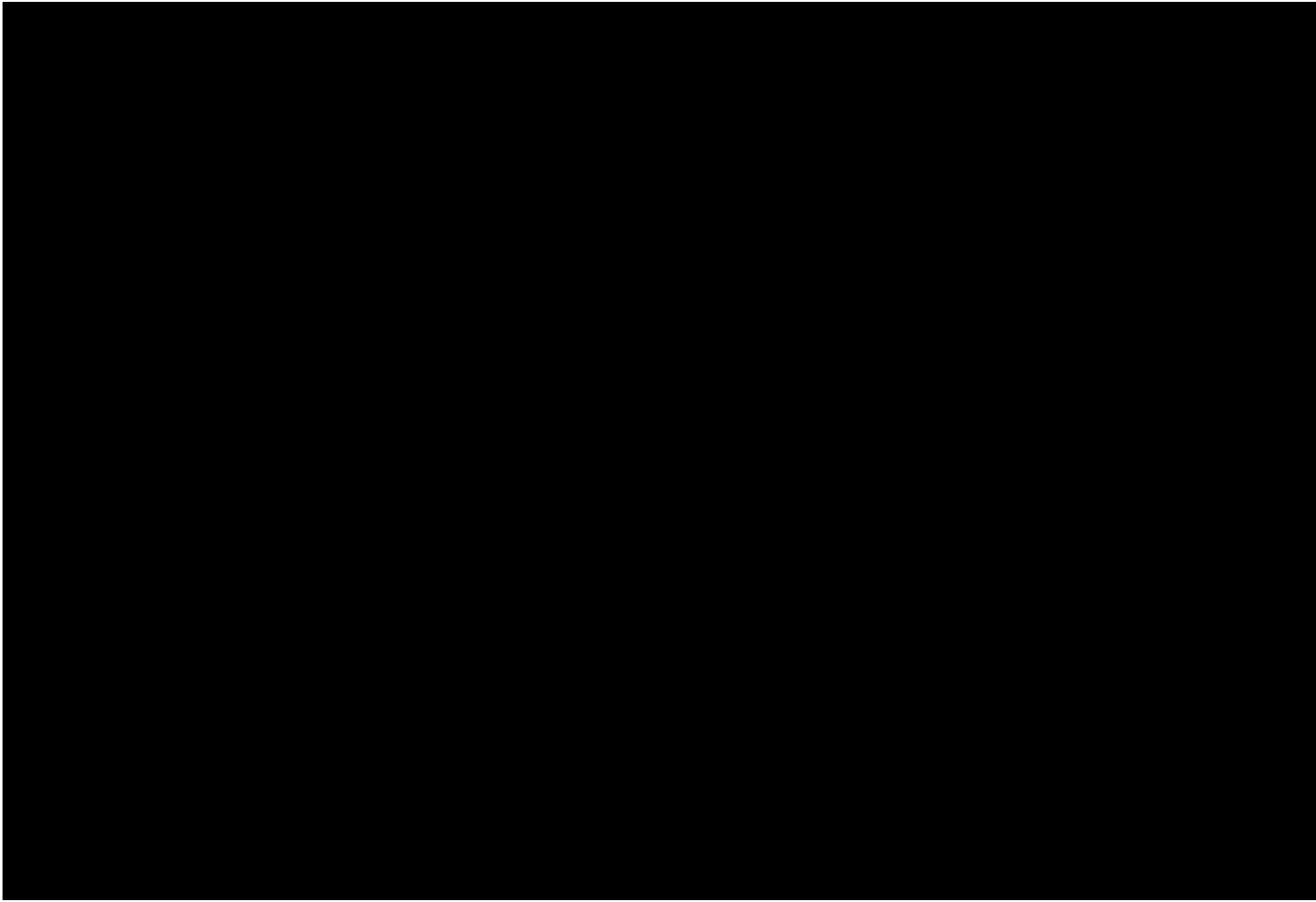


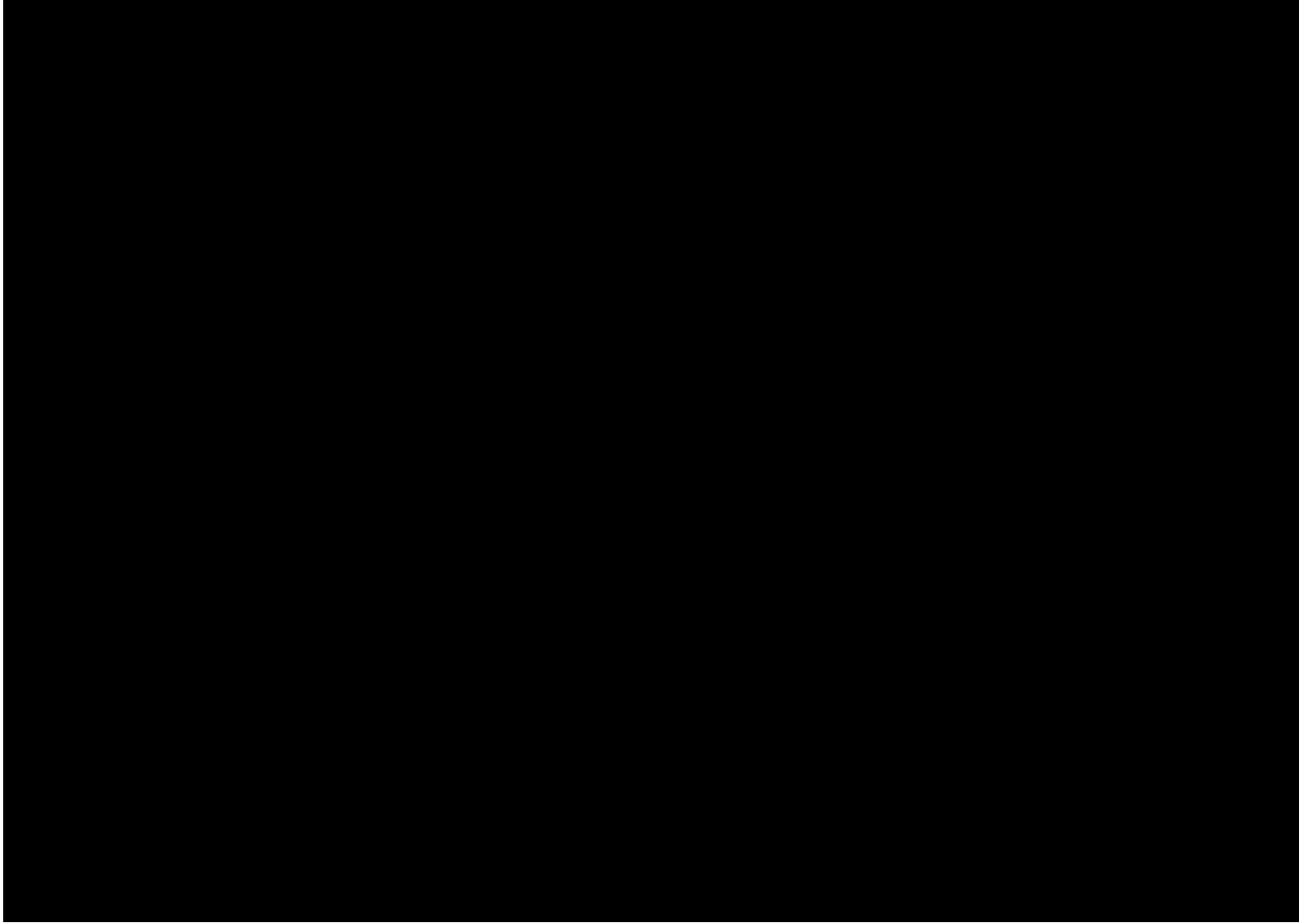


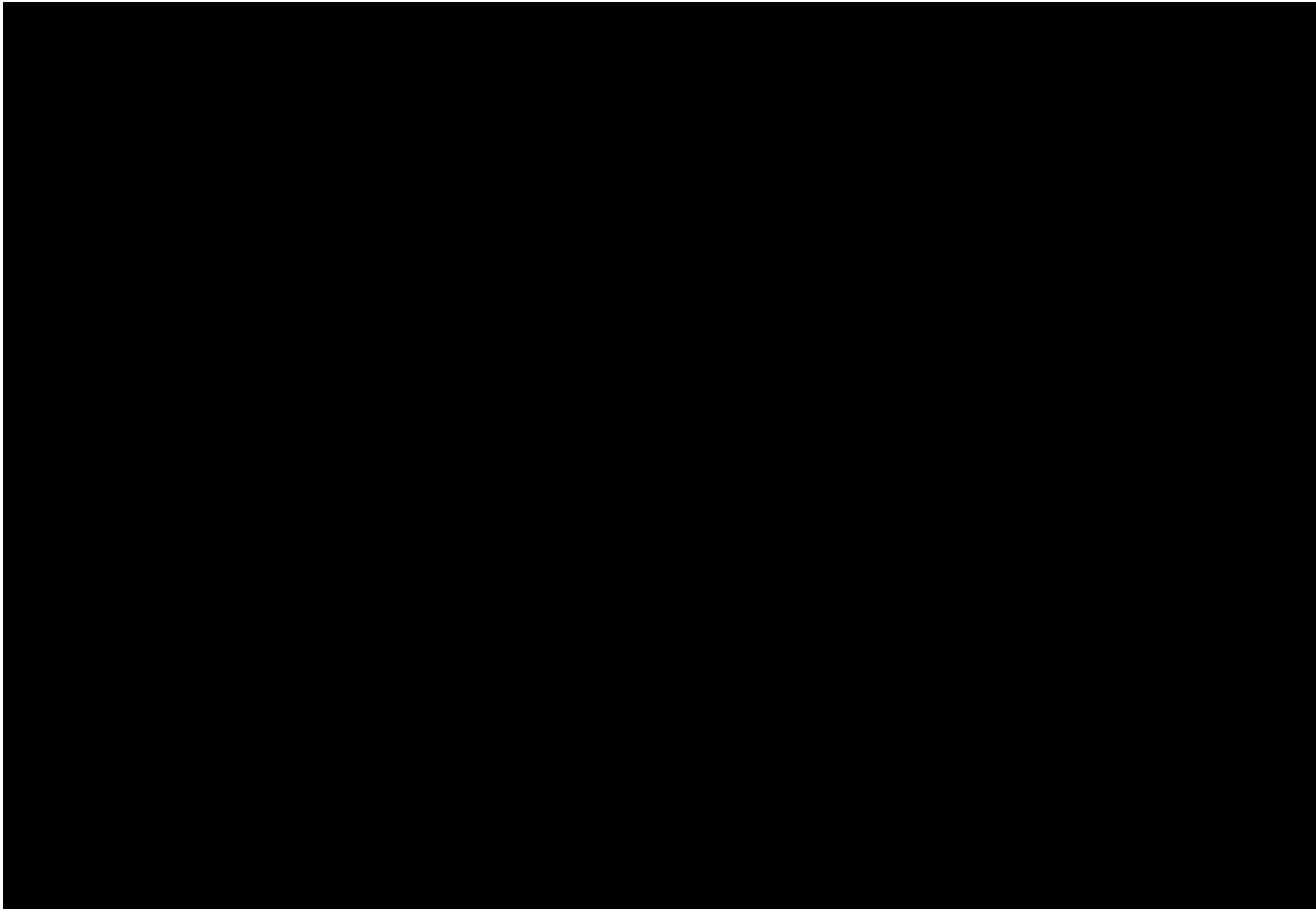


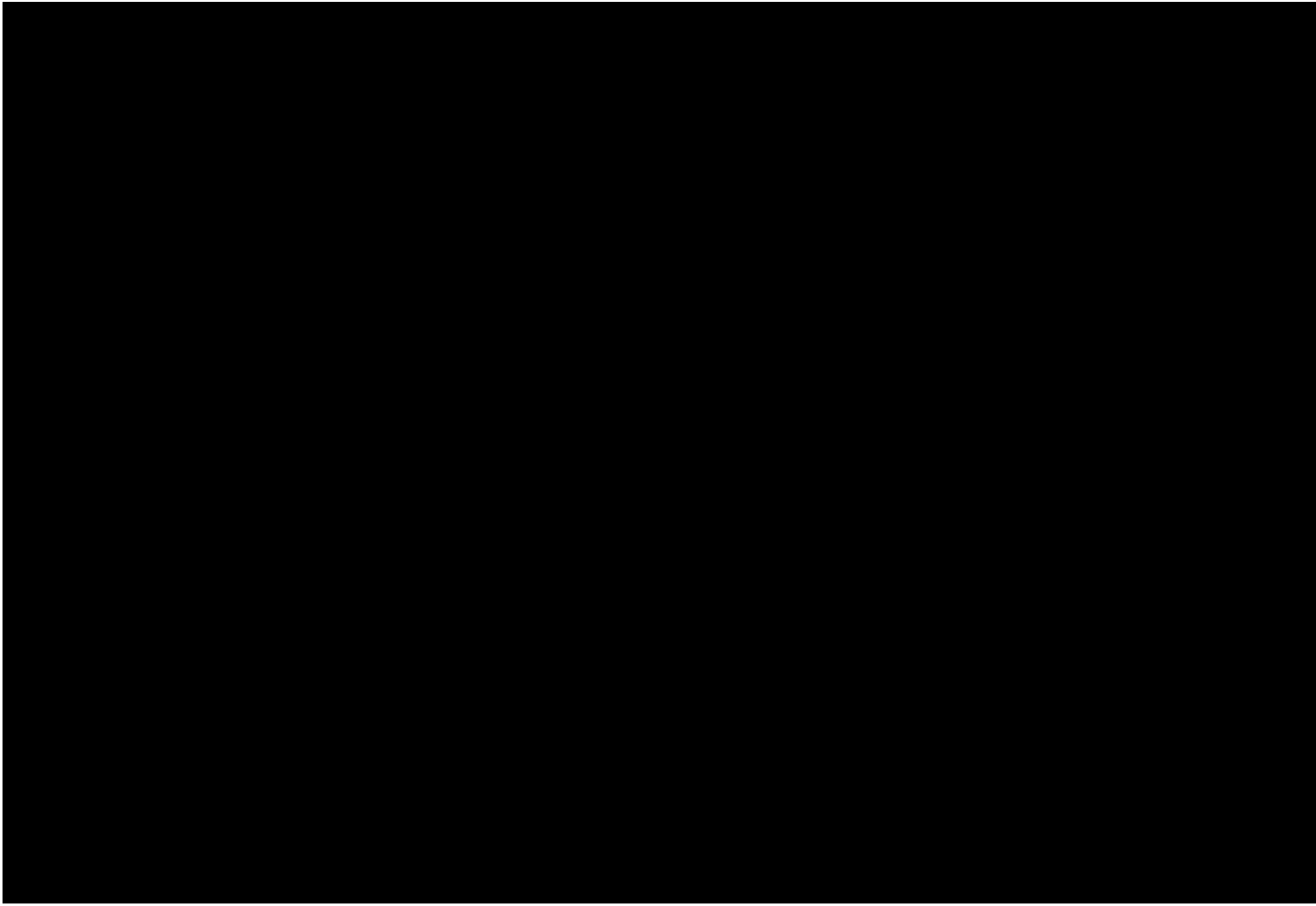


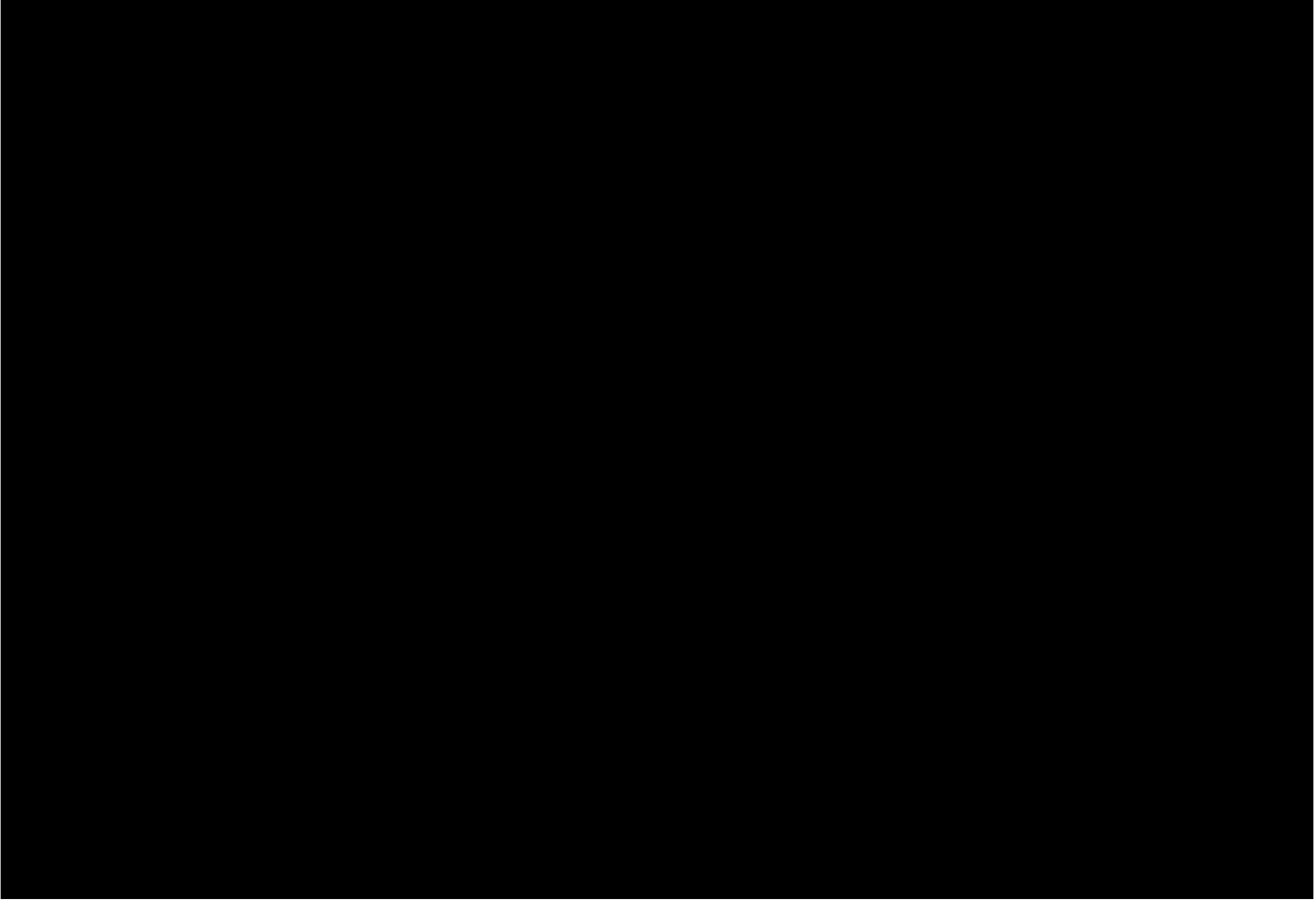


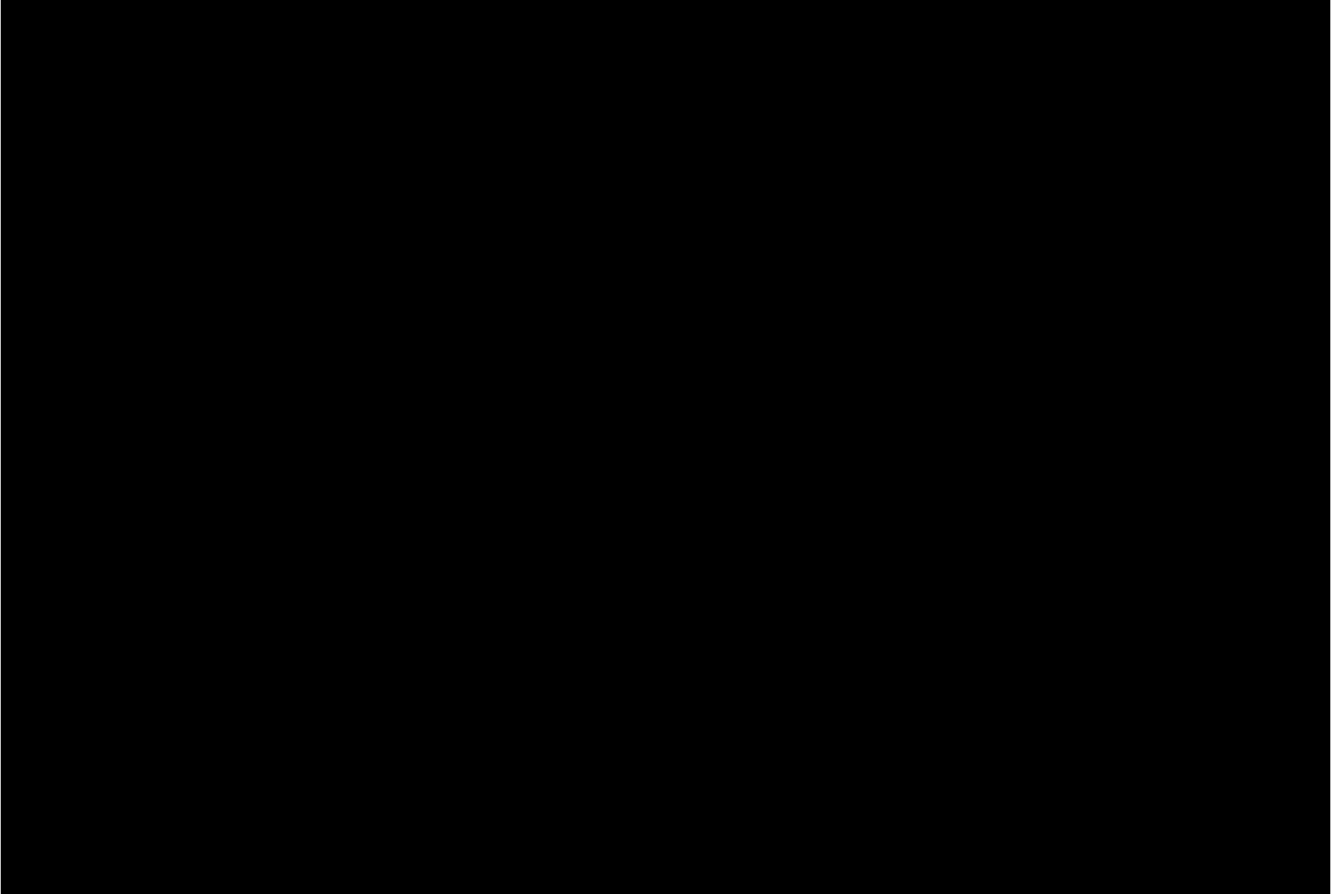


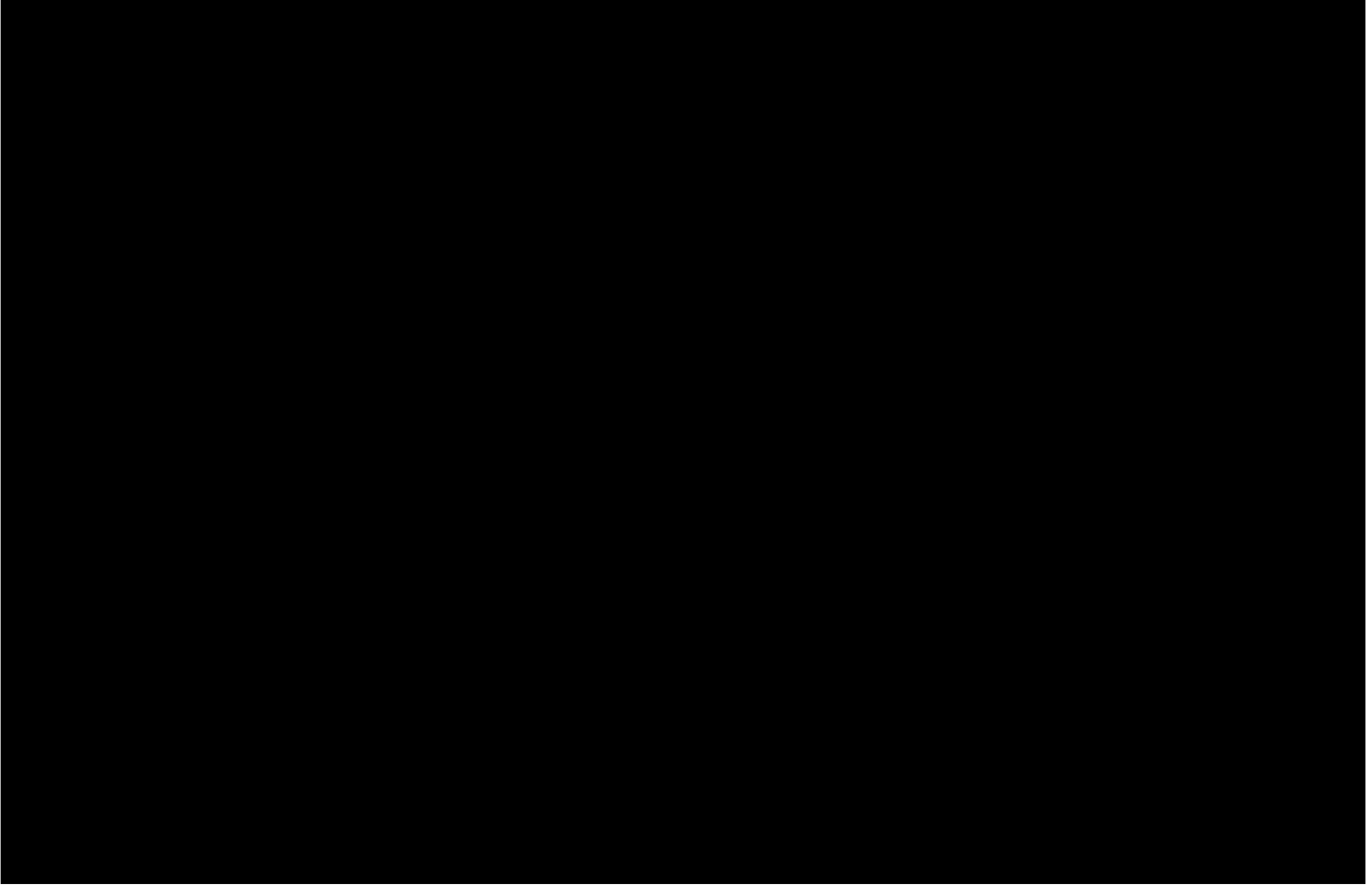


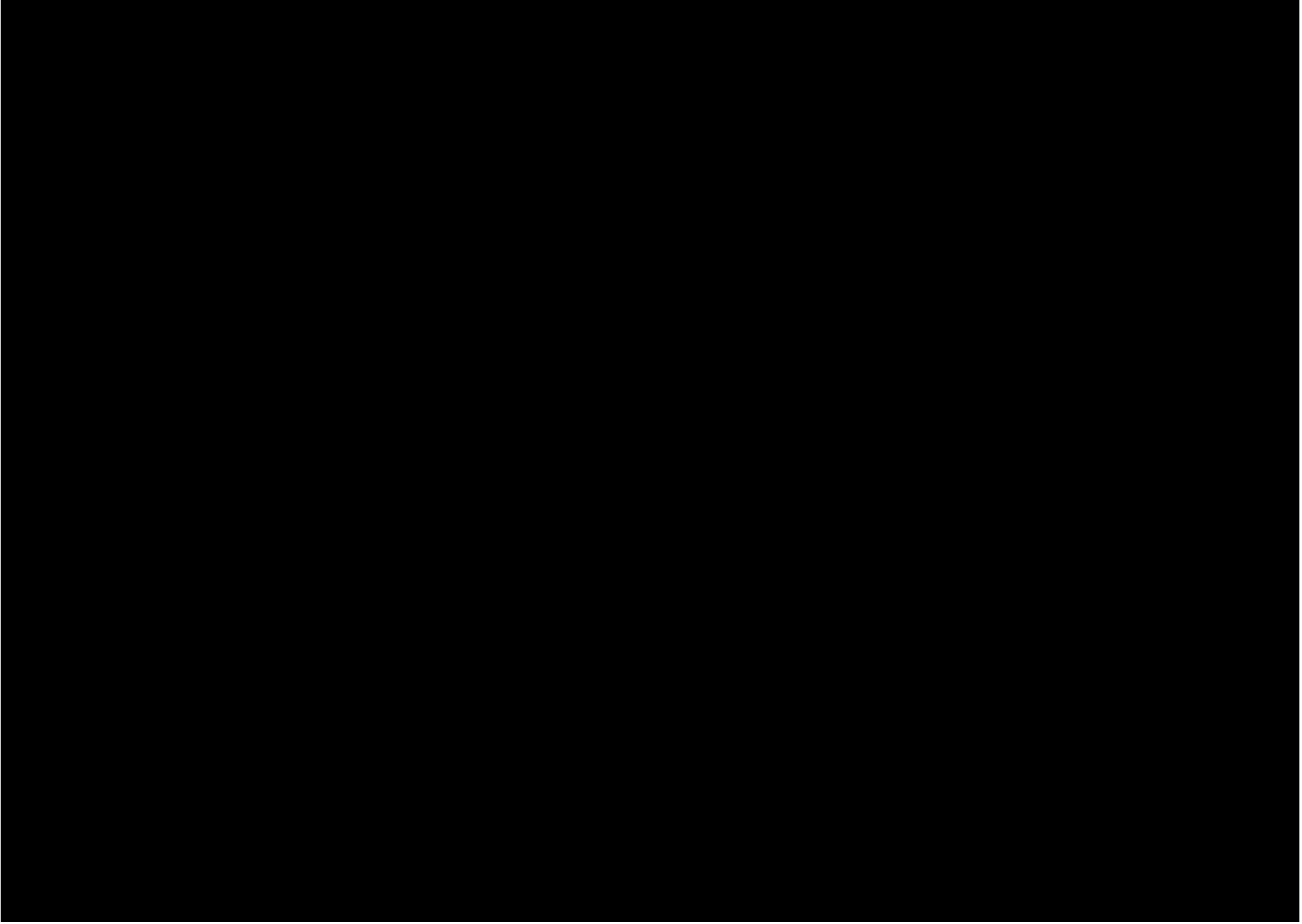


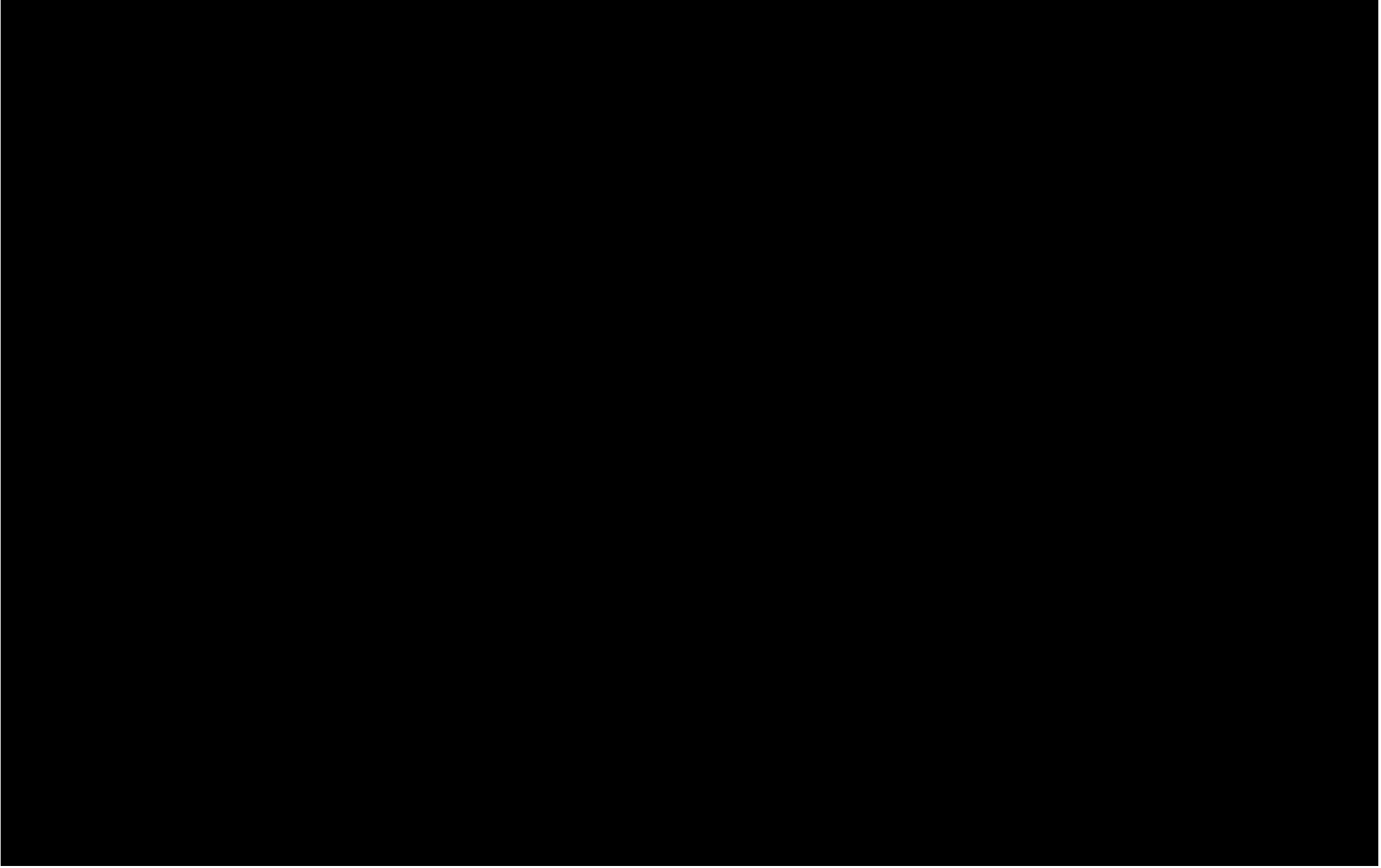


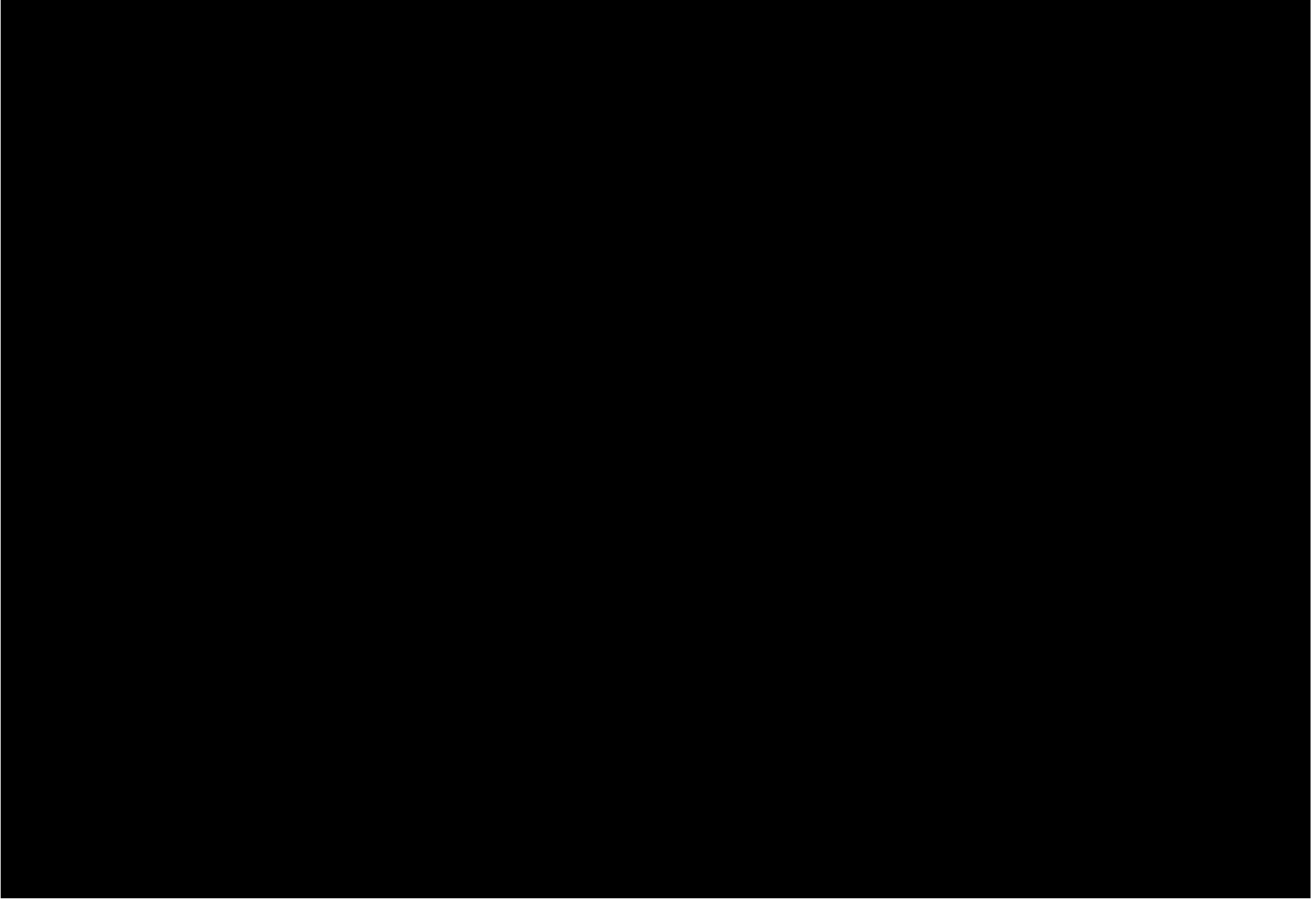


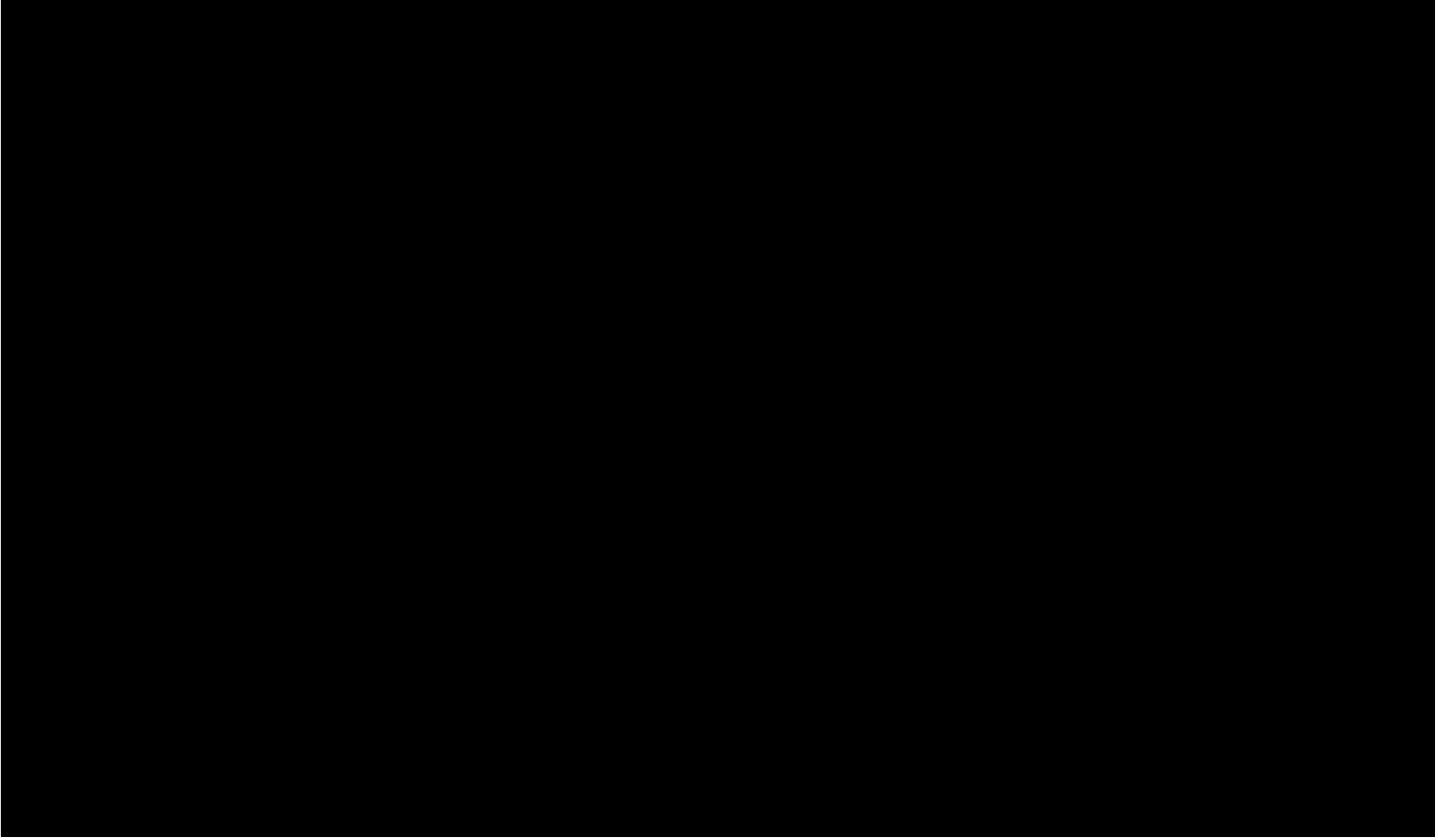


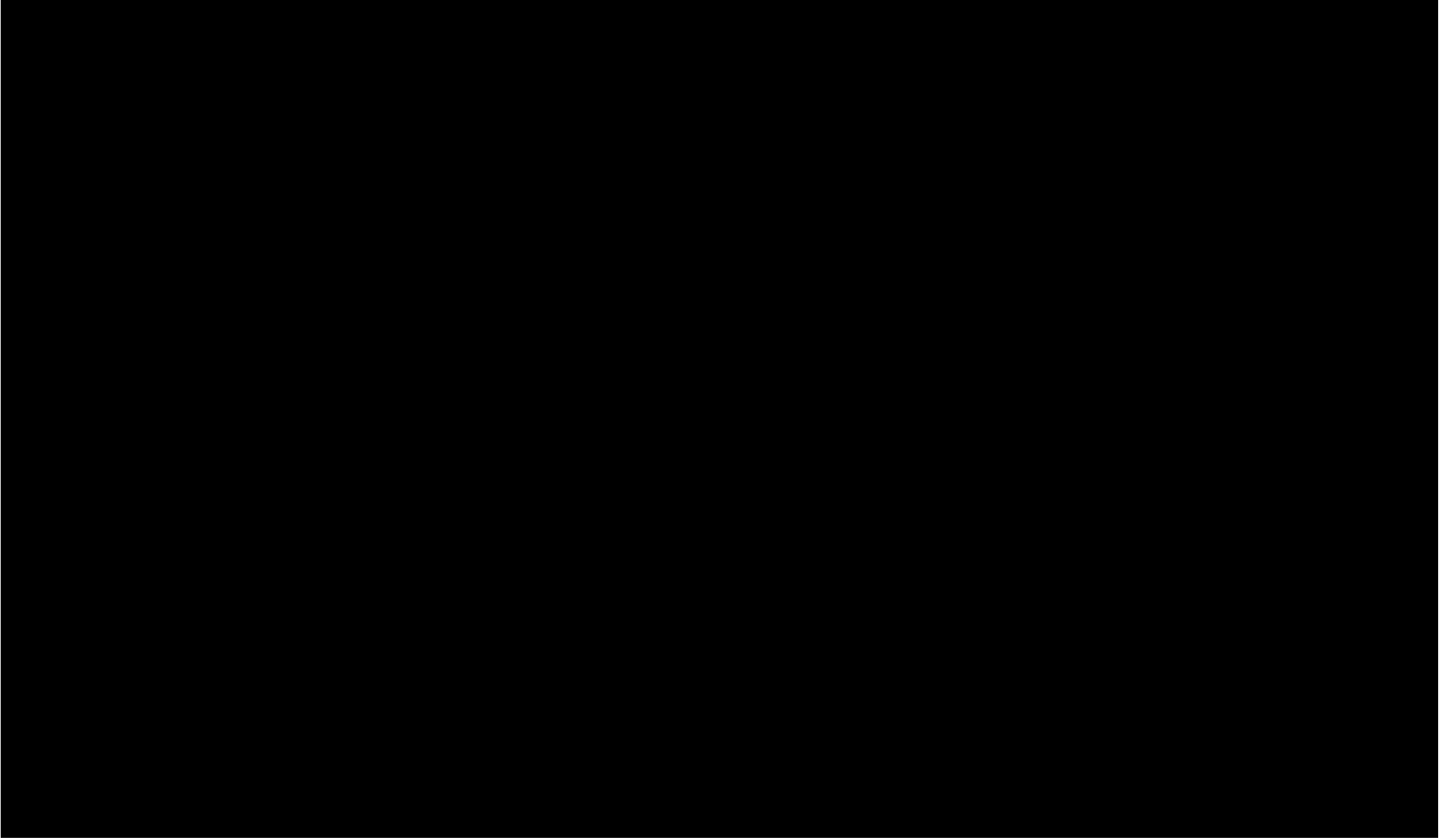


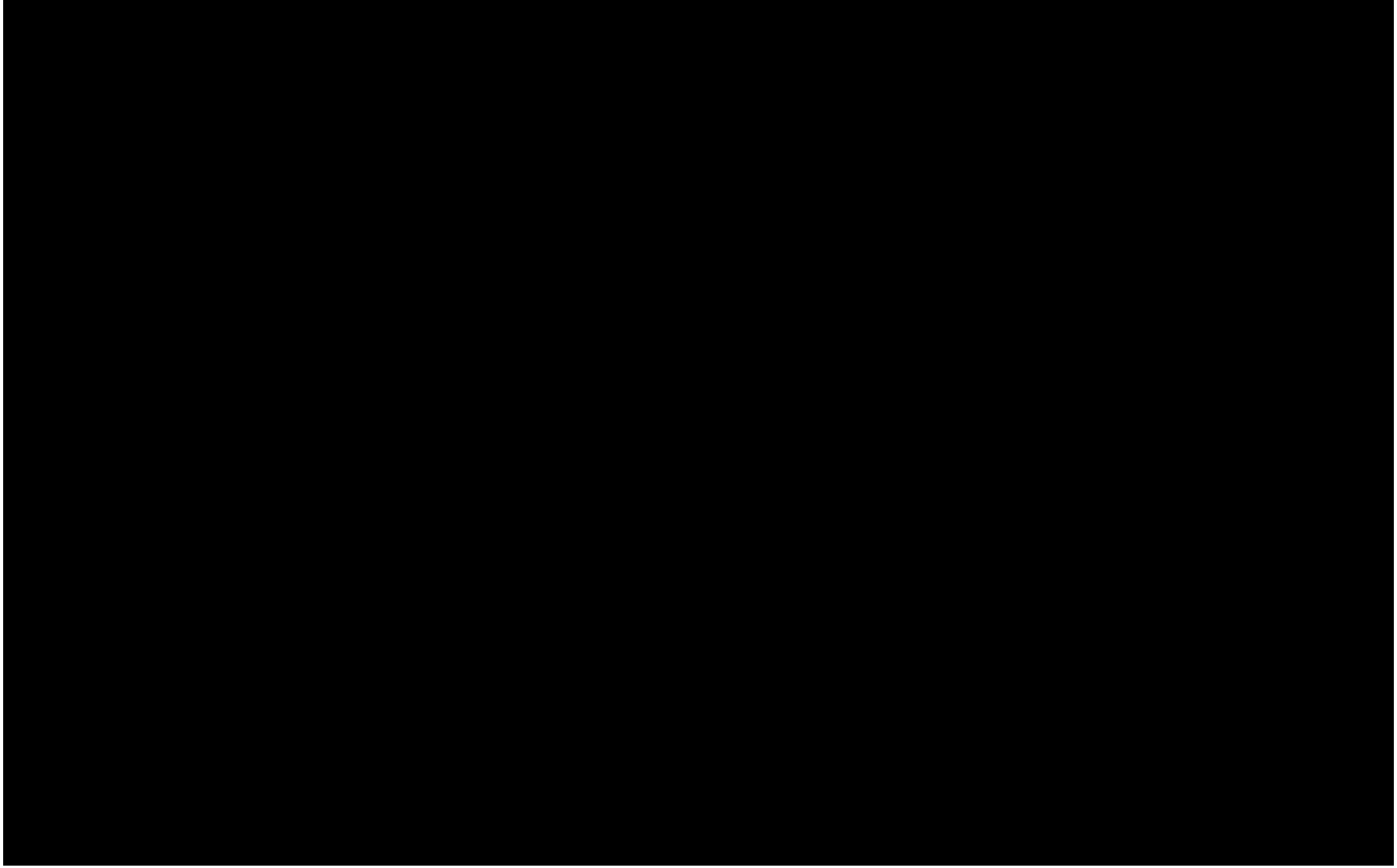


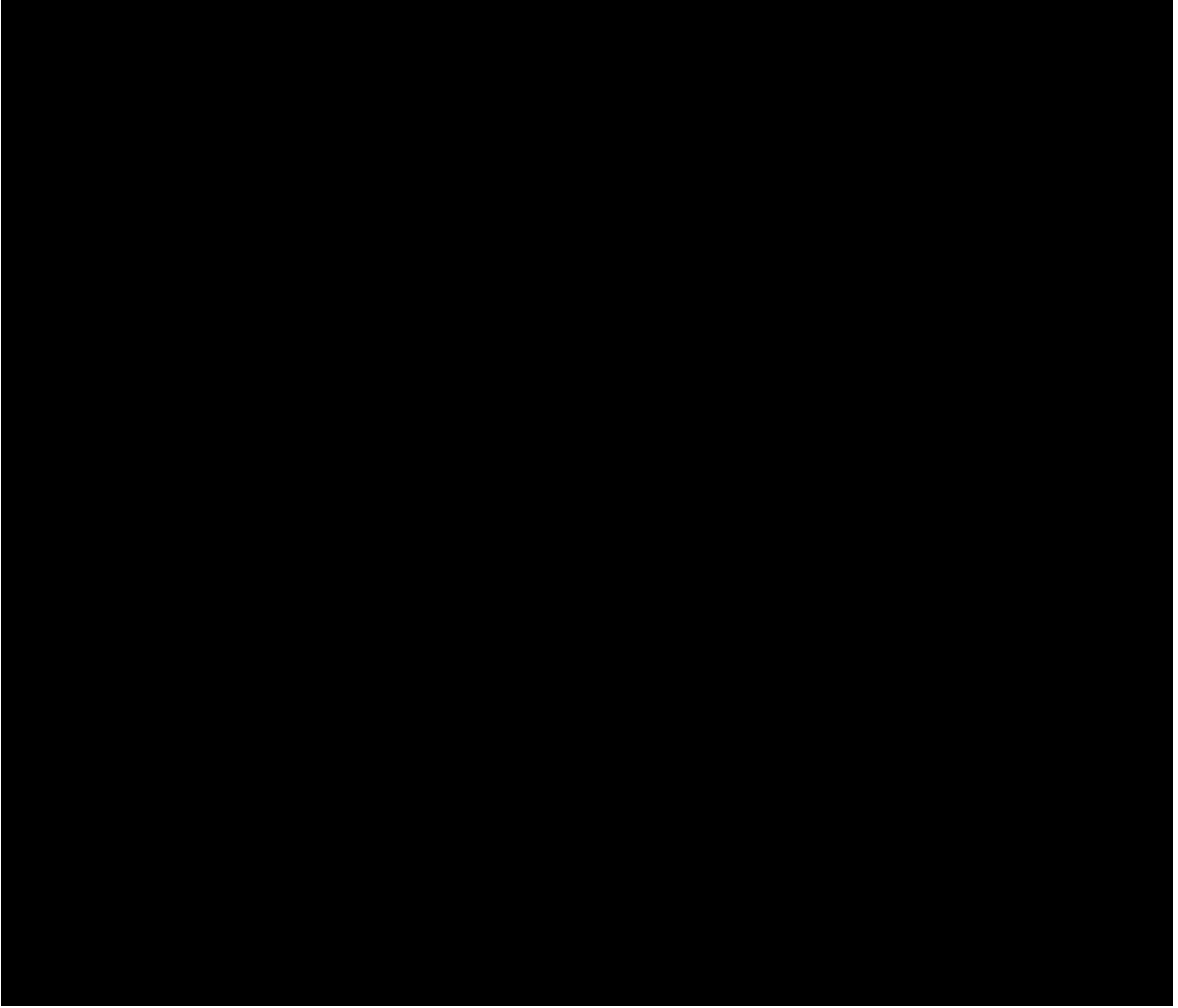


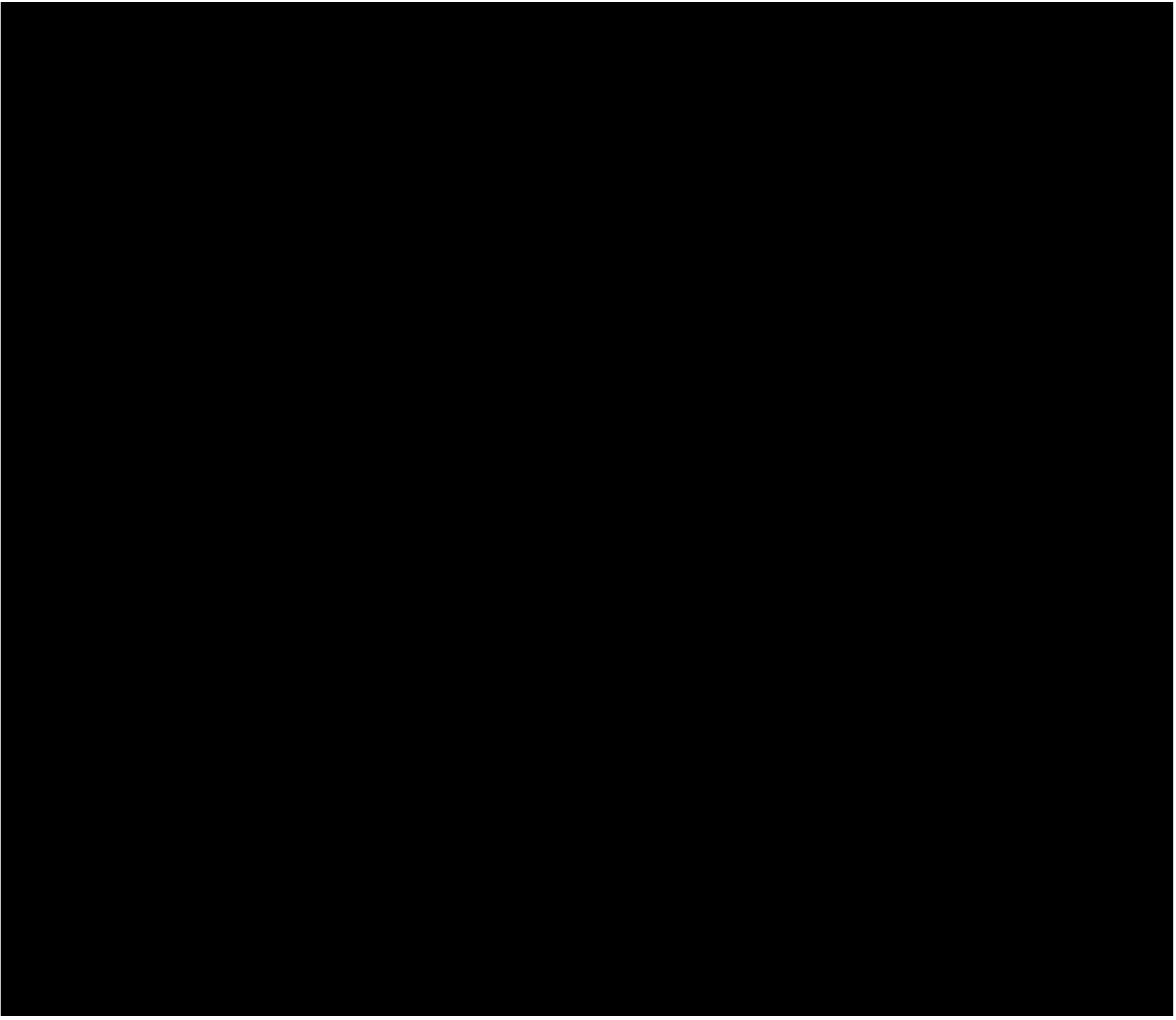




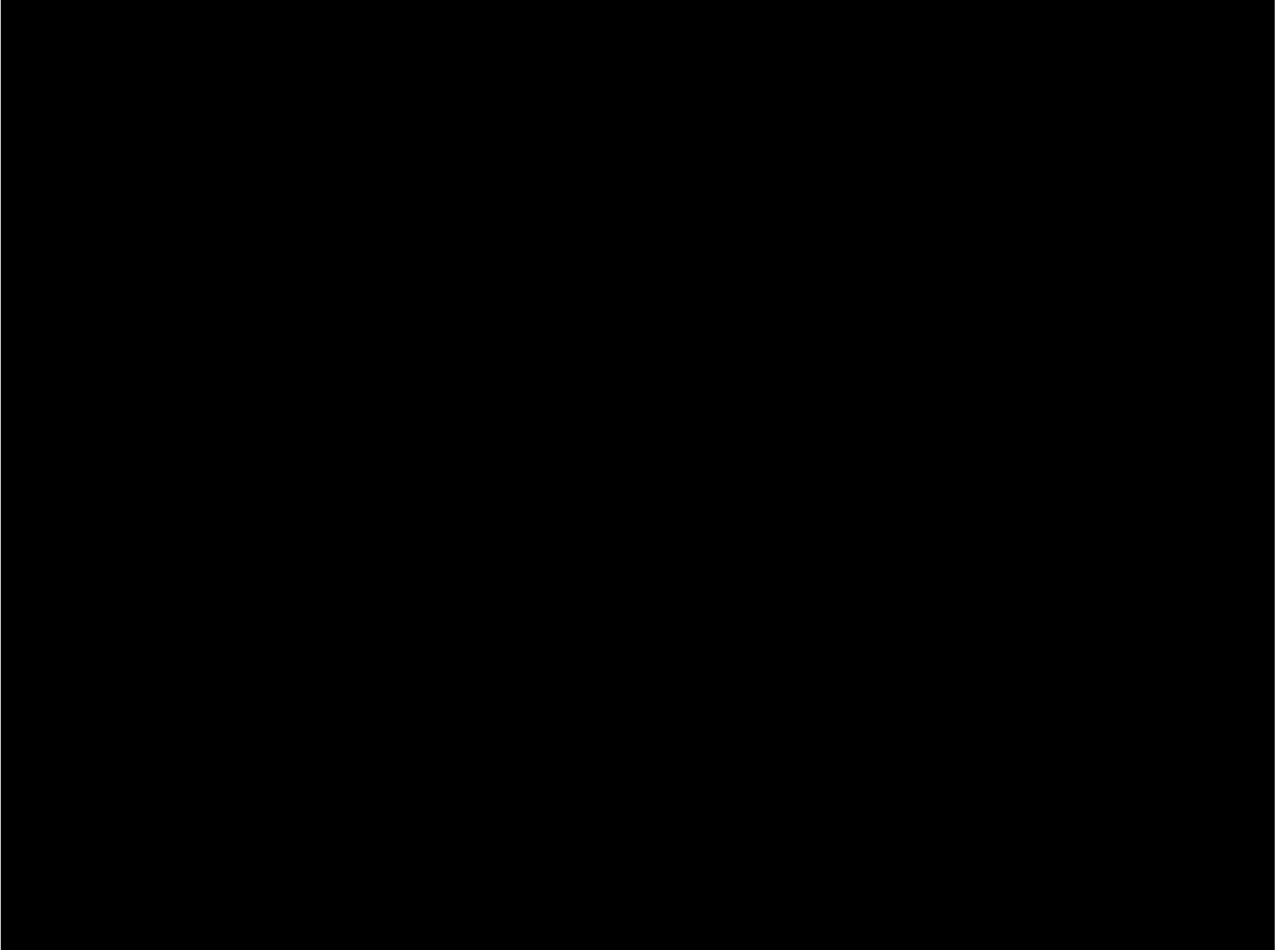


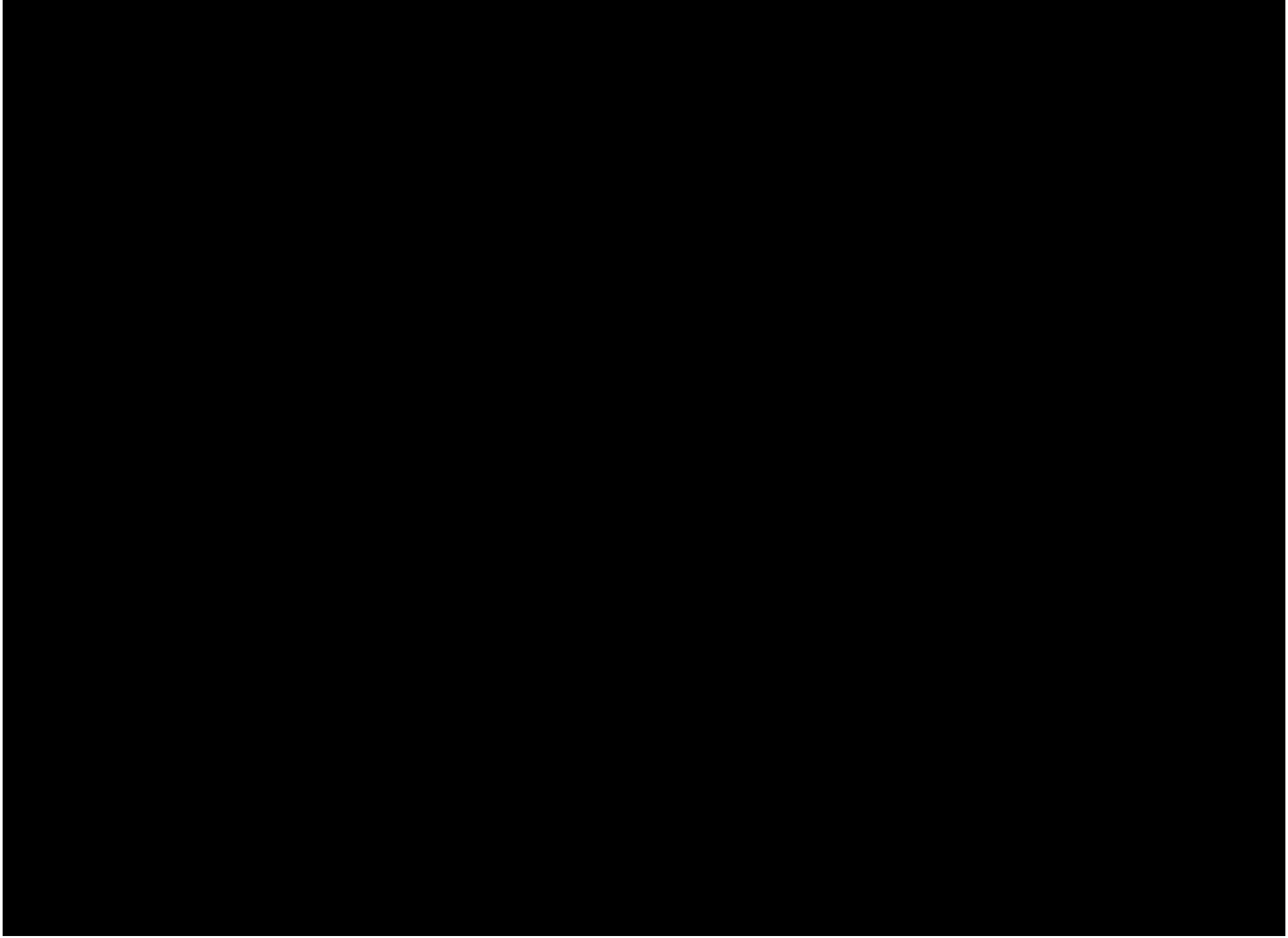


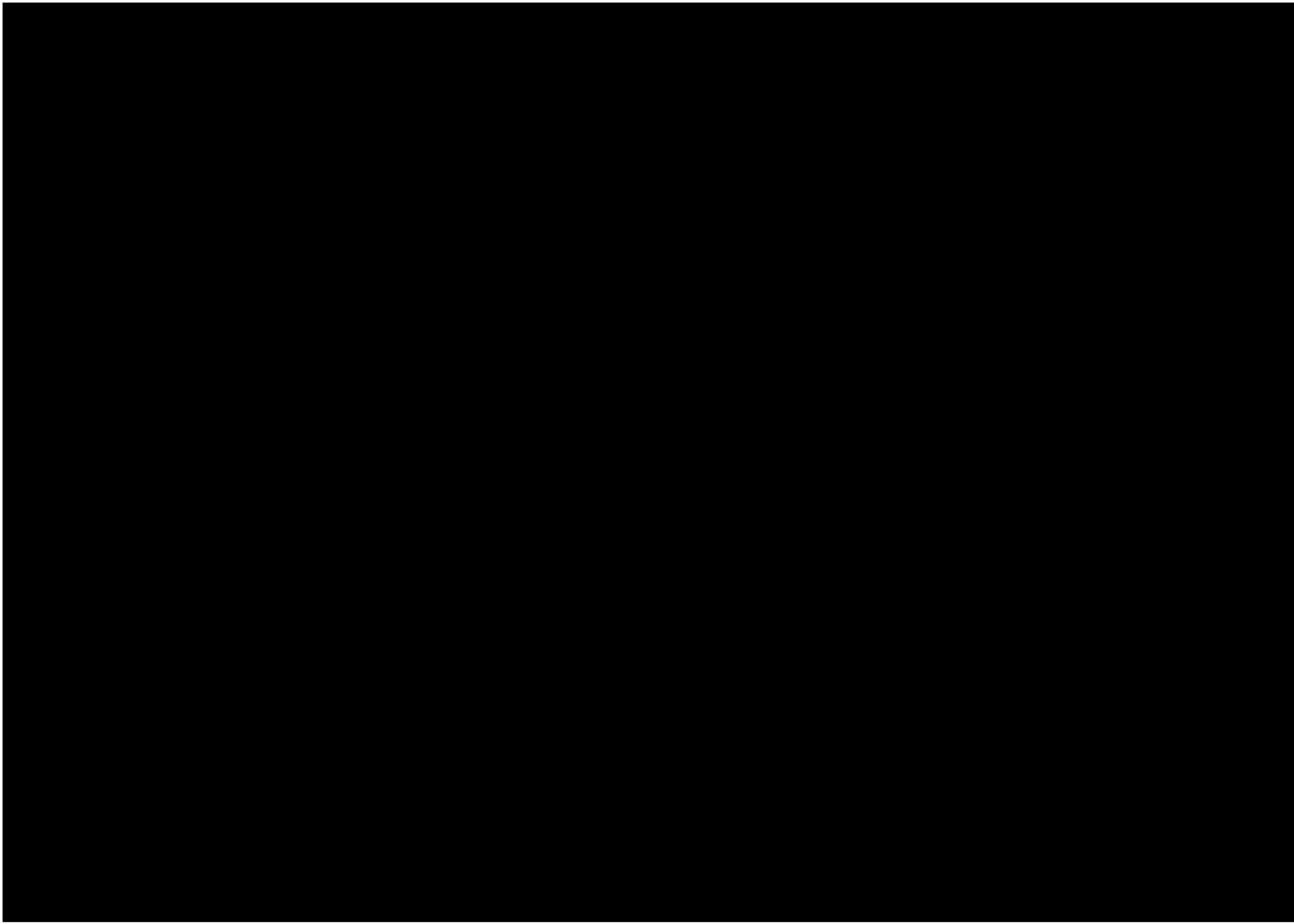


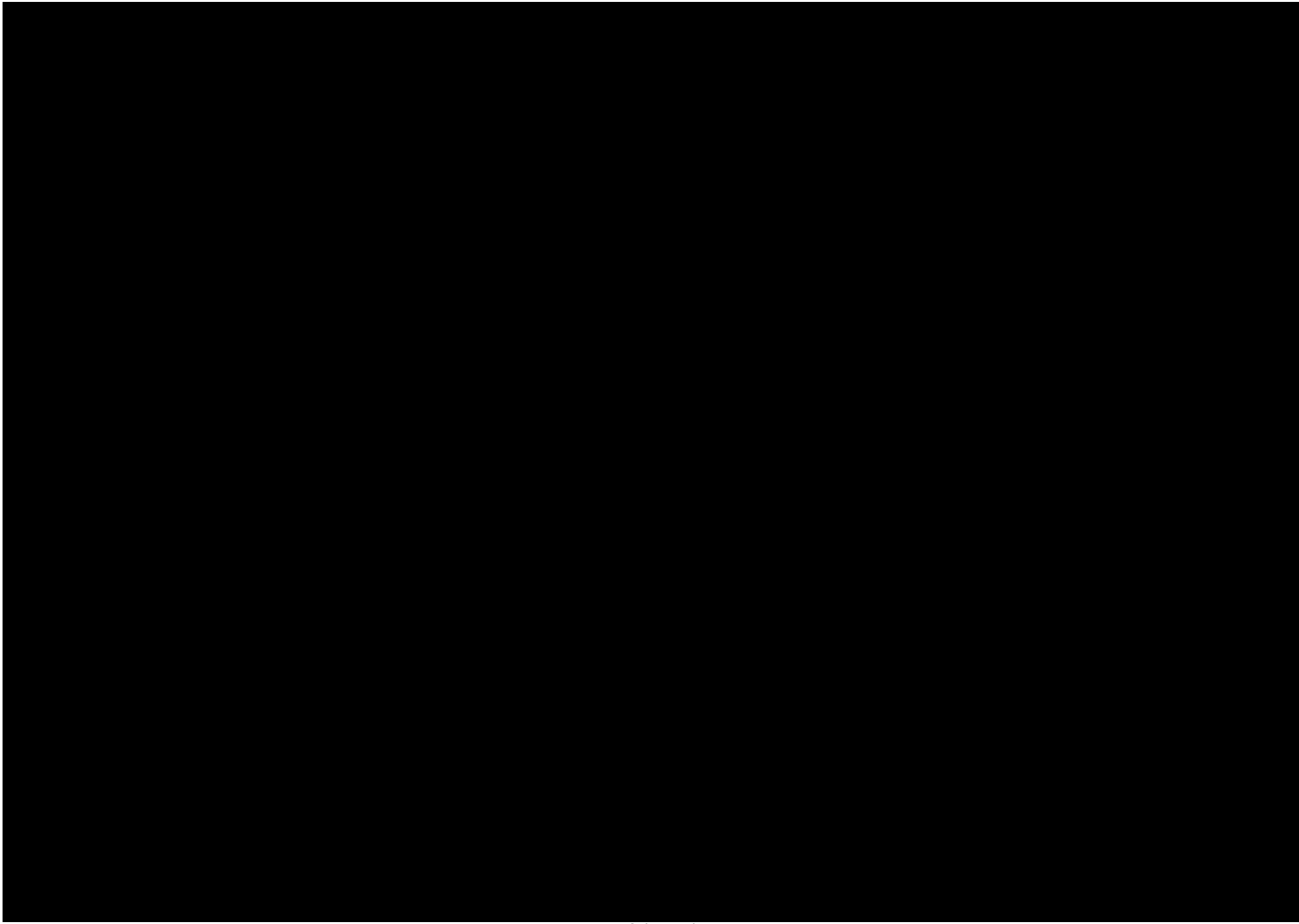


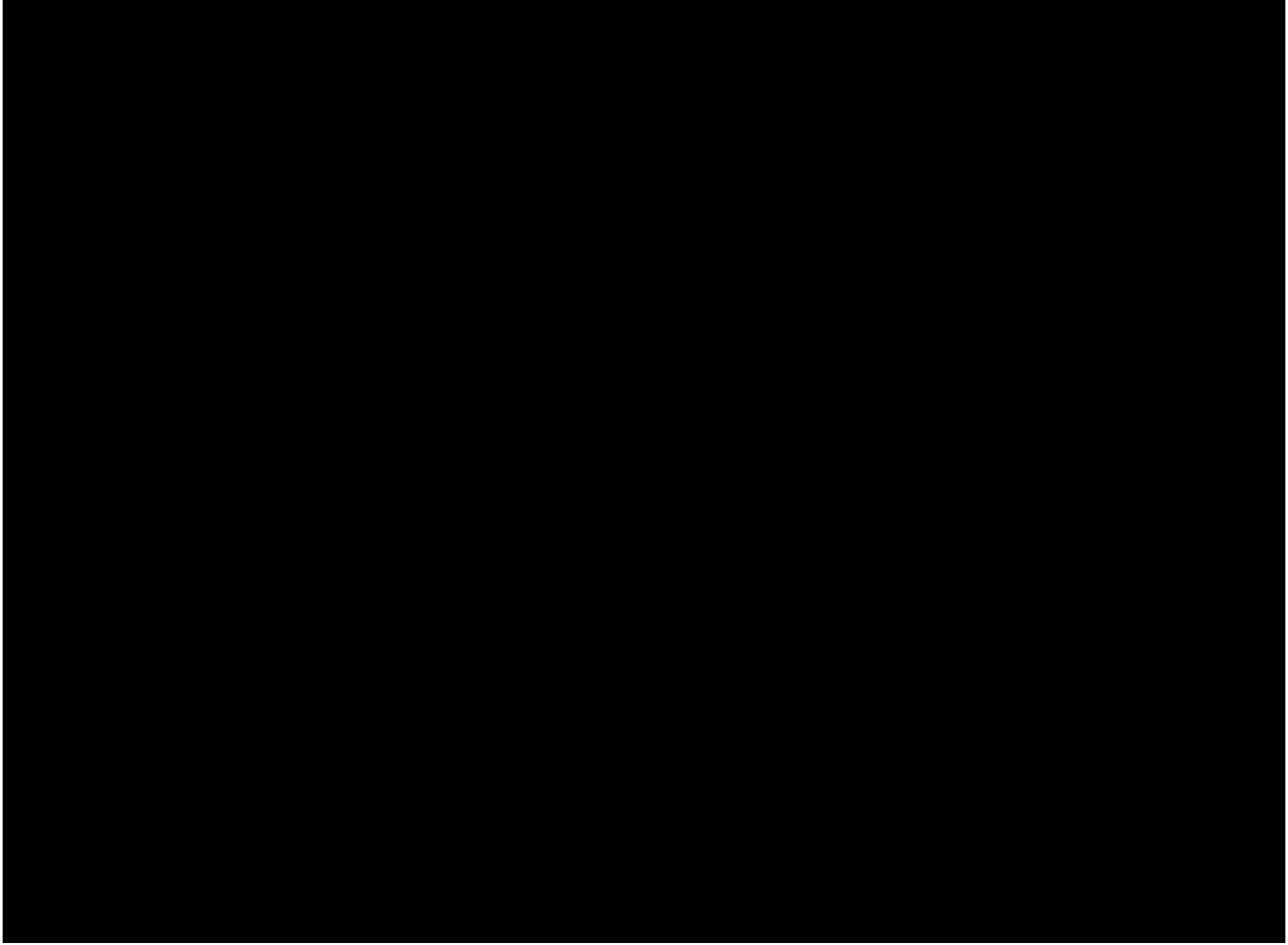
This document is for the sole purposes of managing and administering
the Data PowerHouse project for the Commonwealth of Pennsylvania

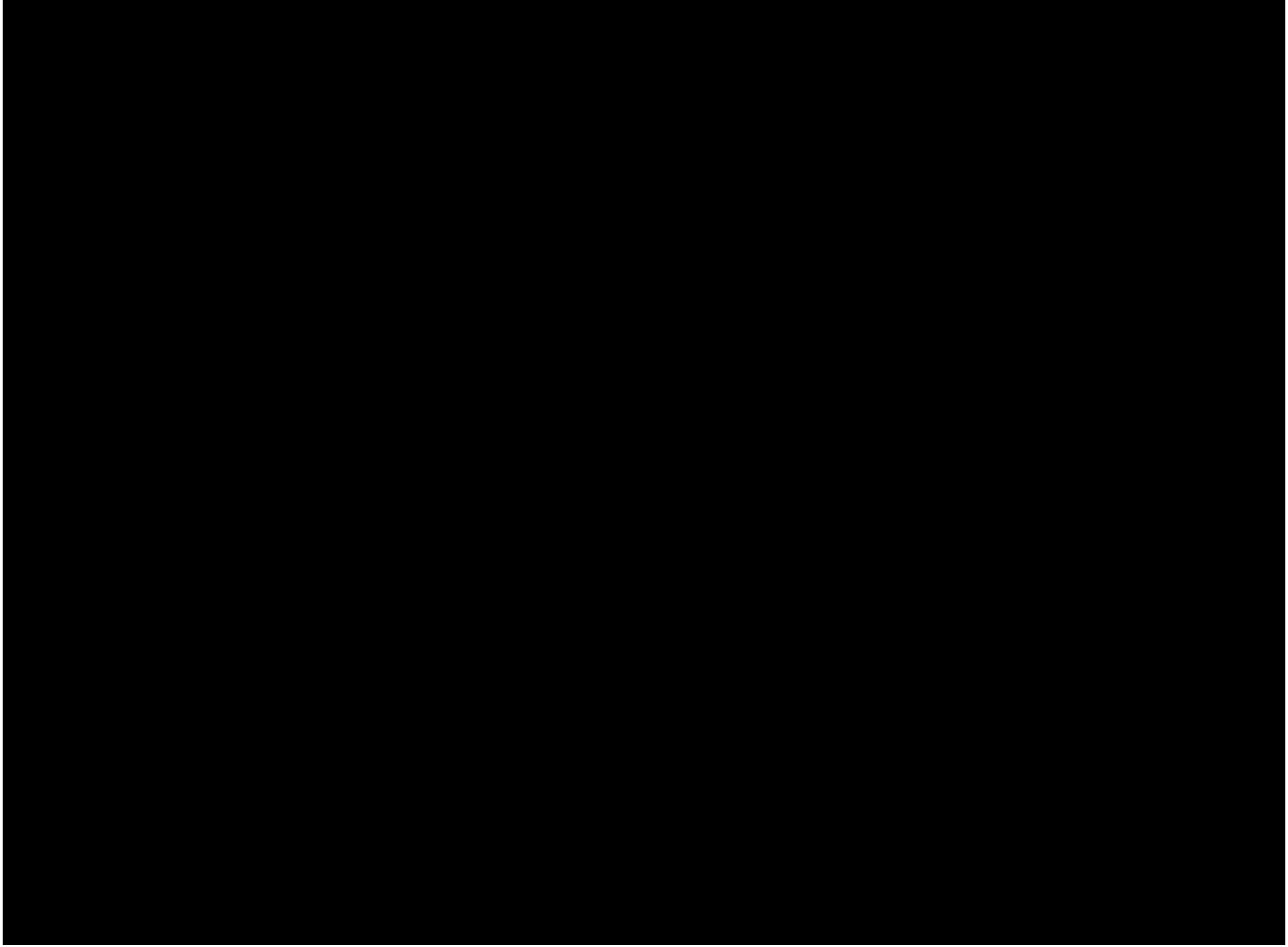


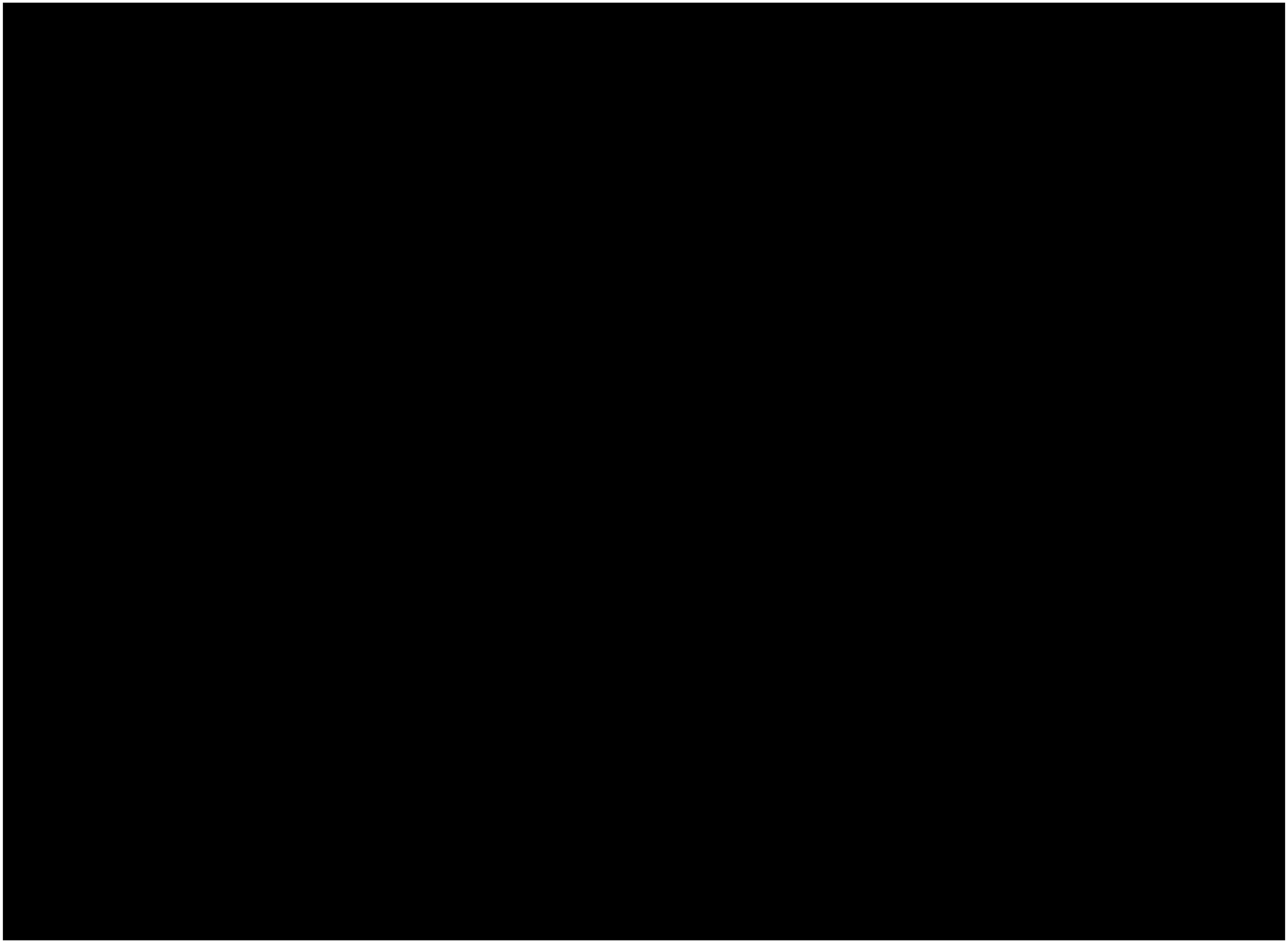


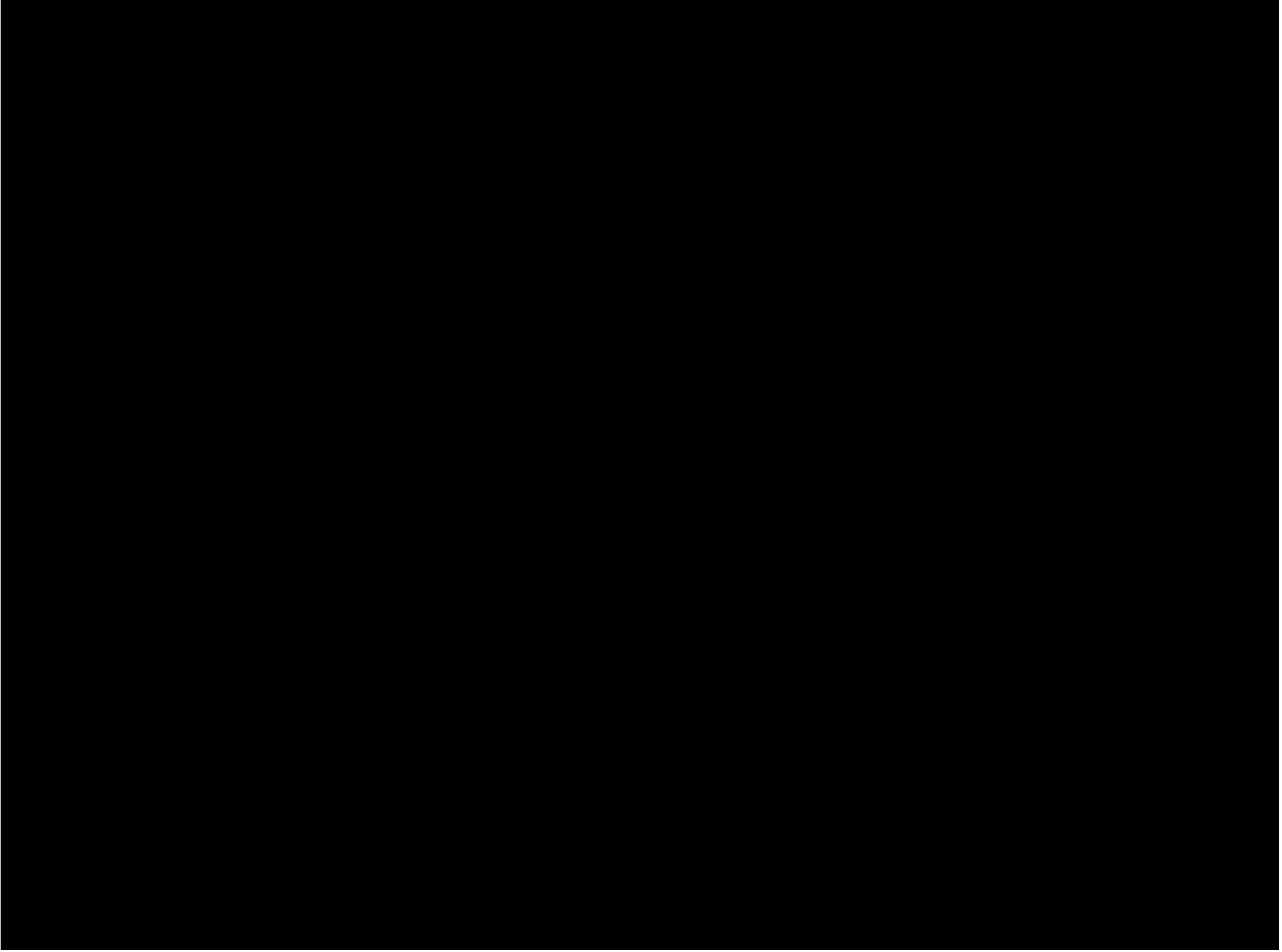


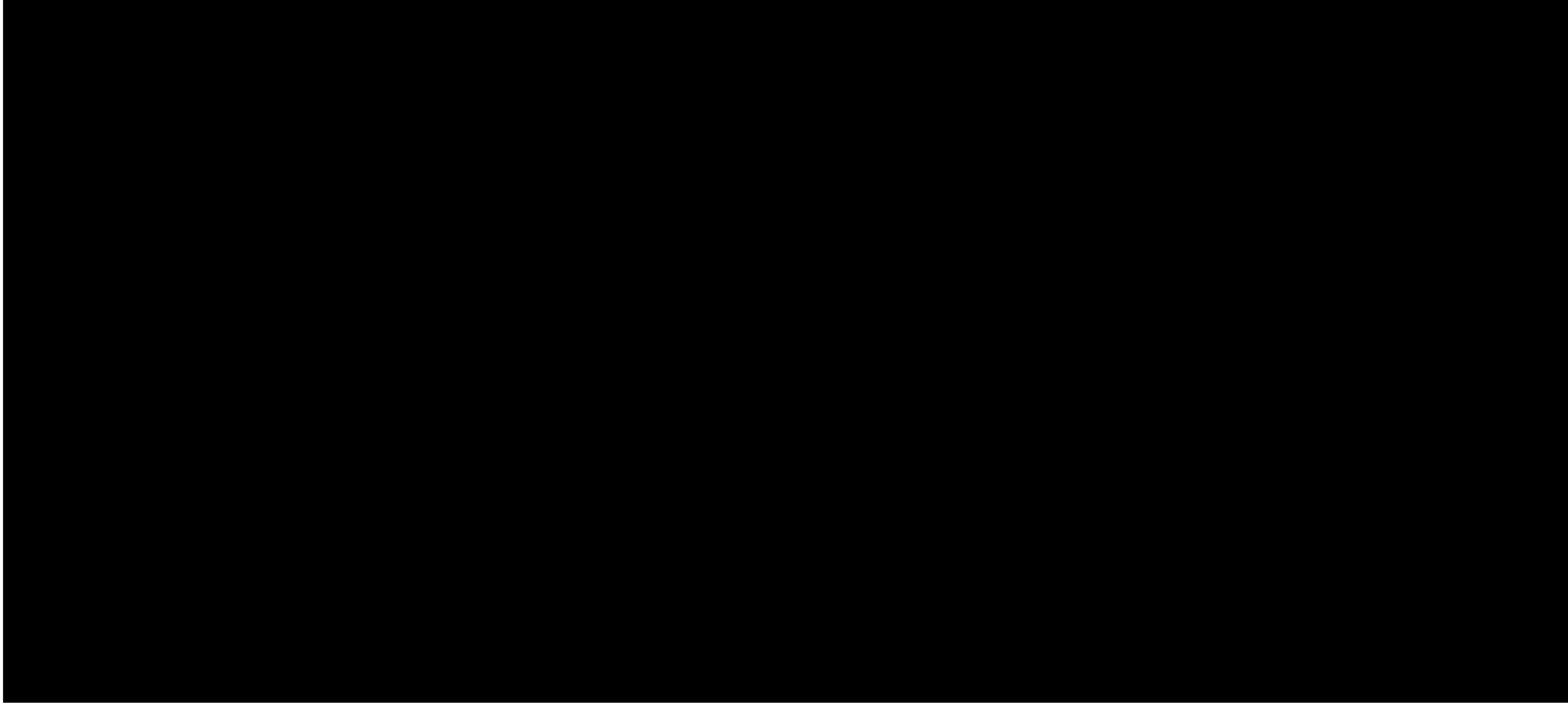


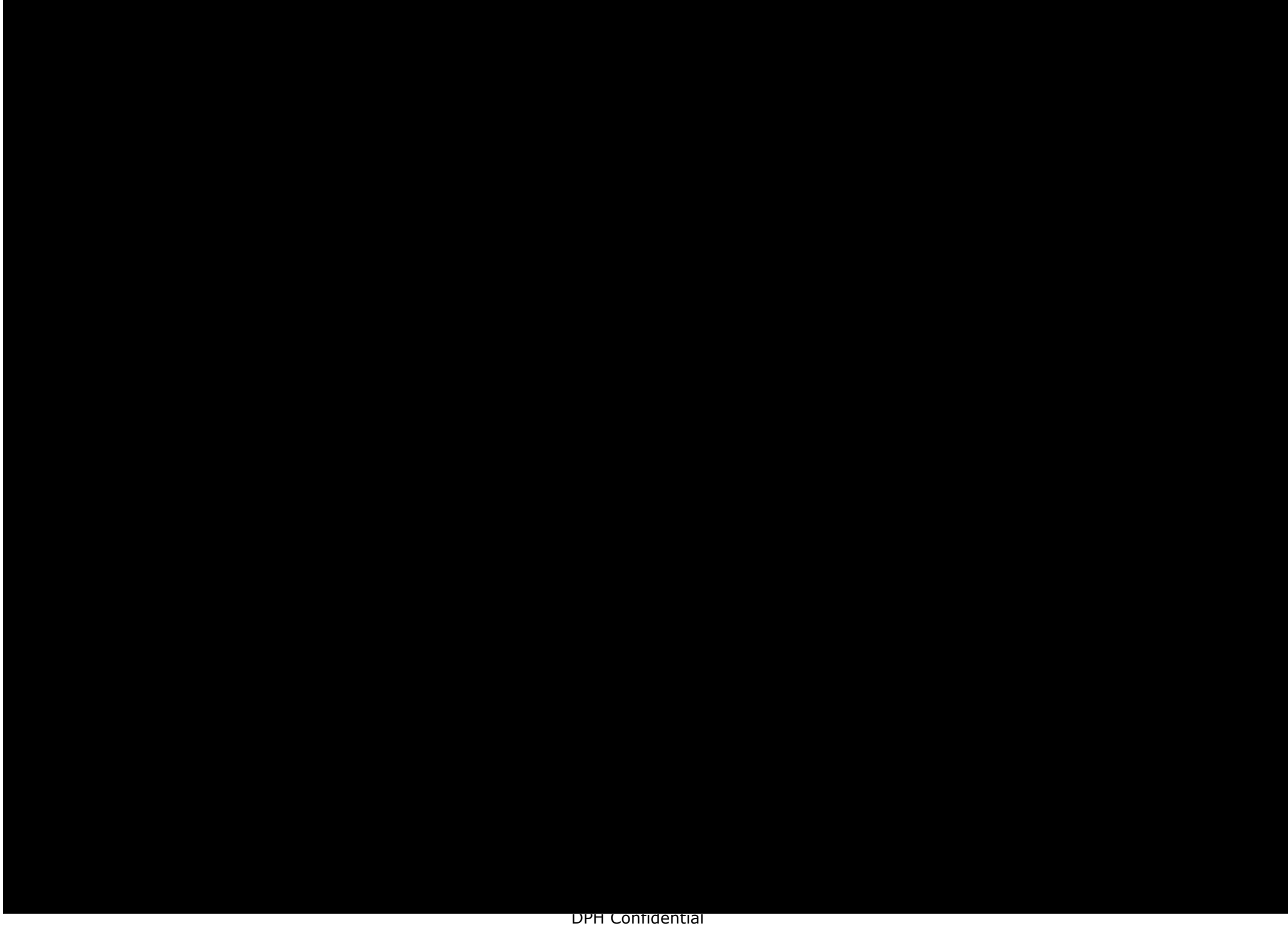












Attachment F-3 – AMOS Enterprise Architecture Project SOW

This attachment shows a sample architecture template document that is used to guide Unisys architects in the design of infrastructure architecture. **Please note this attachment should be redacted for public view.**

This page intentionally left blank.

Application Modernization and Outsourcing (AMOS) Enterprise Architecture Project Statement of Work

Authorized for issue by:

	Signature	**Date**
	Signature	**Date**

June 17, 2013

Document No. xxx.v1.0

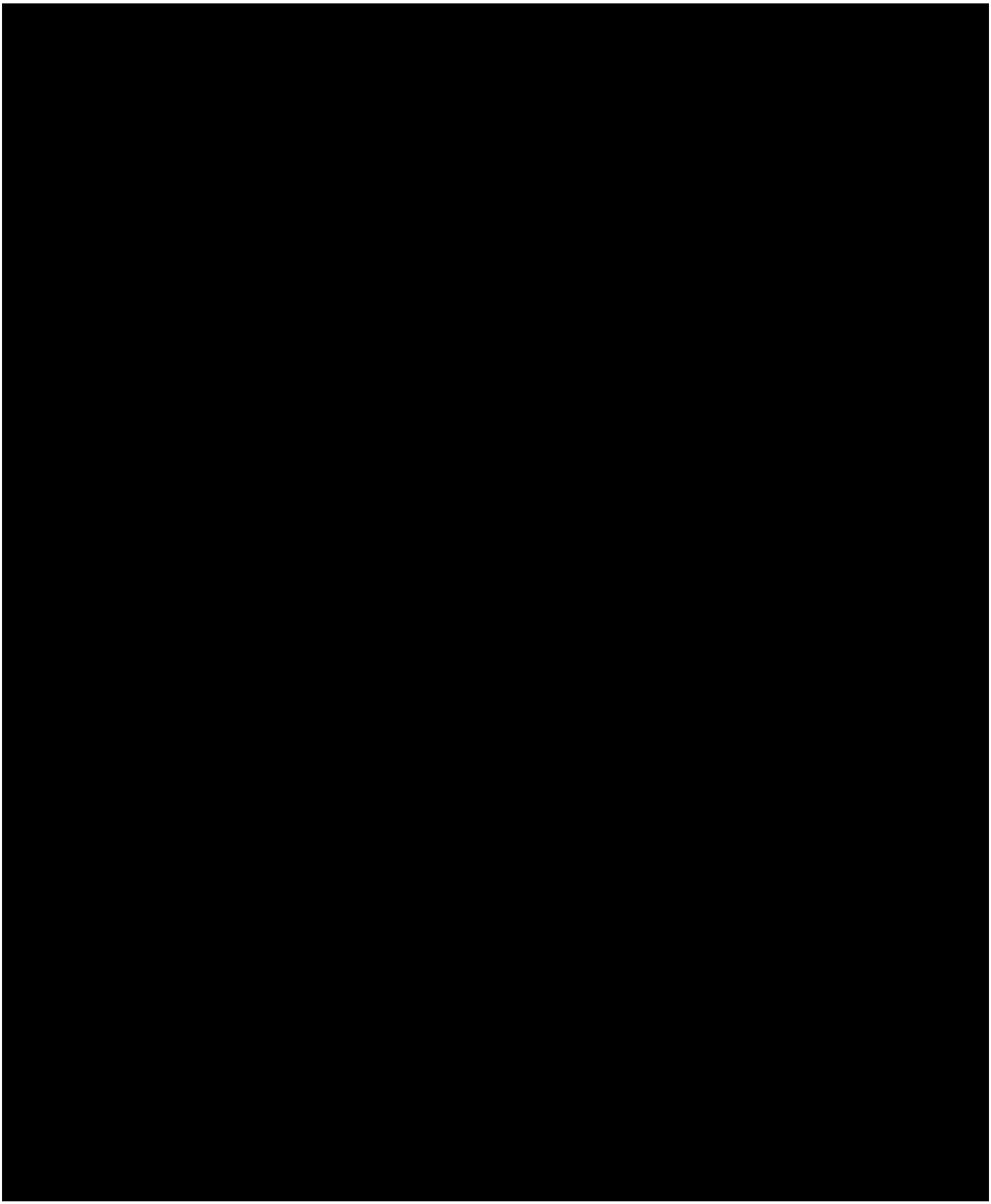
Copyright © 2009 Unisys Corporation
All rights reserved

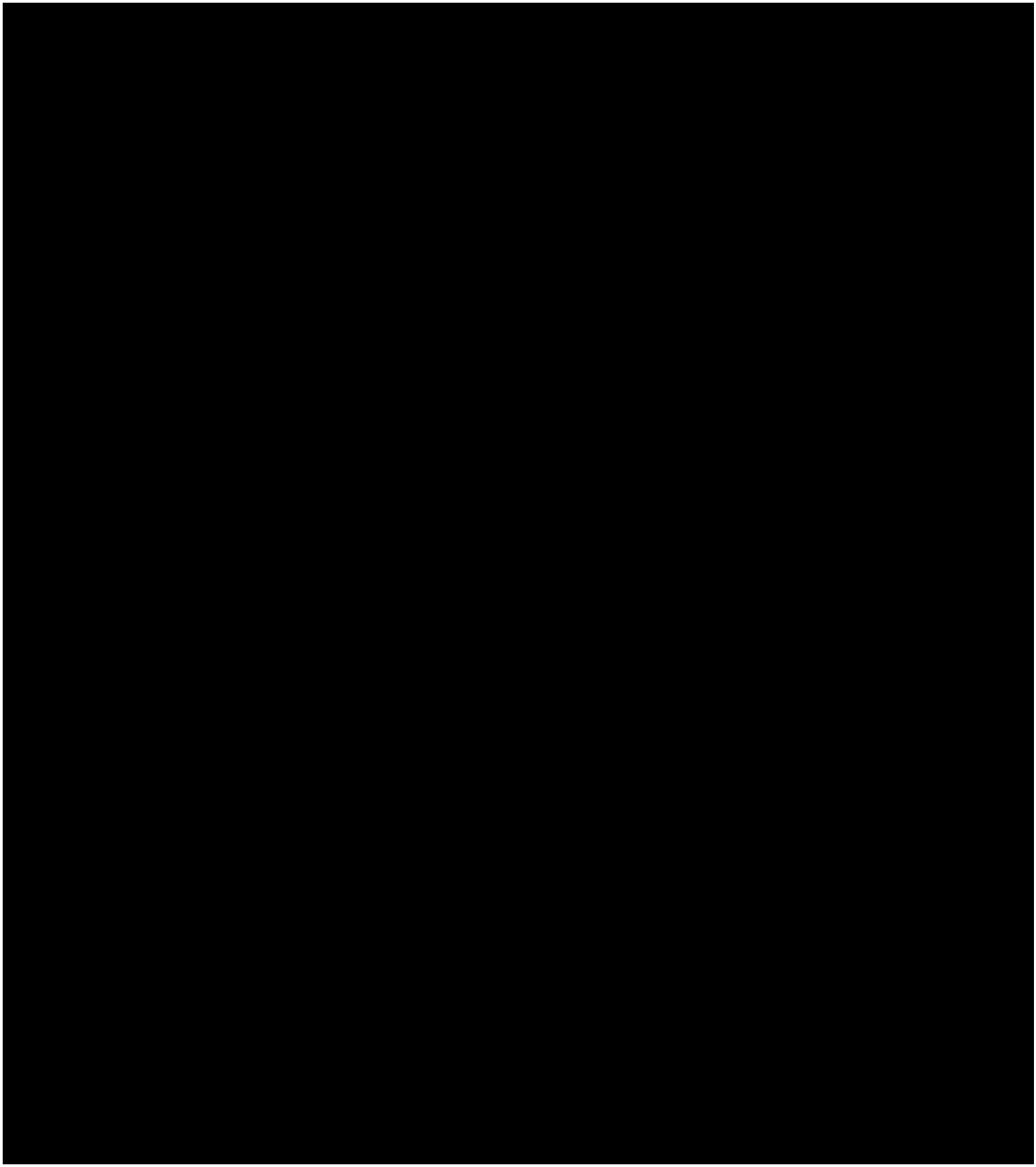
Revision History

Version	Date	Author	Summary of Changes
1.00	8-19-2009	[redacted]	Initial Release

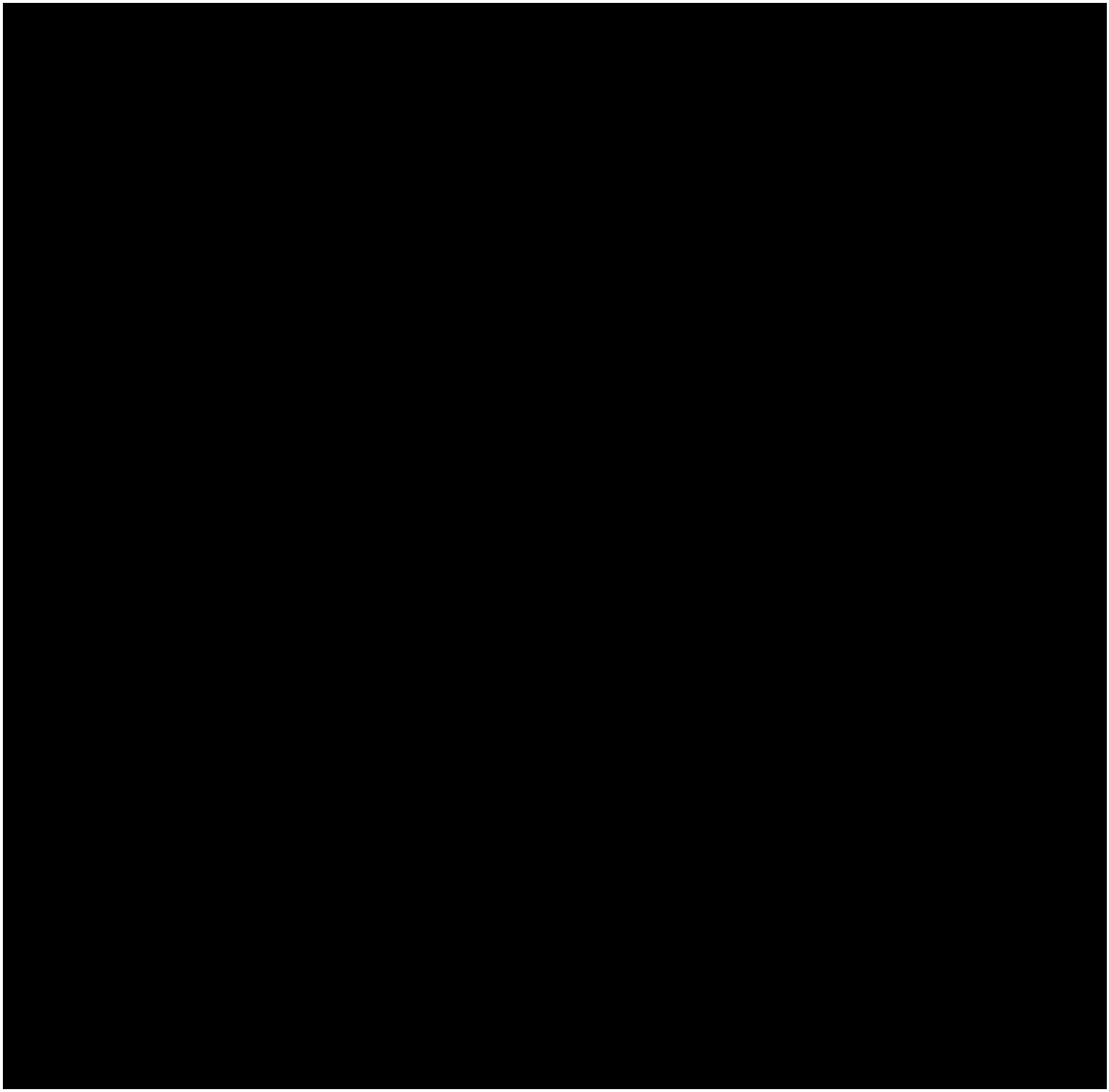
[redacted]

[redacted]

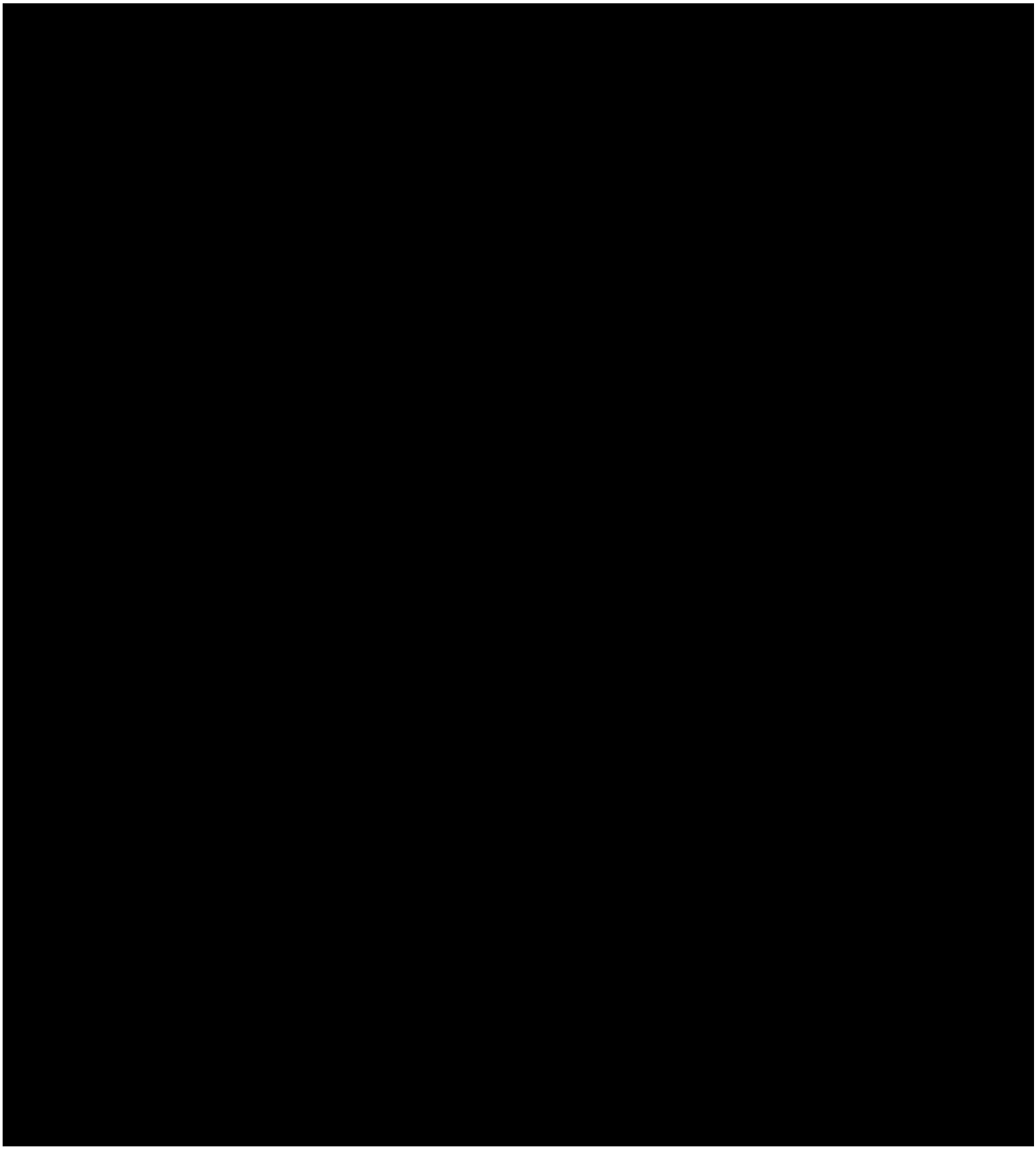




□ □ □□□□

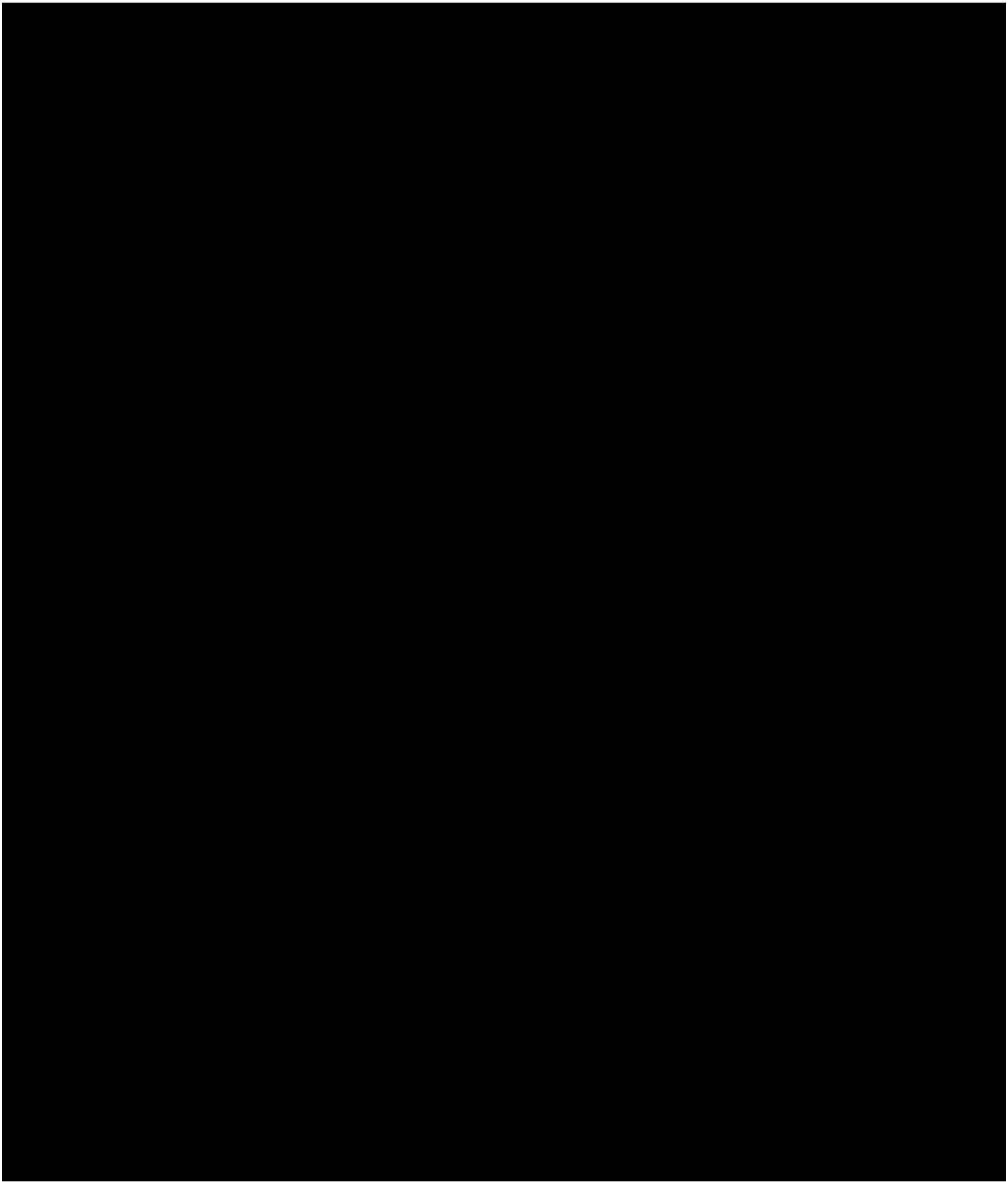


□ □ □□□□



□ □ □□□□

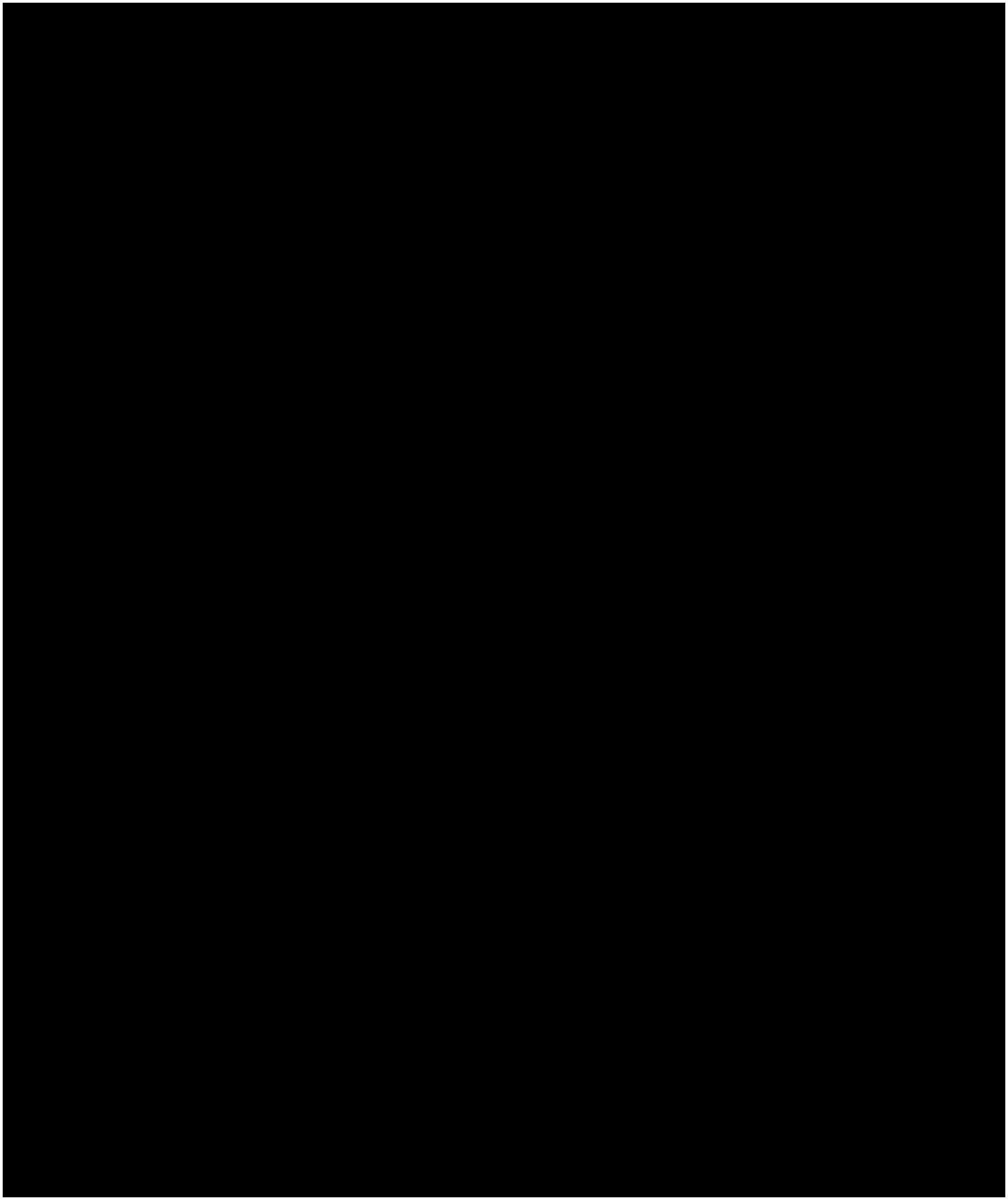
□ □ □□□□



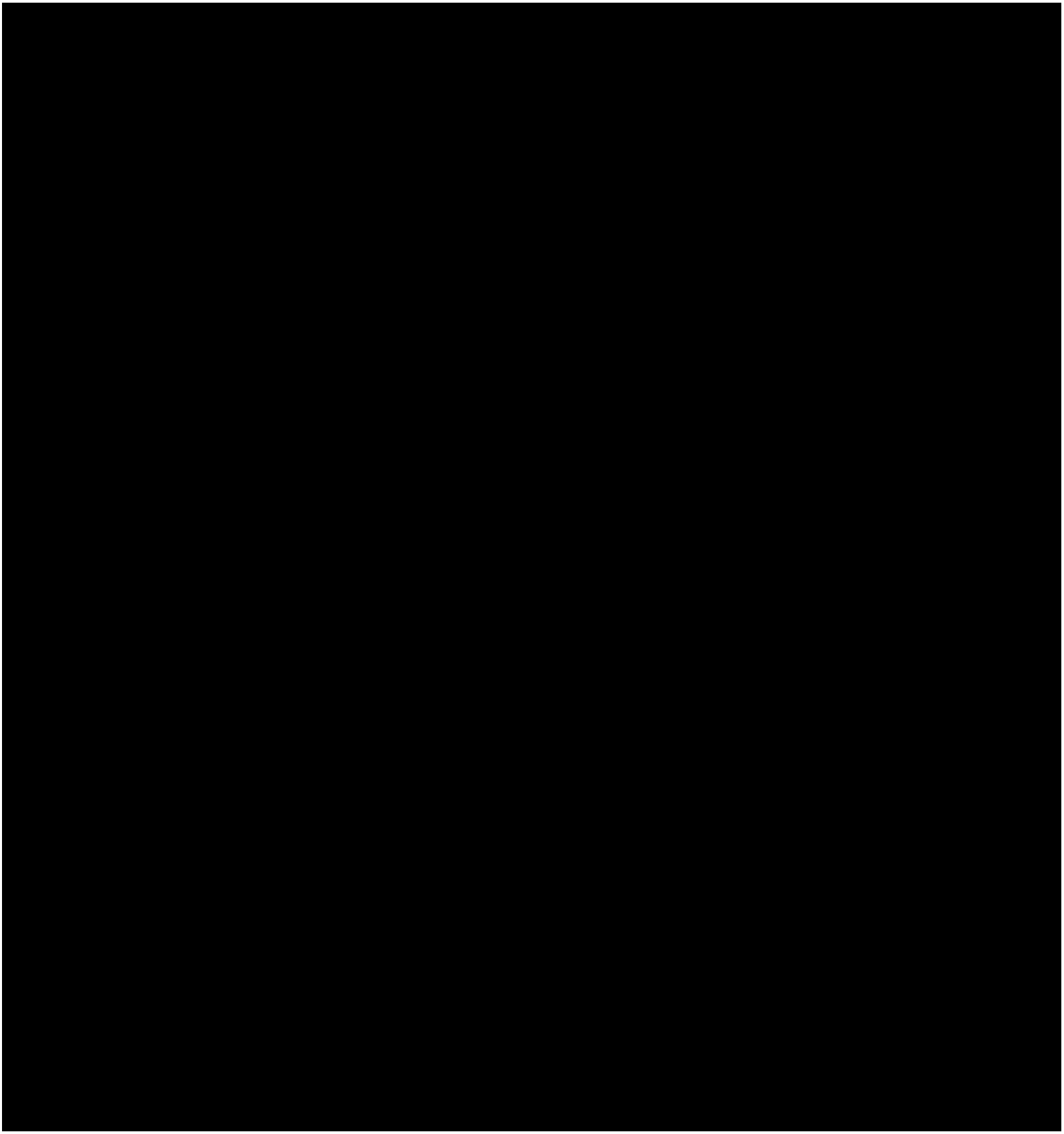
□ □ □□□□

[redacted]

□ □ □□□□



□ □ □□□□



□ □ □□□□

[redacted]

[redacted]

[redacted]

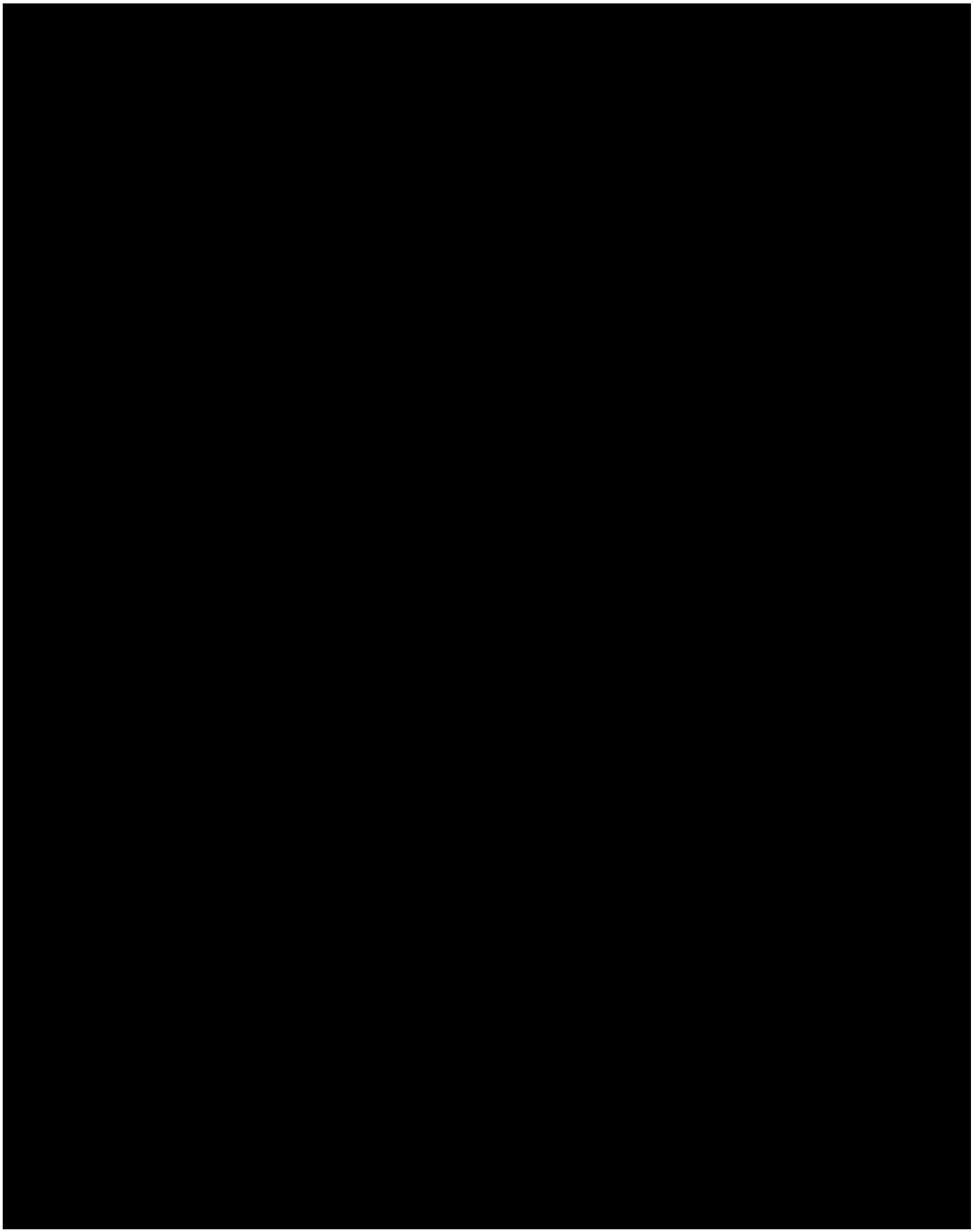
[redacted]

[redacted]

[redacted]

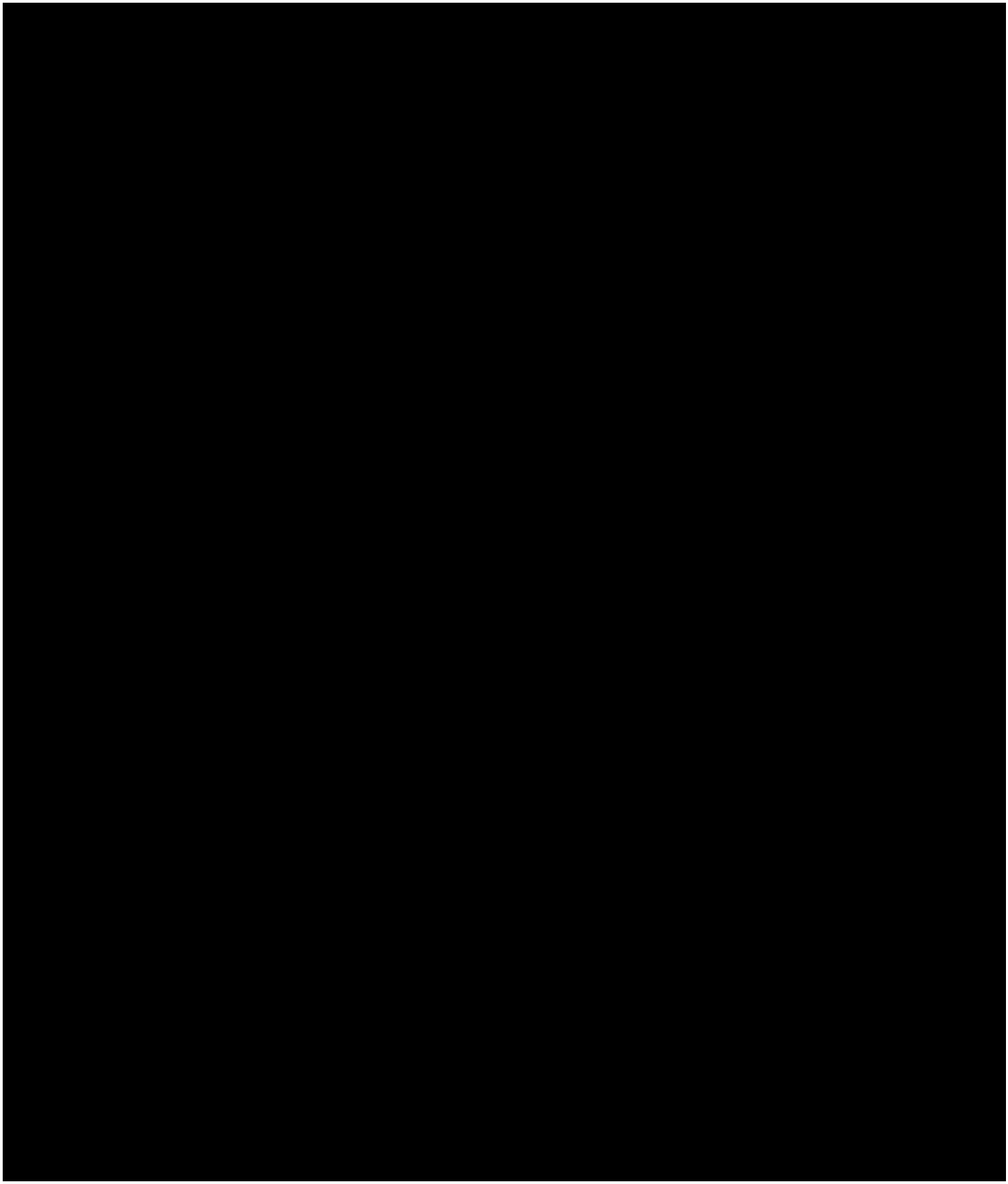
[redacted]

[redacted]

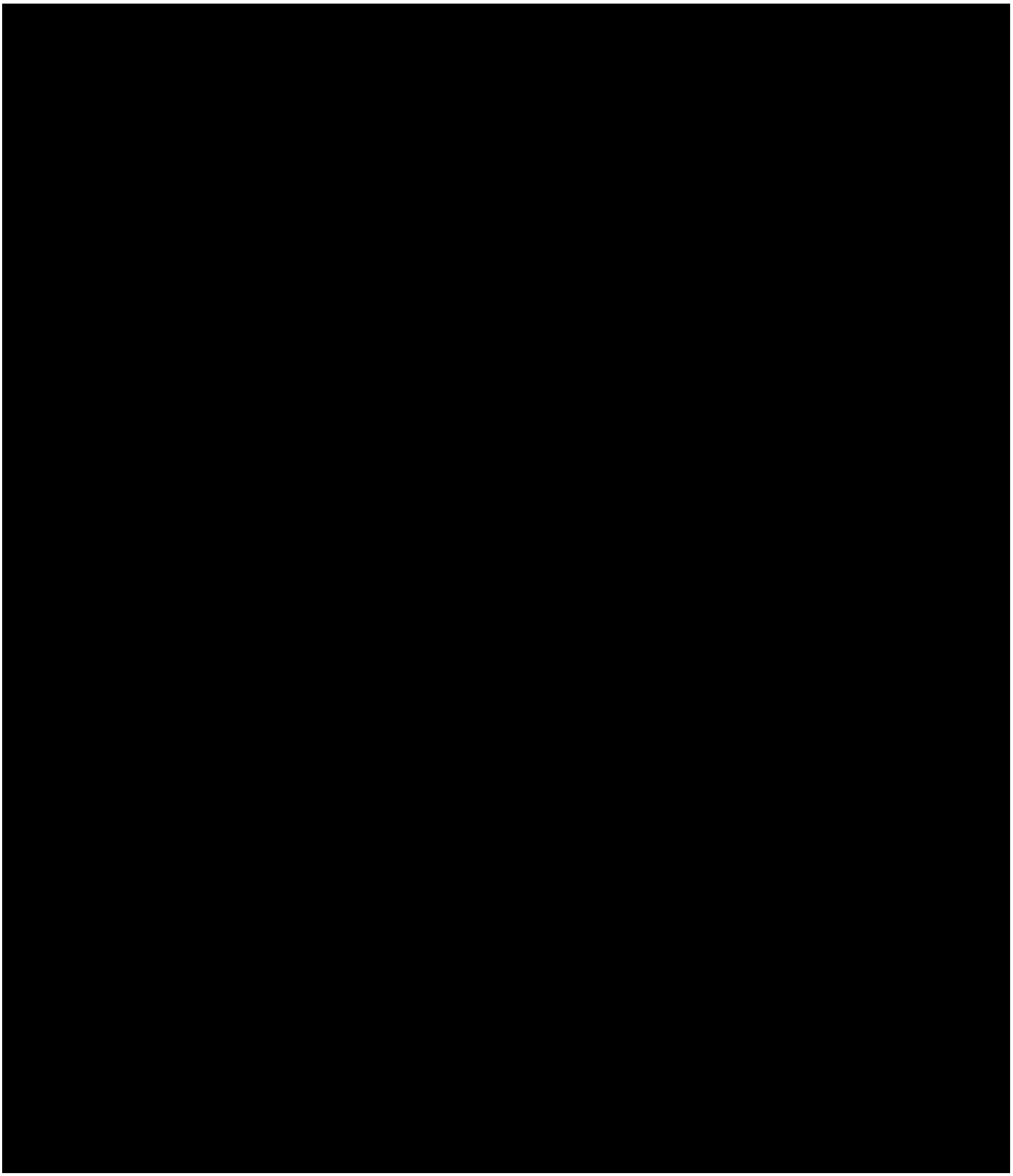


□ □ □□□□

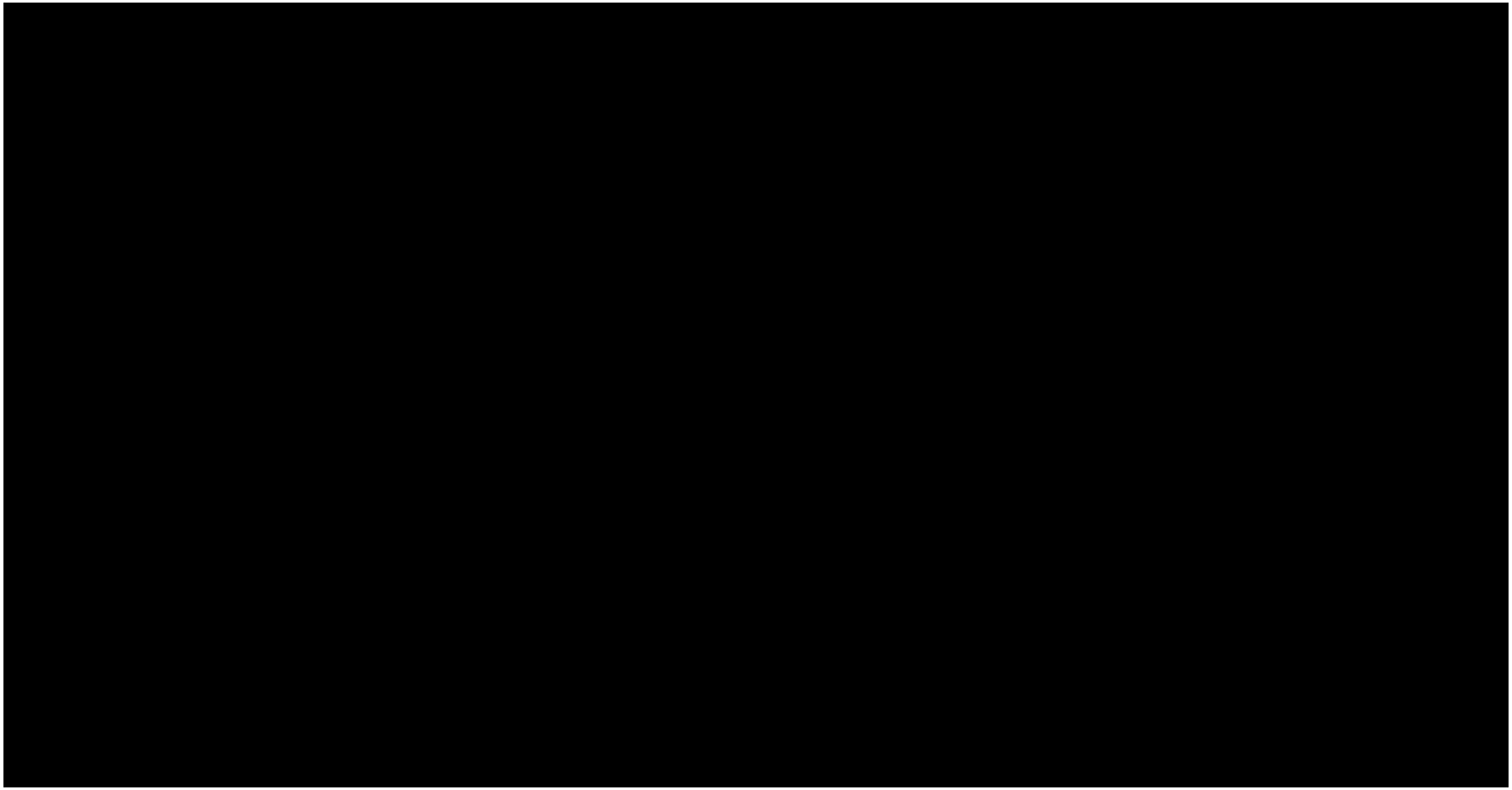
[redacted]



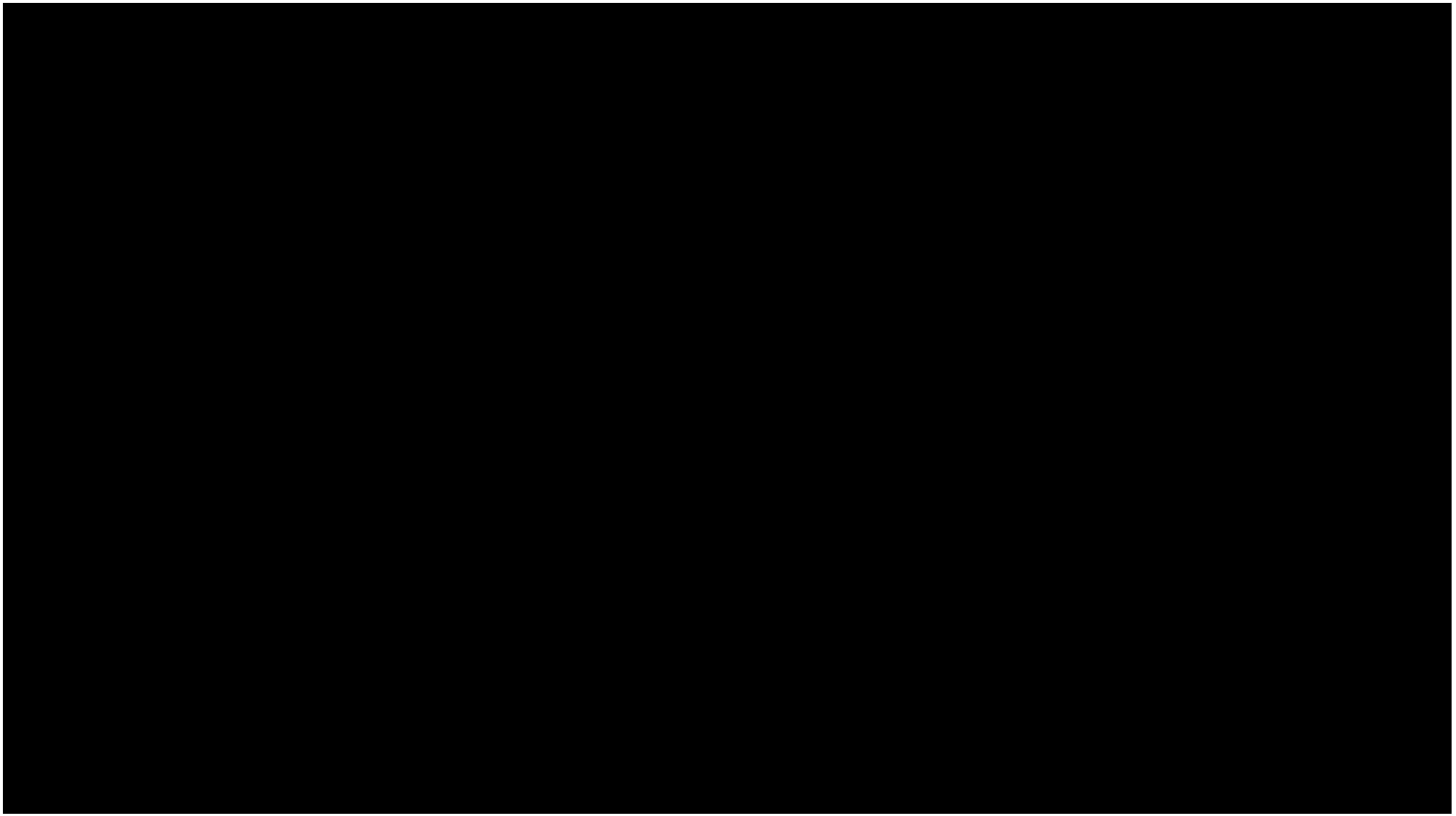
□ □ □□□□

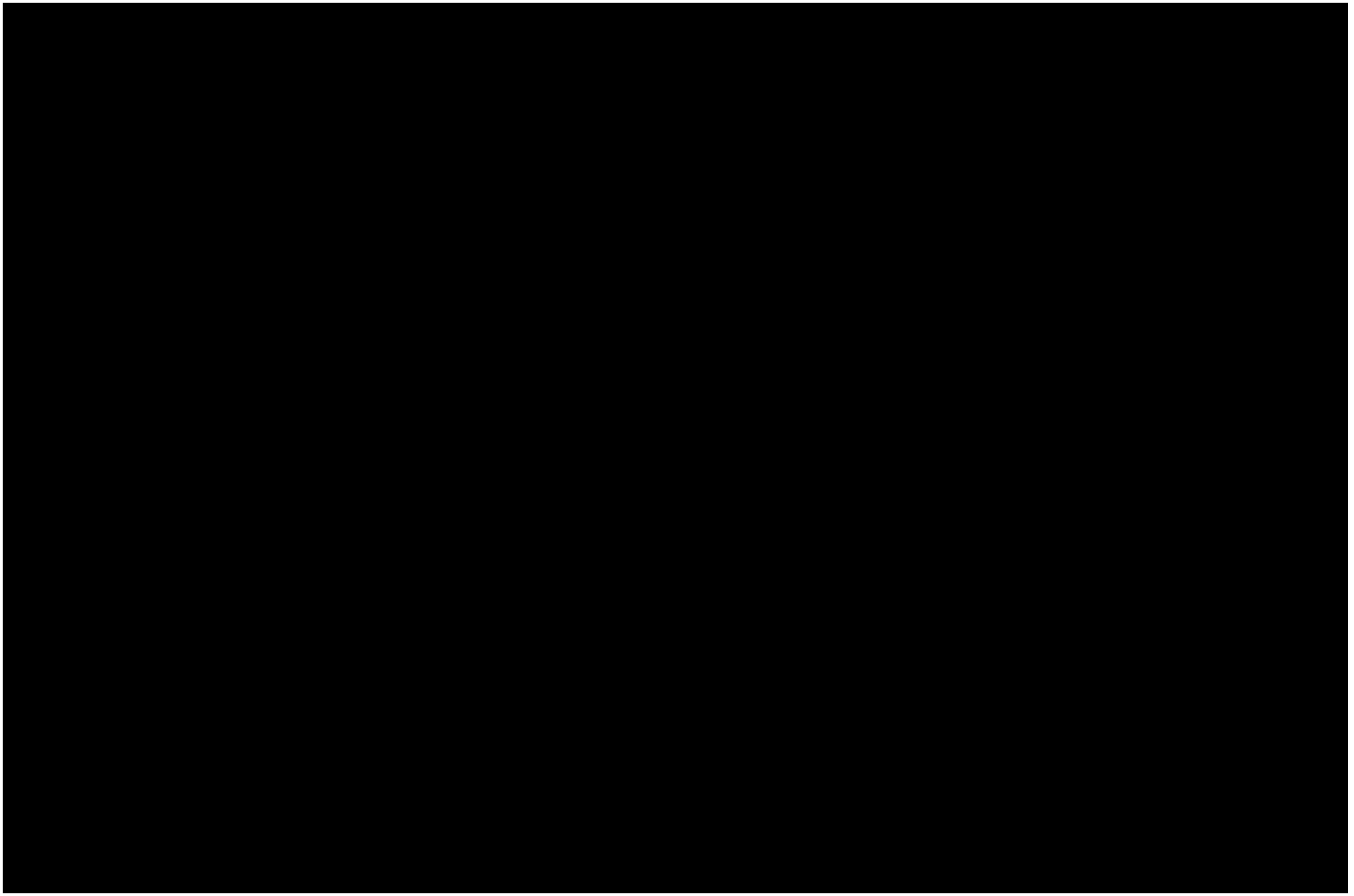


□ □ □□□□

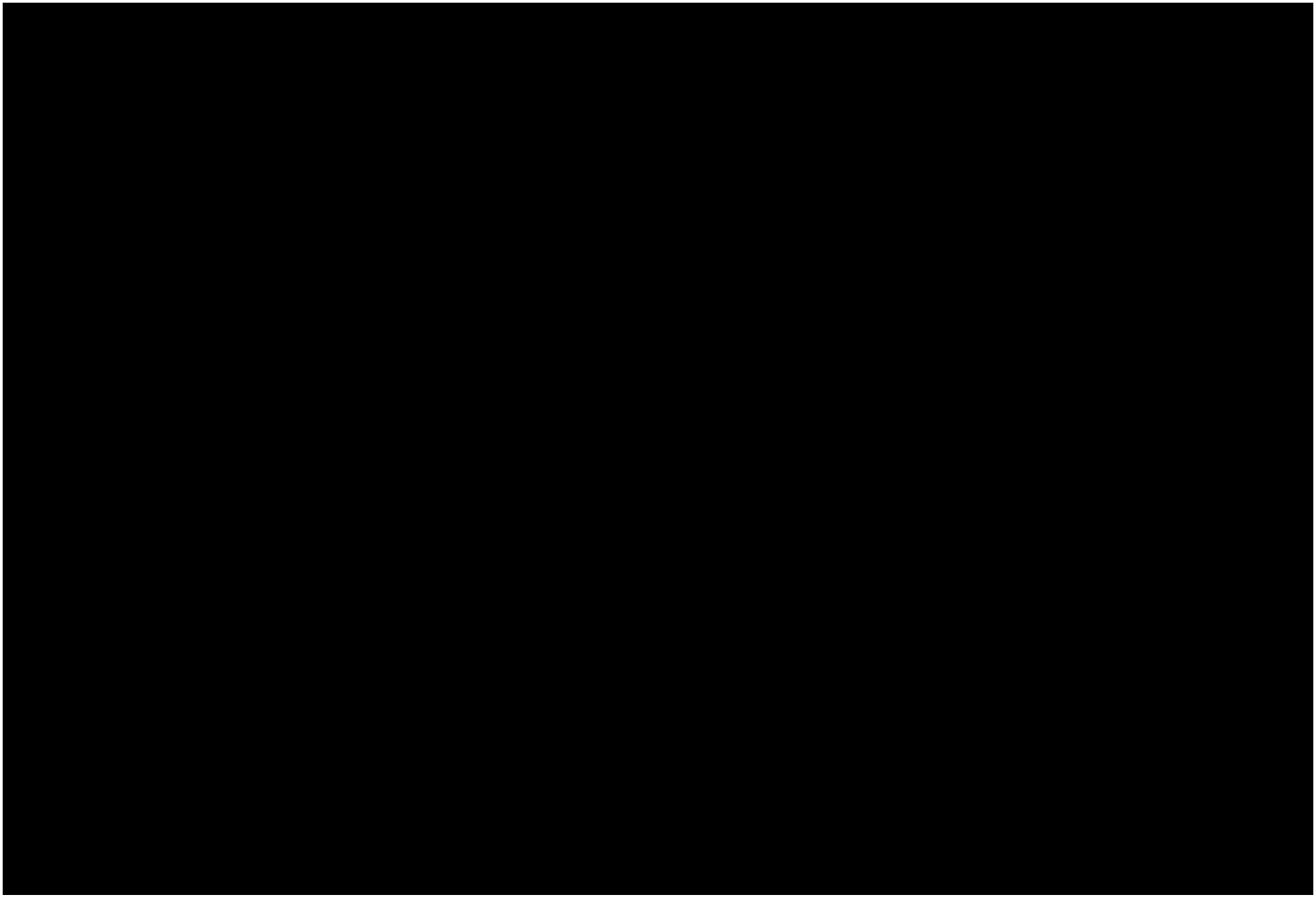


□ □ □□□□

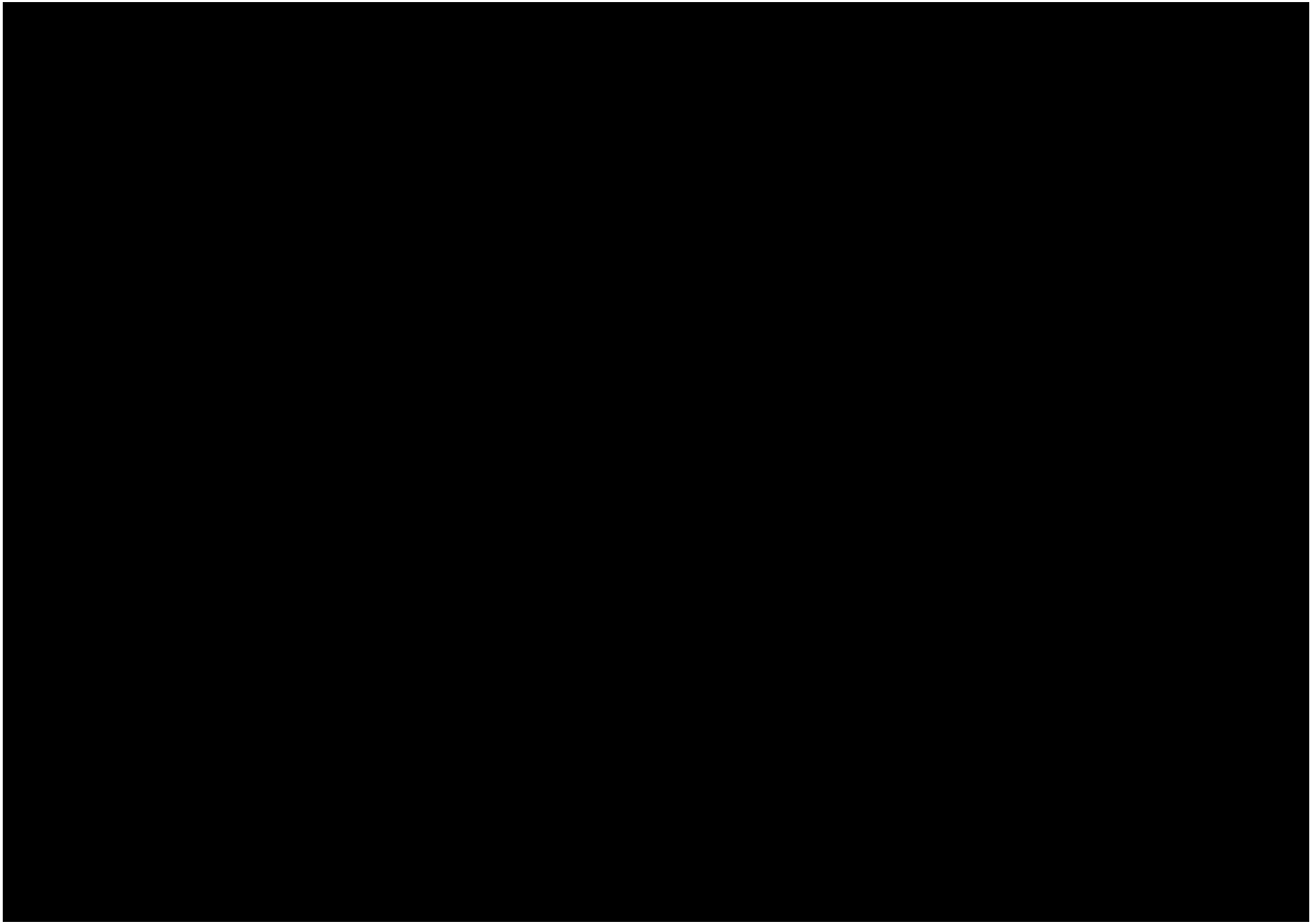




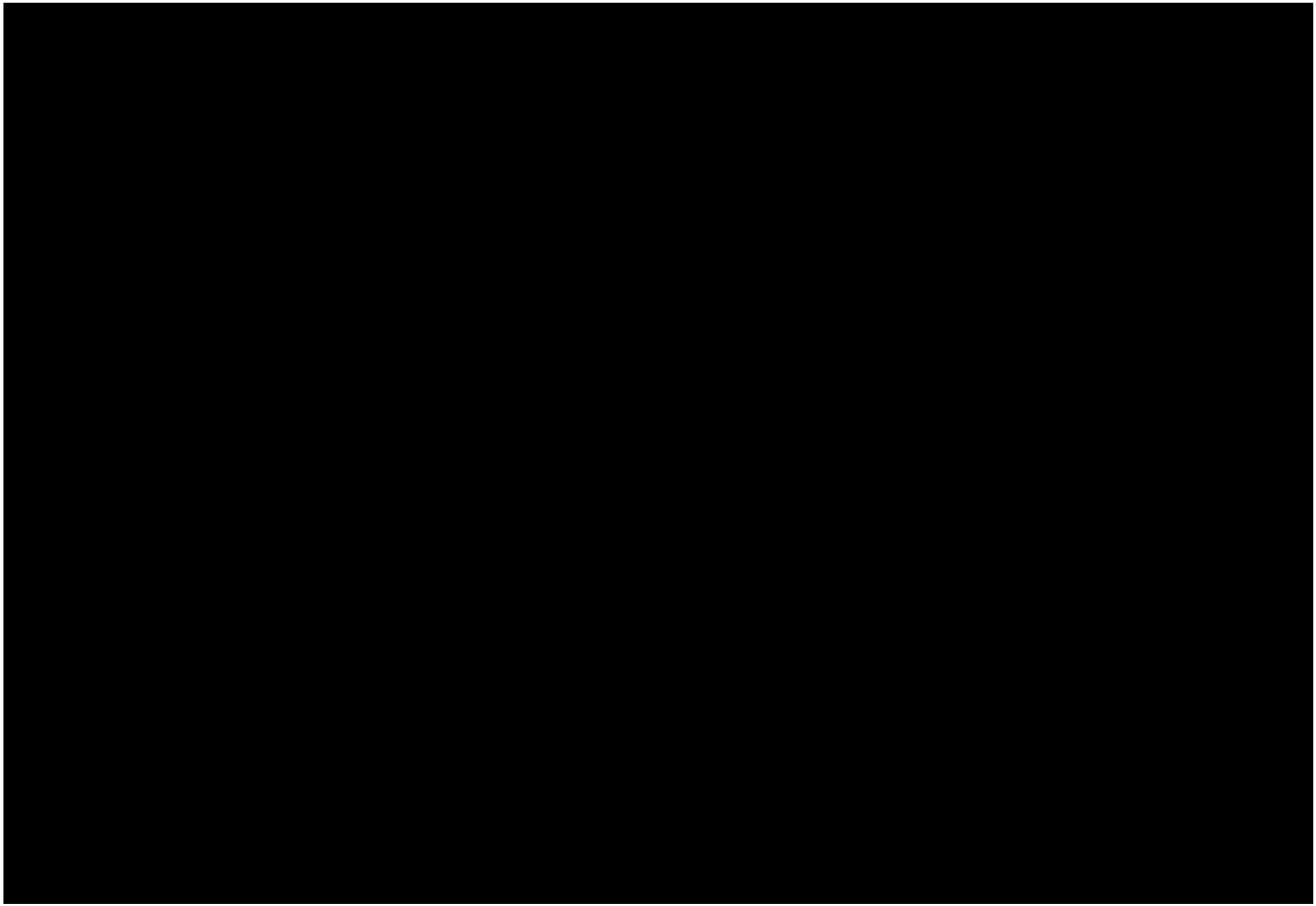
□ □ □□□□



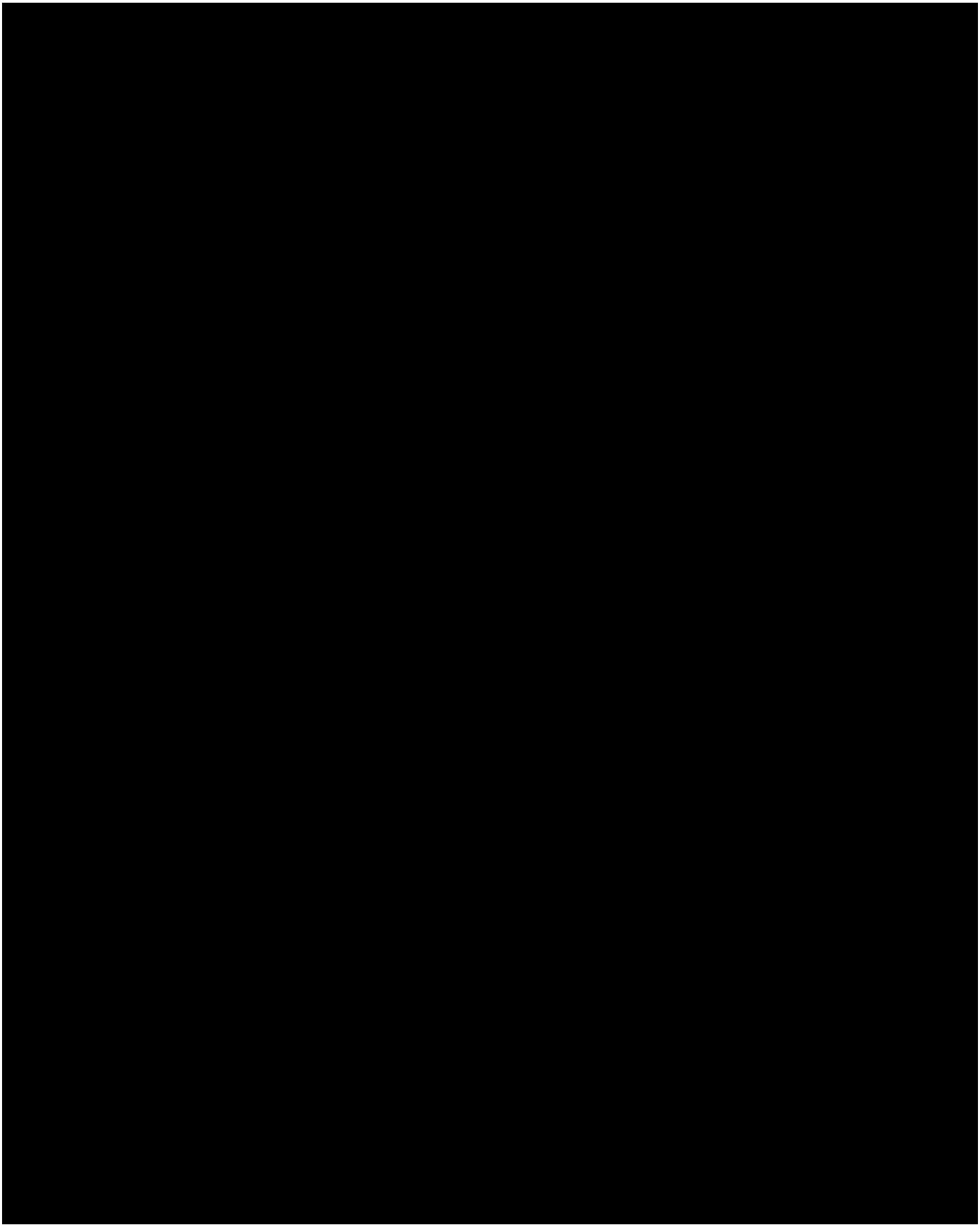
□ □ □□□□



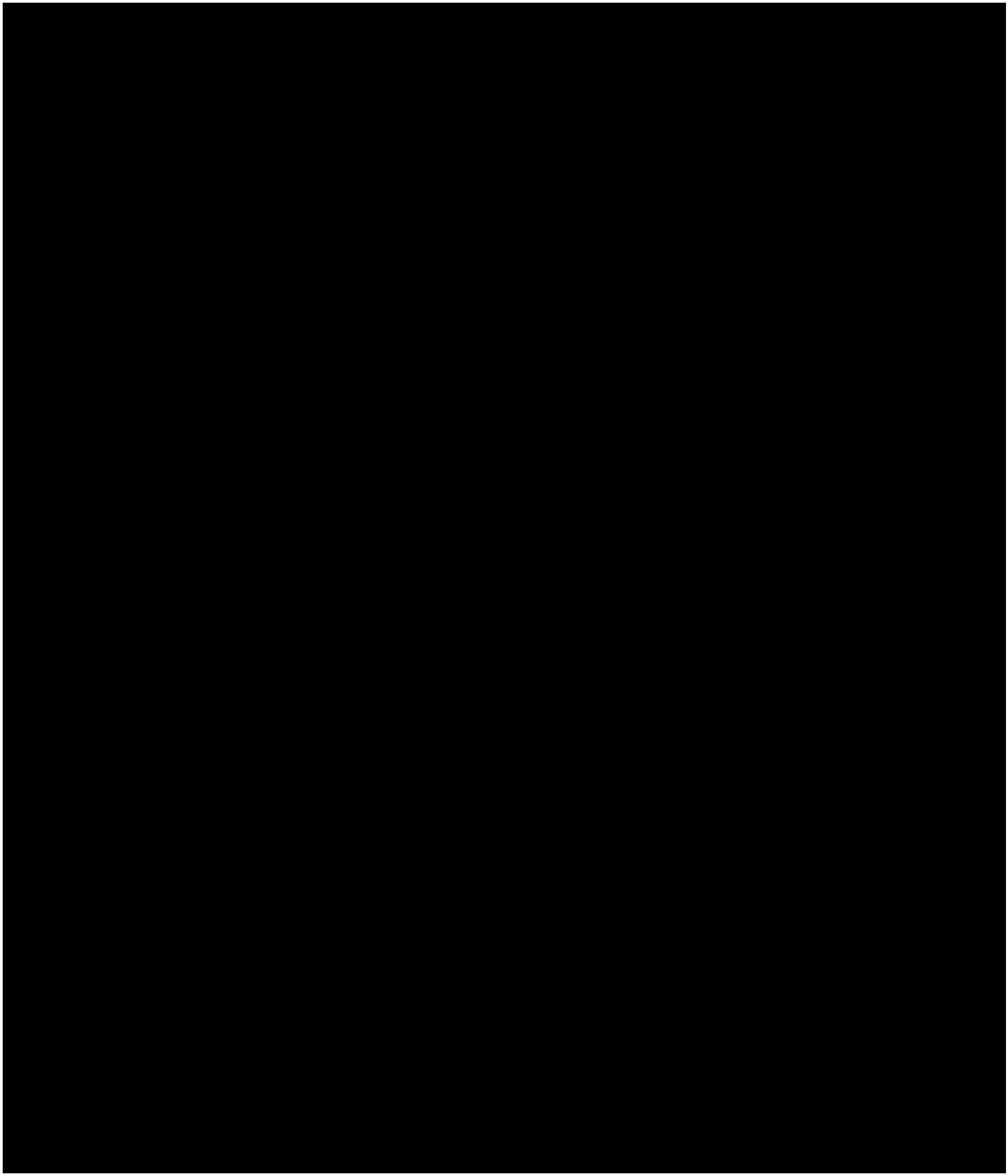
□ □ □□□□



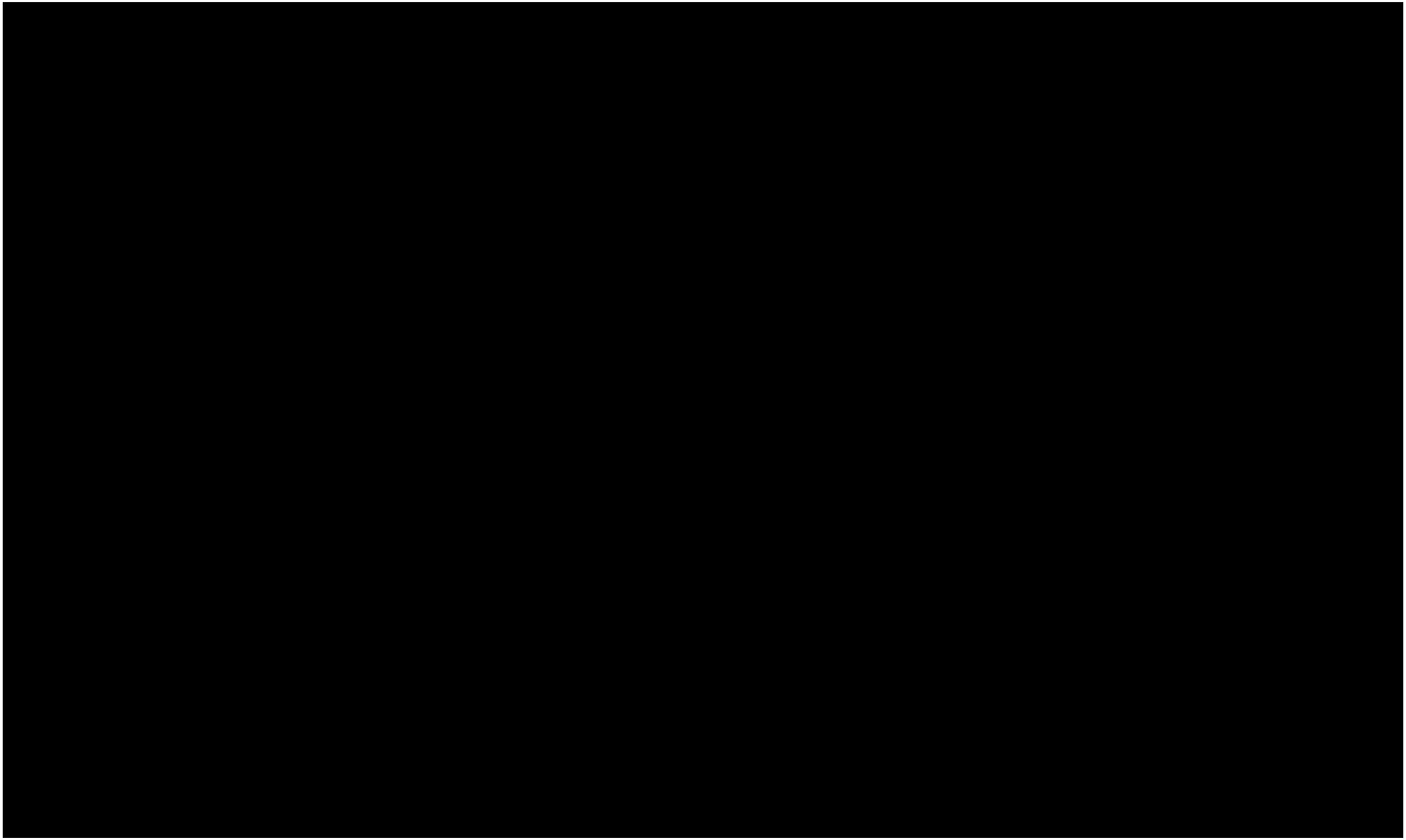
□ □ □□□□



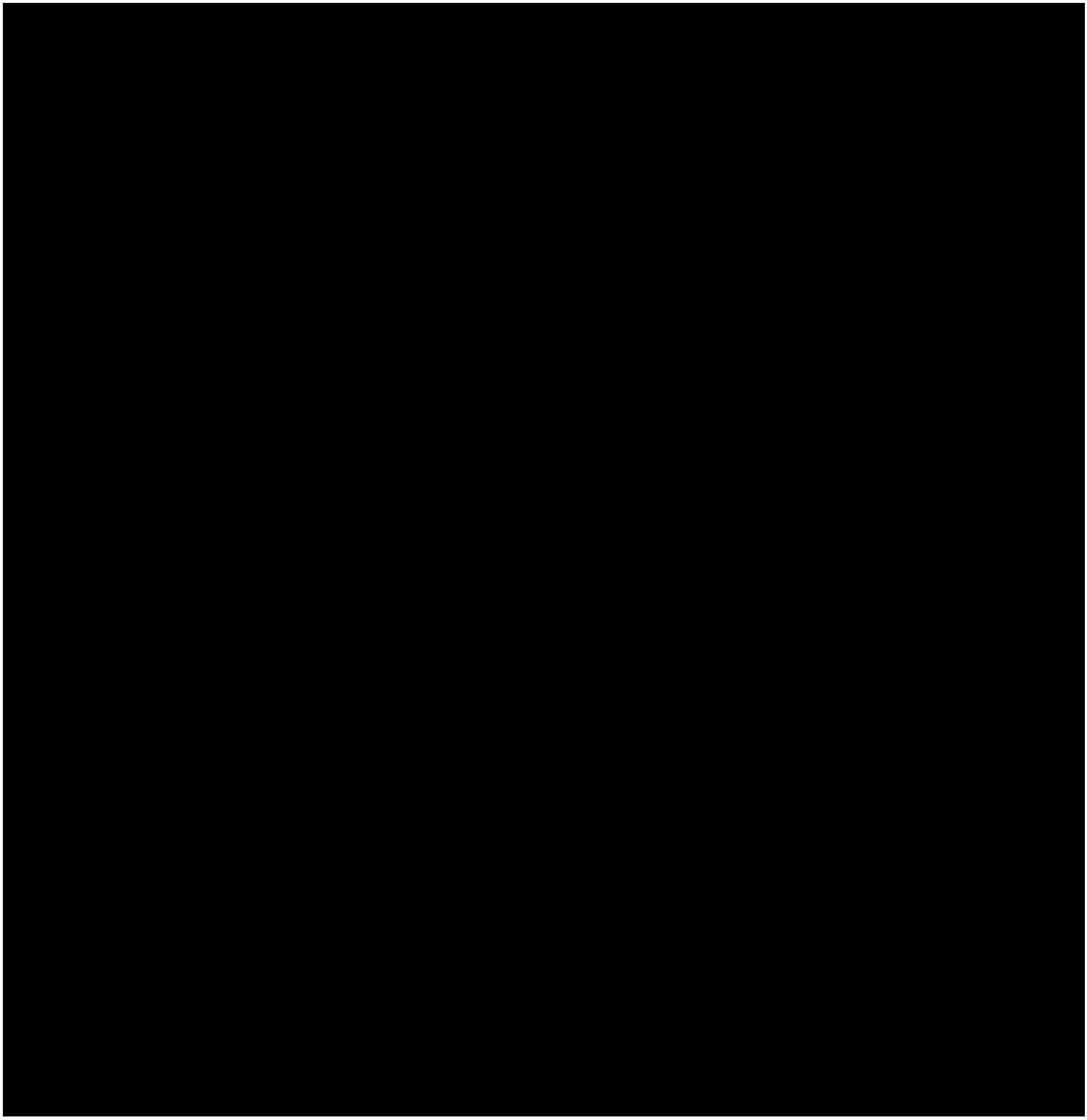
□ □ □□□□



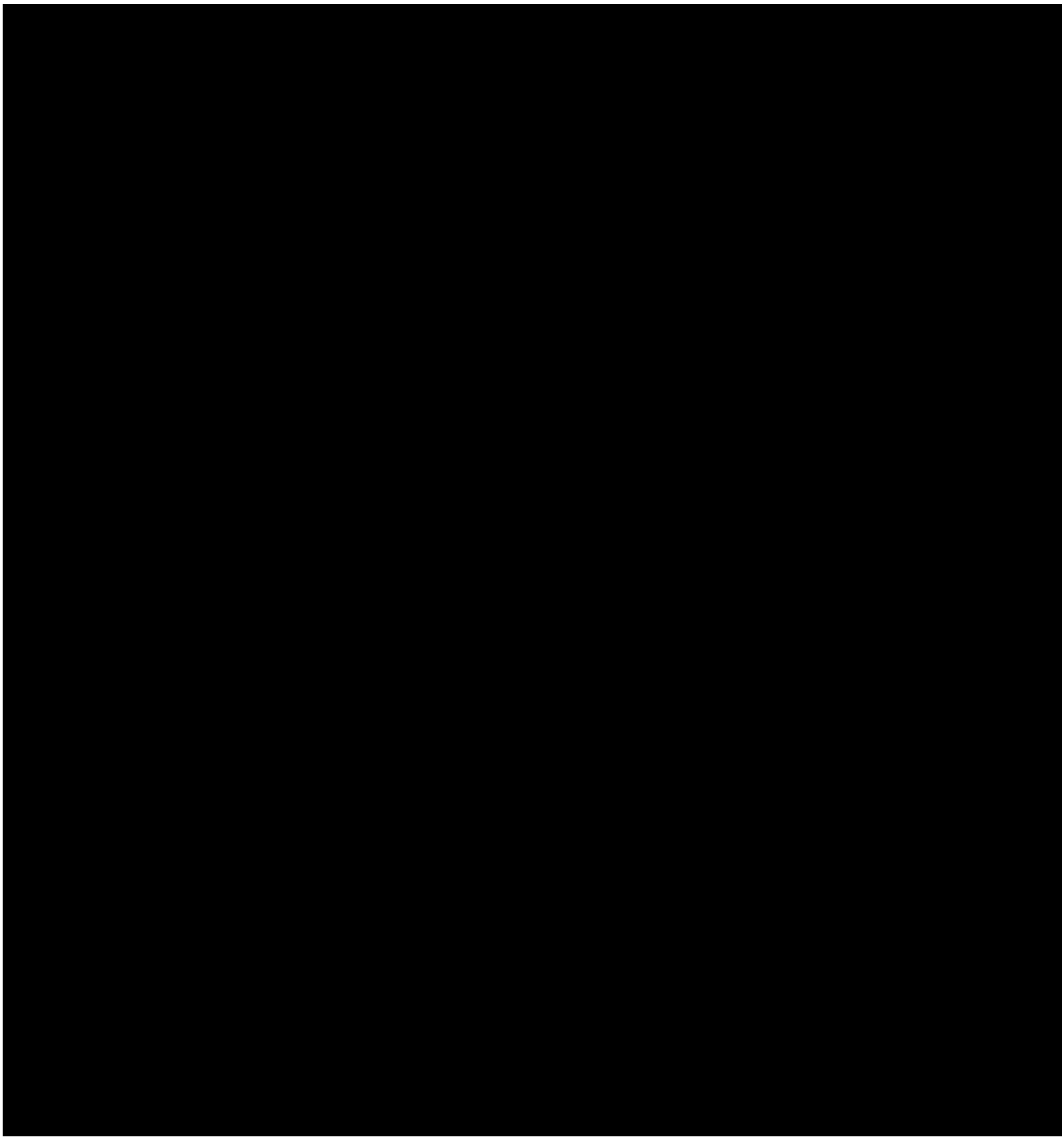
□ □ □□□□



□ □ □□□□

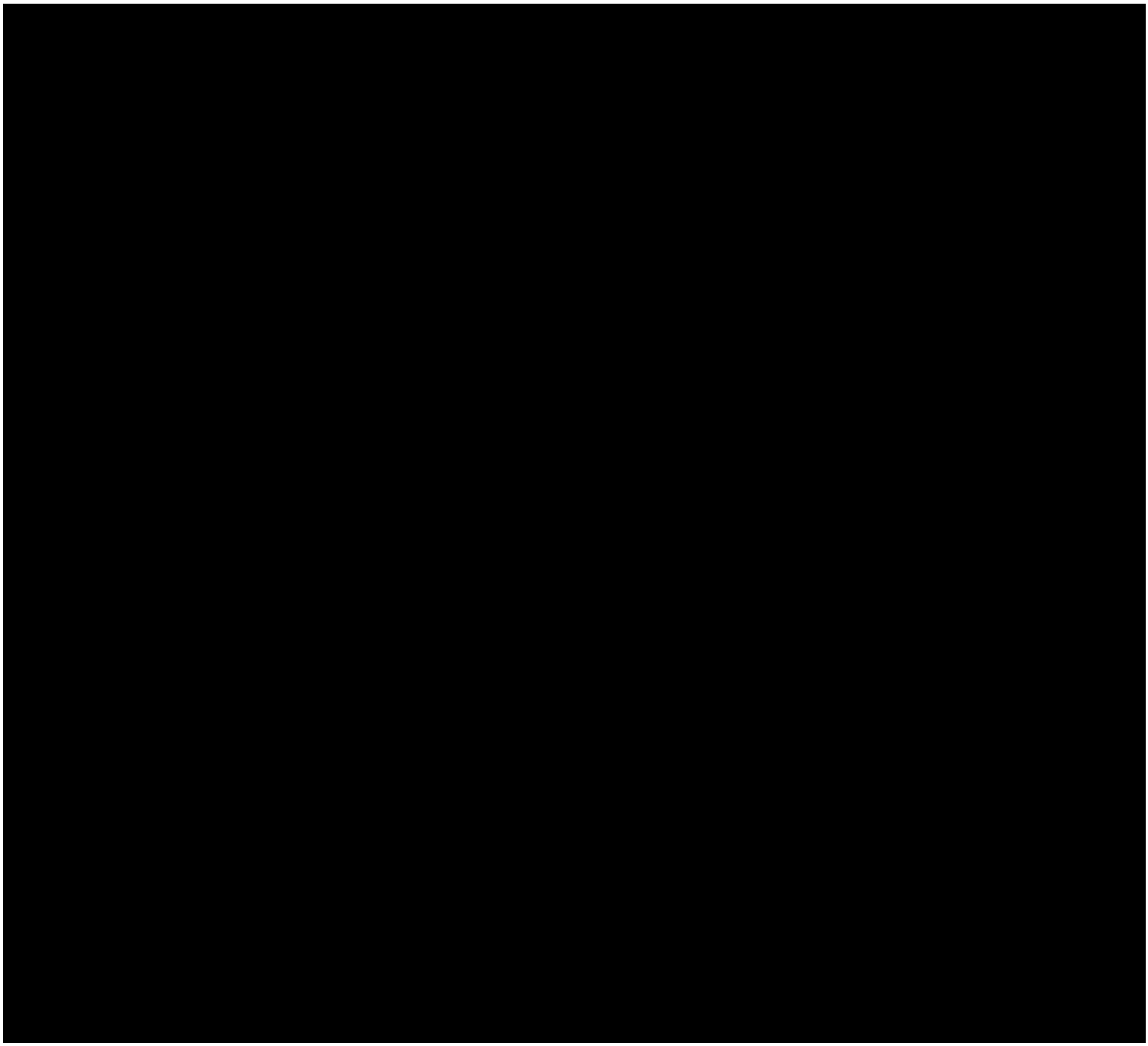


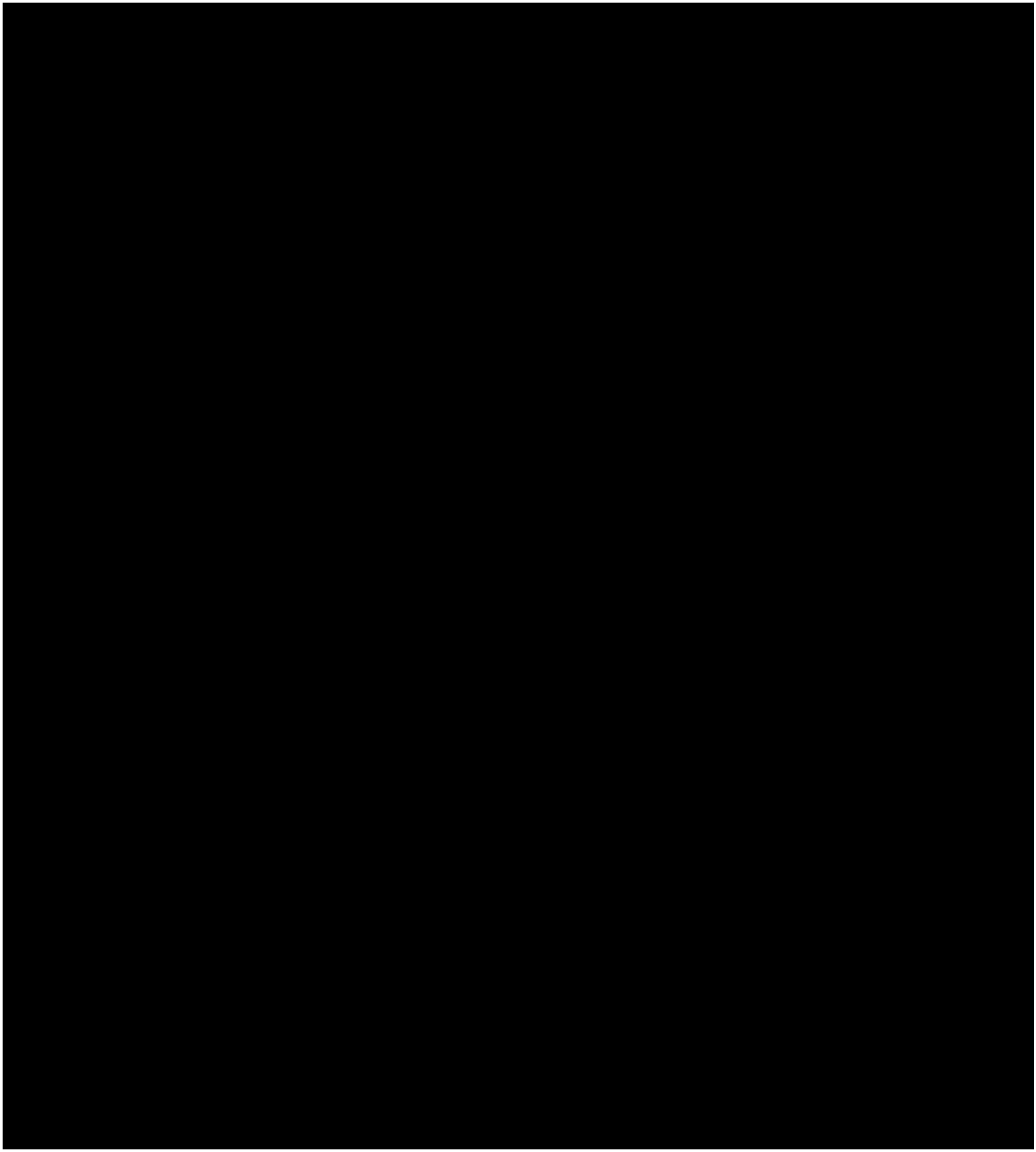
□ □ □□□□



□ □ □□□□

[redacted]

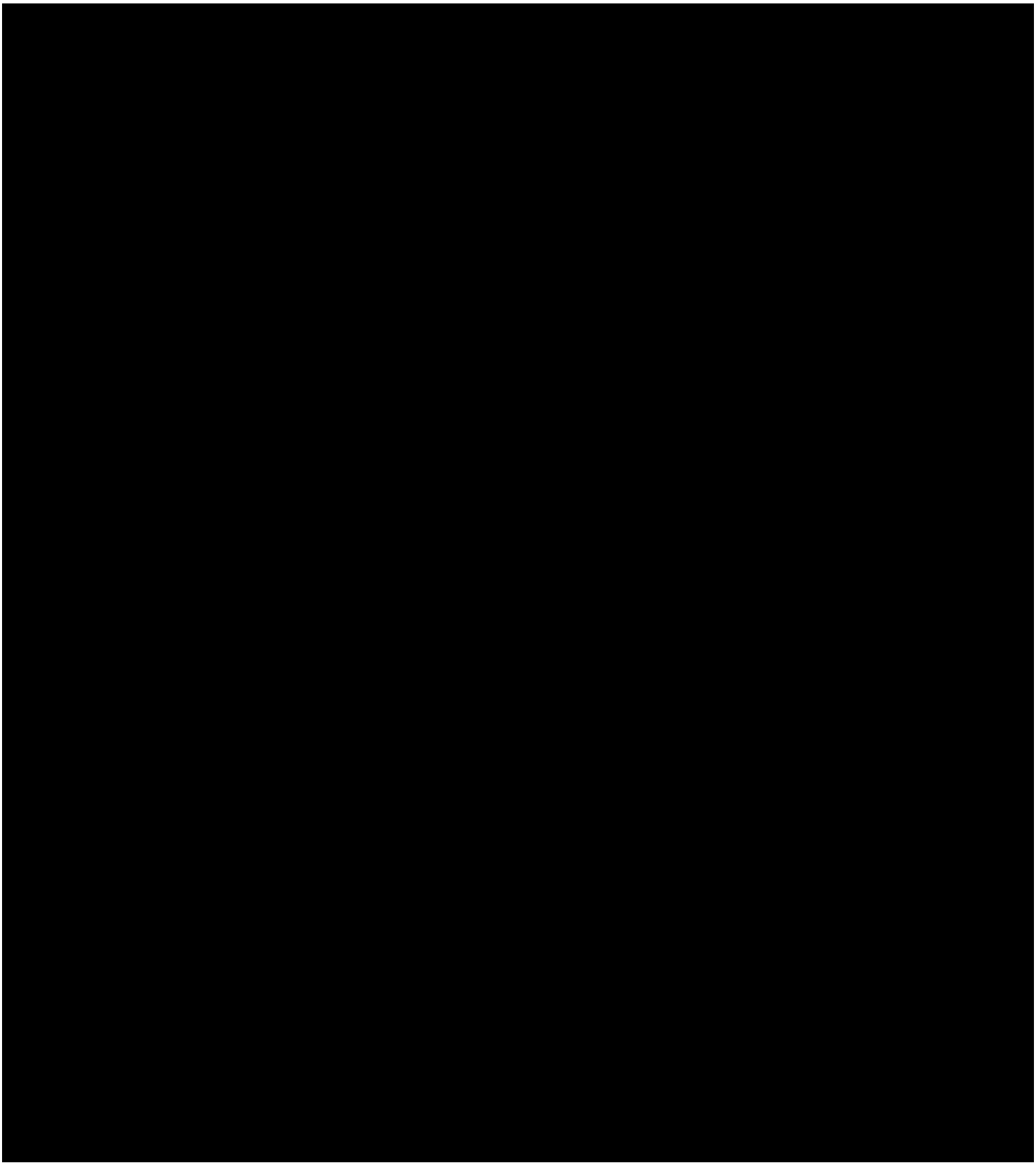




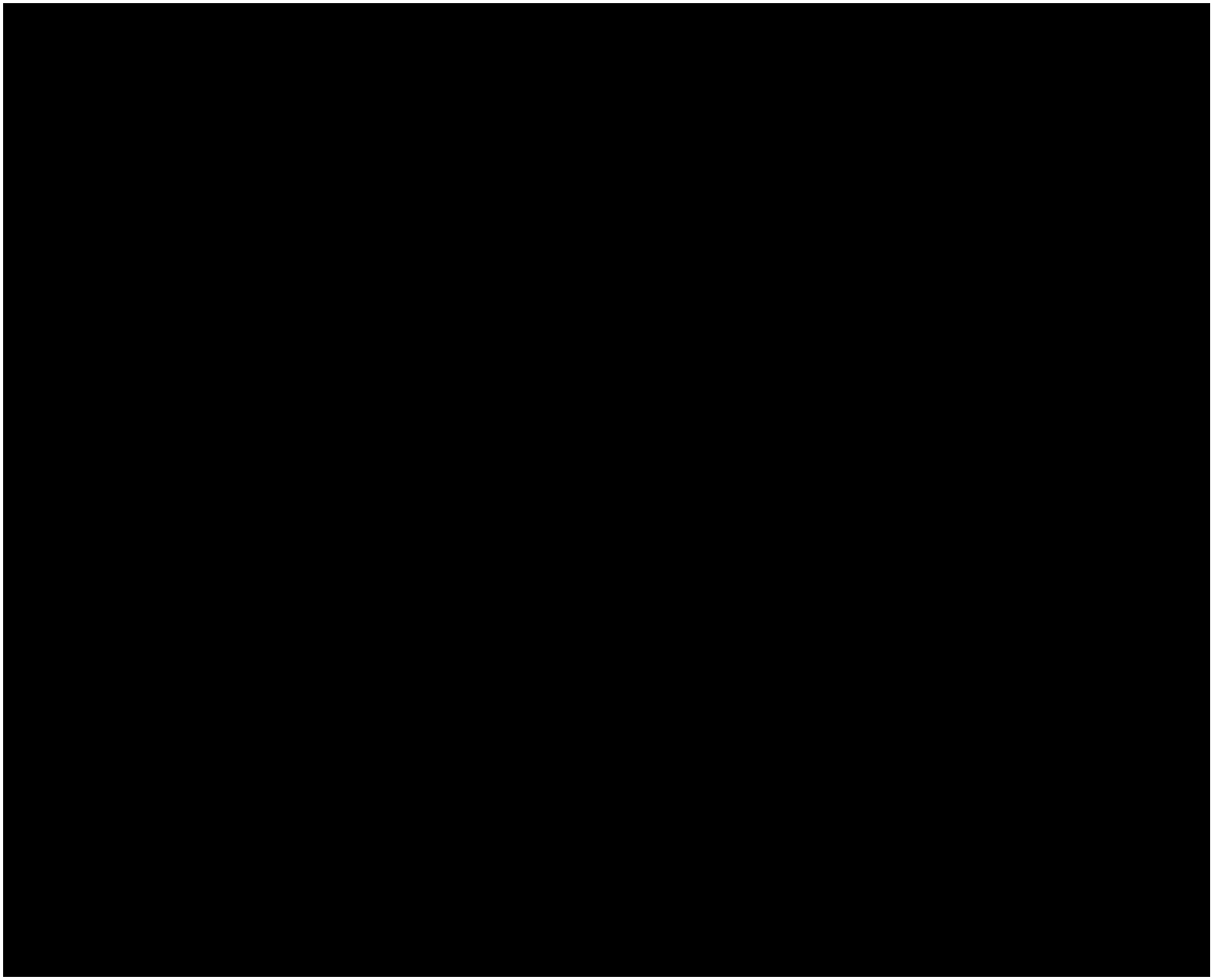
□ □ □□□□

[redacted]

[redacted]



□ □ □□□□



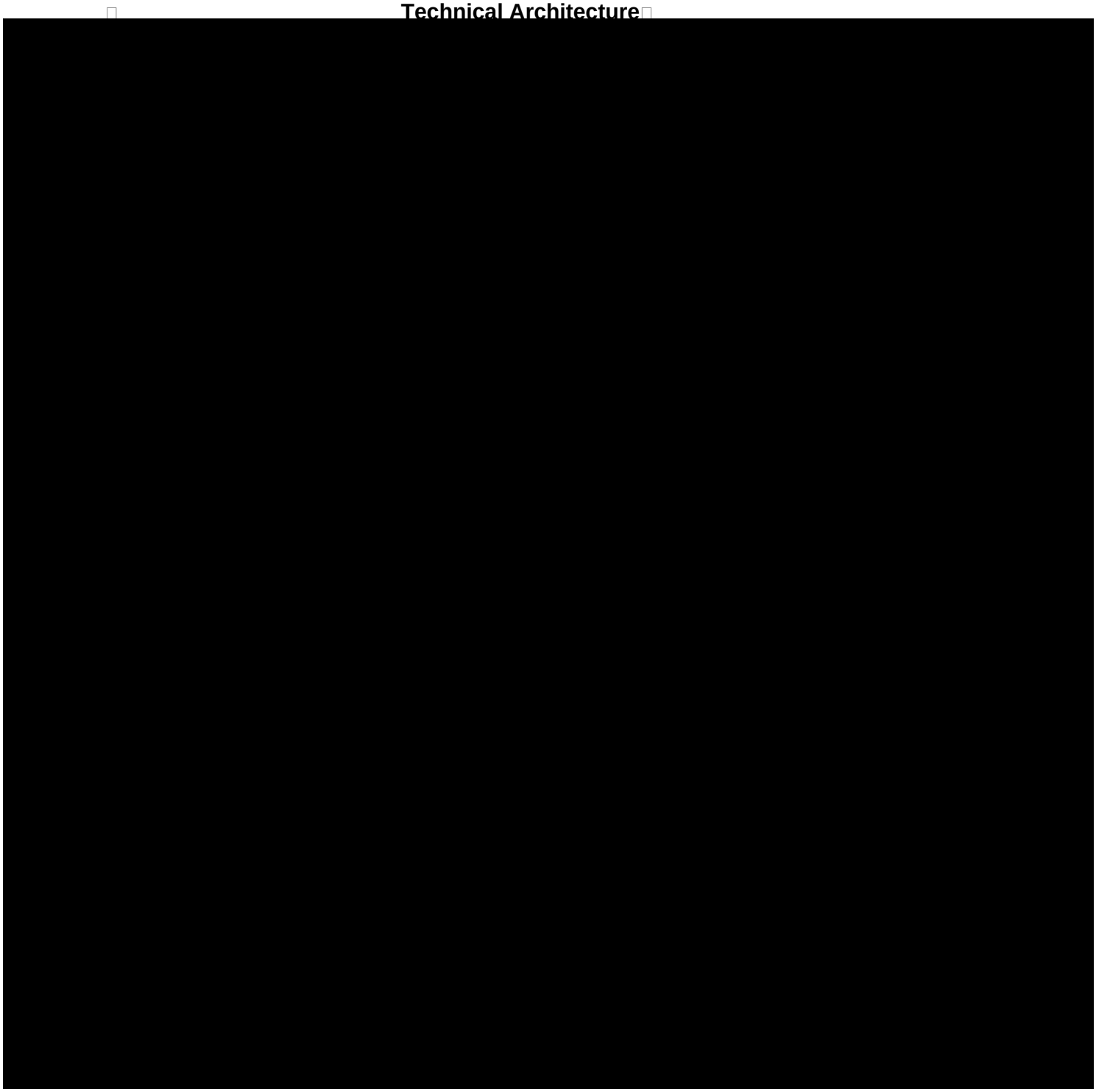
Attachment F-4 – Technical Architecture Deliverable Guide

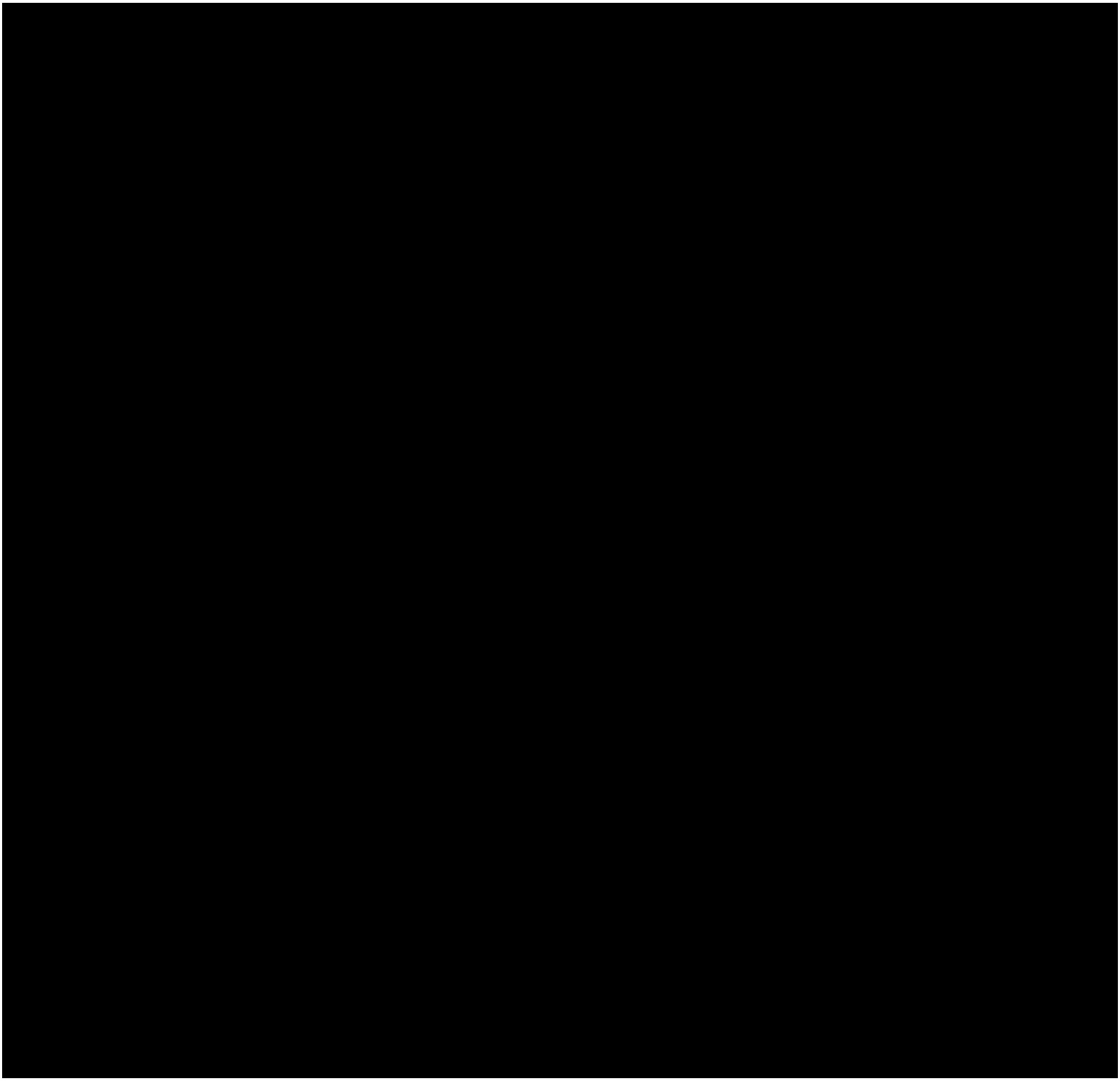
This attachment shows a sample architecture template document that is used to guide Unisys architects in the design of infrastructure architecture. **Please note that this attachment should be redacted for public view.**

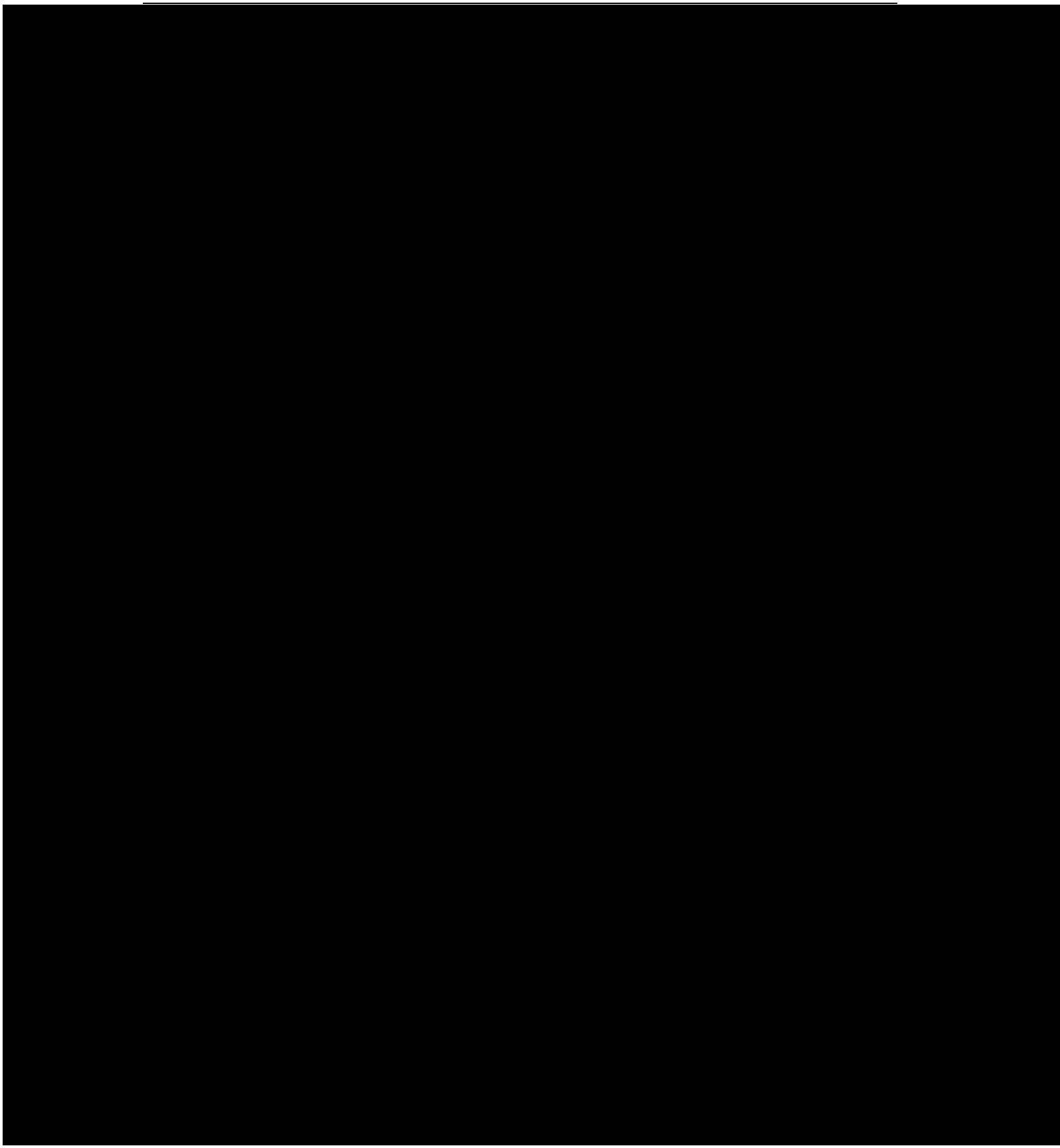
This page intentionally left blank.

Unisys

Technical Architecture







Attachment F-5 – Sample SAP Sizing Estimate

This attachment provides a sample of a recent sizing report

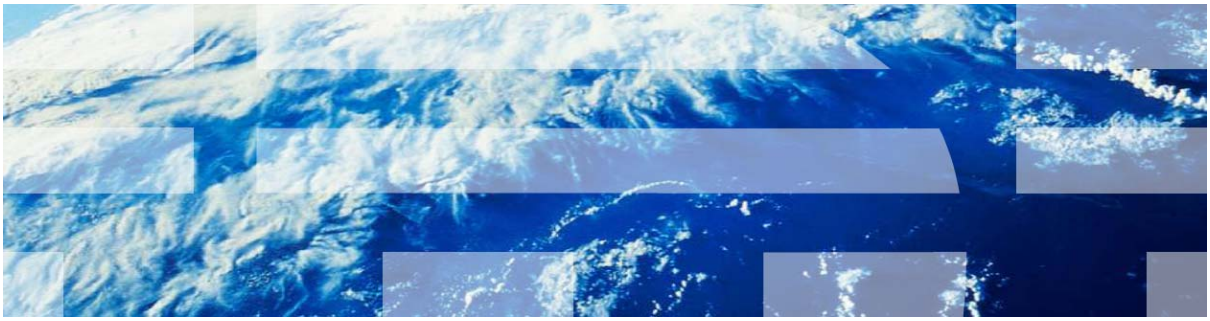
This page intentionally left blank.

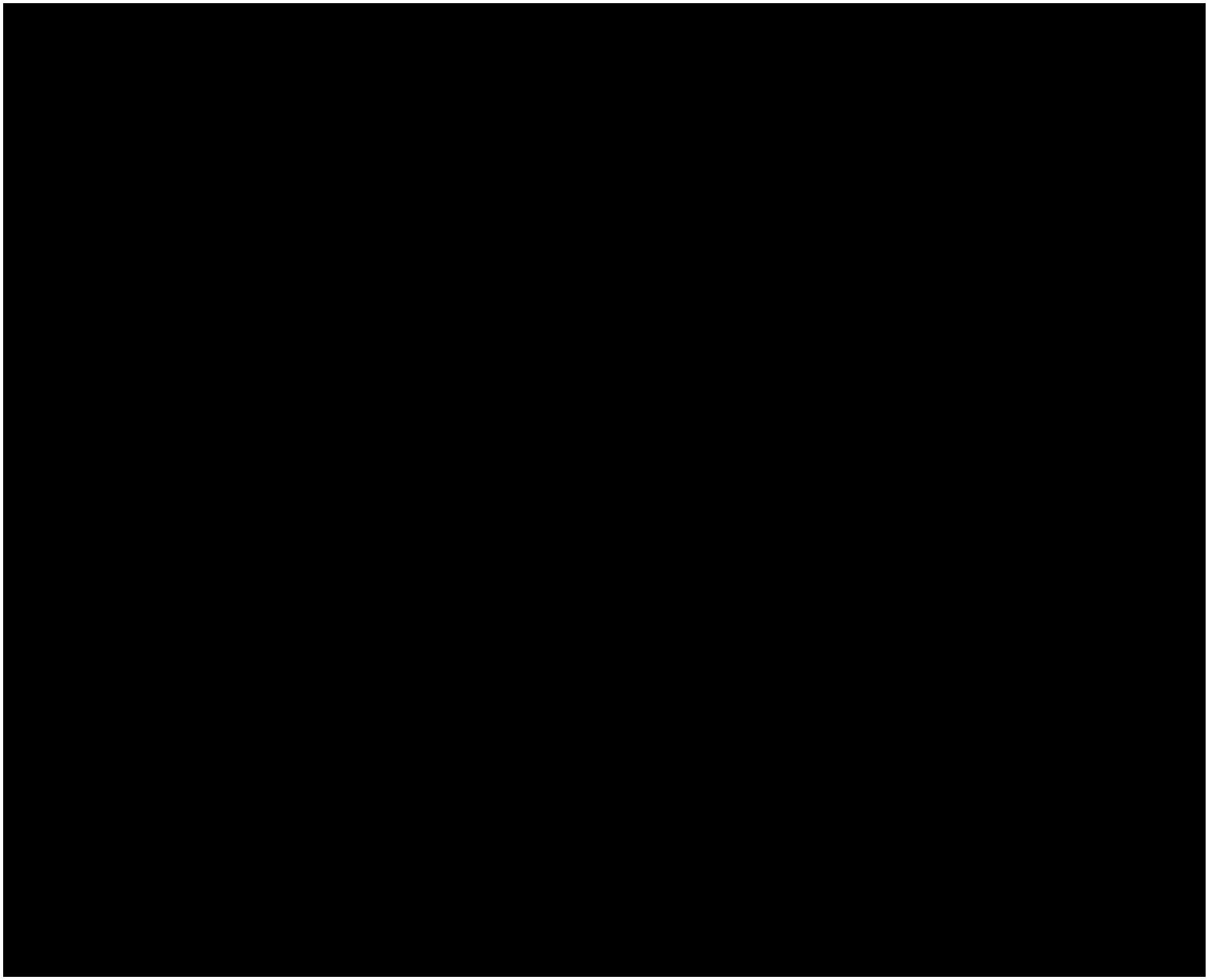
Customer

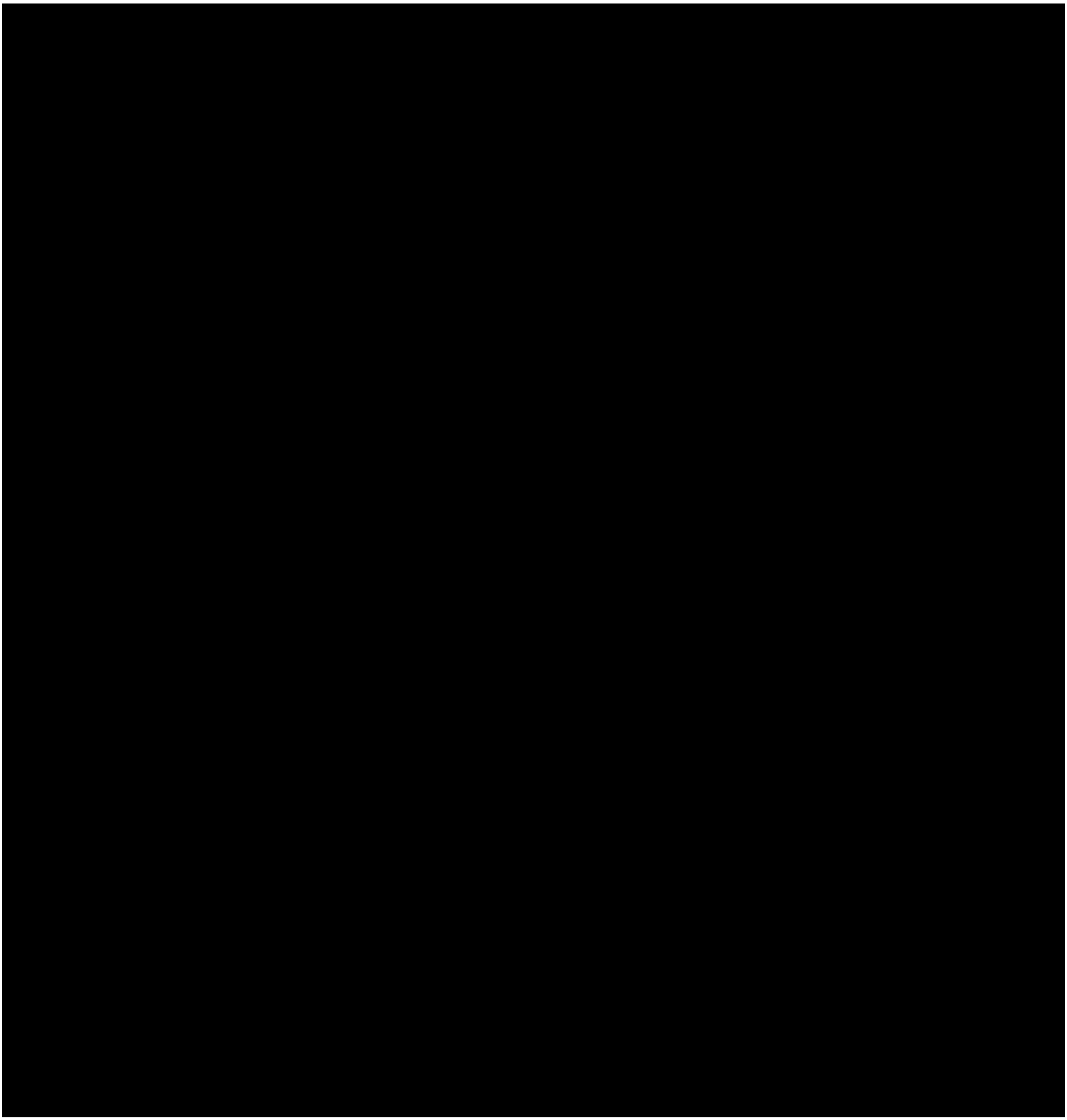
SAP Business Suite 7 Sizing Estimate

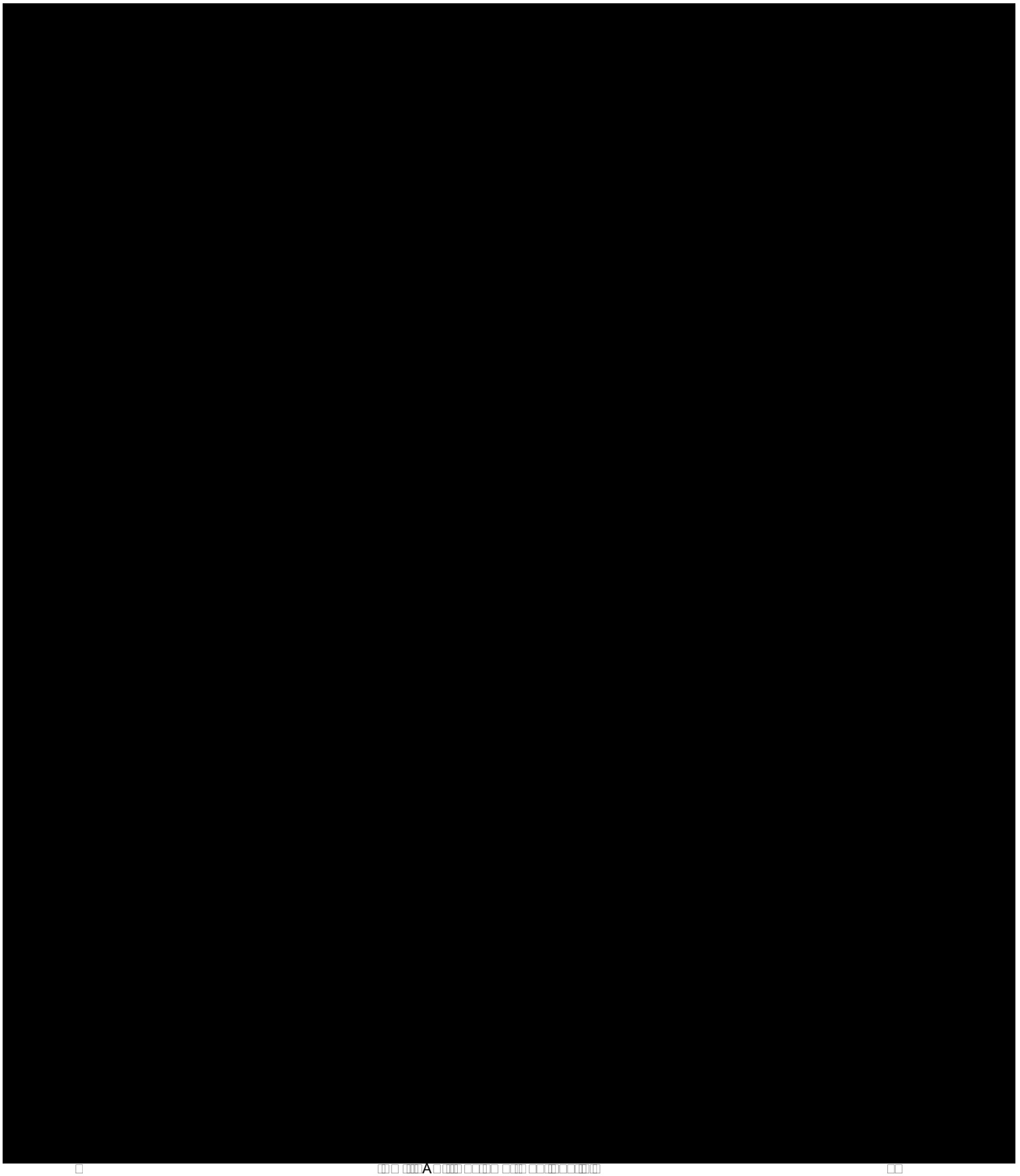
[redacted]

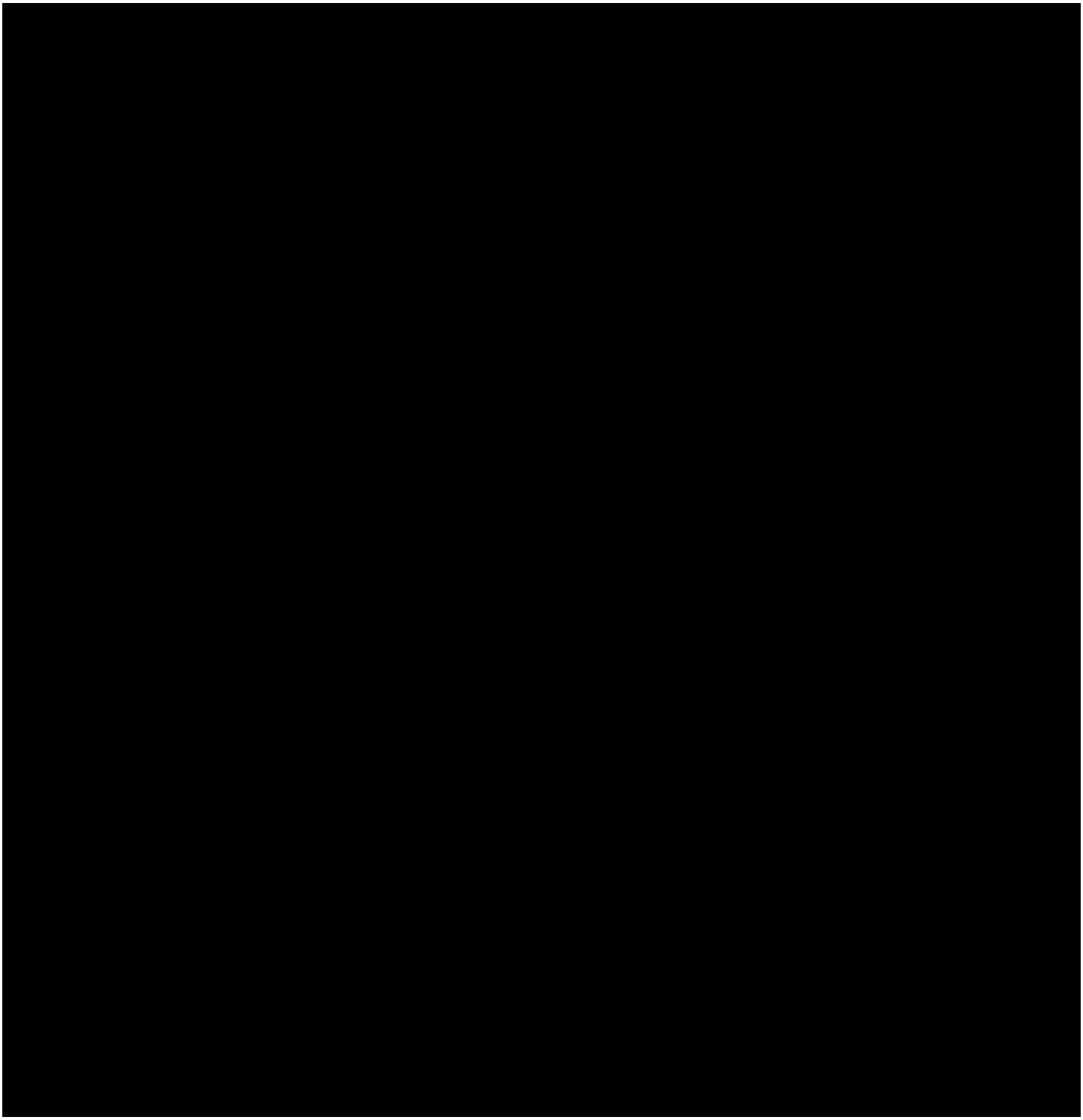
[redacted]@us.ibm.com

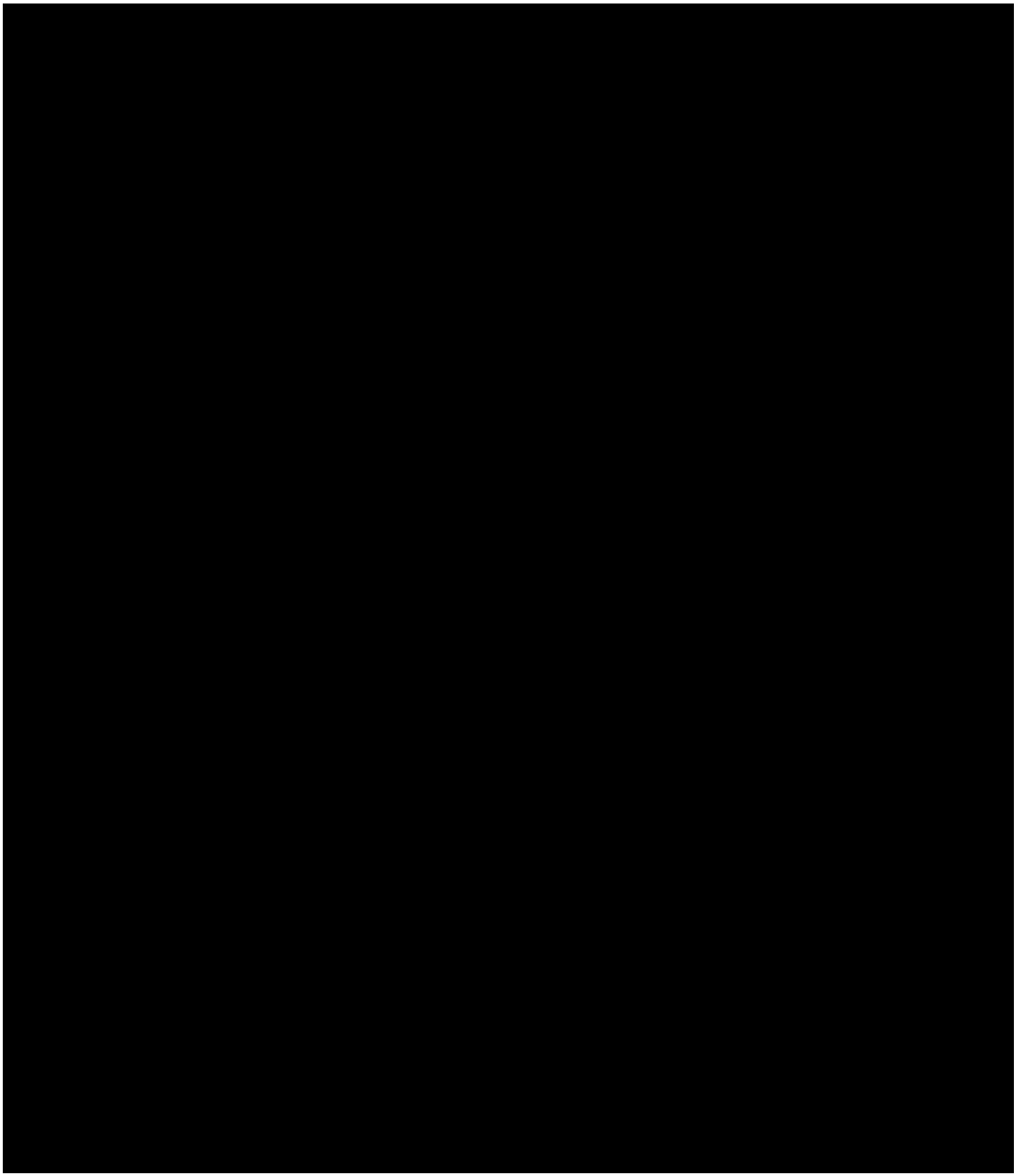


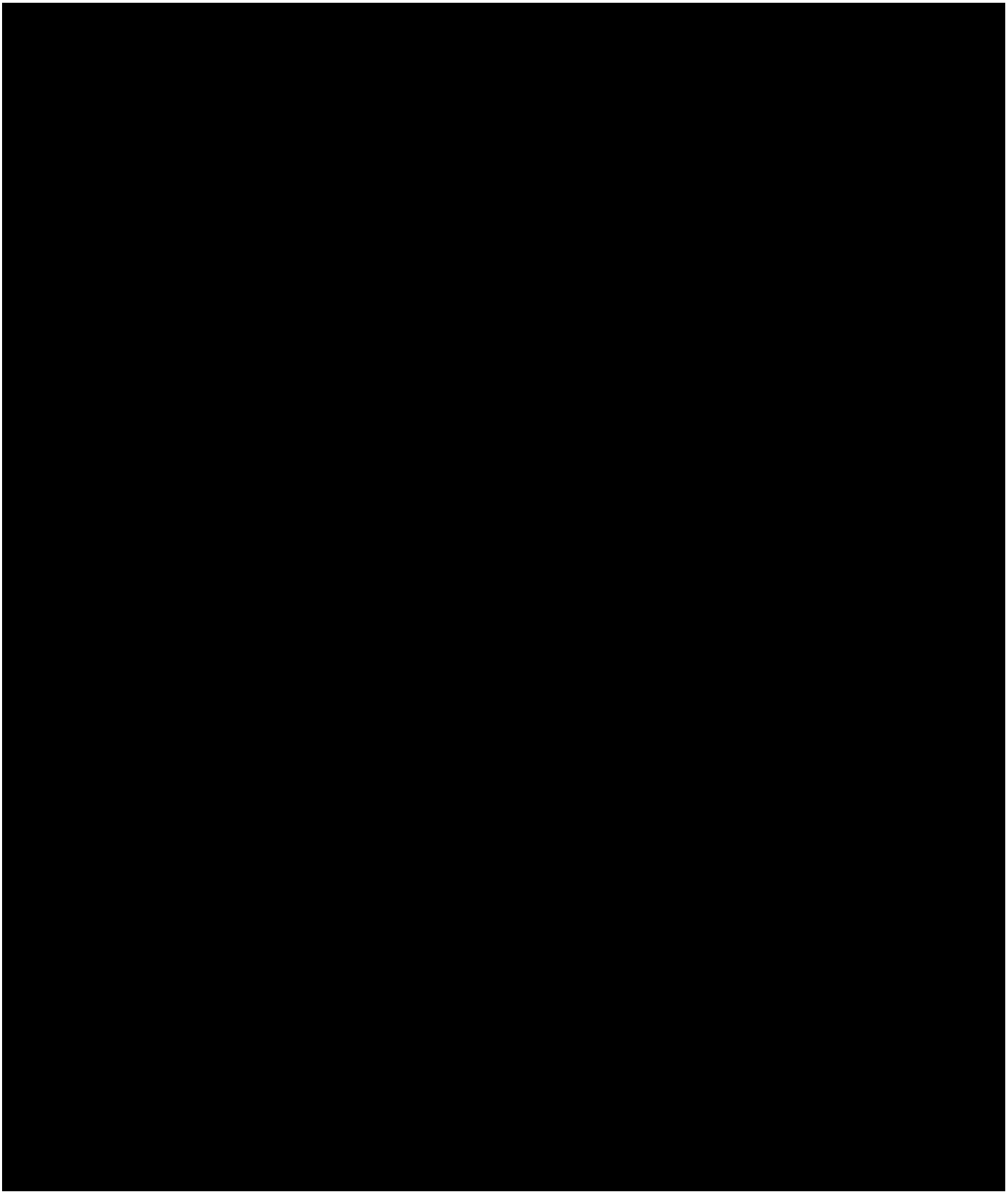


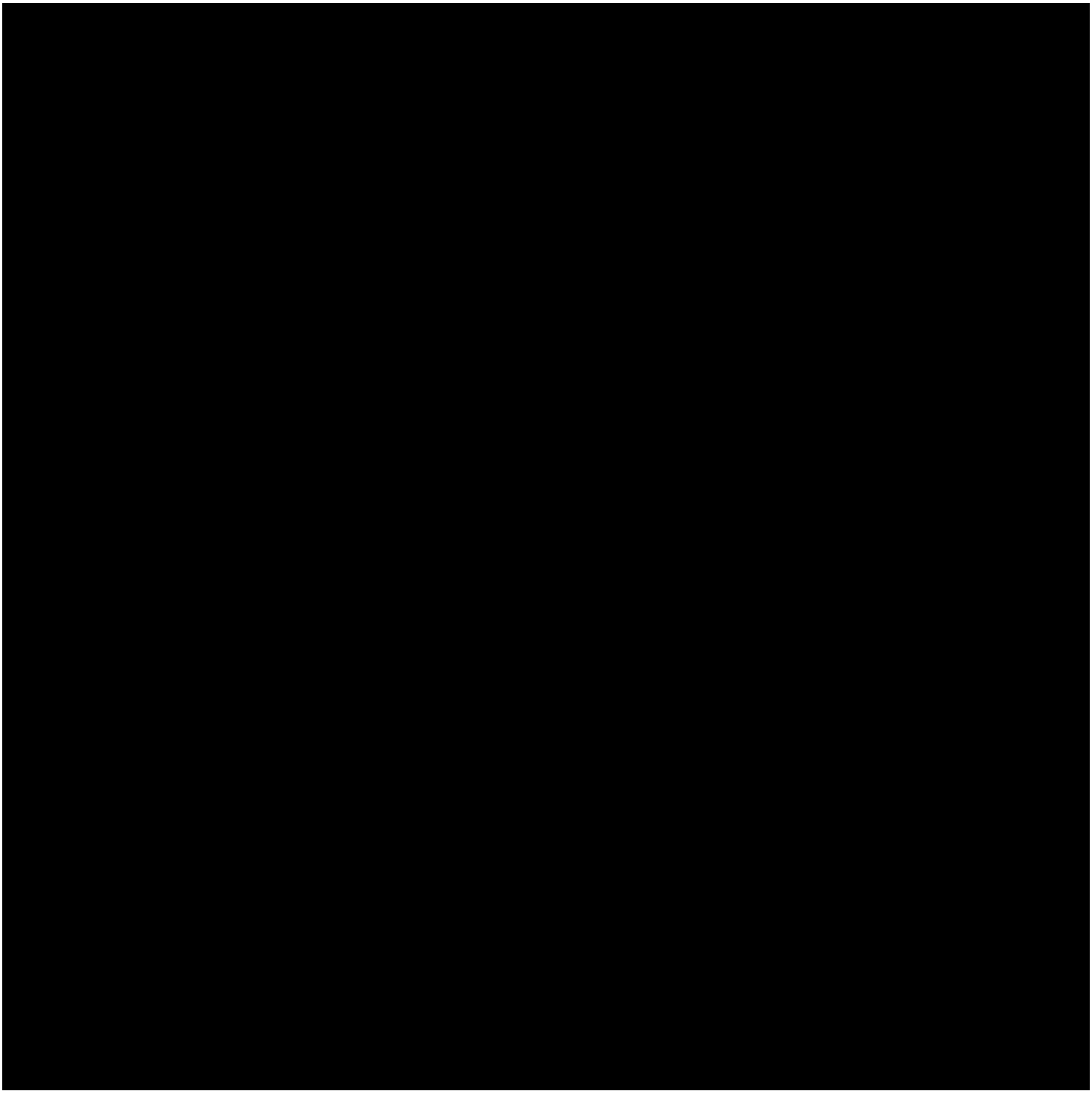


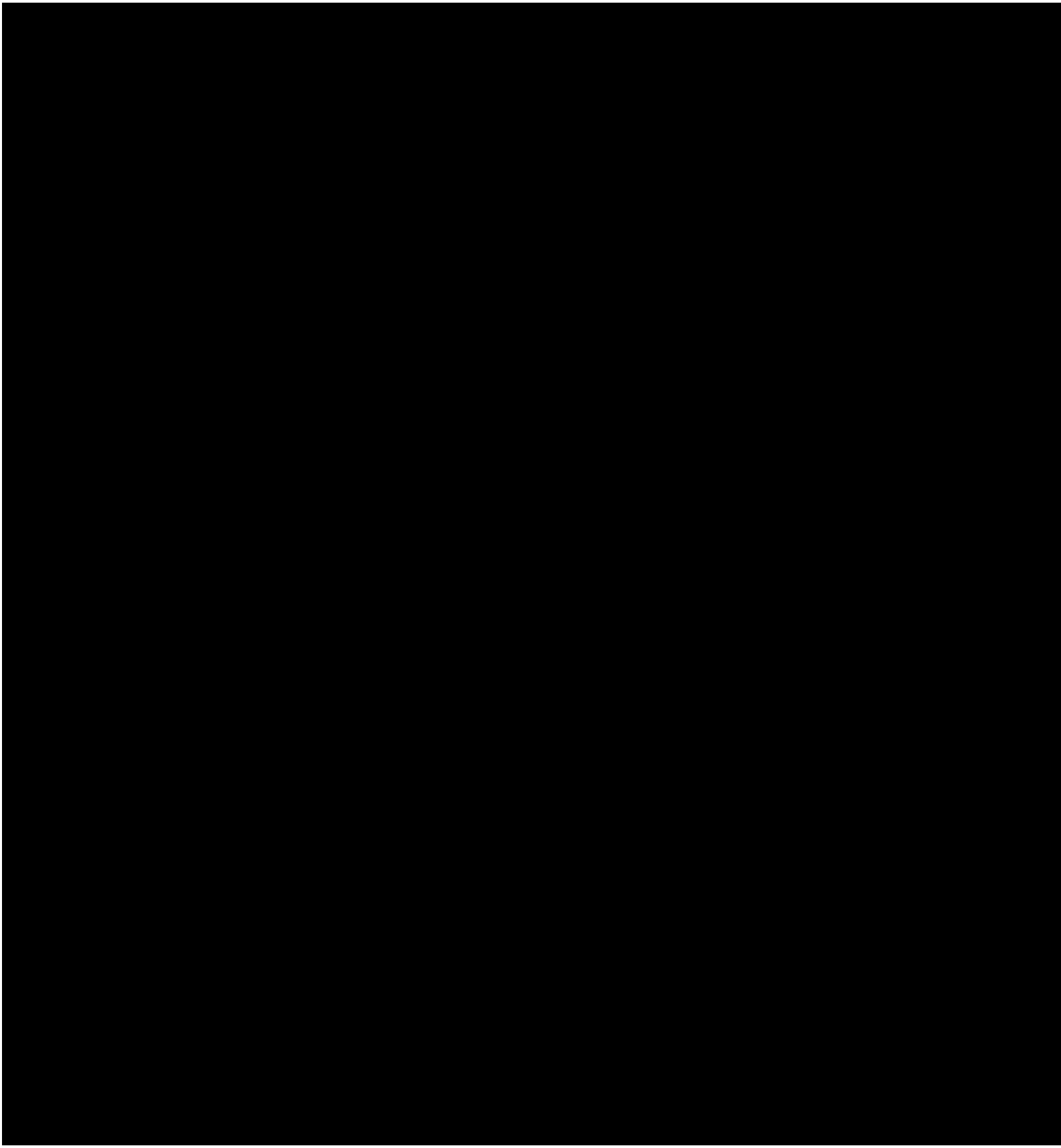


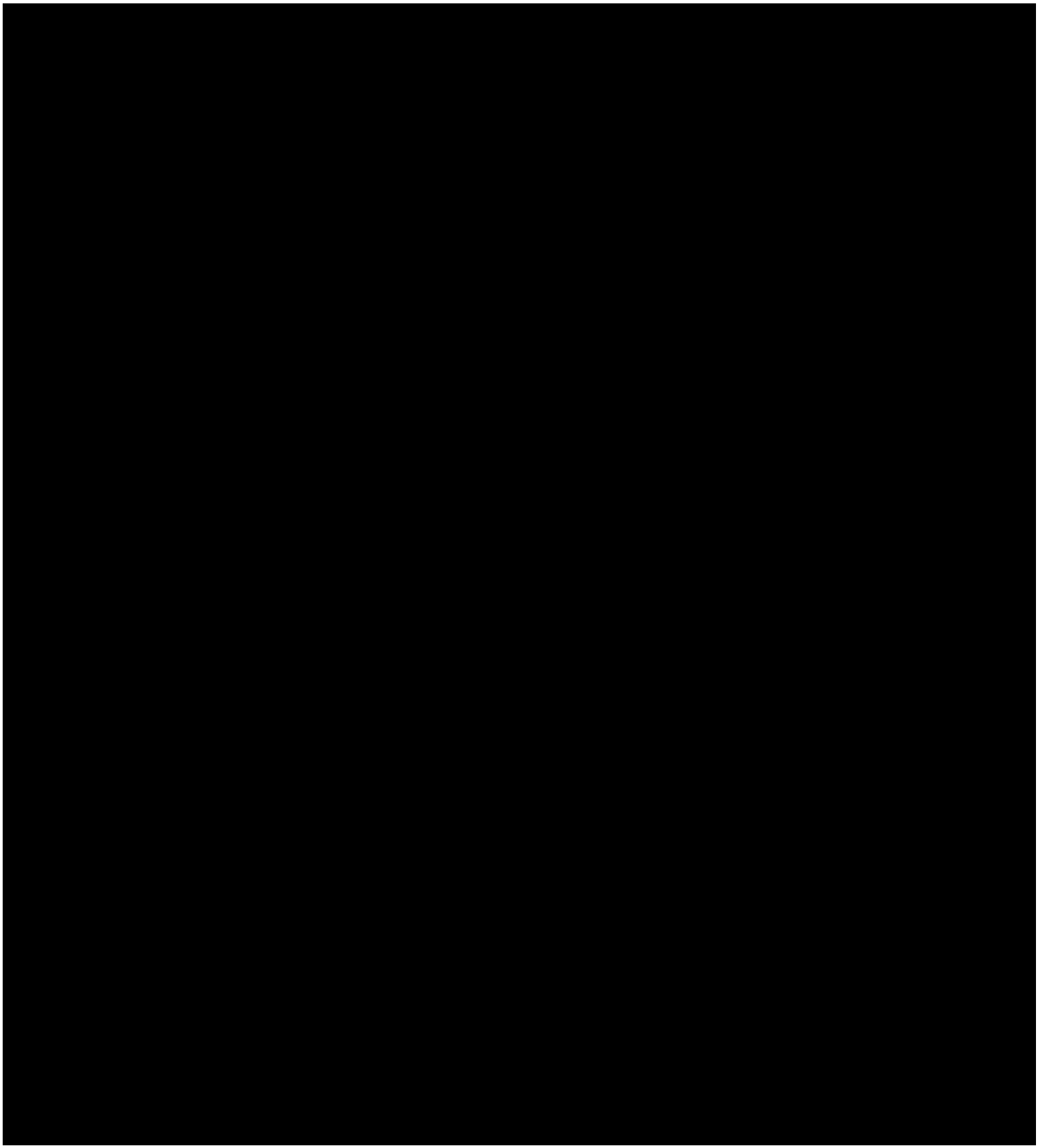


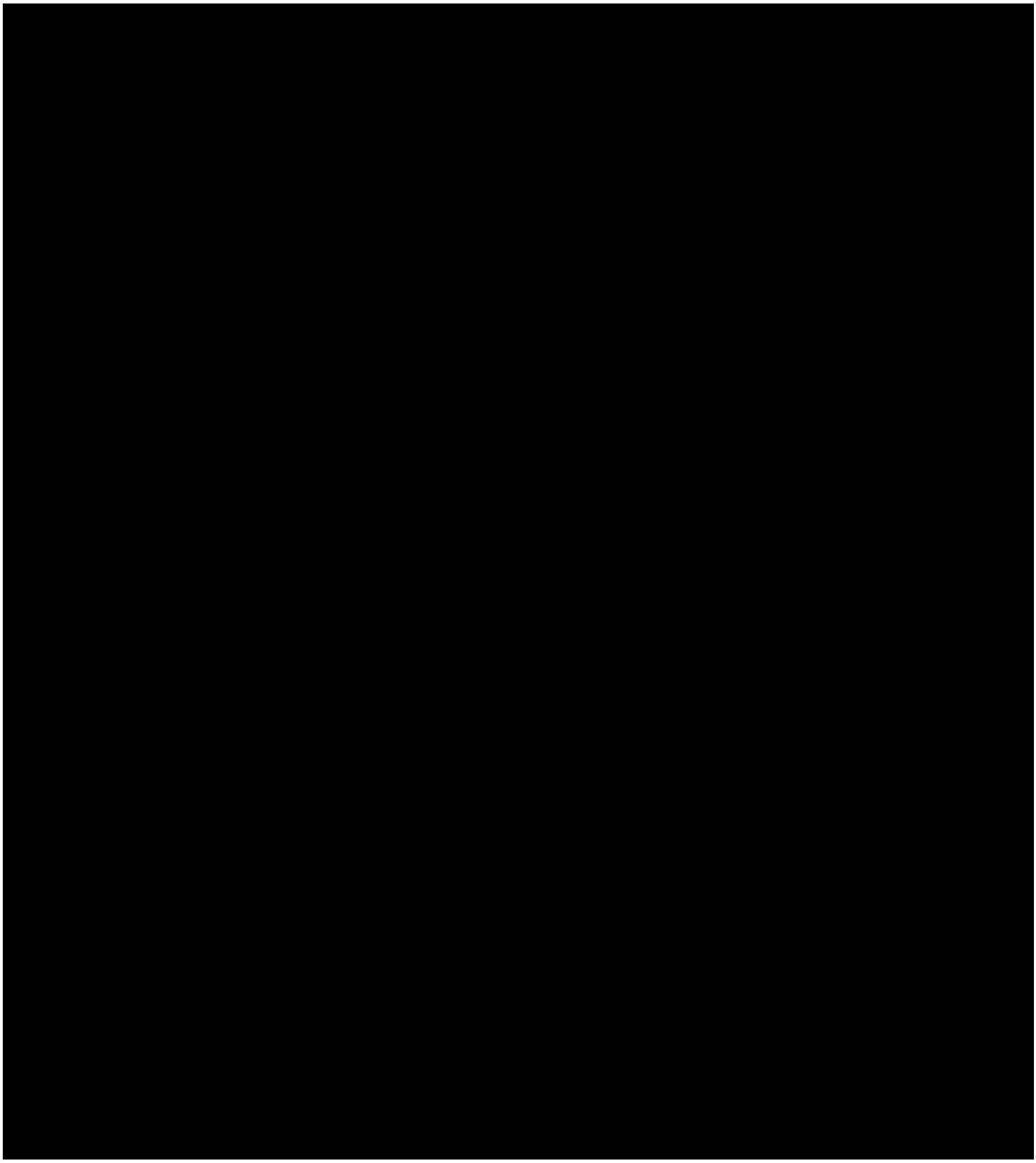


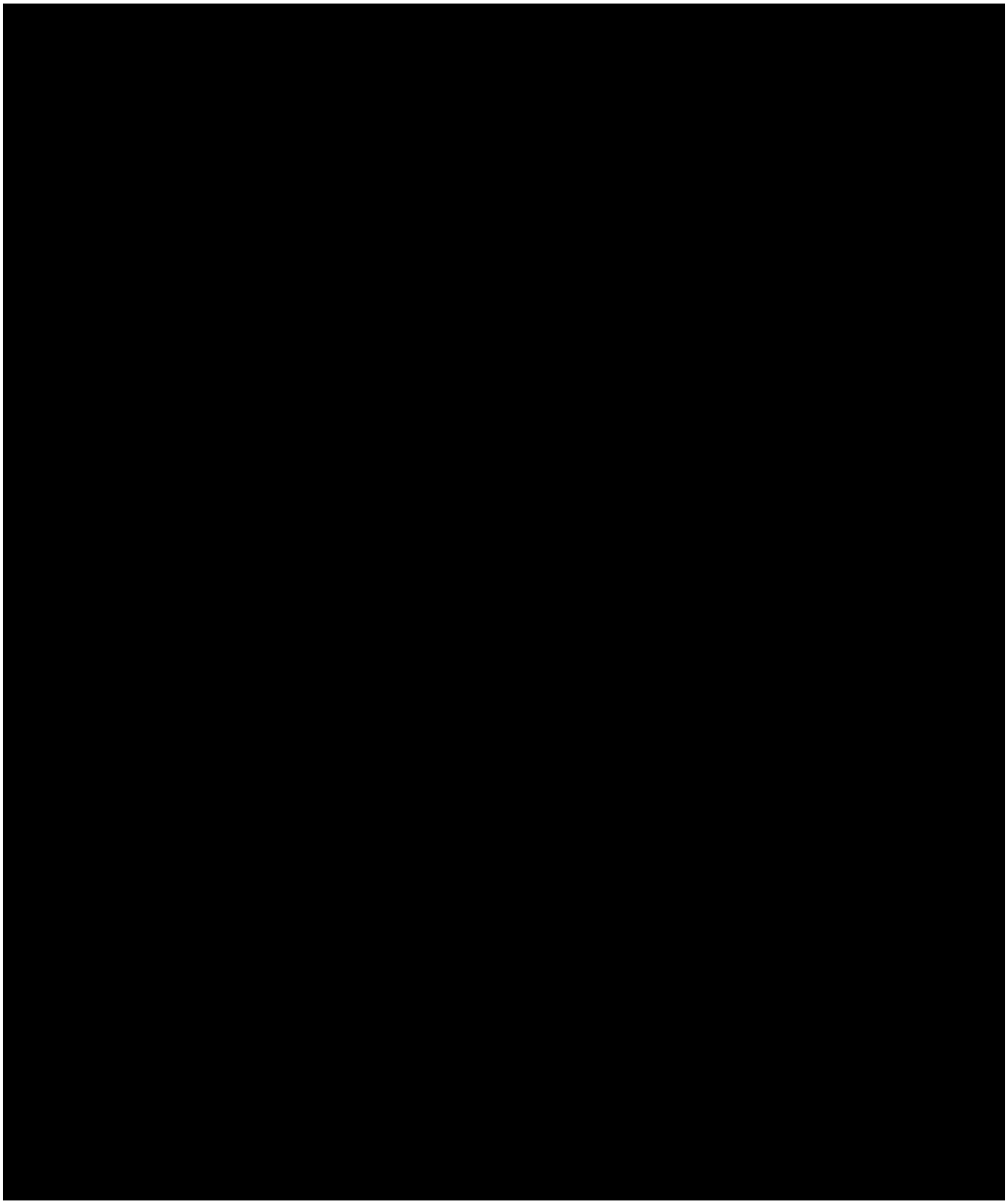






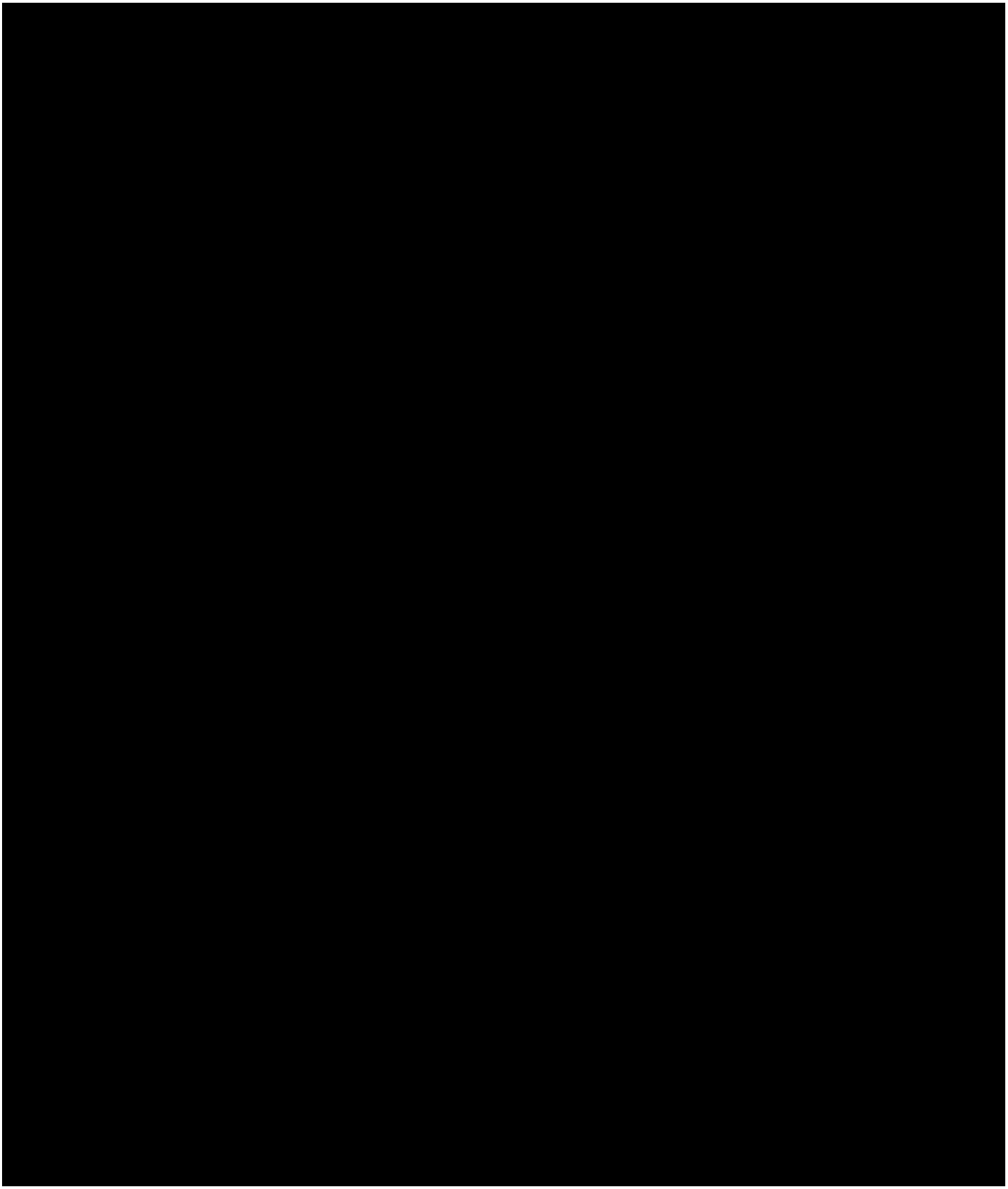


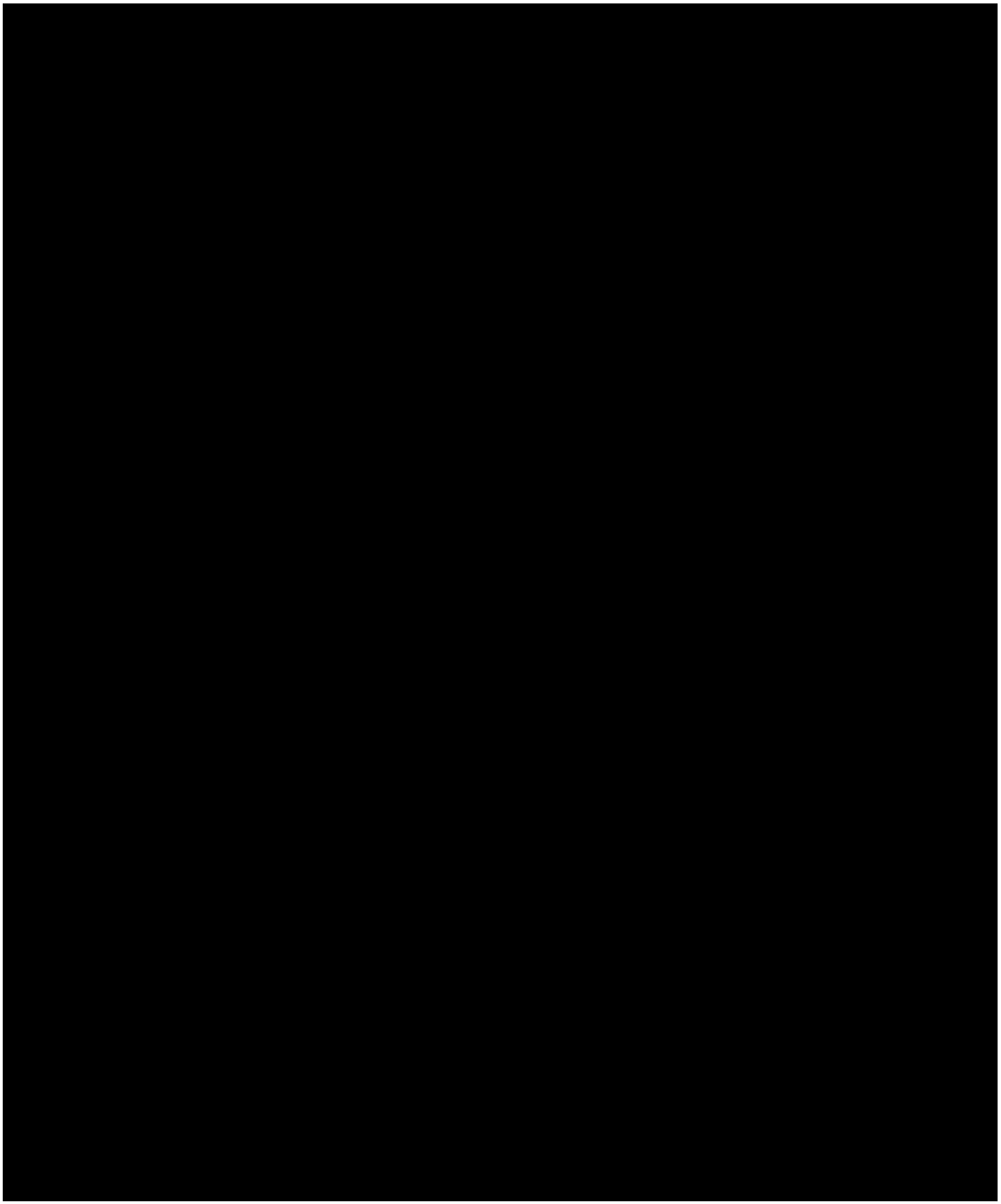


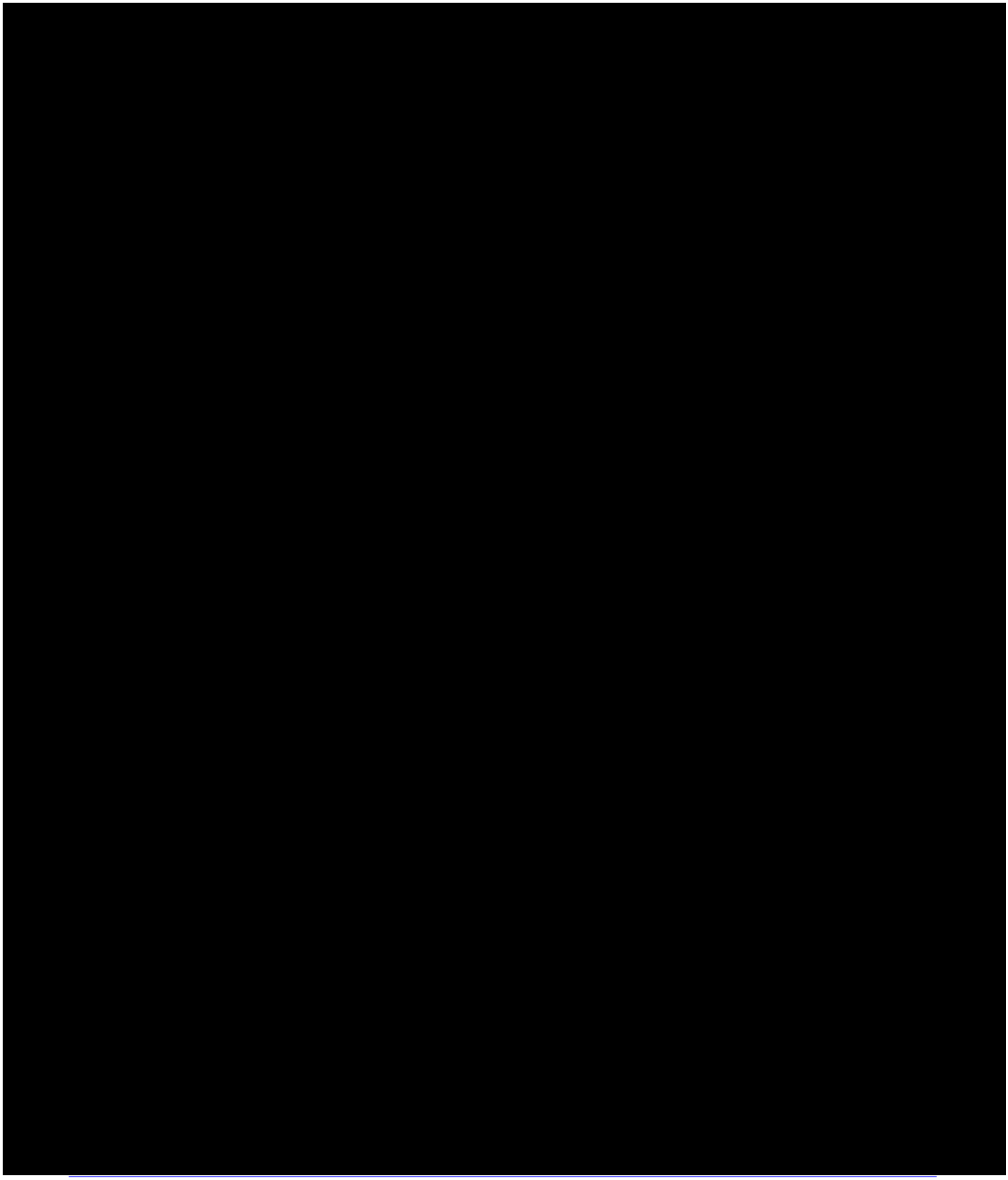


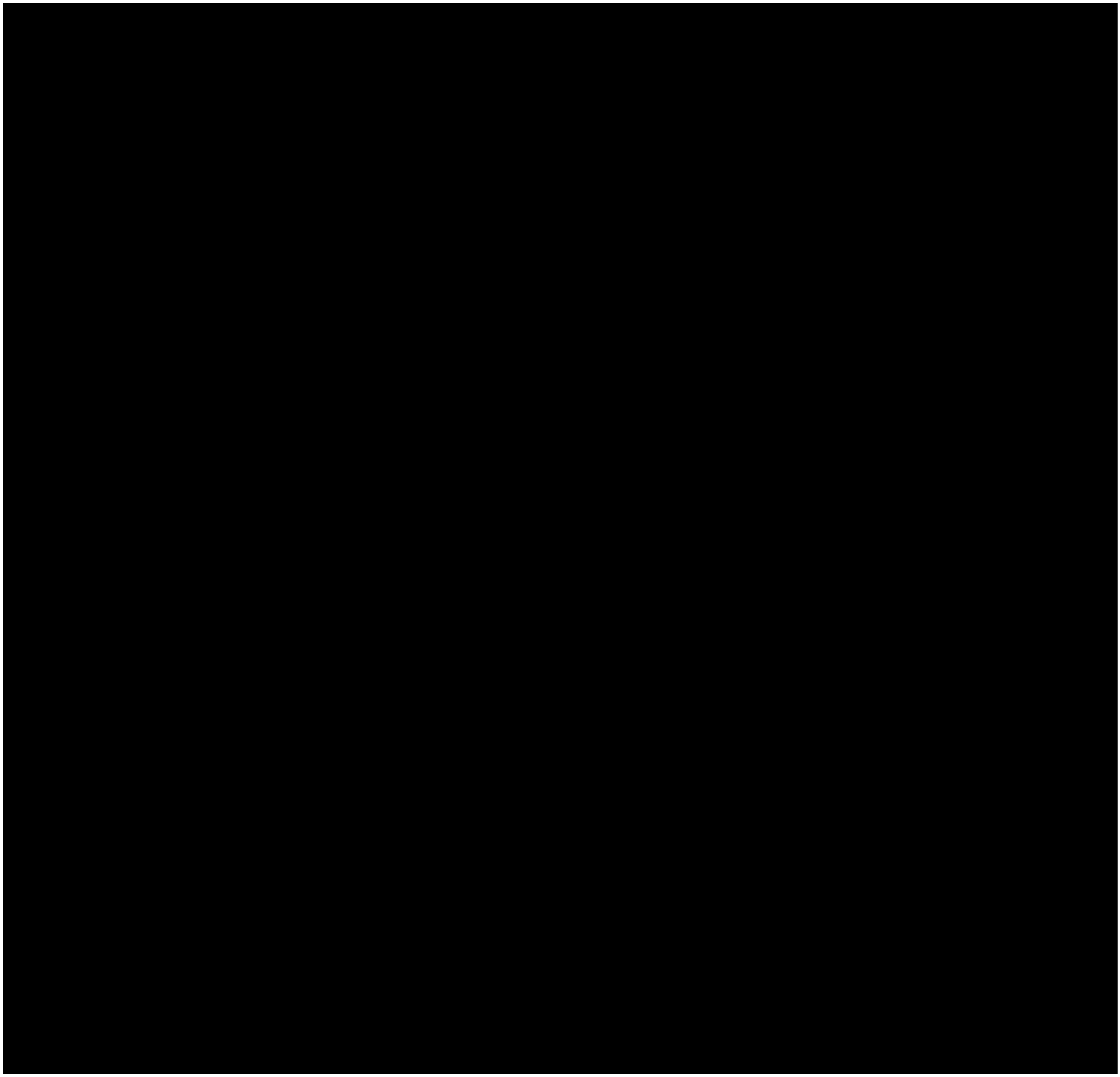
[redacted]

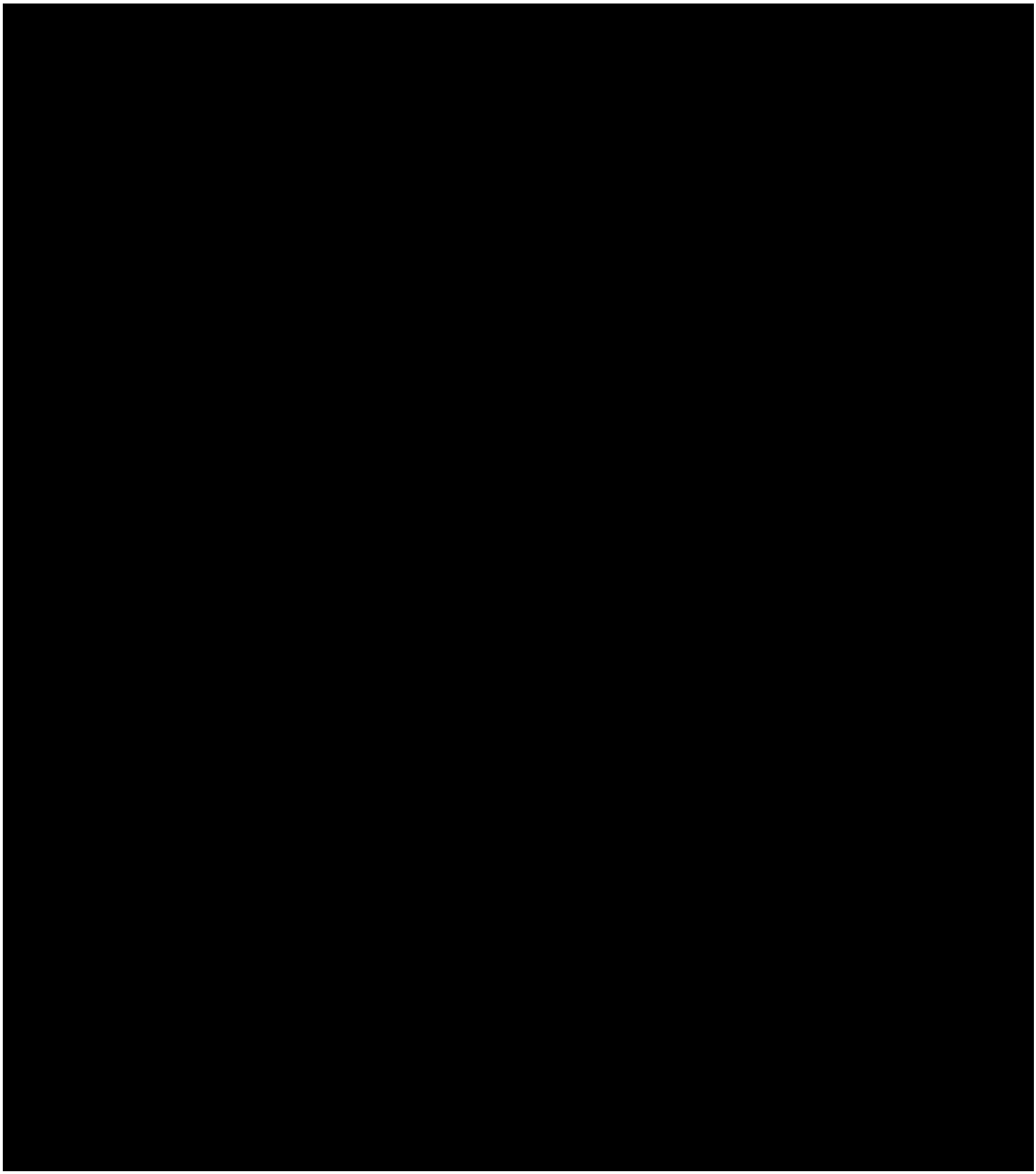
© Copyright IBM Corporation, 2013











Attachment F-6 – Sample Capacity Management Plan

This attachment provides a sample of a sample capacity management plan.

This page intentionally left blank.

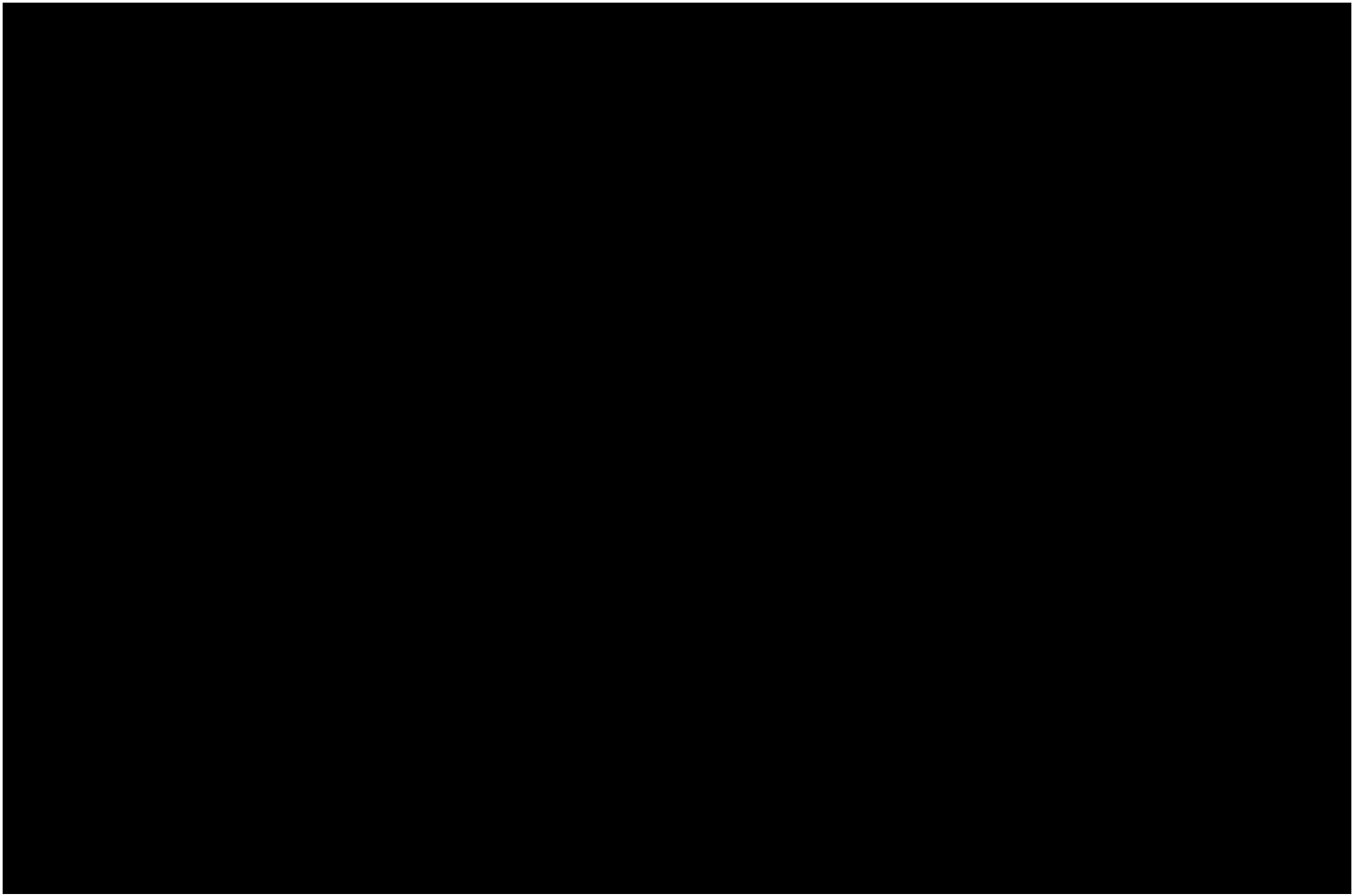
2013 Capacity Planning

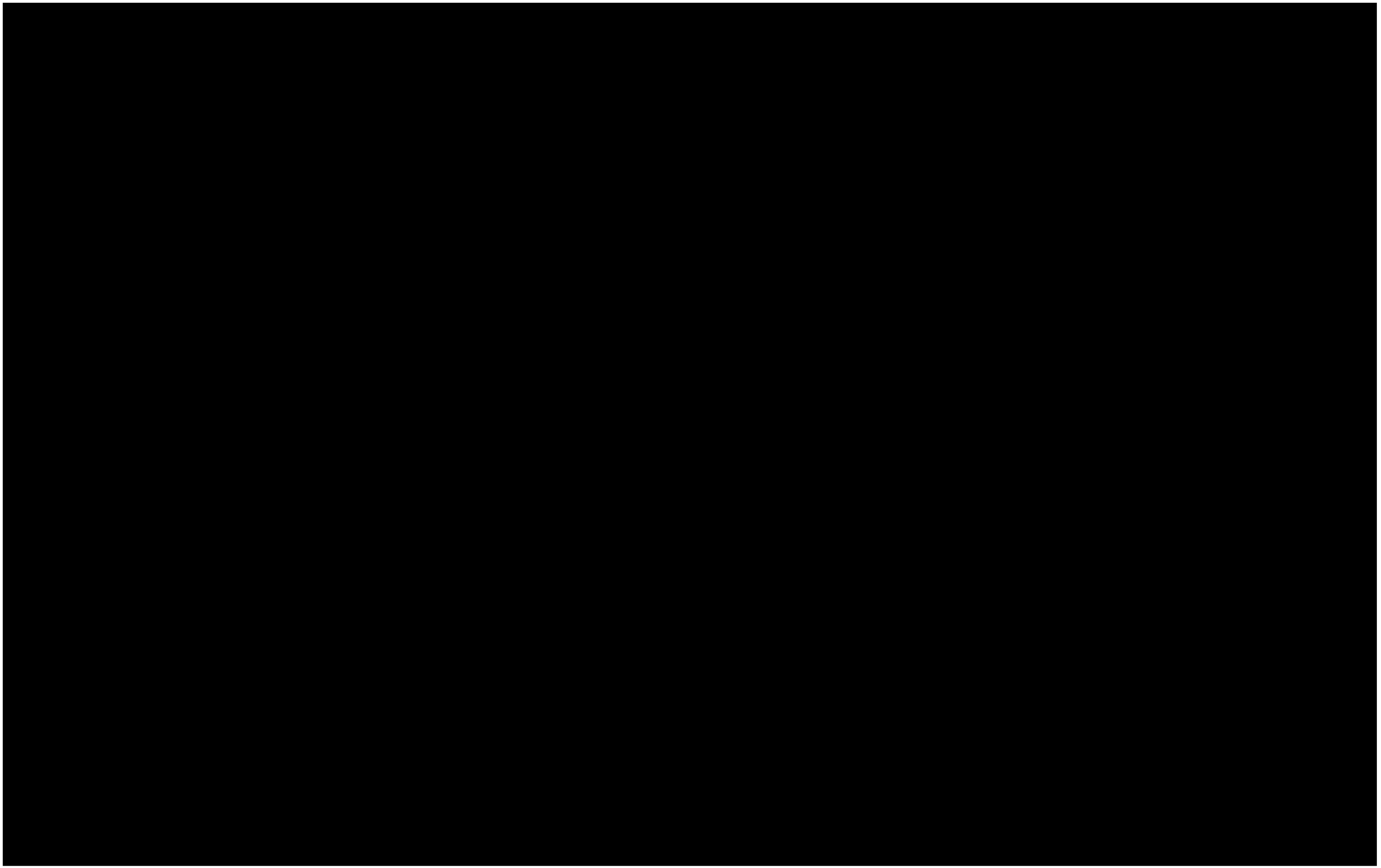
Data PowerHouse Project

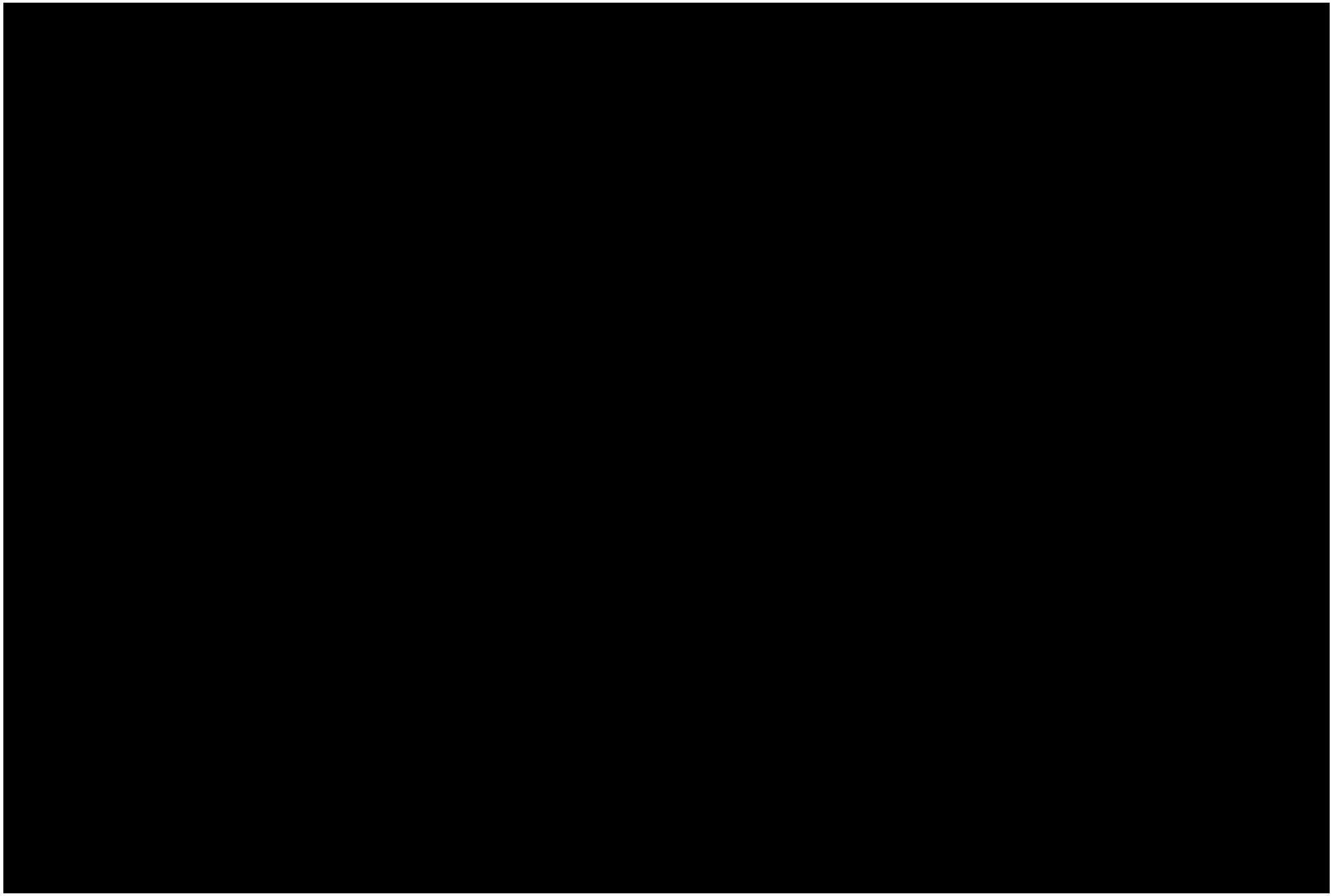
Enterprise Report

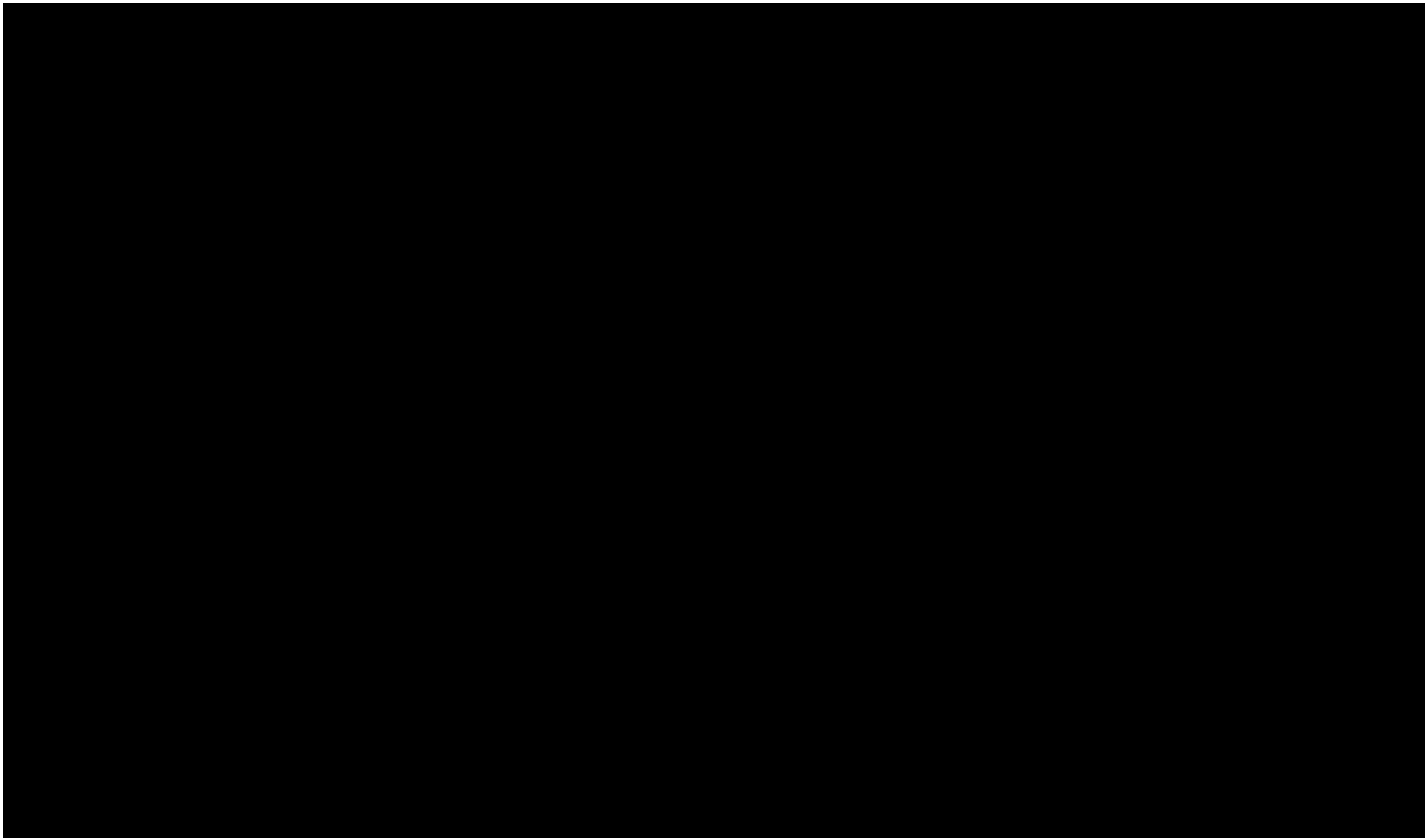
April 30, 2013

UNISYS





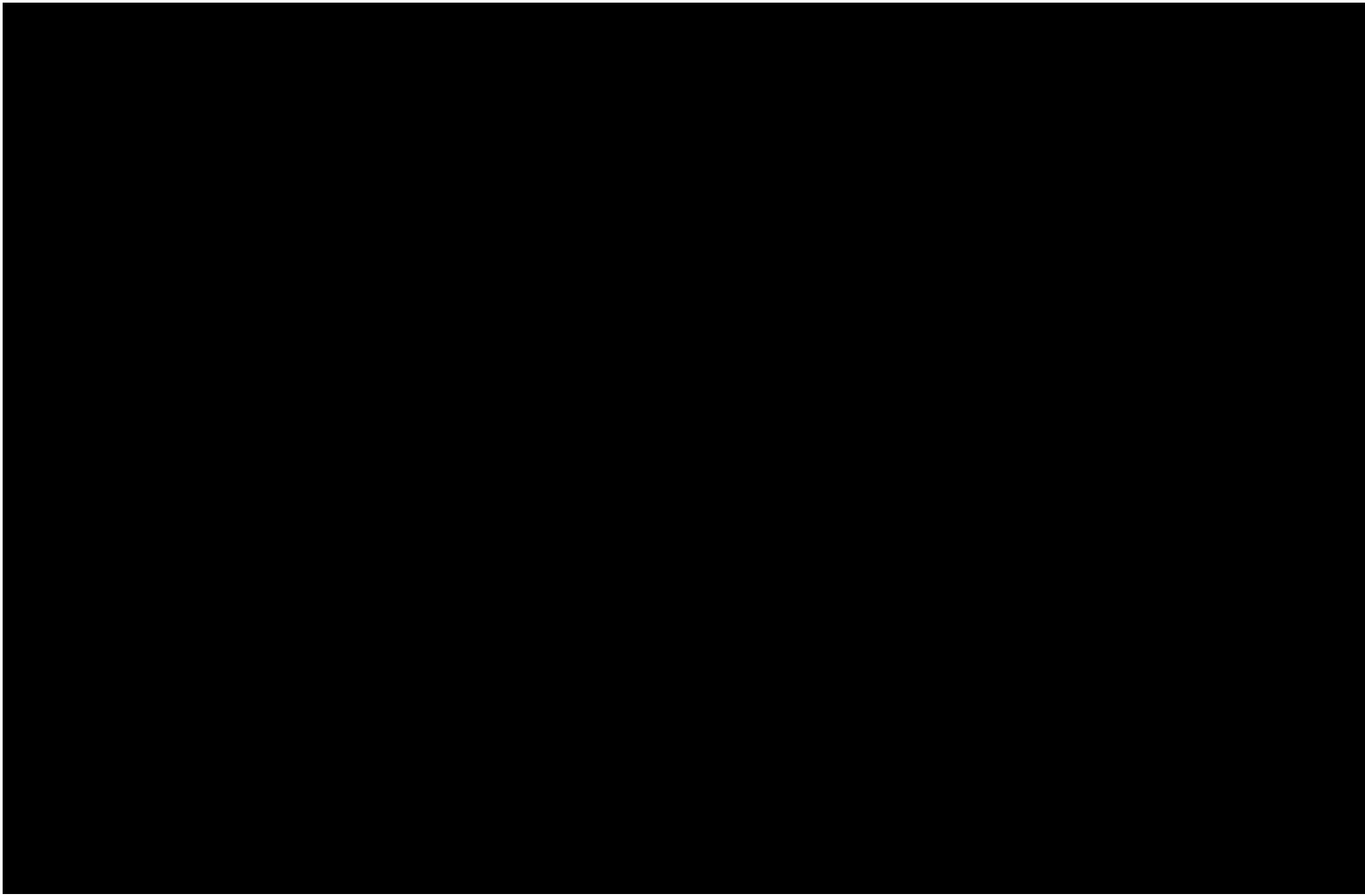


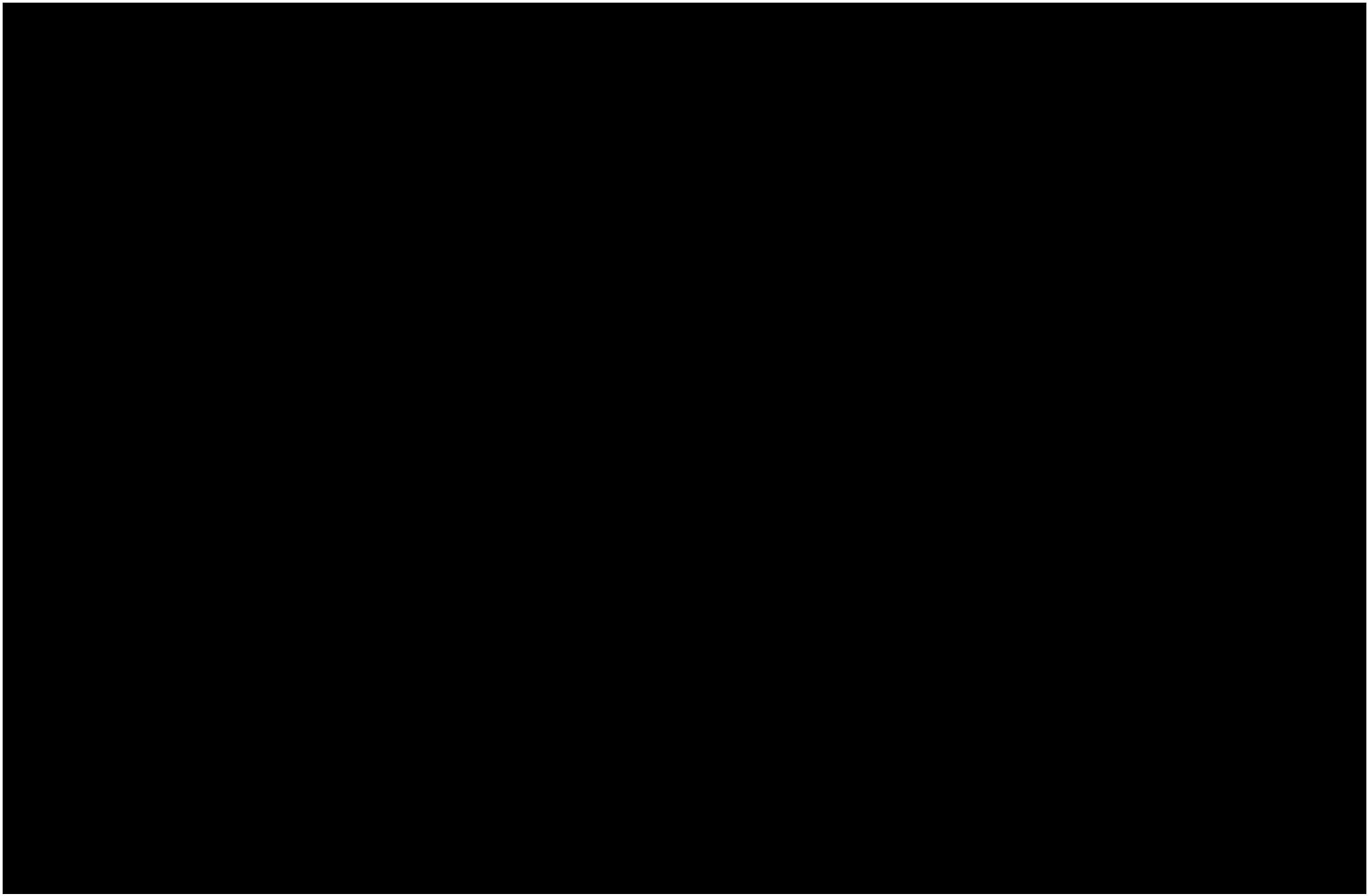


© 2012 Unisys Corporation. All

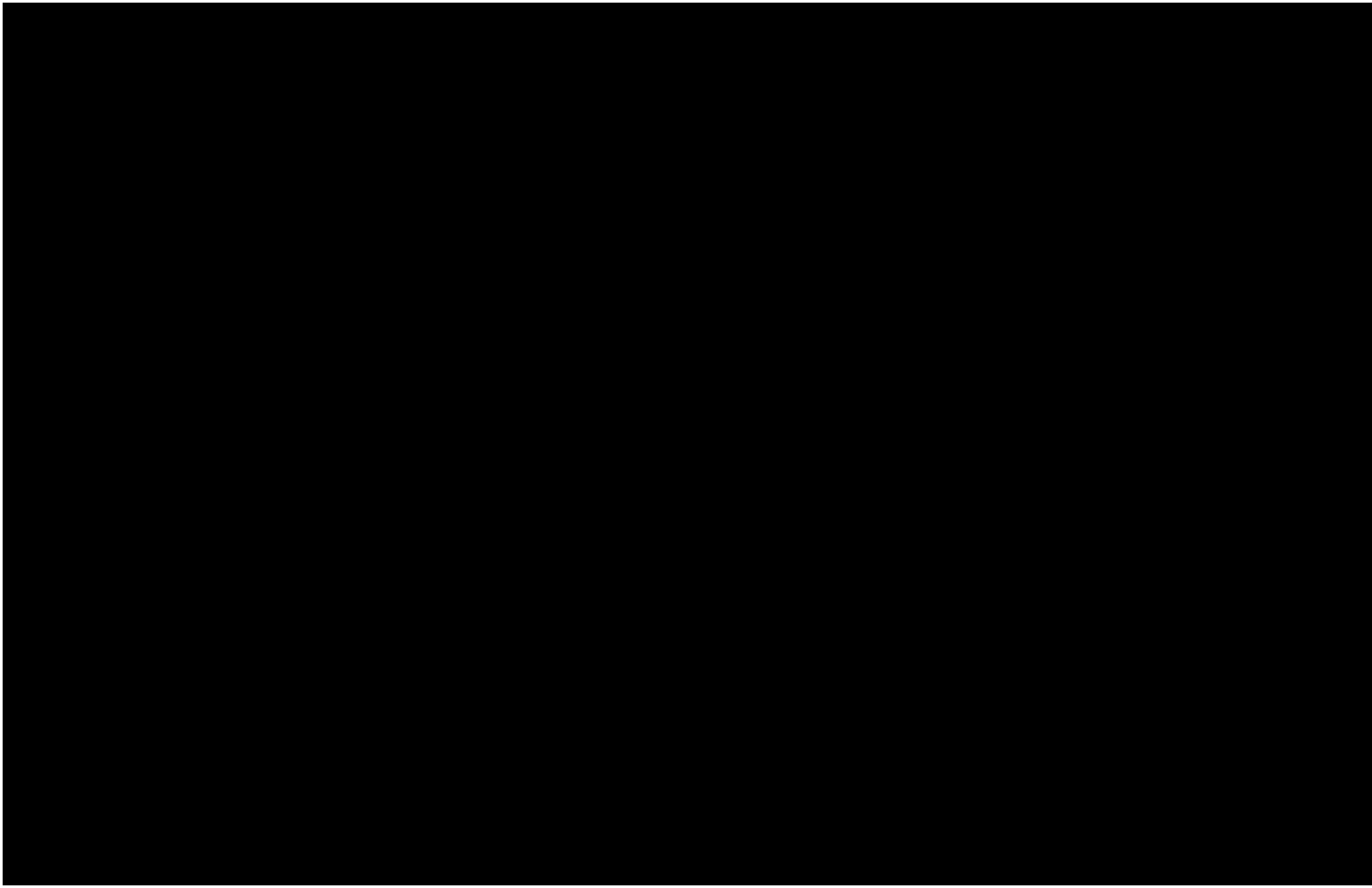
[redacted]

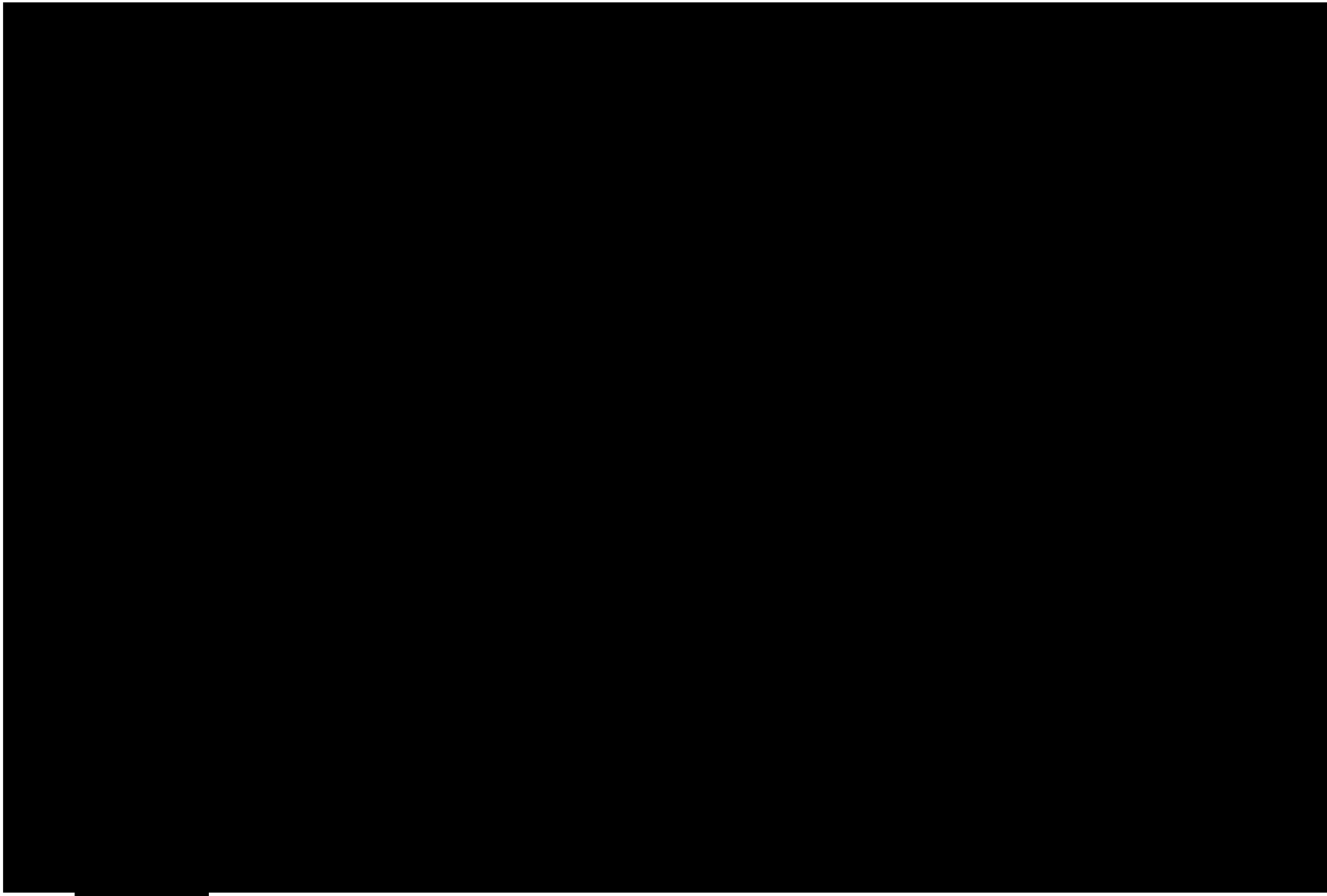
UNISYS



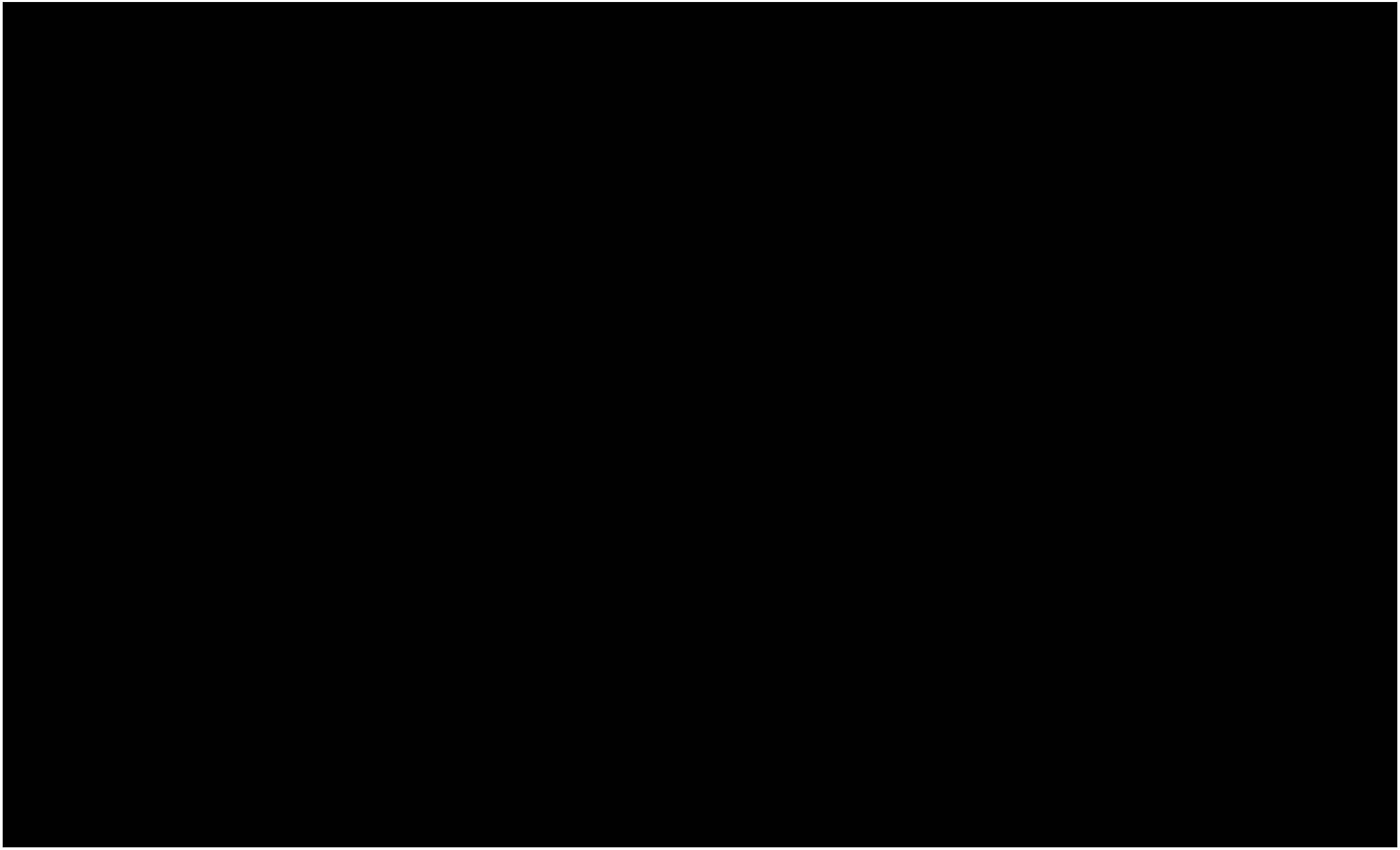


© 2012 Unisys Corporation. All rights reserved.

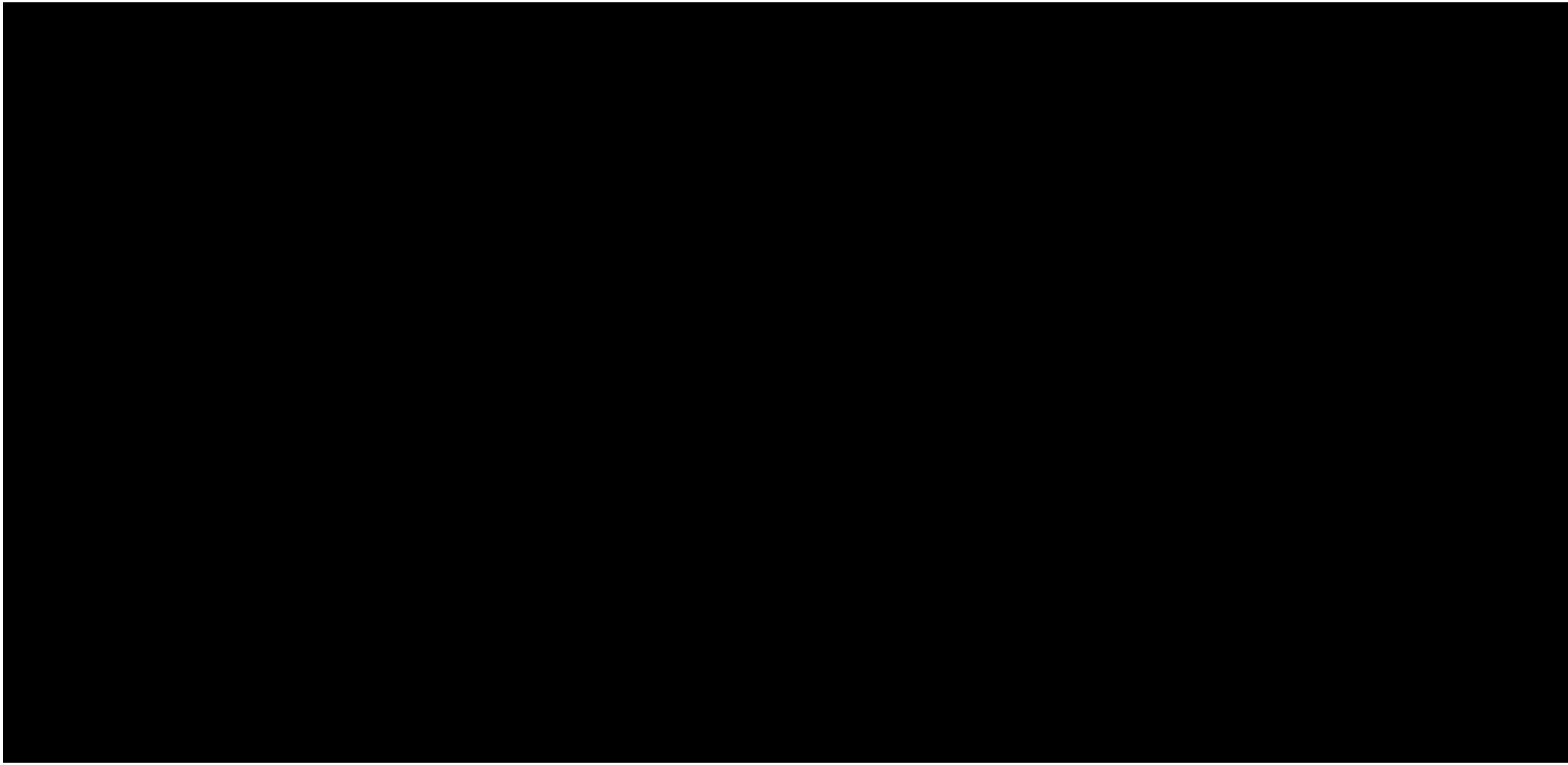


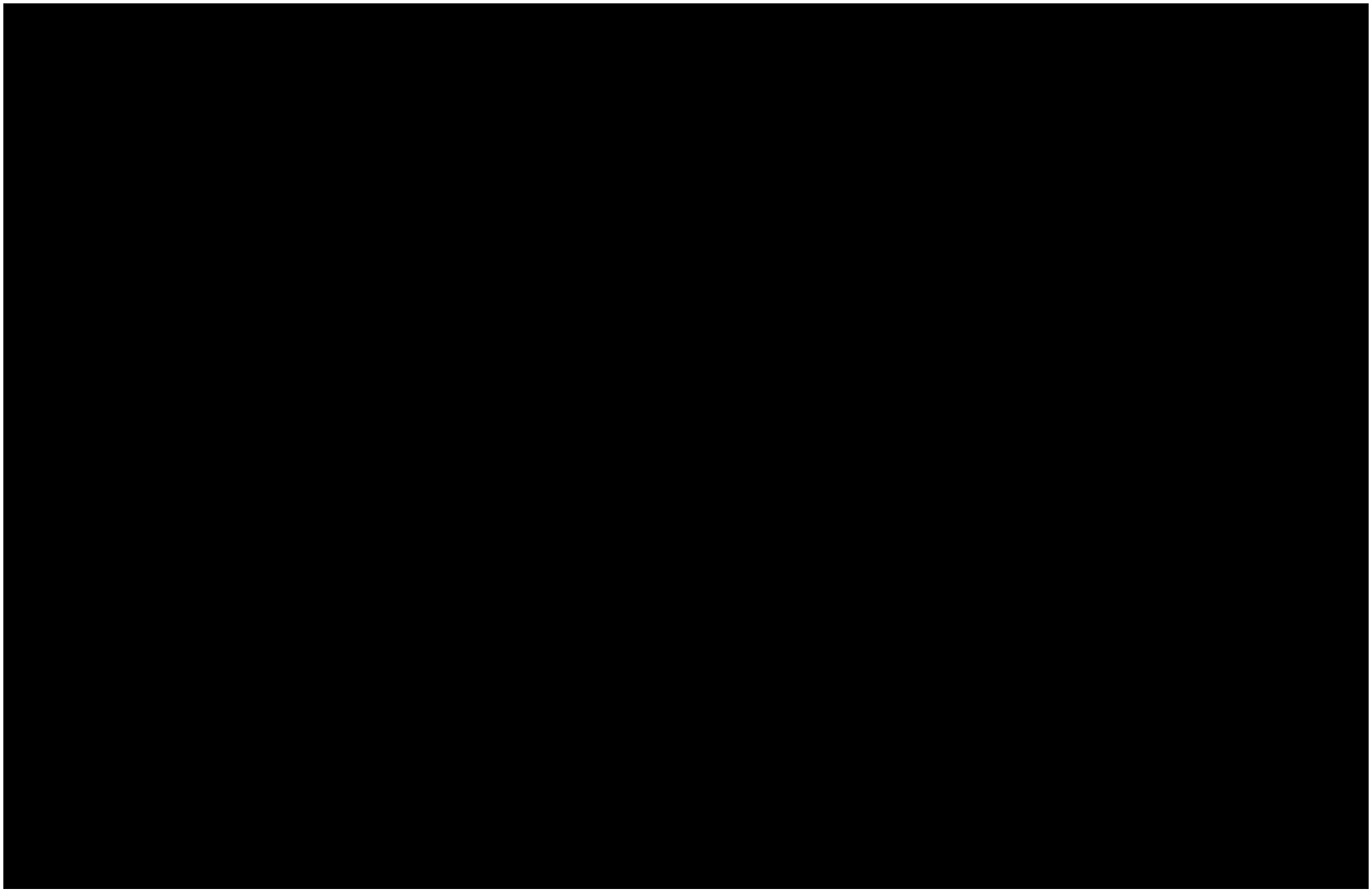


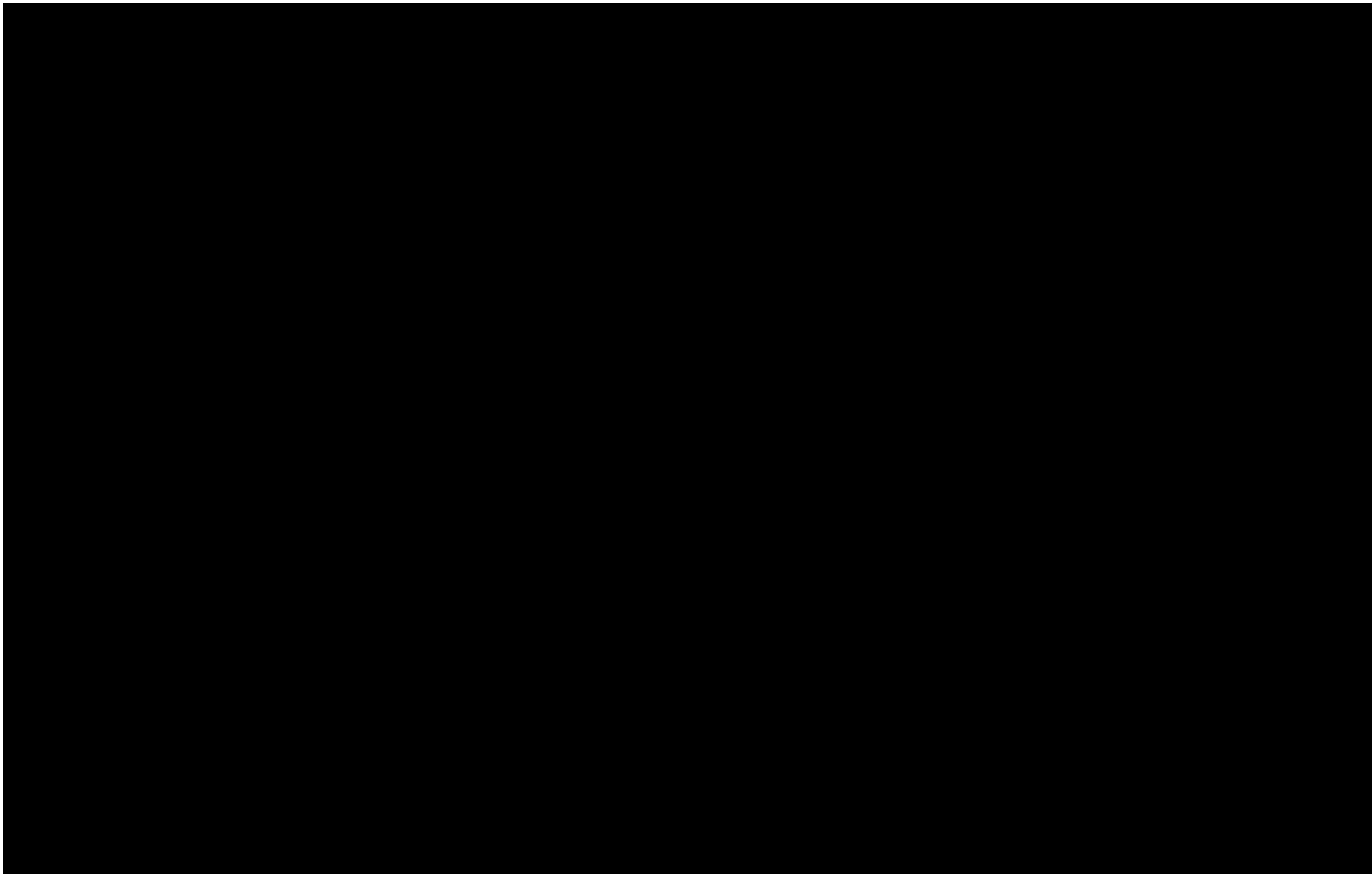
© 2012 Unisys Corporation. All rights reserved.

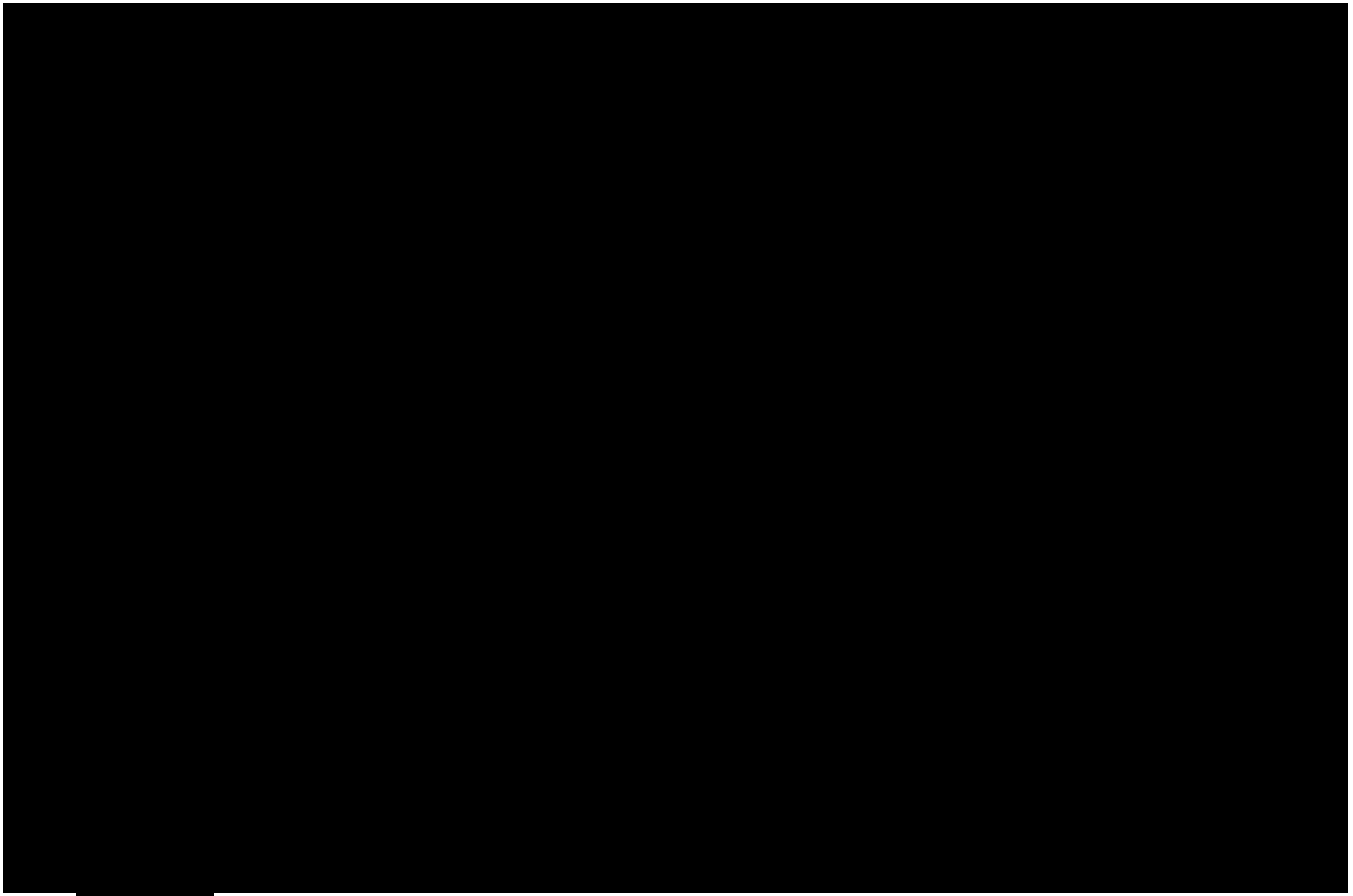


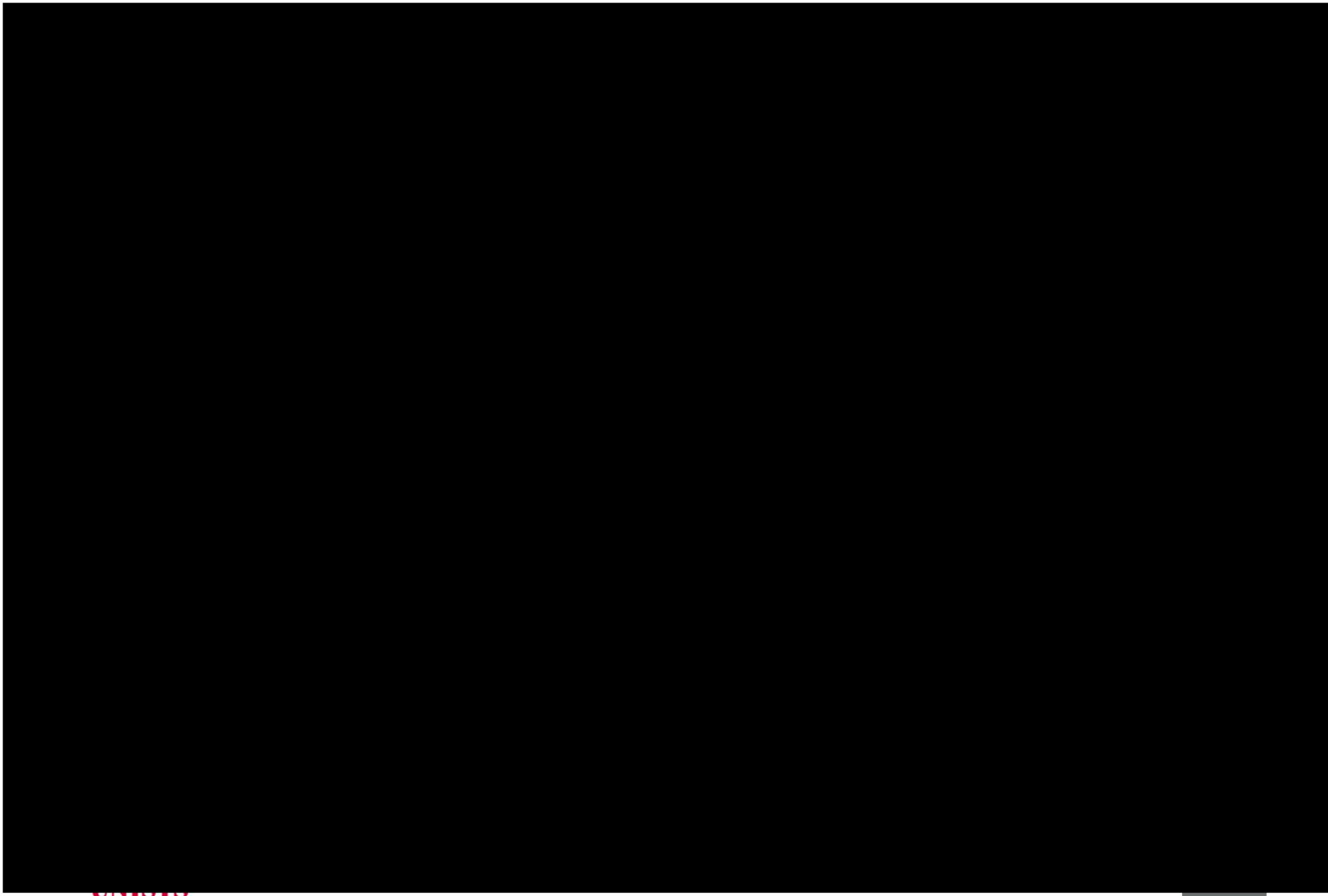
UNISYS



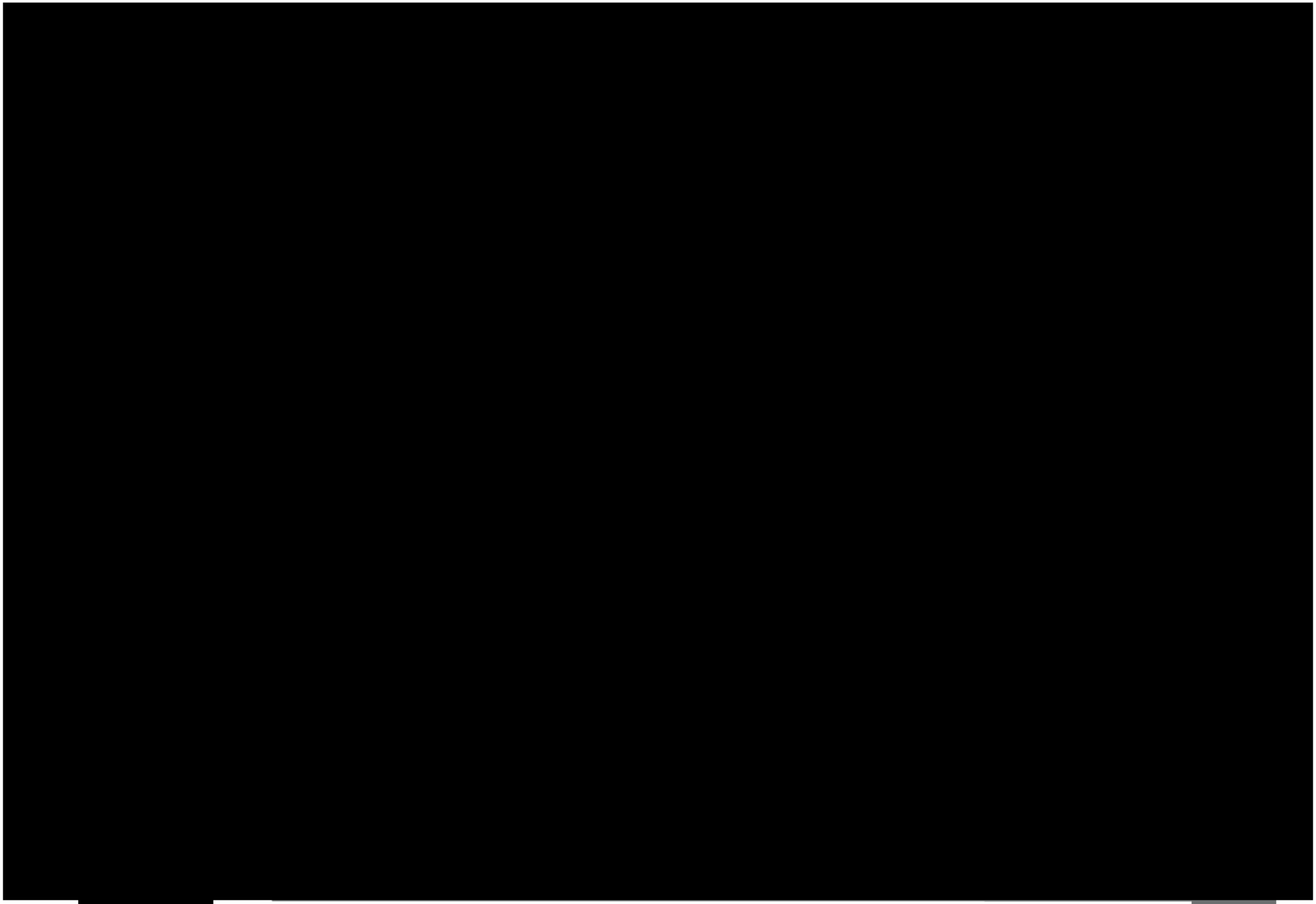




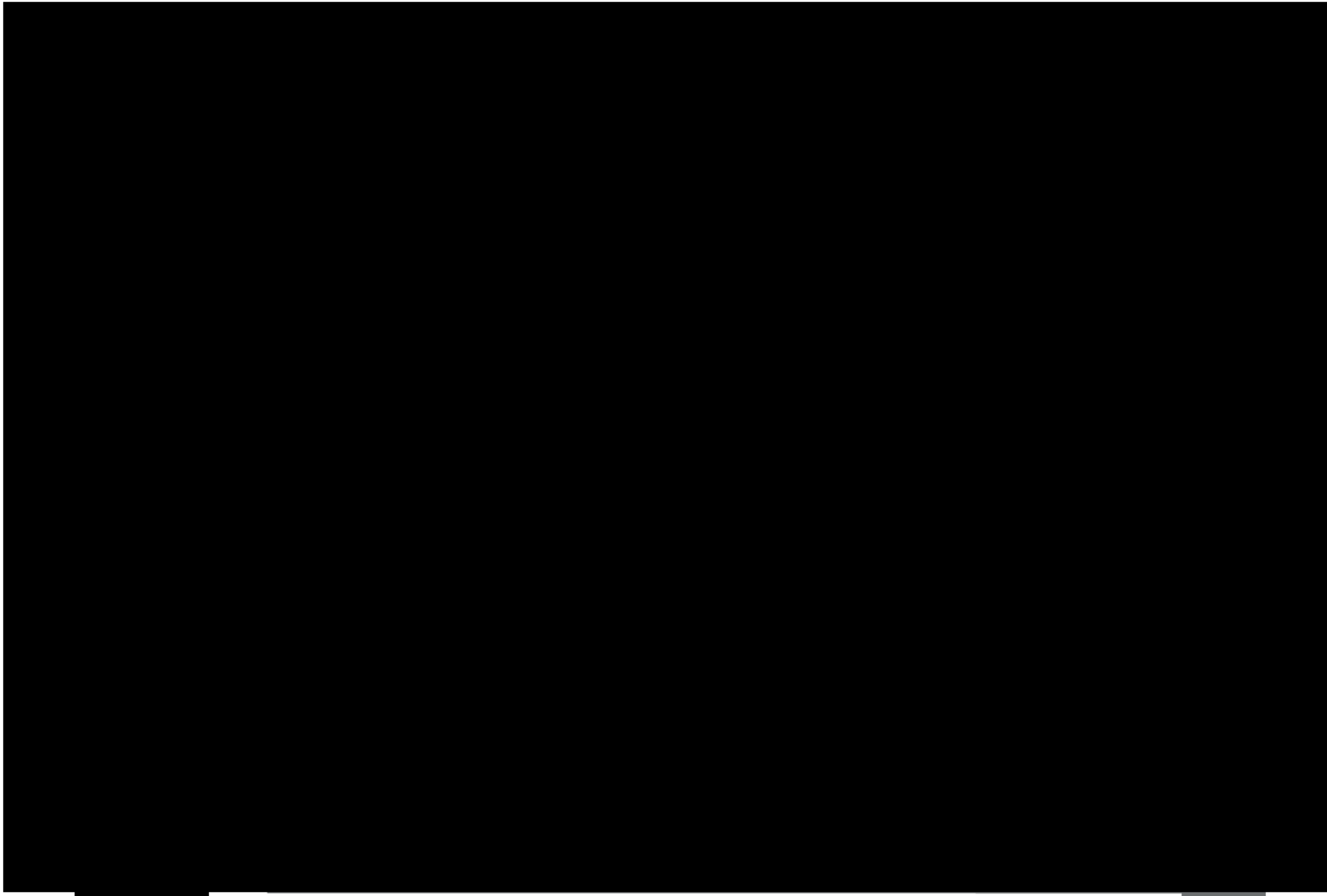




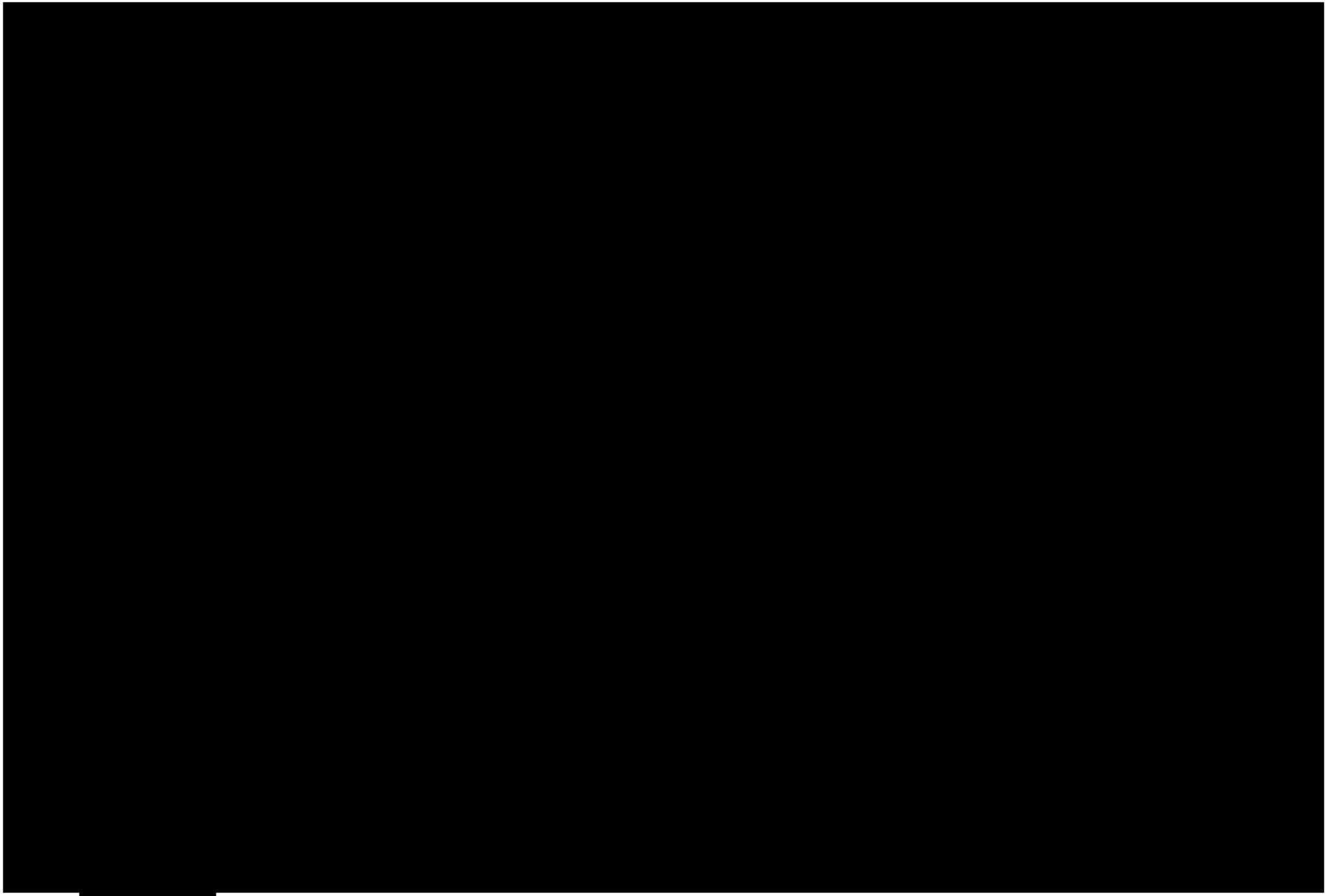
© 2012 Unisys Corporation. All rights reserved.



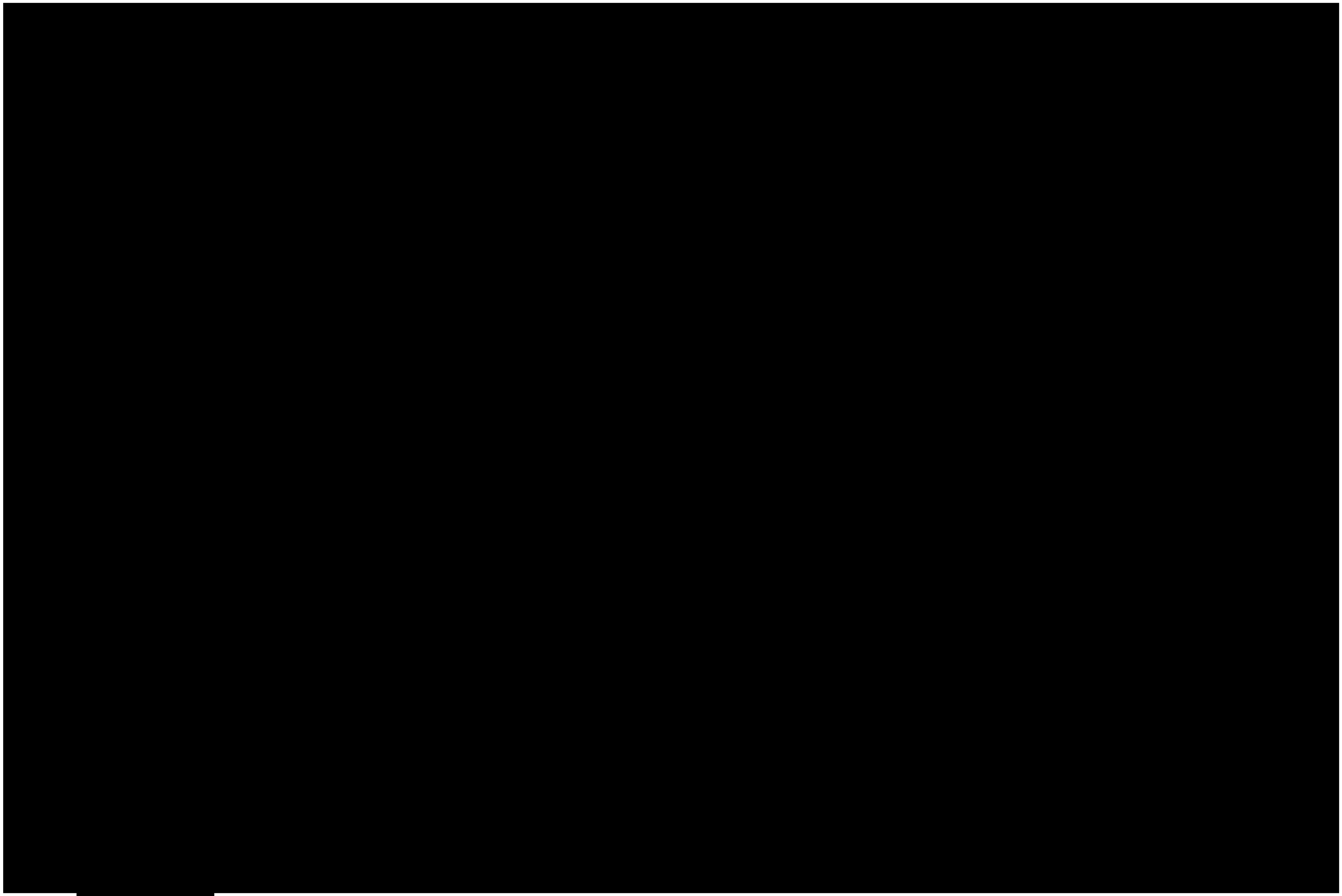
© 2012 Unisys Corporation. All rights reserved.



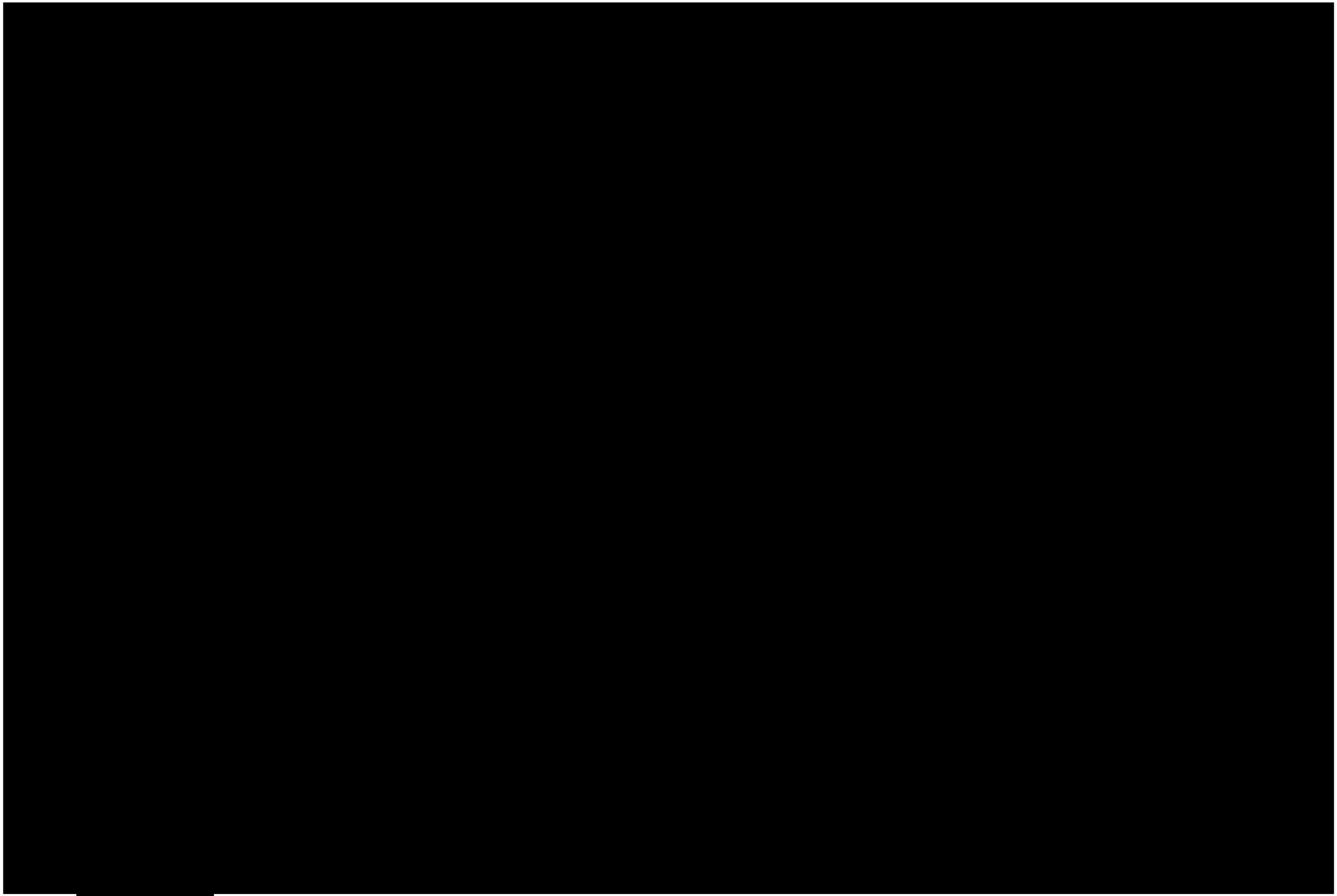
© 2012 Unisys Corporation. All rights reserved.



© 2012 Unisys Corporation. All rights reserved.

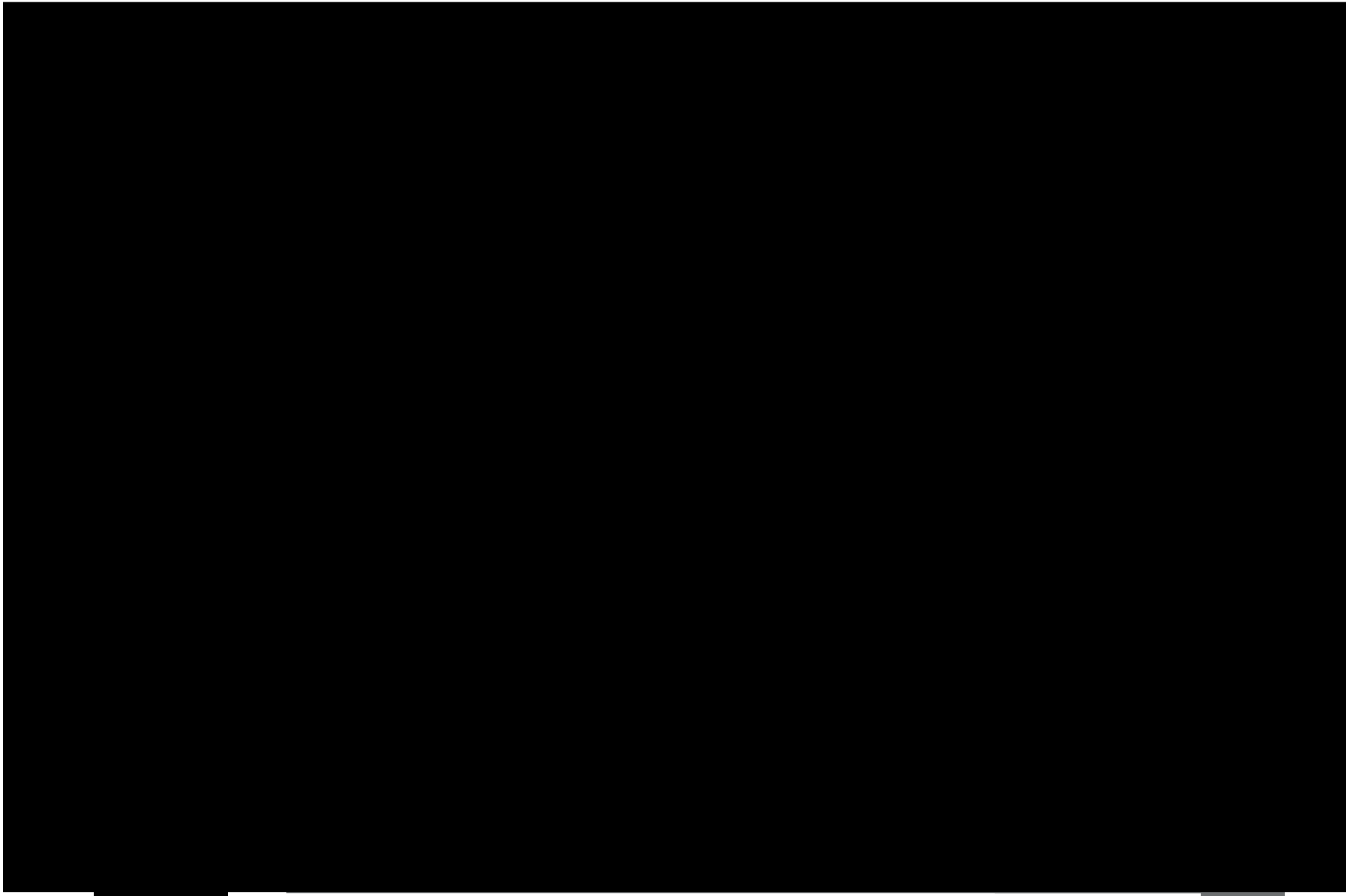


© 2012 Unisys Corporation. All rights reserved.



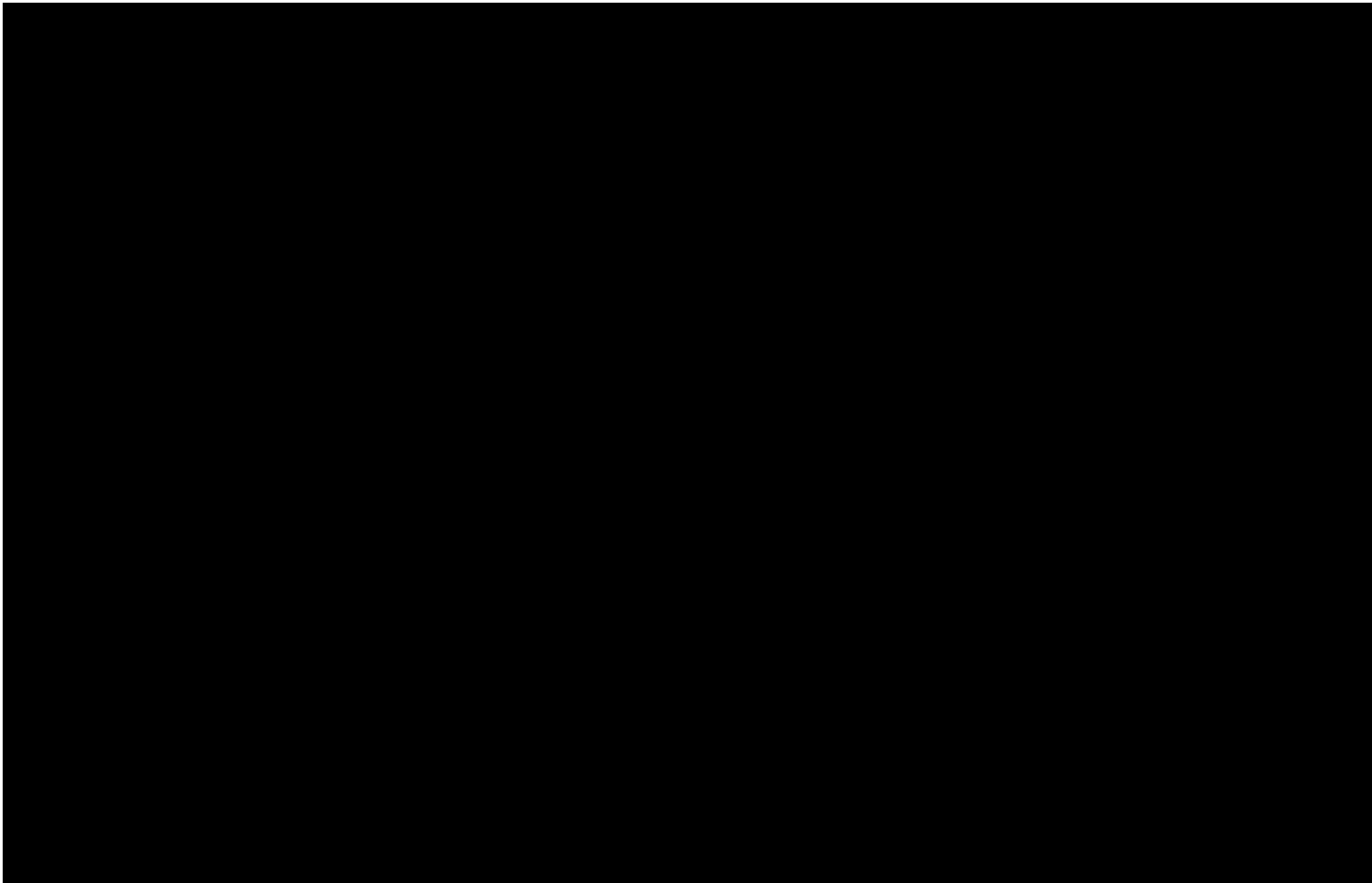
© 2012 Unisys Corporation. All rights reserved.

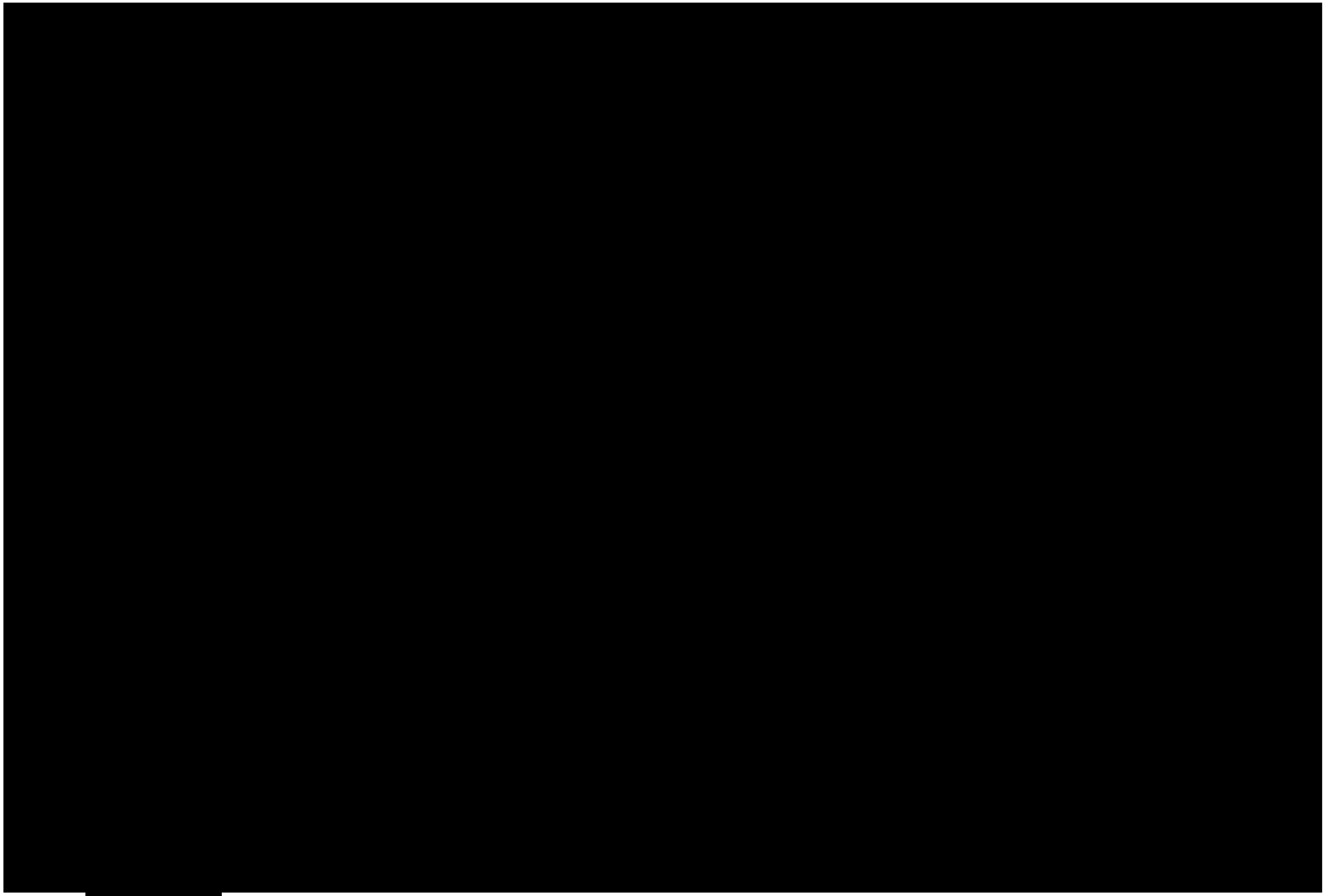
© 2012 Unisys Corporation. All rights reserved.



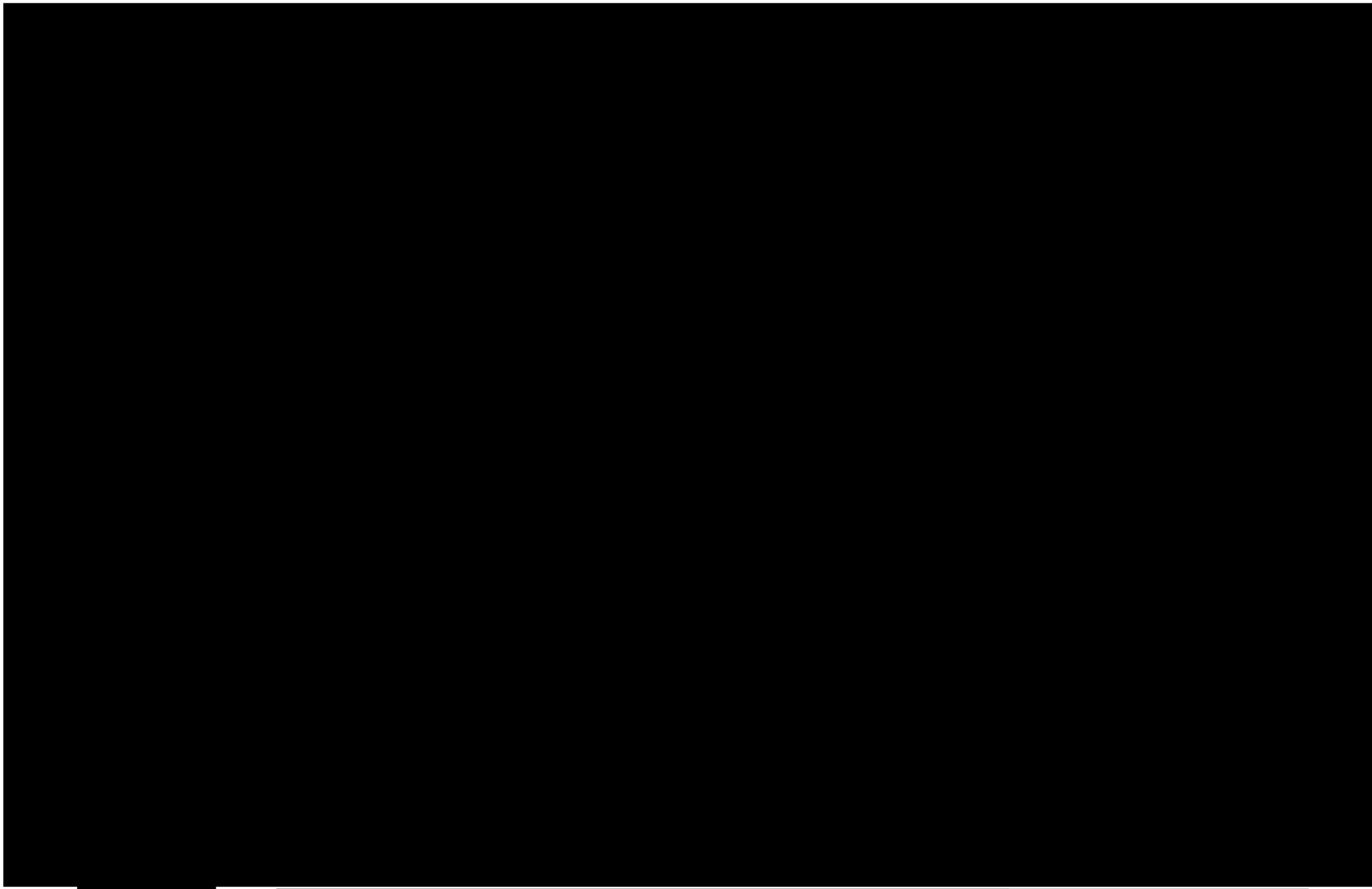
© 2012 Unisys Corporation. All rights reserved.

[redacted]

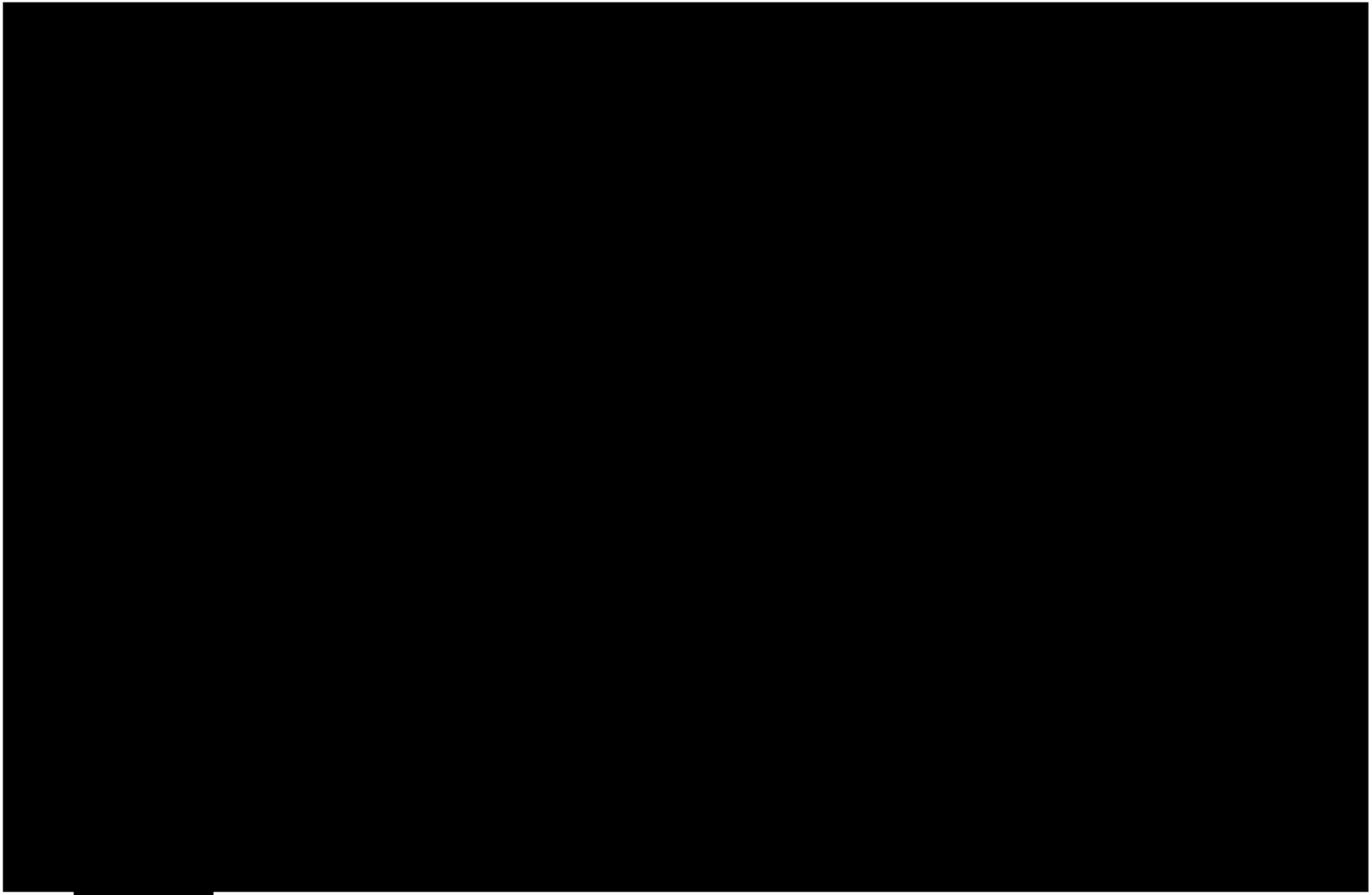




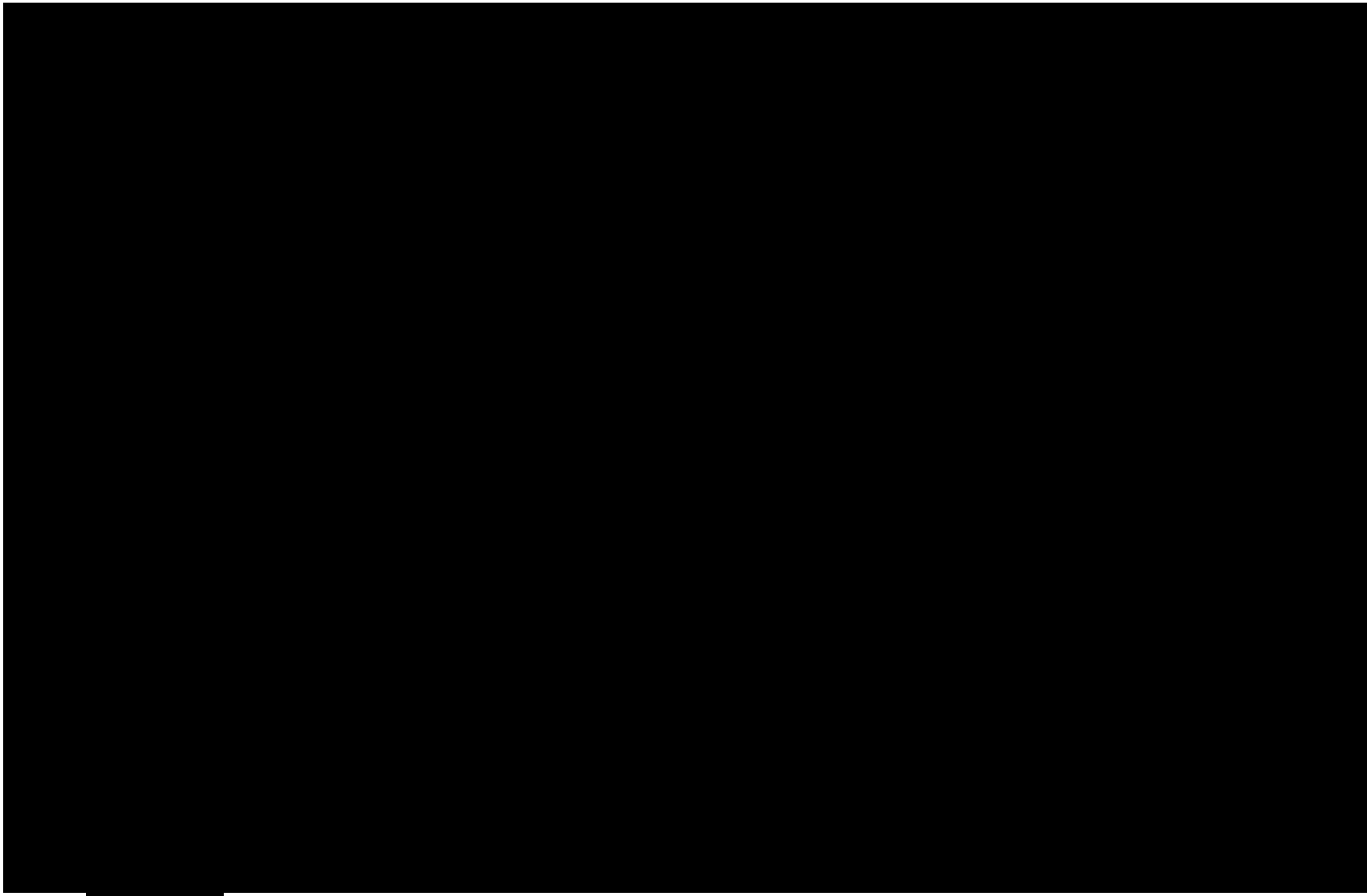
© 2012 Unisys Corporation. All rights reserved.

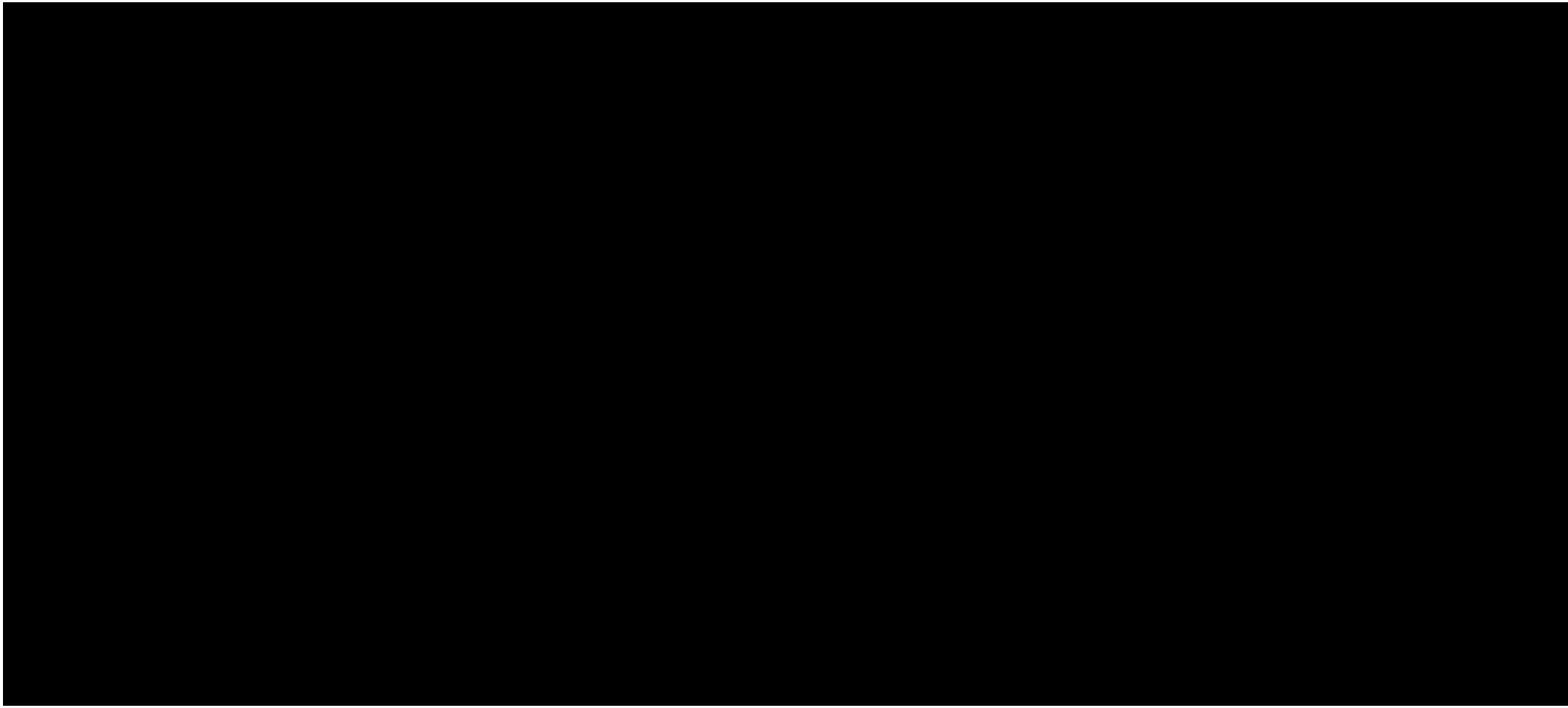


© 2012 Unisys Corporation. All rights reserved.

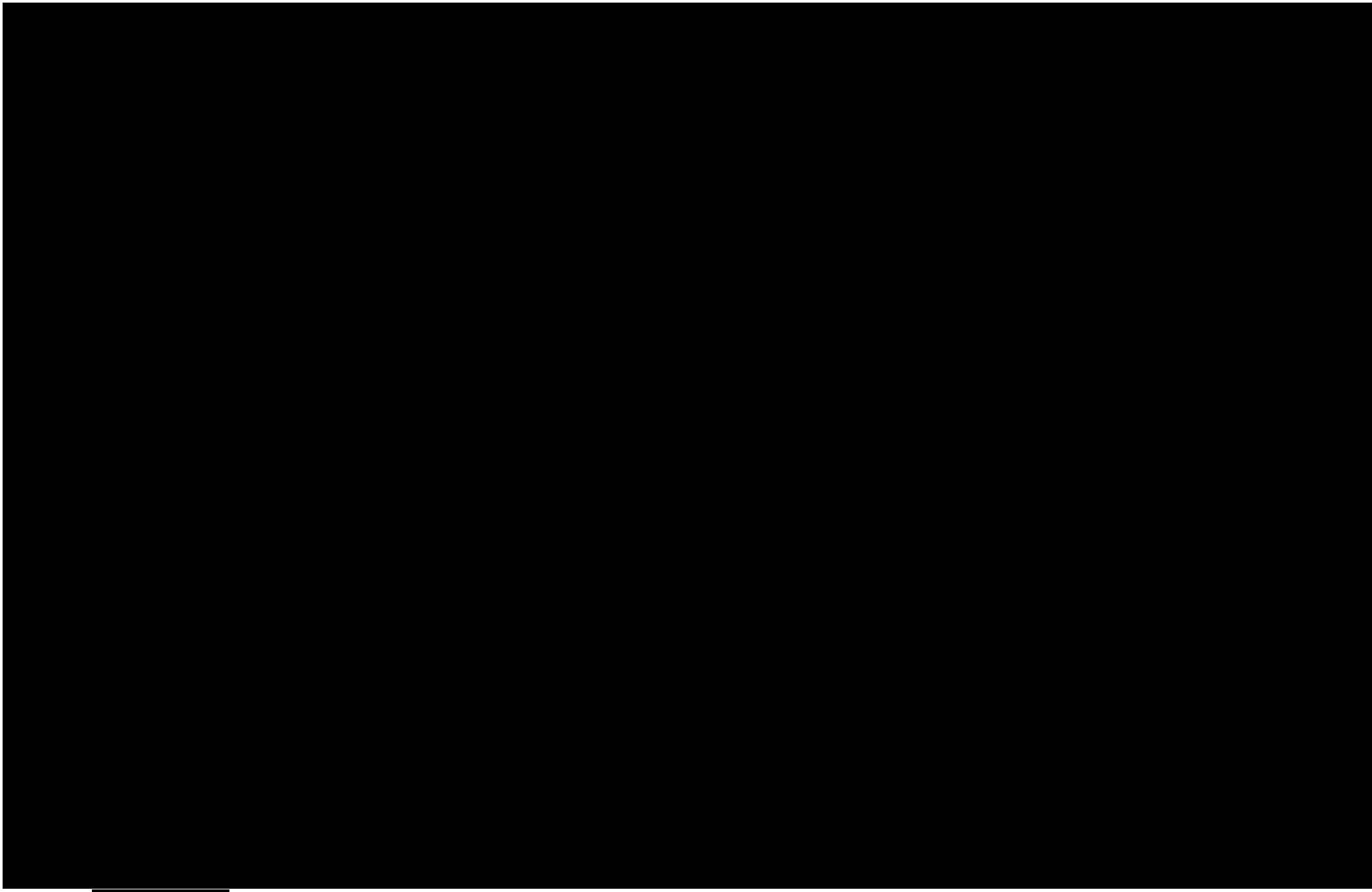


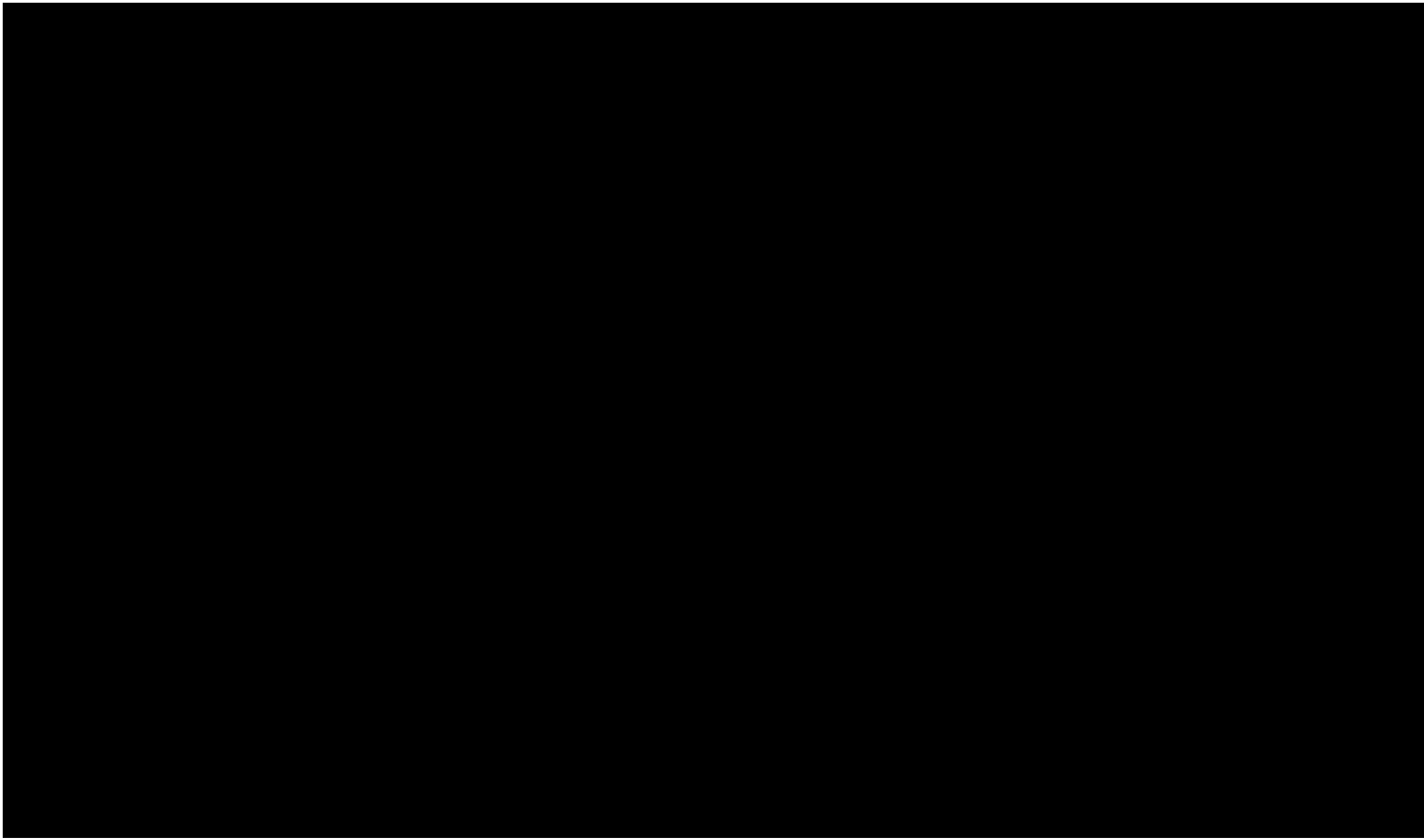
© 2012 Unisys Corporation. All rights reserved.

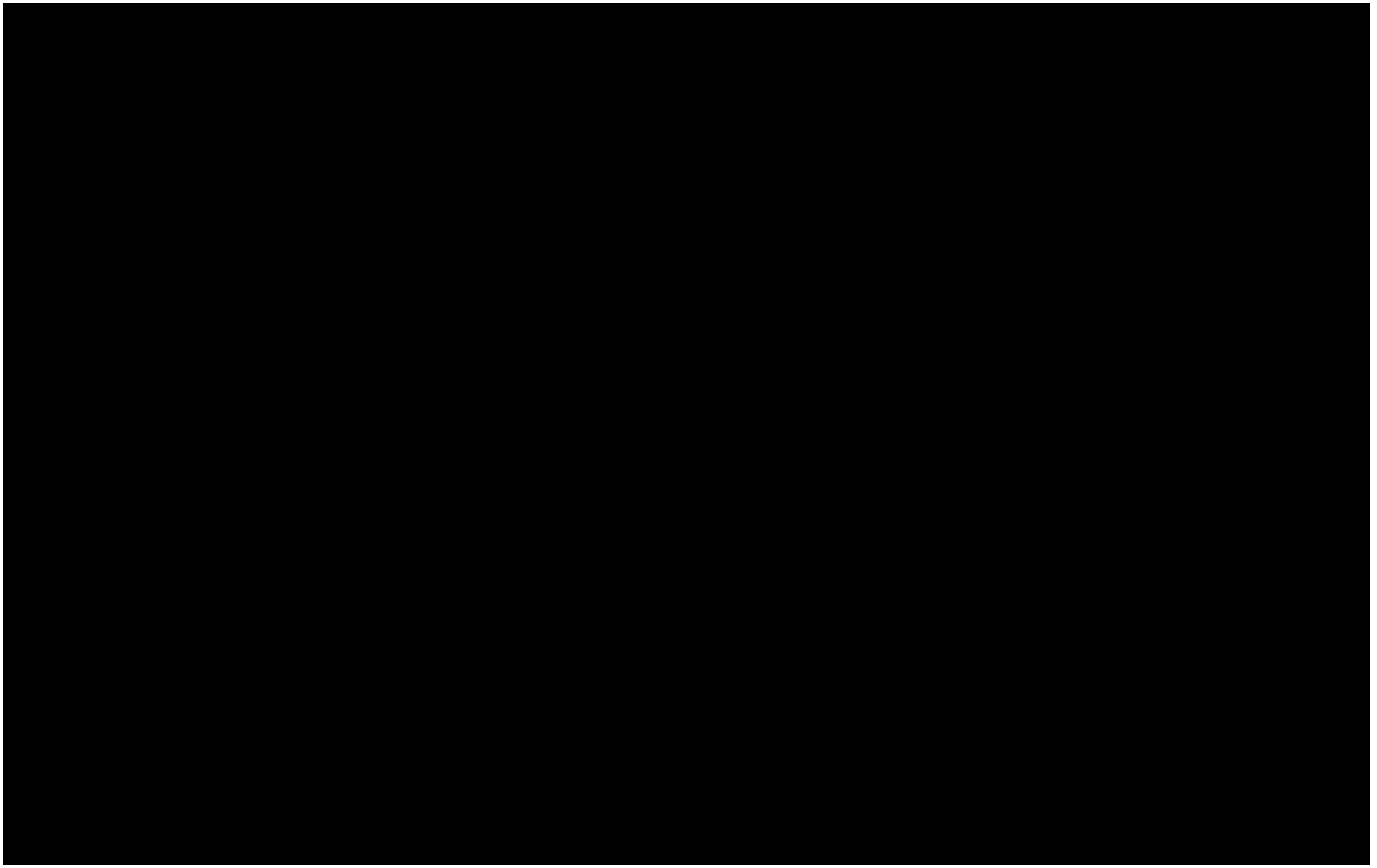


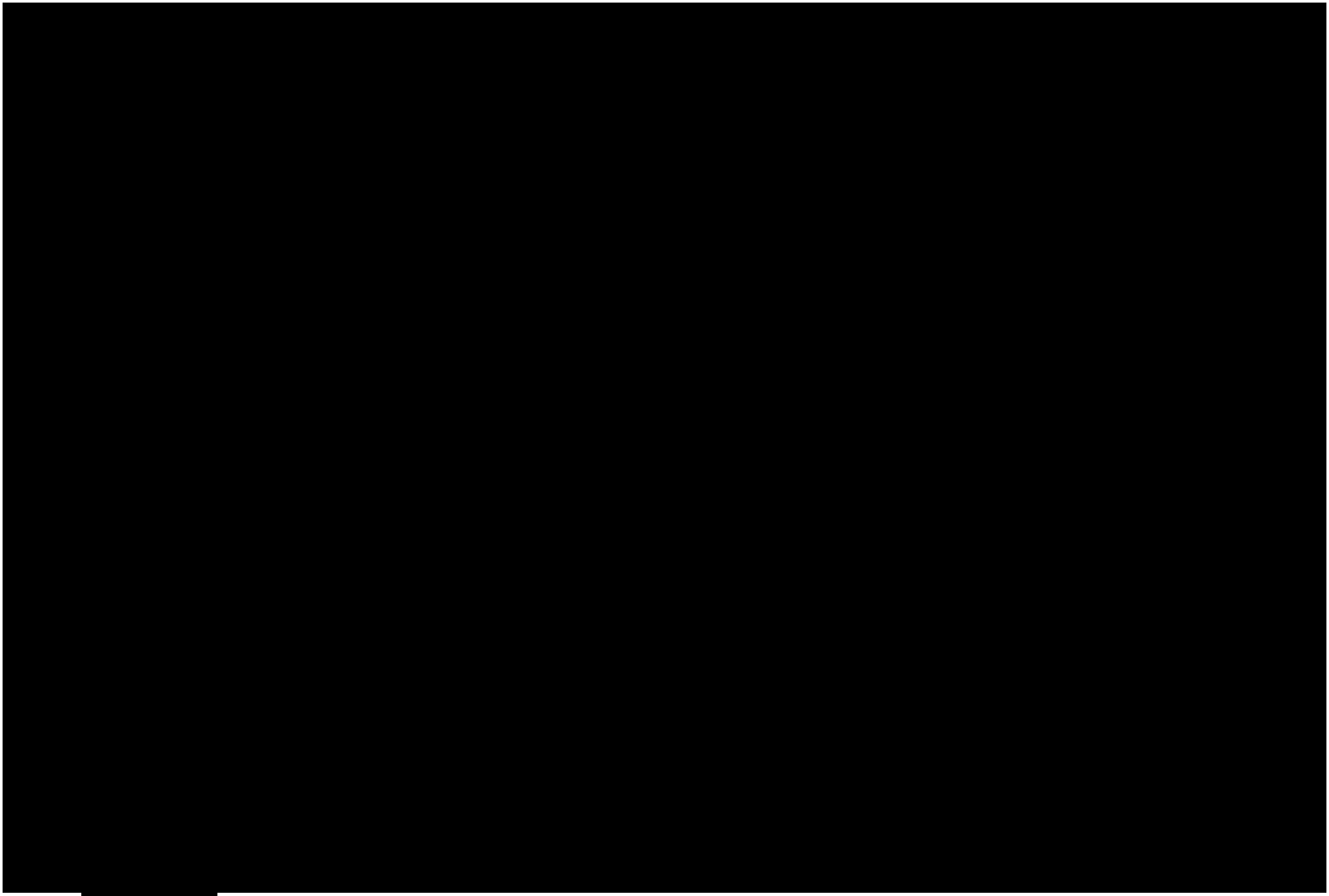


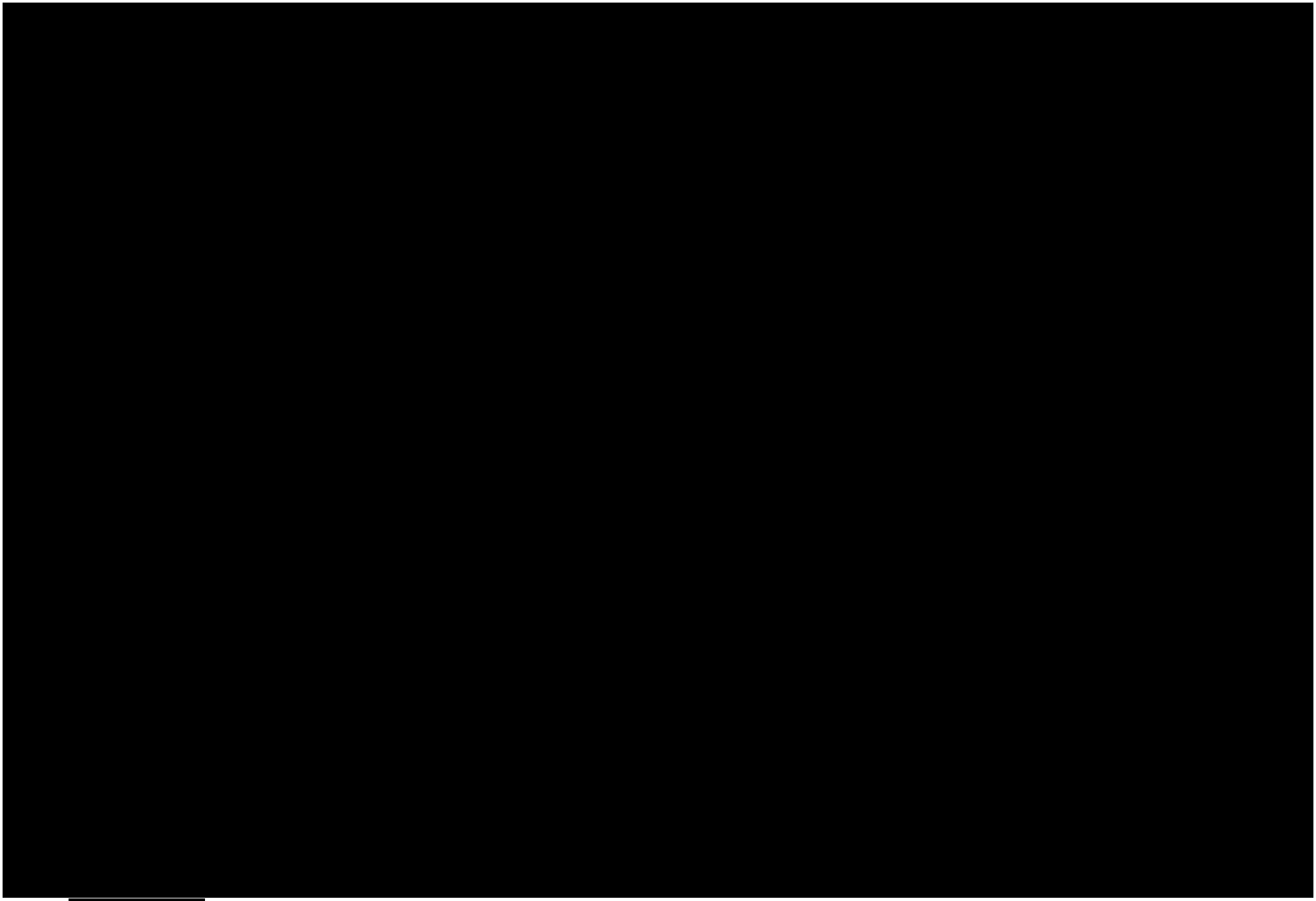
[redacted]











Attachment F-7 – IES DPH Capacity Planning Report

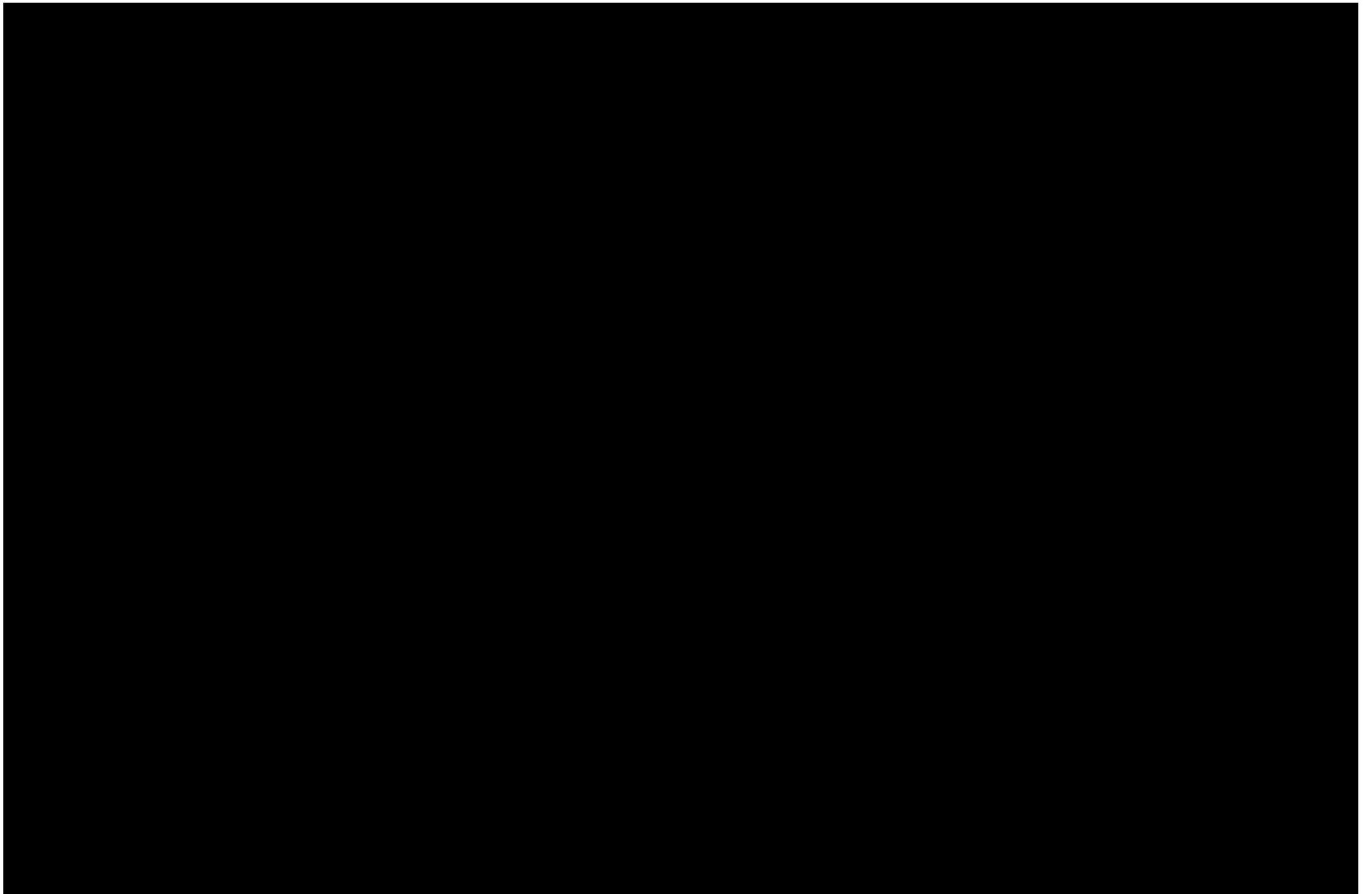
This attachment provides a sample capacity management report, that includes metrics in support of the Commonwealth Integrated Enterprise System (IES) SAP application environment.

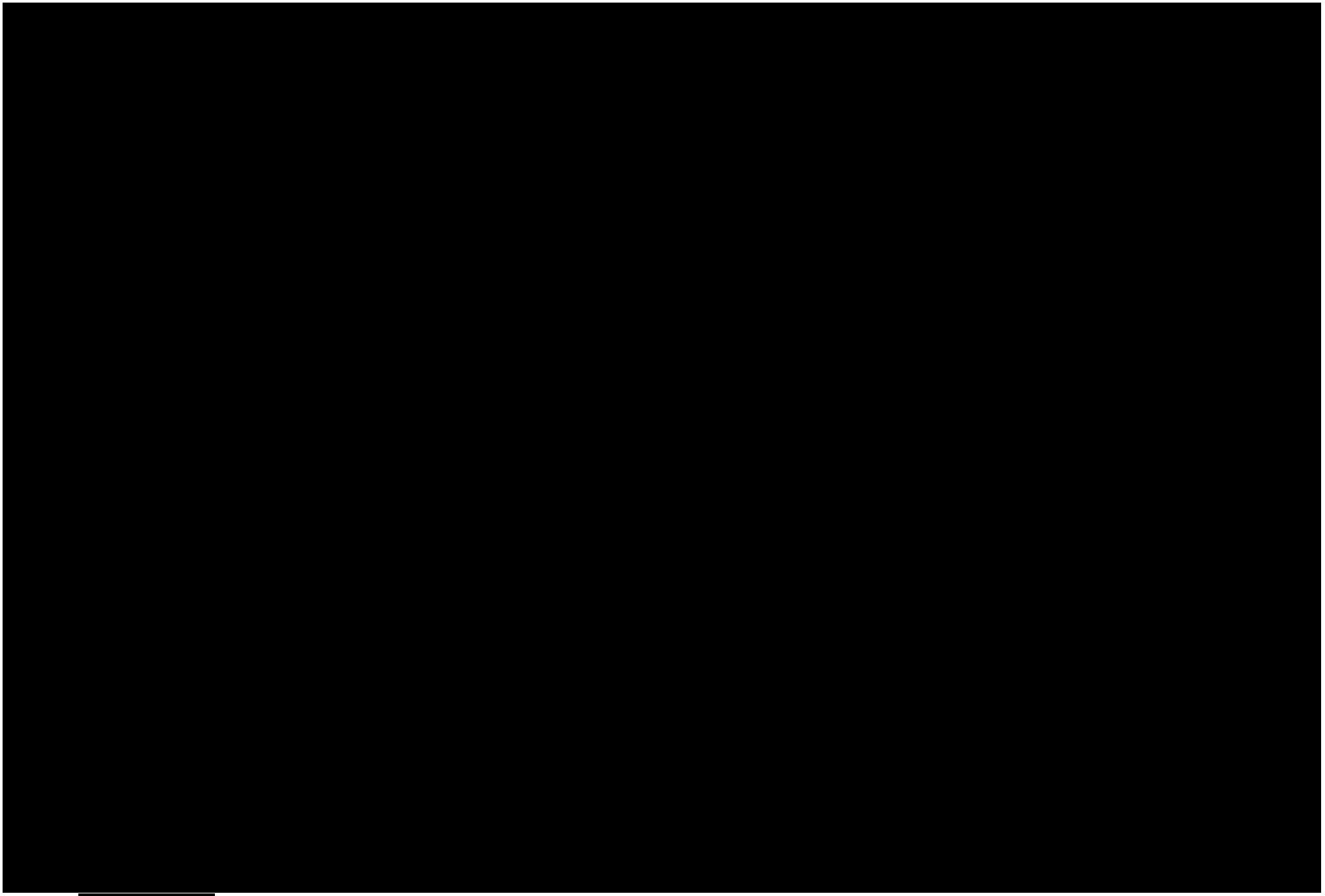
This page intentionally left blank.

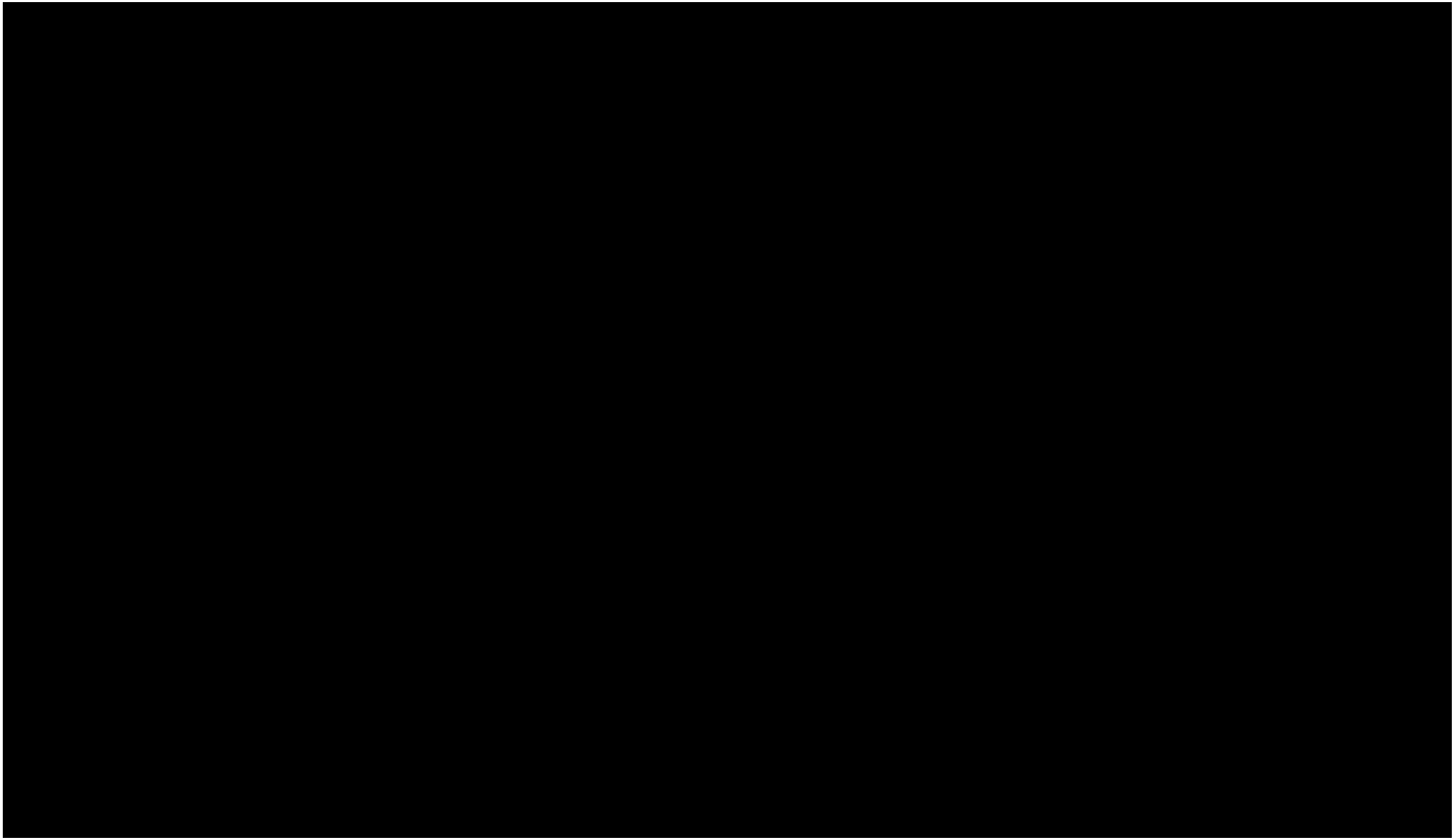
2013 Capacity Planning

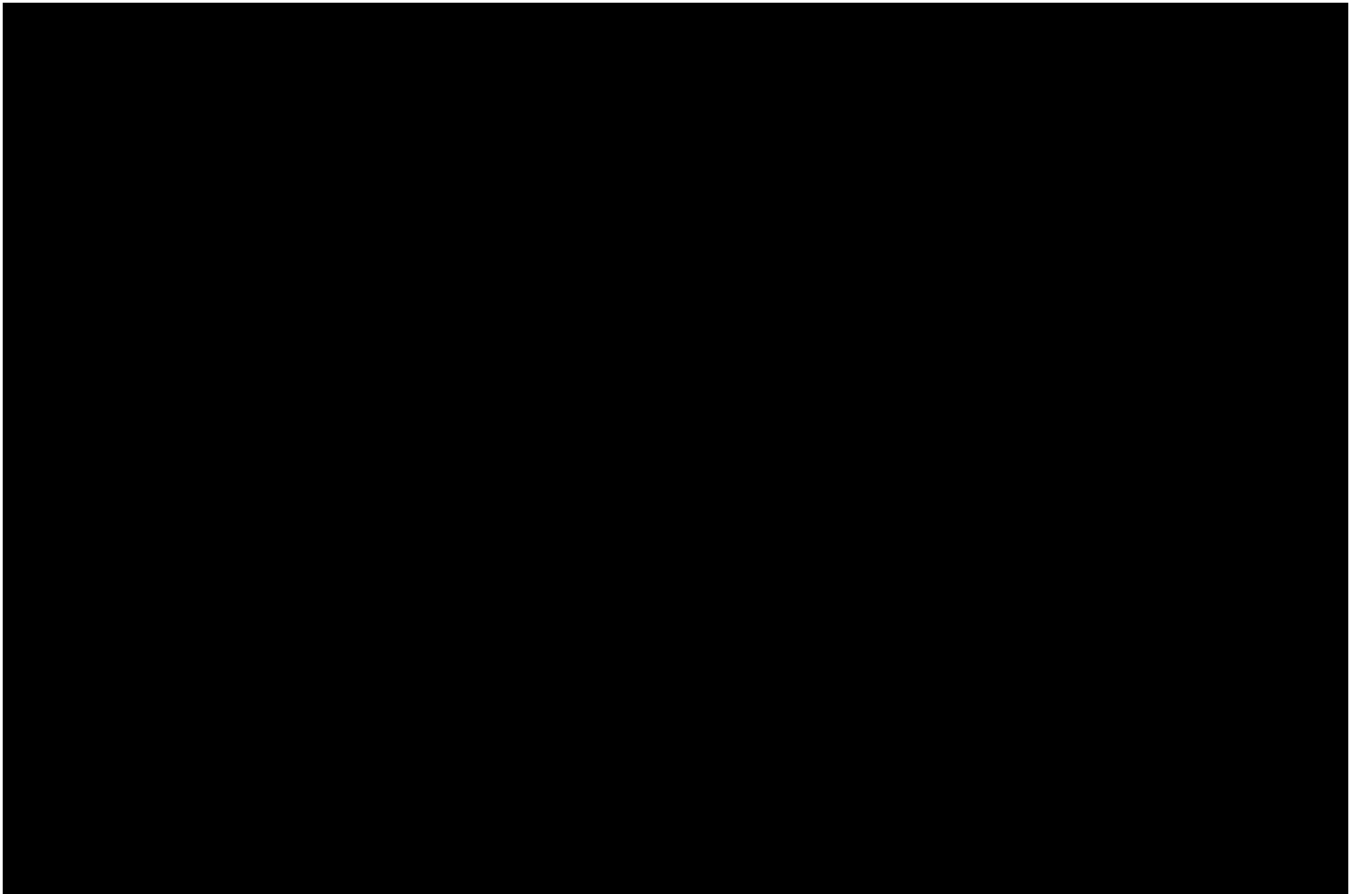
[redacted]

UNISYS

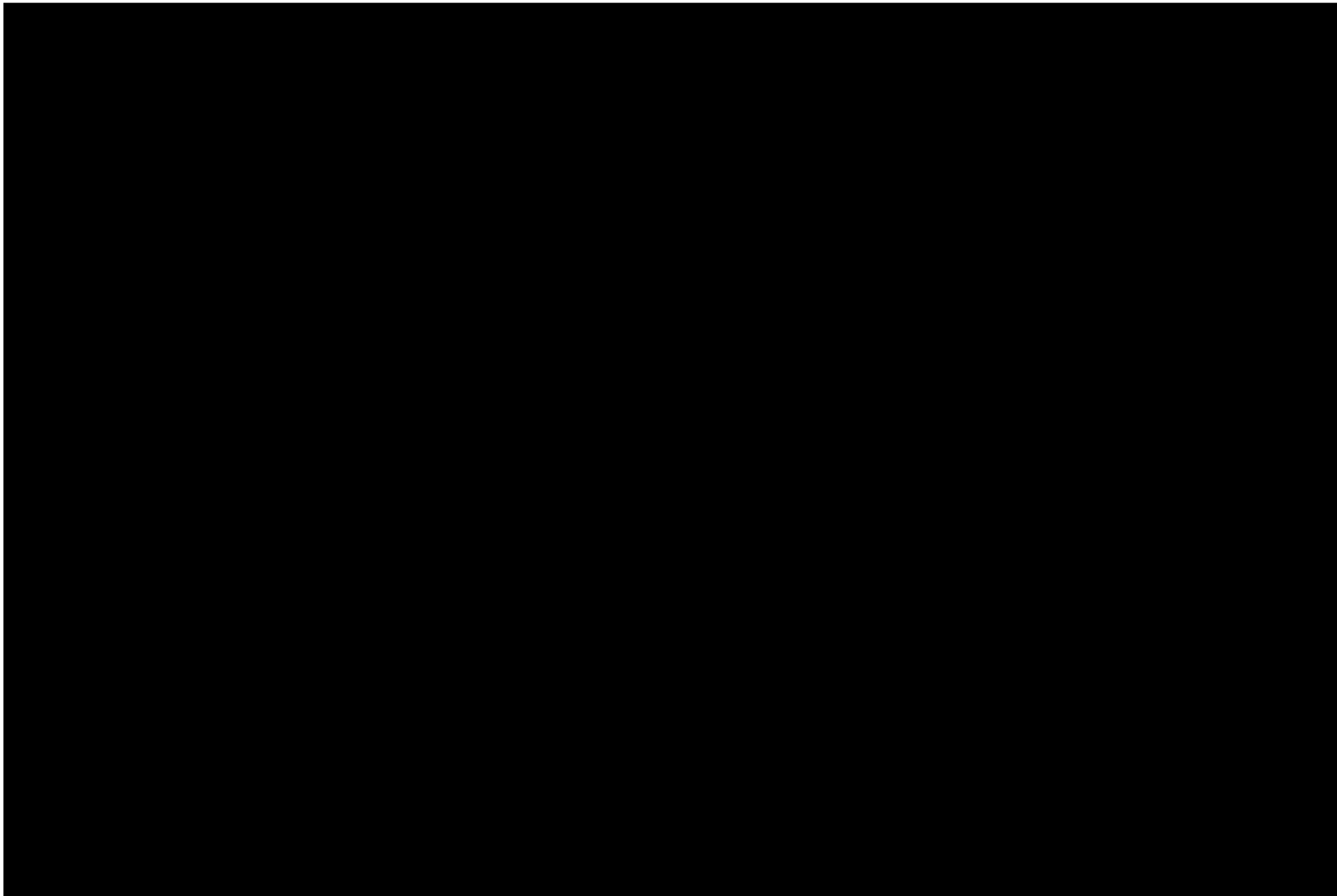




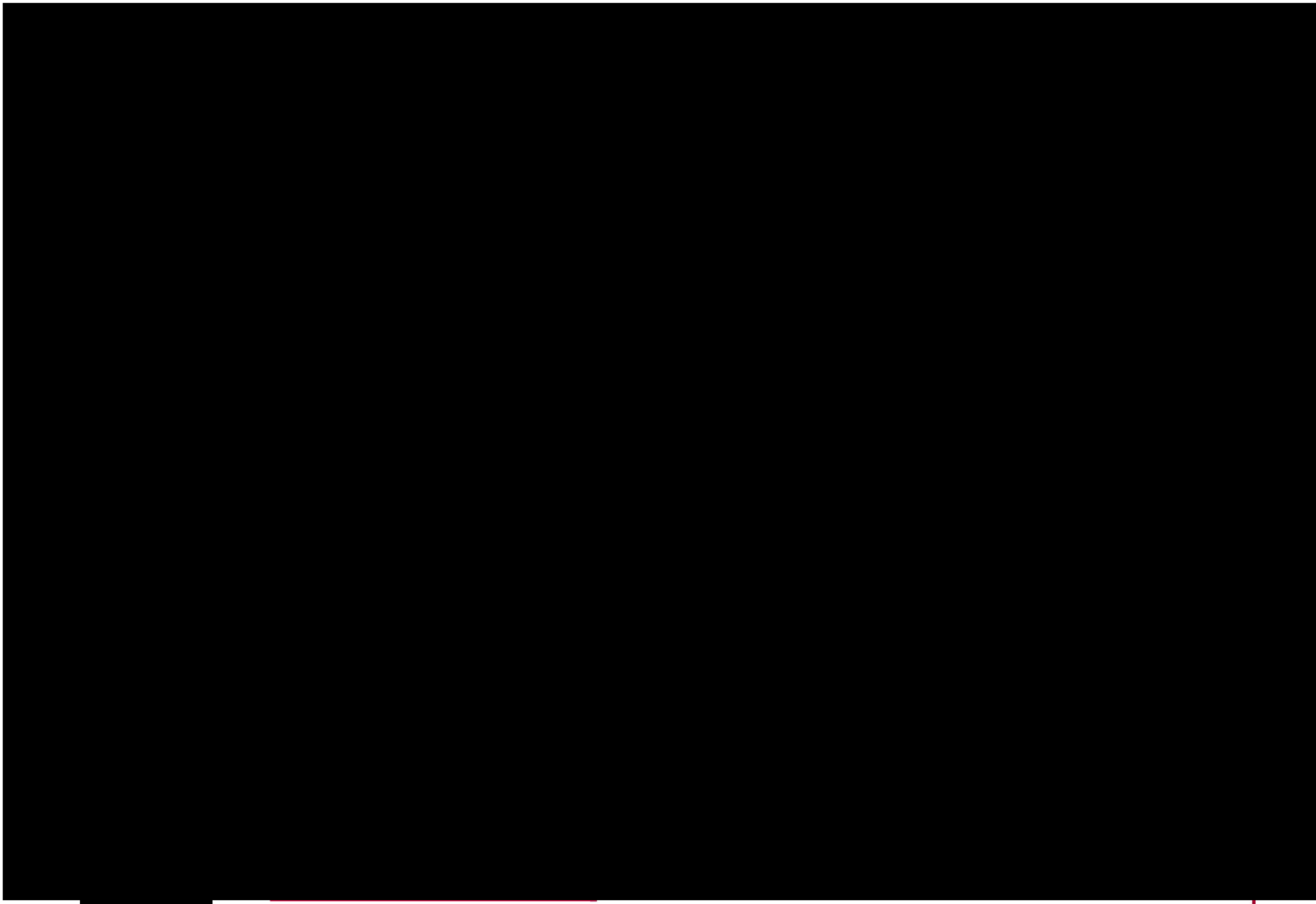




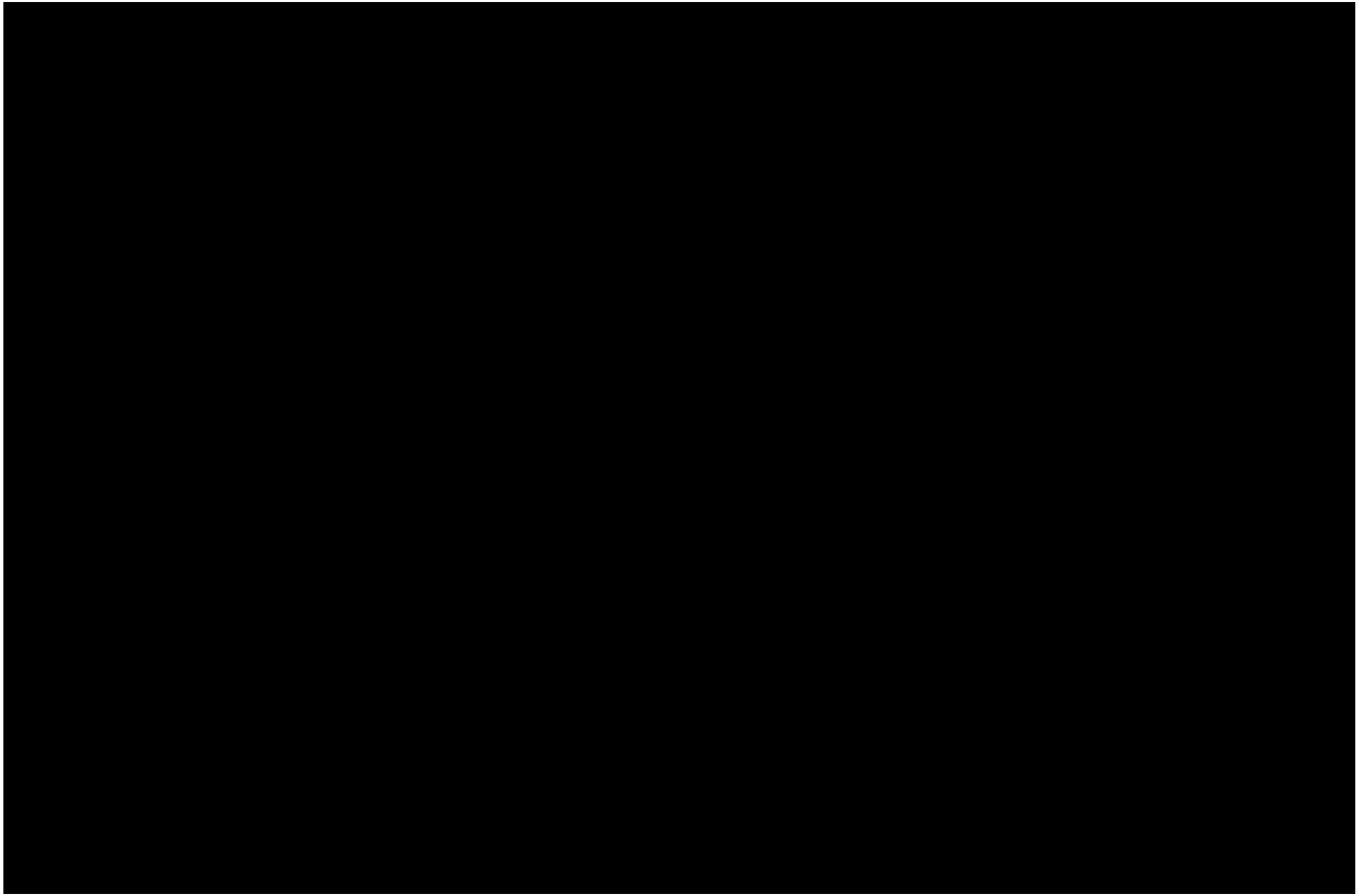
© 2013 Unisys Corporation. All rights reserved.

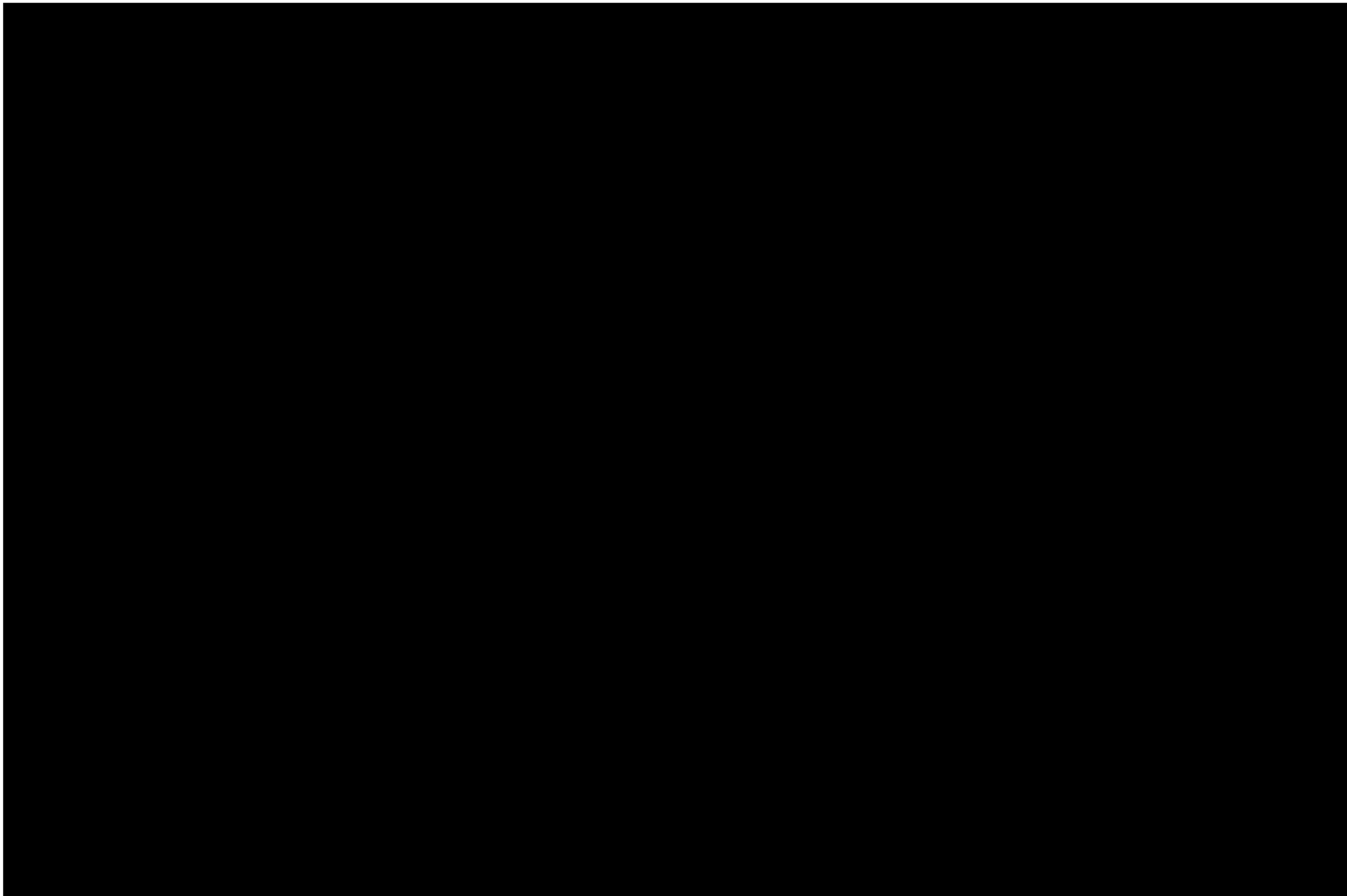


© 2013 Unisys Corporation. All rights reserved.

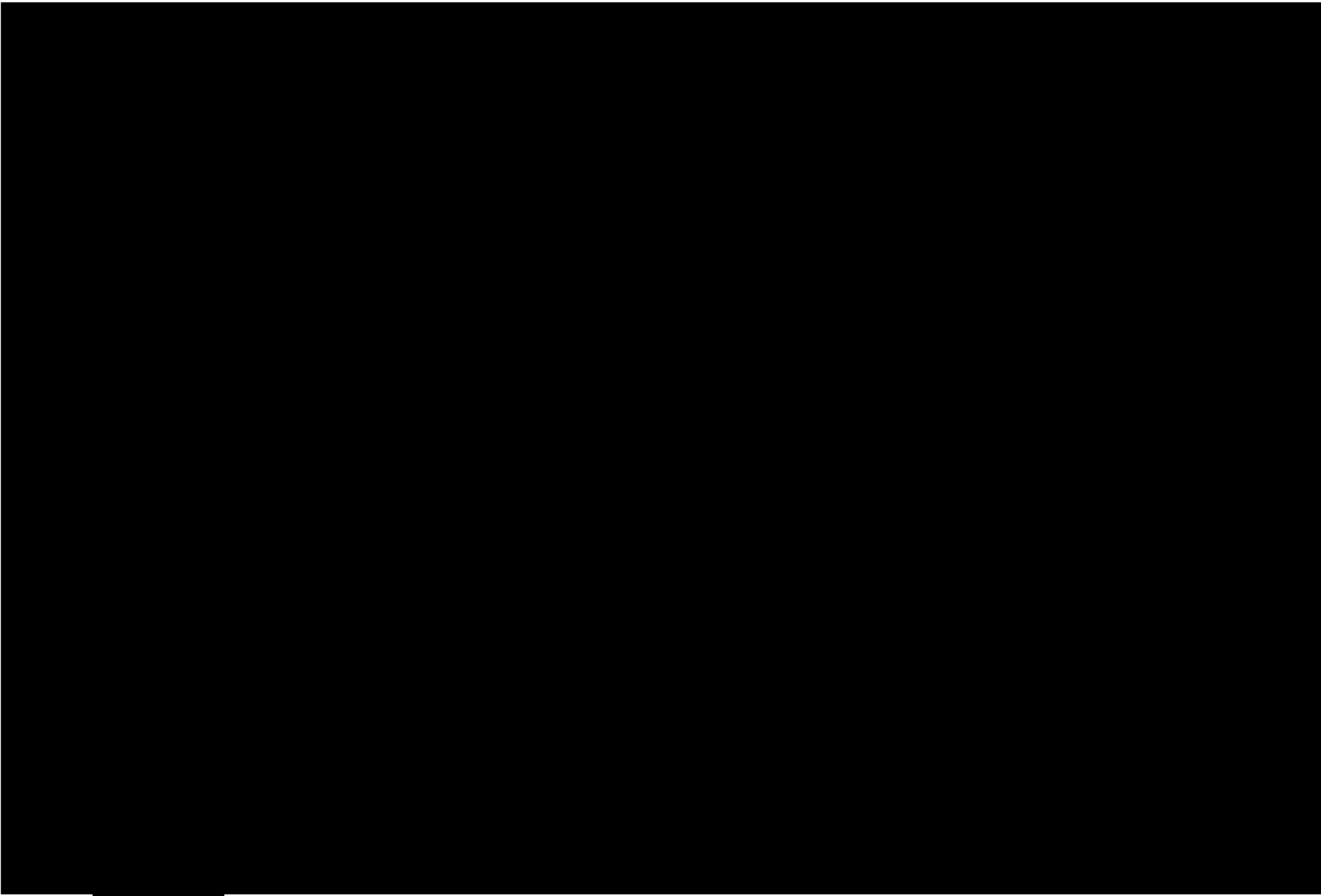


© 2013 Unisys Corporation. All rights reserved.

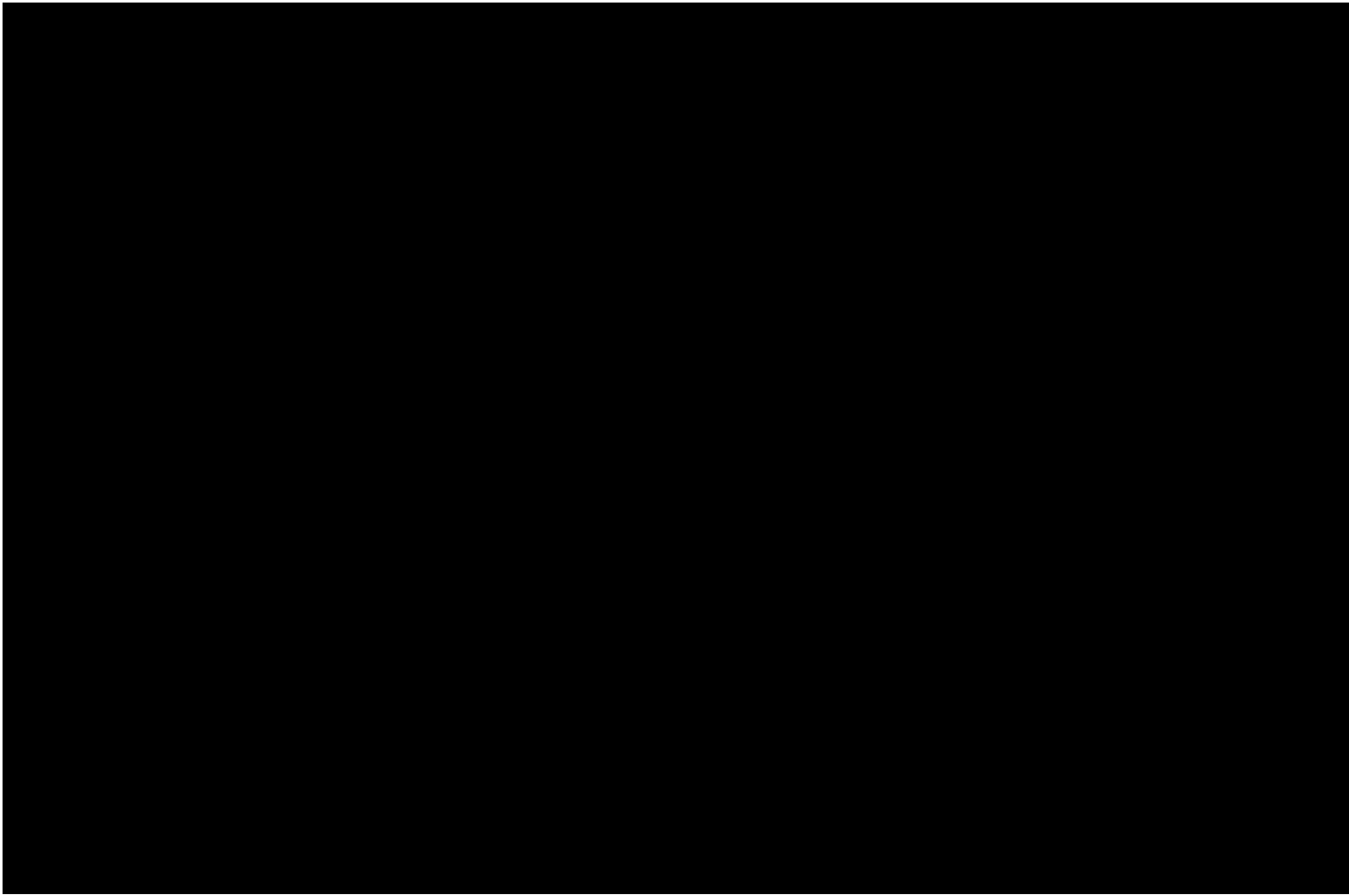




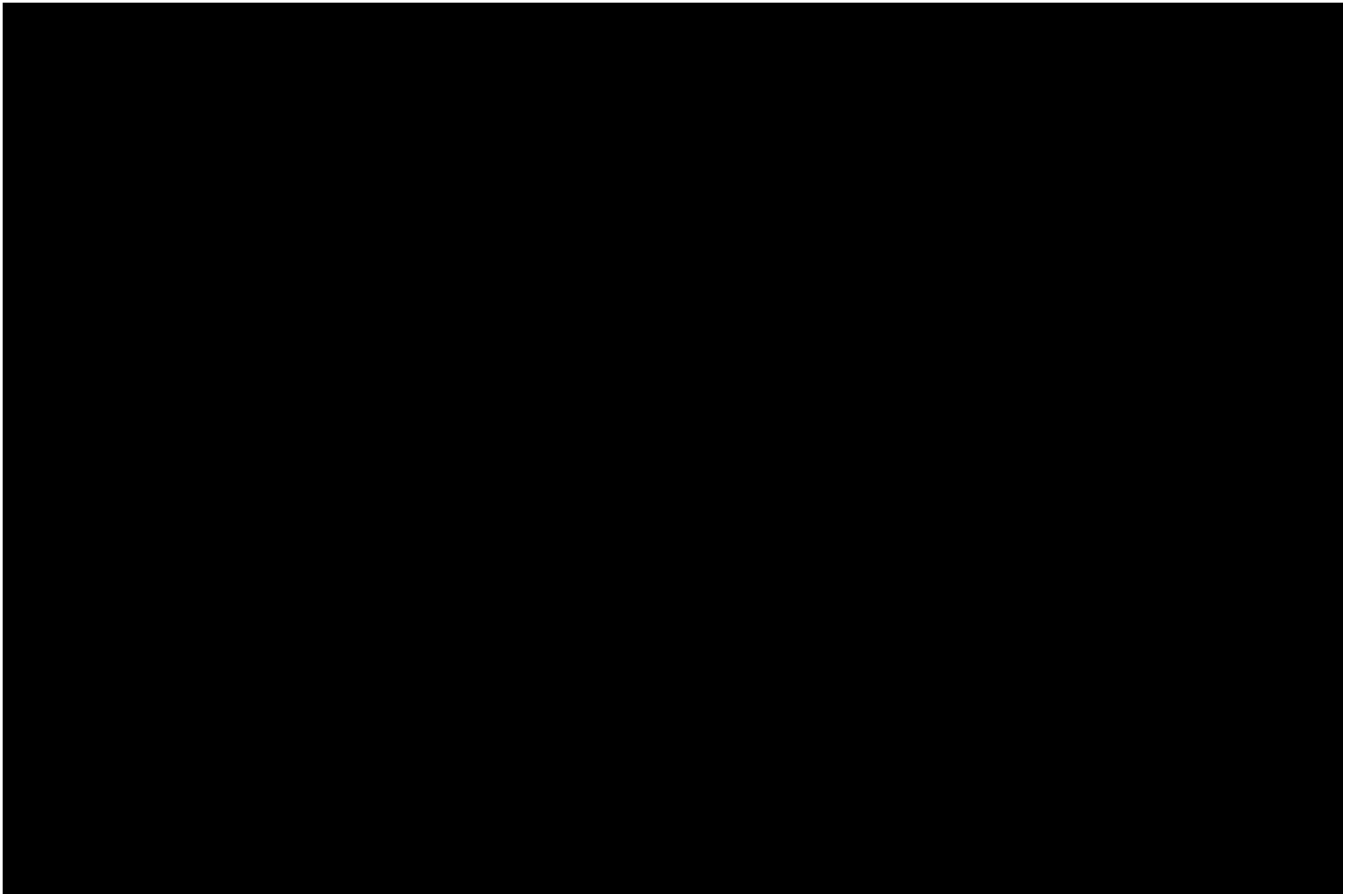
© 2013 Unisys Corporation. All rights reserved.



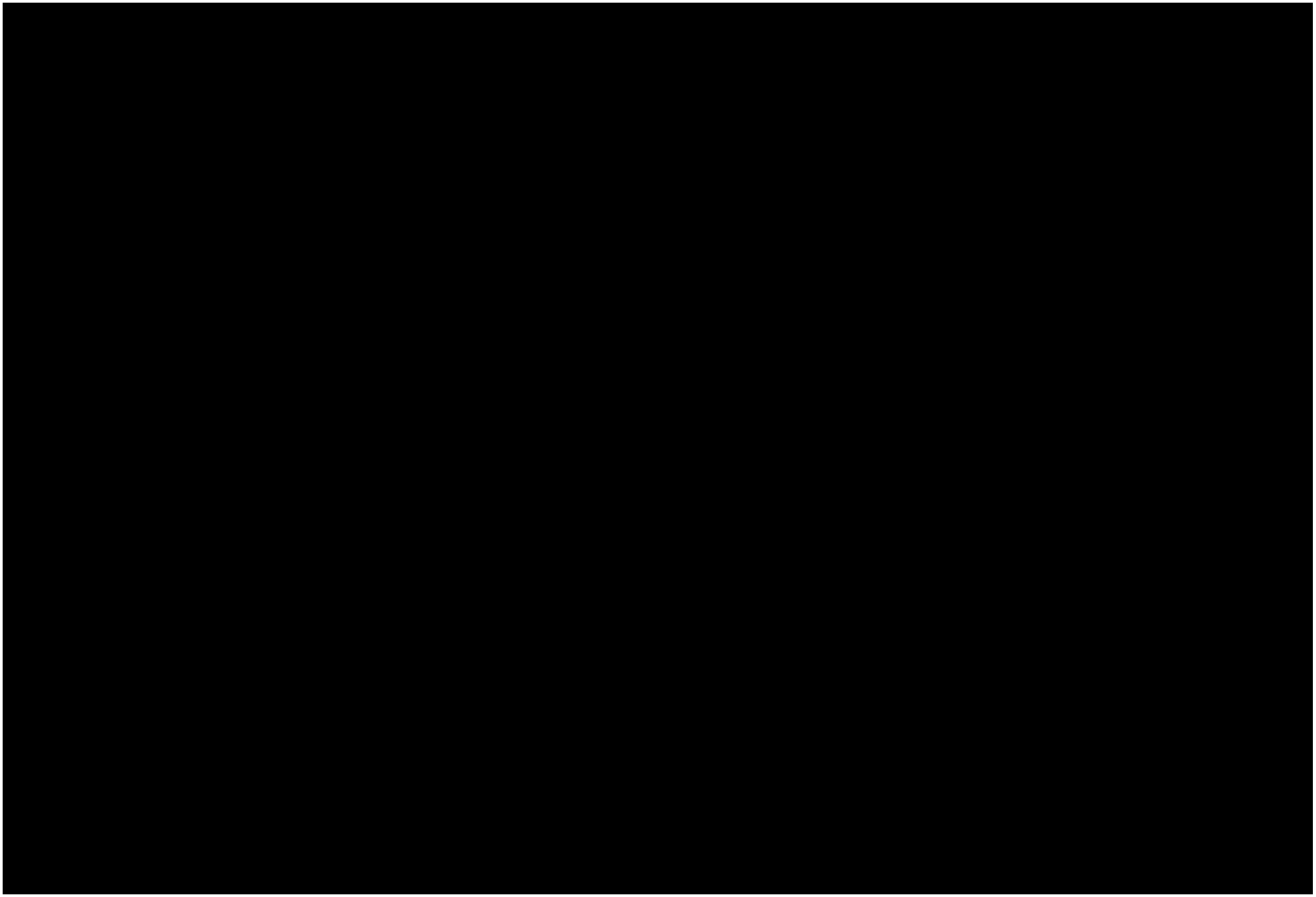
© 2013 Unisys Corporation. All rights reserved.

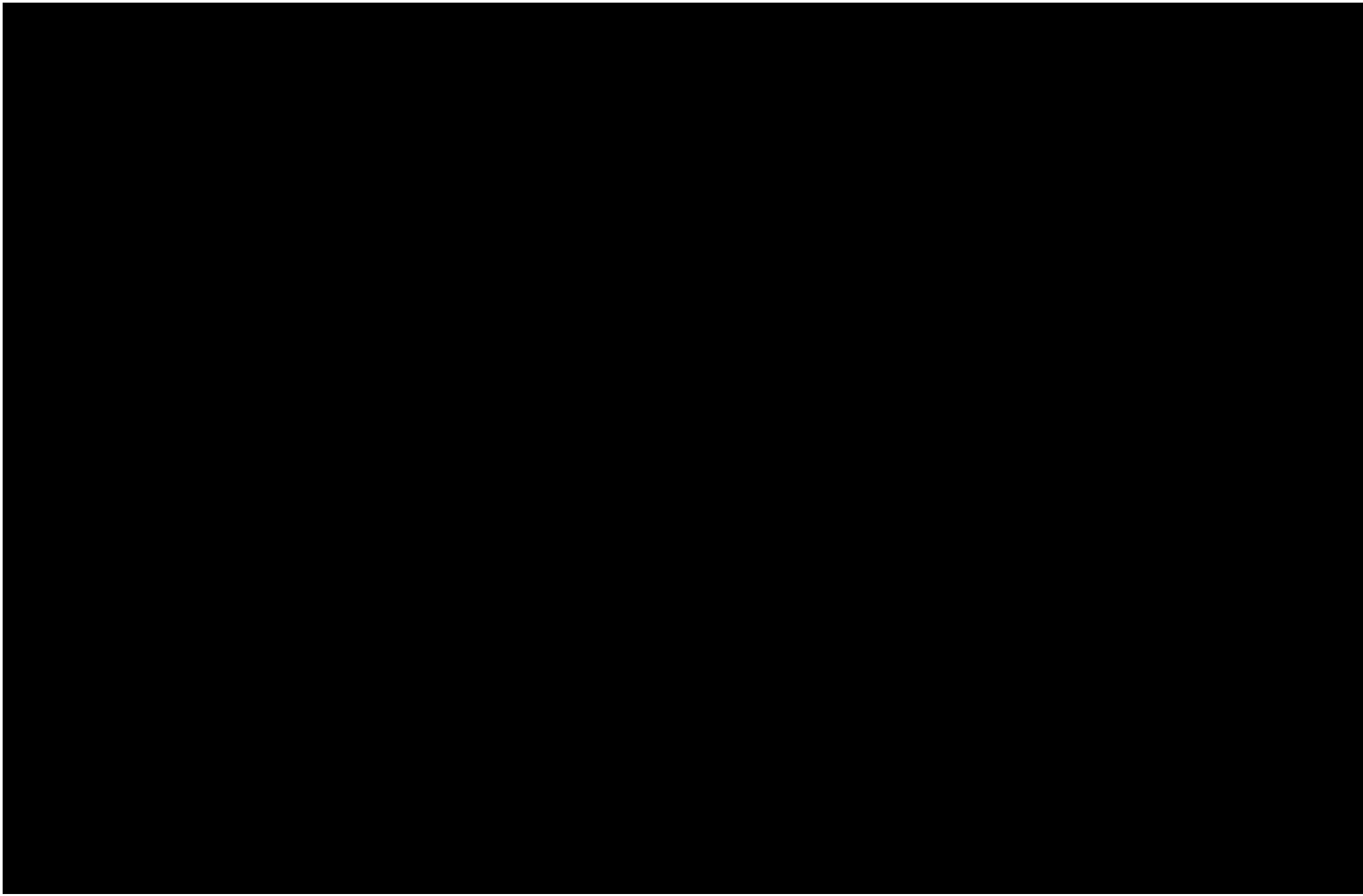


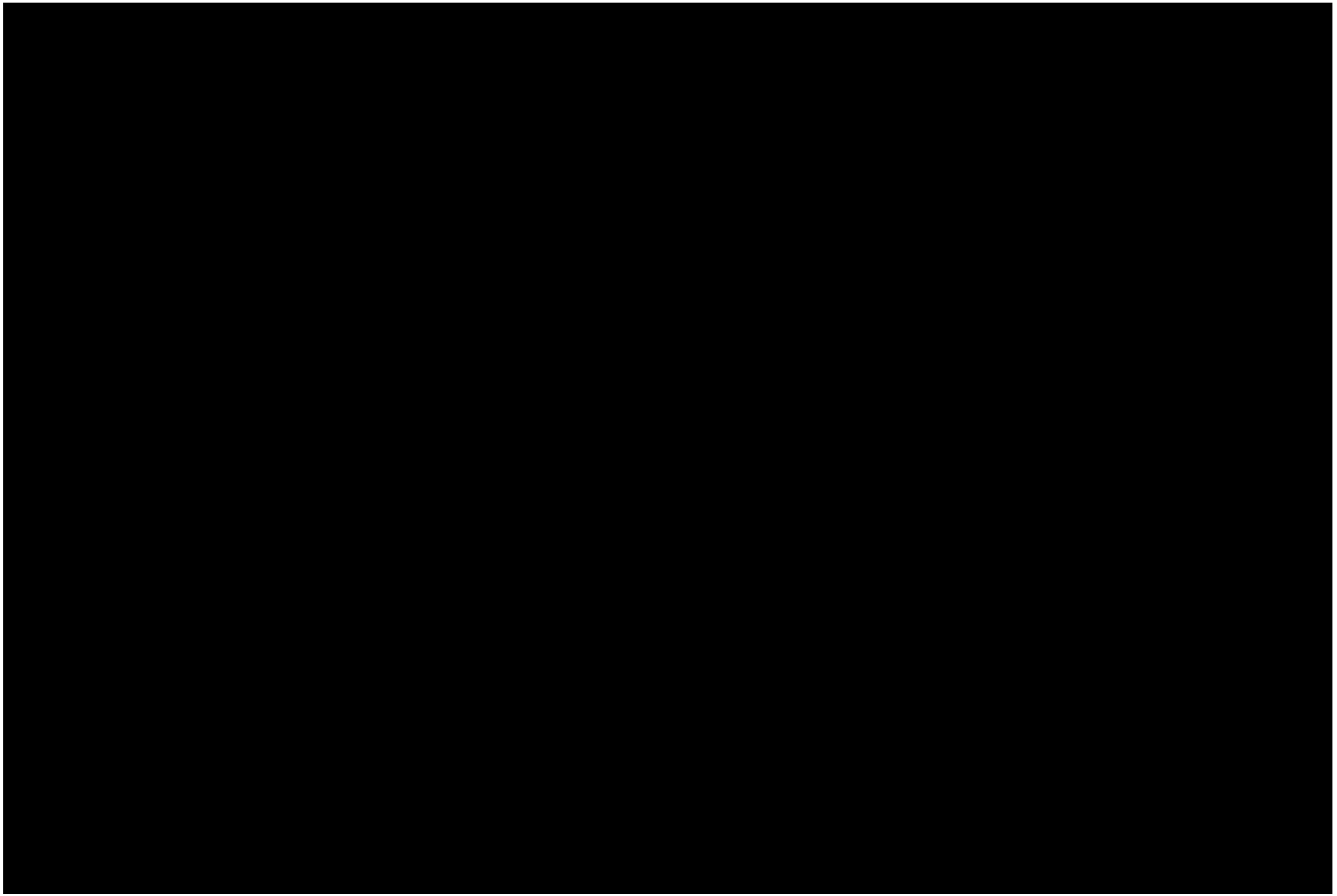
© 2013 Unisys Corporation. All rights reserved.

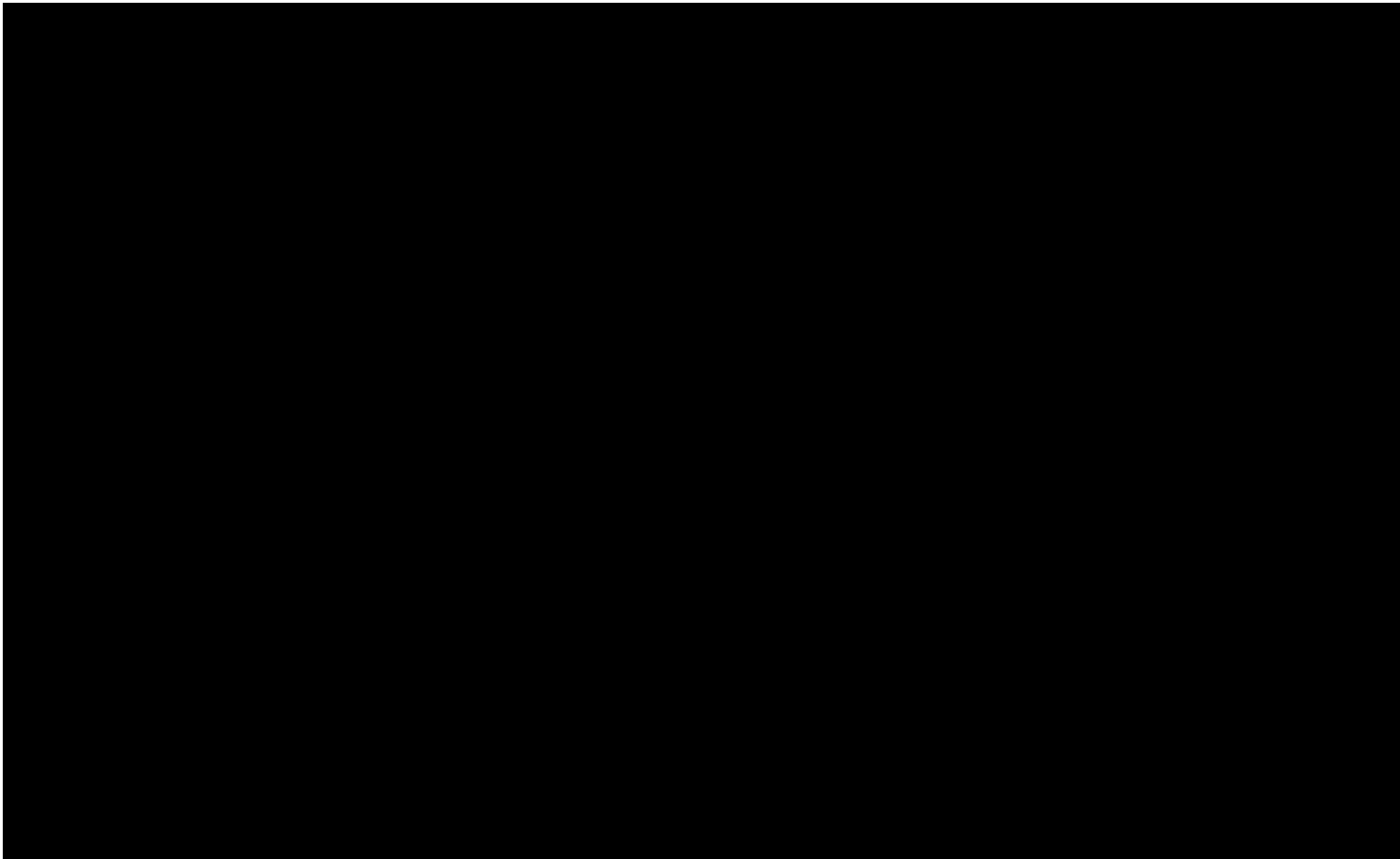


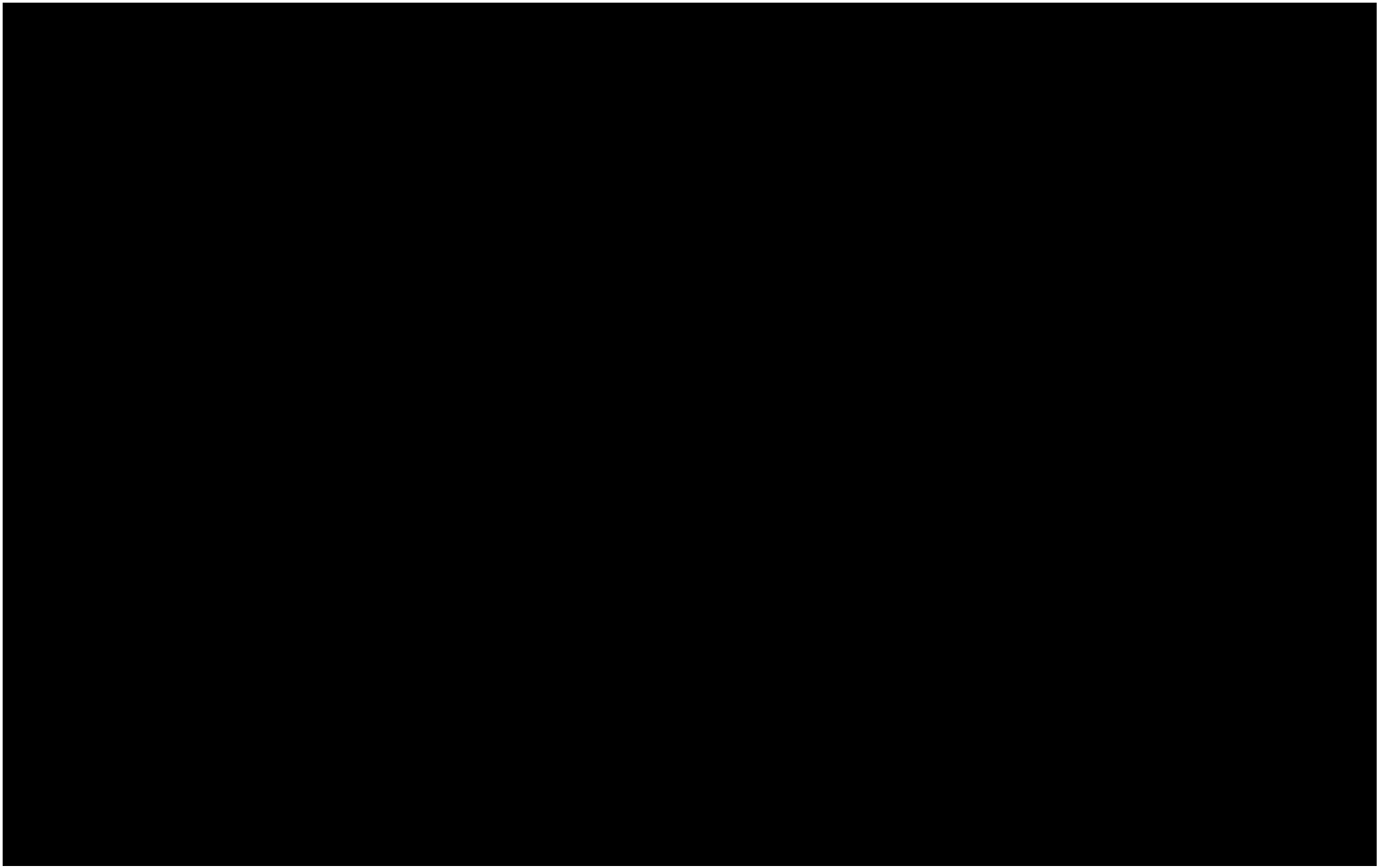
UNISYS

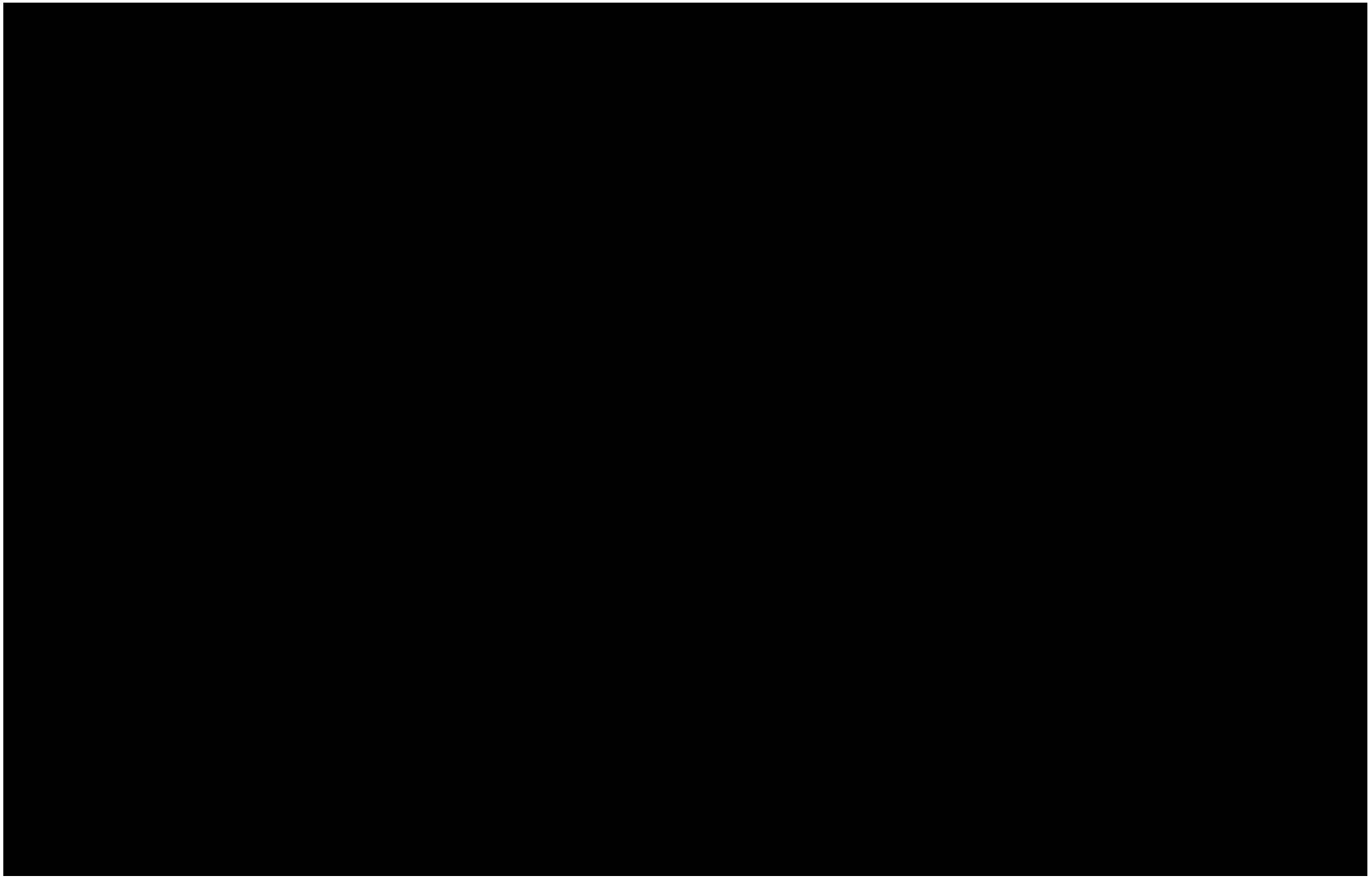


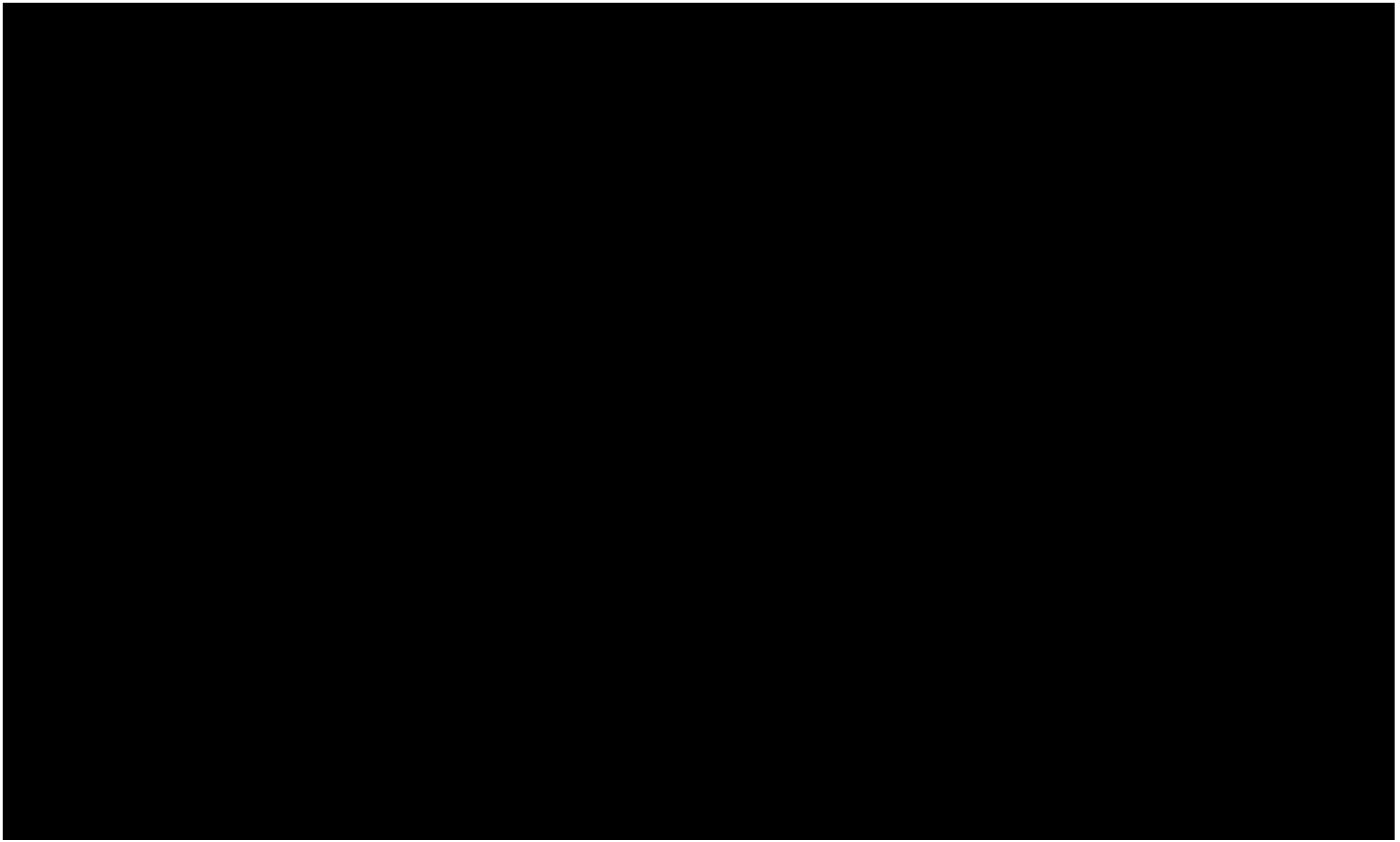


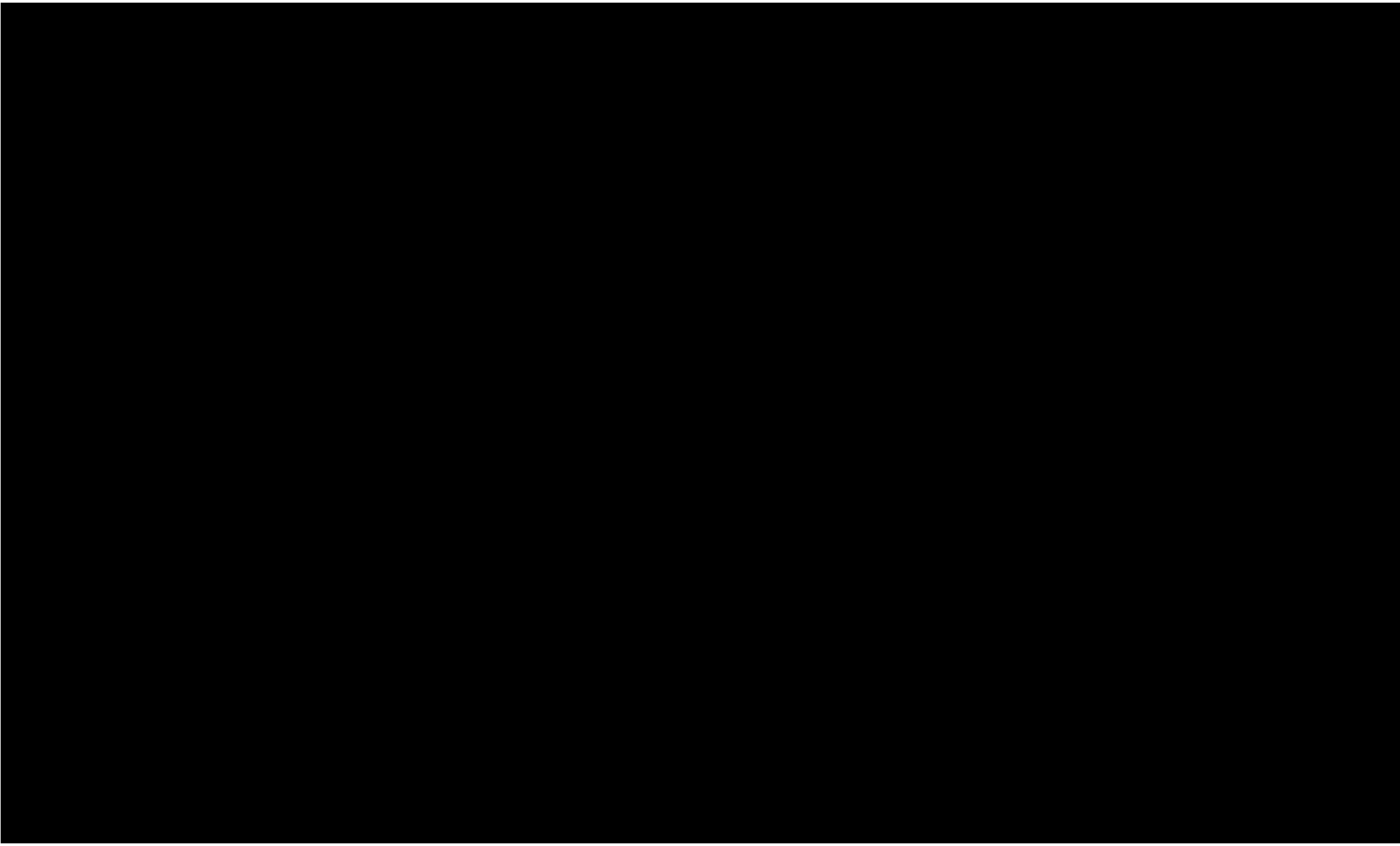


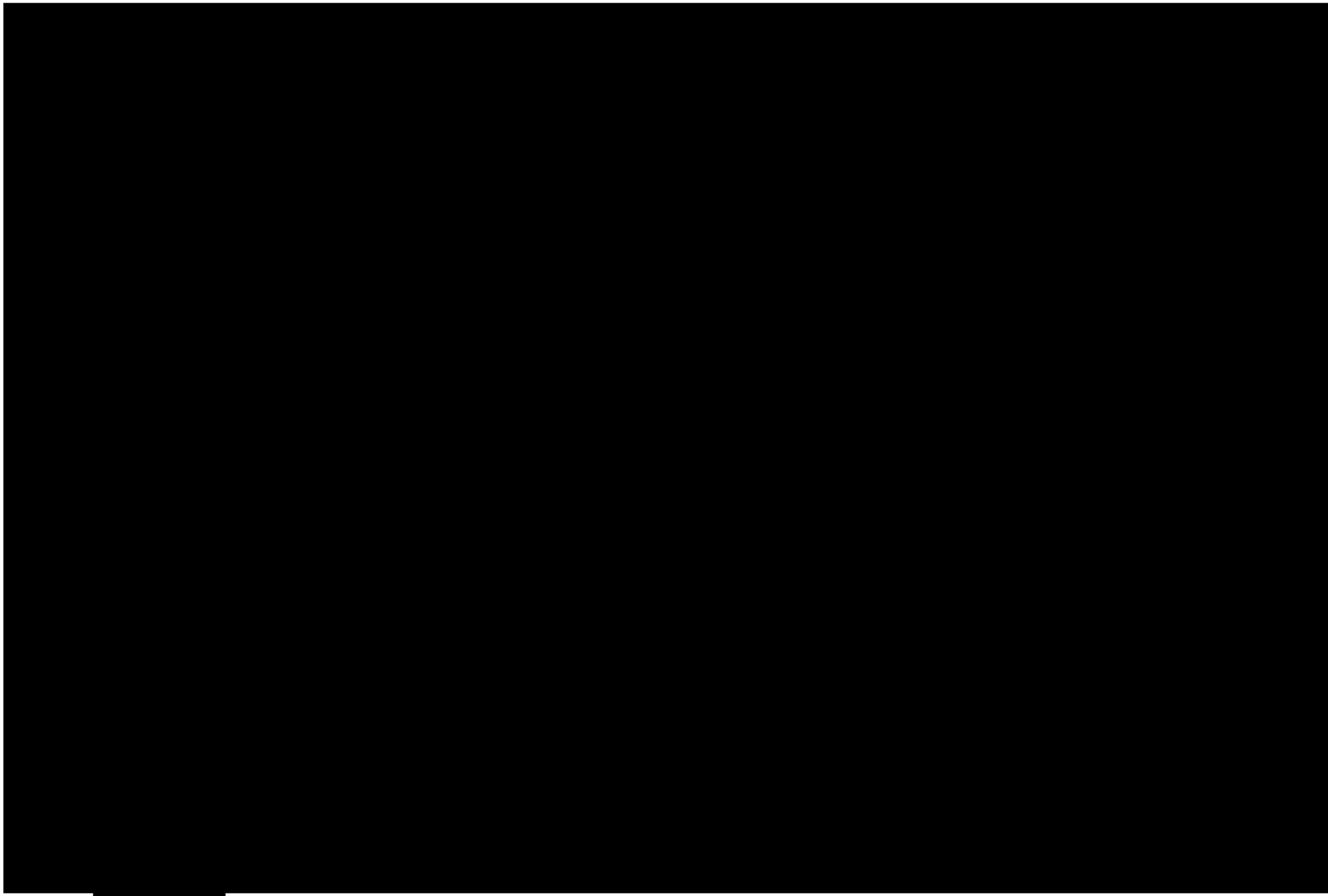






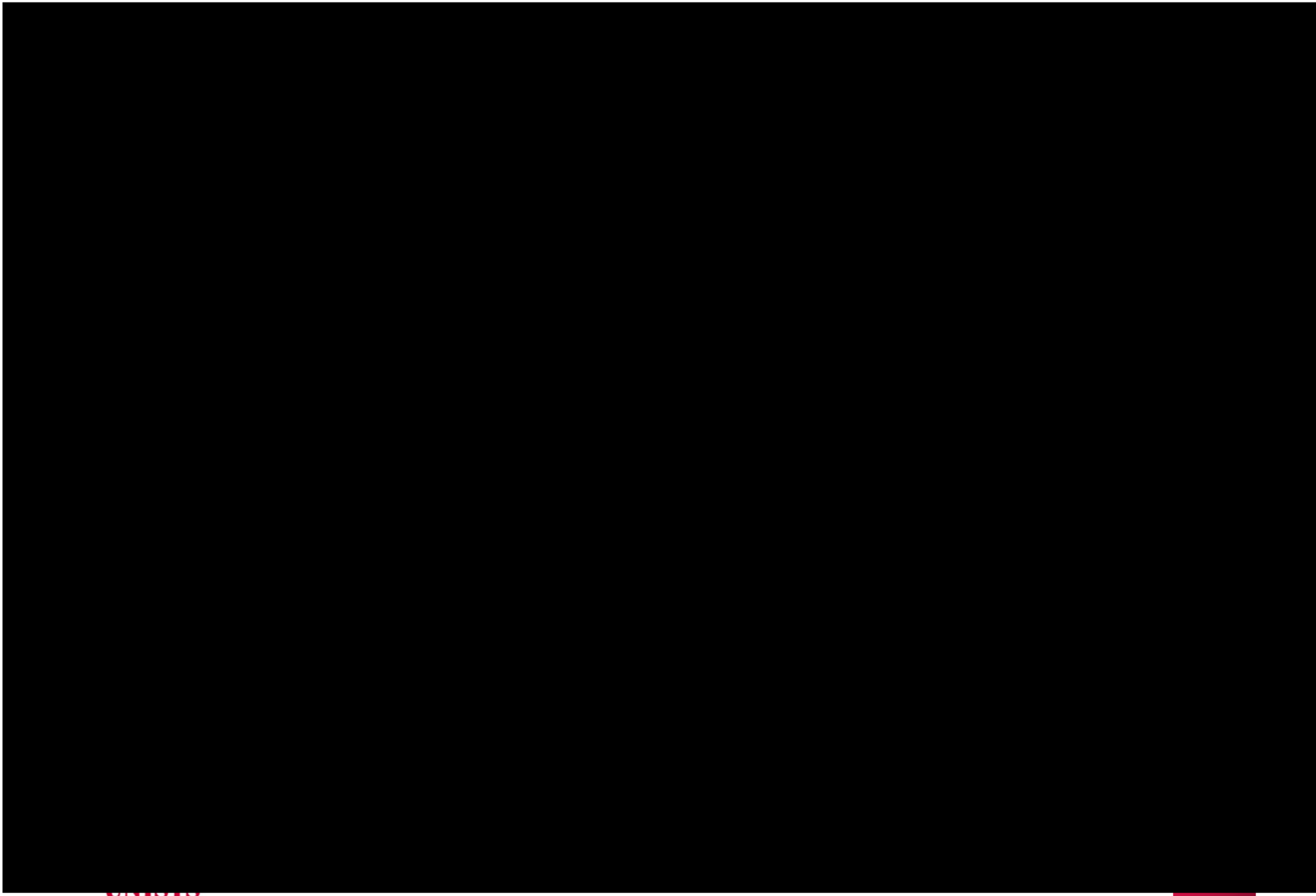




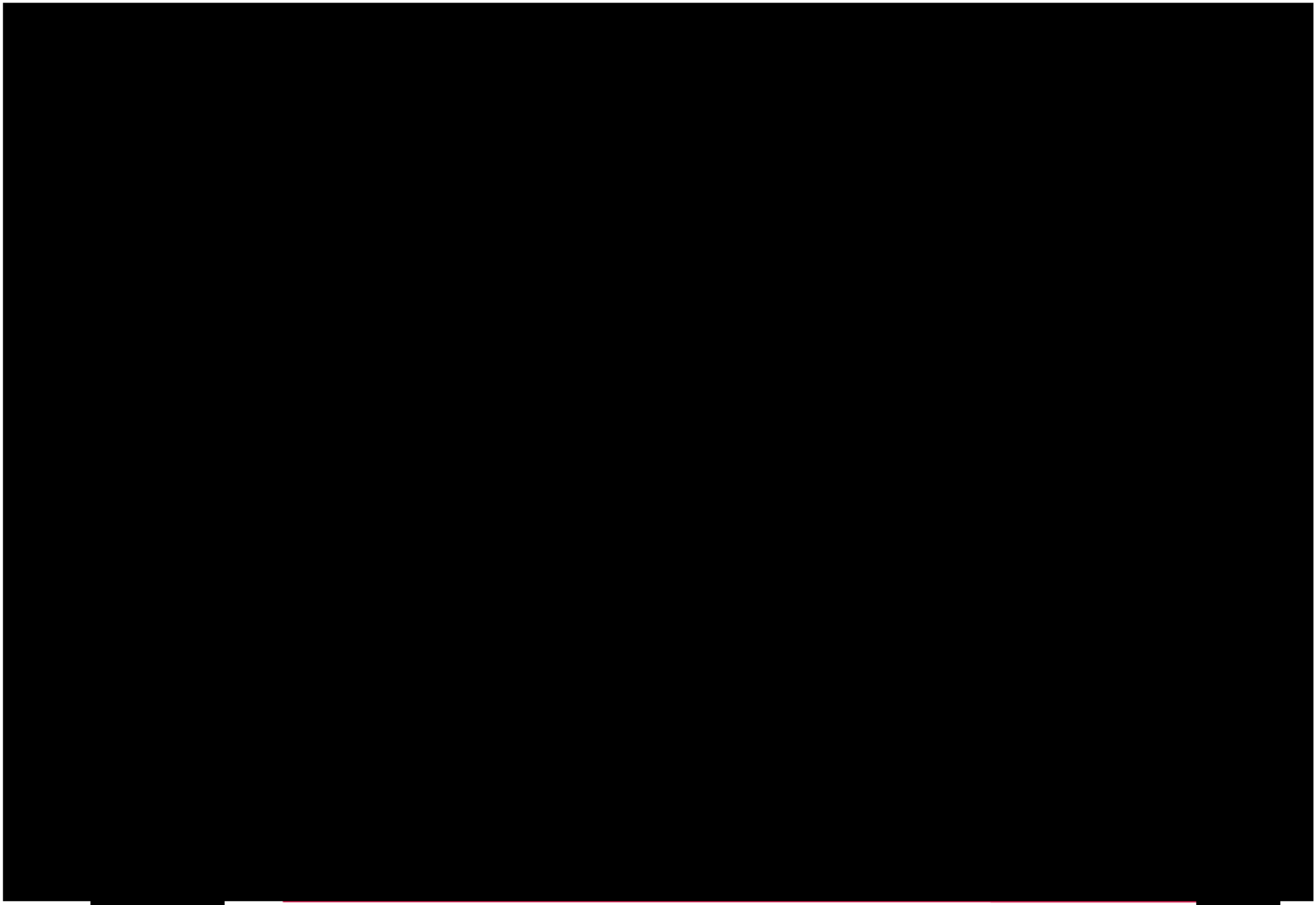


© 2013 Unisys Corporation. All rights reserved.

© 2013 Unisys Corporation. All rights reserved.



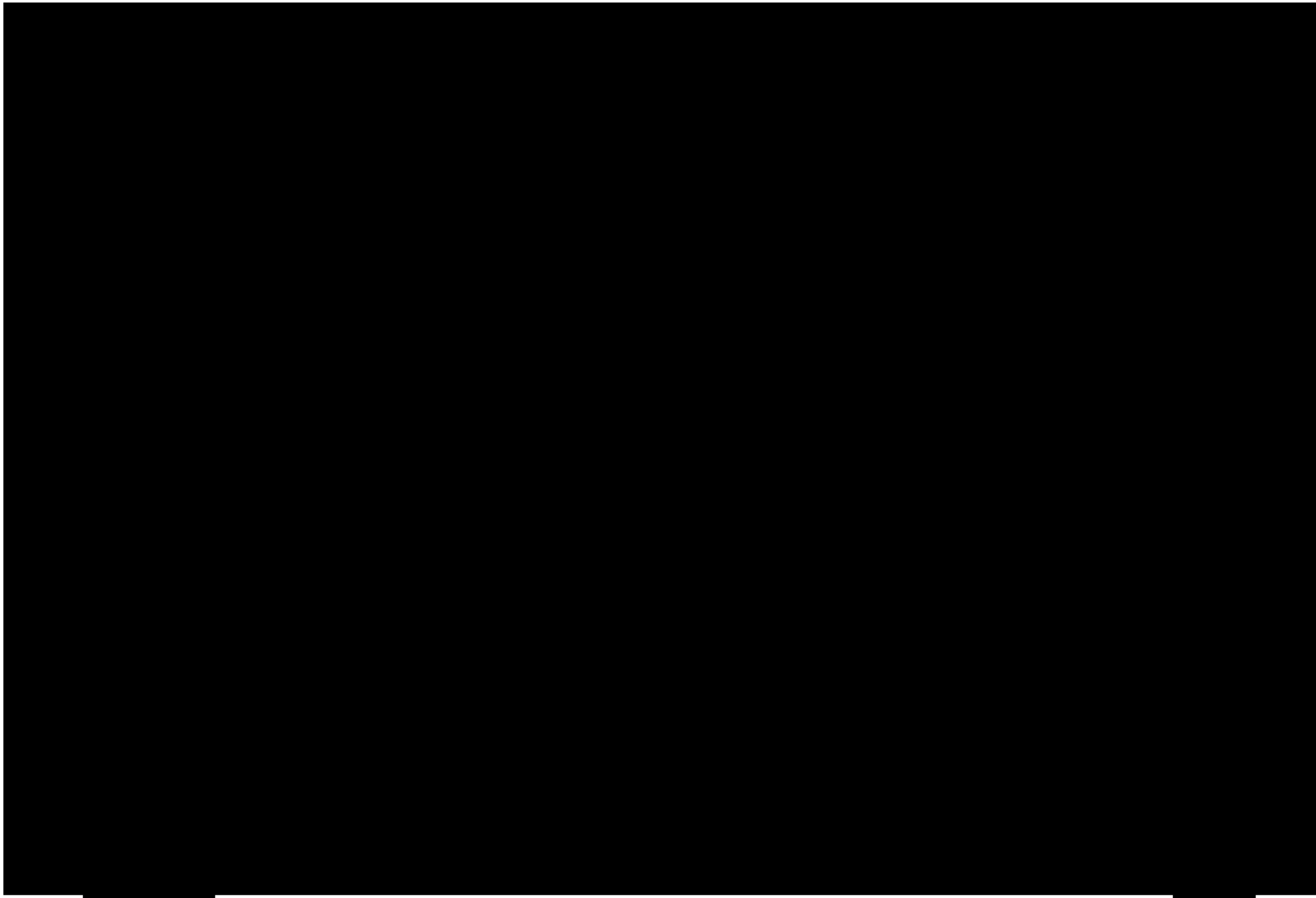
© 2013 Unisys Corporation. All rights reserved.



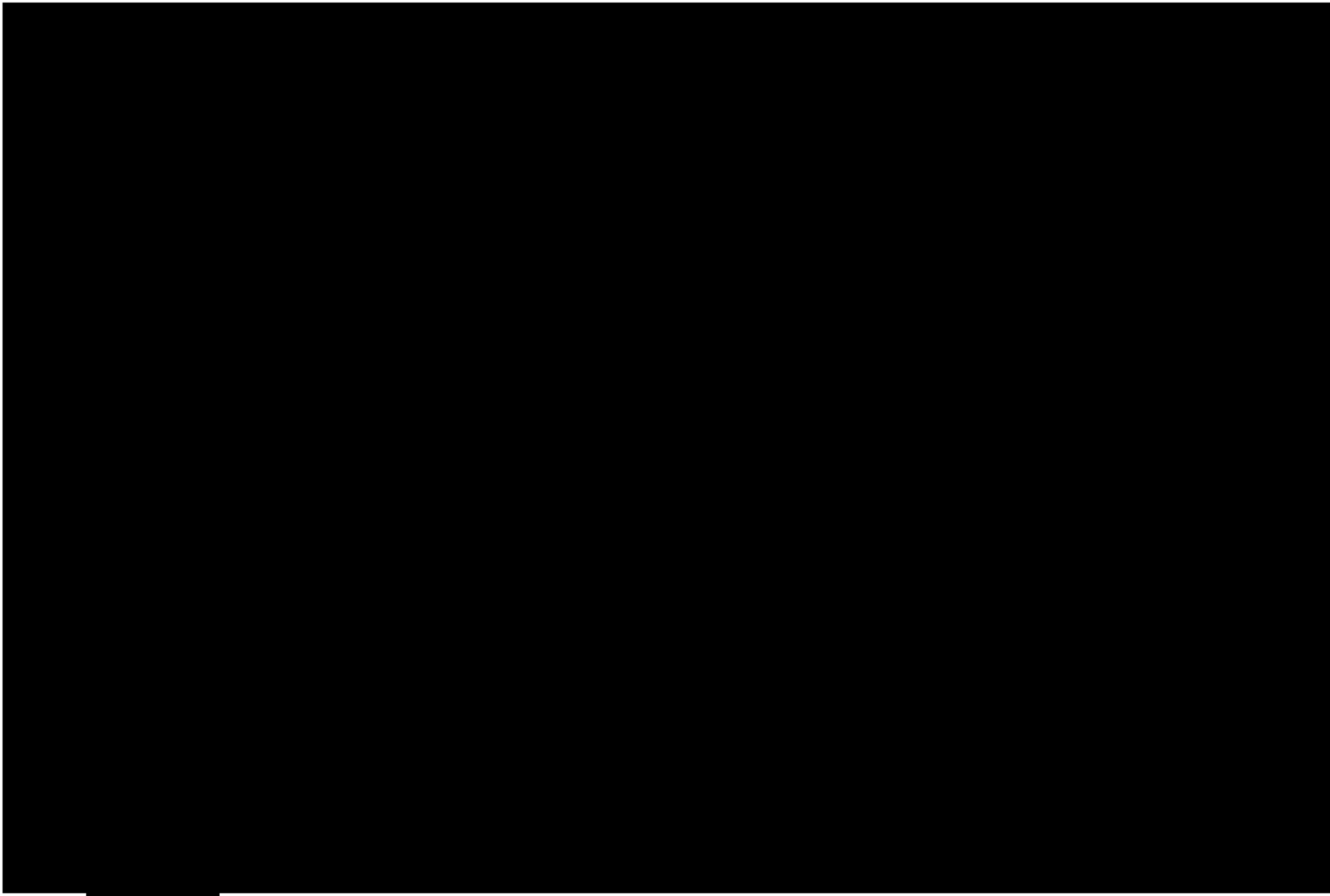
© 2013 Unisys Corporation. All rights reserved.

UNISYS

© 2013 Unisys Corporation. All rights reserved.

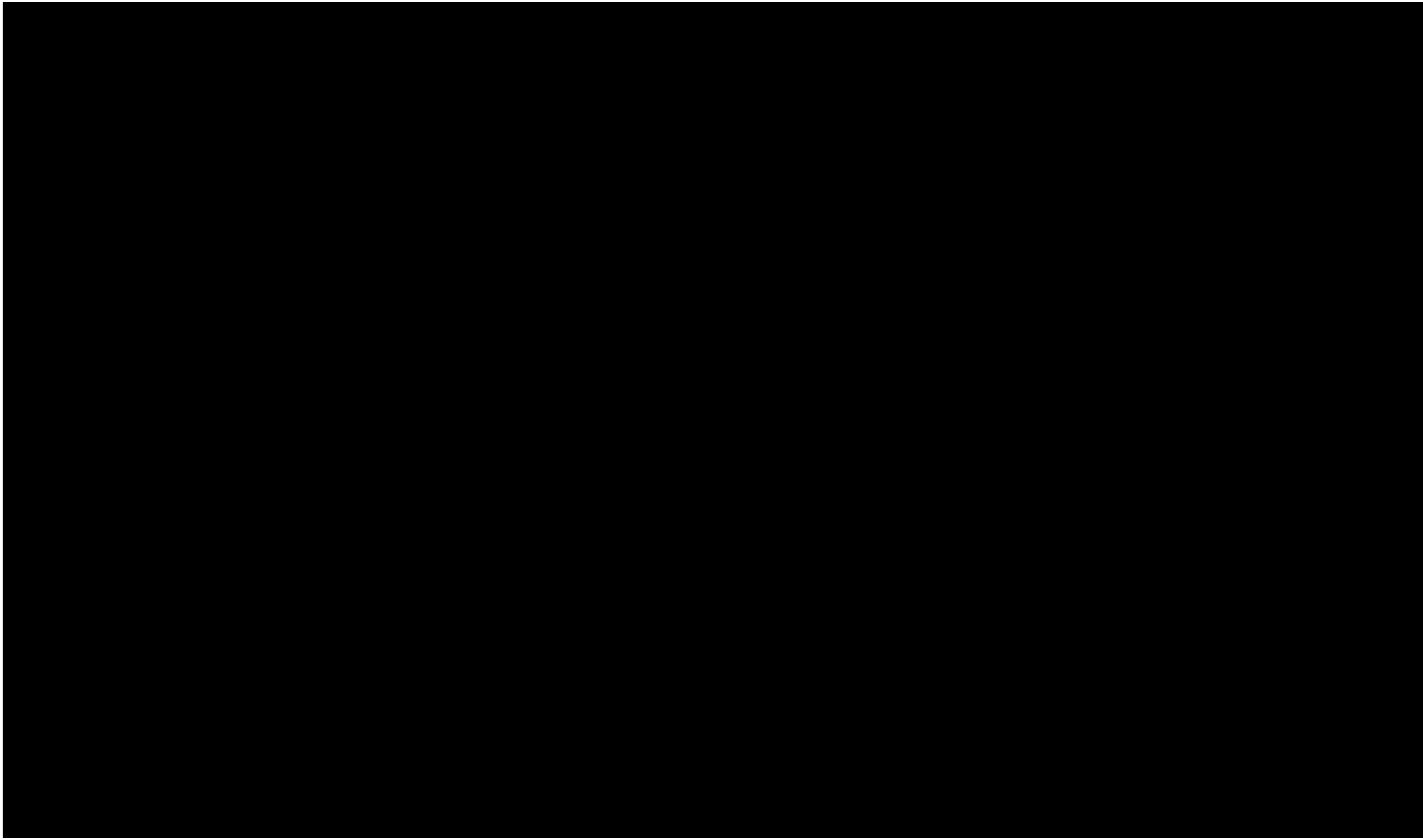


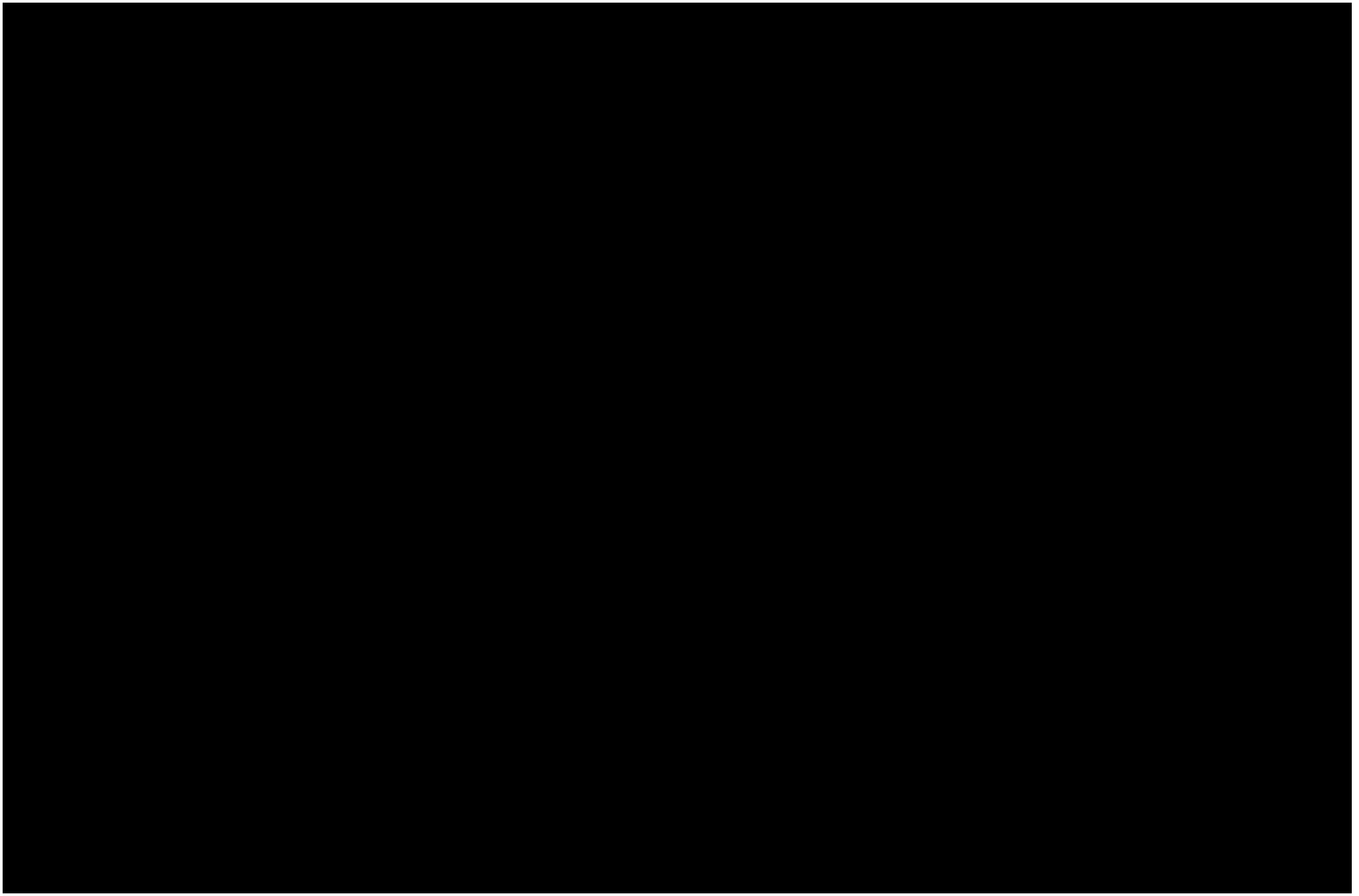
© 2013 Unisys Corporation. All rights reserved.



© 2013 Unisys Corporation. All rights reserved.

© 2013 Unisys Corporation. All rights reserved.





© 2013 Unisys Corporation. All rights reserved.

© 2013 Unisys Corporation. All rights reserved.

Attachment F-8 – Sample Monthly Server Capacity Report

This attachment provides a sample monthly server capacity report.

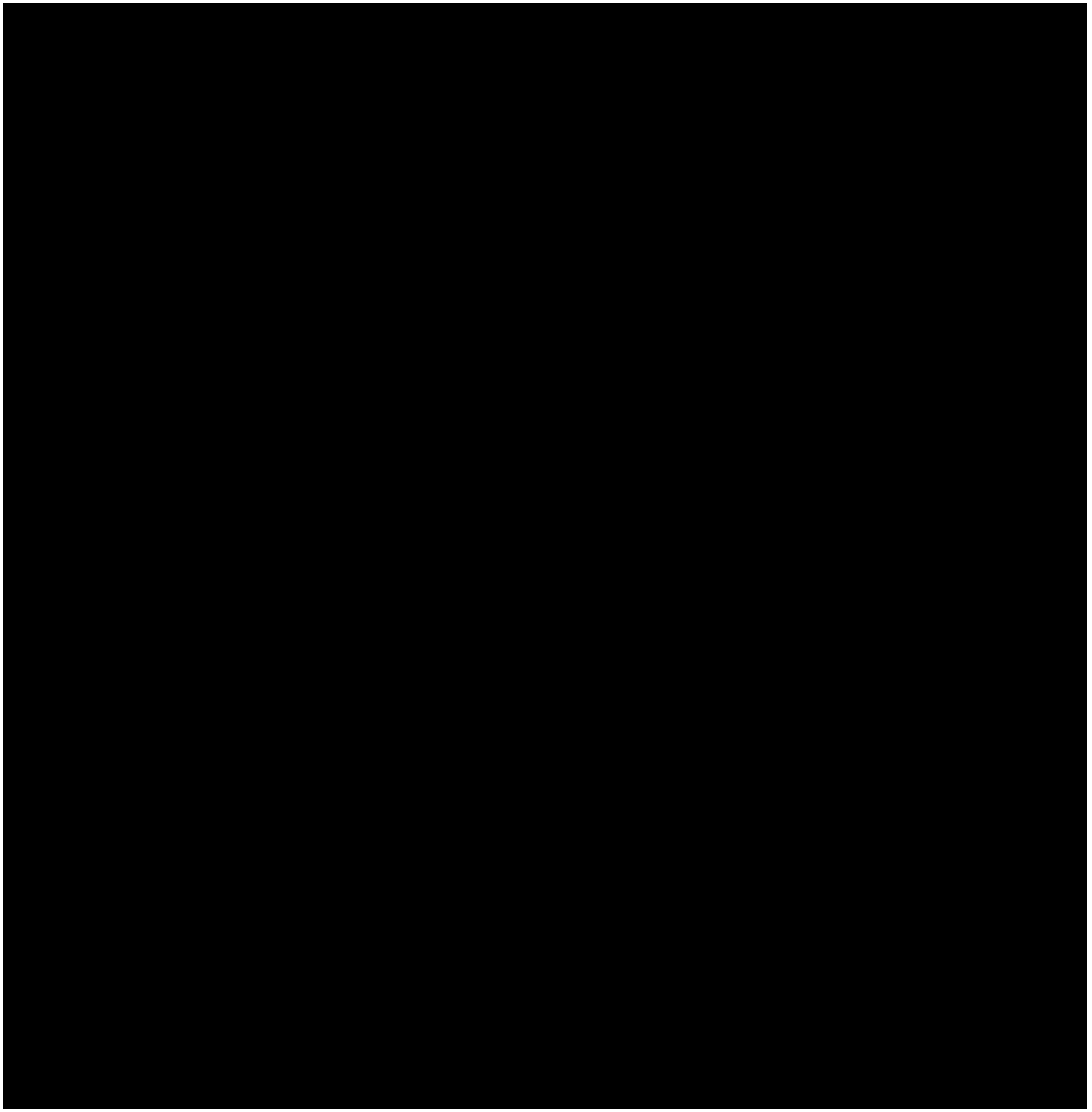
This page intentionally left blank.

UNISYS

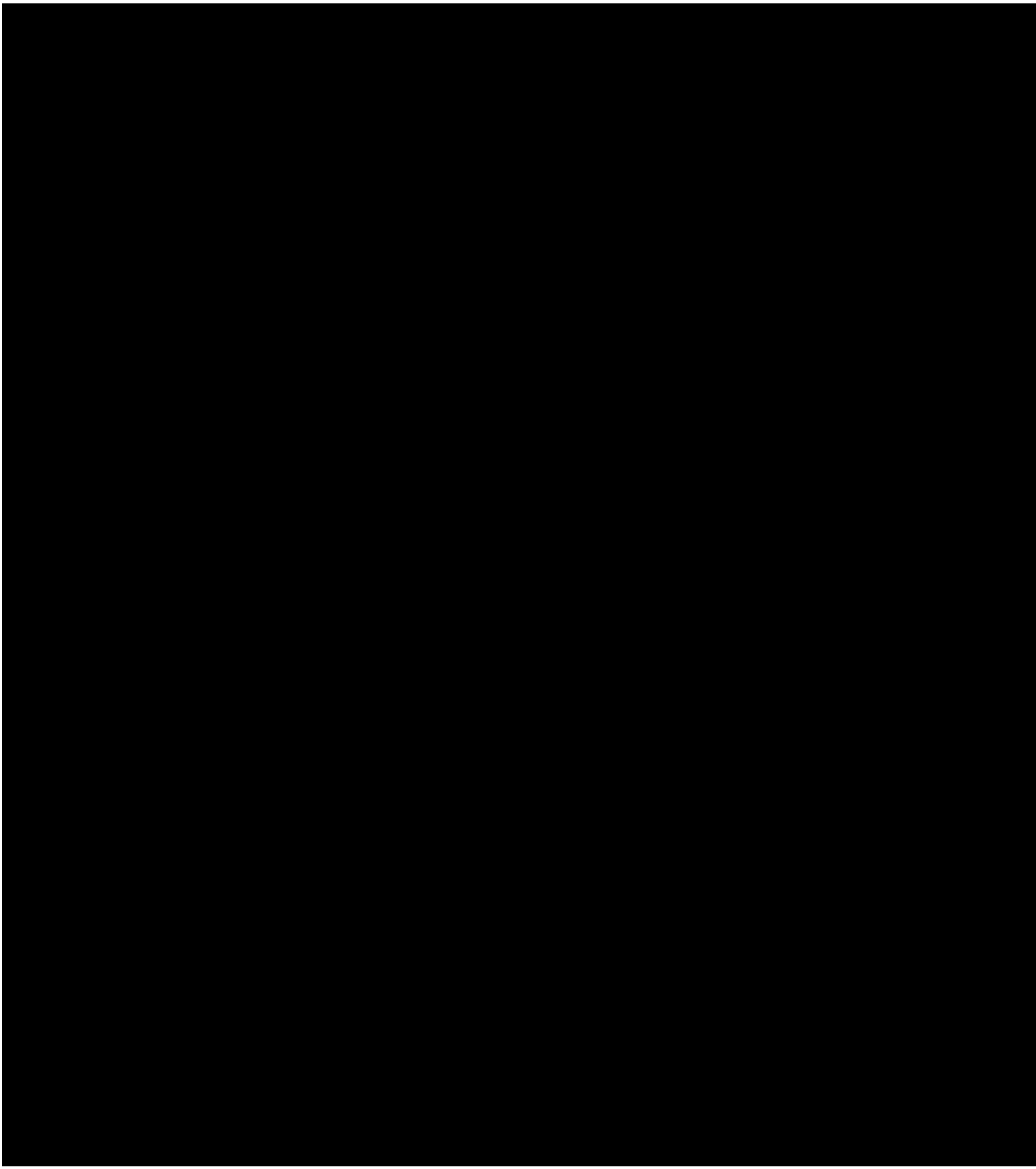
ABC Monthly Capacity Report

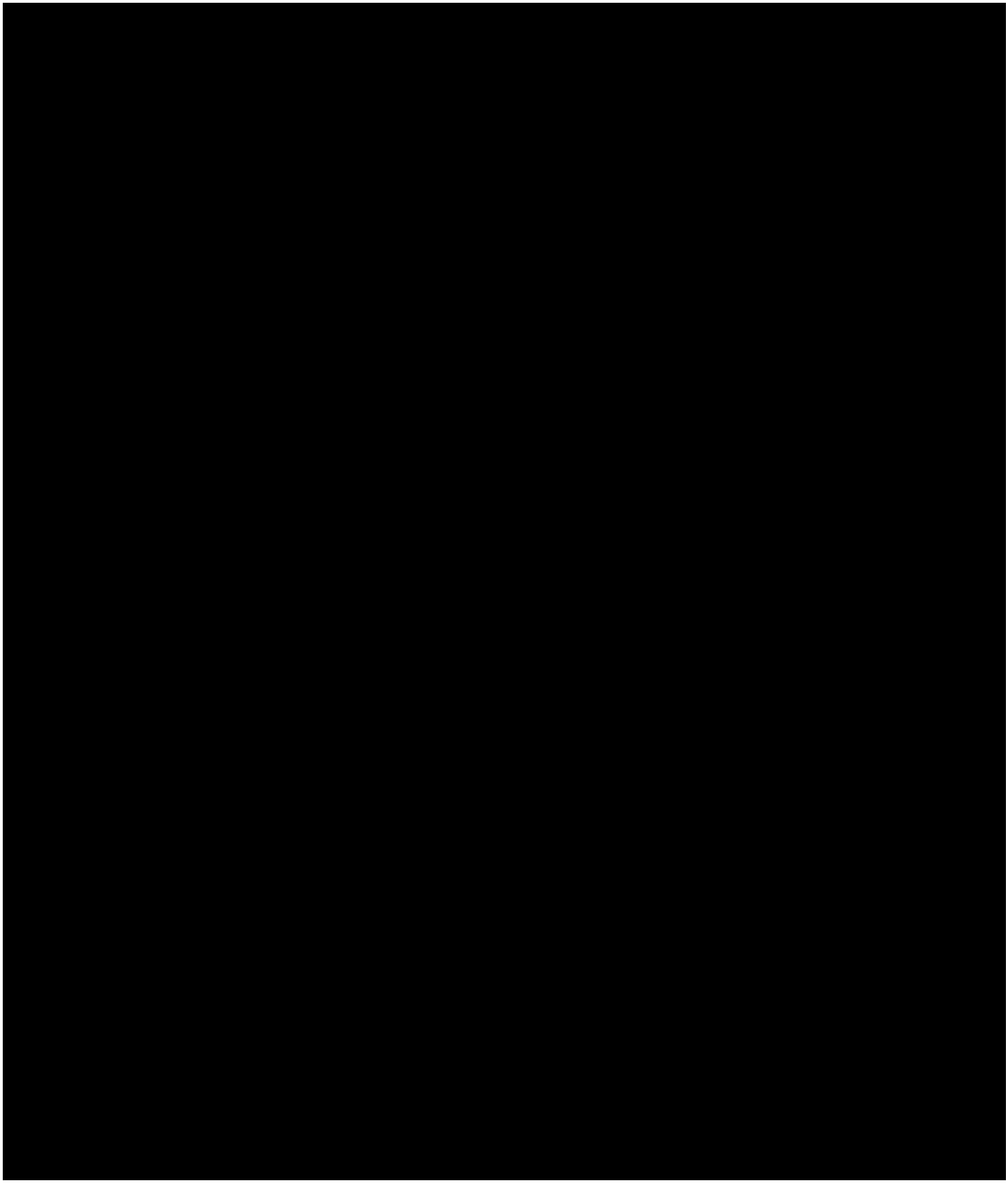
August, 2011

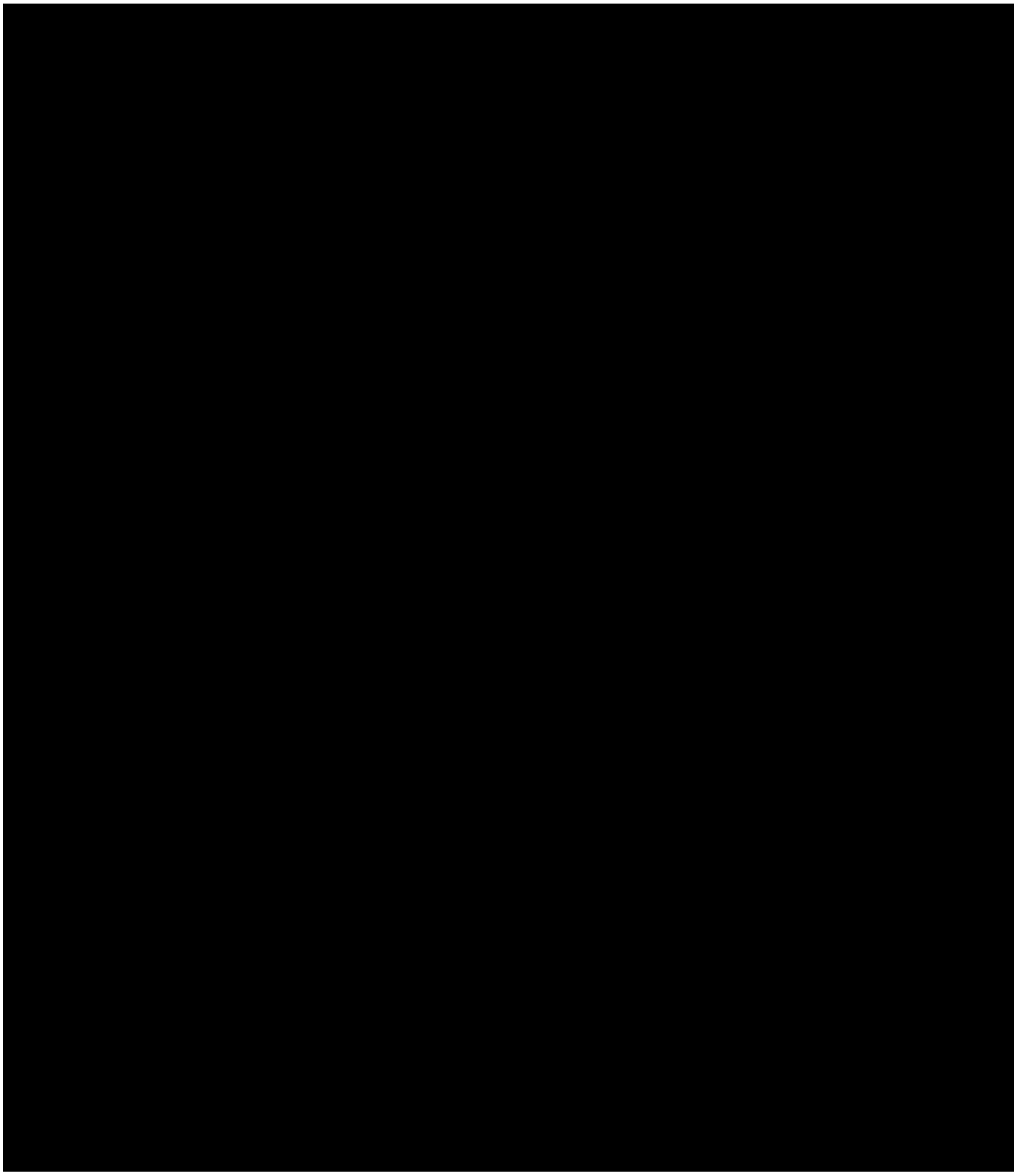
This page intentionally left blank.

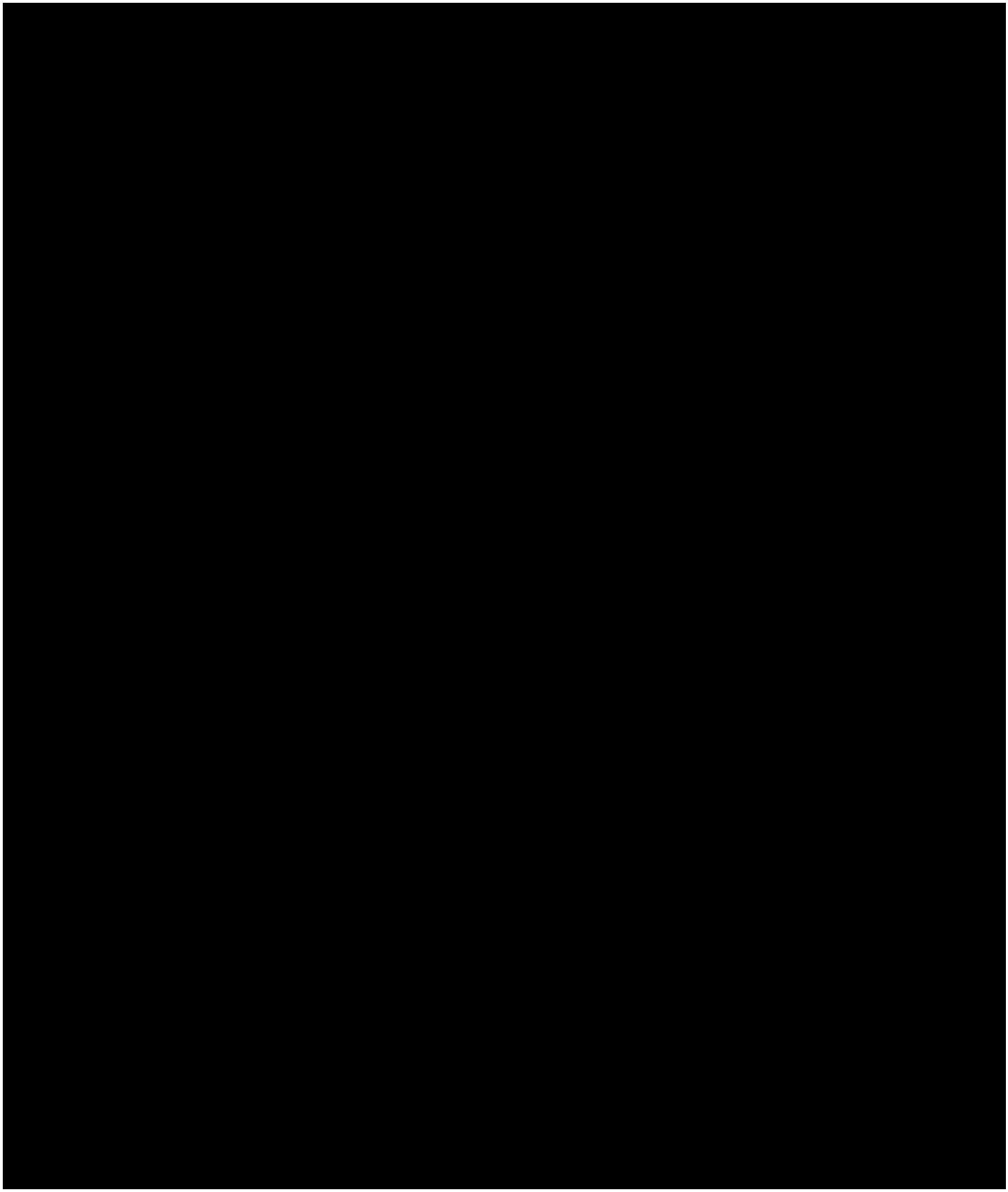


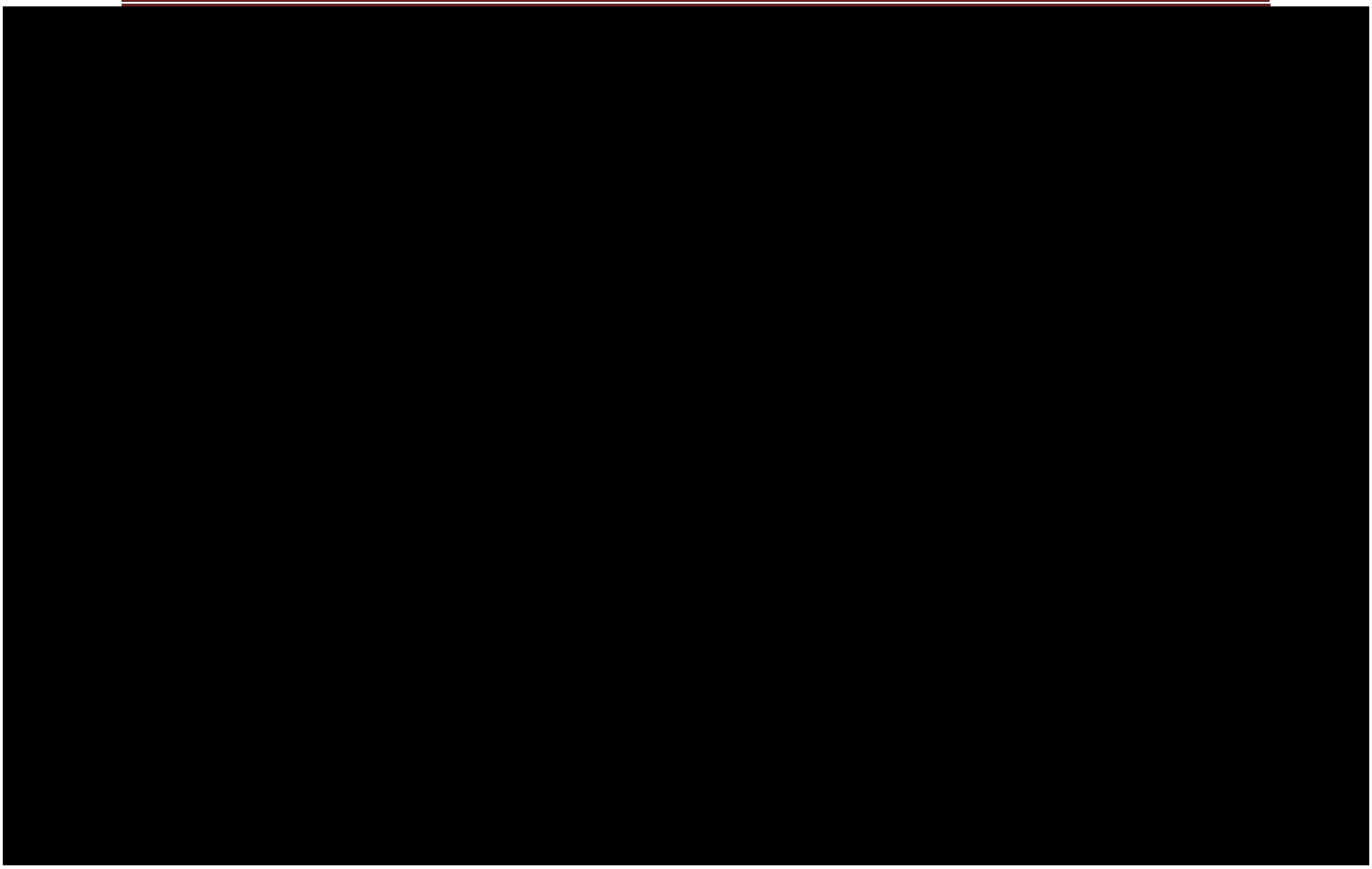
Revision History



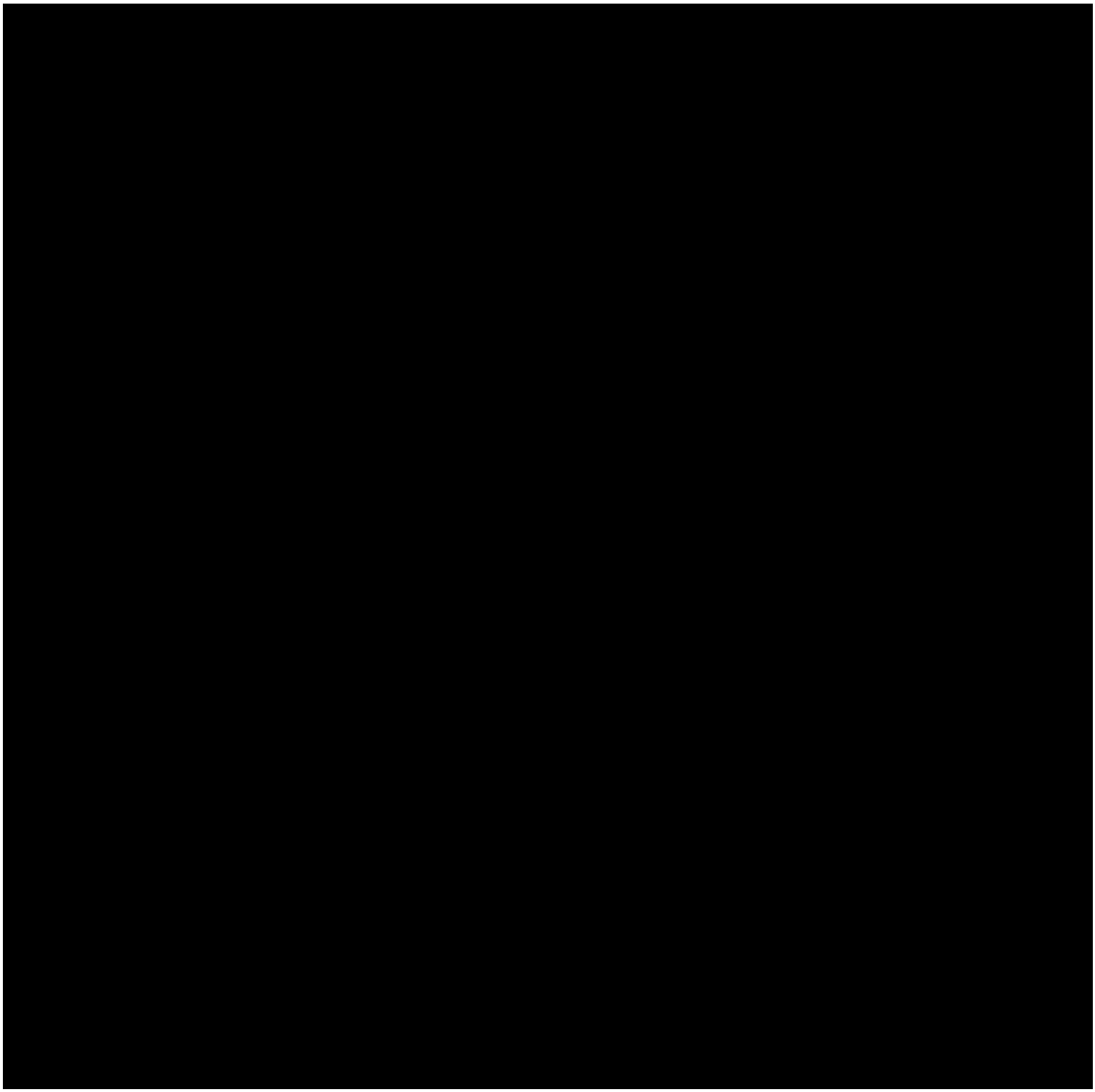




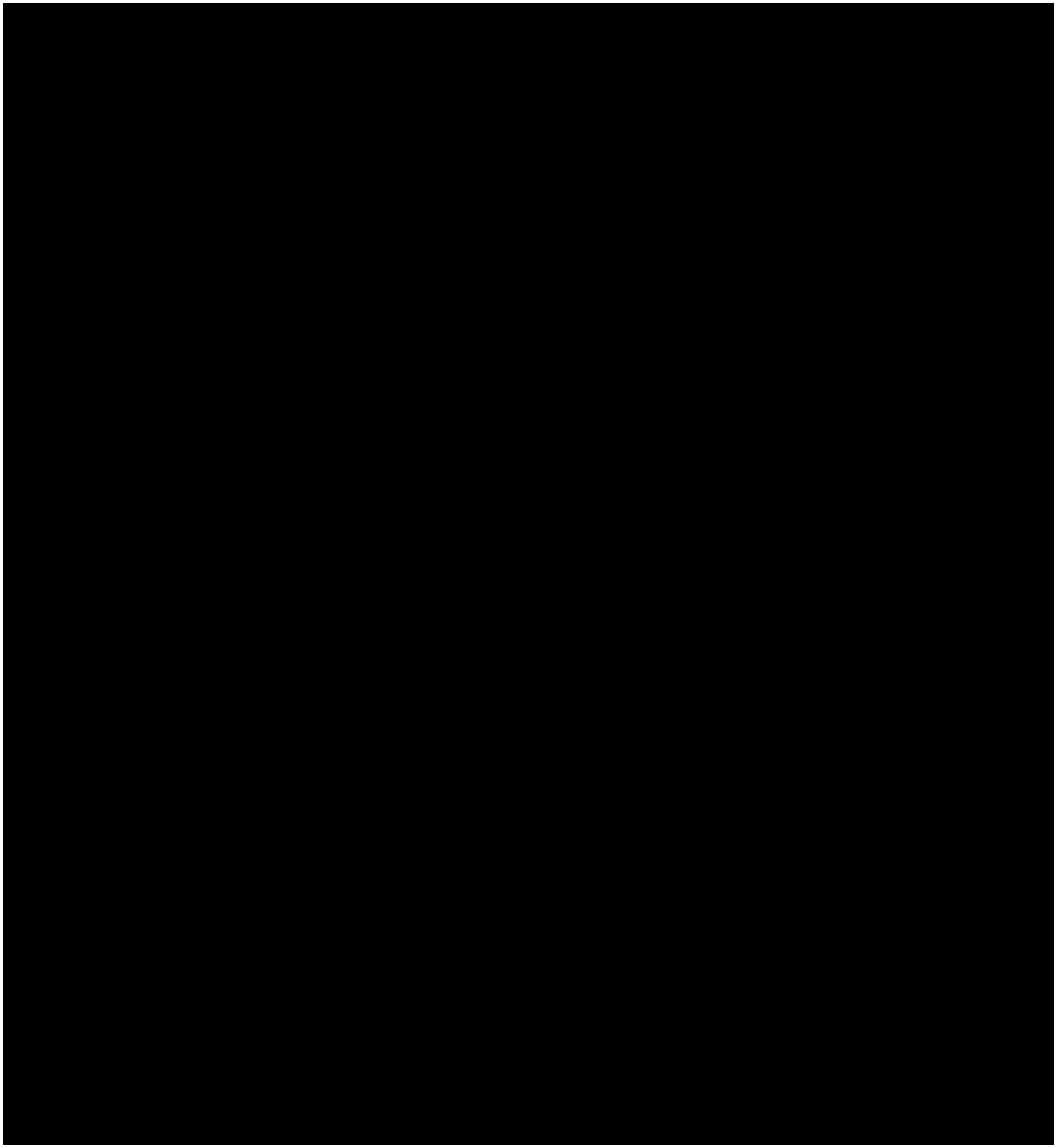


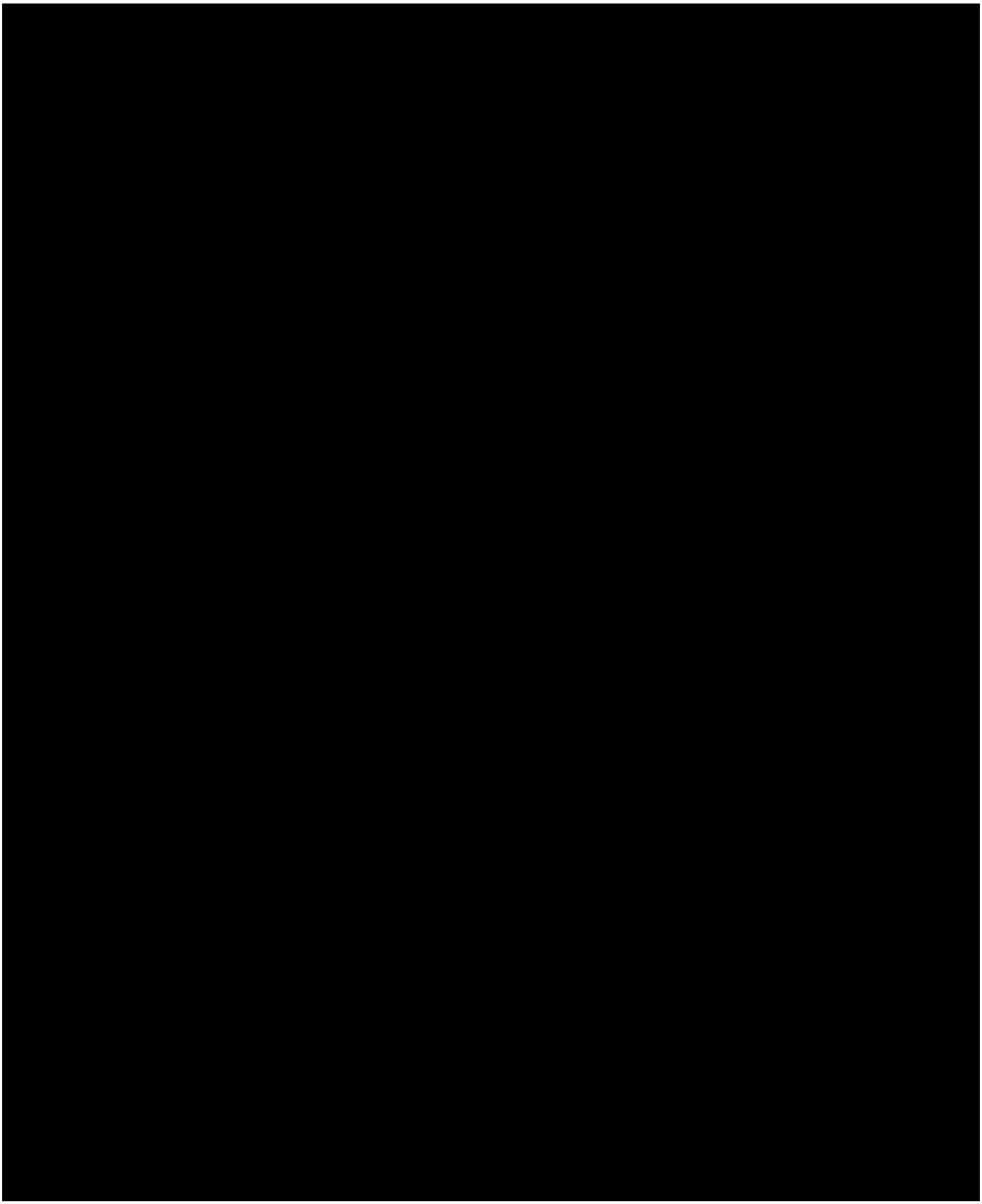


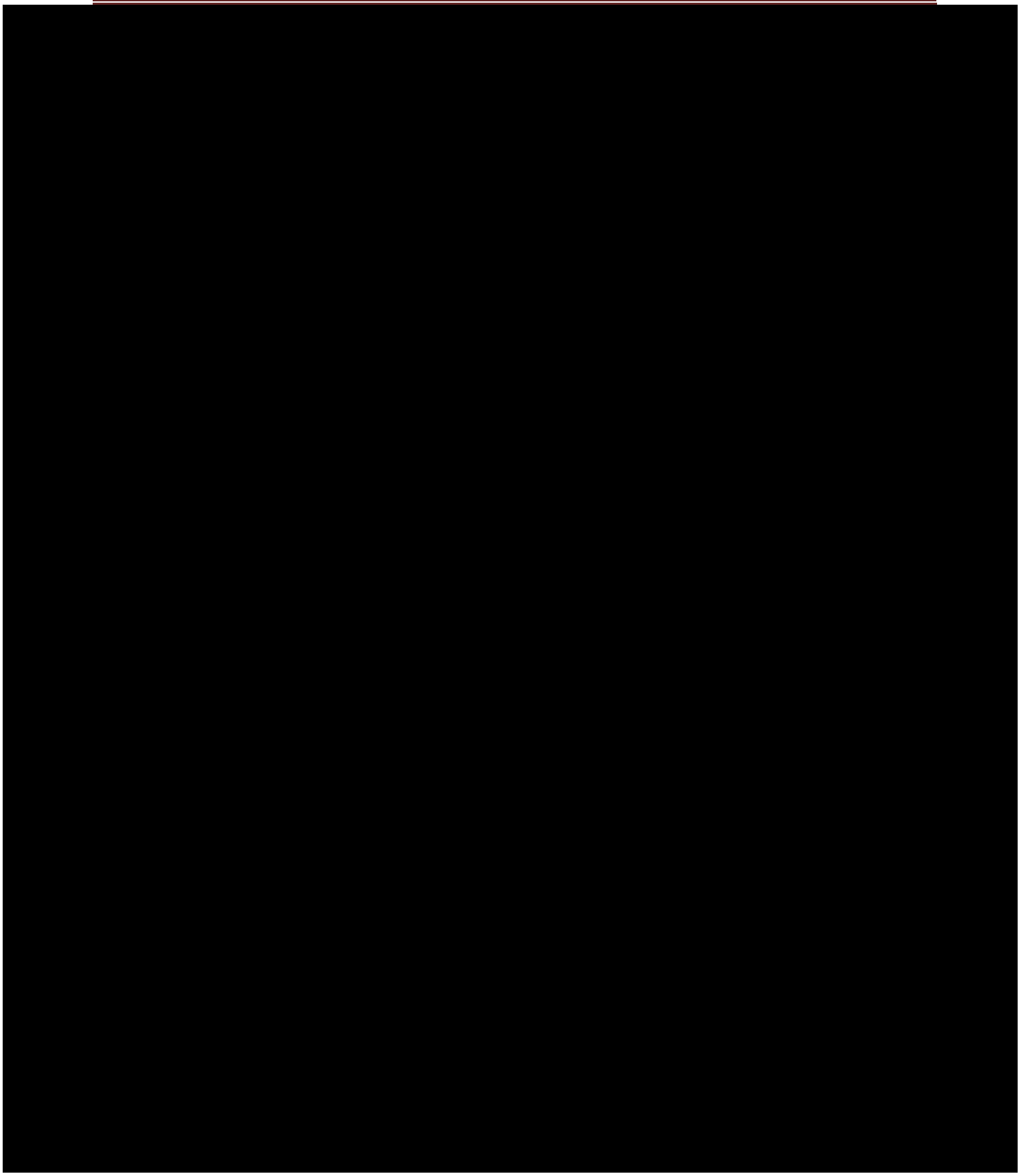
[redacted]

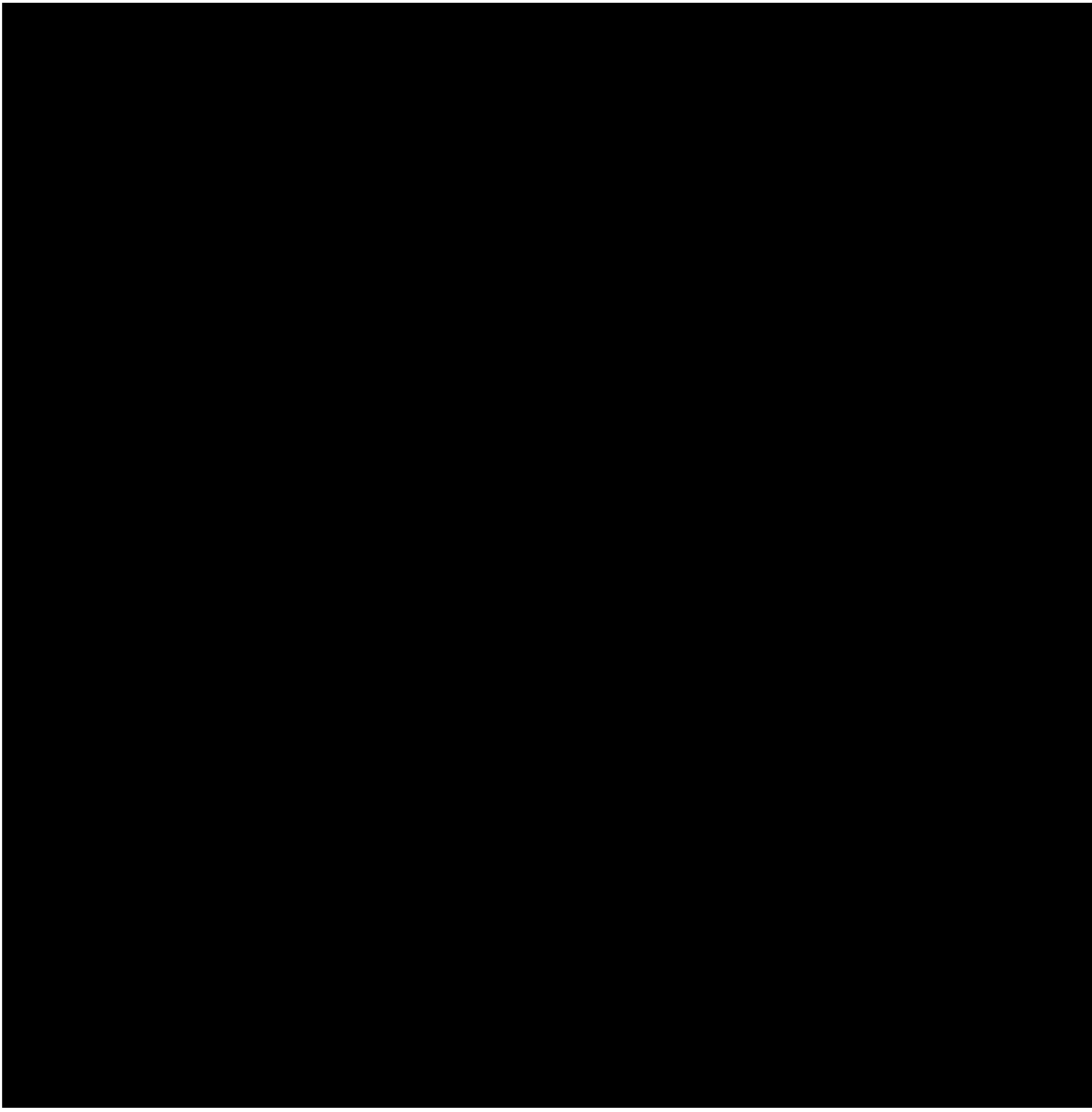


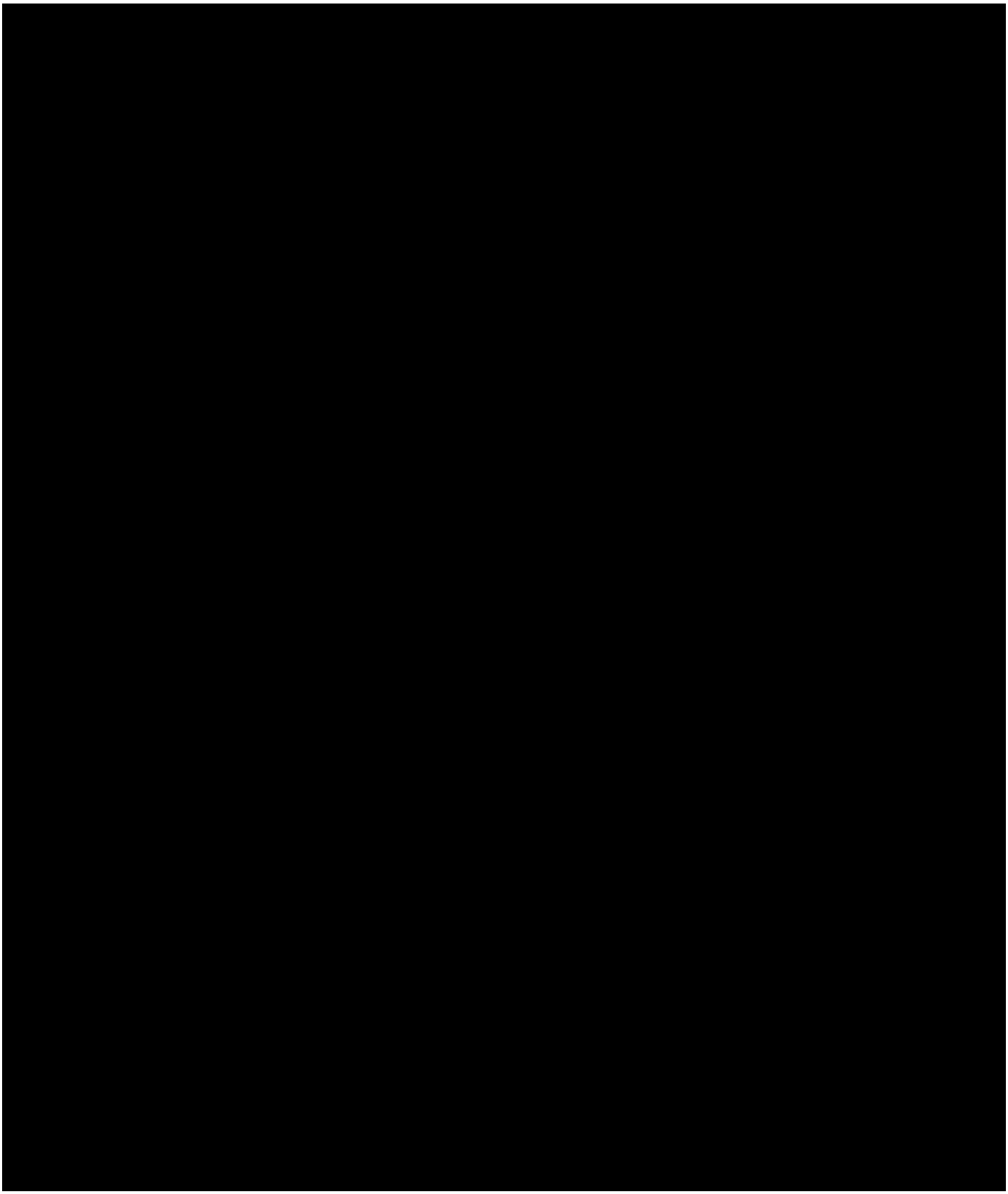
This page intentionally left blank.

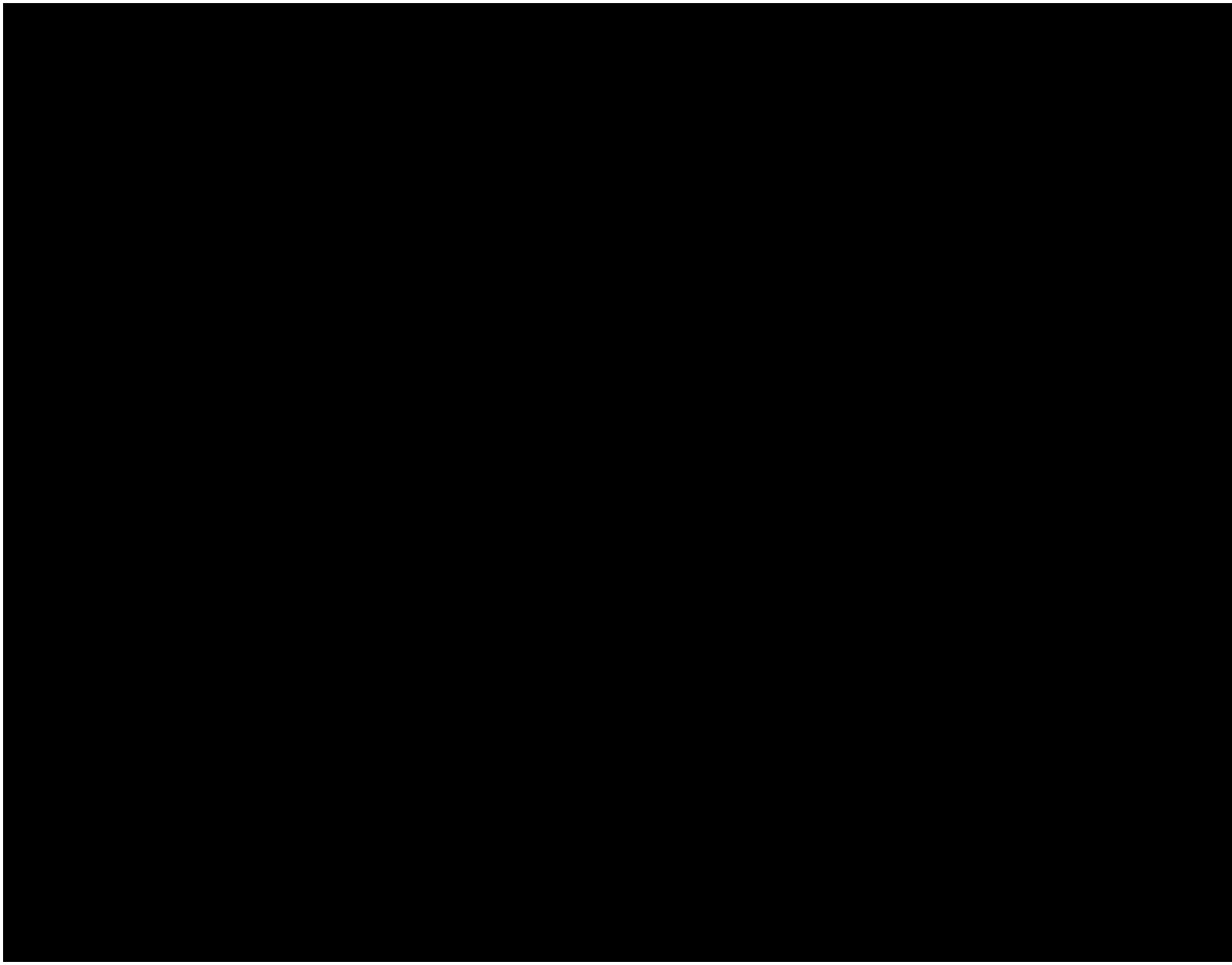


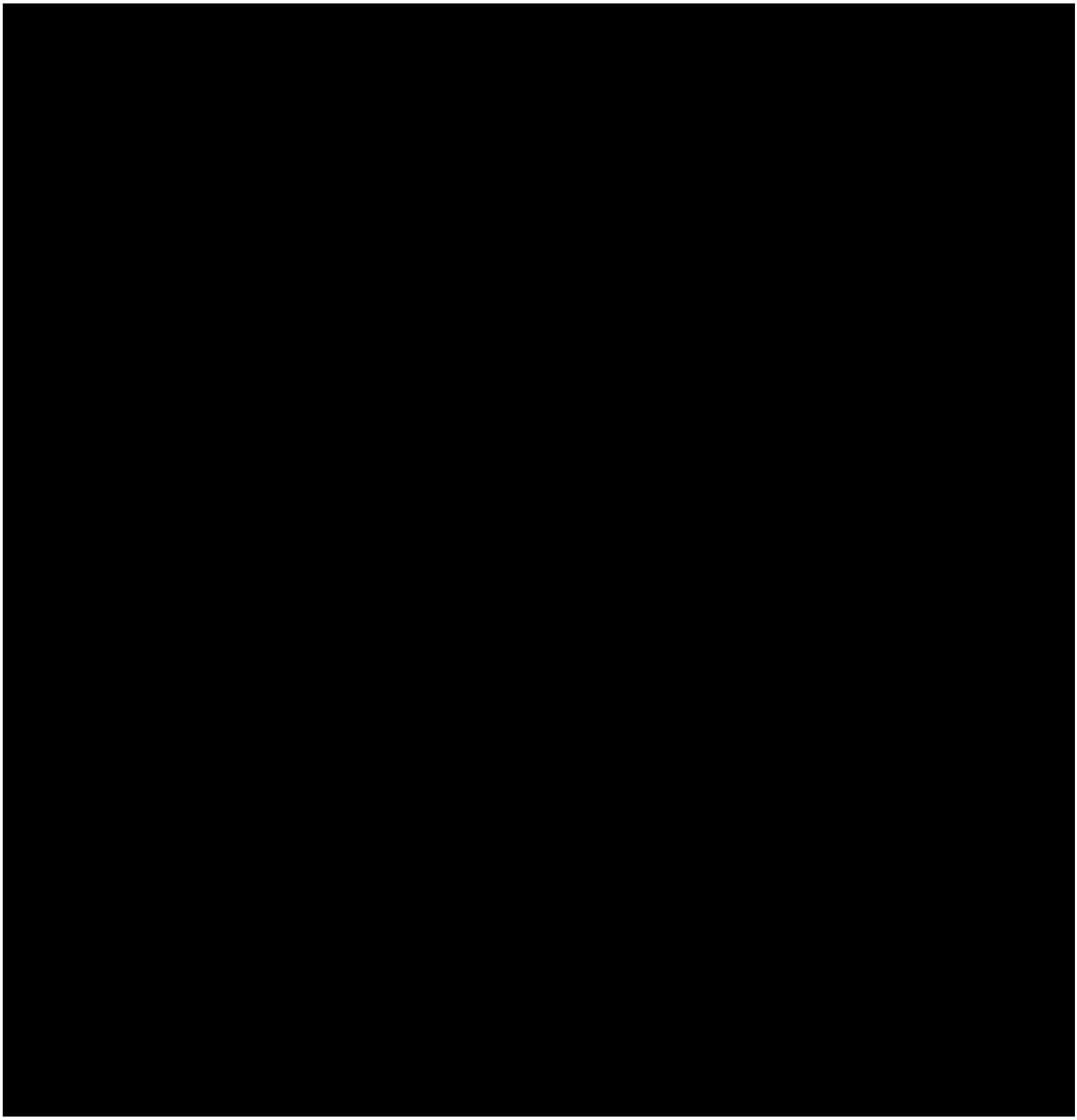












This page intentionally left blank.

Attachment F-9 – Commonwealth of Pennsylvania – Office of Information Technology Enterprise Data Center Security Management Plan

This attachment provides a sample security management plan.

This page intentionally left blank.

Commonwealth of PA
Enterprise Data Center

Security Management Plan Workbook

Date:
Version Number:

(This Page Intentionally Blank)

Access Control (AC) – *Technical*

AC-1 – Access Control Policy and Procedures (Moderate)	
Control The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days: a. A formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

AC-2 – Account Management (Moderate)	
Control The organization manages information system accounts, including: a. Identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary); b. Establishing conditions for group membership; c. Identifying authorized users of the information system and specifying access privileges; d. Requiring appropriate approvals for requests to establish accounts; e. Establishing, activating, modifying, disabling, and removing accounts; f. Specifically authorizing and monitoring the use of guest/anonymous and temporary accounts; g. Notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes; h. Deactivating: (i) temporary accounts that are no longer required; and (ii) accounts of terminated or transferred users; i. Granting access to the system based on: (i) a valid access authorization; (ii) intended system usage; and (iii) other attr butes as required by the organization or associated missions/business functions; and j. Reviewing accounts using the frequency specified in Implementation Standard 1. For FTI: The agency must ensure that only authorized employees or contractors (as allowed by statute) of the agency receiving the information has access to FTI. (Pub 1075, Ref 9.2) **Implementation Standard(s)** 1. Review information system accounts within every one hundred eighty (180) days and require annual certification. 2. Remove or disable default user accounts. Rename active default accounts. 3. Implement centralized control of user access administrator functions. 4. Regulate the access provided to contractors and define security requirements for contractors.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

AC-2(1) – Enhancement (Moderate)	
Control The organization employs automated mechanisms to support the management of information system accounts.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AC-2(2) – Enhancement (Moderate)	
Control The information system automatically terminates emergency accounts within twenty-four (24) hours and temporary accounts with a fixed duration not to exceed three hundred sixty-five (365) days.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AC-2(3) – Enhancement (Moderate)	
Control The information system automatically disables inactive accounts after one hundred eighty (180) days.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AC-2(4) – Enhancement (Moderate)	
Control The information system automatically audits account creation, modification, disabling, and termination actions and notifies, as required, appropriate individuals.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AC-2(7) – Enhancement (Moderate)	
Control The organization: (a) Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles; (b) Tracks and monitors privileged role assignments; and (c) Inspects administrator groups, root accounts and other system related accounts on demand, but at least once every fourteen (14) days to ensure that unauthorized accounts have not been created.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or*

	Common; Indicate All Control Provider(s)]

AC-3 – Access Enforcement (Moderate)

Control

The information system enforces approved authorizations for logical access to the system in accordance with applicable policy.

Implementation Standard(s)

1. If encryption is used as an access control mechanism it must meet approved (FIPS 140-2 compliant and a NIST validated module) encryption standards (see SC-13).
2. If e-authentication is utilized in connection to access enforcement, refer to ARS Appendix D: E-authentication Standard.
3. Configure operating system controls to disable public "read" and "write" access to files, objects, and directories that may directly impact system functionality and/or performance, or that contain sensitive information.
4. Data stored in the information system must be protected with system access controls.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

AC-3(1) – Enhancement (Moderate)

Control

[Withdrawn: Incorporated into AC-6].

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

AC-4 – Information Flow Enforcement (Moderate)

Control

The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

AC-5 – Separation of Duties (Moderate)

Control

The organization:
a. Separates duties of individuals as necessary, to prevent malevolent activity without collusion;
b. Documents separation of duties; and
c. Implements separation of duties through assigned information system access authorizations.

Implementation Standard(s)
1. Ensure that audit functions are not performed by security personnel responsible for administering access control.
2. Maintain a limited group of administrators with access based upon the users' roles and responsibilities.
3. Ensure that critical mission functions and information system support functions are divided among separate individuals.
4. Ensure that information system testing functions (i.e., user acceptance, quality assurance, information security) and production functions are divided among separate individuals or groups.
5. Ensure that an independent entity, not the Business Owner, System Developer(s)/Maintainer(s), or System Administrator(s) responsible for the information system, conducts information security testing of the information system.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

AC-6 – Least Privilege (Moderate)

Control

The organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with missions and business functions.

For FTI: Access to FTI must be strictly on a need-to-know basis. FTI must never be indiscriminately disseminated, even within the recipient agency, body or commission. No person should be given more FTI than is needed for performance of his/her duties.

Implementation Standard(s)
1. Disable all file system access not explicitly required for system, application, and administrator functionality.
2. Contractors must be provided with minimal system and physical access, and must agree to and support the security requirements. The contractor selection process must assess the contractor's ability to adhere to and support security policy.
3. Restrict the use of database management utilities to only authorized database administrators. Prevent users from accessing database data files at the logical data view, field, or field-value level. Implement table-level access control.
4. Ensure that only authorized users are permitted to access those files, directories, drives, workstations, servers, network shares, ports, protocols, and services that are expressly required for the performance of job duties.
5. Disable all system and removable media boot access unless it is explicitly authorized by the CIO for compelling operational needs. If authorized, boot access is password protected.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

AC-6(1) – Enhancement (Moderate)	
Control The organization explicitly authorizes access to privileged functions (e.g., system-level software, administrator tools, scripts, utilities) deployed in hardware, software, and firmware; and security relevant information is restricted to explicitly authorized individuals.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

AC-6(2) – Enhancement (Moderate)	
Control The organization requires that users of information system accounts, or roles, with access to administrator accounts or security functions, use non-privileged accounts, or roles, when accessing other system functions, and if feas ble, audits any use of privileged accounts, or roles, for such functions.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

AC-7 – Unsuccessful Login Attempts (Moderate)	
Control The information system: a. Enforces the limit of consecutive invalid login attempts by a user specified in Implementation Standard 1 during the time period specified in Implementation Standard 1; and b. Automatically disables or locks the account/node until released after the time period specified in Implementation Standard 1 when the maximum number of unsuccessful attempts is exceeded. The control applies regardless of whether the login occurs via a local or network connection. **Implementation Standard(s)** 1. Configure the information system to lock out the user account automatically after three (3) failed log-on attempts by a user. For FTI: Automatically lock the account/node until an authorized system administrator reinstates the account (Pub 1075 Ref. Exhibit 8)	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

AC-8 – System Use Notification (Moderate)

Control

The information system:
a. Displays an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The approved banner for information systems is:
- You are accessing a U.S. Government information system, which includes: (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only.
- Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties.
- By using this information system, you understand and consent to the following:
  * You have no reasonable expectation of privacy regarding any communication or data transiting or stored on this information system. At any time, and for any lawful Government purpose, the Government may monitor, intercept, and search and seize any communication or data transiting or stored on this information system.
  * Any communication or data transiting or stored on this information system may be disclosed or used for any lawful Government purpose.

b. Retains the notification message or banner on the screen until users take explicit actions to log on to or further access the information system; and
c. For publicly accessible systems: (i) displays the system use information when appropriate, before granting further access; (ii) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and (iii) includes in the notice given to public users of the information system, a description of the authorized uses of the system.

For FTI: The warning banner must contain reference to the civil and criminal penalty sections of Title 26 Sections 7213, 7213A and 7431. (Pub 1075, Sec 9.2; Exhibit 13)

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

AC-10 – Concurrent Session Control (Moderate)

Control

The information system limits the number of concurrent sessions for each system account to one (1) session. The number of concurrent application/process sessions is limited and enforced to the number of sessions expressly required for the performance of job duties and any requirement for more than one (1) concurrent application/process session is documented in the security plan.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

AC-11 – Session Lock (Moderate)

Control

The information system:
a. Prevents further access to the system by initiating a session lock after fifteen (15) minutes of inactivity; and
b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

AC-12 – Session Termination (Moderate)	
Control [Withdrawn: Incorporated into SC-10].	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AC-13 – Supervision and Review--Access Control (Moderate)	
Control [Withdrawn: Incorporated into AC-2 and AU-6].	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AC-14 – Permitted Actions without Identification or Authentication (Moderate)	
Control The organization: a. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification and authentication; and b. Configures Information systems to permit public access only to the extent necessary to accomplish mission objectives, without first requiring individual identification and authentication. **Implementation Standard(s)** 1. Identify and document specific user actions that can be performed on the information system without identification or authentication.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AC-14(1) – Enhancement (Moderate)	
Control The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission/business objectives.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

AC-15 – Automated Marking (Moderate)	
Control [Withdrawn: Incorporated into MP-3].	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

AC-17 – Remote Access (Moderate)	
Control Remote access for privileged functions shall be permitted only for compelling operational needs, shall be strictly controlled, and must be explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the organization: a. Documents allowed methods of remote access to the information system; b. Establishes usage restrictions and implementation guidance for each allowed remote access method; c. Monitors for unauthorized remote access to the information system; d. Authorizes remote access to the information system prior to connection; and e. Enforces requirements for remote connections to the information system. **Implementation Standard(s)** 1. Require callback capability with re-authentication to verify connections from authorized locations when the Medicare Data Communications Network (MDCN) or Multi-Protocol Label Switching (MPLS) service network cannot be used. 2. If e-authentication is implemented as a remote access solution or associated with remote access, refer to ARS Appendix D: E-authentication Standard. For FTI, complete Safeguard Procedures Report (SPR) section 9.20.3.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

AC-17(1) – Enhancement (Moderate)	
Control The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

AC-17(2) – Enhancement (Moderate)	
Control The organization uses cryptography to protect the confidentiality and integrity of remote access sessions.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or*

	Common; Indicate All Control Provider(s)]
AC-17(3) – Enhancement (Moderate)	
Control The information system routes all remote accesses through a limited number of managed access control points.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AC-17(4) – Enhancement (Moderate)	
Control The organization authorizes the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs and documents the rationale for such access in the security plan for the information system.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AC-17(5) – Enhancement (Moderate)	
Control The organization monitors for unauthorized remote connections to the information system at least quarterly, and takes appropriate action if an unauthorized connection is discovered.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AC-17(7) – Enhancement (Moderate)	
Control The organization ensures that remote sessions used for remote administration employ additional security measures (e.g., Secure Shell [SSH], Virtual Private Networking [VPN] with blocking mode enabled) and the approved encryption standard (see SC-13), and the sessions are audited.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AC-17(8) – Enhancement (Moderate)	
Control The organization disables Bluetooth and peer-to-peer networking protocols within the information system except for explicitly identified components in support of specific operational requirements.	

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

AC-18 – Wireless Access (Moderate)

Control

The organization prohibits the installation of wireless access points (WAP) to information systems unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the organization:
a. Monitors for unauthorized wireless access to the information system; and
b. Enforces requirements for wireless connections to the information system.

Implementation Standard(s)
1. If wireless access is explicitly approved, wireless device service set identifier broadcasting is disabled and the following wireless access controls are implemented:
(a) Encryption protection is enabled;
(b) Access points are placed in secure areas;
(c) Access points are shut down when not in use (i.e., nights, weekends);
(d) A firewall is implemented between the wireless network and the wired infrastructure;
(e) MAC address authentication is utilized;
(f) Static IP addresses, not DHCP, is utilized;
(g) Personal firewalls are utilized on all wireless clients;
(h) File sharing is disabled on all wireless clients;
(i) Intrusion detection agents are deployed on the wireless side of the firewall; and
(j) Wireless activity is monitored and recorded, and the records are reviewed on a regular basis.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

AC-18(1) – Enhancement (Moderate)

Control

If wireless access is explicitly approved, the information system protects wireless access to the system using authentication and encryption.

For FTI: The agency shall authorize, document, and monitor all wireless access to the information system in accordance with NIST 800-48 Revision 1 (Pub 1075 Ref. 9.2)

For FTI, complete SPR section 9.20.3.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

AC-18(2) – Enhancement (Moderate)

Control

The organization monitors for unauthorized wireless connections to the information system, including scanning for unauthorized wireless access points quarterly, and takes

appropriate action if an unauthorized connection is discovered.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

AC-19 – Access Control for Mobile Devices (Moderate)

Control

The organization prohibits the connection of portable and mobile devices (e.g., notebook computers, personal digital assistants [PDA], cellular telephones, and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations) to information systems unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the organization:
a. Employs an approved method of cryptography (see SC-13) to protect information residing on portable and mobile information devices, and utilizes whole-disk encryption solution for laptops;
b. Monitors for unauthorized connections of mobile devices to information systems;
c. Enforces requirements for the connection of mobile devices to information systems;
d. Disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction;
e. Issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures; and
f. Protects the storage and transmission of information on portable and mobile information devices with activities such as scanning the devices for malicious code, virus protection software.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

AC-19(1) – Enhancement (Moderate)

Control

The organization restricts the use of writable, removable media in information systems.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

AC-19(2) – Enhancement (Moderate)

Control

The organization prohibits the use of personally owned, removable media in information systems.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

AC-19(3) – Enhancement (Moderate)

Control

The organization prohibits the use of removable media in information systems when the media has no identifiable owner.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

AC-20 – Use of External Information Systems (Moderate)

Control

The organization proh bits the use of external information systems, including but not limited to, Internet kiosks, personal desktop computers, laptops, tablet personal computers, personal digital assistant (PDA) devices, cellular telephones, facsimile machines, and equipment available in hotels or airports to store, access, transmit, or process sensitive information, unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the organization establishes strict terms and conditions for their use. The terms and conditions shall address, at a minimum:
a. The types of applications that can be accessed from external information systems;
b. The maximum FIPS 199 security category of information that can be processed, stored, and transmitted;
c. How other users of the external information system will be prevented from accessing federal information;
d. The use of virtual private networking (VPN) and firewall technologies;
e. The use of and protection against the vulnerabilities of wireless technologies;
f. The maintenance of adequate physical security controls;
g. The use of virus and spyware protection software; and
h. How often the security capabilities of installed software are to be updated.

Implementation Standard(s)
1. Instruct all personnel working from home to implement fundamental security controls and practices, including passwords, virus protection, and personal firewalls. Limit remote access only to information resources required by home users to complete job duties. Require that any government-owned equipment be used only for business purposes by authorized employees.
2. (For PII only) Only organization owned computers and software can be used to process, access, and store PII.

For FTI:
3. If the agency allows alternative work sites, such as employee's home or other non-traditional work sites, the FTI remains subject to the same safeguard requirements as the agency's offices. (Pub. 1075, Ref 4.7)
4. Only agency-owned computers, media and software will be used to receive, process, access and store FTI. The agency must retain ownership and control for the security configuration of all hardware, software and end-point equipment connecting to public communication networks including encryption keys. (Pub. 1075, Ref 4.7.1)

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

AC-20(1) – Enhancement (Moderate)

Control

The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization:
(a) Can verify the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or
(b) Has approved information system connection or processing agreements with the organizational entity hosting the external information system.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or*

	Common; Indicate All Control Provider(s)]
AC-20(2) – Enhancement (Moderate)	
Control The organization limits the use of organization-controlled portable storage media by authorized individuals on external information systems.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AC-22 – Publicly Accessible Content (Moderate)	
Control The organization: a. Designates individuals authorized to post information onto an information system that is publicly accessible; b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information; c. Reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the information system; d. Reviews the content on the publicly accessible information system for nonpublic information monthly; and e. Removes nonpublic information from the publicly accessible information system, if discovered.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Access Control Family (AC) Security Controls Detail and Comment

Awareness and Training (AT) – *Operational*

AT-1 – Security Awareness and Training Policy and Procedures (Moderate)	
Control The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days: a. A formal, documented security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

AT-2 – Security Awareness (Moderate)	
Control The organization provides basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users prior to accessing any system's information, when required by system changes, and within every three hundred sixty-five (365) days thereafter. For FTI: Awareness training specific to protecting FTI and the sanctions for misuse of FTI must be provided initially prior to granting access to FTI and annually thereafter. (Pub. 1075 Ref. 6.2, 9.4)	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

AT-3 – Security Training (Moderate)	
Control The organization provides role-based security-related training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) refresher training within every three hundred sixty-five (365) days thereafter. For FTI: The disclosure awareness requirements apply to all agency employees with access to FTI, including program and information technology personnel and contractors, such as case workers, managers, system administrators, database administrators and application developers. (Pub. 1075, Ref 6.2 and 9.4) **Implementation Standard(s)** 1. Require personnel with significant information security roles and responsibilities to undergo appropriate information system security training prior to authorizing access to networks, systems, and/or applications; when required by system changes; and refresher training within every three hundred sixty-five (365) days thereafter.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

AT-4 – Security Training Records (Moderate)	
Control The organization: a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and b. Retains individual training records for three (3) years. For FTI: Granting employees or contractors access to FTI must be preceded by each employee or contractor certifying his/her understanding of the agency's security policy and procedures for safeguarding FTI. The certification must be maintained for 5 years. (Pub 1075, section 6.2)	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Awareness and Training Family (AT) Security Controls Detail and Comment

Audit and Accountability (AU) – *Technical*

AU-1 – Audit and Accountability Policy and Procedures (Moderate)	
Control The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days: a. A formal, documented audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

AU-2 – Auditable Events (Moderate)

Control

The organization:
a. Determines, based on a risk assessment and mission/business needs, that the information system must be capable of auditing the list of auditable events specified in the Implementation Standards;
b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events; and
c. Determines, based on current threat information and ongoing assessment of risk, which events require auditing on a continuous basis and which events require auditing in response to specific situations.

For FTI: Audit logs must enable tracking activities taking place on the system. Pub 1075, Exh bit 9, System Audit Management Guidelines, contains requirements for creating audit-related processes at both the application, auditing must be enabled to the extent necessary to capture access, modification, deletion and movement of FTI by each unique user. This auditing requirement also applies to data tables or databases embedded in or residing outside of the application that contain FTI. (Pub 1075 9.3, Ref. Exhibit 9)

Implementation Standard(s)
1. Generate audit records for the following events:
(a) User account management activities,
(b) System shutdown,
(c) System reboot,
(d) System errors,
(e) Application shutdown,
(f) Application restart,
(g) Application errors,
(h) File creation,
(i) File deletion,
(j) File modification,
(k) Failed and successful log-ons,
(l) Security policy modifications, and
(m) Use of administrator privileges.
2. Enable logging for perimeter devices, including firewalls and routers.
(a) Log packet screening denials originating from un-trusted networks,
(b) Packet screening denials originating from trusted networks,
(c) User account management,
(d) Modification of packet filters,
(e) Application errors,
(f) System shutdown and reboot,
(g) System errors, and
(h) Modification of proxy services.
3. Verify that proper logging is enabled in order to audit administrator activities.

For FTI: Generate audit records for the following events in addition to those specified in other controls, plus those bolded above:
(a) All successful and unsuccessful authorization attempts.
(b) All changes to logical access control authorities (e.g., rights, permissions).
(c) All system changes with the potential to compromise the integrity of audit policy configurations, security policy configurations and audit record generation services.
(d) The audit trail shall capture the enabling or disabling of audit report generation services.

(e) The audit trail shall capture command line changes, batch file changes and queries made to the system (e.g., operating system, application, and database).

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AU-2(1) – Enhancement (Moderate)	
Control [Withdrawn: Incorporated into AU-12].	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AU-2(2) – Enhancement (Moderate)	
Control [Withdrawn: Incorporated into AU-12].	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AU-2(3) – Enhancement (Moderate)	
Control The organization reviews and updates the list of auditable events within every three hundred sixty-five (365) days.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AU-2(4) – Enhancement (Moderate)	
Control The organization includes execution of privileged functions in the list of events to be audited by the information system, including administrator and user account activities, failed and successful log-on, security policy modifications, use of administrator privileges, system shutdowns, reboots, errors and access authorizations.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

AU-3 – Content of Audit Records (Moderate)	
Control The information system produces audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event. **Implementation Standard(s)** 1. (For PHI only) Record disclosures of sensitive information, including protected health and financial information. Log information type, date, time, receiving party, and releasing party. Verify within every ninety (90) days for each extract that the data is erased or its use is still required.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AU-3(1) – Enhancement (Moderate)	
Control The information system includes the capability to include more detailed information in the audit records for audit events identified by type, location, or subject.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AU-4 – Audit Storage Capacity (Moderate)	
Control The organization allocates audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AU-5 – Response to Audit Processing Failures (Moderate)	
Control The information system: a. Alerts designated organizational officials in the event of an audit processing failure; and b. Takes the following additional actions in response to an audit failure or audit storage capacity issue: - Shutdown the information system, - Stop generating audit records, or - Overwrite the oldest records, in the case that storage media is unavailable. For FTI: Shutting down the system, stopping the generation of audit reports or overwriting the oldest records is not an appropriate action. (Pub 1075 section 3.0)	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

AU-6 – Audit Review, Analysis, and Reporting (Moderate)	
Control The organization: a. Reviews and analyzes information system audit records regularly for indications of inappropriate or unusual activity, and reports findings to designated organizational officials; and b. Adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to operations, assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information. For FTI: All requests for return information, including receipt and/or disposal of returns or return information, shall be maintained in a log. (see IRS Pub. 1075, section 3.0) **Implementation Standard(s)** 1. Review system records for initialization sequences, log-ons and errors; system processes and performance; and system resources utilization to determine anomalies on demand but no less than once within a twenty-four (24) hour period. Generate alert notification for technical personnel review and assessment. 2. Review network traffic, bandwidth utilization rates, alert notifications, and border defense devices to determine anomalies on demand but no less than once within a twenty-four (24) hour period. Generate alerts for technical personnel review and assessment. 3. Investigate suspicious activity or suspected violations on the information system, report findings to appropriate officials and take appropriate action. 4. Use automated utilities to review audit records at least once every seven (7) days for unusual, unexpected, or suspicious behavior. 5. Inspect administrator groups on demand but at least once every fourteen (14) days to ensure unauthorized administrator accounts have not been created. 6. Perform manual reviews of system audit records randomly on demand but at least once every thirty (30) days.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AU-6(1) – Enhancement (Moderate)	
Control The information system integrates audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AU-6(2) – Enhancement (Moderate)	
Control [Withdrawn: Incorporated into SI-4].	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

AU-7 – Audit Reduction and Report Generation (Moderate)	
Control The information system provides an audit reduction and report generation capability.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AU-7(1) – Enhancement (Moderate)	
Control The information system provides the capability to automatically process audit records for events of interest based on selectable event criteria.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AU-8 – Time Stamps (Moderate)	
Control The information system uses internal system clocks to generate time stamps for audit records.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AU-8(1) – Enhancement (Moderate)	
Control The information system synchronizes internal information system clocks daily and at system boot.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AU-9 – Protection of Audit Information (Moderate)	
Control The information system protects audit information and audit tools from unauthorized access, modification, and deletion.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

AU-10 – Non-Repudiation (Moderate)

Control

The information system protects against an individual falsely denying having performed a particular action.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

AU-11 – Audit Record Retention (Moderate)

Control

The organization retains audit records for ninety (90) days and archive old records for one (1) year to provide support for after-the-fact investigations of security incidents and to meet regulatory and information retention requirements.

For FTI:
1. Employ a permanent system of standardized records of request for disclosure of FTI and maintain the records for five (5) years or the applicable records control schedule, whichever is longer. (Pub 1075 Ref. 3.1)
2. To support the audit of FTI activities, all organizations must ensure that audit information is archived for six (6) years to enable the recreation of computer-related accesses to both the operating system and to the application wherever FTI is stored. (Pub 1075 Ref. 9.3)

Implementation Standard(s)
1. (For PII only) Audit inspection reports, including a record of corrective actions, shall be retained by the organization for a minimum of three (3) years from the date the inspection was completed.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

AU-12 – Audit Generation (Moderate)

Control

The information system:
a. Provides audit record generation capability for the following events in addition to those specified in other controls:
- All successful and unsuccessful authorization attempts.
- All changes to logical access control authorities (e.g., rights, permissions).
- All system changes with the potential to compromise the integrity of audit policy configurations, security policy configurations and audit record generation services.
- The audit trail shall capture the enabling or disabling of audit report generation services.
- The audit trail shall capture command line changes, batch file changes and queries made to the system (e.g., operating system, application, and database).

b. Allows designated organizational personnel to select which auditable events are to be audited by specific components of the system; and
c. Generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

AU-12(1) – Enhancement (Moderate)	
Control The information system compiles audit records from multiple components throughout the system into a system-wide (logical or physical) time-correlated audit trail.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Audit and Accountability Family (AU) Security Controls Detail and Comment

Security Assessment and Authorization (CA) – *Management*

CA-1 – Security Assessment and Authorization Policies and Procedures (Moderate)	
Control The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days: a. Formal, documented security assessment and authorization policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the security assessment and authorization policies and associated security assessment and authorization controls.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

CA-2 – Security Assessments (Moderate)	
Control The organization: a. Develops a security assessment plan that describes the scope of the assessment including: - Security controls and control enhancements under assessment; - Assessment procedures to be used to determine security control effectiveness; and - Assessment environment, assessment team, and assessment roles and responsibilities; b. Assesses the security controls in the information system within every three hundred sixty-five (365) days in accordance with the Information Security (IS) Acceptable Risk Safeguards (ARS) Including Minimum Security Requirements (CMSR) Standard, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system; c. Produces a security assessment report that documents the results of the assessment; and d. Provides the results of the security control assessment within every three hundred sixty-five (365) days, in writing, to the Business Owner who is respons ble for reviewing the assessment documentation and updating system security documentation where necessary to reflect any changes to the system. For FTI: The agency shall conduct, periodically, but at least annually, an assessment of the security controls in the systems that receive, store, process or transmit FTI. (Pub 1075, Ref. 9.4) **Implementation Standard(s)** 1. A security assessment of all security controls must be conducted prior to issuing the initial authority to operate for all newly implemented systems. 2. The annual security assessment requirement mandated by OMB requires all CMSRs attributable to a system or application to be assessed over a 3-year period. To meet this requirement, a subset of the CMSRs shall be tested each year so that all security controls are tested during a 3-year period. 3. The Business Owner notifies the CISO within thirty (30) days whenever updates are made to system security authorization artifacts or significant role changes occur (e.g., Business Owner, System Developer/Maintainer, ISSO).	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

CA-2(1) – Enhancement (Moderate)	
Control The organization employs an independent assessor or assessment team to conduct an assessment of the security controls in the information system.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CA-3 – Information System Connections (Moderate)	
Control The organization: a. Authorizes connections from the information system to other information systems outside of the authorization boundary through the use of Interconnection Security Agreements; b. Documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated; and c. Monitors the information system connections on an ongoing basis verifying enforcement of security requirements. **Implementation Standard(s)** 1. Record each system interconnection in the Security Management Plan (SMP) and Information Security (IS) Risk Assessment (RA) for the system that is connected to the remote location.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CA-4 – Security Certification (Moderate)	
Control [Withdrawn: Incorporated into CA-2].	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

CA-5 – Plan of Action and Milestones (POA&M) (Moderate)	
Control The organization: a. Develops and submits a Plan of Action and Milestones (POA&M) for the information system within thirty (30) days of the final results for every internal/external audit/review or test (e.g., ST&E, penetration test) to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and b. Updates and submits existing POA&M monthly until all the findings are resolved based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities. **Implementation Standards** For FTI: The agency must submit an updated Corrective Action Plan (CAP) twice each year to address corrective actions identified during an on-site safeguards review until all findings are closed. The CAP is submitted as an attachment to the SAR, and on the CAP due date which is six months from the scheduled SAR due date. (Pub 1075, Ref. 7.5)	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CA-5(1) – Enhancement (Moderate)	
Control The organization employs automated mechanisms to help ensure that the POA&M for the information system is accurate, up to date, and readily available.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

CA-6 – Security Authorization (Moderate)

Control

The organization updates the security authorization:
- At least every three (3) years;
- When substantial changes are made to the system;
- When changes in requirements result in the need to process data of a higher sensitivity;
- When changes occur to authorizing legislation or federal requirements;
- After the occurrence of a serious security violation which raises questions about the validity of an earlier security authorization; and
- Prior to expiration of a previous security authorization.

For FTI: Owners of FTI shall accredit the security controls used to protect FTI before initiating operations. This shall be done for any infrastructure associated with FTI. The authorization shall occur every three (3) years or whenever there is a significant change to the control structure. A senior agency official shall sign and approve the authorization. (Pub 1075, Ref 9.5)

Note: For Federal agencies that receive FTI, a NIST compliant systems certification (C&A) is required in accordance with FISMA. For state agencies that receive FTI, a third-party accreditation is not required. Instead, these agencies may internally attest in writing that the security controls have been adequately implemented to protect FTI. The accreditation shall occur every three (3) years or whenever there is a significant change to the control structure. (Pub 1075, Ref. 9.5)

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

CA-7 – Continuous Monitoring (Moderate)

Control

The organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes:
a. A configuration management process for the information system and its constituent components;
b. A determination of the security impact of changes to the information system and environment of operation;
c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; and
d. Reporting the security state of the information system to appropriate organizational officials within every three hundred sixty-five (365) days.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

CA-7(1) – Enhancement (Moderate)

Control

The use of independent security assessment agents or teams to monitor security controls is not required. However, if the organization employs an independent assessor or assessment team to monitor the security controls in the information system on an ongoing basis, this can be used to satisfy ST&E requirements.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CA-7(2) – Enhancement (Moderate)	
Control plans, schedules, and conducts automated or manual assessments on a continuous and unannounced basis, of all information systems and information systems that are processing data on behalf of or directly for including, but not limited to, in-depth monitoring of systems and networks, vulnerability and configuration scanning, and announced penetration testing to ensure compliance with all vulnerability mitigation procedures.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Security Assessment and Authorization Family (CA) Security Controls Detail and Comment

Configuration Management (CM) – *Operational*

CM-1 – Configuration Management Policy and Procedures (Moderate)	
Control The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days: a. A formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CM-2 – Baseline Configuration (Moderate)	
Control The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CM-2(1) – Enhancement (Moderate)	
Control The organization reviews and updates the baseline configuration of the information system: (a) At least once every three hundred sixty-five (365) days; (b) When required due to major system changes/upgrades; and (c) As an integral part of information system component installations and upgrades.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CM-2(3) – Enhancement (Moderate)	
Control The organization retains older versions of baseline configurations as deemed necessary to support rollback.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CM-2(4) – Enhancement (Moderate)	
Control The organization: (a) Develops and maintains a list of software programs authorized (white list) or unauthorized (black list) to execute on the information system; and	

(b) Employs an allow-all, deny-by-exception authorization policy to identify software allowed to execute on the information system.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

CM-3 – Configuration Change Control (Moderate)

Control

The organization:
a. Determines the types of changes to the information system that are configuration controlled;
b. Approves configuration-controlled changes to the system with explicit consideration for security impact analyses;
c. Documents approved configuration-controlled changes to the system;
d. Retains and reviews records of configuration-controlled changes to the system;
e. Audits activities associated with configuration-controlled changes to the system; and
f. Coordinates and provides oversight for configuration change control activities through change request forms which must be approved by an organizational and/or change control board which meets frequently enough to accommodate proposed change requests, and other appropriate organization officials including, but not limited to, the System Developer/Maintainer and information system support staff.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

CM-3(2) – Enhancement (Moderate)

Control

The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

CM-4 – Security Impact Analysis (Moderate)

Control

The organization analyzes changes to the information system to determine potential security impacts prior to change implementation. Activities associated with configuration changes to the information system are audited.

Fully explain control implementation ***(or fully explain why control requirement is not applicable)***	Responsible for Control Implementation *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

CM-4(1) – Enhancement (Moderate)

Control

The organization analyzes new software in a separate test environment before installation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	Responsible for Control Implementation *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CM-4(2) – Enhancement (Moderate)	
Control The organization, after the information system is changed, checks the security functions to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security requirements for the system.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CM-5 – Access Restrictions for Change (Moderate)	
Control The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system. Records reflecting all such changes shall be generated, reviewed, and retained.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

CM-6 – Configuration Settings (Moderate)	
Control The organization: a. Establishes and documents mandatory configuration settings for information technology products employed within the information system using the latest security configuration guidelines listed in Implementation Standard 1 that reflect the most restrictive mode consistent with operational requirements; b. Implements the configuration settings; c. Identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures. For FTI: Establish mandatory configuration settings for systems that receive, store, process and transmit FTI using the Safeguards Computer Security Evaluation Matrices (SCSEMs). (Pub 1075, Ref 9.6) **Implementation Standard(s)** 1. Security configuration guidelines may be developed by different agencies, so it is possible that a guideline could include configuration information that conflicts with another agency or guideline. To resolve configuration conflicts among multiple security guidelines, the hierarchy for implementing all security configuration guidelines is as follows: (a) NIST (b) DISA (c) OMB For FTI: SCSEMs – All agency information systems used for receiving, processing, storing and transmitting FTI must be hardened in accordance with the requirements of Publication 1075. Agency information systems include the equipment, facilities, and people that collect, process, store, display and disseminate information. This includes computers, hardware, software, and communications, as well as policies and procedures for their use. Safeguard Computer Security Evaluation Matrices (SCSEMs) provide hardening guidance for specific technologies and are publicly available on the Office of Safeguards IRS.gov website, keyword: safeguards program.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CM-6(3) – Enhancement (Moderate)	
Control The organization incorporates detection of unauthorized, security-relevant configuration changes into the organization's incident response capability to ensure that such detected events are tracked, monitored, corrected, and available for historical purposes.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

CM-7 – Least Functionality (Moderate)	
Control The organization configures the information system to provide only essential capabilities and specifically disables, proh bits, or restricts the use of system services, ports, network protocols, and capabilities that are not explicitly required for system or application functionality. A list of specifically needed system services, ports, and network protocols will be maintained and documented in the SMP; all others will be disabled.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CM-7(1) – Enhancement (Moderate)	
Control The organization reviews the information system within every three hundred sixty-five (365) days to identify and eliminate unnecessary functions, ports, protocols, and/or services.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CM-8 – Information System Component Inventory (Moderate)	
Control The organization develops, documents, and maintains an inventory of information system components that: a. Accurately reflects the current information system; b. Is consistent with the authorization boundary of the information system; c. Is at the level of granularity deemed necessary for tracking and reporting; d. Includes manufacturer, model/type, serial number, version number, location (i.e., physical location and logical position within the information system architecture), and ownership; and e. Is available for review and audit by designated organizational officials.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CM-8(1) – Enhancement (Moderate)	
Control The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

CM-8(5) – Enhancement (Moderate)	
Control The organization verifies that all components within the authorization boundary of the information system are either inventoried as a part of the system or recognized by another system as a component within that system.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CM-9 – Configuration Management Plan (Moderate)	
Control The organization develops, documents, and implements a configuration management plan for the information system that: a. Addresses roles, responsibilities, and configuration management processes and procedures; b. Defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management; and c. Establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Configuration Management Family (CM) Security Controls Detail and Comment

Contingency Planning (CP) – *Operational*

CP-1 – Contingency Planning Policy and Procedures (Moderate)	
Control The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days: a. A formal, documented contingency planning policy that addresses purpose, scope, roles, respons bilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CP-2 – Contingency Plan (Moderate)	
Control The organization: a. Develops a Contingency Plan (CP) for the information system that: - Identifies essential missions and business functions and associated contingency requirements; - Provides recovery objectives, restoration priorities, and metrics; - Addresses contingency roles, responsibilities, assigned individuals with contact information; - Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; - Addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented; and - Is reviewed and approved by designated officials within the organization; b. Distributes copies of the CP plan to key contingency personnel (identified by name and/or by role) and organizational elements; c. Coordinates contingency planning activities with incident handling activities; d. Reviews the CP for the information system annually; (Pub 1075, Ref 9.7) e. Revises the CP to address changes to the organization, information system, or environment of operation and problems encountered during CP implementation, execution, or testing; and f. Communicates CP changes to key contingency personnel (identified by name and/or by role) and organizational elements.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CP-2(1) – Enhancement (Moderate)	
Control The organization coordinates contingency plan development with organizational elements responsible for related plans. Enhancement Supplemental Guidance: Examples of related plans include Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Crisis Communications Plan, Critical Infrastructure Plan, Cyber Incident Response Plan, and Occupant Emergency Plan.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

CP-2(2) – Enhancement (Moderate)	
Control The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CP-3 – Contingency Training (Moderate)	
Control The organization trains operational and support personnel (including managers and users of the information system) in their contingency roles and responsibilities with respect to the information system and provides refresher training within every three hundred sixty-five (365) days.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CP-4 – Contingency Plan Testing and Exercises (Moderate)	
Control The organization: a. Tests and/or exercises the contingency plan for the information system within every three hundred sixty-five (365) days using defined tests and exercises, such as the tabletop test in accordance with the current contingency plan procedure to determine the plan's effectiveness and the organization's readiness to execute the plan; and b. Documents and reviews the contingency plan test/exercise results and initiates reasonable and appropriate corrective actions to close or reduce the impact of contingency plan failures and deficiencies.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CP-4(1) – Enhancement (Moderate)	
Control The organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CP-5 – Contingency Plan Update (Moderate)	
Control [Withdrawn: Incorporated into CP-2].	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or*

	Common; Indicate All Control Provider(s)]
CP-6 – Alternate Storage Site (Moderate)	
Control The organization establishes an alternate storage site including necessary agreements to permit the storage and recovery of information system backup information. For FTI: The agency must identify alternative storage sites and initiate necessary agreements to permit the secure storage of information system and FTI backups and ensure the alternative storage sites meet FTI secure storage requirements. (Pub 1075 section 9.7)	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CP-6(1) – Enhancement (Moderate)	
Control The organization identifies an alternate storage site that is separated from the primary storage site so as not to be susceptible to the same hazards. Enhancement Supplemental Guidance: Hazards of concern to the organization are typically defined in an organizational assessment of risk.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CP-6(3) – Enhancement (Moderate)	
Control The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions. Enhancement Supplemental Guidance: Explicit mitigation actions include, for example, duplicating backup information at another alternate storage site if access to the first alternate site is hindered; or, if electronic accessibility to the alternate site is disrupted, planning for physical access to retrieve backup information	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

CP-7 – Alternate Processing Site (Moderate)

Control

The organization:
a. Establishes an alternate processing site including necessary agreements to permit the resumption of information system operations for essential missions and business functions within the time period specified in Implementation Standard 1 when the primary processing capabilities are unavailable; and
b. Ensures that equipment and supplies required to resume operations are available at the alternate site or contracts are in place to support delivery to the site in time to support the time period for resumption specified in Implementation Standard 1.

Implementation Standard(s)
1. Ensure all equipment and supplies required for resuming system operations at the alternate processing site are available, or contracts are in place to support delivery to the site, to permit resumption of essential missions and business functions within one (1) week of contingency plan activation.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

CP-7(1) – Enhancement (Moderate)

Control

The organization identifies an alternate processing site that is separated from the primary processing site so as not to be susceptible to the same hazards.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

CP-7(2) – Enhancement (Moderate)

Control

The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

CP-7(3) – Enhancement (Moderate)

Control

The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with the organization's availability requirements.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

CP-7(5) – Enhancement (Moderate)

Control

The organization ensures that the alternate processing site provides information security measures equivalent to that of the primary site.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CP-8 – Telecommunications Services (Moderate)	
Control The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential missions and business functions within the resumption time period specified in Implementation Standard 1 when the primary telecommunications capabilities are unavailable. **Implementation Standard(s)** 1. Ensure alternate telecommunications service agreements are in place to permit resumption of information system operations for essential missions and business functions within one (1) week of contingency plan activation when primary telecommunications capabilities are unavailable.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CP-8(1) – Enhancement (Moderate)	
Control The organization develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with the organization's availability requirements. And b) Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CP-8(2) – Enhancement (Moderate)	
Control The organization obtains alternate telecommunications services with consideration for reducing the likelihood of sharing a single point of failure with primary telecommunications services.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

CP-9 – Information System Backup (Moderate)

Control

The organization:
a. Conducts backups of user-level information contained in the information system in accordance with the frequency specified in Implementation Standard 1;
b. Conducts backups of system-level information contained in the information system in accordance with the frequency specified in Implementation Standard 1;
c. Conducts backups of information system documentation including security-related documentation and other forms of data, including paper records; and
d. Protects the confidentiality and integrity of backup information at the storage location.

Implementation Standard(s)
1. Perform full backups weekly to separate media. Perform incremental or differential backups daily to separate media. Backups to include user-level and system-level information (including system state information). Three (3) generations of backups (full plus all related incremental or differential backups) are stored off-site. Off-site and on-site backups must be logged with name, date, time and action.
2. (For PII only) Ensure that a current, retrievable, copy of PII is available before movement of servers.

For FTI: Back-up tapes must be labeled as containing FTI, must be logged, must be transported securely using two barriers and a transmittal, and must be inventoried on a semi-annual basis. (Pub 1075 sections 3.0, 4.0)

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

CP-9(1) – Enhancement (Moderate)

Control

The organization tests backup information following each backup to verify media reliability and information integrity.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

CP-10 – Information System Recovery and Reconstitution (Moderate)

Control

The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure. Recovery of the information system after a failure or other contingency shall be done in a trusted, secure, and verifiable manner.

Implementation Standard(s)
1. Secure information system recovery and reconstitution includes, but not limited to:
(a) Reset all system parameters (either default or organization-established),
(b) Reinstall patches,
(c) Reestablish configuration settings,
(d) Reinstall application and system software, and
(e) Fully test the system.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or*

	Common; Indicate All Control Provider(s)]
CP-10(2) – Enhancement (Moderate)	
Control The information system implements transaction recovery for systems that are transaction-based. Enhancement Supplemental Guidance: Database management systems and transaction processing systems are examples of information systems that are transaction-based. Transaction rol back and transaction journaling are examples of mechanisms supporting transaction recovery.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CP-10(3) – Enhancement (Moderate)	
Control The organization provides compensating security controls for circumstances that inhibit recovery and reconstitution to a known state.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Contingency Planning Family (CP) Security Controls Detail and Comment

Identification and Authentication (IA) – *Technical*

IA-1 – Identification and Authentication Policy and Procedures (Moderate)	
Control The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days: a. A formal, documented identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
IA-2 – Identification and Authentication (Organizational Users) (Moderate)	
Control The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users). **Implementation Standard(s)** 1. Require the use of system and/or network authenticators and unique user identifiers. 2. Help desk support requires user identification for any transaction that has information security implications. For FTI: Complete section 2.10 (e-Authentication level) in the SMP Template.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
IA-2(1) – Enhancement (Moderate)	
Control The information system uses multifactor authentication for network access to privileged accounts. For FTI: Two-factor authentication is required whenever FTI is being accessed from an alternative work location or if accessing FTI via agency's web portal by an employee or contractor.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
IA-2(2) – Enhancement (Moderate)	
Control The information system uses multifactor authentication for network access to non-privileged accounts.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or ~~Common; Indicate All Control Provider(s)~~]*

IA-2(3) – Enhancement (Moderate)	
Control The information system uses multifactor authentication for local access to privileged accounts.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
IA-2(8) – Enhancement (Moderate)	
Control The information system uses replay resistant authentication mechanisms for network access to privileged accounts. Enhancement Supplemental Guidance: An authentication process resists replay attacks if it is impractical to achieve a successful authentication by recording and replaying a previous authentication message. Techniques used to address this include protocols that use nonces or challenges (e.g., TLS), and time synchronous or challenge-response one-time authenticators.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
IA-3 – Device Identification and Authentication (Moderate)	
Control The information system uniquely identifies and authenticates specific and/or types of devices before establishing a connection.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
IA-4 – Identifier Management (Moderate)	
Control The organization manages information system identifiers for users and devices by: a. Receiving authorization from a designated organizational official to assign a user or device identifier; b. Selecting an identifier that uniquely identifies an individual or device; c. Assigning the user identifier to the intended party or the device identifier to the intended device; d. Preventing reuse of user or device identifiers until all previous access authorizations are removed from the system, including all file accesses for that identifier but not before a period of at least three hundred sixty-five (365) days has expired; and e. Disabling the user identifier after the time period of inactivity specified in Implementation Standard 1 and deleting disabled accounts during the annual re-certification process. **Implementation Standard(s)** 1. Disable user identifiers after one hundred eighty (180) days of inactivity. For FTI: Disable user identifier after ninety (90) days of inactivity.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation**

	[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]

IA-5 – Authenticator Management (Moderate)

Control

The organization manages information system authenticators for users and devices by:
a. Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator;
b. Establishing initial authenticator content for authenticators defined by the organization;
c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
e. Changing default content of authenticators upon information system installation;
f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate);
g. Changing/refreshing password authenticators as defined in IA-5(1);
h. Protecting authenticator content from unauthorized disclosure and modification; and
i. Requiring users to take, and having devices implement, specific measures to safeguard authenticators.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

IA-5(1) – Enhancement (Moderate)

Control

The information system, for password-based authentication:
(a) Automatically forces users (including administrators) to change user account passwords every sixty (60) days and system account passwords every one hundred eighty (180) days;
(b) Prohibits the use of dictionary names or words;
(c) Enforces minimum password complexity consisting of at least eight (8) alphanumeric (i.e., upper- and lower-case letters, and numbers) and/or special characters;
(d) Enforces at least a minimum of four (4) changed characters when new passwords are created;
(e) Encrypts passwords in storage and in transmission;
(f) Enforces password minimum and maximum lifetime restrictions of one (1) day for the minimum, and sixty (60) days for a user account and one hundred eighty (180) days for a system account maximum; and
(g) Prohibits password reuse for six (6) generations prior to reuse.

For FTI: Change/refresh authenticators every 90 days, at a minimum, for a standard user account, every 60 days, at a minimum, for privileged users. (Pub 1075, Ref Exhibit 8)

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

IA-5(2) – Enhancement (Moderate)

Control

The information system, for PKI-based authentication:
(a) Validates certificates by constructing a certification path with status information to an accepted trust anchor;
(b) Enforces authorized access to the corresponding private key; and
(c) Maps the authenticated identity to the user account.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
IA-5(3) – Enhancement (Moderate)	
Control The organization requires that the registration process to receive hardware tokens be verified in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor).	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
IA-6 – Authenticator Feedback (Moderate)	
Control The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
IA-7 – Cryptographic Module Authentication (Moderate)	
Control The information system uses mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
IA-8 – Identification and Authentication (Non-Organizational Users) (Moderate)	
Control The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Identification and Authentication Family (IA) Security Controls Detail and Comment

Incident Response (IR) – *Operational*

IR-1 – Incident Response Policy and Procedures (Moderate)	
Control The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days: a. A formal, documented incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls. For FTI: Policies and procedures must cover both physical and information security relative to the protection of FTI. For FTI: Complete SPR section 9.11.1	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
IR-2 – Incident Response Training (Moderate)	
Control The organization: a. Trains personnel in their incident response roles and responsibilities with respect to the information system; and For FTI: Provides refresher training prior to access of FTI and annually thereafter on incident response policy and procedure regarding FTI. (Pub 1075, section 6.2, 9.9) **Supplemental Guidance**: Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources. For FTI: Complete SPR section 9.11.2	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
IR-3 – Incident Response Testing and Exercises (Moderate)	
Control The organization tests and/or exercises the incident response capability for the information system annually using reviews, analyses, and simulations to determine the incident response effectiveness and documents the results. For FTI: Include procedures to exercise responding o unauthorized FTI access and reporting unauthorized FTI access to IRS and TIGTA. (Pub 1075, Ref 9.9) Complete SPR section 9.11.3.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or*

	Common; Indicate All Control Provider(s)]
IR-4 – Incident Handling (Moderate)	
Control The organization: a. Implements an incident handling capability using Information Security Incident Handling and Breach Notification Procedures; b. Coordinates incident handling activities with contingency planning activities; and c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly. For FTI: The agency's incident response policy and procedures must include specific guidance relative to a data incidents involving FTI. (Pub 1075 Section 9.9) **Implementation Standard(s)** 1. Document relevant information related to a security incident according to Information Security Incident Handling and Breach Notification Procedures. 2. Preserve evidence through technical means, including secured storage of evidence media and "write" protection of evidence media. Use sound forensics processes and utilities that support legal requirements. Determine and follow chain of custody for forensic evidence. 3. Identify vulnerability exploited during a security incident. Implement security safeguards to reduce risk and vulnerability exploit exposure. For FTI: Complete SPR section 9.11.4	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
IR-4(1) – Enhancement (Moderate)	
Control The organization employs automated mechanisms to support the incident handling process. Enhancement Supplemental Guidance: An online incident management system is an example of an automated mechanism.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

IR-5 – Incident Monitoring (Moderate)	
Control The organization tracks and documents information system security incidents. Supplemental Guidance: Documenting information system security incidents includes, for example, maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources including, for example, incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. For FTI: Once the incident has been addressed, the agency will conduct a post-incident review to ensure the incident response policies and procedures provide adequate guidance. (Pub 1075 section 10.3) For FTI: Complete SPR section 9.11.5	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
IR-6 – Incident Reporting (Moderate)	
Control The organization: a. Requires personnel to report suspected security incidents to the organizational incident response capability within timeframe established in the current Information Security Incident Handling and Breach Analysis/Notification Procedure; and b. Reports security incident information to designated authorities. For FTI: Any data incident potentially involving FTI must immediately be reported to the Treasury Inspector General for Tax Administration (TIGTA) and the IRS Office of Safeguards immediately, but no later than 24-hours after identification of a possible issue involving FTI. (Pub. 1075, Ref 9.9, 10.4) Supplemental Guidance: The intent of this control is to address both specific incident reporting requirements within an organization and the formal incident reporting requirements for federal agencies and their subordinate organizations. The types of security incidents reported, the content and timeliness of the reports, and the list of designated reporting authorities are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Current federal policy requires that all federal agencies (unless specifically exempted from such requirements) report security incidents to the United States Computer Emergency Readiness Team (US-CERT) within specified time frames designated in the US-CERT Concept of Operations for Federal Cyber Security Incident Handling. Related controls: IR-4, IR-5. For FTI: Complete SPR section 9.11.6	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
IR-6(1) – Enhancement (Moderate)	
Control The organization employs automated mechanisms to assist in the reporting of security incidents.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or*

	Common; Indicate All Control Provider(s)]

IR-7 – Incident Response Assistance (Moderate)	
Control The organization provides an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the information system for the handling and reporting of security incidents. Supplemental Guidance: Poss ble implementations of incident response support resources in an organization include a help desk or an assistance group and access to forensics services, when required. For FTI: Complete SPR section 9.11.7	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
IR-7(1) – Enhancement (Moderate)	
Control The organization employs automated mechanisms to increase the availability of incident response-related information and support. Enhancement Supplemental Guidance: Automated mechanisms can provide a push and/or pull capability for users to obtain incident response assistance. For example, individuals might have access to a website to query the assistance capability, or conversely, the assistance capability may have the ability to proactively send information to users (general distribution or targeted) as part of increasing understanding of current response capabilities and support.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

IR-8 – Incident Response Plan (Moderate)	
Control The organization: a. Develops an incident response plan that: - Provides the organization with a roadmap for implementing its incident response capability; - Describes the structure and organization of the incident response capability; - Provides a high-level approach for how the incident response capability fits into the overall organization; - Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; - Defines reportable incidents; - Provides metrics for measuring the incident response capability within the organization. - Defines the resources and management support needed to effectively maintain and mature an incident response capability; and - Is reviewed and approved by designated officials within the organization; b. Distributes copies of the incident response plan to incident response personnel and organizational elements; c. Reviews the incident response plan within every three hundred sixty-five (365) days; d. Revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; and e. Communicates incident response plan changes to incident response personnel and organizational elements. Supplemental Guidance: It is important that organizations have a formal, focused, and coordinated approach to responding to incidents. The organization's mission, strategies, and goals for incident response help determine the structure of its incident response capability. For FTI: Complete SPR section 9.11.8.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Incident Response Family (IR) Security Controls Detail and Comment

Maintenance (MA) – *Operational*

MA-1 – System Maintenance Policy and Procedures (Moderate)	
Control The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days: a. A formal, documented information system maintenance policy that addresses purpose, scope, roles, respons bilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

MA-2 – Controlled Maintenance (Moderate)	
Control The organization: a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements; b. Controls all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location; c. Requires that a designated official explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs; d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; and e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions. **Implementation Standard(s)** 1. (For PII only) In facilities where PII is stored or accessed, document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

MA-2(1) – Enhancement (Moderate)	
Control the organization maintains maintenance records for the information system that include: - date and time of maintenance; - name of the individual performing the maintenance; - name of escort, if necessary; - a description of the maintenance performed; - a list of equipment removed or replaced (including identification numbers, if applicable).	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

MA-3 – Maintenance Tools (Moderate)	
Control The organization approves, controls, monitors the use of, and maintains on an ongoing basis, information system maintenance tools.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
MA-3(1) – Enhancement (Moderate)	
Control The organization inspects all maintenance tools carried into a facility by maintenance personnel for obvious improper modifications. Enhancement Supplemental Guidance: Maintenance tools include, for example, diagnostic and test equipment used to conduct maintenance on the information system.	
Fully explain control implementation (or fully explain why control requirement is not applicable)	**Responsible for Control Implementation** [Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]
MA-3(2) – Enhancement (Moderate)	
Control The organization checks all media containing diagnostic and test programs for malicious code before the media are used in the information system.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
MA-4 – Non-Local Maintenance (Moderate)	
Control The organization prohibits non-local system maintenance unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the organization: a. Monitors and controls non-local maintenance and diagnostic activities; b. Allows the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system; c. Employs strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions; d. Maintains records for non-local maintenance and diagnostic activities; and e. Terminates all sessions and network connections when non-local maintenance is completed. **Implementation Standard(s)** 1. If password-based authentication is used during remote maintenance, change the passwords following each remote maintenance service.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

MA-4(1) – Enhancement (Moderate)	
Control The organization audits non-local maintenance and diagnostic sessions and designated organizational personnel review the maintenance records of the sessions.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
MA-4(2) – Enhancement (Moderate)	
Control The organization documents, in the security plan for the information system, the installation and use of non-local maintenance and diagnostic connections.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
MA-4(3) – Enhancement (Moderate)	
Control The organization: (a) Requires that non-local maintenance and diagnostic services be performed from an information system that implements a level of security at least as high as that implemented on the system being serviced; or (b) Removes the component to be serviced from the information system and prior to non-local maintenance or diagnostic services, sanitizes the component (with regard to sensitive information) before removal from organizational facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software and surreptitious implants) before reconnecting the component to the information system.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
MA-5 – Maintenance Personnel (Moderate)	
Control The organization: a. Establishes a process for maintenance personnel authorization and maintains a current list of authorized maintenance organizations or personnel; and b. Ensures that personnel performing maintenance on the information system have required access authorizations or designates organizational personnel with required access authorizations and technical competence deemed necessary to supervise information system maintenance when maintenance personnel do not possess the required access authorizations.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

MA-6 – Timely Maintenance (Moderate)	
Control The organization obtains maintenance support and/or spare parts for critical systems and applications (including Major Applications [MA] and General Support Systems [GSS] and their components) within twenty-four (24) hours of failure.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Maintenance Family (MA) Security Controls Detail and Comment

Media Protection (MP) – *Operational*

MP-1 – Media Protection Policy and Procedures (Moderate)	
Control The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days: a. A formal, documented media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls. **Implementation Standard(s)** 1. (For PII only) Semi-annual inventories of magnetic tapes containing PII are conducted. The organization accounts for any missing tape containing PII by documenting the search efforts and notifying the tape initiator of the loss.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
MP-2 – Media Access (Moderate)	
Control The organization restricts access to sensitive digital and non-digital media to authorized individuals using automated mechanisms to control access to media storage areas.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
MP-2(1) – Enhancement (Moderate)	
Control The organization employs automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

MP-3 – Media Marking (Moderate)	
Control The organization: a. Marks, in accordance with organizational policies and procedures, removable information system media and information system output indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and b. Exempts specific types of media or hardware components, as specified, in writing, by the CIO or his/her designated representative, from marking as long as the exempted items remain within a secure environment. For FTI: The agency must label removable media and information system output containing FTI. IRS Notice 129-A or Notice 129-B are available for this purpose. (Pub. 1075, Ref. 9.11)	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

MP-4 – Media Storage (Moderate)	
Control The organization: a. Physically controls and securely stores digital and non-digital media within controlled areas using safeguards prescr bed for the highest system security level of the information ever recorded on it; b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures. **Implementation Standard(s)** 1. (For PII only) Evaluate employing an approved method of cryptography (see SC-13) to protect PII at rest, consistent with NIST SP 800-66 guidance. 2. (For PII only) If PII is recorded on magnetic media with other data, it should be protected as if it were entirely personally identifiable information.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

MP-5 – Media Transport (Moderate)

Control

The organization:
a. Protects and controls digital and non-digital media containing sensitive information during transport outside of controlled areas using cryptography and tamper evident packaging and (i) if hand carried, using securable container (e.g., locked briefcase) via authorized personnel, or (ii) if shipped, trackable with receipt by commercial carrier;
b. Maintains accountability for information system media during transport outside of controlled areas; and
c. Restricts the activities associated with transport of such media to authorized personnel.

For FTI: All FTI transported through the mail or courier/messenger service must be double sealed; that is one envelope within another envelope. The inner envelope should be marked confidential with some indication that only the designated official or delegate is authorized to open it. Using sealed boxes serves the same purpose as double sealing and prevents anyone from viewing the contents thereof. (Pub 1075, Ref 4.5)

Implementation Standard(s)
1. (For PII only) Protect and control PII media during transport outside of controlled areas and restricts the activities associated with transport of such media to authorized personnel. PII must be in locked cabinets or sealed packing cartons while in transit.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

MP-5(2) – Enhancement (Moderate)

Control

The organization documents activities associated with the transport of information system media.

For FTI: All shipments of FTI (including electronic media and microfilm) must be documented on a transmittal form and monitored to ensure that each shipment is properly and timely received and acknowledged. (Pub 1075, Ref 4.5)

Implementation Standard(s):

For FTI: Describe the permanent record(s) (logs) used to document requests for, receipt of, distribution of (if applicable), and disposition (return to IRS or destruction) of the FTI (including tapes, cartridges or other removable media) (e.g. FTI receipt logs, transmission logs, or destruction logs in electronic or paper format) (Please include a sample of the agency logs as an attachment).

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

MP-5(4) – Enhancement (Moderate)

Control

The organization employs cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

Enhancement Supplemental Guidance: This control enhancement also applies to mobile devices. Mobile devices include portable storage media (e.g., USB memory sticks, external hard disk drives) and portable computing and communications devices with storage capability (e.g.,notebook/laptop computers, personal digital assistants, cellular

telephones).

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

MP-6 – Media Sanitization (Moderate)

Control

The organization:
a. Sanitizes information system media, both digital and non-digital, prior to disposal, release out of organizational control, or release for reuse; and
b. Employs sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information.

For FTI:
1. FTI furnished to the user and any paper material generated therefrom, such as extra copies, photo impressions, computer printouts, carbon paper, notes, stenographic notes, and work papers must be destroyed by burning, mulching, pulping, shredding, or disintegrating. (See Pub 1075, Ref 8.3 for detailed procedures)
2. FTI must never be disclosed to an agency's agents or contractors during disposal unless authorized by the Internal Revenue Code. Generally, destruction should be witnessed by an agency employee.

Implementation Standard(s)
1. Finely shred, using a minimum of cross-cut shredding, hard-copy documents, using approved equipment, techniques, and procedures.
2. (For PII only) Authorized employees of the receiving entity must be respons ble for securing magnetic tapes/cartridges before, during, and after processing, and they must ensure that the proper acknowledgment form is signed and returned. Inventory records must be maintained for purposes of control and accountability. Tapes containing PII, any hard-copy printout of a tape, or any file resulting from the processing of such a tape will be recorded in a log that identifies:
- date received
- reel/cartridge control number contents
- number of records, if available
- movement, and
- if disposed of, the date and method of disposition.

For FTI, complete SPR section 8.1.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

MP-6(1) – Enhancement (Moderate)

Control

The organization tracks, documents, and verifies media sanitization and disposal actions.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

MP-6(2) – Enhancement (Moderate)	
Control The organization tests sanitization equipment and procedures to verify correct performance periodically.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
MP-6(5) – Enhancement (Moderate)	
Control The organization sanitizes information system media containing sensitive information using National Security Agency (NSA) guidance (www.nsa.gov/ia/government/mdg.cfm) and NIST SP 800-88, Guidelines for Media Sanitization. For FTI: Electronic media containing FTI must not be made available for reuse by other offices or released for destruction without first being subject to electromagnetic erasing. If reuse is not intended, the electronic media should be destroyed. Whenever physical media leaves the physical or systemic control of the agency for maintenance, exchange or other servicing, any FTI on it must be cleared completely by overwriting all data tracks a minimum of three times. (Pub 1075 section 8.4)	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
MP-6(6) – Enhancement (Moderate)	
Control The organization destroys media containing sensitive information that cannot be sanitized. For FTI: Paper FTI may be burned, cross-cut shredded to 5/16" wide or small strips or pulped.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

MP-EDC-1 – Media Related Records (Moderate)	
Control Inventory and disposition records for information system media shall be maintained to ensure control and accountability of Commonwealth of PA information. The media related records shall contain sufficient information to reconstruct the data in the event of a breach. **Implementation Standard(s)** 1. The media records must, at a minimum, contain: (a) The name of media recipient; (b) Signature of media recipient; (c) Date/time media received; (d) Media control number and contents; (e) Movement or routing information; and (f) If disposed of, the date, time, and method of destruction.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Media Protection Family (MP) Security Controls Detail and Comment

Physical and Environmental Protection (PE) – *Operational*

PE-1 – Physical and Environmental Protection Policy and Procedures (Moderate)	
Control The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days: a. A formal, documented physical and environmental protection policy that addresses purpose, scope, roles, respons bilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

PE-2 – Physical Access Authorizations (Moderate)	
Control The organization: a. Develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); b. Issues authorization credentials; c. Reviews and approves the access list and authorization credentials in accordance with the frequency specified in Implementation Standard 1, removing from the access list personnel no longer requiring access. For FTI: A visitor access log containing specific data elements will be used to authenticate and authorize visitor's access to any facility where FTI resides, either electronically or in paper, at the location where the outside (2nd) barrier is breached. (See IRS Pub. 1075, sections 4.3.2) **Implementation Standard(s)** 1. Review and approve lists of personnel with authorized access to facilities containing information systems at least once every one hundred eighty (180) days. 2. (For PII only) Create a restricted area, security room, or locked room to control access to areas containing PII. These areas will be controlled accordingly. 3. (For FTI) Complete SPR section 5.2.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

PE-3 – Physical Access Control (Moderate)

Control

The organization:
a. Enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible);
b. Verifies individual access authorizations before granting access to the facility;
c. Controls entry to the facility containing the information system using physical access devices and/or guards;
d. Controls access to areas officially designated as publicly access ble in accordance with the organization's assessment of risk;
e. Secures keys, combinations, and other physical access devices;
f. Inventories physical access devices within every three hundred sixty-five (365) days; and
g. Changes combinations and keys when keys are lost, combinations are compromised, or individuals are transferred or terminated.

For FTI:
h. Minimum protection standards require two physical barriers between FTI and an individual not authorized to access FTI. This may be achieved through secured perimeter/locked container, locked perimeter/secured interior or locked perimeter/security container. FTI must be containerized in areas where other than authorized employees or authorized contractors may have access after-hours. (See IRS Pub. 1075, sections 4.2)
i. A security guard, custodial services worker or landlord may have access to a locked building or a locked room if FTI is in a locked container. If FTI is in a locked room, but not in a locked container, the guard, janitor or landlord may have a key to the building but not to the room. (See IRS Pub. 1075, sections 4.2)
j. During business hours, if authorized personnel serve as the second barrier between FTI and unauthorized individuals, the authorized personnel must wear an identification badge or credential clearly displayed, preferably work above the waist. (See IRS Pub. 1075, sections 4.2)
k. Unauthorized access to areas containing FTI during duty and non-duty hours must be denied. This can be done utilizing a combination of methods: secured or locked perimeter, secured area or containerization. (See IRS Pub. 1075, sections 4.3)
l. The physical security and control of computers and electronic media must be addressed. Computer operations must be in a secure area with restricted access. . (See IRS Pub. 1075, sections 4.6)

Implementation Standard(s)
1. Control data center/facility access by use of door and window locks, and security personnel or physical authentication devices, such as biometrics and/or smart card/PIN combination.
2. Store and operate servers in physically secure environments, and grant access to explicitly authorized personnel only. Access is monitored and recorded.
3. Restrict access to grounds/facilities to authorized persons only.
4. (For PII only) Require two barriers to access PII under normal security: secured perimeter/locked container, locked perimeter/secured interior, or locked perimeter/security container. Protected information must be containerized in areas where other than authorized employees may have access after-hours.

For FTI: Complete SPR sections 5.3.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

PE-4 – Access Control for Transmission Medium (Moderate)	
Control The organization controls physical access to information system distr bution and transmission lines within organizational facilities. **Implementation Standard(s)** 1. Permit access to telephone closets and information system distribution and transmission lines within organizational facilities only to authorized personnel. 2. Disable any physical ports (e.g., wiring closets, patch panels, etc) not in use. For FTI: Complete SPR section 5.4.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

PE-5 – Access Control for Output Devices (Moderate)	
Control The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output. For FTI: Output from printers and fax machines should be in a controlled area and secured when not in use. Physical access to monitors displaying FTI should be controlled to prevent unauthorized access to the display output. (Pub. 1075, Ref 4.3, 4.3.2) For FTI: Complete SPR section 5.5.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

PE-6 – Monitoring Physical Access (Moderate)	
Control The organization: a. Monitors physical access to the information system to detect and respond to physical security incidents; b. Reviews physical access logs in accordance with the frequency specified in Implementation Standard 1; and c. Coordinates results of reviews and investigations with the organization's incident response capability. **Implementation Standard(s)** 1. Review physical access logs every at least once every two (2) months. For FTI: Complete SPR section 5.6.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

PE-6(1) – Enhancement (Moderate)	
Control The organization monitors real-time physical intrusion alarms and surveillance equipment.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
PE-7 – Visitor Control (Moderate)	
Control The organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible. For FTI: A restricted area visitor log will be maintained at a designated entrance to the restricted area and all visitors (persons not assigned to the area) entering the area shall be directed to the designated entrance. The entry control monitor should verify the identify of visitors by comparing the name and signature entered into the register with some type of photo identification card. For FTI: Complete SPR section 5.7.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
PE-7(1) – Enhancement (Moderate)	
Control The organization escorts visitors and monitors visitor activity, when required.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
PE-8 – Access Records (Moderate)	
Control The organization: a. Maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); and b. Reviews visitor access records monthly. For FTI: The restricted area visitor log shall include the visitor's name, signature, assigned work area, escort, purpose of entry, and time and date of entry. For FTI: Complete SPR section 5.8.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or*

	Common; Indicate All Control Provider(s)]

PE-9 – Power Equipment and Power Cabling (Moderate)

Control

The organization protects power equipment and power cabling for the information system from damage and destruction.

Implementation Standard(s)
1. Permit only authorized maintenance personnel to access infrastructure assets, including power generators, HVAC systems, cabling, and wiring closets.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

PE-10 – Emergency Shutoff (Moderate)

Control

The organization:
a. Provides the capability of shutting off power to the information system or individual system components in emergency situations;
b. Places emergency shutoff switches or devices in a location that does not require personnel to approach the equipment to facilitate safe and easy access for personnel; and
c. Protects emergency power shutoff capability from unauthorized activation.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

PE-11 – Emergency Power (Moderate)

Control

The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

PE-12 – Emergency Lighting (Moderate)

Control

The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

PE-13 – Fire Protection (Moderate)	
Control The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
PE-13(1) – Enhancement (Moderate)	
Control The organization employs fire detection devices/systems for the information system that activate automatically and notify the organization and emergency responders in the event of a fire.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
PE-13(2) – Enhancement (Moderate)	
Control The organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to the organization and emergency responders.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
PE-13(3) – Enhancement (Moderate)	
Control The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

PE-14 – Temperature and Humidity Controls (Moderate)	
Control The organization: a. Maintains temperature and humidity levels within the facility where the information system resides within acceptable vendor-recommended levels; and b. Monitors temperature and humidity levels. **Implementation Standard(s)** 1. Evaluate the level of alert and follow prescribed guidelines for that alert level. 2. Alert component management of possible loss of service and/or media. 3. Report damage and provide remedial action. Implement contingency plan, if necessary.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

PE-15 – Water Damage Protection (Moderate)	
Control The organization protects the information system from damage resulting from water leakage by providing master shutoff valves that are access ble, working properly, and known to key personnel.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

PE-16 – Delivery and Removal (Moderate)	
Control The organization authorizes, monitors, and controls the flow of information system-related components entering and exiting the facility and maintains records of those items. For FTI: All transportation or shipments of FTI (including electronic media or microfilm) must be documented on a transmittal form and monitored to ensure that each shipment is properly and timely received and acknowledged. All FTI transported through the mail or courier/messenger service must be double-sealed; that is one envelope within another envelope. The inner envelope should be marked confidential with some indication that only the designed official or delegate is authorized to open it. (Pub. 1075, sections 4.5) For FTI: Complete SPR section 5.9.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

PE-17 – Alternate Work Site (Moderate)	
Control The organization: a. Employs appropriate security controls at alternate work sites to include, but not limited to, laptop cable locks, recording serial numbers and other identification information about laptops, and disconnecting modems; b. Assesses as feasible, the effectiveness of security controls at alternate work sites; and c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems. For FTI: Descr be the policies and procedures for meeting the minimum protection standards for alternative work sites (e.g. employee's homes or other non-traditional work sites). (Pub 1075, Ref 5.3). For FTI: Complete SPR section 5.10.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

PE-18 – Location of Information System Components (Moderate)	
Control The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access. For FTI: Complete SPR section 5.11.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Physical and Environmental Protection Family (PE) Security Controls Detail and Comment

Planning (PL) – *Management*

PL-1 – Security Planning Policy and Procedures (Moderate)	
Control The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days: a. A formal, documented security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

PL-2 – Security Management Plan (SMP) (Moderate)

Control

The organization:
a. Develops a security plan for the information system that:
- Is consistent with the Security Management Plan (SMP) Procedure;
- Is consistent with the organization's enterprise architecture;
- Explicitly defines the authorization boundary for the system;
- Describes the operational context of the information system in terms of missions and business processes;
- Provides the security categorization of the information system including supporting rationale;
- Describes the operational environment for the information system;
- Describes relationships with or connections to other information systems;
- Provides an overview of the security requirements for the system;
- Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and
- Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;
b. Reviews the security plan for the information system within every three hundred sixty-five (365) days; and
c. Updates the plan, minimally every three (3) years, to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.

For FTI:
1. When FTI is incorporated into a Data Warehouse, the controls descr bed in IRS Pub. 1075, Exh bit 11 are to be followed, in addition to those specified in other controls.
2. Develop and submit a Safeguard Procedures Report (SPR) that describes the procedures established and used by the organization for ensuring the confidentiality of the information received from the IRS. Annually thereafter, the organization must file a Safeguard Activity Report (SAR). The SAR advises the IRS of minor changes to the procedures or safeguards described in the SPR. It also advises the IRS of future actions that will affect the organization's safeguard procedures, summarizes the organization's current efforts to ensure the confidentiality of FTI, and finally, certifies that the organization is protecting FTI pursuant to IRC Section 6103(p)(4) and the organization's own security requirements. Whenever significant changes occur in the safeguard program the SPR will be updated and resubmitted. (See IRS Pub. 1075, sections 7.0 and 9.13)

Implementation Standard(s)
1. (For PHI only) Retain documentation of policies and procedures relating to HIPAA 164.306 for six (6) years from the date of its creation or the date when it last was in effect, whichever is later. (See HIPAA 164.316(b).)

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

PL-3 – System Security Plan Update (Moderate)

Control

[Withdrawn: Incorporated into PL-2].

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

PL-4 – Rules of Behavior (ROB) (Moderate)	
Control The organization: a. Establishes and makes readily available to all information system users, the rules that descr be their respons bilities and expected behavior with regard to information, information system, and network use; and b. Receives signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

PL-5 – Privacy Impact Assessment (PIA) (Moderate)	
Control The organization conducts a Privacy Impact Assessment (PIA) on the information system in accordance with OMB policy.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

PL-6 – Security-Related Activity Planning (Moderate)	
Control The organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on operations (i.e., mission, functions, image, and reputation), assets, and individuals. **Implementation Standard(s)**	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Planning Family (PL) Security Controls Detail and Comment

Personnel Security (PS) – *Operational*

PS-1 – Personnel Security Policy and Procedures (Moderate)	
Control The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days: a. A formal, documented personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

PS-2 – Position Categorization (Moderate)	
Control The organization: a. Assigns a criticality/sensitivity risk designation to all positions; b. Establishes screening criteria for individuals filling those positions; and c. Reviews and revises position criticality/sensitivity risk designations within every three hundred sixty-five (365) days.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

PS-3 – Personnel Screening (Moderate)	
Control The organization: a. Screens individuals prior to authorizing access to the information system; and b. Rescreens individuals periodically, consistent with the criticality/sensitivity rating of the position. For FTI: Individuals must be screened before authorizing access to information systems and devices containing FTI. (Pub 1075, Ref. 9.12) **Implementation Standard(s)** 1. Perform criminal history check for all persons prior to employment. 2. Require appropriate personnel to obtain and hold a moderate-risk security clearance as defined in the DHHS Personnel Security/Suitability Handbook.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

PS-4 – Personnel Termination (Moderate)	
Control The organization, upon termination of individual employment: a. Revokes system and physical access immediately following employee termination; b. Conducts exit interviews; c. Retrieves all security-related information system-related property; d. Retains access to information and information systems formerly controlled by terminated individual; and e. Immediately escorts employees terminated for cause out of the organization. **Implementation Standard(s)** 1. System access must be revoked prior to or during the employee termination process.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

PS-5 – Personnel Transfer (Moderate)	
Control The organization reviews logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within the organization and initiates the following transfer or reassignment actions during the formal transfer process: a. Re-issuing appropriate information system-related property (e.g., keys, identification cards, building passes); b. Notification to security management; c. Closing obsolete accounts and establishing new accounts; and d. Revocation of all system access privileges (if applicable).	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

PS-6 – Access Agreements (Moderate)	
Control The organization: a. Ensures that individuals requiring access to information or information systems sign appropriate access agreements prior to being granted access; and b. Reviews/updates the access agreements as part of the system security authorization or when a contract is renewed or extended. For FTI: Agencies must review information system access authorizations and initiate appropriate actions when personnel are reassigned or transferred to other positions within the organization. (See IRS Pub. 1075, sections 9.12)	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

PS-7 – Third-Party Personnel Security (Moderate)	
Control The organization: a. Establishes personnel security requirements including security roles and responsibilities for third-party providers; b. Documents personnel security requirements; and c. Monitors provider compliance. **Implementation Standard(s)** 1. Regulate the access provided to contractors and define security requirements for contractors. Contractors must be provided with minimal system and physical access, and must agree to and support the information security requirements. The contractor selection process must assess the contractor's ability to adhere to and support information security policies and standards.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
PS-8 – Personnel Sanctions (Moderate)	
Control The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Personnel Security Family (PS) Security Controls Detail and Comment

Risk Assessment (RA) – *Management*

RA-1 – Risk Assessment Policy and Procedures (Moderate)	
Control The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days: a. A formal, documented risk assessment policy that addresses purpose, scope, roles, respons bilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

RA-2 – Security Categorization (Moderate)	
Control The organization: a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and c. Ensures the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

RA-3 – Risk Assessment (Moderate)	
Control The organization: a. Conducts an assessment of risk, including the l kelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; b. Documents risk assessment results in accordance with the Information Security (IS) Risk Assessment (RA) Procedures; c. Reviews risk assessment results within every three hundred sixty-five (365) days; and d. Updates the risk assessment within every three (3) years or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security or authorization state of the system.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

RA-4 – Risk Assessment Update (Moderate)	
Control [Withdrawn: Incorporated into RA-3].	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

RA-5 – Vulnerability Scanning (Moderate)	
Control The organization: a. Scans for vulnerabilities in the information system and hosted applications within every ninety (90) days and when new vulnerabilities potentially affecting the system/applications are identified and reported; b. Employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for: - Enumerating platforms, software flaws, and improper configurations; - Formatting and making transparent, checklists and test procedures; and - Measuring vulnerability impact; c. Analyzes vulnerability scan reports and results from security control assessments; d. Remediates legitimate vulnerabilities based on the Business Owner's risk prioritization in accordance with an organizational assessment of risk; and e. Shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization on a "need to know" basis to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies). For FTI: At a minimum, systems containing FTI shall be scanned quarterly to identify any vulnerability in the information system. (Pub. 1075, Ref 9.13) **Implementation Standard(s)** 1. Perform external network penetration testing and conduct enterprise security posture review as needed but no less than once within every three hundred sixty-five (365) days, in accordance with IS procedures.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

RA-5(1) – Enhancement (Moderate)	
Control The organization employs vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Risk Assessment Family (RA) Security Controls Detail and Comment

System and Services Acquisition (SA) – *Management*

SA-1 – System and Services Acquisition Policy and Procedures (Moderate)

Control

The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:
a. A formal, documented system and services acquisition policy that includes information security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b. Formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the system and services acquisition family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The system and services acquisition policy can be included as part of the general information security policy for the organization. System and services acquisition procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the system and services acquisition policy. Related control: PM-9.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SA-2 – Allocation of Resources (Moderate)

Control

The organization:
a. Includes a determination of information security requirements for the information system in mission/business process planning;
b. Determines, documents, and allocates the resources required to protect the information system as part of its capital planning and investment control process;
c. Includes information security requirements in mission/business case planning, and
d. Establishes a discrete line item in programming and budgeting documentation for the implementation and management of information systems security.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SA-3 – Life Cycle Support (Moderate)

Control

The organization:
a. Manages the information system using the information security steps of IEEE 12207.0 standard for SDLC, as provided in the Integrated IT Investment & System Life Cycle Framework (ILC);
b. Defines and documents information system security roles and responsibilities throughout the system development life cycle; and
c. Identifies individuals having information system security roles and responsibilities.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SA-4 – Acquisitions (Moderate)

Control

The organization includes the following requirements and/or specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards:
a. Security functional requirements/specifications;
b. Security-related documentation requirements; and
c. Developmental and evaluation-related assurance requirements.

Supplemental Guidance: The acquisition documents for information systems, information system components, and information system services include, either explicitly or by reference, security requirements that describe: (i) required security capabilities (i.e., security needs and, as necessary, specific security controls and other specific FISMA requirements); (ii) required design and development processes; (iii) required test and evaluation procedures; and (iv) required documentation. The requirements in the acquisition documents permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented. Acquisition documents also include requirements for appropriate information system documentation. The documentation addresses user and system administrator guidance and information regarding the implementation of the security controls in the information system. The level of detail required in the documentation is based on the security categorization for the information system. In addition, the required documentation includes security configuration settings and security implementation guidance. FISMA reporting instructions provide guidance on configuration requirements for federal information systems.

Implementation Standard(s)
1. Each contract and Statement of Work (SOW) that requires development or access to information must include language requiring adherence to security policies and standards, define security roles and responsibilities, and receive approval from officials.

For FTI:
1. Whenever information systems contain FTI, the agency shall include security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk. The contract for the acquisition must contain Exhibit 7 language. (Pub 1075 section 9.15)
2. Agencies using a consolidated data center must implement appropriate controls to ensure the protection of FTI, including a Service Level Agreement (SLA) between the agency authorized to receive FTI and the data center. (Pub 1075, section 5.5.2)

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SA-4(1) – Enhancement (Moderate)

Control

The organization requires in acquisition documents that vendors/contractors provide information descr bing the functional properties of the security controls to be employed within the information system, information system components, or information system services in sufficient detail to permit analysis and testing of the controls.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SA-4(4) – Enhancement (Moderate)

Control

The organization ensures that each information system component acquired is explicitly assigned to an information system, and that the owner of the system acknowledges this

assignment.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SA-5 – Information System Documentation (Moderate)

Control

The organization:
a. Obtains, protects as required, and makes available to authorized personnel, administrator documentation for the information system that describes:
- Secure configuration, installation, and operation of the information system;
- Effective use and maintenance of security features/functions; and
- Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; and
b. Obtains, protects as required, and makes available to authorized personnel, user documentation for the information system that describes:
- User-accessible security features/functions and how to effectively use those security features/functions;
- Methods for user interaction with the information system, which enables individuals to use the system in a more secure manner; and
- User responsibilities in maintaining the security of the information and information system; and
c. Documents attempts to obtain information system documentation when such documentation is either unavailable or nonexistent.

Supplemental Guidance: The inability of the organization to obtain necessary information system documentation may occur, for example, due to the age of the system and/or lack of support from the vendor/contractor. In those situations, organizations may need to recreate selected information system documentation if such documentation is essential to the effective implementation and/or operation of security controls.

Implementation Standard(s)
1. Develop system documentation to describe the system and to specify the purpose, technical operation, access, maintenance, and required training for administrators and users.
2. Maintain an updated list of related system operations and security documentation.
3. Update documentation upon changes in system functions and processes. Must include date and version number on all formal system documentation.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SA-5(1) – Enhancement (Moderate)

Control

The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SA-5(3) – Enhancement (Moderate)

Control

The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the high-level design of the

information system in terms of subsystems and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SA-6 – Software Usage Restrictions (Moderate)

Control

The organization:
a. Uses software and associated documentation in accordance with contract agreements and copyright laws;
b. Employs tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution; and
c. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distr bution, display, performance, or reproduction of copyrighted work.

Supplemental Guidance: Tracking systems can include, for example, simple spreadsheets or fully automated, specialized applications depending on the needs of the organization.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SA-7 – User-Installed Software (Moderate)

Control

The organization prohibits users from downloading or installing software, unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, explicit rules govern the installation of software by users.

Supplemental Guidance: If provided the necessary privileges, users have the ability to install software. The organization identifies what types of software installations are permitted (e.g., updates and security patches to existing software) and what types of installations are prohibited (e.g., software whose pedigree with regard to being potentially malicious is unknown or suspect). Related control: CM-2.

Implementation Standard(s)
1. If user installed software is authorized, ensure that business rules and technical controls enforce the documented authorizations and prohibitions.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SA-8 – Security Engineering Principles (Moderate)	
Control The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system. **Supplemental Guidance:** The application of security engineering principles is primarily targeted at new development information systems or systems undergoing major upgrades and is integrated into the system development life cycle. For legacy information systems, the organization applies security engineering principles to system upgrades and modifications to the extent feasible, given the current state of the hardware, software, and firmware within the system. Examples of security engineering principles include, for example: (i) developing layered protections; (ii) establishing sound security policy, architecture, and controls as the foundation for design; (iii) incorporating security into the system development life cycle; (iv) delineating physical and logical security boundaries; (v) ensuring system developers and integrators are trained on how to develop secure software; (vi) tailoring security controls to meet organizational and operational needs; and (vii) reducing risk to acceptable levels, thus enabling informed risk management decisions.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SA-9 – External Information System Services (Moderate)

Control

The organization:
a. Requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and
c. Monitors security control compliance by external service providers.
d. Prohibits service providers from outsourcing any system function outside the U.S. or its territories.

For FTI: FTI may not be accessed by agency employees, agents, representatives or contractors located "off-shore", outside of the United States or its territories. FTI may not be received, stored, processed or disposed via information technology systems located off-shore.

Supplemental Guidance: An external information system service is a service that is implemented outside of the authorization boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system). Relationships with external service providers are established in a variety of ways, for example, through joint ventures, business partnerships, outsourcing arrangements (i.e., contracts, interagency agreements, lines of business arrangements), licensing agreements, and/or supply chain exchanges. The responsibility for adequately mitigating risks arising from the use of external information system services remains with the authorizing official. Authorizing officials require that an appropriate chain of trust be established with external service providers when dealing with the many issues associated with information security. For services external to the organization, a chain of trust requires that the organization establish and retain a level of confidence that each participating provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered to the organization. The extent and nature of this chain of trust varies based on the relationship between the organization and the external provider. Where a sufficient level of trust cannot be established in the external services and/or service providers, the organization employs compensating security controls or accepts the greater degree of risk. The external information system services documentation includes government, service provider, and end user security roles and responsibilities, and any service-level agreements. Service-level agreements define the expectations of performance for each required security control, descr be measurable outcomes, and identify remedies and response requirements for any identified instance of noncompliance.

Implementation Standard(s)
1. (For PHI only) A covered entity under HIPAA may permit a business associate to create, receive, maintain, or transmit EPHI on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with HIPAA regulations. Such assurances must be documented and meet the requirements set forth in HIPAA regulations. (See HIPAA 164.308(b) and 164.314(a).)

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SA-10 – Developer Configuration Management (Moderate)	
Control The organization requires that information system developers/integrators: a. Perform configuration management during information system design, development, implementation, and operation; b. Manage and control changes to the information system; c. Implement only organization-approved changes; d. Document approved changes to the information system; and e. Track security flaws and flaw resolution. **Supplemental Guidance:** Related controls: CM-3, CM-4, CM-9	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SA-11 – Developer Security Testing (Moderate)	
Control The organization requires that information system developers/integrators, in consultation with associated security personnel (including security engineers): a. Create and implement a security test and evaluation plan in accordance with, but not limited to the, current procedures; b. Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security control assessment process; and c. Document the results of the security control assessment and flaw remediation processes. For FTI: The agency must submit a request to the IRS Office of Safeguards for authority to use live data for testing, providing a detailed explanation of the safeguards in place to protect the FTI over the Internet to a customer (Pub 1075, Ref. 9.18.8) **Supplemental Guidance:** Developmental security test results are used to the greatest extent feasible after verification of the results and recognizing that these results are impacted whenever there have been security-relevant modifications to the information system subsequent to developer testing. Test results may be used in support of the security authorization process for the delivered information system. Related control: CA-2, SI-2. **Implementation Standard(s)** 1. If the security control assessment results are used in support of the security authorization process for the information system, ensure that no security relevant modifications of the information systems have been made subsequent to the assessment and after selective verification of the results. 2. Use hypothetical data when executing test scripts or in a test environment that is configured to comply with the security controls as if it is a production environment.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

System and Services Acquisition Family (SA) Security Controls Detail and Comment

System and Communications Protection (SC) – *Technical*

SC-1 – System and Communications Protection Policy and Procedures (Moderate)	
Control The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days: a. A formal, documented system and communications protection policy that addresses purpose, scope, roles, respons bilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls. **Supplemental Guidance:** This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the system and communications protection family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The system and communications protection policy can be included as part of the general information security policy for the organization. System and communications protection procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the system and communications protection policy. Related control: PM-9.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SC-2 – Application Partitioning (Moderate)	
Control The information system separates user functionality (including user interface services [e.g., web services]) from information system management (e.g., database management systems) functionality. **Supplemental Guidance:** Information system management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. The separation of user functionality from information system management functionality is either physical or logical and is accomplished by using different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate. An example of this type of separation is observed in web administrative interfaces that use separate authentication methods for users of any other information system resources. This may include isolating the administrative interface on a different domain and with additional access controls.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SC-4 – Information in Shared Resources (Moderate)

Control

The information system prevents unauthorized and unintended information transfer via shared system resources.

Supplemental Guidance: The purpose of this control is to prevent information, including encrypted representations of information, produced by the actions of a prior user/role (or the actions of a process acting on behalf of a prior user/role) from being available to any current user/role (or current process) that obtains access to a shared system resource (e.g., registers, main memory, secondary storage) after that resource has been released back to the information system. Control of information in shared resources is also referred to as object reuse. This control does not address: (i) information remanence which refers to residual representation of data that has been in some way nominally erased or removed; (ii) covert channels where shared resources are manipulated to achieve a violation of information flow restrictions; or (iii) components in the information system for which there is only a single user/role.

Implementation Standard(s)
1. Ensure that users of shared system resources cannot intentionally or unintentionally access information remnants, including encrypted representations of information, produced by the actions of a prior user or system process acting on behalf of a prior user. Ensure that system resources shared between two (2) or more users are released back to the information system, and are protected from accidental or purposeful disclosure.

For FTI: When authorized to make further disclosures is present (e.g., agents/contractors), information disclosed outside the organization must be recorded on a separate list that reflects to whom the disclosure was made, what was disclosed, and why and when it was disclosed. Organizations transmitting FTI from one computer to another need only identify the bulk records transmitted. This identification will contain the approximate number of personal records, the date of the transmissions, the best possible description of the records, and the name of the individual making/receiving the transmission.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SC-5 – Denial of Service Protection (Moderate)

Control

The information system protects against or limits the effects of the following types of denial of service attacks defined on the following sites or in the following documents:
- SANS Organization www.sans.org/dosstep;
- SANS Organization's Roadmap to Defeating DDoS www.sans.org/dosstep/roadmap.php; and
- NIST CVE List http://checklists.nist.gov/home.cfm.

Supplemental Guidance: A variety of technologies exist to limit, or in some cases, eliminate the effects of denial of service attacks. For example, boundary protection devices can filter certain types of packets to protect devices on an organization's internal network from being directly affected by denial of service attacks. Employing increased capacity and bandwidth combined with service redundancy may reduce the susceptibility to some denial of service attacks. Related control: SC-7.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SC-7 – Boundary Protection (Moderate)	
Control The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and b. Connects to external networks or information systems only through managed interfaces consisting of automated boundary protection devices arranged in accordance with a organizational security architecture. **Supplemental Guidance:** Restricting external web traffic only to organizational web servers within managed interfaces and prohibiting external traffic that appears to be spoofing an internal address as the source are examples of restricting and proh biting communications. Managed interfaces employing boundary protection devices include, for example, proxies, gateways, routers, firewalls, guards, or encrypted tunnels arranged in effective security architecture (e.g., routers protecting firewalls and application gateways residing on protected subnetworks commonly referred to as a demilitarized zone or DMZ). The organization considers the intrinsically shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may include third-party provided access lines and other service elements. Consequently, such interconnecting transmission services may represent sources of increased risk despite contract security provisions. Therefore, when this situation occurs, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. Related controls: AC-4, IR-4, SC-5. **Implementation Standard(s)** 1. Ensure that access to all proxies is denied, except for those hosts, ports, and services that are explicitly required. 2. Utilize stateful inspection/application firewall hardware and software. 3. Utilize firewalls from at least two (2) different vendors at the various levels within the network to reduce the poss bility of compromising the entire network.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SC-7(1) – Enhancement (Moderate)	
Control The organization physically allocates publicly accessible information system components to separate subnetworks with separate physical network interfaces. Enhancement Supplemental Guidance: Publicly accessible information system components include, for example, public web servers.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SC-7(2) – Enhancement (Moderate)	
Control The information system prevents public access into the organization's internal networks except as appropriately mediated by managed interfaces employing boundary protection devices.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SC-7(3) – Enhancement (Moderate)	
Control The organization limits the number of access points to the information system (e.g., proh biting desktop modems) to allow for more comprehensive monitoring of inbound and outbound communications and network traffic. Enhancement Supplemental Guidance: The Trusted Internet Connection (TIC) initiative is an example of limiting the number of managed network access points.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SC-7(4) – Enhancement (Moderate)	
Control The organization: (a) Implements a managed interface for each external telecommunication service; (b) Establishes a traffic flow policy for each managed interface; (c) Employs security controls as needed to protect the confidentiality and integrity of the information being transmitted; (d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; (e) Reviews exceptions to the traffic flow policy within every three hundred sixty-five (365) days; and (f) Removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SC-7(5) – Enhancement (Moderate)	
Control The information system at managed interfaces, denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception).	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SC-7(6) – Enhancement (Moderate)	
Control The organization prevents the unauthorized release of information outside of the information system boundary or any unauthorized communication through the information system boundary when there is an operational failure of the boundary protection mechanisms.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SC-7(7) – Enhancement (Moderate)	
Control The information system prevents remote devices that have established a non-remote connection with the system from communicating outside of that communications path with resources in external networks.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SC-8 – Transmission Integrity (Moderate)	
Control The information system protects the integrity of transmitted information. **Implementation Standard(s)** 1. Employ appropriate approved mechanisms (e.g., digital signatures, cryptographic hashes) to protect the integrity of data while in transit from source to destination outside of a secured network (see SC-13). 2. For FTI: All FTI in transit must be encrypted when moving across a Wide Area Network (WAN) and within the agency's Local Area Network (LAN). If encryption is not used, the agency must use other compensating mechanisms (e.g. switched VLAN technology, f ber optic medium, etc.) to ensure FTI is not accessible to unauthorized users. (Pub 1075, ref. 9.18.2) 3. For FTI: FTI should not be transmitted or used on the agency's internal e-mail systems. If transmittal of FTI within the agency's e-mail system is necessary, specific precautions must be taken to protect the FTI. FTI must not be transmitted outside of the agency, either in the body of an e-mail or as an attachment. (Pub. 1075, Ref 9.18.5) 4. For FTI: The agency must follow specific precautions when faxing FTI. (Pub 1075 section 9.18.6) **Supplemental Guidance:** This control applies to communications across internal and external networks. If the organization is relying on a commercial service provider for transmission services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission integrity. When it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. Related controls: AC-17, PE-4.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SC-8(1) – Enhancement (Moderate)	
Control The organization employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SC-9 – Transmission Confidentiality (Moderate)

Control

The information system protects the confidentiality of transmitted information.

For FTI:
1. All FTI in transit must be encrypted when moving across a Wide Area Network (WAN) and within the agency's Local Area Network (LAN). If encryption is not used, the agency must use other compensating mechanisms (e.g. switched VLAN technology, fiber optic medium, etc.) to ensure FTI is not accessible to unauthorized users. (Pub 1075, ref. 9.18.2)
2. FTI should not be transmitted or used on the agency's internal e-mail systems. If transmittal of FTI within the agency's e-mail system is necessary, specific precautions must be taken to protect the FTI. FTI must not be transmitted outside of the agency, either in the body of an e-mail or as an attachment. (Pub. 1075, Ref 9.18.5)
3. The agency must follow specific precautions when faxing FTI. (Pub. 1075, Ref. 9.18.6)

Supplemental Guidance: This control applies to communications across internal and external networks. If the organization is relying on a commercial service provider for transmission services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality. When it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. Related controls: AC-17, PE-4.

Implementation Standard(s)
1. (For PII only) When sending or receiving faxes containing PII: (i) fax machines must be located in a locked room with a trusted staff member having custodial coverage over outgoing and incoming transmissions or fax machines must be located in a secured area; (ii) accurate broadcast lists and other preset numbers of frequent fax recipients must be maintained; and (iii) a cover sheet must be used that explicitly provides guidance to the recipient that includes: a notification of the sensitivity of the data and the need for protection, and a notice to unintended recipients to telephone the sender (collect if necessary) to report the disclosure and confirm destruction of the information.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SC-9(1) – Enhancement (Moderate)

Control

The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures. **[*Assignment: organization-defined alternative physical measures*].**

Enhancement Supplemental Guidance: Alternative physical protection measures include, for example, protected distribution systems. Related control: SC-13.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SC-10 – Network Disconnect (Moderate)	
Control The information system automatically terminates the network connection associated with a communications session at the end of the session, or: a. Forcibly de-allocates communications session Dynamic Host Configuration Protocol (DHCP) leases after seven (7) days; and b. Forcibly disconnects inactive Virtual Private Network (VPN) connections after thirty (30) minutes of inactivity. For FTI: Forcibly disconnects inactive VPN connections after 15 minutes of inactivity. (Pub 1075 section 9.16) **Supplemental Guidance:** This control applies to both internal and external networks. Terminating network connections associated with communications sessions include, for example, de-allocating associated TCP/IP address/port pairs at the operating-system level, or de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-level network connection. The time period of inactivity may, as the organization deems necessary, be a set of time periods by type of network access or for specific accesses.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SC-12 – Cryptographic Key Establishment and Management (Moderate)	
Control When cryptography is required and used within the information system, the organization establishes and manages cryptographic keys for required cryptography employed within the information system. **Supplemental Guidance:** Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. In addition to being required for the effective operation of a cryptographic mechanism, effective cryptographic key management provides protections to maintain the availability of the information in the event of the loss of cryptographic keys by users.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SC-13 – Use of Cryptography (Moderate)	
Control When cryptographic mechanisms are used, the information system implements required cryptographic protections using cryptographic modules that comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SC-13(1) – Enhancement (Moderate)	
Control When cryptographic mechanisms are used, the organization employs, at a minimum, FIPS 140-2 compliant and NIST-validated cryptography to protect unclassified information.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SC-14 – Public Access Protections (Moderate)	
Control The information system protects the integrity and availability of publicly available information and applications. **Supplemental Guidance:** The purpose of this control is to ensure that organizations explicitly address the protection needs for public information and applications with such protection likely being implemented as part of other security controls. **Implementation Standard(s)** 1. Ensure that network access controls, operating system file permissions, and application configurations protect the integrity of information stored, processed, and transmitted by publicly accessible systems, as well as the integrity of publicly accessible applications. 2. If e-authentication is required and implemented in conjunction with or related to public access protections, refer to ARS Appendix D: E-authentication Standard.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SC-15 – Collaborative Computing Devices (Moderate)	
Control The organization prohibits running collaborative computing mechanisms, unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the authorization shall specifically identify allowed mechanisms, allowed purpose, and the information system upon which the mechanisms can be used. The information system: a. Prohibits remote activation of collaborative computing devices; and b. Provides an explicit indication of use to users physically present at the devices. **Supplemental Guidance:** Collaborative computing devices include, for example, networked white boards, cameras, and microphones. Explicit indication of use includes, for example, signals to users when collaborative computing devices are activated.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SC-15(1) – Enhancement (Moderate)
Control If collaborative computing is authorized, the information system provides physical disconnect of collaborative computing devices in a manner that supports ease of use.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SC-17 – Public Key Infrastructure Certificates (Moderate)

Control

The organization issues public key certificates under an appropriate certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider.

Supplemental Guidance: For user certificates, each organization attains certificates from an approved, shared service provider, as required by OMB policy. For federal agencies operating a legacy public key infrastructure cross-certified with the Federal Bridge Certification Authority at medium assurance or higher, this Certification Authority will suffice. This control focuses on certificates with a visibility external to the information system and does not include certificates related to internal system operations, for example, application-specific time services.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SC-18 – Mobile Code (Moderate)

Control

The organization:
a. Defines acceptable and unacceptable mobile code and mobile code technologies;
b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and
c. Authorizes, monitors, and controls the use of mobile code within the information system.

Supplemental Guidance: Decisions regarding the employment of mobile code within organizational information systems are based on the potential for the code to cause damage to the system if used maliciously. Mobile code technologies include, for example, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on organizational servers and mobile code downloaded and executed on individual workstations. Policy and procedures related to mobile code, address preventing the development, acquisition, or introduction of unacceptable mobile code within the information system.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SC-19 – Voice Over Internet Protocol (Moderate)	
Control The organization prohibits the use of Voice over Internet Protocol (VoIP) technologies, unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the organization: a. Establishes usage restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to the information system if used maliciously; and b. Authorizes, monitors, and controls the use of VoIP within the information system. For FTI: The agency must meet specific technical requirements to utilize a VoIP network that provides FTI to a customer (Pub 1075, Ref. 9.18.13) For FTI: Complete SPR section 9.28.3.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SC-20 – Secure Name /Address Resolution Service (Authoritative Source) (Moderate)	
Control The information system provides additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address resolution queries. **Supplemental Guidance:** This control enables remote clients to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service. A domain name system (DNS) server is an example of an information system that provides name/address resolution service. Digital signatures and cryptographic keys are examples of additional artifacts. DNS resource records are examples of authoritative data. Information systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to assure the authenticity and integrity of response data. The DNS security controls are consistent with, and referenced from, OMB Memorandum 08-23.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SC-20(1) – Enhancement (Moderate)	
Control The information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces and (if the child supports secure resolution services) enable verification of a chain of trust among parent and child domains.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SC-22 – Architecture and Provisioning for Name /Address Resolution Service (Moderate)	
Control The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation. **Supplemental Guidance:** A domain name system (DNS) server is an example of an information system that provides name/address resolution service. To eliminate single points of failure and to enhance redundancy, there are typically at least two authoritative domain name system (DNS) servers, one configured as primary and the other as secondary. Additionally, the two servers are commonly located in two different network subnets and geographically separated (i.e., not located in the same physical facility). With regard to role separation, DNS servers with an internal role, only process name/address resolution requests from within the organization (i.e., internal clients). DNS servers with an external role only process name/address resolution information requests from clients external to the organization (i.e., on the external networks including the Internet). The set of clients that can access an authoritative DNS server in a particular role is specified by the organization (e.g., by address ranges, explicit lists).	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SC-23 – Session Authenticity (Moderate)	
Control The information system provides mechanisms to protect the authenticity of communications sessions. **Supplemental Guidance:** This control focuses on communications protection at the session, versus packet, level. The intent of this control is to establish grounds for confidence at each end of a communications session in the ongoing identity of the other party and in the validity of the information being transmitted. For example, this control addresses man-in-the-middle attacks including session hijacking or insertion of false information into a session. This control is only implemented where deemed necessary by the organization (e.g., sessions in service-oriented architectures providing web-based services).	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SC-28 – Protection of Information at Rest (Moderate)	
Control The information system protects the confidentiality and integrity of information at rest. **Supplemental Guidance:** This control is intended to address the confidentiality and integrity of information at rest in non-mobile devices and covers user information and system information. Information at rest refers to the state of information when it is located on a secondary storage device (e.g., disk drive, tape drive) within an organizational information system. Configurations and/or rule sets for firewalls, gateways, intrusion detection/prevention systems, and filtering routers and authenticator content are examples of system information I kely requiring protection. Organizations may choose to employ different mechanisms to achieve confidentiality and integrity protections, as appropriate.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SC-32 – Information System Partitioning (Moderate)

Control

The organization partitions the information system into components residing in separate physical domains (or environments) as deemed necessary.

Supplemental Guidance: Information system partitioning is a part of a defense-in-depth protection strategy. An organizational assessment of risk guides the partitioning of information system components into separate physical domains (or environments). The security categorization also guides the selection of appropriate candidates for domain partitioning. Managed interfaces restrict or proh bit network access and information flow among partitioned information system components. Related controls: AC-4, SC-7.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SC-EDC-1 – Electronic Mail (Moderate)

Control

Controls shall be implemented to protect EDC sensitive information (such as FTI or Privacy Act protected information) that is sent via email.

Implementation Standard(s)

1. Prior to sending an email, place all EDC sensitive information in an encrypted attachment.

Guidance

A good place to obtain recommended security practices for handling sensitive information via e-mail is NIST SP 800-45 (as amended), Guidelines on Electronic Mail Security.

Applicability: All	**Reference(s):**	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SC-EDC-1.1

Assessment Objective

Determine if:
(i) the organization effectively implements protections for EDC sensitive information that is sent via e-mail;
(ii) the organization meets all the requirements specified in the applicable implementation standard(s).

Assessment Methods And Objects

Examine: Email policy and procedures; other relevant documents or records.

System and Communications Protection Family (SC) Security Controls Detail and Comment

System and Information Integrity (SI) – *Operational*

SI-1 – System and Information Integrity Policy and Procedures (Moderate)	
Control The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days: a. A formal, documented system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls. **Supplemental Guidance:** This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the system and information integrity family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The system and information integrity policy can be included as part of the general information security policy for the organization. System and information integrity procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the system and information integrity policy. Related control: PM-9.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SI-2 – Flaw Remediation (Moderate)

Control

The organization:
a. Identifies, reports, and corrects information system flaws;
b. Tests software updates related to flaw remediation for effectiveness and potential side effects on information systems before installation; and
c. Incorporates flaw remediation into the organizational configuration management process.

Supplemental Guidance: The organization identifies information systems containing software affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws) and reports this information to designated organizational officials with information security responsibilities (e.g., senior information security officers, information system security managers, information systems security officers). The organization (including any contractor to the organization) promptly installs security-relevant software updates (e.g., patches, service packs, and hot fixes). Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling, are also addressed expeditiously. Organizations are encouraged to use resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in organizational information systems. By requiring that flaw remediation be incorporated into the organizational configuration management process, it is the intent of this control that required/anticipated remediation actions are tracked and verified. An example of expected flaw remediation that would be so verified is whether the procedures contained in US CERT guidance and Information Assurance Vulnerability Alerts have been accomplished. Related controls: CA-2, CA-7, CM-3, MA-2, IR-4, RA-5, SA-11, SI-11.

Implementation Standard(s)
1. Correct identified information system flaws on production equipment in a timeframe based on the National Vulnerability Database (NVD) Vulnerability Severity Rating of the flaw: flaws rated as High severity within seven (7) calendar days; Medium severity within fifteen (15) calendar days; and all others within thirty (30) calendar days.
(a) Evaluate system security patches, service packs, and hot fixes in a test bed environment to determine the effectiveness and potential side effects of such changes, and
(b) Manage the flaw remediation process centrally.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SI-2(1) – Enhancement (Moderate)

Control

The organization centrally manages the flaw remediation process and installs software updates automatically.

Enhancement Supplemental Guidance: Due to information system integrity and availability concerns, organizations give careful consideration to the methodology used to carry out automatic updates.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SI-2(2) – Enhancement (Moderate)

Control

The organization employs automated mechanisms monthly to determine the state of information system components with regard to flaw remediation.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SI-3 – Malicious Code Protection (Moderate)

Control

The organization:
a. Employs malicious code protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code:
- Transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or
- Inserted through the exploitation of information system vulnerabilities;
b. Updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with configuration management policy and procedures;
c. Configures malicious code protection mechanisms to:
- Perform critical system file scans during system boot, information system scans using the frequency specified in Implementation Standard 1, and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy; and
- Block and quarantine malicious code and send alert to administrator in response to malicious code detection; and
d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

Supplemental Guidance: Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, and remote-access servers. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode) or contained within a compressed file. Removable media includes, for example, USB devices, diskettes, or compact disks. A variety of technologies and methods exist to limit or eliminate the effects of malicious code attacks. Pervasive configuration management and strong software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber-attacks that could affect organizational missions and business functions. Traditional malicious code protection mechanisms are not built to detect such code. In these situations, organizations must rely instead on other risk mitigation measures to include, for example, secure coding practices, trusted procurement processes, configuration management and control, and monitoring practices to help ensure that software does not perform functions other than those intended. Related controls: SA-4, SA-8, SA-12, SA-13, SI-4, SI-7.

Implementation Standard(s)
1. Desktop malicious code scanning software is configured to perform critical system file scans every twenty (24) hours.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SI-3(1) – Enhancement (Moderate)

Control

The organization centrally manages malicious code protection mechanisms.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SI-3(2) – Enhancement (Moderate)	
Control The information system automatically updates malicious code protection mechanisms (including signature definitions).	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SI-3(3) – Enhancement (Moderate)	
Control The information system prevents non-privileged users from circumventing malicious code protection capabilities.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SI-4 – Information System Monitoring (Moderate)	
Control The organization: a. Monitors events on the information system in accordance with Information Security Incident Handling and Breach Analysis/Notification Procedure and detects information system attacks; b. Identifies unauthorized use of the information system; c. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; and e. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations. **Supplemental Guidance:** Information system monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the system (e.g., within internal organizational networks and system components). Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, audit record monitoring software, network monitoring software). Strategic locations for monitoring devices include, for example, at selected perimeter locations and near server farms supporting critical applications, with such devices typically being employed at the managed interfaces associated with controls SC-7 and AC-17. The Einstein network monitoring device from the Department of Homeland Security is an example of a system monitoring device. The granularity of the information collected is determined by the organization based on its monitoring objectives and the capability of the information system to support such activities. An example of a specific type of transaction of interest to the organization with regard to monitoring is Hyper Text Transfer Protocol (HTTP) traffic that bypasses organizational HTTP proxies, when use of such proxies is required. Related controls: AC-4, AC-8, AC-17, AU-2, AU-6, SI-3, SI-7. **Implementation Standard(s)** 1. Install IDS devices at network perimeter points and host-based IDS sensors on critical servers.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SI-4(1) – Enhancement (Moderate)	
Control The organization interconnects and configures individual intrusion detection tools into a system wide intrusion detection system using common protocols.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SI-4(2) – Enhancement (Moderate)	
Control The organization employs automated tools to support near real-time analysis of events.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SI-4(4) – Enhancement (Moderate)	
Control The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions. Enhancement Supplemental Guidance: Unusual/unauthorized activities or conditions include, for example, internal traffic that indicates the presence of malicious code within an information system or propagating among system components, the unauthorized export of information, or signaling to an external information system. Evidence of malicious code is used to identify potentially compromised information systems or information system components.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SI-4(5) – Enhancement (Moderate)	
Control The information system provides near real-time alerts when the following indications of compromise or potential compromise occur: (a) Presence of malicious code, (b) Unauthorized export of information, (c) Signaling to an external information system, or (d) Potential intrusions. Enhancement Supplemental Guidance: Alerts may be generated, depending on the organization defined list of indicators, from a variety of sources, for example, audit records or input from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SI-4(6) – Enhancement (Moderate)	
Control The information system prevents non-privileged users from circumventing intrusion detection and prevention capabilities.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SI-5 – Security Alerts, Advisories, and Directives (Moderate)	
Control The organization: a. Receives information system security alerts, advisories, and directives from designated external organizations on an ongoing basis; b. Generates internal security alerts, advisories, and directives as deemed necessary; c. Disseminates security alerts, advisories, and directives to appropriate personnel; and d. Implements security directives in accordance with established time frames, or notifies the degree of noncompliance. **Supplemental Guidance:** Security alerts and advisories are generated by the United States Computer Emergency Readiness Team (US-CERT) to maintain situational awareness across the federal government. Security directives are issued by OMB or other designated organizations with the responsibility and authority to issue such directives. Compliance to security directives is essential due to the critical nature of many of these directives and the potential immediate adverse affects on organizational operations and assets, individuals, other organizations, and the Nation should the directives not be implemented in a timely manner.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SI-7 – Software and Information Integrity (Moderate)	
Control The information system detects unauthorized changes to software and information. **Supplemental Guidance:** The organization employs integrity verification applications on the information system to look for evidence of information tampering, errors, and omissions. The organization employs good software engineering practices with regard to commercial off-the-shelf integrity mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and uses tools to automatically monitor the integrity of the information system and the applications it hosts.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SI-7(1) – Enhancement (Moderate)	
Control The organization reassesses the integrity of software and information by performing daily integrity scans of the information system.	

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SI-8 – Spam Protection (Moderate)	
Control The organization: a. Employs spam protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, or other common means; and b. Updates spam protection mechanisms (including signature definitions) when new releases are available in accordance with configuration management policy and procedures. **Supplemental Guidance:** Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, and remote-access servers. Related controls: SC-5, SI-3.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SI-8(1) – Enhancement (Moderate)	
Control The organization centrally manages spam protection mechanisms.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SI-9 – Information Input Restrictions (Moderate)	
Control The organization restricts the capability to input information to the information system to authorized personnel. **Supplemental Guidance:** Restrictions on organizational personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities. Related controls: AC-5, AC-6.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SI-10 – Information Input Validation (Moderate)	
Control The information system uses automated mechanisms to check the validity of information inputs for accuracy, completeness, validity, and authenticity as close to the point of origin as possible. **Supplemental Guidance:** Rules for checking the valid syntax and semantics of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to verify that inputs match specified definitions for format and content. Inputs passed to interpreters are prescreened to prevent the content from being unintentionally interpreted as commands.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SI-11 – Error Handling (Moderate)	
Control The information system: a. Identifies potentially security-relevant error conditions; b. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries in error logs and administrative messages that could be exploited by adversaries; and c. Reveals error messages only to authorized personnel. For FTI: Generates error messages that provide information necessary for corrective actions in error logs and administrative messages. (Pub 1075 section 9.17) **Supplemental Guidance:** The structure and content of error messages are carefully considered by the organization. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements. Sensitive information includes, for example, account numbers, social security numbers, and credit card numbers.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SI-12 – Information Output Handling and Retention (Moderate)	
Control The organization handles and retains both information within and output from the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. **Supplemental Guidance:** The output handling and retention requirements cover the full life cycle of the information, in some cases extending beyond the disposal of the information system. The National Archives and Records Administration provides guidance on records retention. Related controls: MP-2, MP-4. **Implementation Standard(s)** 1. Retain output, including, but not limited to audit records, system reports, business and financial reports, and business records, from the information system in accordance with Policy and all applicable National Archives and Records Administration (NARA) requirements.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

System and Information Integrity Family (SI) Security Controls Detail and Comment

Project Management (PM) – *Management*

PM-1 INFORMATION SECURITY PROGRAM PLAN	
Control	
The organization: a. Develops and disseminates an organization-wide information security program plan that: - Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements; - Provides sufficient information about the program management controls and common controls (including specification of parameters for any assignment and selection operations either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended; - Includes roles, responsibilities, management commitment, coordination among organizational entities, and compliance; - Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; b. Reviews the organization-wide information security program plan [Assignment: organization defined frequency]; and c. Revises the plan to address organizational changes and problems identified during plan implementation or security control assessments. **Supplemental Guidance**: The information security program plan can be represented in a single document or compilation of documents at the discretion of the organization. The plan documents the organization-wide program management controls and organization-defined common controls. The security plans for individual information systems and the organization-wide information security program plan together, provide complete coverage for all security controls employed within the organization. Common controls are documented in an appendix to the organization's information security program plan unless the controls are included in a separate security plan for an information system (e.g., security controls employed as part of an intrusion detection system providing organization-wide boundary protection inherited by one or more organizational information systems). The organization-wide information security program plan will indicate which separate security plans contain descriptions of common controls. Organizations have the flexibility to describe common controls in a single document or in multiple documents. In the case of multiple documents, the documents descr bing common controls are included as attachments to the information security program plan. If the information security program plan contains multiple documents, the organization specifies in each document the organizational official or officials respons ble for the development, implementation, assessment, authorization, and monitoring of the respective common controls. For example, the organization may require that the Facilities Management Office develop, implement, assess, authorize, and continuously monitor common physical and environmental protection controls from the PE family when such controls are not associated with a particular information system but instead, support multiple information systems. Related control: PM-8.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

PM-2 SENIOR INFORMATION SECURITY OFFICER
Control:
The organization appoints a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program. **Supplemental Guidance:** The security officer described in this control is an organizational official. For a federal agency (as defined in applicable federal laws, Executive Orders, directives, policies, or regulations) this official is the Senior Agency Information Security Officer. Organizations may also refer to this organizational official as the Senior

Information Security Officer or Chief Information Security Officer.

Control Enhancements: None.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

PM-3 INFORMATION SECURITY RESOURCES

Control:

The organization:
a. Ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement;
b. Employs a business case/Exhibit 300/Exhibit 53 to record the resources required; and
c. Ensures that information security resources are available for expenditure as planned.

Supplemental Guidance: Organizations may designate and empower an Investment Review Board (or similar group) to manage and provide oversight for the information security-related aspects of the capital planning and investment control process. Related controls: PM-4, SA-2.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation**
	Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]

PM-4 PLAN OF ACTION AND MILESTONES PROCESS

Control:

The organization implements a process for ensuring that plans of action and milestones for the security program and the associated organizational information systems are maintained and document the remedial information security actions to mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation. Supplemental Guidance: The plan of action and milestones is a key document in the information security program and is subject to federal reporting requirements established by OMB. The plan of action and milestones updates are based on the findings from security control assessments, security impact analyses, and continuous monitoring activities. OMB FISMA reporting guidance contains instructions regarding organizational plans of action and milestones. Related control:
CA-5.

Control Enhancements: None.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

PM-5 INFORMATION SYSTEM INVENTORY

Control:

The organization develops and maintains an inventory of its information systems.

Supplemental Guidance: This control addresses the inventory requirements in FISMA. OMB provides guidance on developing information systems inventories and associated reporting requirements.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

PM-6 INFORMATION SECURITY MEASURES OF PERFORMANCE

Control:

The organization develops, monitors, and reports on the results of information security measures of performance.

Supplemental Guidance: Measures of performance are outcome-based metrics used by an organization to measure the effectiveness or efficiency of the information security program and the security controls employed in support of the program. Control Enhancements: None.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

PM-7 ENTERPRISE ARCHITECTURE

Control:

The organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.

Supplemental Guidance: The enterprise architecture developed by the organization is aligned with the Federal Enterprise Architecture. The integration of information security requirements and associated security controls into the organization's enterprise architecture helps to ensure that security considerations are addressed by organizations early in the system development life cycle and are directly and explicitly related to the organization's mission/business processes. This also embeds into the enterprise architecture, a integral security architecture consistent with organizational risk management and information security strategies. Security requirements and control integration are most effectively accomplished through the application of the Risk Management Framework and supporting security standards and guidelines. The Federal Segment Architecture Methodology provides guidance on integrating information security requirements and security controls into enterprise architectures. Related controls: PL-2, PM-11, RA-2.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

PM-8 CRITICAL INFRASTRUCTURE PLAN

Control:

The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.
Supplemental Guidance: The requirement and guidance for defining critical infrastructure and key resources and for preparing an associated critical infrastructure protection plan are found in applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Related controls: PM-1, PM-9, PM-11, RA-3.

Control Enhancements: None.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

PM-9 RISK MANAGEMENT STRATEGY

Control:

The organization:
a. Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems; and
b. Implements that strategy consistently across the organization. Supplemental Guidance: An organization-wide risk management strategy includes, for example, an unambiguous expression of the risk tolerance for the organization, acceptable risk assessment methodologies, risk mitigation strategies, a process for consistently evaluating risk across the organization with respect to the organization's risk tolerance, and approaches for monitoring risk over time. The use of a risk executive function can facilitate consistent, organization-wide application of the risk management strategy. The organization-wide risk management strategy can be informed by risk-related inputs from other sources both internal and external to the organization to ensure the strategy is both broad-based and comprehensive. Related control: RA-3.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

PM-10 SECURITY AUTHORIZATION PROCESS	
Control:	
The organization: a. Manages (i.e., documents, tracks, and reports) the security state of organizational information systems through security authorization processes; b. Designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and c. Fully integrates the security authorization processes into an organization-wide risk management program. **Supplemental Guidance:** The security authorization process for information systems requires the implementation of the Risk Management Framework and the employment of associated security standards and guidelines. Specific roles within the risk management process include a designated authorizing official for each organizational information system. Related control: CA-6.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

PM-11 MISSION/BUSINESS PROCESS DEFINITION	
Control:	
The organization: a. Defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and b. Determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until an achievable set of protection needs is obtained. **Supplemental Guidance:** Information protection needs are technology-independent, required capabilities to counter threats to organizations, individuals, or the Nation through the compromise of information (i.e., loss of confidentiality, integrity, or availability). Information protection needs are derived from the mission/business needs defined by the organization, the mission/business processes selected to meet the stated needs, and the organizational risk management strategy. Information protection needs determine the required security controls for the organization and the associated information systems supporting the mission/business processes. Inherent in defining an organization's information protection needs is an understanding of the level of adverse impact that could result if a compromise of information occurs. The security categorization process is used to make such potential impact determinations. Mission/business process definitions and associated information protection requirements are documented by the organization in accordance with organizational policy and procedure. Related controls: PM-7, PM-8, RA-2.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Project Management (PM) Security Controls Detail and Comment

ADDITIONAL CONTROLS REQUIRED BY IRS PUBLICATION 1075 – Protection of FTI in Virtual Environments	
Control:	
Notification Requirements • The agency must notify the IRS Office of Safeguards 45 days prior to putting FTI in a virtual environment. • If the agency's approved SPR is less than six years old and reflects the agency's current process, procedures and systems, the agency must submit the Virtualization Notification (see Exh bit 15), which will serve as an addendum to their SPR. • If the agency's SPR is more than six years old or does not reflect the agency's current process, procedures and systems, the agency must submit a new SPR and the Virtualization Notification (see Exhibit 15). Technical Requirements • When FTI is stored in a shared location, the agency must have policies in place to restrict access to FTI to authorized users. • Programs that control the hypervisor should be secured and restricted to authorized administrators only. • FTI data transmitted via hypervisor management communication systems on untrusted networks must be encrypted using FIPS-approved methods, provided by either the virtualization solution or third party-solution, such as a virtual private network (VPN) that encapsulates the management traffic. • Separation between virtual machines (VMs) must be enforced, and functions which allow one VM to share data with the hypervisor or another VM, such as clipboard sharing or shared disks, must be disabled. • Virtualization providers must be able to monitor for threats and other activity that is occurring within the virtual environment. This includes being able to monitor the movement of FTI into and out of the virtual environment. • The VMs and hypervisor/ host OS software for each system within the virtual environment that receives, processes, stores or transmits FTI must be hardened in accordance with the requirements of Publication 1075 and be subject to frequent vulnerability testing. • Special VM functions available to system administrators in a virtualized environment that can leverage the shared memory space in a virtual environment between the hypervisor and VM should be disabled. • Virtual systems are configured to prevent FTI from being dumped outside of the VM when system errors occur. • Vulnerability assessment must be performed on systems in a virtualized environment prior to system implementation. • Backups (virtual machine snapshot) must be properly secured and must be stored in a logical location where the backup is only accessible to those with a need to know. For FTI: Complete SPR section 9.28.2	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

ADDITIONAL CONTROLS REQUIRED BY IRS PUBLICATION 1075 – Protection of FTI in Voice over IP (VOIP) Networks	
Control:	
• VoIP traffic that contains FTI should be segmented off from non-VoIP traffic via a virtual Local Area Network (vLAN) or other segmentation method. If complete segmentation is not feasible, the agency must have compensating controls in place and properly applied which restrict access to VoIP traffic which contains FTI. • When FTI is in-transit across the network (either Internet or state agency's network) the VoIP traffic must be encrypted using a NIST-approved method operating in a NIST-approved mode. • VoIP network hardware (servers, routers, switches, firewalls) must be physically protected in accordance with the minimum protection standards for physical security outlined in IRS Publication 1075, section 4.0, Secure Storage. • Each system within the agency's network that transmits FTI to an external customer through the VoIP network is hardened in accordance with the requirements of Publication 1075 and is subject to frequent vulnerability testing. • VoIP-ready firewalls must be used to filter VoIP traffic on the network. • Security testing must be conducted on the VoIP system prior to implementation with FTI and annually thereafter. • VoIP phones must be logically protected and agencies must be able to track and audit all FTI-applicable conversations and access For FTI: Complete SPR section 9.28.3	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

ADDITIONAL CONTROLS REQUIRED BY IRS PUBLICATION 1075 – Protection of FTI in Cloud Computing Environments
Control:
Notification Requirements • The agency must notify the IRS Office of Safeguards 45 days prior to putting FTI in a cloud environment. • If the agency's approved SPR is less than six years old and reflects the agency's current process, procedures and systems, the agency must submit the Cloud Computing Notification (see Exhibit 16), which will serve as an addendum to their SPR. • If the agency's SPR is more than six years old or does not reflect the agency's current process, procedures and systems, the agency must submit a new SPR and the Cloud Computing Notification (see Exhibit 16). Technical Requirements • Data Isolation. Software, data, and services that receive, transmit, process, or store FTI must be isolated within the cloud environment so that tenants sharing physical space cannot access their neighbors' physically co-located data and applications. • Service Level Agreements (SLA). The agency must establish security policies and procedures based on IRS Publication 1075 for how FTI is stored, handled, and accessed inside the cloud through a legally binding contract or Service Level Agreement (SLA) with their third party cloud provider. • Data Encryption in Transit. FTI must be encrypted in transit within the cloud environment. All mechanisms used to encrypt FTI must be FIPS 140-2 compliant, and operate utilizing the FIPS 140-2 compliant module. This requirement must be included in the SLA. • Data Encryption at Rest. FTI must be encrypted while at rest in the cloud. All mechanisms used to encrypt FTI must be FIPS 140-2 compliant, and operate utilizing the FIPS 140-2 compliant module. This requirement must be included in the SLA. • Security Control Validation. Agencies must validate security control implementation claims made by cloud providers through a security plan and security control assessments. For FTI: Complete SPR section 9.28.4

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Attachment F-10 – Sample Security Assessment Report

In this attachment Unisys provides a sample quarterly Vulnerability Analyses (VA) and penetration testing report.

This page intentionally left blank.

Attachment B: Sample Security Assessment Report

Deloitte.

CLIENTX

Vulnerability Assessment Report

As of mm/dd/2013

DRAFT - Representative Sample Only

All Rights Reserved
As used in this document, 'Deloitte' means Deloitte Consulting LLP and Deloitte & Touche LLP. These entities are separate subsidiaries of Deloitte LLP. Deloitte Consulting LLP will be responsible for the services and the other subsidiaries may act as subcontractors. Please see www.deloitte com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Copyright © 2013 Deloitte Development LLC. All rights reserved.

This report is the property of, and is proprietary to Deloitte. It is not to be disclosed in whole or in part without the express written authorization of Deloitte. No portion of this Document shall be duplicated in any manner for any purpose other than as specifically permitted herein.

This page intentionally left blank.

□□□ □ □□□ □□□□

1. Overview

Prov des an overview about the project listing the scope details, time line and vulnerability sever ty matrix.

1.1 Scope & Objective

The Scope of ClientX assessment was to perform vulnerability assessment and Penetration Testing on selected external systems and web appl cations. The primary objective of this engagement was to:

- Identify potential vulnerabilities that may compromise the integr ty, conf dentiality and reliabil ty of ClientX's IT infrastructure
- Prov de technical recommendat ons to ClientX to mitigate risks associated with the identified vulnerabilities and improve the secur ty posture of the in-scope systems and web appl cations

The external systems, web applicat ons, databases and wireless instances that are in the scope of the assessment are listed in the table below:

External IP addresses in-scope for network assessment

IP Ranges	Network Block	Number of IP Addresses
XX.XX.26.0 - XX.XX.26.255	XX.XX.26.0/24	256

Internal IP addresses in-scope for network assessment

IP Ranges	Network Block	Number of IP Addresses
XX.XX.81.0 - XX.XX.81.255	XX.XX.80.0/24	256

Appl cations in-scope for appl cation assessment

Appl cation	User Details
Appl cation1	DttAdmin (Administrator) DttTest (Normal User)
Appl cation2	
Appl cation3	DttAdmin1 (Administrator) DttTest1 (Normal User)
Appl cation4	

1. Overview

Database Instances in-scope:

Database Name:
Database 1
Database 2
Database 3

Wireless Access points in-scope:

Access point:
Access point1
Access point2

List of devices in-scope for configurat on

Dev ce Name:
Dev ce1
Dev ce2

1.2 Timeline

The ons te and remote vulnerabil ty assessment activ ties were conducted from xx-May-2013 through xx-June-2013. The specific fieldwork performed for the vulnerabil ty assessments included non-intrusive testing of the selected ClientX's external network systems, web applications, databases and wireless infrastructure is described in the tables below:

IP addresses in-scope for network assessment

IP Ranges	Location	Date	Local Time(EDT)	India Time(IST)
XX.XX.26.0 - XX.XX.26.255	Location1 (Internal)	xx-Dec-2009	9:30 PM	7:00 AM
XX.XX.81.0 - XX.XX.81.255	Locat on2 (External)	xx-Dec-2009	9:30 PM	7:00 AM

Appl cations in-scope for appl cation assessment

Applicat ons	Location	Date	Local Time(EDT)	India Time(IST)
Appl cation1	Location1	xx-Dec-2009	9:30 PM	7:00 AM
Appl cation2	Location2	xx-Dec-2009	9:30 PM	7:00 AM
Appl cation3	Location2	xx-Dec-2009	9:30 PM	7:00 AM
Appl cation4	Location3	xx-Dec-2009	9:30 PM	7:00 AM

1.3 Vulnerability Severity & Effort of Fix Rating Matrix

Vulnerabil ties dentified in the target IT infrastructure are pr oritized by assigning severity to the vulnerabil ties based on factors associated w th the vulnerabil ty (such as impact, exploitability, affected users, ease of explo tation etc.). Another factor that helps in pr oritizing the vulnerability and developing the m tigat on strategy is the effort required to fix the vulnerability. The definition of the severity parameter and effort to fix the vulnerability is detailed below:

Severity	Definit ons
High	Exploitat on of the vulnerabil ty will result in super user access (i.e., Administrator) or unauthorized access to the privileged information.
Medium	Exploitat on of the vulnerabil ty could gain access to the sens tive information on the host or unauthorized access to non-sensitive data.
Low	Exploitat on of the vulnerabil ty could result in unauthorized access to informat onal data only.

These risk ratings are based on our judgment. The decis on as to the risk and implementat on of any remediation is the responsibility of ClientX management.

1. Overview

1.4 Confirmed vs. Probable Findings

As part of our analysis the team conducted add t onal manual tests to confirm vulnerabil ties, where vulnerabil ties cannot be positively confirmed they were categorized as probable.

Draft - Representative Sample Only

End of Report

2. Assessment Summary

Summary of the vulnerabilities identified, vulnerabil ty implicat ons, tactical and strateg c recom mendat ons to mitigate the vulnerabilities.

2.1 Assessment Findings

As part of the internal, external and application security assessment activities, Delo tte identified a total of 10 vulnerabilities including the following:

- Improper data val dat on is present in multiple instances of the internet facing web portal of ClientX. The data val dat on issue may allow malicious users to execute database and HTML script commands through the web appl cation. This may lead to disclosure of sens tive information such as user credentials and database details, affecting the confidentiality and integrity of the applicat on and related infrastructure

- Insecure remote access services were found enabled on the Internet facing systems. This service is susceptible to confidential ty breaches as data is transmitted in clear text over the Internet
- SSL certif cate pol cy implemented on the systems enables the use of obsolete SSL vers ons w th known weaknesses that have demonstrated SSL based attacks
- Obsolete and vulnerable vers ons of operating system and software technology was found running on the target systems. This may affect the availability of the applicat ons running on the vulnerable systems
- Technology information and system details are revealed through service banner of the system and application error page
- Printing serv ce and HTTP method was found enabled on the Internet facing web servers of ClientX.

Of the 10 vulnerabilities, the team was not able to confirm 3 vulnerabilities due to the nature of the vulnerabil ties and considering the scope of assessment activ ties. These vulnerabil ties were categorized as probable.

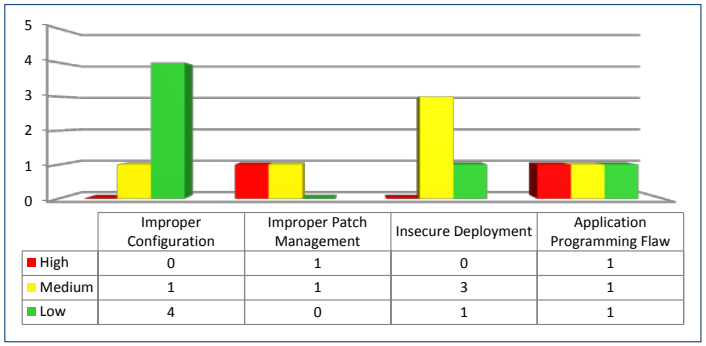
The vulnerabilities along with their severity are presented in the table below.

Assessment Area	Vulnerabil ty Instances			TOTAL
	High	Medium	Low	
External	1	1	2	3
Internal		2	1	4
Appl cation	1	1	1	3
Database	0	1	1	
Wireless	0	1	1	
Total	2	6	6	10

2. Assessment Summary

2.2 Root Cause Analysis

The testing team analyzed the possible root causes associated with the confirmed and probable vulnerabilities. After the analysis, team devised root cause categories by organizing them based on common attributes and issues. The results of this analysis are depicted below.



	Improper Configuration	Improper Patch Management	Insecure Deployment	Application Programming Flaw
High	0	1	0	1
Medium	1	1	3	1
Low	4	0	1	1

2.3 Detailed-Level Recommendations for Remediation

In order to improve ClientX's security posture and m tigate the potential risks from the observed vulnerabil ties, Deloitte suggests ClientX to implement following tact cal and strategic measures.

Tactical Recommendations

The tact cal steps are associated with the resolut on of specific vulnerabilities observed during this engagement. These activities typ cally focus on addressing the vulnerabilities in a timely and pr oritized manner, and involve following activ ties:

- Implement a central library for input validations to ensure that all the input and output parameters are validated both at the client side and server s de, before they are used and transm tted
- Use secure services such as SecureFTP and TelnetS wh ch use encrypted communication channel to transmit informat on
- Secure the systems by disabling the outdated and deprecated SSL protocols, and enforce the use of strong ciphers
- Implement effective patch management in order to ensure that target operating system and software are running w th latest versions
- Customize the service banner information of the systems so that technology and system details are not disclosed to the end users
- Handle all the errors and exceptions generated by the appl cation and redirect the user to a customized error page without disclosing technology and system details
- Ensure that only required services and HTTP methods are enabled on the Internet systems

At a minimum, ClientX should prior tize and remediate the technical observat ons in this report. Deloitte recommends that the vulnerabil ties observed should be treated in order of their risk significance to ClientX namely - High severity vulnerabilities should be addressed immediately, followed by the Medium severity findings, followed by Low sever ty ones.

2. Assessment Summary

Strategic Recommendations

In addition to solving the technical issues, ClientX should also consider resolution of the system root causes that may have led to the individual vulnerabilities observed. ClientX should provide a more strategic focus to preventing similar issues from recurring and negatively impacting the organization's security posture in the future. Some security areas that ClientX may want to consider as part of its strategic efforts should include secure application design and development, network architecture planning and deployment, configuration management, patch management, security assessments and other similar items.

In summary, ClientX should consider implementing the following strategic actions:

- Lifecycle based vulnerability management solution that integrates closely with ClientX's processes, capable of timely discovery, remediation of vulnerabilities and prepares ClientX to face and respond to new threats. An effective vulnerability management solution is well-aligned with applicable industry standards, regulations and requirements such as, but not limited to: ISO/IEC 27001, COBIT, PCI-DSS and ITIL.
- Proactive and comprehensive secure development solution to enable incorporating security activities to identify, prioritize and mitigate application/database security vulnerabilities during development, deployment and maintenance processes. Security activities including application foot printing, information classification and periodic vulnerability testing enable development of appropriate access control guidelines for ClientX in order to maintain the security posture of the respective applications and databases.
- An effective configuration management and change management process should be established and appropriately publicized. This should include proactive monitoring of configuration violations and unauthorized changes to the environment.
- Periodic infrastructure risk assessments should be performed, especially where ClientX is deploying extensions to their trusted environment. ClientX should consider as part of its periodic risk assessments external infrastructure such as routers, firewalls, application, risks associated with internal infrastructure devices, servers and databases, and any extensions of its network through leased or dedicated partner networks.
- An information security awareness program to train all end-users (technical and non-technical) of relevant information security policies and procedures.

Draft - Representative Sample Only

End of Report

3. External Active Hosts

Detailed results from our Intelligence gathering effort to identify active hosts within the ranges, ports/serv ces open on these active systems, applicat ons hosted other protocol specif c information.

3.1 Open TCP / UDP Ports List

		Open Ports					
IP address	Host Name	123/UDP (NTP)	22/TCP (ssh)	23/TCP (telnet)	443/TCP (https)	80/TCP (http)	Grand Total
XX.XX.26.1	Not resolved			1		1	2
XX.XX.26.3	Not resolved		1				1
XX.XX.26 51	Not resolved		1		1		2
XX.XX.26 52	Not resolved		1				1
XX.XX.26 53	www.xxx.com	1		1		1	3
Grand Total		1	3	2	1	2	9

3.2 Operating System Details

		Operating System version			
IP address	Host Name	Linux	Not Found	Windows	Grand Total
XX.XX.26.1	Not resolved			1	1
XX.XX.26.3	Not resolved	1			1
XX.XX.26 51	Not resolved		1		1
XX.XX.26 52	Not resolved			1	1
XX.XX.26 53	www.xxx.com			1	1
Grand Total		1	1	3	5

4.3 Service Version Details

		Service Vers on Cisco IOS administrative httpd				
IP address	Host Name		Cisco SSH 1.25	Not Found	OpenSSH 3.2.3p1	Grand Total
XX.XX.26.1	Not resolved	1				1
XX.XX.26.3	Not resolved			1		1
XX.XX.26 51	Not resolved		1			1
XX.XX.26 52	Not resolved				1	1
XX.XX.26 53	www.xxx.com				1	1
Grand Total		1	1	1	2	5

4.4 ICMP Details

		ICMP Enabled (Yes/No)		
IP address	Host Name	No	Yes	Grand Total
XX.XX.26.1	Not resolved		1	1
XX.XX.26.3	Not resolved	1		1
XX.XX.26 51	Not resolved		1	1
XX.XX.26 52	Not resolved		1	1
XX.XX.26 53	www.xxx.com		1	1
Grand Total		1	4	5

Draft - Representative Sample Only

End of Report

4. External Vulnerabilities

Detailed list of vulnerabilities identified on the Internet facing hosts along w th description, impact, severity and recommendat ons.

4.1 External Network Vulnerability List

	External Vulnerabilities			
IP address / Host Name	Insecure Services were found running	Microsoft IIS 5 .printer ISAPI Filter Enabled	PHP Mail Funct on Header Spoofing Vulnerability	Grand Total
XX.XX.26.1	**1**			**1**
XX.XX.26.51		**1**	**1**	**2**
XX.XX.26.52			**1**	**1**
XX.XX.26.53			**1**	**1**
Grand Total	1	1	3	5

4.2 External Network Vulnerability Details

IP address	Vulnerabil ty ID	Vulnerability	Vulnerabil ty Description & Explo tation Steps (if appl cable)	Vulnerability Remediation	Severity	Likelihood	Effort to Fix
XX.XX.26.1	V_1	Insecure Services were found running	FTP, Telnet are application layer protocols, that either use clear text communication channel to exchange information or weak symmetric encryption. This type of communication is susceptible to sniffing attacks and man-in-the-middle attack. Also, these protocols are inherently vulnerable to bruteforce and session hijacking attacks.	Deloitte & Touche recommends following measures to prevent the existence of this vulnerability : • Implement secure service like Secure FTP, SSH (Secure Shell) and/or TelnetS, which are ciphered and support cryptographic functions. • Implement two-factor authentication system to evade brute-force attacks.	Medium	Low	Medium
XX.XX 26.51 XX.XX 26.52 XX.XX 26.53	V_2	PHP Mail Function Header Spoofing Vulnerability	PHP is a scripting language for producing dynamic web based applications and sites. Nessus vulnerability scanner reported that the remote host is running a outdated and vulnerable version of PHP (<= 4.2 2). This version of PHP has a vulnerable mail() function which does not properly sanitize user input. This allows users to forge email to make it look like it is coming from a different source other than the server. Attackers can exploit this vulnerability to forge emails to any entity, even if SAFE_MODE is enabled **References**: CVE: 2002-0985 [redacted]	Deloitte & Touche recommends following measures to prevent the existence of this vulnerability : • Implement a Patch Management system, which enforces the system to apply released patches for vulnerabilities and ensure all Internet Systems are fully patched and updated till the latest version of the application, base technology and Operating System being used • Implement a perimeter based deterrent technology (i.e. firewall, IDS/IPS, etc) to restricts, blocks malicious packets from reaching the vulnerable services	Medium	Low	Medium
XX.XX 26.51	V_3	Microsoft IIS 5 printer ISAPI Filter Enabled	IPP Facilitates printing over an IP based network and for managing print requests over the Internet, WAN, LAN and other types of IP based networks. This service allows users to print jobs by queuing several jobs simultaneously. IPP on IIS 5 0 is implemented as an extension of ISAPI filter. This service/extension has been reported by "publicly disclosed vulnerability lists" to be vulnerable to several buffer overflow attacks. It is possible to perform a Denial-of Service attack on the host(s) by sending numerous print jobs from the Internet. An attacker can also exploit this vulnerable service/extension to gain unauthorized access. **References:** CVE: 2001-0241 [redacted]	Deloitte & Touche recommends following measures to prevent the existence of this vulnerability : • Disable the Internet Printing Protocol (IPP) if there is no business requirement • Enable proper application boundary controls to allow only white listed hosts to use the service In order to disable the IPP service, Delete the Internet Print Provider Registry Key: - Go to Administrative Tools - Double-click Services - Stop the Print Spooler service - Use the Microsoft Registry Editor (Regedit exe) to delete the following key from the registry: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Providers\Internet Print Provider - Restart the Print Spooler service	Low	Low	Low

Draft - Representative Sample Only

End of Report

5. Database Vulnerabilities

Detailed list of vulnerabilities identified on the in-scope database instances along w th description, impact, severity and recommendat ons.

5.1 Database Vulnerability List

IP Address / Database instance Name	Database Vulnerabil ties			
	Default, blank or weak (Insecure) Password	Improper input validation leading to SQL Injection	Extensive user and group previlages	Grand Total
Database 1			**1**	**1**
Database 2	**1**	**1**		**2**
Database 3			**1**	**1**
Grand Total	1	1	2	4

5.2 Database Vulnerability Details

IP address/ Database Instance Name	Vulnerabil ty ID	Vulnerability	Vulnerability Descript on & Exploitat on Steps (if applicable)	Vulnerabil ty Remediation	Status	Severity	Likelihood	Effort to Fix
Application1	V_8	Default, blank or weak (Insecure) password			Confirmed	High	Medium	High
Application1	V_9	Improper input validation leading to SQL Injection	SQL Injection is a technique where SQL queries injected through the web application are executed in the backend database, due to lack of appropriate input validation in the web application. The attacker sends a specially crafted SQL scripts in order to modify queries being sent to the database. SQL Injection is possible in the “Search” and “Advanced Search” modules of the “xxxx.com” application by tampering the form parameter “Search Name”. Team was able to exploit the vulnerability by entering malicious SQL commands in the form parameter. Exploitation The steps that are required to exploit the vulnerability on the “Search” module are detailed below, Steps 1. Access “xxxx.com” web application by browsing the URL http://www.xxxx com/homePage.aspx 2. Click the “Search” tab on “Members” menu (URL is http://www.xxxx com/formularySearch_2009.aspx) 3. In “Search” page, enter invalid search criteria (along with single quotes – for example, “test'”) for the form parameter “Search Name”. This will generate a SQL error message, as the application is not properly validating the value of “Search name” form parameter. 4. After confirming the existence of SQL Injection, team	Deloitte recommends following measures to prevent the existence of this vulnerability: • Implement a central library for input validations (both at the client side and server side) and ensure that all the input/output parameters are validated before they are used/transmitted • Do not send or receive parts of SQL statement to/from client browser	Confirmed	Medium	Medium	Medium

5. Database Vulnerabilities

Detailed list of vulnerabilities identified on the in-scope database instances along w th description, impact, severity and recommendat ons.

5.1 Database Vulnerability List

IP Address / Database instance Name	Database Vulnerabil ties			
	Default, blank or weak (Insecure) Password	Improper input validation leading to SQL Injection	Extensive user and group previlages	Grand Total
Database 1			**1**	**1**
Database 2	**1**	**1**		**2**
Database 3			**1**	**1**
Grand Total	1	1	2	4

5.2 Database Vulnerability Details

IP address/ Database Instance Name	Vulnerabil ty ID	Vulnerability	Vulnerability Descript on & Exploitat on Steps (if applicable)	Vulnerabil ty Remediation	Status	Severity	Likelihood	Effort to Fix
Application2 Application3	V_10	Extensive user and group previlages			Confirmed	Low	Low	Low

Draft - Representative Sample Only

End of Report

6. Application Vulnerabilities

Detailed list of vulnerabil ties dentified on the in-scope web applicat ons along w th descript on, impact, severity and recommendations.

6.1 Web Application Vulnerability List

	Application Vulnerabil ties			
IP Address / Applicat on Name	Improper input val dat on leading to SQL Injection	Improper Input/Output val dat on leading to Cross S te Scripting attack	Applicat on error page reveals technology and system details	Grand Total
Application1	**1**	**1**		**2**
Application2			**1**	**1**
Application3			**1**	**1**
Grand Total	1	1	2	4

6.2 Web Application Vulnerability Details

IP address/ Applicat on Name	Vulnerability ID	Vulnerabil ty	Vulnerability Description & Exploitation Steps (if appl cable)	Vulnerabil ty Remediation	Severity	Likelihood	Effort to Fix
Application1	V_8	Improper input validation leading to SQL Injection	SQL Injection is a technique where SQL queries injected through the web application are executed in the backend database, due to lack of appropriate input validation in the web application. The attacker sends a specially crafted SQL scripts in order to modify queries being sent to the database. SQL Injection is possible in the “Search” and “Advanced Search” modules of the “xxxx com” application by tampering the form parameter “Search Name”. Team was able to exploit the vulnerability by entering malicious SQL commands in the form parameter. Exploitation The steps that are required to exploit the vulnerability on the “Search” module are detailed below, Steps 1. Access “xxxx.com” web application by browsing the URL http://www xxxx.com/homePage aspx 2. Click the “Search” tab on “Members” menu (URL is http://www xxxx.com/formularySearch_2009.aspx) 3. In “Search” page, enter invalid search criteria (along with single quotes – for example, “test’”) for the form parameter “Search Name”. This will generate a SQL error message, as the application is not properly validating the value of “Search name” form parameter. 4. After confirming the existence of SQL Injection, team injected the SQL command “‘ and 1=convert(int,db_name(0)) --” for the “Search Name” form parameter. This resulted in a SQL error	Deloitte recommends following measures to prevent the existence of this vulnerability: • Implement a central library for input validations (both at the client side and server side) and ensure that all the input/output parameters are validated before they are used/transmitted • Do not send or receive parts of SQL statement to/from client browser • Do not use dynamic SQL statements • Use parameterized stored procedures that enforce the data type to be accepted from the client and will not allow modifications to the syntax of the SQL query.	High	Medium	High
Application1	V_9	Improper Input/Output validation leading to Cross Site Scripting attack	Cross site scripting (XSS) is caused by the failure of the application to properly validate user input before returning it to the client’s web browser. This weakness allows attackers to embed malicious HTML-based content, such as JavaScript, within client HTTP requests. Cross site scripting has been identified in different areas of the web application. One instance is on the Search module (‘searchresults aspx’) of the application. There is no proper input validation on ‘searchtext’ query string parameter available in the ‘searchresults.aspx’ web page. This will allow the malicious user to enter scripts and other invalid characters which will get executed in the application page. The vulnerable URL is “http://<<hostname>>/searchresults.aspx?searchterm=<script >alert(‘TEST’)</script> ”. Cross Site Scripting could allow a malicious user to launch following type of attacks, • Session hijacking • Page defacement • Phishing attack This allows to steal sensitive information such as user credentials and affects the confidentiality, integrity and availability o the user and application.	Deloitte recommends following measures to prevent the existence of this vulnerability: • Implement a central library for input validations and ensure that all input parameters (such as HTTP headers, query strings, form fields, cookies and hidden fields) which can be controlled and tampered by the end user, are validated before being used or transmitted. • Preferably, input validation should be performed against a known whitelist of valid characters. In other words, allow only those characters that are in the whitelist and block/filter every other input. • Encode all the user supplied data which becomes part of the application output using HTML entity encoding, for e.g. • “<” to < “>” to > “(“ to (“)” to) “&” to & Further as a best practice, • Implement a perimeter based application level firewall to filter out malicious URL and to restrict malicious URL redirection • Avoid redirection to external sites and 3rd party domains. If it is necessary to do so, make sure to validate the URL to which the application is redirected to, and avoid redirections to unknown sites.	Medium	Medium	Medium

6. Application Vulnerabilities

Detailed list of vulnerabil ties dentified on the in-scope web applicat ons along w th descript on, impact, severity and recommendations.

6.1 Web Application Vulnerability List

	Application Vulnerabil ties			
IP Address / Applicat on Name	Improper input val dat on leading to SQL Injection	Improper Input/Output val dat on leading to Cross S te Scripting attack	Applicat on error page reveals technology and system details	Grand Total
Application1	**1**	**1**		**2**
Application2			**1**	**1**
Application3			**1**	**1**
Grand Total	1	1	2	4

6.2 Web Application Vulnerability Details

IP address/ Applicat on Name	Vulnerability ID	Vulnerabil ty	Vulnerability Description & Exploitation Steps (if appl cable)	Vulnerabil ty Remediation	Severity	Likelihood	Effort to Fix
Application2 Application3	V_10	Application error page reveals technology and system details	Error page of the application reveals technology and system details such as application framework, version details, web server technology and physical path of the system. Error page revealing technology and system details are present through the applications. These error pages are generated when the user tries to enter invalid characters or accesses files that are not present in the target server. The information present in the error page allows the malicious user to understand the technology that is running on the host and the directory structure. This will allow to launch targeted attacks on the application and related infrastructure.	Deloitte recommends following measures to prevent the existence of this vulnerability: • Redirect the user to a customized error page which contains generic information rather than technology and system specific details • Log the error details in the log server which will help to diagnose the problem, identify the root cause of the error and fix the issue.	Low	Low	Low

Draft - Representative Sample Only

End of Report

7. Wireless Infrastructure Vulnerabilities

Detailed list of vulnerabilities identified on the in-scope wireless access points along with descript on, impact, sever ty and recommendations.

7.1 Wireless Vulnerability List

	Wireless Vulnerabilities			
Access Point Name	Improper access controls	Insecure encryption protocol in use	Insecure Configuration	Grand Total
XX.XX.26.1	1			1
XX.XX.26.51		1	1	2
XX.XX.26.52			1	1
XX.XX.26.53			1	1
Grand Total	1	1	3	5

7.2 External Network Vulnerability Details

Access Point	Vulnerabil ty ID	Vulnerability	Vulnerabil ty Description & Explo tation Steps (if appl cable)	Vulnerability Remediation	Severity	Likelihood	Effort to Fix
Name1	V_1	Improper Access Controls	FTP, Telnet are application layer protocols, that either use clear text communication channel to exchange information or weak symmetric encryption. This type of communication is susceptible to sniffing attacks and man-in-the-middle attack. Also, these protocols are inherently vulnerable to bruteforce and session hijacking attacks.	Deloitte & Touche recommends following measures to prevent the existence of this vulnerability : • Implement secure service like Secure FTP, SSH (Secure Shell) and/or TelnetS, which are ciphered and support cryptographic functions. • Implement two-factor authentication system to evade brute-force attacks.	Medium	Low	Medium
Name1	V_2	Insecure Encryption protocol in use	PHP is a scripting language for producing dynamic web based applications and sites. Nessus vulnerability scanner reported that the remote host is running a outdated and vulnerable version of PHP (<= 4.2 2). This version of PHP has a vulnerable mail() function which does not properly sanitize user input. This allows users to forge email to make it look like it is coming from a different source other than the server. Attackers can exploit this vulnerability to forge emails to any entity, even if SAFE_MODE is enabled **References**: CVE: 2002-0985 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0985	Deloitte & Touche recommends following measures to prevent the existence of this vulnerability : • Implement a Patch Management system, which enforces the system to apply released patches for vulnerabilities and ensure all Internet Systems are fully patched and updated till the latest version of the application, base technology and Operating System being used • Implement a perimeter based deterrent technology (i.e. firewall, IDS/IPS, etc) to restricts, blocks malicious packets from reaching the vulnerable services	Medium	Low	Medium
Name2	V_3	Insecure Configuration	IPP Facilitates printing over an IP based network and for managing print requests over the Internet, WAN, LAN and other types of IP based networks. This service allows users to print jobs by queuing several jobs simultaneously. IPP on IIS 5 0 is implemented as an extension of ISAPI filter. This service/extension has been reported by "publicly disclosed vulnerability lists" to be vulnerable to several buffer overflow attacks. It is possible to perform a Denial-of Service attack on the host(s) by sending numerous print jobs from the Internet. An attacker can also exploit this vulnerable service/extension to gain unauthorized access. **References:** CVE: 2001-0241 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0241	Deloitte & Touche recommends following measures to prevent the existence of this vulnerability : • Disable the Internet Printing Protocol (IPP) if there is no business requirement • Enable proper application boundary controls to allow only white listed hosts to use the service In order to disable the IPP service, Delete the Internet Print Provider Registry Key: - Go to Administrative Tools - Double-click Services - Stop the Print Spooler service - Use the Microsoft Registry Editor (Regedit exe) to delete the following key from the registry: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Providers\Internet Print Provider - Restart the Print Spooler service	Low	Low	Low

Draft - Representative Sample Only

End of Report

8. Social Engineering Analysis

Analysis of social engineering test performed to identify the Commonwealth's potential vulnerabil ty to email based phishing attacks.

8.1 List of Social Engineering Tests

	Social Engineeirng Tests			
Group ID	Email Phishing Attack	Phone Call Phishing Attack	USB Social Engoneering Attack	Grand Total
Group 1	**1**	**1**		**2**
Group 2			**1**	**1**
Group 3			**1**	**1**
Grand Total	1	1	2	4

8.2 Social Engineering Analysis Details

Group ID	Vulnerability ID	Vulnerabil ty	Vulnerability Description & Exploitation Steps (if applicable)	Vulnerability Remediat on	Severity	Likelihood	Effort to Fix
Group 1	A_1	Email Phishing Attack			High	Low	High
Group 2	A-2	Phone Call Phishing Attack			Low	Low	Low
Group 2 Group3	A-3	USB Social Engineering Attack			Medium	Medium	Medium

Draft - Representative Sample Only

End of Report

Appendix - Legend

Prov des definit on of the risk ratings and descript on of the high-level categories

A.1 Vulnerability Severity & Likelihood Rating Matrix

Vulnerabil ties dentified in the target IT infrastructure are pr oritized by assigning severity to the vulnerabil ties based on factors associated w th the vulnerability (such as impact, affected users, ease of explo tation, etc.). Other factor that is used to pr oritize the vulnerabil ty is likelihood of exploiting the vulnerabil ty . The defin tion of these parameters are detailed below:

Rating	Severity	Likelihood	Estimated Effort to fix
High	Explo tation of the vulnerability will result in super user access (i.e., Administrator) or unauthorized access to the privileged information.	High probabilistic of a successful exploit w th an easily available explo t and the ability to avoid detect on.	Remediation effort requires multiple Full-Time Equivalent durat on of greater than 80 hours.
Medium	Explo tation of the vulnerability could gain access to the sensitive informat on on the host or unauthorized access to non-sens tive data.	Medium probabilist c of a successful explo t with a diff cult to obtain exploit and the abil ty to avo d detection.	Remediation effort requires multiple FTE and a durat on be hours.
Low	Explo tation of the vulnerability could result in unauthorized access to informat onal data only.	Low probabilistic of a successful exploit w th a difficult to obtain explo t and diff culty to avoid detect on.	Remediation effort requires one FTE and a durat on of less

These risk ratings are based on our experience in dentifying these issues. The decis on as to factor business risk, validate issue, determine and implement appropriate remediation is the responsibil ty of Client X

A.2 High Level Category Analysis

High Level Category Analysis

Several common themes were identified revealing the probable reasons for the vulnerabilities to exist. The analysis shows that the majority of issues fall into 3 distinct high level categories described below:

High-level Category	Description
Improper authent cation and authorizat on controls	Improper authenticat on & authorizat on controls on critical production information systems and networks may lead to unauthorized access to sensitive informat on
Missing patches	Software technologies, information systems or devices which are outdated, not updated or patched regularly with the publ cly disclosed secur ty fixes increases the risk of compromise or affect its reliabil ty.increase the threat surface.
Mis-configurations	Improperly configured services on information systems and networks including default configuration could provide unauthorized access and disclosure of sensitive informat on or configuration data.

Draft - Representative Sample Only

End of Section

Appendix B - Glossary and Tools

Glossary of terms and the tools used during the secur ty assessment activ ties.

B.1 Glossary of terms used in this assessment report

Term	Description
ICMP Sweep	Probe the IP address range to dentify the live hosts that are responding to ICMP request.
Delete and PUT	The PUT is HTTP method allows that the enclosed ent ty be stored to a web server and DELETE HTTP method requests that the origin server to delete the resource on web server.
Vulnerability ID	Vulnerability ID is used to map the ID (V_X) present in the "Impact vs Likelihood" graph present in the worksheet "2-High Level Executive Summary" with indiv dual vulnerabil ties.
Confirmed	"Confirmed" vulnerabil ties are those vulnerabilities wh ch the team confirmed during the course of assessment activ ties.
Probable	Probable vulnerabilities are those vulnerabilities wh ch are reported either by tool or by publ c advisories, and the team was not able confirm these vulnerabilities e ther due to the nature of testing required for confirming the vulnerabil ties or due to lack of information available for confirming the vulnerabil ties.
Risk	Risk is the probability of a loss happening by the occurrence of an event, and depends on three elements, impact, vulnerabil ty and exposure.
Risk Level	Risk level denotes the level of risk based on three factors - vulnerability severity, impact and likelihood of occurrence of the event.
SSLv3/TLSv1	Secure socket Layers /Transport Layer security provide secur ty and data integrity for commun cations over networks. TLS and SSL encrypt the segments of network connections at the Transport Layer end-to-end.
Vulnerability	A weakness in an IT system that can be exploited by an attacker.

Appendix B - Glossary and Tools

Glossary of terms and the tools used during the security assessment activities.

B.2 List of support tools used for this assessment

Tool Name	Usage
Nmap	A stealth port scanner that identifies network devices, operating systems open ports.
Solarwinds	SolarWinds is a network discovery tool used to identify network devices. It includes tools from the following nine categories: CMTS & Subscriber Modem Tools, Bandwidth and Performance Management, Network Monitoring, Network Discovery Tools, Tools for Cisco Routers, Fault Monitoring Tools, MIB Browser Tools, Ping and Diagnostic Tools, IP Address Management Tools.
Superscan	Multithreaded connect-based port scanner, hostname resolver and ping tool that uses asynchronous techniques to identify open ports of network systems.
Nessus	A vulnerability scanner that allows customization of the ports and services to be scanned to identify vulnerabilities.
Nikto	A perl script that attempts to identify well-known URLs that may indicate a security weakness.
AppScan	AppScan is a commercial web application vulnerability scanner which is used to identify security weaknesses present in web applications.
Paros	Paros is a web application proxy and a vulnerability scanner which is used to intercept the web request and response, and also to identify the security weaknesses present in web applications.
TamperIE	TamperIE acts as a plug-in of Internet Explorer web browser, which is used to tamper the web request sent from the client browser.

Draft - Representative Sample Only

End of Report

Attachment F-11 – Sample Performance Reports

In this attachment Unisys includes a sample performance report titled, BPPM08.01 - Server Capacity - Drill down.

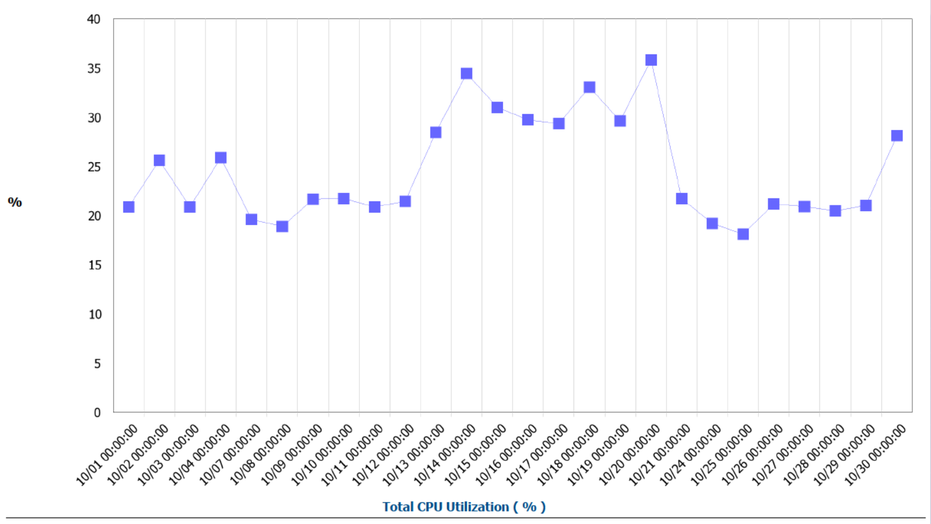
This page intentionally left blank.

BPPM08.01 - Server Capacity - Drill down

Aggregate Function: Min

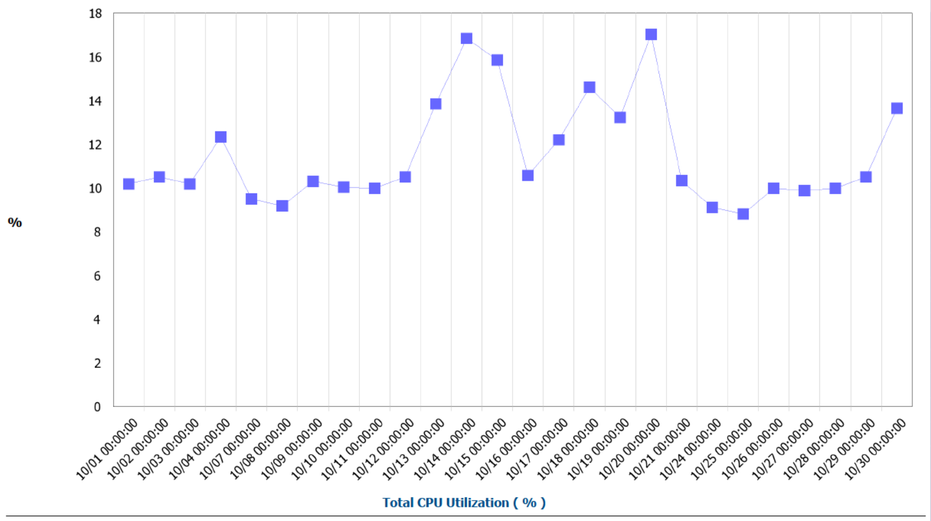
Report Period: 10-01-2012 00:00:00 to 10-30-2012 23:59:59 - IST

Server CPU Capacity



Daily	Value (%)
10/01 00:00:00	20.88
10/02 00:00:00	25.6
10/03 00:00:00	20.88
10/04 00:00:00	25.87
10/07 00:00:00	19.6
10/08 00:00:00	18.88
10/09 00:00:00	21.65
10/10 00:00:00	21.74
10/11 00:00:00	20.86
10/12 00:00:00	21.42
10/13 00:00:00	28.44
10/14 00:00:00	34.43
10/15 00:00:00	31
10/16 00:00:00	29.7
10/17 00:00:00	29.35
10/18 00:00:00	33.02
10/19 00:00:00	29.61
10/20 00:00:00	35.82
10/21 00:00:00	21.73
10/24 00:00:00	19.2
10/25 00:00:00	18.12
10/26 00:00:00	21.17
10/27 00:00:00	20.91
10/28 00:00:00	20.45
10/29 00:00:00	21
10/30 00:00:00	28.13

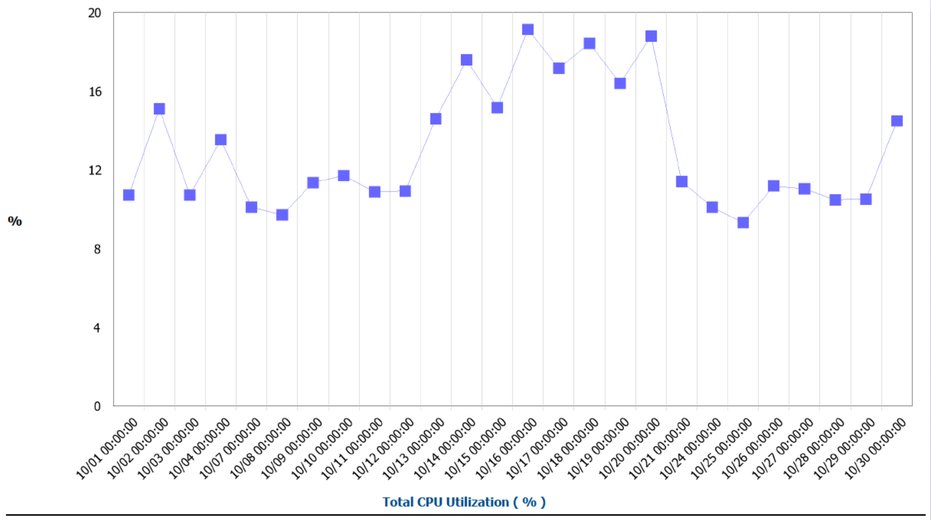
vm-w28-rds1627.pune-labs.bmc.com / vm-w28-rds1627.pune-labs.bmc.com Windows System



Daily	Value (%)
10/01 00:00:00	10.18
10/02 00:00:00	10.5
10/03 00:00:00	10.18
10/04 00:00:00	12.34
10/07 00:00:00	9.5
10/08 00:00:00	9.18
10/09 00:00:00	10.29
10/10 00:00:00	10.03
10/11 00:00:00	9.98
10/12 00:00:00	10.5
10/13 00:00:00	13.84
10/14 00:00:00	16.84
10/15 00:00:00	15.84
10/16 00:00:00	10.56
10/17 00:00:00	12.19
10/18 00:00:00	14.6
10/19 00:00:00	13.22
10/20 00:00:00	17.02
10/21 00:00:00	10.34
10/24 00:00:00	9.1
10/25 00:00:00	8.81
10/26 00:00:00	9.99
10/27 00:00:00	9.88
10/28 00:00:00	9.98
10/29 00:00:00	10.5
10/30 00:00:00	13.64

BPPM08.01 - Server Capacity - Drill down

vm-w23-rds28 / 10.128.28.62



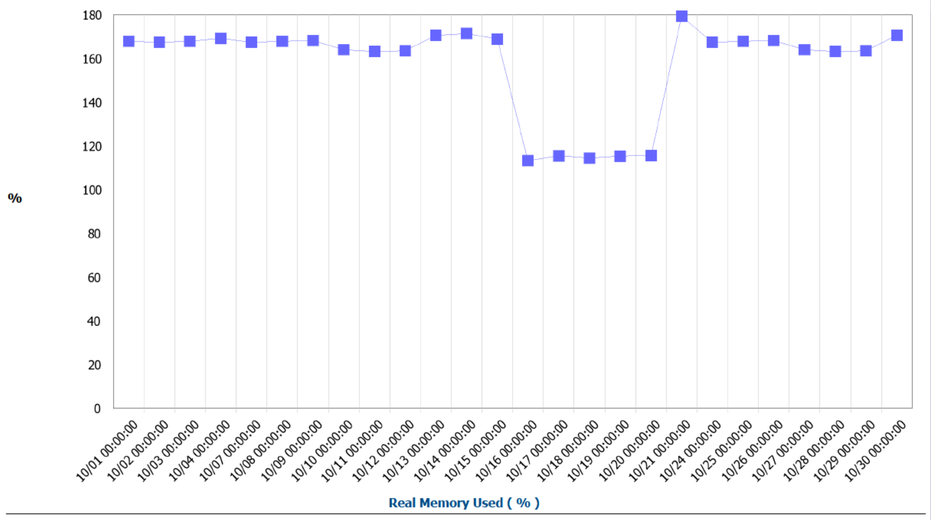
Daily	Value (%)
10/01 00:00:00	10.71
10/02 00:00:00	15.1
10/03 00:00:00	10.71
10/04 00:00:00	13.53
10/07 00:00:00	10.1
10/08 00:00:00	9.71
10/09 00:00:00	11.36
10/10 00:00:00	11.71
10/11 00:00:00	10.88
10/12 00:00:00	10.92
10/13 00:00:00	14.6
10/14 00:00:00	17.59
10/15 00:00:00	15.16
10/16 00:00:00	19.14
10/17 00:00:00	17.16
10/18 00:00:00	18.43
10/19 00:00:00	16.39
10/20 00:00:00	18.81
10/21 00:00:00	11.4
10/24 00:00:00	10.1
10/25 00:00:00	9.31
10/26 00:00:00	11.19
10/27 00:00:00	11.03
10/28 00:00:00	10.47
10/29 00:00:00	10.5
10/30 00:00:00	14.49

BPPM08.01 - Server Capacity - Drill down

Aggregate Function: Min

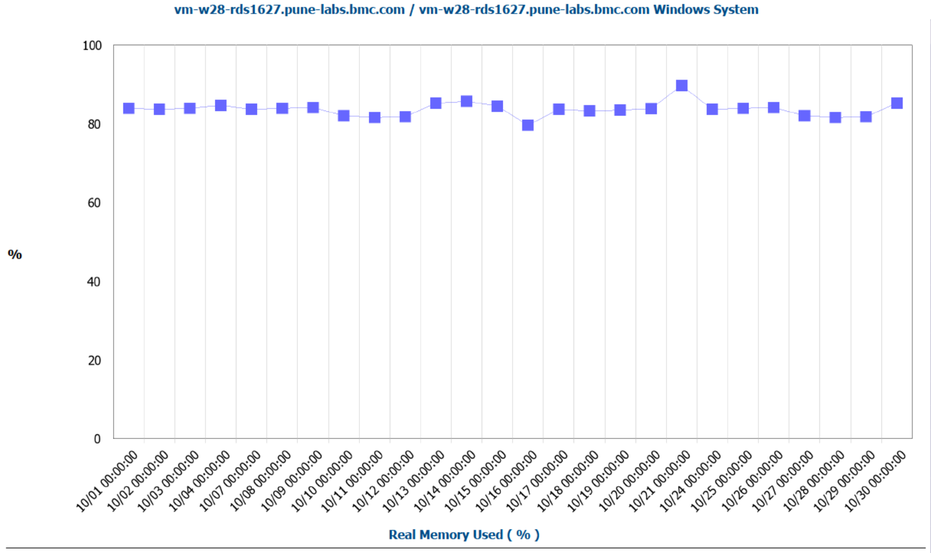
Report Period: 10-01-2012 00:00:00 to 10-30-2012 23:59:59 - IST

Server Memory Capacity



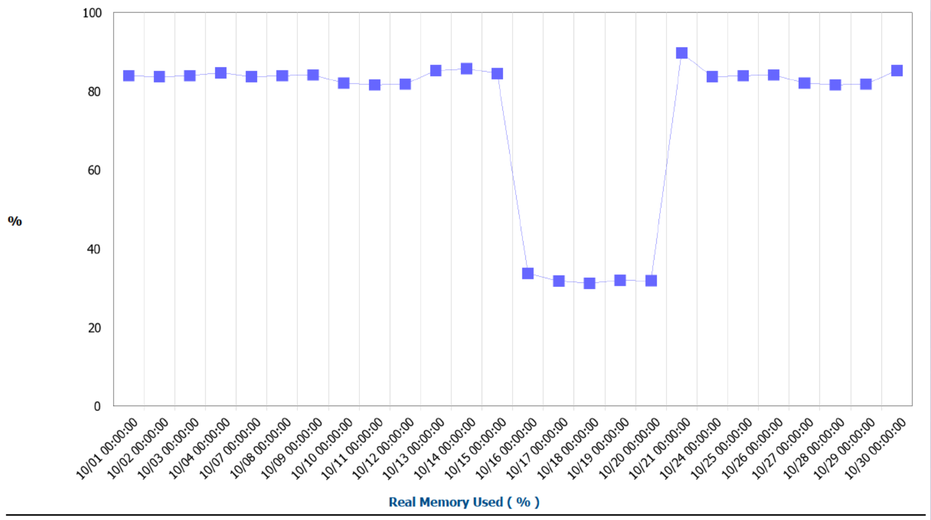
Daily	Value (%)
10/01 00:00:00	167.9
10/02 00:00:00	167.32
10/03 00:00:00	167.9
10/04 00:00:00	169.27
10/07 00:00:00	167.32
10/08 00:00:00	167.9
10/09 00:00:00	168.25
10/10 00:00:00	164
10/11 00:00:00	163.16
10/12 00:00:00	163.56
10/13 00:00:00	170.49
10/14 00:00:00	171.32
10/15 00:00:00	168.88
10/16 00:00:00	113.28
10/17 00:00:00	115.39
10/18 00:00:00	114.4
10/19 00:00:00	115.32
10/20 00:00:00	115.61
10/21 00:00:00	179.33
10/24 00:00:00	167.32
10/25 00:00:00	167.9
10/26 00:00:00	168.25
10/27 00:00:00	164
10/28 00:00:00	163.16
10/29 00:00:00	163.56
10/30 00:00:00	170.49

vm-w28-rds1627.pune-labs.bmc.com / vm-w28-rds1627.pune-labs.bmc.com Windows System



Daily	Value (%)
10/01 00:00:00	83.95
10/02 00:00:00	83.66
10/03 00:00:00	83.95
10/04 00:00:00	84.64
10/07 00:00:00	83.66
10/08 00:00:00	83.95
10/09 00:00:00	84.12
10/10 00:00:00	82
10/11 00:00:00	81.58
10/12 00:00:00	81.78
10/13 00:00:00	85.25
10/14 00:00:00	85.66
10/15 00:00:00	84.44
10/16 00:00:00	79.6
10/17 00:00:00	83.66
10/18 00:00:00	83.27
10/19 00:00:00	83.44
10/20 00:00:00	83.78
10/21 00:00:00	89.67
10/24 00:00:00	83.66
10/25 00:00:00	83.95
10/26 00:00:00	84.12
10/27 00:00:00	82
10/28 00:00:00	81.58
10/29 00:00:00	81.78
10/30 00:00:00	85.25

vm-w23-rds28 / 10.128.28.62

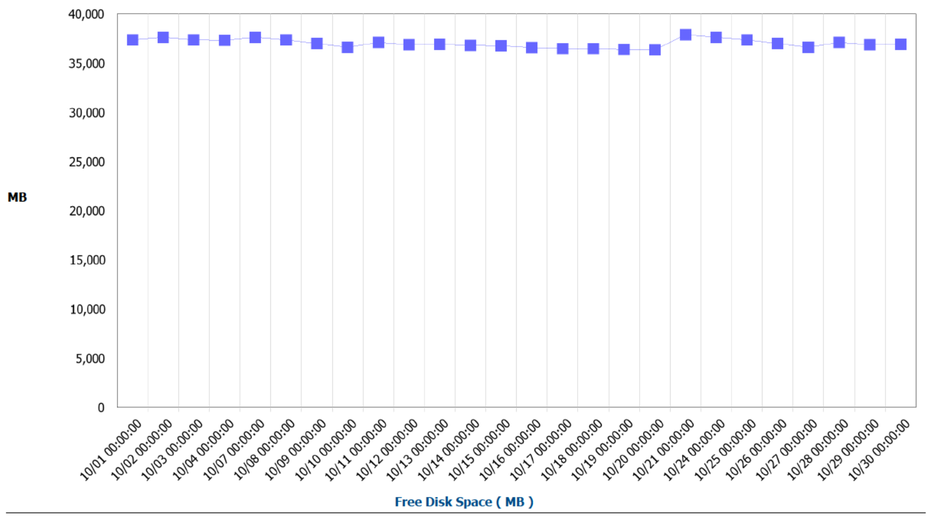


Daily	Value (%)
10/01 00:00:00	83.95
10/02 00:00:00	83.66
10/03 00:00:00	83.95
10/04 00:00:00	84.64
10/07 00:00:00	83.66
10/08 00:00:00	83.95
10/09 00:00:00	84.12
10/10 00:00:00	82
10/11 00:00:00	81.58
10/12 00:00:00	81.78
10/13 00:00:00	85.25
10/14 00:00:00	85.66
10/15 00:00:00	84.44
10/16 00:00:00	33.67
10/17 00:00:00	31.73
10/18 00:00:00	31.13
10/19 00:00:00	31.88
10/20 00:00:00	31.83
10/21 00:00:00	89.67
10/24 00:00:00	83.66
10/25 00:00:00	83.95
10/26 00:00:00	84.12
10/27 00:00:00	82
10/28 00:00:00	81.58
10/29 00:00:00	81.78
10/30 00:00:00	85.25

Aggregate Function: Min

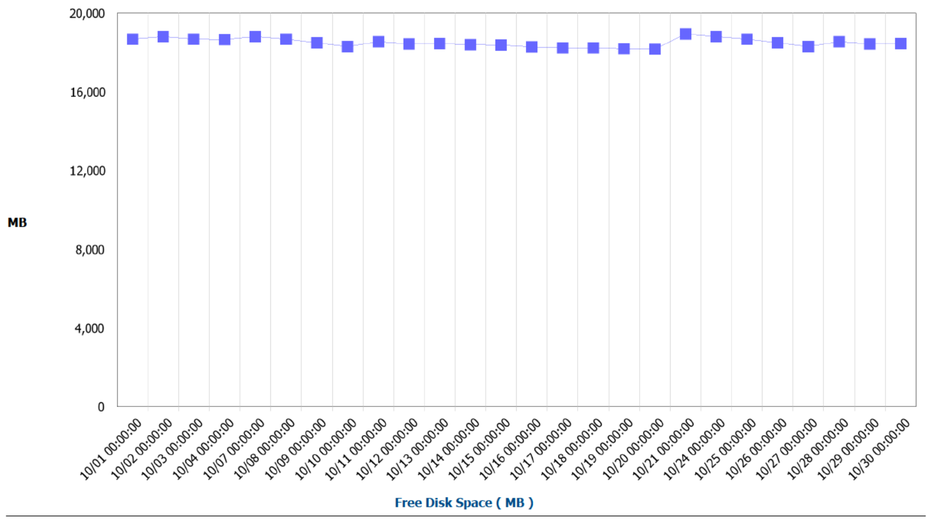
Report Period: 10-01-2012 00:00:00 to 10-30-2012 23:59:59 - IST

Server Disk Capacity



Daily	Value (MB)
10/01 00:00:00	37,326
10/02 00:00:00	37,590
10/03 00:00:00	37,326
10/04 00:00:00	37,294
10/07 00:00:00	37,590
10/08 00:00:00	37,326
10/09 00:00:00	36,974
10/10 00:00:00	36,596
10/11 00:00:00	37,084
10/12 00:00:00	36,858
10/13 00:00:00	36,890
10/14 00:00:00	36,788
10/15 00:00:00	36,728
10/16 00:00:00	36,564
10/17 00:00:00	36,438
10/18 00:00:00	36,430
10/19 00:00:00	36,352
10/20 00:00:00	36,330
10/21 00:00:00	37,858
10/24 00:00:00	37,590
10/25 00:00:00	37,326
10/26 00:00:00	36,974
10/27 00:00:00	36,596
10/28 00:00:00	37,084
10/29 00:00:00	36,858
10/30 00:00:00	36,890

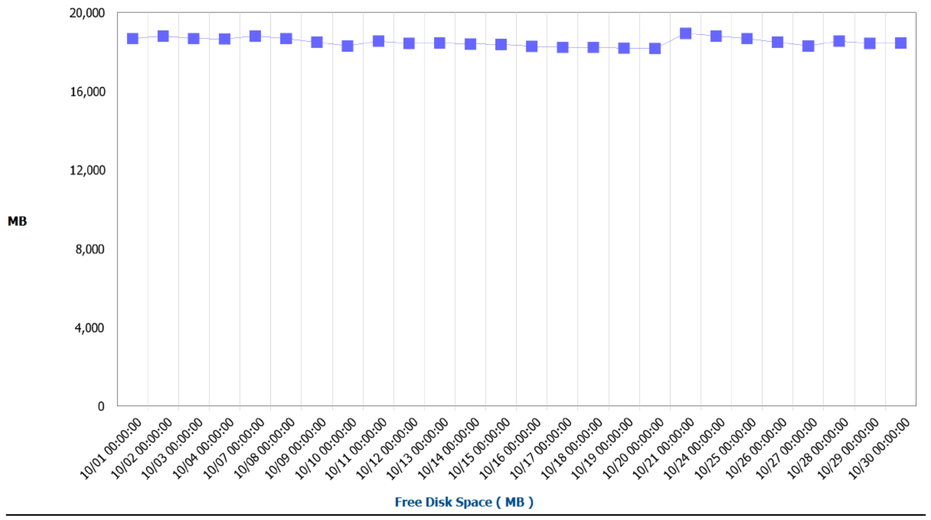
vm-w28-rds1627.pune-labs.bmc.com / Drive = C:\PROGRA~1\BMCSOF~1\PROACT~1, Target IP/Host Name = 10.128.32.94



Daily	Value (MB)
10/01 00:00:00	18,663
10/02 00:00:00	18,795
10/03 00:00:00	18,663
10/04 00:00:00	18,647
10/07 00:00:00	18,795
10/08 00:00:00	18,663
10/09 00:00:00	18,487
10/10 00:00:00	18,298
10/11 00:00:00	18,542
10/12 00:00:00	18,429
10/13 00:00:00	18,445
10/14 00:00:00	18,394
10/15 00:00:00	18,364
10/16 00:00:00	18,282
10/17 00:00:00	18,219
10/18 00:00:00	18,215
10/19 00:00:00	18,176
10/20 00:00:00	18,165
10/21 00:00:00	18,929
10/24 00:00:00	18,795
10/25 00:00:00	18,663
10/26 00:00:00	18,487
10/27 00:00:00	18,298
10/28 00:00:00	18,542
10/29 00:00:00	18,429
10/30 00:00:00	18,445

BPPM08.01 - Server Capacity - Drill down

vm-w28-rds1627.pune-labs.bmc.com / Drive = C:, Target IP/Host Name = 10.128.32.94



Daily	Value (MB)
10/01 00:00:00	18,663
10/02 00:00:00	18,795
10/03 00:00:00	18,663
10/04 00:00:00	18,647
10/07 00:00:00	18,795
10/08 00:00:00	18,663
10/09 00:00:00	18,487
10/10 00:00:00	18,298
10/11 00:00:00	18,542
10/12 00:00:00	18,429
10/13 00:00:00	18,445
10/14 00:00:00	18,394
10/15 00:00:00	18,364
10/16 00:00:00	18,282
10/17 00:00:00	18,219
10/18 00:00:00	18,215
10/19 00:00:00	18,176
10/20 00:00:00	18,165
10/21 00:00:00	18,929
10/24 00:00:00	18,795
10/25 00:00:00	18,663
10/26 00:00:00	18,487
10/27 00:00:00	18,298
10/28 00:00:00	18,542
10/29 00:00:00	18,429
10/30 00:00:00	18,445

BPPM08.01 - Server Capacity - Drill down

Aggregated Capacity Resource for Total CPU Utilization

Index	Monitor Name	Monitor Type	Min Value (%)	Avg Value (%)	Max Value (%)
1	vm-w23-rds28 10.128.28.62	Windows System	9.31	24.92	99.35
2	vm-w28-rds1627.pune-labs.bmc.com vm-w28-rds1627.pune-labs.bmc.com Windows System	Windows System	8.81	23.56	99.35

Aggregated Capacity Resource for Real Memory Used

Index	Monitor Name	Monitor Type	Min Value (%)	Avg Value (%)	Max Value (%)
1	vm-w23-rds28 10.128.28.62	Windows System	31.13	76.44	98.51
2	vm-w28-rds1627.pune-labs.bmc.com vm-w28-rds1627.pune-labs.bmc.com Windows System	Windows System	79.6	86.55	98.51

Aggregated Capacity Resource for Free Disk Space

Index	Monitor Name	Monitor Type	Min Value (MB)	Avg Value (MB)	Max Value (MB)
1	vm-w28-rds1627.pune-labs.bmc.com Drive = C:\PROGRA~1\BMCSOF~1 \PROACT~1, Target IP/Host Name = 10.128.32.94	Windows File System	18,165	18,572.32	18,931
2	vm-w28-rds1627.pune-labs.bmc.com Drive = C:, Target IP/Host Name = 10.128.32.94	Windows File System	18,165	18,572.32	18,931

This page intentionally left blank.

Attachment F-12 – Application Migration Plan

In this attachment Unisys includes a sample application migration plan.

This page intentionally left blank.

ID	Task Name	Duration	Start	Finish	Predecessors	Resource Names
1	**- Sample MOVE PACKAGE Schedule (to**	**129 days**	**Tue 7/1/14**	**Sun**		
2	Project Start Date	0 days	Tue 7/1/14	Tue 7/1/14		
3	**DCM_MP - PLAN MIGRATION**	**129 days**	**Tue 7/1/14**	**Sun 12/28/14**		
4	**Project Management Tasks**	**129 days**	**Tue 7/1/14**	**Sun 12/28/14**		
5	Goverance Plan	180 edays	Tue 7/1/14	Sun 12/28/14	2	
6	Risk Plan	180 edays	Tue 7/1/14	Sun 12/28/14	2	
7	Validate Data Gathering	180	Tue 7/1/14	Sun	2	
8	Configuration/Test Plan	180 edays	Tue 7/1/14	Sun 12/28/14	2	
9	**DCM_MP - MOVE**	**13 days**	**Tue 7/1/14**	**Thu 7/17/14**		
10	Schedule Individual Application	1 day	Tue 7/1/14	Tue 7/1/14		Customer
11	Conduct One-on-One	1 wk	Wed 7/9/14	Tue 7/15/14	10FS+1 wk	PM(s)[20%],PC(s)[2
12	Conduct Internal Planning	2 hrs	Wed	Wed	11	PM(s),PC(s),Custon
13	Identify In-Scope P2P, V2V,	4 hrs	Wed	Wed	12SS	Wintel
14	Validate Move Strategy & Initial	4 hrs	Wed	Wed	13SS	Facilities
15	Validate Out-of-Warranty	4 hrs	Wed	Wed	14	Asset Manager
16	Determine HA, backup and DR	4 hrs	Thu 7/17/14	Thu 7/17/14	15	
17	Refine MP Move Baseline (Unix	4 hrs	Thu 7/17/14	Thu 7/17/14	15	PM(s),Asset
18	**DCM_MP - CODE FREEZE**	**0.5 days**	**Thu 7/17/14**	**Thu 7/17/14**		
19	Initiate MP Server Baseline	0.5 hrs	Thu 7/17/14	Thu 7/17/14	17	Asset
20	Initiate MP Code Freeze for all	0.5 hrs	Thu 7/17/14	Thu 7/17/14	19SS	Customer App
21	Remove any remaining hard	4 hrs	Thu 7/17/14	Thu 7/17/14	20SS	Customer App
22	COMPLETED: DCM_MP -	0 days	Thu 7/17/14	Thu 7/17/14	19,21	PM(s)
23	COMPLETED: DCM_MP - MOVE	0 days	Thu 7/17/14	Thu 7/17/14	17,22	PM(s)
24	**DCM_MP - MOVE STRATEGY**	**1.5 days**	**Fri 7/18/14**	**Mon**		
25	Review Move Package Contents	1 day	Fri 7/18/14	Fri 7/18/14	23	PM(s),PC(s),Custon
26	Provide Move Package Contents	2 hrs	Mon	Mon	25	PM(s)[50%],PC(s)[5
27	Receive Move Package Content	2 hrs	Mon	Mon	26	PM(s),PC(s),Custon
28	COMPLETED: MP - MOVE	0 days	Mon	Mon	27	PM(s)
29	**DCM_MP - DUE DILIGENCE**	**1.63 days**	**Mon**	**Wed**		
30	Schedule, Prepare, Perform MP	1 hr	Mon	Mon	28	PM(s),PC(s),Custon
31	Establish Weekly Meetings with	1.5 days	Mon	Wed	30	Unix Team,Wintel
32	Schedule WAN Analysis	0.06 days	Mon	Mon	30	PM(s)
33	Check if WAN Analysis is	0.5 days	Mon	Tue 7/22/14	32	PC(s)[50%],PM(s)[5
34	COMPLETED: DCM_MP - DUE	0 days	Wed	Wed	31,32,33	Core Networks

ID	Task Name	Duration	Start	Finish	Predecessors	Resource Names
35	**DCM_MP - CREATE WORKBOOK**	**18 days**	**Mon 7/21/14**	**Thu 8/14/14**		
36	Initiate Workbook for Move	1 wk	Mon 7/21/14	Mon 7/28/14	28	PM(s)[50%]
37	Assess MP in-flight projects,	1 day	Mon	Tue 7/29/14	36	PM(s)[25%]
38	**DCM_MP - DEVELOP RISK**	**4 days**	**Mon**	**Fri 8/1/14**		
39	**MP_RISK - RISK MITIGATION**	**1 day**	**Mon 7/28/14**	**Tue 7/29/14**		
40	Review Standard Move	0.5 days	Mon	Mon	36	PM(s)[25%],PC(s)[2
41	Document Move Package	0.5 days	Tue 7/29/14	Tue 7/29/14	40	PM(s)[25%],PC(s)[2
42	**MP_RISK - CONTINGENCY**	**4 days**	**Mon**	**Fri 8/1/14**		
43	Identify / Review	1 day	Mon	Tue 7/29/14	40SS	PM(s)[25%],PC(s)[2
44	Review Options for	1 day	Tue 7/29/14	Wed	43	PM(s)[25%],PC(s)[2
45	Review Options with to	1 day	Wed	Thu 7/31/14	44	PM(s)[25%],PC(s)[2
46	Finalize Contingency Plan	1 day	Thu 7/31/14	Fri 8/1/14	45	PM(s)[25%],PC(s)[2
47	COMPLETED: MP_RISK -	0 days	Fri 8/1/14	Fri 8/1/14	46	PM(s)
48	COMPLETED: DCM_MP_PM -	0 days	Fri 8/1/14	Fri 8/1/14	41,47	PC(s)
49	**MP_APPS - DEVELOP TEST**	**13 days**	**Mon**	**Thu 8/14/14**		
50	Review Initial Test Plan	4 hrs	Mon	Mon	36,64	PM(s)[25%],PC(s)[2
51	Identify Applications to be	16 hrs	Tue 7/29/14	Wed	50	PM(s)[25%]
52	Identify Application Testers	16 hrs	Thu 7/31/14	Fri 8/1/14	51	PM(s)[50%]
53	Commit to Re-IP Planned	8 hrs	Mon 8/4/14	Mon 8/4/14	52	Service Delivery
54	Work with Application Test	8 hrs	Tue 7/29/14	Tue 7/29/14	50	Service Delivery
55	Develop the High Level Test	16 hrs	Wed	Thu 7/31/14	54	Customer App
56	Create Test Cases / Scripts	5 days	Mon 8/4/14	Fri 8/8/14	52,55	PM(s)[60%]
57	Finalize Test Plan	8 hrs	Mon	Mon	56	Customer App
58	Execute Dry Run of Test Cases	8 hrs	Tue 8/12/14	Tue 8/12/14	57	Service Delivery
59	Establish Success Criteria	4 hrs	Wed	Wed	58	PM(s)[50%],Custor
60	Receive Written Approval of	1 day	Wed	Thu 8/14/14	57,58,59	Customer App
61	COMPLETED: MP_APPS -	0 days	Thu 8/14/14	Thu 8/14/14	53,60	Customer App
62	**DCM_MP - SITE PREPARATION**	**12.13**	**Wed**	**Fri 8/8/14**		
63	**DCM_MP_SP - SERVER IP**	**7.25 days**	**Wed**	**Fri 8/1/14**		
64	Gather MP IP requirements	1 day	Wed	Thu 7/24/14	34	Customer App
65	Prepare and Submit MP IP	4 hrs	Thu 7/24/14	Thu 7/24/14	64	PM(s)[20%],Custor
66	Receive MP IP Addresses	2 hrs	Mon	Mon	65FS+2 days	PM(s)[20%],Core
67	Identify MP DNS Entries	12 hrs	Mon	Wed	66	Customer App
68	Acquire any required	2 days	Wed	Fri 8/1/14	67	DBA[50%],Unix

ID	Task Name	Duration	Start	Finish	Predecessors	Resource Names
69	Plan MP Resolution for	4 hrs	Mon	Tue 7/29/14	66	Firewall Engineer
70	Receive MP Status Update	8 hrs	Tue 7/29/14	Wed	69	Storage Team
71	MP Hardcoded IP Address	16 hrs	Wed	Fri 8/1/14	70	Unix Team
72	COMPLETED: DCM_MP_SP	0 days	Fri 8/1/14	Fri 8/1/14	67,68,71	Wintel Team
73	**DCM_MP_SP - FIREWALL**	**10 days**	**Wed**	**Wed 8/6/14**		
74	Determine MP Firewall	1 day	Wed	Thu 7/24/14	64SS	Customer App
75	Identify MP Domain	4 hrs	Wed	Wed	74SS	DBA[50%],Unix
76	Conduct MP Peer Review of	4 hrs	Thu 7/24/14	Thu 7/24/14	74,75	Firewall
77	Submit MP Load Balancer	4 hrs	Thu 7/24/14	Fri 7/25/14	76	Unix
78	Fill MP Load Balancer RM	3 days	Fri 8/1/14	Wed 8/6/14	77FS+5 days	Customer App
79	COMPLETED: DCM_MP_SP	0 days	Wed 8/6/14	Wed 8/6/14	76,78	DBA[50%],Unix
80	**DCM_MP_SP - WINTEL**	**4.38 days**	**Mon**	**Mon 8/4/14**		
81	Validate/Update MP	4 hrs	Mon	Tue 7/29/14	66	Firewall Engineer
82	Validate MP Intel server	2 hrs	Tue 7/29/14	Tue 7/29/14	81	Storage
83	Determine MP Intel Backup	4 hrs	Tue 7/29/14	Tue 7/29/14	81	Storage SME
84	Prepare and Submit MP	8 hrs	Tue 7/29/14	Wed	83SS	Storage SME
85	MP Intel Grid Space	3 hrs	Thu 7/31/14	Thu 7/31/14	84FS+1 day	PM(s)
86	Submit MP RM for Intel	4 hrs	Thu 7/31/14	Fri 8/1/14	85	Customer App
87	Create MP Rack Diagrams	12 hrs	Thu 7/31/14	Mon 8/4/14	85	Customer App
88	Submit MP RM to get PTC	4 hrs	Thu 7/31/14	Fri 8/1/14	85	Customer App
89	Determine MP Phone line	4 hrs	Fri 8/1/14	Fri 8/1/14	88	Customer App
90	Submit MP Intel SAN/NAS	4 hrs	Fri 8/1/14	Fri 8/1/14	88	Firewall Engineer
91	Submit MP Power	4 hrs	Fri 8/1/14	Fri 8/1/14	86,88	Core Networks
92	COMPLETED: DCM_MP_SP	0 days	Mon 8/4/14	Mon 8/4/14	82,85,87,89,90,	Core
93	**DCM_MP_SP - UNIX SERVICE**	**3.75 days**	**Mon**	**Fri 8/1/14**		
94	Validate/Update MP	1 hr	Mon	Mon	66	Firewall Engineer
95	Validate MP Unix server	0.67 hrs	Tue 7/29/14	Tue 7/29/14	94	Firewall
96	Determine MP Unix Backup	2 hrs	Tue 7/29/14	Tue 7/29/14	95SS	Core
97	Prepare and Submit MP	6 hrs	Tue 7/29/14	Tue 7/29/14	96SS	Core Networks
98	MP Unix Grid Space	3 hrs	Wed	Thu 7/31/14	97FS+1 day	Firewall Engineer
99	Submit MP RM for Unix	2 hrs	Thu 7/31/14	Thu 7/31/14	98	Core Networks
100	Submit MP RM to get	2 hrs	Thu 7/31/14	Thu 7/31/14	99SS	Wintel Team
101	Create MP Visio Rack	4 hrs	Thu 7/31/14	Thu 7/31/14	100SS	Wintel Team
102	Submit MP RM to get Unix	1 hr	Thu 7/31/14	Thu 7/31/14	101SS	Intel Team

ID	Task Name	Duration	Start	Finish	Predecessors	Resource Names
103	Determine MP Phone line	1 hr	Thu 7/31/14	Thu 7/31/14	102	Asset Manager
104	Submit: MP SAN/NAS	1 hr	Thu 7/31/14	Thu 7/31/14	103SS	Wintel Team
105	Submit MP Cable Test	1 hr	Thu 7/31/14	Thu 7/31/14	104SS	Storage Team
106	Submit MP Unix Monitoring	1 hr	Thu 7/31/14	Thu 7/31/14	105SS	Wintel Team
107	Submit MP Power	1 hr	Thu 7/31/14	Thu 7/31/14	99,102	Wintel Team
108	Submit MP Power Test	1 hr	Thu 7/31/14	Thu 7/31/14	99,102	Wintel Team
109	Submit MP Port Test	1 hr	Thu 7/31/14	Thu 7/31/14	102	Wintel Team
110	Submit MP Premount	1 hr	Thu 7/31/14	Thu 7/31/14	102	Wintel Team
111	Submit MP Route Cables in	1 hr	Thu 7/31/14	Thu 7/31/14	102	Wintel Team
112	Order Additional MP NIC	1 hr	Thu 7/31/14	Thu 7/31/14	102	Wintel Team
113	Arrange for OEM SOW for	2 hrs	Mon	Tue 7/29/14	94SS	Wintel Team
114	Produce and Send OEM MP	2 days	Tue 7/29/14	Thu 7/31/14	113	Wintel Team
115	Receive, Approve and	1 day	Thu 7/31/14	Fri 8/1/14	114	Storage
116	Confirm OEM MP SOW	4 hrs	Fri 8/1/14	Fri 8/1/14	115	Unix Team
117	COMPLETED: DCM_MP	0 days	Fri 8/1/14	Fri 8/1/14	95,100,101,103	Unix Team
118	DCM_MP_SP - Confirm SAN	1 day	Wed 8/6/14	Thu 8/7/14	72,79,92,117	Asset Manager
119	**MP_APPS - FIREWALL**	**2.13 days**	**Wed 8/6/14**	**Fri 8/8/14**		
120	Create & Submit	1 day	Wed 8/6/14	Thu 8/7/14	76SS,79SS	Unix Team
121	InfoSec Review of	2 hrs	Thu 8/7/14	Thu 8/7/14	120	Storage Team
122	InfoSec Releases InfoSec	4 hrs	Thu 8/7/14	Thu 8/7/14	121	Unix Team
123	Firewall Team	1 hr	Thu 8/7/14	Thu 8/7/14	122	Unix Team
124	Firewall Team Stages and	2 hrs	Fri 8/8/14	Fri 8/8/14	123	Unix Team
125	COMPLETED: MP_APPS -	0 days	Fri 8/8/14	Fri 8/8/14	124	Unix Team
126	COMPLETED: DCM_MP_SP -	0 days	Fri 8/8/14	Fri 8/8/14	72,79,92,118,1	Unix Team
127	COMPLETED: DCM_MP - CREATE	0 days	Thu 8/14/14	Thu 8/14/14	37,48,61,126	Unix Team
128	COMPLETED: DCM_MP - PLAN	0 days	Thu 8/14/14	Thu 8/14/14	28,34,127	Unix Team
129	**DCM_MP - MIGRATION TO DC1**	**47.75**	**Mon**	**Thu 10/2/14**		
130	**DCM_MP - REVIEW AUDITS AND**	**47.75**	**Mon**	**Thu 10/2/14**		
131	**Pre-Re-IP Notifications**	**20.5 days**	**Mon 7/28/14**	**Mon 8/25/14**		
132	Prepare & Send 30 Day	4 hrs	Mon	Mon	171SS-30	Unix Team
133	Prepare & Send 7 Day	0.5 days	Mon	Mon	132,171SS-10	Unix Team
134	Prepare & Send 2 Day	4 hrs	Mon	Mon	133,171SS-2	Unix Team
135	**Pre-DCM Notifications**	**26.88**	**Tue 8/26/14**	**Thu 10/2/14**		
136	Prepare & Send 30 Day	4 hrs	Tue 8/26/14	Tue 8/26/14	223SS-30	Unix Team

ID	Task Name	Duration	Start	Finish	Predecessors	Resource Names
137	Prepare & Send 7 Day	4 hrs	Thu 9/11/14	Thu 9/11/14	223SS-14	Unix Team
138	Prepare & Send 2 Day	4 hrs	Tue 9/23/14	Tue 9/23/14	223SS-2 edays	Unix Team
139	Completion Notification (3	2 hrs	Thu 10/2/14	Thu 10/2/14	223FS+3 days	Unix Team
140	COMPLETED: DCM_MP REVIEW	0 days	Thu 10/2/14	Thu 10/2/14	132,134,136,13	Unix Team
141	**DCM_MP - Re-IP/Mock Move**	**12 days**	**Wed**	**Thu 8/28/14**		
142	**DCM_MP_Re-IP - EXECUTION**	**11.5 days**	**Wed 8/13/14**	**Thu 8/28/14**		
143	**MP_Re-IP - PREPARE**	**5.25 days**	**Wed**	**Wed**		
144	Confirm Application Test	2 hrs	Wed	Wed	58	Unix Team
145	Check if WAN Analysis is	4 hrs	Wed	Wed	144	PC(s)[25%],OEM[2
146	Create Resource Plan for	4 hrs	Fri 8/15/14	Mon	145FS+2 days	OEM,Transition /
147	Develop/Distribute Re-IP	2 days	Mon	Wed	34,144FF,146	PC(s)
148	**Submit CRQ Numbers to**	**0.13 days**	**Mon**	**Mon**		
149	x86	0.13 days	Mon 8/18/14	Mon 8/18/14	147SS	Unix SA
150	Unix	0.13 days	Mon 8/18/14	Mon 8/18/14	147SS	Storage Team
151	Interfaces	0.13 days	Mon 8/18/14	Mon 8/18/14	147SS	Firewall Engineer
152	Network	0.13 days	Mon 8/18/14	Mon 8/18/14	147SS	Firewall Engineer
153	Perimeter	0.13 days	Mon 8/18/14	Mon 8/18/14	147SS	Firewall Engineer
154	Databases	0.13 days	Mon 8/18/14	Mon 8/18/14	147SS	Firewall Engineer
155	Storage	0.13 days	Mon 8/18/14	Mon 8/18/14	147SS	Firewall Engineer
156	COMPLETE: Submit CRQ	0 days	Mon	Mon	149,150,151,15	PM(s)
157	Confirm All Servers are	4 hrs	Mon	Mon	147SS	PM(s)
158	Arrange Sites Access	4 hrs	Mon	Tue 8/19/14	157	PM(s)[25%]
159	Submit Re-IP Master	4 hrs	Tue 8/19/14	Tue 8/19/14	158	PM(s)[50%]
160	COMPLETED: MP_Re-IP -	0 days	Wed	Wed	144,145,146,14	PM(s)
161	**MP_Re-IP - GO/NO-GO**	**5.25 days**	**Wed**	**Wed**		
162	Finalize the Re-IP Hr-By-Hr	4 hrs	Wed	Wed	147,156	PM(s)
163	Finalize and Distribute the	4 hrs	Wed	Thu 8/21/14	162	PM(s)
164	Review Re-IP Package Risks	4 hrs	Thu 8/21/14	Thu 8/21/14	162,163	PM(s)[25%]
165	Validate and Approve Re-IP	4 hrs	Thu 8/21/14	Fri 8/22/14	164	PM(s)[25%]
166	Submit finalized Re-IP list to	2 hrs	Fri 8/22/14	Fri 8/22/14	165	PM(s)
167	Conduct Re-IP Informal	1 hr	Fri 8/22/14	Fri 8/22/14	160,165	PM(s)
168	Conduct Re-IP Formal	1 hr	Wed	Wed	167FS+3 days	PM(s)
169	COMPLETED: MP_Re-IP -	0 days	Wed	Wed	166,167,168	Customer App
170	**MP_Re-IP - EXECUTE Re-IP**	**1 day**	**Wed**	**Thu 8/28/14**		

ID	Task Name	Duration	Start	Finish	Predecessors	Resource Names
171	Execute Re-IP Activities	1 eday	Wed	Thu 8/28/14	162,169	Core
172	Conduct Re-IP Application	4 hrs	Thu 8/28/14	Thu 8/28/14	171FF	PM(s)[50%],PC(s)[5
173	Receive Written Validation	2 hrs	Thu 8/28/14	Thu 8/28/14	171FF	Customer App
174	COMPLETED: MP_Re-IP -	0 days	Thu 8/28/14	Thu 8/28/14	172,173	Core Networks
175	COMPLETED: DCM_MP_Re-IP	0 days	Thu 8/28/14	Thu 8/28/14	160,169,174	DBA
176	**DCM_MP_Re-IP - POST RE-IP**	**2.25 days**	**Tue 8/26/14**	**Thu 8/28/14**		
177	Update/Verify new IP	4 hrs	Thu 8/28/14	Thu 8/28/14	175	Unix
178	Commit to Move Package	2 hrs	Thu 8/28/14	Thu 8/28/14	177SS	Storage Team
179	Make Initial Move Logistics	2 hrs	Thu 8/28/14	Thu 8/28/14	178SS	Unix Team
180	Install any required data	2 hrs	Thu 8/28/14	Thu 8/28/14	179	Wintel Team
181	Develop/Distribute Move	7 hrs	Tue 8/26/14	Wed	162FS+4 days	PM(s)
182	**Submit CRQ Numbers to PM**	**0.13 days**	**Tue 8/26/14**	**Tue 8/26/14**		
183	x86	0.13 days	Tue 8/26/14	Tue 8/26/14	181SS	Wintel Team
184	Unix	0.13 days	Tue 8/26/14	Tue 8/26/14	181SS	Unix SA
185	Interfaces	0.13 days	Tue 8/26/14	Tue 8/26/14	181SS	Interface Team
186	Network	0.13 days	Tue 8/26/14	Tue 8/26/14	181SS	Core Networks
187	Perimeter	0.13 days	Tue 8/26/14	Tue 8/26/14	181SS	Firewall Engineer
188	Databases	0.13 days	Tue 8/26/14	Tue 8/26/14	181SS	DBA
189	Storage	0.13 days	Tue 8/26/14	Tue 8/26/14	181SS	Storage Team
190	COMPLETE: Submit CRQ	0 days	Tue 8/26/14	Tue 8/26/14	183,184,185,18	PM(s)
191	Reserve War Room	2 hrs	Thu 8/28/14	Thu 8/28/14	175	PM(s)
192	Arrange Site Access for Move	2 hrs	Thu 8/28/14	Thu 8/28/14	175	PC(s)
193	COMPLETED: DCM_MP_Re-IP	0 days	Thu 8/28/14	Thu 8/28/14	177,179,180,18	SMEs
194	COMPLETED: DCM_MP - Re-IP	0 days	Thu 8/28/14	Thu 8/28/14	175,193	Core Networks
195	**DCM_MP - MOVE PACKAGE**	**21.25**	**Tue 9/2/14**	**Thu 10/2/14**		
196	**DCM_MP_MOVE - PERFORM**	**12 days**	**Tue 9/2/14**	**Thu 9/18/14**		
197	Submit Final Logistics Request	0 days	Tue 9/2/14	Tue 9/2/14	28FS+2	DBA
198	Request ISSA Approval to ship	0.5 hrs	Wed 9/3/14	Wed 9/3/14	197	Unix SA
199	Provide Logisitics Quote &	1 day	Wed 9/3/14	Wed 9/3/14	197	Firewall Engineer
200	Receive Approved Logistics	1 day	Thu 9/4/14	Thu 9/4/14	199	Storage Team
201	Initiate Logistics Plan &	10 days	Fri 9/5/14	Thu 9/18/14	200	Unix Team[10%]
202	Confirm DC Physical Security	2 hrs	Fri 9/5/14	Fri 9/5/14	200	Wintel Team
203	Confirm security access	2 hrs	Fri 9/5/14	Fri 9/5/14	202	PM(s)
204	Submit Change Request for	1 hr	Fri 9/5/14	Fri 9/5/14	203	Transition /

ID	Task Name	Duration	Start	Finish	Predecessors	Resource Names
205	AC-Verify CCPM contains	4 hrs	Wed 9/3/14	Wed 9/3/14	197	
206	AC-Validate Monitoring is in	1 hr	Wed 9/3/14	Wed 9/3/14	197	
207	AC-Confirm SLAs are in place	0.13 days	Wed 9/3/14	Wed 9/3/14	197	
208	AC-Confirm ITSM ready to	0.13 days	Wed 9/3/14	Wed 9/3/14	197	
209	AC-Verify DR plans and test	0.13 days	Wed 9/3/14	Wed 9/3/14	197	
210	COMPLETED:	0 days	Thu 9/18/14	Thu 9/18/14	198,201,204	PM(s)
211	**DCM_MP_MOVE - GO/NO-GO**	**4.38 days**	**Fri 9/19/14**	**Thu 9/25/14**		
212	Finalize the Move Hr-By-Hr	2 hrs	Fri 9/19/14	Fri 9/19/14	181,190,210	PC(s)
213	Prepare for Move GO/NO-GO	2 hrs	Fri 9/19/14	Fri 9/19/14	212	PM(s)
214	Review Final Move Package	1 hr	Fri 9/19/14	Fri 9/19/14	41,213	PM(s)
215	Validate and Approve Move	1 hr	Fri 9/19/14	Fri 9/19/14	214	PM(s)
216	Submit Supplemental CMDB	1 hr	Fri 9/19/14	Fri 9/19/14	215	PM(s)
217	Final Receiving Site(s)	2 hrs	Fri 9/19/14	Mon	216	PM(s)[50%]
218	Conduct Internal Move	1 hr	Mon	Mon	212,217	PM(s)
219	Conduct Formal Move	1 hr	Thu 9/25/14	Thu 9/25/14	218FS+3 days	PM(s),Customer
220	COMPLETED:	0 days	Thu 9/25/14	Thu 9/25/14	128,213,214,21	Wintel Team
221	**DCM_MP_MOVE - EXECUTE**	**3.63 days**	**Thu 9/25/14**	**Tue 9/30/14**		
222	Relocate Equipment (Forklift)	30 ehrs	Thu 9/25/14	Fri 9/26/14	212,220	PC(s)
223	Migration Activities (See	2 edays	Thu 9/25/14	Sat 9/27/14	222SS	Core
224	Conduct Move Application	1 eday	Sat 9/27/14	Sun 9/28/14	223	PM(s)[25%]
225	Final Conf Call and Verbal	1 ehr	Sun 9/28/14	Sun 9/28/14	224	PM(s)
226	AC-Provide MP Completion	2 ehrs	Sun 9/28/14	Sun 9/28/14	225	Intel Team
227	AC-Received Approved MP	2 days	Mon	Tue 9/30/14	225,226	Wintel Team[23%]
228	COMPLETED:	0 days	Tue 9/30/14	Tue 9/30/14	227	PM(s)
229	**DCM_MP_POST-MOVE LESSONS**	**1.25 days**	**Wed**	**Thu 10/2/14**		
230	MP_Post- Move Lessons	1 hr	Wed	Wed	223FS+2 days	PC(s)
231	MP_Post- Move Lessons	1 hr	Thu 10/2/14	Thu 10/2/14	230FS+1 day	PC(s),PM(s),Wintel
232	COMPLETED:	0 days	Thu 10/2/14	Thu 10/2/14	231	Storage Team
233	COMPLETED: DCM_MP - MOVE	0 days	Thu 10/2/14	Thu 10/2/14	140,210,220,22	PM(s)

This page intentionally left blank.

Request for Proposal

RFP # 6100022698

Commonwealth of Pennsylvania

Office of Administration

Office for Information Technology

Data Center Computing Services

Schedule H

Commonwealth Computing Procedures Manual (CCPM)

Contents

1 PURPOSE 3
1.1 Organizational Overview 3
1.2 Transition and Support Activities and Responsibilities 4
1.3 IT Service Management Procedures 5
1.4 Financial Management Procedures 12
1.5 Contract Management Procedures 14
1.6 Relationship Management Procedures 16
1.7 Offeror Operational Procedures 17
1.8 The Commonwealth Customer Operations Manuals 18

Content	Description
1 PURPOSE	The Offeror should describe the purpose of the Commonwealth Computing Procedures Manual. This section should address who should use the Manual, how the Manual is organized, how the initial version and updates will be distributed, version control procedures for the Manual, when updates will occur, and procedures for authorizing and implementing updates. It is intended that the structure of the Manual will require that the individual compliance requirements and business rules of each participating Commonwealth Customer are separately identified where applicable for each section or component part of the Manual.
1.1 Organizational Overview	
1. Offeror Governance Organization	Include organization charts, description of functions performed, contact information.
2. Offeror Management and Delivery Organization	Include organization charts, description of functions performed, contact information.
3. Key Contacts - Offeror	A list of contacts that are key users of the Services and/or perform a liaison function in regard to the Services (by Commonwealth and Commonwealth Agencies, by location).

Content	Description
4. Key Contacts – Third Parties	A list of key Third Parties (maintenance providers, software providers, telecom carriers, etc).
1.2 Transition and Support Activities and Responsibilities	
1. Overall Management and Reporting Process	A description of Offeror management structure, reporting, and review process associated with Transition Services and Transformation Services.
2. Critical Deliverables and Milestones	A list of Critical Deliverables, milestones and timeline for the Transition Services and Transformation Services periods.
3. Interim Performance Management Procedures	A description of interim procedures to monitor and coordinate Service delivery, including Problem Management, Change Management, Service Level monitoring and reporting, physical and Logical Security, project management, work authorization, etc. A description of the responsibilities of both Parties.

Content	Description
4. Interim Financial Management Procedures	A description of interim procedures for invoicing, invoice verification, charge back to the Commonwealth Customers, determining Resource Unit volume by Service Component, asset management, asset transfers, forecasting, Commonwealth Customer support, etc. A description of the responsibilities of both Parties.
5. Interim Contract Management Procedures	A description of interim procedures for managing and administering the Agreement including proposed changes to the Agreement, interpretation procedures, issue-escalation process, and disputes. A description of the responsibilities of both Parties.
6. Other Transition and Support Procedures and Responsibilities	Any other pertinent procedures and responsibilities.
1.3 IT Service Management Procedures	
1. Service Desk	The facilities, associated technologies, and fully trained staff who respond to Calls, coordinate all Incident Management, Problem Management and Request Management activities, and act as a single point of contact for Authorized Users in regard to the Services.

Content	Description
2. Incident Management	The use of people, processes and technology with the primary goal to restore normal Service operations as quickly as possible and minimize the adverse impact on business operations, thus ensuring that the best achievable levels of service quality and availability are maintained.
3. Problem Management	The process, software, techniques and procedures that aid in identification, tracking, communication, and resolution of Problems arising in Customer's IT Environment, and resolving those Problems arising from or related to the Services. The goal of Problem Management is to minimize the adverse impact of Incidents and Problems on the business that are caused by errors within the IT infrastructure, and to prevent recurrence of Incidents related to these errors. In order to achieve this goal, Problem Management seeks to get to the root cause of Incidents and then initiate actions to improve or correct the situation.
4. Change Management	The processes relating to planning and performing all changes in IT environment pertaining to the Services, including changes to individual components and coordination of changes across all components. The Change Management processes will support and include checkpoints to determine any potential or required Change Control Procedures and includes a process of controlling changes to the infrastructure or any aspect of Services, in a controlled manner, enabling approved changes with minimum disruption.

<table>
<tr><th>Content</th><th>Description</th></tr>
<tr><td>5. Configuration Management</td><td>The process of identifying and defining CIs in a system, recording and reporting the status of CIs and RFCs, and verifying the completeness and correctness of the CIs.

The following data fields are required as a minimum for Asset/Configuration Management (any number of these may require that auditing be enabled.):
<table>
<tr><th>Physical Attributes</th><th>Logical Attributes</th></tr>
<tr><td>CI Name</td><td>System Role</td></tr>
<tr><td>Serial Number</td><td>Primary Capability</td></tr>
<tr><td>Commonwealth Asset Tag</td><td>Capability</td></tr>
<tr><td>Owner</td><td>Complexity</td></tr>
<tr><td>Ownership Type</td><td>Priority</td></tr>
<tr><td>Funding Source</td><td>Storage (currently TPC tool)</td></tr>
<tr><td>Purchase Date</td><td>24 x 7 Access</td></tr>
</table></td></tr>
</table>

Content	Description	
	Life Cycle Dates	**OS Billing Platform**
	Status	**Operating System (OS)**
	Physical Location	**OS Version**
	Region	**OS Manufacturer**
	Product Name	**Last Scan Date**
	CI Type	**Audit Report**
	Model/Version	**Relationships**
	Manufacturer	**Applications**
	Supplier Name	**Application SW Info**
	Tier	**Disaster Recovery Priority**
	Asset Classification	**Customer Project Identification**

Content	Description	
		Drivers and Version Numbers
	Date of Last Inventory	**Service Pack**
		Network Protocol
		Assigned IP Address(s)
		DNS Host Name
		Domain
		Physical or Virtual Identifier
		Funding Source
		Memory allocated
		Installation date **Related CIs**

Content	Description
6. Release Management	The process responsible for planning, scheduling and controlling the movement of Releases to Test and Live Environments. The primary objective of Release Management is to ensure that the integrity of the Live Environment is protected and that the correct Components are released. Release Management works closely with Configuration Management and Change Management.
7. Request Management and Fulfillment	The process responsible for managing the lifecycle of all Service Requests.
8. Availability Management	The process responsible for defining, analyzing, Planning, measuring and improving all aspects of the Availability of IT services. Availability Management is responsible for ensuring that all IT Infrastructure, Processes, tools, roles etc. are appropriate for the agreed Service Level targets for Availability.
9. Capacity Management	The process responsible for ensuring that the Capacity of IT Services and the IT Infrastructure are able to deliver agreed Service Level targets in a cost effective and timely manner. Capacity Management considers all Resources required to deliver the IT Service, and plans for short, medium and long term business requirements.

Content	Description
10. Service Level Management (SLM)	The process responsible for negotiating SLAs, and ensuring that these are met. SLM is responsible for ensuring that all IT Service Management Processes, OLAs, and Underpinning Contracts, are appropriate for the agreed Service Level targets. SLM monitors and reports on Service Levels, facilitates Service Delivery Failure actions with the appropriate Governance Committee and holds regular Commonwealth Customer reviews.
11. IT Service Continuity Management (ITSCM)	The process responsible for managing risks that could seriously impact IT Services. ITSCM ensures that the IT Offeror can Always provide minimum agreed Service Levels, by reducing the risk to an acceptable level and Planning for the recovery of IT Services. ITSCM should be designed to support Business Continuity Management.
12. IT Financial Management	The process responsible for managing the Budgeting, Accounting, Invoicing and Chargeback requirements).
13. Information Security Management	The process that ensures the confidentiality, integrity and Availability of an organization's Assets, information, data and IT Services. Information Security Management usually has a wider scope than the Offeror. It normally includes handling of paper, building access, phone calls etc., for the entire organization.

Content	Description
14. Project Management and Support	Project Management and Support will align projects to Commonwealth requirements and deliver projects from request through end-to-end solutioning including turnover to the Commonwealth Customers and validation that project requirements were met in terms of timing, quality, and cost.
15. Service Catalog	A database or structured Document with information about select Services, including those available for Deployment. The Service Catalog is the only part of the Service portfolio published to Commonwealth Customers, and is used to support the request and delivery of select Services. The Service Catalog may include information about Deliverables, prices, contact points, ordering and request processes.
1.4 Financial Management Procedures	
1. Invoicing	The Offeror should describe procedures for invoicing. The content should include procedures for calculating Resource Unit volumes for pricing (per Service Component, as applicable), invoicing of Projects, etc. The content should include procedures regarding disputed invoice amounts.

Content	Description
2. Chargeback	The Offeror should describe procedures for charge back of costs related to the Services and the overall Agreement to the Commonwealth Customers (to include responsibilities and support by both the Offeror and the Commonwealth).
3. Budgeting	The Offeror should describe how it would assist the Commonwealth with the annual budgeting cycle. Process should include estimation of Resource Unit volumes (by Service Component and Commonwealth Customer as appropriate), potential Projects, review cycle, etc. The content should include the responsibilities of Offeror, the Commonwealth, and Commonwealth Agencies.
4. Forecasting	The Offeror should describe procedures for forecasting cost versus budget.
5. Procurement	The Offeror should describe procedures for procurement Services (where Offeror performs procurement on behalf of the Commonwealth, as applicable). The content should include responsibilities and process for both the Commonwealth staff and Offeror.

Content	Description
6. Service Level Credits and Earnback	The Offeror should describe procedures for calculating Service Level Credits on invoices and Earnback calculations.
1.5 Contract Management Procedures	
1. Contract Change Control	The Offeror should describe procedures regarding changes to the Agreement, including changes to any Exhibit or Attachment. Content should include procedures to classify services as a New Service, and resulting process to change the Agreement (including pricing). Content should include notification period and process, authority levels, and escalation procedures for changes to the Agreement.
2. Reporting	The Offeror should describe procedures and activities regarding key standard Reports and requests for ad hoc reports from the Commonwealth and The Commonwealth Agencies.
3. New Service Levels	The Offeror should describe procedures for determining new Service Levels (based on continuous improvement and/or Commonwealth request).

Content	Description
4. Benchmarking	The Offeror should describe procedures for Benchmarking exercises, including determination and agreement of benchmark firm, sample peer group and process used for benchmark, payment for benchmark, review of results, and potential outcome. Content should include dispute resolution process.
5. Auditing	The Offeror should describe procedures for operational and/or financial audits (as required by the Commonwealth auditing and/or regulatory agencies). The Offeror should describe notification process and procedures to resolve audit findings.
6. Offeror Key Personnel and Subcontractors	The Offeror should describe procedures for Commonwealth approval regarding replacement or removal of Offeror Key Personnel and major Subcontractors to Offeror.
7. Dispute Resolution	The Offeror should describe procedures regarding formal dispute resolution process.

Content	Description
1.6 Relationship Management Procedures	
1. Customer Satisfaction Surveys	The Offeror should describe the process to be used for conducting customer satisfaction surveys. Content should include procedures regarding action items and attempts to resolve customer issues.
2. Commonwealth Agencies	The Offeror should describe procedures and responsibilities regarding the relationship between the Commonwealth, the Commonwealth Agencies and the Offeror. Content should include procedures regarding communication and coordination regarding work requests, Service delivery issues, budgeting and financial issues, etc.
3. Authorized Users	The Offeror should describe procedures and responsibilities regarding responding to Authorized Users (including listing of Authorized Users) problems, requests, and questions.

Content	Description
4. Third Party Vendors	Offeror to describe procedures for relationship regarding Third Party Vendors which may provide services, Equipment, and/or Software that are ancillary to (or support) the overall delivery of Services. Procedures and coordination with key Third Party Vendors should be documented.
5. Other Third Parties	The Offeror should describe procedures for any other contact or requests from other Third Parties in regard to the Agreement.
1.7 Offeror Operational Procedures	
1. Operating Level Agreements (OLA)	OLAs are internal "back-to-back" agreements that define how two different Service Component Providers will work together to support the delivery of defined IT Services to the Commonwealth and Commonwealth agencies. The OLAs will define how Service Component Providers will work together to meet the Service Requirements documented in SOWs and Service Level Requirements documented in formal SLAs for the DCS initiative. The OLAs are a set of operational processes that supplements the IT Service Management section of the Commonwealth Computing Procedures Manual providing the second level detail required for individual Service Components to interoperate. Simply stated, the OLA "bolts" multiple Service Components together operationally.

Content	Description
2. Operational Procedures (by Service Component, as applicable)	The Offeror should describe the activities that the Offeror proposes to undertake in order to provide the Services, including those directions, supervision, monitoring, staffing, reporting, Planning and oversight activities normally undertaken by the Offeror which shall be consistent with those Offeror activities used to provide services similar to the Services.
3. Service Responsibility Matrix (SRM)	A map of the Functional Service Areas which potentially overlap Offeror responsibility and Commonwealth responsibility required to deliver business solutions to the business units. A Service Responsibility Matrix will be developed for each such area to delineate which party is responsible for performing select service elements and/or providing assistance or input.
1.8 The Commonwealth Customer Operations Manuals	

Content	Description
1. Individual Commonwealth Customer Operations Manual	The Commonwealth Computing Procedures Manual will also contain specific sections dedicated to operational procedures for Services provided to individual The Commonwealth Customers (each a "**The Commonwealth Customer Operations Manual**"). Each The Commonwealth Customer Operations Manual will address unique operational requirements of the respective The Commonwealth Customer, including operational areas such as the following: • Runbooks • Data safeguarding, use and release restrictions • Data security policies • Disaster Recovery requirements • Notification levels and procedures (e.g. problems and initial Severity Level procedures)

Content	Description
Purpose	The Offeror should describe the purpose of the Commonwealth Computing Procedures Manual. This section should address who should use the Manual, how the Manual is organized, how the initial version and updates will be distributed, version control procedures for the Manual, when updates will occur, and procedures for authorizing and implementing updates. It is intended that the structure of the Manual will require that the individual compliance requirements and business rules of each participating Commonwealth Customer are separately identified where applicable for each section or component part of the Manual.
3.5.2.1 Organizational Overview	
2. Offeror Governance Organization	Include organization charts, description of functions performed, contact information.
3. Offeror Management and Delivery Organization	Include organization charts, description of functions performed, contact information.
4. Key Contacts – Offeror	A list of contacts that are key users of the Services and/or perform a liaison function in regard to the Services (by Commonwealth and Commonwealth Agencies, by location).

Content	Description
5. Key Contacts – Third Parties	A list of key Third Parties (maintenance providers, software providers, telecom carriers, etc).
3.5.2.2 Transition and Support Activities and Responsibilities	
6. Overall Management and Reporting Process	A description of Offeror management structure, reporting, and review process associated with Transition Services and Transformation Services.
7. Critical Deliverables and Milestones	A list of Critical Deliverables, milestones and timeline for the Transition Services and Transformation Services periods.
8. Interim Performance Management Procedures	A description of interim procedures to monitor and coordinate Service delivery, including Problem Management, Change Management, Service Level monitoring and reporting, physical and Logical Security, project management, work authorization, etc. A description of the responsibilities of both Parties.

Content	Description
9. Interim Financial Management Procedures	A description of interim procedures for invoicing, invoice verification, charge back to the Commonwealth Customers, determining Resource Unit volume by Service Component, asset management, asset transfers, forecasting, Commonwealth Customer support, etc. A description of the responsibilities of both Parties.
10. Interim Contract Management Procedures	A description of interim procedures for managing and administering the Agreement including proposed changes to the Agreement, interpretation procedures, issue-escalation process, and disputes. A description of the responsibilities of both Parties.
11. Other Transition and Support Procedures and Responsibilities	Any other pertinent procedures and responsibilities.
3.5.2.3 IT Service Management Procedures	
12. Service Desk	The facilities, associated technologies, and fully trained staff who respond to Calls, coordinate all Incident Management, Problem Management and Request Management activities, and act as a single point of contact for Authorized Users in regard to the Services.

Content	Description
13. Incident Management	The use of people, processes and technology with the primary goal to restore normal Service operations as quickly as possible and minimize the adverse impact on business operations, thus ensuring that the best achievable levels of service quality and availability are maintained.
14. Problem Management	The process, software, techniques and procedures that aid in identification, tracking, communication, and resolution of Problems arising in Customer's IT Environment, and resolving those Problems arising from or related to the Services. The goal of Problem Management is to minimize the adverse impact of Incidents and Problems on the business that are caused by errors within the IT infrastructure, and to prevent recurrence of Incidents related to these errors. In order to achieve this goal, Problem Management seeks to get to the root cause of Incidents and then initiate actions to improve or correct the situation.
15. Change Management	The processes relating to planning and performing all changes in IT environment pertaining to the Services, including changes to individual components and coordination of changes across all components. The Change Management processes will support and include checkpoints to determine any potential or required Change Control Procedures and includes a process of controlling changes to the infrastructure or any aspect of Services, in a controlled manner, enabling approved changes with minimum disruption.

<table>
<tr><th>Content</th><th>Description</th></tr>
<tr><td>16. Configuration Management</td><td>The process of identifying and defining CIs in a system, recording and reporting the status of CIs and RFCs, and verifying the completeness and correctness of the CIs.

The following data fields are required as a minimum for Asset/Configuration Management (any number of these may require that auditing be enabled.):
<table>
<tr><th>Physical Attributes</th><th>Logical Attributes</th></tr>
<tr><td>CI Name</td><td>System Role</td></tr>
<tr><td>Serial Number</td><td>Primary Capability</td></tr>
<tr><td>Commonwealth Asset Tag</td><td>Capability</td></tr>
<tr><td>Owner</td><td>Complexity</td></tr>
<tr><td>Ownership Type</td><td>Priority</td></tr>
<tr><td>Funding Source</td><td>Storage (currently TPC tool)</td></tr>
<tr><td>Purchase Date</td><td>24 x 7 Access</td></tr>
<tr><td>Life Cycle Dates</td><td>OS Billing Platform</td></tr>
<tr><td>Status</td><td>Operating System (OS)</td></tr>
<tr><td>Physical Location</td><td>OS Version</td></tr>
<tr><td>Region</td><td>OS Manufacturer</td></tr>
<tr><td>Product Name</td><td>Last Scan Date</td></tr>
<tr><td>CI Type</td><td>Audit Report</td></tr>
<tr><td>Model/Version</td><td>Relationships</td></tr>
<tr><td>Manufacturer</td><td>Applications</td></tr>
<tr><td>Supplier Name</td><td>Application SW Info</td></tr>
<tr><td>Tier</td><td>Disaster Recovery Priority</td></tr>
<tr><td>Asset Classification</td><td>Customer Project Identification</td></tr>
<tr><td></td><td>Drivers and Version Numbers</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Content</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><td>Date of Last Inventory</td><td>Service Pack</td></tr>
<tr><td></td><td>Network Protocol</td></tr>
<tr><td></td><td>Assigned IP Address(s)</td></tr>
<tr><td></td><td>DNS Host Name</td></tr>
<tr><td></td><td>Domain</td></tr>
<tr><td></td><td>Physical or Virtual Identifier</td></tr>
<tr><td></td><td>Funding Source</td></tr>
<tr><td></td><td>Memory allocated</td></tr>
<tr><td></td><td>Installation date
Related CIs</td></tr>
</table>
</td></tr>
<tr><td>17.□ Release Management</td><td>The process responsible for planning, scheduling and controlling the movement of Releases to Test and Live Environments. The primary objective of Release Management is to ensure that the integrity of the Live Environment is protected and that the correct Components are released. Release Management works closely with Configuration Management and Change Management.</td></tr>
<tr><td>18.□ Request Management and Fulfillment</td><td>The process responsible for managing the lifecycle of all Service Requests.</td></tr>
<tr><td>19.□ Availability Management</td><td>The process responsible for defining, analyzing, Planning, measuring and improving all aspects of the Availability of IT services. Availability Management is responsible for ensuring that all IT Infrastructure, Processes, tools, roles etc. are appropriate for the agreed Service Level targets for Availability.</td></tr>
</table>

Content	Description
20. Capacity Management	The process responsible for ensuring that the Capacity of IT Services and the IT Infrastructure are able to deliver agreed Service Level targets in a cost effective and timely manner. Capacity Management considers all Resources required to deliver the IT Service, and plans for short-, medium-, and long-term business requirements.
21. Service Level Management (SLM)	The process responsible for negotiating SLAs, and ensuring that these are met. SLM is responsible for ensuring that all IT Service Management Processes, OLAs, and Underpinning Contracts, are appropriate for the agreed Service Level targets. SLM monitors and reports on Service Levels, facilitates Service Delivery Failure actions with the appropriate Governance Committee and holds regular Commonwealth Customer reviews.
22. IT Service Continuity Management (ITSCM)	The process responsible for managing risks that could seriously impact IT Services. ITSCM ensures that the IT Offeror can Always provide minimum agreed Service Levels, by reducing the risk to an acceptable level and Planning for the recovery of IT Services. ITSCM should be designed to support Business Continuity Management.

Content	Description
23. IT Financial Management	The process responsible for managing the Budgeting, Accounting, Invoicing and Chargeback requirements).
24. Information Security Management	The process that ensures the confidentiality, integrity and Availability of an organization's Assets, information, data and IT Services. Information Security Management usually has a wider scope than the Offeror. It normally includes handling of paper, building access, phone calls etc., for the entire organization.
25. Project Management and Support	Project Management and Support will align projects to Commonwealth requirements and deliver projects from request through end-to-end solutioning including turnover to the Commonwealth Customers and validation that project requirements were met in terms of timing, quality, and cost.
26. Service Catalog	A database or structured Document with information about select Services, including those available for Deployment. The Service Catalog is the only part of the Service portfolio published to Commonwealth Customers, and is used to support the request and delivery of select Services. The Service Catalog may include information about Deliverables, prices, contact points, ordering and request processes.

Content	Description
3.5.2.4 Financial Management Procedures	
27. Invoicing	The Offeror should describe procedures for invoicing. The content should include procedures for calculating Resource Unit volumes for pricing (per Service Component, as applicable), invoicing of Projects, etc. The content should include procedures regarding disputed invoice amounts.
28. Chargeback	The Offeror should describe procedures for charge back of costs related to the Services and the overall Agreement to the Commonwealth Customers (to include responsibilities and support by both the Offeror and the Commonwealth).
29. Budgeting	The Offeror should describe how it would assist the Commonwealth with the annual budgeting cycle. Process should include estimation of Resource Unit volumes (by Service Component and Commonwealth Customer as appropriate), potential Projects, review cycle, etc. The content should include the responsibilities of Offeror, the Commonwealth, and Commonwealth Agencies.

Content	Description
30. Forecasting	The Offeror should describe procedures for forecasting cost versus budget.
31. Procurement	The Offeror should describe procedures for procurement Services (where Offeror performs procurement on behalf of the Commonwealth, as applicable). The content should include responsibilities and process for both the Commonwealth staff and Offeror.
32. Service Level Credits and Earnback	The Offeror should describe procedures for calculating Service Level Credits on invoices and Earnback calculations.
3.5.2.5 Contract Management Procedures	
33. Contract Change Control	The Offeror should describe procedures regarding changes to the Agreement, including changes to any Exhibit or Attachment. Content should include procedures to classify services as a New Service, and resulting process to change the Agreement (including pricing). Content should include notification period and process, authority levels, and escalation procedures for changes to the Agreement.

Content	Description
34. Reporting	The Offeror should describe procedures and activities regarding key standard Reports and requests for ad hoc reports from the Commonwealth and The Commonwealth Agencies.
35. New Service Levels	The Offeror should describe procedures for determining new Service Levels (based on continuous improvement and/or Commonwealth request).
36. Benchmarking	The Offeror should describe procedures for Benchmarking exercises, including determination and agreement of benchmark firm, sample peer group and process used for benchmark, payment for benchmark, review of results, and potential outcome. Content should include dispute resolution process.
37. Auditing	The Offeror should describe procedures for operational and/or financial audits (as required by the Commonwealth auditing and/or regulatory agencies). The Offeror should describe notification process and procedures to resolve audit findings.
38. Offeror Key Personnel and Subcontractors	The Offeror should describe procedures for Commonwealth approval regarding replacement or removal of Offeror Key Personnel and major Subcontractors to Offeror.

Content	Description
39. Dispute Resolution	The Offeror should describe procedures regarding formal dispute resolution process.
3.5.2.6 Relationship Management Procedures	
40. Customer Satisfaction Surveys	The Offeror should describe the process to be used for conducting customer satisfaction surveys. Content should include procedures regarding action items and attempts to resolve customer issues.
41. Commonwealth Agencies	The Offeror should describe procedures and responsibilities regarding the relationship between the Commonwealth, the Commonwealth Agencies and the Offeror. Content should include procedures regarding communication and coordination regarding work requests, Service delivery issues, budgeting and financial issues, etc.
42. Authorized Users	The Offeror should describe procedures and responsibilities regarding responding to Authorized Users (including listing of Authorized Users) problems, requests, and questions.

Content	Description
43. Third Party Vendors	Offeror to describe procedures for relationship regarding Third Party Vendors which may provide services, Equipment, and/or Software that are ancillary to (or support) the overall delivery of Services. Procedures and coordination with key Third Party Vendors should be documented.
44. Other Third Parties	The Offeror should describe procedures for any other contact or requests from other Third Parties in regard to the Agreement.
3.5.2.7 Offeror Operational Procedures	
45. Operating Level Agreements (OLA)	OLAs are internal "back-to-back" agreements that define how two different Service Component Providers will work together to support the delivery of defined IT Services to the Commonwealth and Commonwealth agencies. The OLAs will define how Service Component Providers will work together to meet the Service Requirements documented in SOWs and Service Level Requirements documented in formal SLAs for the DCS initiative. The OLAs are a set of operational processes that supplements the IT Service Management section of the Commonwealth Computing Procedures Manual providing the second level detail required for individual Service Components to interoperate. Simply stated, the OLA "bolts" multiple Service Components together operationally.

Content	Description
46. Operational Procedures (by Service Component, as applicable)	The Offeror should describe the activities that the Offeror proposes to undertake in order to provide the Services, including those directions, supervision, monitoring, staffing, reporting, Planning and oversight activities normally undertaken by the Offeror, which shall be consistent with those Offeror activities used to provide services similar to the Services.
47. Service Responsibility Matrix (SRM)	A map of the Functional Service Areas which potentially overlap Offeror responsibility and Commonwealth responsibility required to deliver business solutions to the business units. A Service Responsibility Matrix will be developed for each such area to delineate which party is responsible for performing select service elements and/or providing assistance or input.
3.5.2.8 The Commonwealth Customer Operations Manuals	

Content	Description
48. Individual Commonwealth Customer Operations Manual	The Commonwealth Computing Procedures Manual will also contain specific sections dedicated to operational procedures for Services provided to individual The Commonwealth Customers (each a "**The Commonwealth Customer Operations Manual**"). Each The Commonwealth Customer Operations Manual will address unique operational requirements of the respective The Commonwealth Customer, including operational areas such as the following: • Runbooks • Data safeguarding, use and release restrictions • Data security policies • Disaster Recovery requirements • Notification levels and procedures (e.g. problems and initial Severity Level procedures)

UNISYS RESPONSE:

The Offeror should describe the purpose of the Commonwealth Computing Procedures Manual. This section should address who should use the Manual, how the Manual is organized, how the initial version and updates will be distributed, version control procedures for the Manual, when updates will occur, and procedures for authorizing and implementing updates. It is intended that the structure of the Manual will require that the individual compliance requirements and business rules of each participating Commonwealth Customer are separately identified where applicable for each section or component part of the Manual.

Purpose of the Manual. The Commonwealth Computing Procedures Manual (CCPM) is an enterprise document that reflects the procedures for the Outsourcing Program between Unisys and the Commonwealth. It also provides input from subcontracting units. This manual provides process descriptions that meet contract requirements; represents best practices; includes the key elements of a quality enterprise service delivery process; and is easy to find, read, and understand.

The CCPM provides the best possible guidance for supporting infrastructure and technology for the Commonwealth and your participating agencies during the outsourcing term with Unisys.

CCPM Organization. This manual will be organized according to the outline provided below, which matches the requirements on **Schedule H.** The manual's structure will provide the opportunity for the individual compliance requirements and business rules of each participating Commonwealth customer to be separately identified when applicable for each section or component part of the manual.

Users of the CCPM. This manual should be used by each Commonwealth agency using Data Center Computing Services, all key personnel supporting the operations of the Data Center Computing Services, all Technical Support Services teams for all platforms, the subcontractors and Small Diverse Business Partners, and the Bureau of Enterprise Services (BES).

Document Development Timeline and Distribution. The initial version and updates of the CCPM are a key deliverable that will be developed within the timelines listed in **Schedule D — Transition Milestones Document.** The CCPM will be distributed for contributions and an internal review of the Data Center Computing Service key staff. This manual will then be submitted in accordance with **Schedule** D for the Commonwealth's review and preparation of a draft CCPM. On completion, the CCPM will be posted to the Knowledge Management Portal, where it can be accessed by the Commonwealth Office of Administration and the agencies.

Document Location. The Knowledge Management Portal will provide a central repository, security, and version control for all documents in the interim and through final development. An electronic copy is also located on the Unisys SharePoint portal for Data Centers and the Unisys Project Management Office. The Commonwealth will approve this manual before release.

Document Version Management. Version Control for each portion of the manual will contain a Document Tracking and Document Change History section for version control.

Recurring Document Updates. The Data Center Computing Service Offeror proposes to update this document annually or at the Commonwealth's request to reflect any changes in the operations (customer or Offeror) or procedures to be described therein. When updates to the CCPM are made, the revision will be updated and approved, and submitted to the Commonwealth according to **Schedule H.**

The procedures for authorizing and implementing updates is as follows.

1. Unisys and the Commonwealth will work jointly to create a timeline before any updates are authorized to be started.
2. After the Commonwealth approves the timeline, Unisys and our subcontracts will review and update the manual. The Process Manager will review documents with changes.
3. When all updates are completed, Unisys will send the sections of the manual with changes to subcontractors for review. Any disagreements on the documentation will be discussed between subcontractors and Unisys, and a decision will be made on whether to make the change.
4. The sections of the manual with changes will be sent to the Commonwealth for review.
5. The Commonwealth will submit changes back to Unisys in accordance with the timeline, and Unisys will implement the changes. If there are any disagreements, Unisys and the Commonwealth will meet to discuss them.
6. The manual will be sent with the final changes to the Commonwealth for a final review.
7. The Commonwealth will approve the manual, and Unisys will publish it.
8. The approved manual will be uploaded to the Knowledge Management Portal.
9. A letter of acknowledgement will be sent to the Commonwealth and be signed by the Commonwealth designee and returned to Unisys.

10. A signature acknowledgement letter will be sent to the Commonwealth designee which recognizes the joint and individual contributions to the CCPM by the Commonwealth of Pennsylvania and the Unisys Team. This letter will be signed by all third parties and returned to Unisys.

Document Protections. The security classification (Confidential) and the handling of this document will comply with the Commonwealth and vendor requirements. Controlled accessed to the Knowledge Management Portal will be maintained, and paper copies will be discouraged. The paper copies that exist will be kept in a locked cabinet or office and be shredded when obsolete.

Document Organization. The manual's structure will require each participating Commonwealth customer's compliance requirements and business rules to be separately identified when applicable for each section or component part of the manual. Operation Manuals for each Commonwealth agency will be developed where applicable and maintained by Unisys. These manuals will be located in the Data Center in hardcopy and also on our secure SharePoint site in electronic form.

The CCPM will contain the following information:

Organizational Overview document, which will contain the following documents:

- Offeror Governance Organization
  - Organizational charts
  - Brief description of functions performed
  - Contact information
- Offeror Management and Delivery Organization
  - Organizational charts
  - Brief description of functions performed
  - Contact information
- Key Contacts – Offeror
  - List of contacts that are key users of the services, perform a liaison function for the services, or both (by the Commonwealth and your agencies, by location)

- Key Contacts – third parties
  - List of Third Parties (such as maintenance providers, software providers, and telecommunications carriers).

Transition and Support Activities and Responsibilities document, which will contain the following information:

- Overall Management and Reporting Process
  - Description of management structure
  - Reporting process
  - Review processes for Transition and Transformation Services.
- **Critical Deliverables and Milestones** document will contain the following information:
  - List of Critical Deliverables
  - Milestones
  - Timeline for the transition and transformation services periods.
- **Interim Performance Management Procedures** document, which will contain the following information:
  - Interim procedures to monitor and coordinate Service Delivery noting responsibilities of both parties, including:
    - Problem Management
    - Change Management
    - Service Level Monitoring
    - Reporting
    - Physical and logical security
    - Project management
    - Work authorization.
- **Interim Financial Management Procedures** document, which will contain the following information:
  - Description of interim procedures and responsibilities of both parties for:

- Invoicing
- Invoice verification
- Chargeback to the Commonwealth customers
- Determining Resource unity volume by Service Component
- Asset Management
- Asset Transfers
- Forecasting
- Commonwealth Customer Support
- Responsibilities of both parties.

- **Interim Contract Management Procedures** document, which will contain the following information noting the responsibilities of both parties:
  - Description of interim procedures for managing and administering the Master Services Agreement, including:
    - Proposed changes to the agreement
    - Interpretation procedures
    - Issue-escalation process
    - Disputes.
- **Other Transition and Support Procedures and Responsibilities** document, which will contain the following information:
  - Pertinent procedures and responsibilities.

IT Service Management Procedures

- The **Service Desk** document will contain the following information:
  - Facilities details
  - Associated technologies

- A description of training and staffing procedures
- Coordination of all Incident Management and Request Management activities
- Single point of contact for authorized users in regard to the services.

- The **Incident Management** document will contain the following information:
  - People, processes, and technology used to restore normal service operations as quickly as possible and minimize adverse impact on business operations.
- The **Problem Management Incident Management** document will contain the following information:
  - Process, software, techniques, and procedures that aid in:
    - Identification
    - Tracking
    - Communication and resolution of problems arising in the Commonwealth's IT environment
    - Resolving problems arising from or related to the services
  - Root cause analysis procedures.
- The **Change Management** document will contain the following information:
  - Processes for planning and performing all changes in the IT environment pertaining to the services, including changes to individual components and coordination of changes across all components
  - Change Management Checkpoints.
- The **Configuration Management** document will contain procedures for the following activities:
  - Identifying CIs
  - Recording CIs
  - Reporting the status of CIs
  - Verifying completeness and correctness of each CI
  - Required data fields.

- The **Release Management** document will contain the following information:
  - Process planning and scheduling
  - Controlling movement of releases to Test and Live environments
- The **Request Management and Fulfillment Management** document will contain the following information:
  - Process for managing the life cycle of all Service Requests
- The **Availability Management** document will contain the following information:
  - Process responsible for defining, analyzing, planning, measuring, and improving all aspects of the availability of IT services
- The **Capacity Management** document will contain the following information:
  - Process for verifying that the capacity of IT Services and IT Infrastructure can deliver agreed Service Level Targets in a cost-effective and timely way
  - Plans for short-, medium-, and long-term business requirements.
- The **Service Level Management (SLM)** document will contain the following information:
  - Process responsible for negotiating SLAs
  - Monitoring and reporting on Service Levels
  - Commonwealth customer reviews
- The **IT Service Continuity Management (ITSCM)** document will contain the following information:
  - Process for managing risks that could seriously affect IT services
- The **IT Financial Management** document will contain the following information:
  - Process for managing budgeting, accounting, invoicing, and chargeback requirements
- The **Information Security Management** document will contain the following information:
  - Process for maintaining confidentiality, integrity, availability of organizations' assets, information, data, and IT services. Includes the following:
    - Building access

- Handling of paper
- Telephone calls.

- The **Project Management and Support** document will contain the following information:
  - Aligning projects with Commonwealth requirements
  - Delivering projects from request through end-to-end solutioning, including turnover
  - Validating that project requirements for timing, quality, and cost are met.
- The **Service Catalog** document will contain the following information:
  - A document with information about select services, including those available for deployment
  - The Service Catalog may include the following:
    - Deliverables
    - Prices
    - Contact Points
    - Ordering
    - Request Process.

The **Financial Management Procedures** document will contain the following information:

- Invoicing
  - Procedures for invoicing
  - Procedures for calculation of Resource Unit volumes for pricing
  - Invoicing of projects
  - Handling disputed invoice amounts
- Chargeback
  - Procedures for chargeback of costs related to the services and the overall Master Services Agreement to the Commonwealth customers

- Budgeting
  - Process describing how the Offeror will assist the Commonwealth with the annual budgeting cycle
    - Estimation of Resource Unit volumes (by Service Component and Commonwealth customer)
    - Potential projects
    - Review cycle
    - Responsibilities of Unisys, the Commonwealth, and Commonwealth agencies
- Forecasting
  - Procedure for forecasting cost versus budget
- Procurement
  - Procedure for Procurement Services (when Offeror performs them on the Commonwealth's behalf)
- The **Service Level Credits and Earnback** document will contain the following information:
  - Procedures for calculating and Service Level Credits on invoices.

The **Contract Management Procedures** document will contain the following information:

- Contract Change Control
  - Procedures for changes to the agreement, including changes to any exhibit or attachment
  - Procedures to classify services as a New Service
  - Process to change the agreement (including pricing)
  - Notification periods and process
  - Authority levels
  - Escalation procedures for changes to the agreement
- Reporting
  - Procedures and activities for key standard reports

- Procedures for ad hoc reports from the Commonwealth and your agencies

- New Service Levels
  - Procedures for determining new Service Levels (based on continuous improvement, Commonwealth request, or both)
- Benchmarking
  - Procedures for benchmarking exercises, including:
    - Benchmark firm
    - Sample peer group
    - Payment for benchmark
    - Review of results
    - Potential outcome
- Auditing
  - Procedures for performing operational audits, financial audits, or both (as required by the Commonwealth auditing agencies, regulatory agencies, or both)
  - Notification process and procedures to resolve audit findings
- Offeror Key Personnel and Subcontractors
  - Procedures for obtaining the Commonwealth's approval for the replacement or removal of Offeror Key Personnel and major Subcontractors to the Offeror
- Dispute Resolution
  - Procedures for the formal Dispute Resolution process.

The **Relationship Management Procedures Earnback** document will contain the following information:

- Customer Satisfaction Surveys
  - Process for conducting Customer Service Surveys

- Procedures to include for action items and attempts to resolve customer issues

- Commonwealth Agencies
  - Procedures and responsibilities for the relationship between the Commonwealth, the Commonwealth agencies, and the Offeror
  - Communication and coordination of work requests
  - Service Delivery issues
  - Budgeting
  - Financial issues
- Authorized Users
  - Procedures for responding to authorized users' problems, requests, and questions
  - List of authorized users
- Third-party Vendors
  - Procedures for maintaining relationship with third-party vendors, which may provide services, equipment, and software that are ancillary to (or support) the overall delivery of Services
- Other Third Parties
  - Procedures for any other contact or requests from other third parties in regard to the agreement.

The **Offeror Operational Procedures** document will contain the following information:

- Operating Level Agreements (OLAs)
  - Operational procedures that supplement the IT Service Management section of the Commonwealth Computing Procedures Manual, providing second-level detail required for individual Service Component to interoperate.
- Operational Procedures (by Service Component, as applicable)
  - Activities that the Offeror proposes to undertake to provide the Services, including:
    - Directions

- Supervision
- Monitoring
- Staffing
- Reporting
- Planning and oversight of normal activities

- Service Responsibility Matrix (SRM)
  - Map of Functional Service Areas that potentially overlap Offeror responsibility and Commonwealth responsibility required to deliver a business solution to the business units.
- Service Responsibility Matrix for each area to delineate which party performs select service elements, provides assistance or input, or does both.

The **Commonwealth Customer Operations Manuals** will include the following information:

- Individual **Commonwealth Customer Operations Manual**
  - Overview of the Commonwealth Customer Operations Manual to address unique operational requirements of the respective Commonwealth customer, including:
    - Runbooks
    - Data safeguarding, use, and release restrictions
    - Data security policies
    - Disaster Recovery requirements
    - Notification levels and procedures (for example, problems and initial Severity Level).

Request for Proposal

RFP # 6100022698

Commonwealth of Pennsylvania

Office of Administration

Office for Information Technology

Data Center Computing Services

SCHEDULE M

DETAILED TRANSITION PLAN

(Offeror to provide Offeror's Detailed Transition Plan within the Schedule)

UNISYS RESPONSE:

The Commonwealth Data Center Computing Services contract requires extensive transition, but after evaluating the Unisys Transition Plan, you will quickly see that our team offers what no other vendor can offer: rapid startup of the transition. We deliver continuity of service during transition, strong institutional depth of knowledge to mitigate risks before they become problems, and minimal business impact from our transition approach.

By retaining the Unisys Team, the Commonwealth will continue to benefit from our experience across the broad array of data center expertise. Employing this team will stabilize key data center working relationships instantly, mitigate risky transition processes, and protect the larger flow of Commonwealth projects for Pennsylvania's critical initiatives such as transformation and enterprise architecture upgrades and implementations scheduled for the next 10 to 12 years. Simply put, continuing with Unisys provides solid contract transition and continued service delivery reliability.

Our commitment to service permeates everything we deliver. Transitioning large, complex efforts from an incumbent vendor to a new vendor can be very complicated and risky. When it comes to the enterprise data centers supported for the Commonwealth, consistent operation becomes a critical service—Pennsylvania citizens rely on those systems to be reliable, stable, and available for their needs. Even the most diligent transition plan from other vendors cannot capture the knowledge and experience lost in the departure of current system support staff, especially when many of those team members bring years of experience and history with the Commonwealth and your critical enterprise applications.

The team's productivity is an important consideration for the transition period. With a new vendor, the Commonwealth will incur significant unproductive transition costs funded by taxpayer dollars, and ongoing training of new vendor staff to learn the wide range of Commonwealth systems and priorities.

Furthermore, the Commonwealth has several initiatives identified as priorities in progress; these efforts will likely stretch into and throughout the entire transition period. If the transition is unsuccessful, all of these projects will be at risk. It is clear that additional pressures on funding and requirements from the Commonwealth and federal governments—such as the impact of healthcare reform—make it imperative that the Commonwealth engage a team that can accomplish the transition with no delays and deliver reliable operational support to the full range of agencies affected by the Data Center consolidation.

On top of all that, administration changes across the contract's life may bring new priorities to the Commonwealth, driving adaptation of the delivered architecture, system requirements, and costing. No one is in a better position to provide continuity

and continued productivity throughout the transition and for the contract's duration than the Unisys Team.

As the selected contractor, we will complete the transition to the new contract within 28 months, bringing the data centers to full operations capability within the timeline set forth in the contract. We have a solid plan, schedule, team, and solution architecture.

A new vendor will remain almost solely focused on transition during this period, and likely require extensive additional knowledge transfer and training much beyond our team's level. We know the systems, the operations, and your people. We know what is required for an effective transition. Instead of asking questions during the contract's first few weeks, we will be presenting answers and moving forward to be sure we complete the work on time. No other vendor can do this except for the Unisys Team.

We recognize that you are embarking on a procurement that is different from the current contract and how things are operating today. There are some similarities to our current contract structure, but you clearly specify a number of guiding principles and objectives that are new to you. With our proposal to continue as your Data Center provider of choice, we will help you better achieve your objectives by reducing the risk of a broad transition from a new, untested, untrained team.

Sections 3.1 and 3.2 provide a glimpse into some of the details and the timeline of our transition. A detailed project plan is provided at the end of this section.

Transition Approach

The Unisys approach for the Commonwealth's Transition program includes two major categories of effort.

The first is the Transition of Services, which will concentrate on transferring operational responsibility from the current service provider to the Unisys Team. For services where the Unisys Team is the current provider, the Commonwealth benefits from less risk and faster steady state. This area's key transition events will be the gathering, analysis, and documentation of current state information. The knowledge transfer activities will take the documented information and train the steady state team so its members are aware of all aspects of the environment. Transformation activities will also use this information and with the implementation of the Unisys Team's best practices, processes, and tools to provide excellent service.

The second category is Data Center Migration, which will concentrate on using the knowledge gained during the transition activities, along with stakeholder input and Unisys processes to plan and execute the data center migrations. These activities include a joint team of Commonwealth experts working alongside the Unisys Team to plan and execute the migration activities to minimize risk to the end users of the applications.

The Unisys transition method framework defines the comprehensive projects, processes, and deliverables necessary to effectively and efficiently transition services. This framework combines best practices, industry standards, and open communication to help promote a successful transition. The framework is continuously evolving by incorporating the experiences gained by Unisys through all the transitions undertaken. Our framework promptly predicts and mitigates risk, maintains timescales and minimizes disruption to the Commonwealth's business operations.

The Commonwealth is continuously looking for ways to cut costs, improve efficiency, optimize the use of existing assets, improve service levels, and meet stricter security and compliance requirements. Evaluation, consolidation, standardization, and virtualization of data centers are some of the effective ways to meet these growing needs. In particular, we find that consolidation and optimization of data centers reduce complexity, deliver greater cost savings, and enable effective use of technology and the underlying resources.

Unisys accomplished some very large federal transitions that include the Department of Homeland Security, Department of Agriculture, Transportation Security Administration, and General Services Administration. We developed processes and gleaned from lessons learned to guide our transition leaders while consolidating and transitioning multiple data centers to a few data centers. Unisys recognizes that any large data center undergoes a level of organic growth and a natural evolution over time. The challenge for any IT organization is to take its current, organically grown and matured data center and be able to reconstruct it with minimal user impact, low risk, and low

costs, and in an efficient way. This challenge is further complicated with the absolute requirement to support and maintain the current course while provisioning for the planned future during the transition process.

The Unisys Transition Leadership model is a holistic approach that guides our transition directors and managers through the day-to-day activities. The approach involves four steps:

1. Discover
2. Plan
3. Implement
4. Course Correct.

Discover: Conduct a full inventory all the data centers, applications and agency requirements; identify every component (hardware, software, interface, document) and determine the disposition for each component in each data center (move, decommission, leave in place, and so forth); monitor changes to data centers and maintain the discovery documents, using the inventories; and initiate modeling of the transition activities.

Plan: Gather the findings of the discovery task; analyze them to build a cohesive transition plan; validate the estimates, dependencies, and status for each data center component. Identify other agency activities, plans, and projects that will intersect with transition activities. Resolve the collision between the projects. Conceptualize the overall plan, staff the plan, and cost the plan. Assess the risk of the schedule, staffing, milestones, deliverables, and all aspects of the transition. Identify and implement mitigations. Document the Transition Plan for coordination, review, and approval by the Commonwealth.

Implement: Use the plan and schedule to drive the transition. Manage the resources to execute the schedule. Measure progress with metrics and quality assessments; control the assigned staff to enable them to move as a unit, always working toward common goals.

Course Correct: Conduct governance meetings staffed by senior Commonwealth stakeholders and senior Unisys stakeholders. Discuss issues; work the issues closely to closure. Conduct risk assessments as part of the summit meeting. Identify risks, define mitigation for the risks, and contain each risk. When needed, adjust the schedule (not the milestones), adding staff, adjusting methods, and improving performance, to meet the milestones. Oversee the implementation of mitigation and make risk contingency plans available as a backup if mitigation fails.

Unisys garnered these four steps from years of transition support and refined them during post-transition meetings, reviewing the progression of events, approaches that worked, and others that required extensive attention to confirm they worked as

planned. The Transition and Migration lessons learned table (**Table M-1**) displays the key lessons learned that are applicable to the Commonwealth's transition.

Table M-1. Transition and Migration Lessons Learned

Topic	Finding	Value to Commonwealth
Inventory	Use heterogeneous and comprehensive tools to discover, identify, and document current architecture, systems, applications, and hardware components.	Generates significant savings in time during discovery and eliminates unknowns during implementation.
Control	Define roles and responsibilities of all parties involved, especially when multiple providers are involved in a solution.	Provides a clear line of communications among vendors and reduces project delays.
Budget	Identify funding constraints at the project's beginning.	Understanding funding availability (how much and when) will drive certain technical solutions and avoid major delays on the project.
Modeling	Perform technical reviews of transition solutions for each individual system, application, and hardware component.	The Unisys methodology and toolset allows for very sophisticated modeling capability throughout all phases of the project, which will provide the Commonwealth with the needed agility, accountability, and decision-making capability.
Communication	Workgroup and status meetings that include all technical team members are a key to a complete end-to-end solution.	This provides a forum to discuss plans with key stakeholders, creating a complete solution that avoids re-planning during implementation.
Problem Solving	A tiger team comprised of a member from each responsible area resolves technical issues as they arise during the migration of major systems. For example, a tiger team might include a network engineer, firewall engineer, and systems and application engineer	This provides quick resolution when problems arise during implementation, reducing user downtime and other operational impacts.
Schedule Updates	Identify required schedule adjustments and obtain approvals in advance to avoid delays. Approvals may be required from multiple change management boards if more than one provider is involved in the total management of the data center infrastructure.	Eliminates implementation delays due to lack of coordinated change board approvals that take into account all the elements affected by schedule adjustments.
System Access	Identify and define required user access firewall rules well ahead of the implementation. Test and implement the firewall rules before the cutover to the new systems.	Enables all users requiring access to specific resources to have the necessary system access, reducing user downtime and operational fixes.
Security Planning	Involve the IT security group during planning and obtain tentative approvals for the migration solution.	Involving security professionals during planning enables the solution to be complete and approved by change boards in a timely way.

Building on the Unisys Transition Leadership model and our transition lessons learned, our transition approach implements the new services while maintaining business as usual minimizing impact on end users. No major improvement or transformational

activities should be undertaken during the transition. The transaction's major activities include:

- Establish the Governance Board and the Communication Plan to enable the transition to occur smoothly and be in place to quickly resolve inter-organizational issues
- Plan any knowledge transfer required for the future delivery of the transitioned services
- Perform gap analysis between the SOW and the current operational environment and develop the necessary adjustments to meet all the Commonwealth's requirements and expectations
- Establish the specifications for system, processes, and tools required for delivery of services in the future state environment
- Develop and produce the Commonwealth Computing Procedures Manual
- Establish future organizational structures and the implementation of organizational changes
- Prepare the Transition Project Plan, which after review and approval by the Commonwealth, will be the roadmap to orient all transitional activities until the transition of services is achieved. When the Commonwealth decides to transition services first then transform the infrastructure, transition of services will end when Unisys takes full control at the transition's end. After a stabilization period, the transformation can begin.
- Migrate and consolidate existing data centers such as the DPH and the agency data centers to the Unisys Managed Data Centers.

Transition Plan

Transition Governance

Transition leadership will organize the transition team into projects. Each project will be driven by a project charter and schedule. Project managers will make project-level decisions and conduct project activities at the lowest possible level in the project's structure. Issues, regardless of where they come from or how they surface, will be reported to the appropriate transition manager to be logged and managed. Issues can be acted on (including closure) by any transition leader, including the Transition Executive.

Risks affecting the project can be suggested and reported by anyone but will require approval from the Transition Executive to officially open a project-level risk.

When appropriate, these items will be escalated to the Steering Committee, the Program Manager and/or the Executive Sponsor for action, depending on their severity, and time sensitivity.

Issue, risk, and change management will follow the standard process described in this section.

Transition Focus

The Unisys transition will address Commonwealth and federal laws and regulations intended to support internal controls and provide governance over operational data centers—primarily to reduce costs and waste, manage risk, and promote the public welfare. Unisys will demonstrate compliance with these various regulatory controls and strategic goals. Our program and solution governance brings compliance with security considerations, staffing considerations, milestone requirements, and transfer of control. The overall transition solution will enhance the Commonwealth's presence across Pennsylvania. Activities affected by the transition are:

- Facilities
- Staff Training
- Data Center Consolidation
- Data Center Architecture
- Service Portfolio
- Enterprise Services Catalog
- Service Level Agreements
- Configuration Management
- System and Services Acquisition
- Physical and Environmental Protections
- Identification and Authentication

- Access Control
- System and Information Integrity
- Audit and Accountability
- Contingency Planning
- Data Recovery.

Transition Plan Components

The Unisys Transition Plan will contain a transition description, transition scope statement, and list of transition deliverables. The Transition Plan also will contain the components in **Figure M-2**. A detailed description of each Transition Plan component is provided in the following pages.

Figure M-2. Principal Unisys Transition Plan Components

Unisys Transition Plan Component	High Level Description
Transition Methodology	The Transition method is accomplished in five phases: Planning, Assessment, Design Validation, Deployment, and Handover.
Transition Staffing	The Transition team consists of a Transition Executive, Deputy Transition Executives, Project Managers, and various specialized team members. They work together to accomplish the goals and objectives expressed in the Transition Schedule.
Roles and Responsibilities	Each member of the Transition team has a clearly defined role and specific responsibilities. Their assigned tasks are specified in the Transition Schedule. Each assigned task is allocated to a specific milestone and deliverable. Status meetings confirm all are working on the assigned tasks in the schedule.
Communications Plan	• Team Meetings • Status Reporting • Summit Meetings
Transition Deliverables	Complete list of Transition Deliverables is developed during the planning process along with those in Schedule K.
Transition Schedule	List of tasks organized into activities grouped to meet milestones and deliverables. Structured in a work breakdowns format; presented in Microsoft Project; and provides the task's description, duration, start date, end date, dependencies (on other tasks, deliverables, and milestones), and assigned resources.
Transition Controls	• Transition Metrics Collection • Schedule Management • Risk Management • Issues Management • Change Management
Transition Quality Management	• Quality Audits • Quality Reviews

The plan component discussions that follow are briefly presented to deliver a concise understanding of the Unisys process for developing the final Transition Plan delivered to the Commonwealth.

Transition Methodology

The Unisys Transition methodology combines Gartner best practices, and industry standards with open communication to promote collaboration among Unisys, the Commonwealth, and business partners to make the transition a success.

Unisys follows a phased methodology using our Service and Solutions Delivery Framework (SDF). The Unisys SDF methodology prescribes that the transition be divided into the five phases in **Figure M-1.**

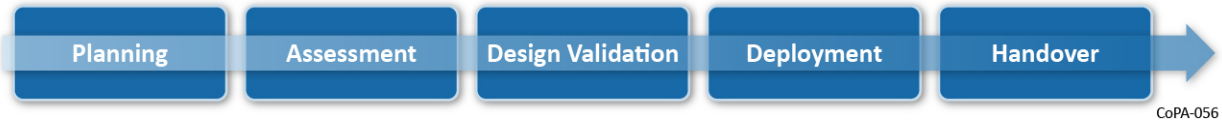


Figure M-1. Service and Solution Delivery Phased Methodology

The Transition methodology used by Unisys is a pragmatic phase-by-phase approach for each deliverable, which provides milestones that the Commonwealth can use to provide input and monitor progress. The Unisys Transition team will not exit a phase until the Commonwealth has had the opportunity to evaluate and approve the transition activities for the current phase. The objective of this approach is to provide the structure for managing the transition with the lowest risk while providing the Commonwealth with visibility and management control throughout the transition. Unisys keeps this methodology in constant evolution by incorporating the experiences we gained from many previous transitions.

The following narrative addresses the five phases of the Unisys Transition methodology in detail.

Planning Phase

During this phase, the Commonwealth and the Unisys Team will work to build the work plan to define the transition tasks and outlined resources required.

The Unisys Transition Executive will structure work packages by the respective project teams and continuously monitor completion of tasks and deliverables. Transition progress will be formally updated and analyzed weekly in the Project Plan. Corrections to the Project Plan will be made when necessary and agreed to in the mutually agreed change control procedures outlined as part of the Transition Governance Plan.

This phase will provide:

- An updated and agreed Transition Project Management Plan
- A detailed plan of activities required to achieve the transition (the Transition Schedule)
- The acceptance criteria for the services provided through transition
- Transition interfaces and dependencies

- Risk management and mitigation plans
- The Unisys and Commonwealth combined resource plans
- Communication plans
- The Unisys governance framework

Detailed planning will be the responsibility of Unisys, with assistance and input from the Commonwealth as reasonably required and will be signed off and agreed on by Unisys and the Commonwealth.

Assessment Phase

Assessment is the second phase of work following completion and approval of the Planning phase. Unisys will commence the knowledge gathering exercise to capture and document operational information that will be required to design and validate the solution to be delivered. This operational information includes details of current performance reporting processes, organization, business context, and users. An in-depth assessment of the Commonwealth's environment and the current procedures is critical to enabling a successful implementation of the solution. This data is used throughout the transition to validate that the solution design is implemented to meet the Commonwealth's business needs and verify that gaps between the current mode of operation and the future mode of operation are identified and remediated.

Representatives from each service stream and the Knowledge Management team will work with the Commonwealth to perform a detailed analysis at all levels of the operations to verify that all aspects are correctly evaluated and understood. The Subject Matter Experts (SMEs) and Knowledge Managers will meet with designated representatives of the Commonwealth and the incumbent agency providers to assess all needed processes and gather historical and current data to validate and finalize our proposed solution. To support these activities, Unisys developed tools, templates, and checklists that cover the various aspects of the business for the service streams. To enable a smooth transition, Unisys will define how the knowledge that is currently with the Commonwealth or the third party, and incumbent agency providers will be captured with the Commonwealth's support.

During the Assessment phase, Unisys will also review support category types of incidents and determine which types of incidents can be performed by the Service Desk to provide resolution as soon as possible. Unisys also will assess server and storage infrastructure and outline any areas of opportunity for cost reduction where the Commonwealth could look to migrate to a cloud-based infrastructure solution. The goal for doing this will be to reduce the manual effort of notifying third parties and provide the Commonwealth with a single view of the enterprise support using the Unisys ITSM solution.

On completion of the Assessment phase, the findings will be reviewed internally at Unisys and then jointly between Unisys and the Commonwealth. The assessment findings document will outline all gaps discovered and remediation plans for those

gaps. Unisys will request formal approval from the Commonwealth on the assessment data so we have a proper baseline from which to start. This approval from the Commonwealth will also signify the completion and acceptance that the Assessment phase is completed.

The Assessment phase will deal with the following actions and deliverables:

- Gather Commonwealth, incumbent agency provider, and third-party performance data Gather Commonwealth, incumbent agency provider, and third-party performance reporting processes and examples
- Gather the Commonwealth IT Services retained organizational model (current and near-term)
- Review staff position responsibilities
- Gather Commonwealth, incumbent agency provider, and third-party interviews
- Conduct workshops with the Commonwealth, incumbent agency provider, and third-party current operational management teams
- Capture documentation on current operational processes
- Capture list and deployment timelines for current and near-term IT projects
- Capture documentation on current operational issues
- Conduct a risk assessment.

Design Phase

The Design phase focuses on finalizing the strategy for developing processes, as well as implementing and deploying a governance structure to manage the current mode of operations. Unisys will design the reporting information consolidation (where possible), organization, and management structure required for managing the current services. The Commonwealth will review and approve the technical designs, plans, processes, and interfaces to confirm that they align with the Commonwealth's requirements. Unisys will conduct go/no-go reviews with the Commonwealth before discontinuing any services from the current systems to the new proposed systems. On successful cutover, Unisys will work with the Commonwealth to conduct post-implementation reviews as well as capture lessons learned and communicate them to all the stakeholders.

This phase will deal with the following actions and deliverables:

- Analyze documentation on the Commonwealth's current mode of operations
- Review the Commonwealth's requirements and expectations
- Review assessment analysis
- Update the risk assessment
- Develop end-to-end process flows for reporting on performance
- Develop the organizational structure for oversight by Unisys operations
- Design the billing process and reports
- Develop billing testing parameters
- Develop testing parameters for consolidated performance reporting

- Review and mutually agree on the feasibility and an approach to implementation of any immediate service improvements
- Agree with the Commonwealth on all the changes to be integrated into the Transition solution design for the current mode of operations.

Deployment Phase

The Deployment phase's activities will be based on the analysis and reviews performed in the previous phases of transition. In this phase, the Transition teams will deploy the resources, processes, tools, and operational solutions, as outlined and agreed by the Commonwealth in the Design phase. The Deployment phase consists of the following steps:

- **Implementation of Tools, Processes and Procedures –** The Transition teams will use the documents and standards from the design phase to implement processes and procedures for supporting the new environment.
- **Data Center Migrations –** The Data Center migrations will occur in accordance with the mutually agreed schedule established in the Planning phase.

Handover Phase

In the Handover phase, the Transition team will finalize all necessary documentation; verify that all processes, procedures, and tools are functioning according to the approved plan and design; review the implementation strategy; review and approve the plan; and hand the ownership of each in-scope service work stream over to the Unisys Agency Account Manager and Steady State team.

As a final activity, lessons learned are conducted and reported back to the Transition Management teams for inclusion in subsequent service deployments. Lessons learned will be solicited from members of the Commonwealth as well as from the Transition and Account teams.

Transition Staffing

Our transition staffing includes the Transition Executive, Deputy Transition Executives, Project Managers, the management team, project steering committees, and the individual transition experts we organized into a cohesive team.

Transition Executive

Unisys appointed a Transition Executive, [redacted] who is responsible for all aspects of delivering the transition, including milestones, meeting of key deliverables, communications, and the identification and assignment of transition resources. The Unisys Transition Executive will represent Unisys as the single point of contact (SPOC) during the transition, provide oversight and direction, and monitor the transition's overall status. The Unisys Transition Executive's role includes:

- Managing all aspects of the Transition program, including planning, staffing, finance, and implementation of transition deliverables
- Maintaining overall business relationship with Unisys, the Commonwealth, and business partners
- Overseeing that all communication is made according to the Communication Plan
- Confirming that resources participating in the transition program have a common understanding of needs of both businesses and the program's deliverables
- Agreeing on the scope, timelines, costs, and delivery timetables for each tower, confirming they are consistent and complementary with the Transition program's objectives
- Establishing effective controls and procedures for the Transition program
- Monitoring progress with all areas contributing to the program
- Reporting the transition's status to all program stakeholders
- Managing professional team performance to meet all transition objectives on time and within budget and quality
- Identifying and resolving conflicting transition priorities
- Managing internal and external relationships and expectations for a successful transition
- Conducting project and program implementation reviews to measure the transition's actual performance against the goals.

Unisys expects that the Commonwealth will also appoint a Transition Executive who shall have the following roles and responsibilities:

- Supporting Unisys tracking and reporting of the transition's progress
- Supporting Unisys management of the transition's key risks and issues
- Informing the Commonwealth's business areas of the transition activities relevant to them and that Unisys is managing the process
- Understanding and agreeing to follow the Unisys Transition Methodology Framework described in this proposal section
- Serving as the SPOC to all matters related to the transition on the Commonwealth stakeholders' behalf
- Assigning the necessary quantity and quality of resources to complete all activities under the Commonwealth's responsibility as planned
- Negotiating and agreeing to changes to the Transition Plan when circumstances caused by new findings justify those changes
- Contributing relevant information for inclusion in the Transition Plan and other transition documentation
- Facilitating the generation, ownership, and implementation of the Commonwealth's plans for management and transition in individual service streams
- Attending and chairing (as agreed and appropriate) designated transition review and progress meetings
- Liaising with any existing suppliers and third-party contributors to the transition, as appropriate.

Transition Team

The Unisys Transition program is organized into major activity-focused teams reporting to a senior member of the Transition Program Management Office.

Figure **M-4** shows the structure of the Unisys Transition Team.

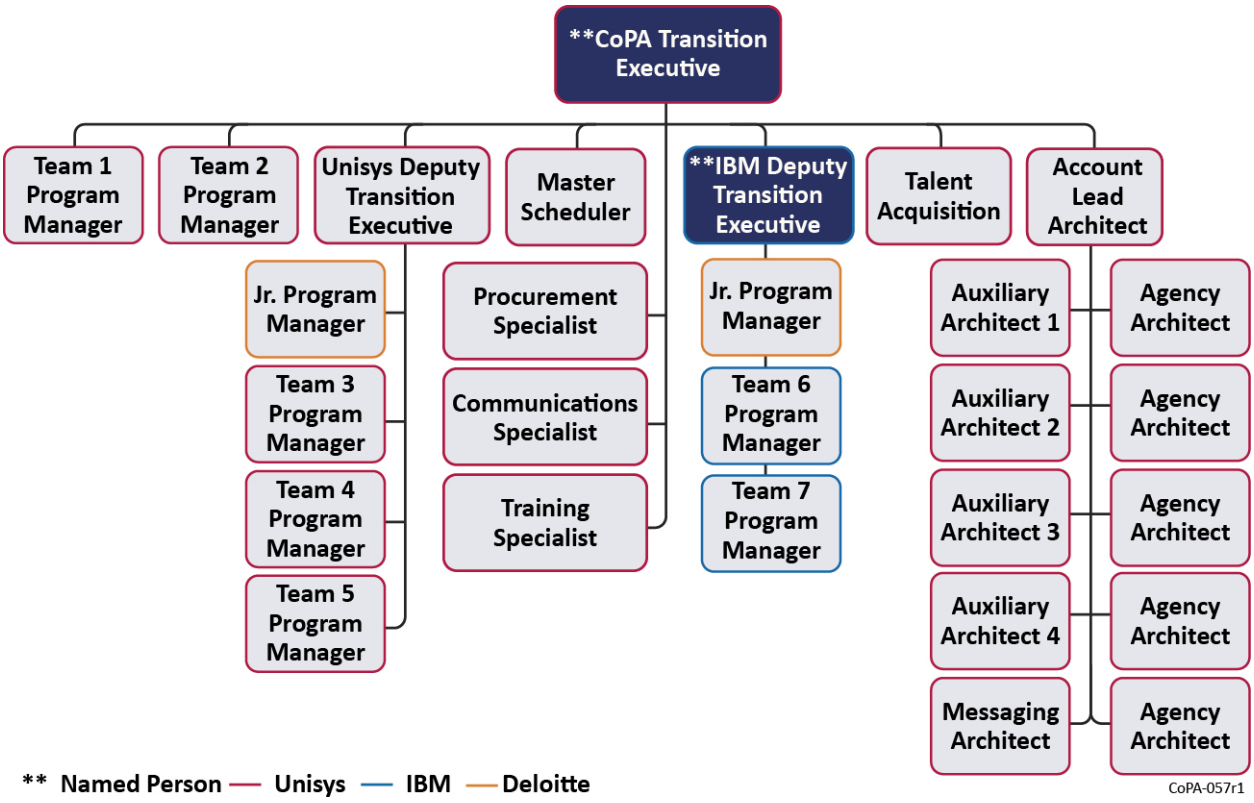


Figure M-4. Transition Program Management Office Structure

Each team has a distinctive purpose and membership. The teams are working teams whose members are actively engaged in the transition. Collectively, their tasks are defined on the Transition Schedule. They are organized to implement the Transition methodology under the watchful eye of the Transition Program Management Office.

During the planning sessions, transition staff will be organized into Teams. Unisys will identify a powerful group of experts to support each team. Each team will have a role in the Unisys Transition program, and each expert will have responsibilities individually assigned. At the transition kickoff meeting, the roles and responsibilities will be briefed to the entire team so each team member knows what he or she is responsible for and how his or her actions affect the larger group. **Figure M-5** provides a high level overview of the roles and responsibilities for each member of the Transition team.

Team Member Role	Team Member Responsibilities
Transition Executive	Responsible for the overall success of the program's goals and objectives
Deputy Transition Executives	Each will oversee a subset of the planning, design, and implementation of the data center migration projects.
Project Managers	Develop project plans and cause the project plans to be executed. They will work with individual agency leads and applications owners to communicate with stakeholders.
Project Coordinator/Jr. PM	Supports Deputy Transition Executives and Project Managers by taking meeting minutes and coordinating meetings.
Technical Implementation Engineers	Responsible for various technical disciplines including Mainframe, AIX, x86 (Windows and Linux), Network, Security, ITSM, Storage, Backup, and Monitoring. Will include technical knowledge of subject matter and tools for implementation and processes.
Master Scheduler	Establishes Microsoft Project standards, consolidation of working project schedules, and reporting.
Procurement Specialist	Verifies that all team members know and understand the procurement process. Assists TIEs with securing BOMs; PO approval; and the tracking, expediting, and receiving of orders. Also notifies appropriate team members when orders are received.
Talent Acquisition Specialist	Confirms that all team members know and understand the staffing process, assists team members with tracking, expediting, and receiving staffing requisitions.
Training Specialist	Coordinates all training needs for the Account PMO and Transition PMO teams, including use of facilities for training, coordination of third-party training required for the transition, and possibly support for the development of account-specific training needs.
Communications Specialist	Confirms that all communications to the Commonwealth and Commonwealth stakeholders are timely, accurate, and professional.
Account Lead Architect	Confirms that overall Commonwealth Supported Architecture meets or exceeds requirements, is documented, and is implemented within quality standards.
Agency and Auxiliary Architects	Responsible for agency- and tower-specific architectures as determined by the Agency Infrastructure Architect.

Figure M-5. Transition Roles and Responsibilities

Approach to the Transition Communications Plan

Communication is the cornerstone of the Unisys Service Transition Methodology (see **Figure M-6**). Our transition organization's structure enables rapid communication of issues, thereby preventing issues from affecting quality, project timelines, and end users' experience. The Unisys Service Transition Methodology will include the Commonwealth every step of the way to enable us to understand your steady state and evolving needs so key personnel are retained or added quickly and mission performance, SLA attainment, and customer satisfaction are not compromised during the transition.

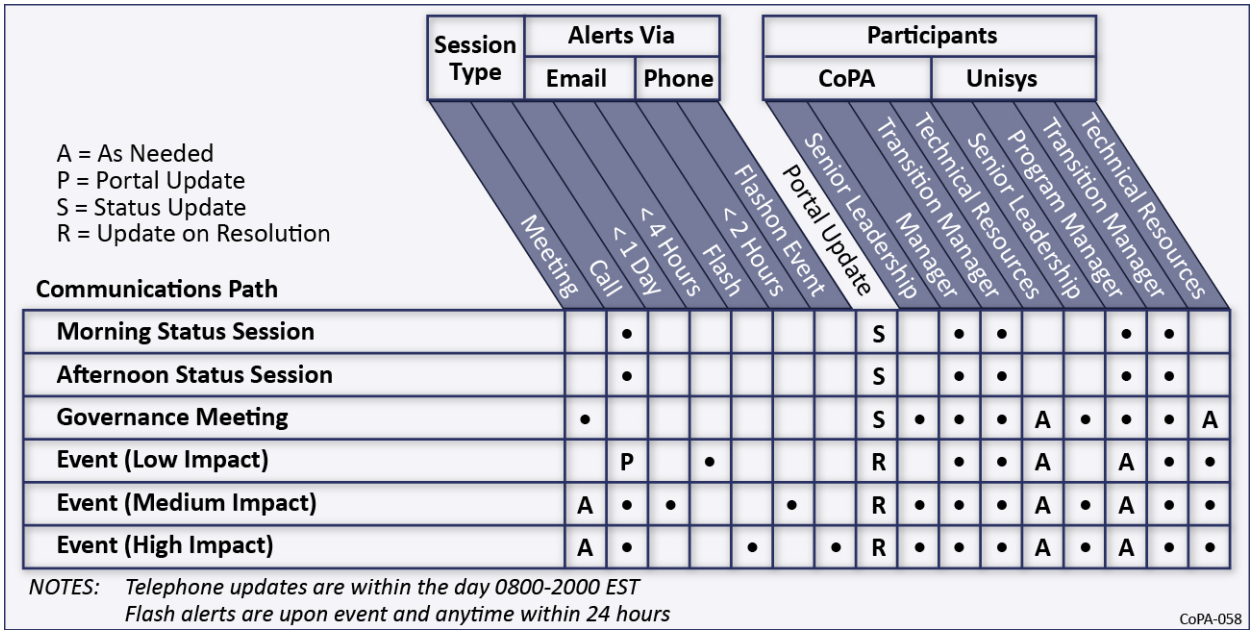


Figure M-6. Unisys Communication Management Approach

Throughout the process, Unisys will enable the Commonwealth's agency project contacts to be fully engaged through an aggressive, three-touch communications strategy. Using this strategy, we will contact agency designated contacts at least three times by using various techniques and media appropriate to your environment before any change affecting them occurs. This process is critical to help overcome resistance to change and minimize confusion. **Figure M-6** depicts our communication management approach for the transition project's delivery.

Transition Status Reporting Approach

The Unisys Service Transition Methodology defines the process steps for managing transition performance and progress reporting, which involves a standard set of reports developed to keep program stakeholders updated on the different aspects of transition work. In addition to the standard reports, Unisys and the Commonwealth can agree on different types of reports to keep the project sponsors and key stakeholders informed of the program's performance and progress.

The standard set of reports is designed to disseminate information on the following aspects of the program:

- **Status and Progress Reports –** Focus on the results achieved in comparison with the plan. Monitor performance (whether the responsibility of Unisys, the Commonwealth, or any third party) against the Transition Plan, documenting significant issues and related information about the actions underway, and informing constituents of upcoming activities.

- **Meeting minutes and ad hoc reports –** Document meetings, discussions, and decisions on several levels of the program, such as the Transition Steering Group, Program Steering Group, any other relevant meetings, and where decisions about the transition are made.

Each week during the transition, unless otherwise requested by the Commonwealth, Unisys will provide the Commonwealth a detailed progress report that describes the following:

- Summary reports including completion statistics, issues encountered, failures, and problems
- An executive-level summary of the transition's progress to date, including an updated summary project schedule and project highlights
- An updated Gantt chart detailing the status of all transition activities (including slippages, changes from the previous plan, and so forth in line with project management best practices)
- A list of all transition milestones, including estimated time to completion, days overdue, contract completion date, actual completion date, comments, and a RAG (Red, Amber, Green) report
- A list of all unresolved issues with the execution of the Transition Plan, including those for which the Commonwealth has primary responsibility, along with due date, priority, responsible party, and an assessment of the potential and actual business impact on the Transition Plan.

Requirements for quality reports will be defined in the detailed transition program planning process. **Figure M-7** shows the structure of transition status governance.

Structure	Timing	Participants	Goals/Agenda
Program Steering Committee	Weekly	• Commonwealth Program Sponsor (Chair) • Commonwealth Transition Executive • Commonwealth Program Steering Committee (3 or 4 representatives of key agencies) • Unisys Engagement Executive • Unisys Enterprise Architect • Unisys Service Delivery Executive • Unisys Transition Executive • IBM Deputy Transition Executive	• Review the transition program's status • Review the transition program's risks and mitigation plans • Discuss and resolve any open issues with the transition program • Discuss and resolve any contractual items related to the transition program or the services
Transition of Services Project Management	Weekly	• Transition of Services Project Manager • ITSM Project Manager • Commonwealth Transition Sponsor	• Review the status of each transition project, including progress against Transition Plan milestones and the status of milestones and

Structure	Timing	Participants	Goals/Agenda
		• Commonwealth Project Steering Committee (3 or 4 representatives of key agencies in the EDC) • Unisys Service Delivery Executive • Unisys Transition Executive • IBM Deputy Transition Executive	deliverables • Review open actions and information requests • Discuss and resolve any issues identified by the transition work streams • Discuss and action any planned changes • Identify any issues or contractual items that require escalation to the Program Steering Committee
Agency Data Center Migration (DCM) Project Work Streams	Weekly	• Agency Data Center Migration Project Sponsor • Agency DCM Director • Application Owners • Unisys Agency DCM Project Manager • Unisys Agency/Service Architect • Unisys Agency Account Manager • Unisys Service Delivery Manager • IBM or Unisys Deputy Transition Executive	• Report progress against DCM Plan milestones • Review open actions and information requests • Discuss and resolve any issues identified by the work stream • Discuss and action any planned changes
Data PowerHouse Data Center Migration (DCM) Project Work Streams	Weekly	• DPH Data Center Migration Project Sponsor • DPH DCM Director • Application Owners • Unisys Agency DCM Project Manager • Unisys Agency/Service Architect • Unisys Account Manager • Unisys and IBM Deputy Transition Executives	• Report progress against DCM Plan milestones • Review open actions and information requests • Discuss and resolve any issues identified by the work stream • Discuss and action any planned changes

Figure M-7. Transition Status Governance Structure

Approach to Transition Team Meetings

Before the first meeting, Unisys will develop meeting agendas, including a dashboard status report for each meeting that the leader will distribute before the meeting. **Figure M-8** lists the types of meetings, their purpose, attendees, and standard frequency.

Meeting	Purpose	Attendees	Frequency
Daily Transition Standup (Unisys Internal)	Results from the previous day and today's plans	Transition Tower Leads, SMEs, and Transition Manager	Daily
Daily Transition Meeting with the Commonwealth Transition Manager	Review of the transition's activities and status	Commonwealth and Unisys Transition Managers and Transition Tower Leads	Daily
Program Management Review	Status of the transition and the implementation	Commonwealth Senior Managers, Unisys Account Executive, and Transition Managers	Twice a week
Change Advisory Board	Review and approval of change requests	Change Control Board members	Weekly
Risk Management Review	Review of risks and issues	Transition Managers and Transition Tower Leads	Twice a week
Ad Hoc Meetings	Discussion of one or more transition-specific topics	T.B.D.	As needed

Figure M-8. Types of Meetings

Transition Deliverables

Unisys does not promise instant gratification with a one-time, "big bang only" approach to deliverable production. Credible transitions take careful planning. We work with Commonwealth stakeholders to establish goals, develop strategic plans, and deliver products and documents that maximize productivity during transition. Each subsequent task in our transitions builds upon the success of the previous one—introducing efficiencies that traverse the overall timeline.

The Unisys approach to data center transition planning drives our top-down approach. With decades of experience in transitioning mission-critical data center environments, Unisys Team is considered expert in business and IT Services—delivering on the needs for a service-structured enterprise. The key transition deliverables in **Schedule K** and other deliverables identified during the Planning phase will be included in scope of the Transition Plan.

Transition Schedule

Data center transition is not a destination; it is a journey that requires thoughtful planning. Unisys views transition as the process through which the Commonwealth Data Centers are prepared for the next generation. The transition does not happen overnight. However, Unisys experience with data center transformation enables us to use best practices and proven tools that accelerate the process and convert time to value. Our Transition Schedule is displayed in **Figure M-9.**

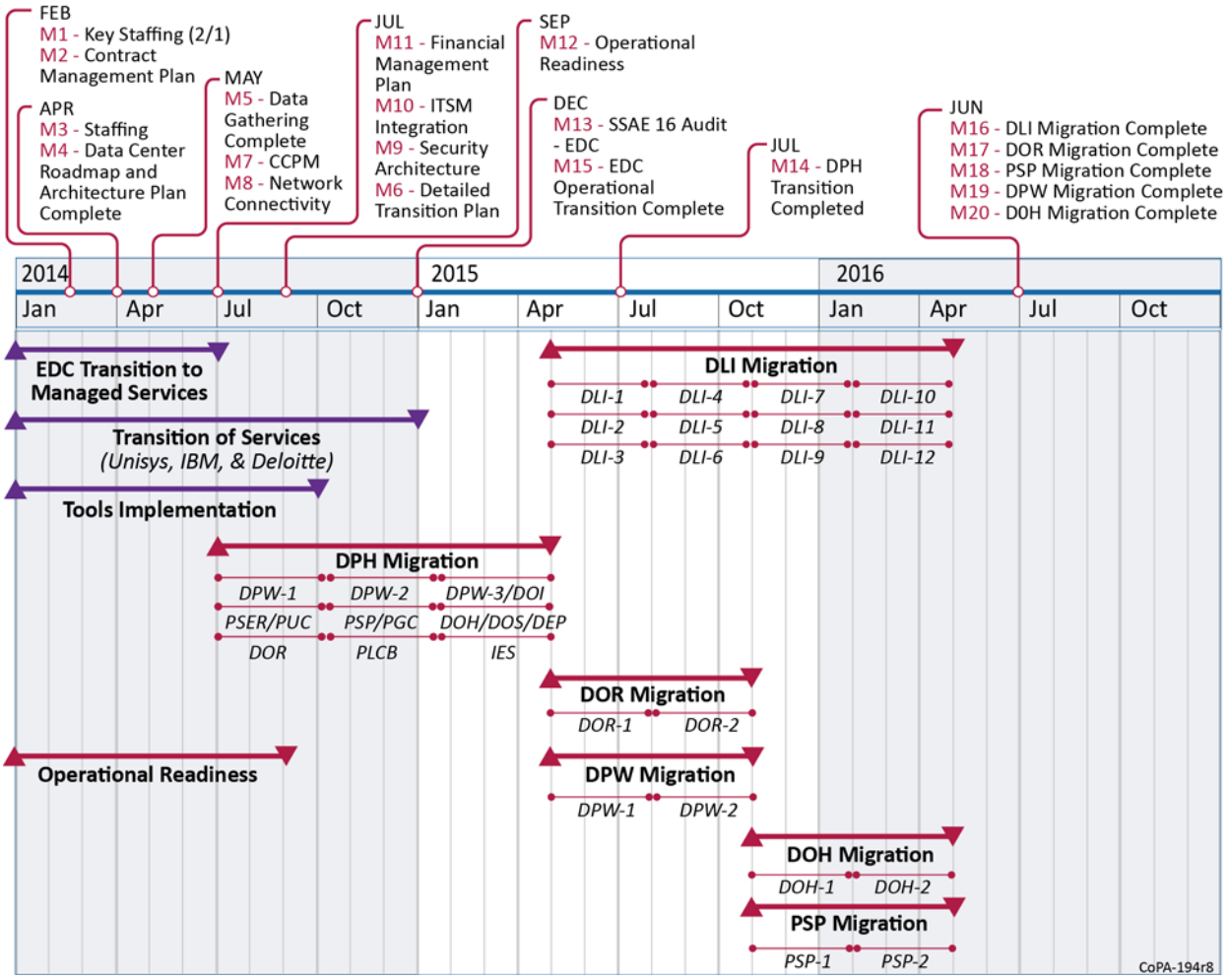


Figure M-9. Transition Schedule

Transition Controls

The Commonwealth Data Center Transition Program will implement three types of project controls to oversee the various projects and activities: Risk Management, Issue Management, and Change Management.

Transition Risk Management

Each Transition team member will document risks, as soon as they are identified, on the Transition Program Risks Log, along with an assessment of the severity, potential impact, and mitigation approach. The Transition Program Risks Log is a dynamic document, which will be reviewed weekly during the progress review meetings. Actions to address, eliminate, or mitigate the risks shall be included in the Transition Program Project Plan, and the Transition Program Issues and Risk Regiser shall be

cleared, as appropriate. Issues and risks that cannot be addressed by the Transition Managers will be escalated to the Program Steering Committee for resolution. The Transition Risks Management Process will follow five basic steps.

Step 1 – Risk Identification

Risk identification is an ongoing process, which is performed, monitored, and updated regularly. Unisys, the Commonwealth, and third parties can all raise concerns about new findings, which can represent issues or risks that can adversely affect the development of activities, the quality of services, or both.

All issues and risks are documented in a specifically defined, tangible item, which can be fully understood, and specific actions can be devised to mitigate or eliminate the problem. Once identified and clearly defined, the risk is documented on the Risk Register for review.

Step 2 – Risk Analysis

Once identified, the risk is will be analyzed to evaluate the events that can trigger the risk, probability of occurrence, and impact on the transition or business. These measures are relevant to determine risk response and priority to be adopted on a scale from lower impact/lower probability to high impact/high probability.

If the risk is determined to adversely affect the transition, the Transition and Project Managers will assign an owner to collect further information and derive options that can be used to mitigate or eliminate the risk.

Step 3 – Risk Mitigation Strategy Definition

This step will (1) analyze the options to mitigate or eliminate the risk and (2) define the risk response if the risk does occur. Basically, this is accomplished by outlining actions and activities to either prevent a risk from occurring or reduce the impact or consequences of its occurrence (or do both) as well as establishing in advance the contingency plan to be activated in case the efforts to prevent the risk fail. An important part of the risk mitigation strategy will be the definition of the level of control that shall be performed during the timeframe for the risk life cycle.

Step 4 – Risk Monitoring

Risks included on the Risk Register will be monitored systematically to understand whether the new events increase or decrease the probability and impact of occurrence in accordance with the level of control defined in the previous step. If changes in the risk parameters happen, the mitigation plan will be reviewed and the Risk Register updated, as appropriate.

Step 5 – Risk Closure

If during the monitoring process, the change to the risk parameters are related to a situation in which the event that triggers the risk, the probability of occurrence, or the impact on the business are no longer valid; the risk will be closed and the Risk Register updated accordingly.

Transition Issue Management

An issue is any item that is perceived as a problem, which is still not formally addressed for resolution. Similar to risk treatment, each team member will document issues, as soon as they are identified, on the Transition Issues and Actions Log. The Transition Issues and Actions Log will be a dynamic document, which contains both a description of the issue and the actions needed to address the issue, including the owners and deadlines for the planned actions.

The Transition Issues and Actions Log shall be reviewed weekly during the progress review meetings. Once the activities to address an issue are identified and agreed, these activities will be included on the Transition Schedule, and the Transition Issues and Actions Log shall be cleared, as appropriate. Issues that cannot be addressed by the Transition Managers will be escalated to the Program Managers for resolution.

The Issues Management process can be described in four basic steps.

Step 1 – Issue Identification

Issue identification is an ongoing process, which will be performed, monitored, and updated regularly. Unisys, the Commonwealth, and third parties can all raise concerns about new findings, which can represent issues that if not addressed promptly, can adversely affect the development of activities, the quality of the transition services, or both. All issues are to be documented on the Issues and Actions Log for review.

Step 2 – Issue Validation

The issue will be analyzed to determine its impact and priority. The issue will be assigned to the appropriate team or individual to identify the best alternative and the set of tasks needed for resolution, including accountability, ownership, and timeframe.

Step 3 – Issue Resolution

Once all the tasks including accountability, ownership, and timeframe, are identified and agreed for resolution, the tasks will be added to the Transition Schedule. From this point forward, the issue will be viewed as a normal requirement of the transition program, which has the tasks associated with its resolution and a standard process for monitoring progress.

Step 4 – Issue Closure

Once the tasks for resolution of the issue are added to the Transition Schedule, the issue will be closed, and the Issues and Actions Log will be updated accordingly. Also, Root Cause Analysis will be performed on common and problematic issues to identify trends and implement corrective actions, as appropriate.

Transition Change Management

Changes in the market, laws, regulations, and technology happen and affect the core business of all organizations. Consequently, changes affect projects and must be managed in an orderly way. Proper change control is essential to effectively manage

the transition program. The Change Management process is an integral part of the Unisys Service Transition Methods Framework. The Change Management process will follow five basic steps.

Step 1 – Establish the Need for a Change Request

Unisys, the Commonwealth, and third parties can all submit change requests. The change control process is essential to maintain the integrity of the project baseline and to manage the delivery schedules and corresponding acceptance criteria. The process is initiated by the submission of a Change Request Form. Some key tasks to create sound change requests are:

- Determine the impact of change on the transition schedule, budget, or both
- Determine the impact of change on the business processes
- Determine the impact of change on the contracted Service Level Agreement
- Determine the impact of change on the resources assigned to do the work
- Determine the impact of change on the associated costs and budget
- Determine the impact of change on any other activity and deliverable
- Assess the risks associated with the changes.

Step 2 – Evaluate the Change Requests

As a change request is received, it will be evaluated to determine if it should be approved. The Unisys Transition Manager will evaluate each request to determine the impact on the transition program. Key team members will be asked to participate in the change impact review, as appropriate. If the change request creates new risks, the risks will be added to the risk plan and factored into the impacts. Once the impacts are known, the values can be added to the Change Request Form. A Change Control Checklist will be used to help in these evaluations.

Change requests may also affect third parties. If third parties are affected, the Unisys Transition Manager will involve each vendor affected by the change to determine the impacts. These impacts will be included in the response given to the Commonwealth Transition Manager.

The Unisys Transition Manager, together with the Commonwealth Transition Manager, will have the ability to reject a change request if they believe the change is not in the transition program's best interests. Some change requests may be deferred instead of rejected if they are not critical to the program's success, and will be reviewed later when circumstances are best fit for discussing the subject.

Once the impacts are known, the Transition Managers will complete the change request with all pertinent information to submit for approval. Some key tasks during the evaluation step are:

- Review the urgency of the change, understand the impact of no action, and act accordingly, as appropriate

- Evaluate the ramification of all impacts and risks associated with the change and decide the next step to be followed: (1) approve changes with minimum impact; (2) reject changes that add no value to services; (3) request for additional or new information, as appropriate; (4) defer opportunity to review; or, (5) submit for analysis and decision of the Transition Steering Committee.

Step 3 – Obtain Change Request Approval

Once the change request is deemed necessary, the Transition Managers will determine if the change will be done by a change order or a contract amendment, depending on whether the nature of changes affects requirements that were originally in scope or the changes bring new requirements that did not belong to the original scope. Some key tasks in this step are:

- Complete the documents, including all information and evidence to support the decision
- Associate the urgency and priority with the change request
- Schedule the meeting for change request approval, including taking the necessary actions to expedite the process, as appropriate.

Step 4 – Submit the Change Order to the Transition Steering Committee

The Unisys Transition Manager will review with the Commonwealth Transition Manager all details of the change request for further approval or rejection. A deadline should be negotiated to approve or reject the request with a default position, with clear impact for no action until the deadline. The change request will then be submitted to the Program Governance Board for approval. The necessary tasks to execute the changes will be incorporated into the Transition Plan for further implementation.

Step 5 – Implement the Changes

Once the change request is formally approved, the following steps will complete the cycle:

- The necessary tasks to execute changes will be incorporated into the Transition Project Plan for implementation
- The Transition Program Change Management Log will be updated
- The executed documents will be sent to the appropriate Commercial Manager to be incorporated into the agreement's scope.

The results of the process will be communicated to the change initiator and all stakeholders affected by the change.

Transition Quality Assurance Plan Approach

Quality Management is to be conducted in accordance with the Commonwealth and Unisys Quality Management methods. The Unisys approach to Quality Management incorporates a set of standards by which Quality Management, Change Management,

Risk Management, and Reporting can be established and maintained. Establishing these standards will enable the project to be controlled and monitored so that deviations from the plan can be detected and addressed.

All deliverable work products are to be reviewed before submission to the Commonwealth. A combination of formal and informal, independent and joint (the Commonwealth and Unisys) reviews will be used. This will enable (1) requirements to be well understood and responded to, (2) issues and errors to be identified and promptly resolved, (3) rework to be minimized, and (4) formal acceptance processes that are trouble free.

During the Design phase, Unisys will review technical designs and plans. We will also conduct go/no-go reviews before cutting any services over from the current system to the new proposed system and require the Commonwealth's acceptance at the end of the cutover before the event is deemed successful. After each cutover, Unisys will conduct post-implementation reviews to capture lessons learned.

Unisys understands that testing is an integral part of a successful transition. Our methodology recommends testing of our solutions and reviewing test results before transitioning any services. Our approach also includes pilot testing, when possible, before full cutover of any services. This approach will help detect issues and limit the impact to only pilot test group users. Another feature of our Quality Management Plan is audits by the Unisys Project Quality Office (PQO). Unisys Quality Assurance staff may audit parts or all of the transition project's management and delivery. We will perform these audits by prior arrangement with the Unisys Engagement Executive.

Detailed Transition Plan

On the following pages, Unisys includes our Detailed Transition Plan for Commonwealth review.

CoPA Proposal Detail Schedule Level 5.pdf

Request for Proposal

RFP # 6100022698

Commonwealth of Pennsylvania
Office of Administration
Office for Information Technology
Data Center Computing Services

Schedule K

Key Program Deliverables

Table of Contents

INTRODUCTION –PROGRAM DELIVERABLES 3
KEY PROGRAM DELIVERABLES 3
D-01 Datacenter Architecture Plan and Roadmap 3
D-02 Commonwealth Computing Procedures Manual (CCPM) 5
D-03 Technology Architecture and Refresh Approach 15
D-04 IT Service Continuity Architecture and Plan 17
D-05 Transition Management Plan 18
D-06 Agency Level DR Plan(s) 19
D-07 Security Management Plan 20
D-08 Facilities Management Plan 22
D-09 Security Risk and Vulnerability Assessment Report 23
D-10 Gap Analysis Report 23
D-11 Contract Management Plan 24
DELIVERABLE ACCEPTANCE CRITERIA MATRIX 25
EXAMPLE - DELIVERABLE ACCEPTANCE MATRIX 27

Introduction –Program Deliverables

This Schedule sets forth certain obligations of Offeror regarding Program Deliverables. The Offeror must deliver to the Commonwealth any Key Program Deliverables as described below, in format and content acceptable to the Commonwealth.

As specified below, Offeror shall provide each Key Program Deliverable on or before the date specified in this Schedule. The Key Program Deliverable Acceptance Criteria and the Commonwealth Sign-off Matrix will be developed prior to the Effective Date and will be in the format referenced below in this document.

Key Program Deliverables

D-01 Datacenter Architecture Plan and Roadmap

The Datacenter Architecture Plan and Roadmap will include the Offeror's proposed Datacenter Architecture that will be utilized to support the Project. The Datacenter Architecture Plan and Roadmap should include at minimum sections that support the following:

- 2+ Datacenter Architecture (with EDC) - describes the overall Datacenter Architecture used in the delivery of the Offeror's Enterprise Datacenter Services. This should include details on datacenter specifications, location, physical security, and capacity. The architecture will show how the Commonwealth's Enterprise Data Center (EDC) will be incorporated into the Offeror's overall datacenter capacity.

- Datacenter Network Architecture - describes the required network connectivity between each of the datacenters. Included are connection requirements to the Commonwealth's network COPANET. The Offeror will also describe its Internet connection to the proposed Datacenter(s).

- Datacenter Security Architecture - describes the security architecture used to ensure the confidentiality, integrity and availability of Commonwealth information and infrastructure systems. The Security Architecture will describe the security technology components such as firewalls, intrusion detection devices, virus detection, etc. that will be utilized in the Offerors solution. Datacenter Security implementation activities must be conducted in accordance with, but not limited to, leading industry and Commonwealth standards such as ISO 27001:2005 and ISO 27002:2005.

- Datacenter Technology Environment - describes the Datacenter technology used in the delivery of the Offeror's Enterprise Datacenter Services. A summary of the planned allocation of platforms within each of the proposed datacenters should be included. Note: more detailed technology specifications shall be provided in the *D-03 Technology Architecture and Refresh Approach* deliverable.

- Datacenter Implementation Roadmap – presents the detailed implementation plan for the enablement of the overall Datacenter Architecture. The Datacenter Implementation Roadmap shall Reference roles and responsibilities, as well as critical dates and timelines.

EDC Assessment

D-01.01	Effective Date + 45 days	Offeror must assess the EDC facilities and provide a report to the Commonwealth as it pertains to: • Required security upgrades • Required HVAC and power upgrades • Required physical access to the EDC facility • Monitoring, maintain and reporting on EDC SLAs • Monitoring, maintaining and operating the installed infrastructure
Multi Datacenter Environment (2+ Architecture)		
D-01.02	Effective Date + 60 days – with quarterly updates	*Datacenter Architecture Plan and Roadmap* Datacenter Architecture Plan and Roadmap includes: • 2+ datacenter architecture (with/plus EDC) • Datacenter Network Architecture • Datacenter Security Architecture • Datacenter Technology Environment • Datacenter Implementation Roadmap Offeror must publish quarterly updates to the Datacenter Architecture Plan and Roadmap to include proposed updates to the technical architecture and implementation plan
Network and Security Architecture		
D-01.03	Effective Date + 60 days – with quarterly updates	*Datacenter Architecture Plan and Roadmap – Network and Security Architecture* The Network and Security Architecture - describes the network and security architecture to support the 2+ datacenter architecture.
Datacenter Architecture and Technology		
D-01.04	Effective Date +60 days– with quarterly updates	*Datacenter Architecture Plan and Roadmap* – Datacenter Technology The Datacenter Technology describes the technology used in the delivery of the Offeror's Enterprise Datacenter Services.
D-01.05	Effective Date +90 days – with quarterly updates	*Datacenter Architecture Plan and Roadmap* – Datacenter Technology Roadmap The Datacenter Technology Roadmap will identify specific, short-term steps and schedules for project of changes with estimated timings and cost impact to Commonwealth datacenter customers.
D-01.06	Effective Date + 180 days	*Datacenter Architecture Plan and Roadmap – Configuration Item Reconciliation* *The Configuration Item Reconciliation is the validation and update of the CMDB of record with the Offeror's configuration information including the EDC assets and CI's.*

Limited-Use Colocation Services		
D-01.07	Effective Date + 30 days	*Datacenter Architecture Plan and Roadmap*

D-02 Commonwealth Computing Procedures Manual (CCPM)

Offeror will develop documentation in accordance with the requirements in **Schedule H - Commonwealth Computing Procedures Manual (CCPM)**. This comprehensive services management manual will include, but not be limited to, the following sections as described in **Schedule H**:

- Organizational Overview
- Transition and Support Activities and Responsibilities
- IT Service Management Procedures
- Financial Management Procedures
- Contract Management Procedures
- Relationship Management Procedures
- Offeror Operational Procedures
- Commonwealth Customer Operations Manuals

Additional Planning Services		
D-02.01	Effective Date + 14 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide the initial version of the Commonwealth Computing Procedures Manual (CCPM) (see Schedule H CCPM Commonwealth Computing Procedures Manual) that includes Offeror's overall program and service management processes and procedures. The comprehensive manual includes the following sections: • Organizational Overview • Transition and Support Activities and Responsibilities • IT Service Management Procedures • Financial Management Procedures • Contract Management Procedures • Relationship Management Procedures • Offeror Operational Procedures • The Commonwealth Customer Operations Manuals PMO & Contract Management will focus on the bolded sections of the CCPM.
D-02.02	As needed during transition	After review and approval from the Commonwealth, Offeror must provide ongoing updates to the CCPM during the startup and transition phase
D-02.03	Yearly or as required	Offeror must provide CCPM updates as required as new services are added and yearly after the transition phase.

Availability/SLA Management		
D-02.04	Effective Date + 30 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must document the Availability and SLA Management approach and providing updates to the CCPM.
D-02.05	Effective Date +45 days	*Commonwealth Computing Procedures Manual (CCPM)* After review and approval from the Commonwealth, Offeror must review the Availability and SLA Management approach and project plan with Commonwealth stakeholders.
D-02.06	Monthly	*Commonwealth Computing Procedures Manual (CCPM)* SLA Achievement Report, detailing system availability, SLA attainment, and reason for outages.
D-02.07	As Needed	*Commonwealth Computing Procedures Manual (CCPM)* Root Cause Analysis (RCA) report for all major outages within SLA (e.g. hours/days of outage).
D-02.08	As requested	*Commonwealth Computing Procedures Manual (CCPM)* Ad hoc – Availability and SLA Reports
Change & Release Management		
D-02.09	Effective Date + 30 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must document the Change and Release Management approach and project plan updating appropriate sections to the CCPM.
D-02.10	Effective Date +45 days	*Commonwealth Computing Procedures Manual (CCPM)* After review and approval from the Commonwealth, Offeror must review the Change and Release Management approach and project plan with Commonwealth stakeholders.
D-02.11	Weekly	*Commonwealth Computing Procedures Manual (CCPM)* Weekly Change Management Meeting with the Change Advisory Board
D-02.12	Monthly	*Commonwealth Computing Procedures Manual (CCPM)* Monthly Change & Release Management summary report containing the number of changes, by platform, by Commonwealth organization, and status.
D-02.13	Yearly	*Commonwealth Computing Procedures Manual (CCPM)* On a yearly basis, randomly select completed Changes & Releases for detail auditing to determine compliance to policies. Create a summary report of the finding and make recommendations for improvements where appropriate.

D-02.14	Per Change Event	*Commonwealth Computing Procedures Manual (CCPM)* Complete Change Control & Release Management process for each change event adhering to the letter and spirit of the policy and process. Maintain a complete copy of the change / release for possible future audit.
Service Desk		
D-02.15	Effective Date + 30 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must document the Service Desk approach, organization, schedule and project plan.
D-02.16	Effective Date +45 days	*Commonwealth Computing Procedures Manual (CCPM)* After review and approval from the Commonwealth, Offeror must review the Service Desk approach and project plan with Commonwealth stakeholders
D-02.17	Effective Date + 60 days	*Knowledge Management Portal (KMP)* Offeror must provide a Knowledge/Service Management portal that describes the Offeror's contract information, pricing schedules, service offerings and operating procedures (operational, service delivery processes, SLAs, service ordering, etc.)
D-02.18	Effective Date +60 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide Commonwealth Computing Procedures Manual (CCPM) including but not limited to the following: Datacenter Operations, Change Management, Service Desk Operations, Security Management, Backup Management, Disaster Recovery, Performance Management, Asset Management, Service Level Management and Configuration Management. The Offeror must make the CCPM available on the Offeror's Knowledge/Service portal. See Schedule H Commonwealth Computing Procedures Manual (CCPM) for additional detail.
D-02.19	Effective Date +180 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must describe the process to keep separate and current specific sections of the CCPM dedicated to the operations of individual Commonwealth customers.
D-02.20	Effective Date +90 days	Knowledge Management Portal Offeror must provide Knowledge/Service portal training to authorized Commonwealth stakeholders
D-02.21	Weekly	*Commonwealth Computing Procedures Manual (CCPM)* Weekly summary report containing the type of incidents and problems being reported to the Service Desk. Identify measures being taken to reduce or eliminate stated incidents and problems.

D-02.22	Monthly	*Commonwealth Computing Procedures Manual (CCPM)* Monthly summary report containing the type of incidents and problems being reported to the Service Desk. Identify measures being taken to reduce or eliminate stated incidents and problems.
Account Management		
D-02.23	Effective Date + 30 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must document their Account Management approach and project plan.
D-02.24	Effective Date +45 days	*Commonwealth Computing Procedures Manual (CCPM)* After review and approval from the Commonwealth, Offeror must review the Account Management approach and project plan with Commonwealth stakeholders
D-02.25	Monthly	Monthly summary report containing the operational availability report on all systems in service, events and issues that occurred during the month. Report shall contain operational metrics by service platform, highlights and exceptions, and project status updates.
Configuration Management		
D-02.26	Effective Date + 30 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must document their Configuration Management approach, tool(s) and project plan.
D-02.27	Effective Date +45 days	*Commonwealth Computing Procedures Manual (CCPM)* After review and approval from the Commonwealth, Offeror must review the Configuration Management approach, tool(s) and project plan with Commonwealth stakeholders
D-02.28	As Requested	Offeror must provide Agency / Commonwealth level Configuration Management Reports
3rd Party License Management		
D-02.29	Effective Date + 30 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must document their 3rd Party License Management approach, tool(s) and project plan.
D-02.30	Effective Date +45 days	*Commonwealth Computing Procedures Manual (CCPM)* After review and approval from the Commonwealth, Offeror must review the 3rd Party License Management approach, tool(s) and project plan with Commonwealth stakeholders
D-02.31	Per request	Offeror must provide Software License Reports

Capacity Management		
D-02.32	Effective Date + 30 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must document their Capacity Management approach, tool(s) and project plan.
D-02.33	Effective Date +45 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must review the Capacity Management approach, tool(s) and project plan with Commonwealth stakeholders
D-02.34	Effective Date + 240 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must present the baseline Capacity Management Plan
D-02.35	Monthly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must issue periodic reports showing usage, trends, capacity forecasts, and recommendations for upgrades.
D-02.36	Annual	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide technology usage report (i.e. MIPS, vcpu, storage, etc.) by stakeholder and overall usage by the Commonwealth. The report must show monthly technology growth patterns by stakeholder.
Windows Support		
D-02.37	Effective Date + 30 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must present their roadmap and project plan to address the Windows Operations and Management including but not limited to the following; windows servers, backups, network connectivity, technical support, staffing, etc.
D-02.38	Effective Date + 45 days	*Commonwealth Computing Procedures Manual (CCPM)* After review and approval from the Commonwealth, Offeror must present plan to address the assessment recommendations identified in the Windows Operations and Management project plan.
D-02.39	Effective Date +60 days	*Commonwealth Computing Procedures Manual (CCPM)* Present a report describing the methodology the Offeror will follow to perform a Windows backups audit finding and recommendation to the Commonwealth Stakeholders, the audit report will include findings, recommendations, project plan and cost estimates.
D-02.40	Monthly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide SLA report(s). Provide a report detailing system availability, SLA attainment, reason for outages, and recommendations for improvements.

D-02.41	Quarterly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide Continuous Improvement Report. Provide a report detailing system availability and SLA attainment. Recommend system and cost improvements as appropriate.
Storage Management		
D-02.42	Effective Date + 30 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must present their roadmap and project plan to address Storage Management including but not limited to the following; data storage, backups, network connectivity, technical support, staffing, etc.
D-02.43	Effective Date + 45 days	*Commonwealth Computing Procedures Manual (CCPM)* After review and approval from the Commonwealth, Offeror must present plan to address the assessment recommendations identified in the Storage Management project plan.
D-02.44	Effective Date +60 days	*Commonwealth Computing Procedures Manual (CCPM)* Present a report describing the methodology the Offeror will follow to perform a system backups audit finding and recommendation to the Commonwealth Stakeholders, the audit report will include findings, recommendations, project plan and cost estimates.
D-02.45	Monthly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide SLA report(s). Provide a report detailing system availability, SLA attainment, reason for outages, and recommendations for improvements.
D-02.46	Quarterly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide Continuous Improvement report(s). Provide a report detailing system availability and SLA attainment. Recommend system and cost improvements as appropriate.
ERP Hosting – SAP / Oracle		
D-02.47	Effective Date + 30 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must present their roadmap and project plan to address ERP Hosting including but not limited to the following; data storage, backups, network connectivity, technical support, staffing, etc.
D-02.48	Effective Date + 45 days	*Commonwealth Computing Procedures Manual (CCPM)* After review and approval from the Commonwealth, Offeror must present plan to address the assessment recommendations identified in the ERP Hosting project plan.

D-02.49	Effective Date +60 days	*Commonwealth Computing Procedures Manual (CCPM)* Present a report describing the methodology the Offeror will follow to perform a system backup audit finding and recommendation to the Commonwealth Stakeholders, the audit report will include findings, recommendations, project plan and cost estimates.
D-02.50	Monthly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide SLA report(s). Provide a report detailing system availability, SLA attainment, reason for outages, and recommendations for improvements.
D-02.51	Quarterly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide Continuous Improvement report(s). Provide a report detailing system availability and SLA attainment. Recommend system and cost improvements as appropriate.
UNIX Support – AIX / Linux		
D-02.52	Effective Date + 30 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must present their roadmap and project plan to address UNIX Support including but not limited to the following; data storage, backups, network connectivity, technical support, staffing, etc.
D-02.53	Effective Date + 45 days	*Commonwealth Computing Procedures Manual (CCPM)* After review and approval from the Commonwealth, Offeror must present plan to address the assessment recommendations identified in the UNIX Support project plan.
D-02.54	Effective Date +60 days	*Commonwealth Computing Procedures Manual (CCPM)* Present UNIX audit finding and recommendation to the Commonwealth Stakeholders, the report will include findings, recommendations, project plan and cost estimates.
D-02.55	Monthly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide SLA report(s). Provide a report detailing system availability, SLA attainment, reason for outages, and recommendations for improvements.
D-02.56	Quarterly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide Continuous Improvement report(s). Provide a report detailing system availability and SLA attainment. Recommend system and cost improvements as appropriate.

Mainframe Services		
D-02.57	Effective Date + 30 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must present their roadmap and project plan to address Mainframe Support (IBM & Unisys) including but not limited to the following; data storage, backups, network connectivity, technical support, staffing, etc.
D-02.58	Effective Date + 45 days	*Commonwealth Computing Procedures Manual (CCPM)* After review and approval from the Commonwealth, Offeror must present project plan to address the assessment recommendations identified in the Mainframe Support (IBM & Unisys) plan.
D-02.59	Effective Date +60 days	*Commonwealth Computing Procedures Manual (CCPM)* Present mainframe audit finding and recommendation to the Commonwealth Stakeholders, the report will include findings, recommendations, project plan and cost estimates.
D-02.60	Monthly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide SLA report(s). Provide a report detailing system availability, SLA attainment, reason for outages, and recommendations for improvements.
D-02.61	Quarterly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide Continuous Improvement report(s). Provide a report detailing system availability and SLA attainment. Recommend system and cost improvements as appropriate.
Database Management Services		
D-02.62	Effective Date + 30 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must document their Database Management approach, tool(s) and project plan.
D-02.63	Effective Date +45 days	*Commonwealth Computing Procedures Manual (CCPM)* After review and approval from the Commonwealth, Offeror must review the Database Management approach, tool(s) and project plan with Commonwealth stakeholders
D-02.64	Effective Date +60 days	*Commonwealth Computing Procedures Manual (CCPM)* Present backup audit finding and recommendation to the Commonwealth Stakeholders, the report will include findings, recommendations, project plan and cost estimates.
D-02.65	Effective Date	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide Database Management Service Architecture document (Oracle, Sybase, and MS SQL).

D-02.66	Monthly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide Database Management Service Usage Reports
Server Capacity on Demand		
D-02.67	Effective Date + 30 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must document their Server Capacity on Demand approach, tool(s) and project plan.
D-02.68	Effective Date +45 days	*Commonwealth Computing Procedures Manual (CCPM)* After review and approval from the Commonwealth, Offeror must review the Server Capacity on Demand approach, tool(s) and project plan with Commonwealth stakeholders
D-02.69	Quarterly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must host a quarterly meeting with the Commonwealth to review current server utilization on all managed server platforms and locations, and forecast future quarter's server processing requirements. Recommendations to increase capacities will be made, when approved by the Commonwealth; the additional equipment will be scheduled for deployment.
Storage Capacity on Demand		
D-02.70	Effective Date + 30 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must document their Storage Capacity on Demand approach, tool(s) and project plan.
D-02.71	Effective Date +45 days	*Commonwealth Computing Procedures Manual (CCPM)* After review and approval from the Commonwealth, Offeror must review the Storage Capacity on Demand approach, tool(s) and project plan with Commonwealth stakeholders
D-02.72	Quarterly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must host a quarterly meeting with the Commonwealth to review current SAN storage utilization on all managed SAN platforms and locations, and forecast future quarter's SAN storage requirements. Recommendations to increase capacities will be made, when approved by the Commonwealth; the additional equipment will be scheduled for deployment.
DR Infrastructure on Demand		
D-02.73	Quarterly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must host a quarterly meeting with the Commonwealth to review current disaster recovery service and capabilities, and forecast future quarter's disaster recovery requirements. Recommendations to increase capacities will be made, when approved by the Commonwealth, the additional equipment and services will be scheduled for deployment.

Additional Technical Services		
D-02.74	Monthly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide a monthly report on technical support services usage by Commonwealth datacenter customer.
Limited-Use Colocation Services		
D-02.75	Effective Date + 30 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must document their approach, tool(s) and project plan for supporting Limited-Use Colocation Services.
D-02.76	Effective Date +45 days	*Commonwealth Computing Procedures Manual (CCPM)* After review and approval from the Commonwealth, Offeror must review the Limited-Use Colocation Services approach, tool(s) and project plan with Commonwealth stakeholders
D-02.77	Effective Date +60 days	*Commonwealth Computing Procedures Manual (CCPM)* Present backup audit finding and recommendation to the Commonwealth Stakeholders, the report will include findings, recommendations, project plan and cost estimates.
D-02.78	Monthly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide Limited-Use Colocation Services Usage Reports
Performance Monitoring & Management		
D-02.79	Monthly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide monthly summary report containing the performance level achieved for each system being monitored. This report will be reviewed with the Commonwealth and plans will be made to address system utilization as appropriate.
D-02.80	Daily	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide daily reports containing the performance level achieved for each system being monitored. Daily reports summarizing incidents for the past 24-hours and immediate reports of incidents and routine status reports of incidents in progress for resolution such as a network or server outage that impacts a facility and our business. These reports will be reviewed with the Commonwealth and plans will be made to address system utilization as appropriate.

Transition Program Management		
D-02.81	Effective Date + 60 days	*Commonwealth Computing Procedures Manual (CCPM)* Establish Interim Contract Management Procedures during the transition of datacenter services. Offeror must describe an interim procedure to monitor and manage service delivery including but not limited to the following; Problem Management, Change Management, Service Level monitoring and reporting, physical and logical security, project management, etc. while the service is transitioned from the Commonwealth to the Offeror.
D-02.82	Weekly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide Transition Status reports, including any schedule variance that cannot be remediated will trigger the escalation procedures outlined in the Transition Plan/Agreement, which will be developed during Transition.
Security & Firewall		
D-02.83	Quarterly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide Continuous Improvement report. Provide a report detailing system availability and SLA attainment. Recommend system and cost improvements as appropriate.

D-03 Technology Architecture and Refresh Approach

The Technology Architecture and Refresh Approach will include the Offeror's proposed the Technology that will be utilized to support the architecture and delivery of services across all platform and services. The Technology Architecture and Refresh Approach should include at minimum sections that support the following:

- Datacenter Technology - describes the technology used in the delivery of the Offeror's Enterprise Datacenter Services. The technology descriptions should include hardware, software that will be included in the overall solution delivery. The technology should also include a complete list of those Service Level measurement and monitoring tools that will be used to measure and report Offeror's performance of the Services at a level of detail sufficient, as determined by the Commonwealth, to verify Offeror's compliance with those Service Levels described in **Schedule J.1 Datacenter Service Level Management** as of the Effective Date.

- Datacenter Technology Roadmap - will identify specific, short and long term steps and schedules for planned and proposed future changes with estimated timings and cost impact to Commonwealth datacenter customers. This should be the basis for generation of technology roadmaps which will include schedules, dependencies and requirements for introduction of new technology changes as well as acquisition, support, and retirement of current software/hardware.

- Configuration Item Reconciliation - is the validation and update of the CMDB of record with the Offerors configuration information including the EDC assets and Configuration Items (CI's).

Technology Refresh		
D-03.01	Effective Date + 30 days	*Technology Architecture and Refresh Approach* Offeror must document the following Technical Architecture approach and project plan including; Service Catalog, IT Architecture, and Technical support
D-03.02	Effective Date +45 days	*Technology Architecture and Refresh Approach* After review and approval from the Commonwealth, Offeror must review the Technical Architecture approach and project plan with Commonwealth stakeholders
D-03.03	Effective Date + 60 days	Offeror must identify the technical architecture organization and staff.
Infrastructure Architecture		
D-03.04	Effective Date + 45 days	*Technology Architecture and Refresh Approach* Offeror must document the approach and project plan for the computing infrastructure architecture and review with Commonwealth Stakeholders
D-03.05	Effective Date + 45 days	*Technology Architecture and Refresh Approach* After review and approval from the Commonwealth, Offeror must document the approach and project plan for the network architecture to connect Offeror's datacenter(s), review with Commonwealth Stakeholders
D-03.06	As requested by Commonwealth Stakeholders	*Technology Architecture and Refresh Approach* Offeror must describe the process to request a review new technologies evaluations by Commonwealth datacenter customers.
D-03.07	Per request – prior to a new application infrastructure service	*Technology Architecture and Refresh Approach* Offeror must provide Infrastructure Architecture Design Reports
Performance Monitoring & Management		
D-03.08	Effective Date + 30 days	*Technology Architecture and Refresh Approach* Offeror must document their Performance Monitoring and Management approach, tool(s) and project plan.
D-03.09	Effective Date +45 days	*Technology Architecture and Refresh Approach* After review and approval from the Commonwealth, Offeror must review the Performance Monitoring and Management approach, tool(s) and project plan with Commonwealth stakeholders

D-04 IT Service Continuity Architecture and Plan

The IT Service Continuity Architecture and Plan will include the Offeror's proposed Disaster Recovery (DR) solution architecture. The DR solution architecture will describe how the Offeror will deliver multiple tiers of disaster recovery services. The IT Service Continuity Architecture and Plan will also describe the Offeror's approach to reviewing the Commonwealth's current DR Plans and the updating of those plans in coordination with the Commonwealth.

IT Service Continuity Architecture		
D-04.01	Effective Date + 30 days	*IT Service Continuity Architecture and Plan* Offeror must describe their methodology for reviewing and refreshing technology on a scheduled basis.
D-04.02	Effective Date + 30 days	*IT Service Continuity Architecture and Plan* Offeror must provide an IT Service Continuity Architecture and Plan to Implement DR solution
D-04.03	30 days prior to transition of each critical application	*IT Service Continuity Architecture and Plan* Offeror must describe their approach to providing Develop/Update Agency Application DR and Business Recovery Plan(s)
D-04.04	Depending on DR Tier Solution • Current DR • Tier 0 • Tier 1 • Tier 2 • Tier 3 • Tier 4	*IT Service Continuity Architecture and Plan* Offeror must develop a plan to transition agencies to Tiered DR Solution • Currently have DR (DPH) – at time of transition • Tier 0 – Transition + 90 days • Tier 1 – Transition + 60 days • Tier 2 – Transition + 30 days • Tier 3 – at time of transition • Tier 4 – at time of transition
DR Planning & Testing		
D-04.05	Effective Date + 30 days	*IT Service Continuity Architecture and Plan* Offeror must document their Tiered Disaster Recovery approach, tool(s) and project plan.
D-04.06	Effective Date +45 days	*IT Service Continuity Architecture and Plan* After review and approval from the Commonwealth, Offeror must review their Tiered Disaster Recovery approach, tool(s) and project plan with Commonwealth stakeholders

D-04.07	Monthly	*IT Service Continuity Architecture and Plan* Offeror must provide report(s) describing schedule of stakeholder participation in DR solution

D-05 Transition Management Plan

The Transition Management Plan will provide a detailed overview of the Offeror's transition management approach, process and procedures. The Transition Management Plan will describe the enablement of the Transition Project Management Office (TPMO) and also provide a detailed implementation schedule of transition activities and milestones. The Transition Management Plan should include at minimum sections that support the following:

- Transition Management Approach
- Transition Project Management Office (TPMO) Organization and Responsibilities
- Transition Management Communications Plan
- Transition Schedule

Transition Management (New Customer and/or Services)		
D-05.01	Effective Date + 60 days	*Transition Management Plan* Offeror must create a Transition Roadmap with major milestones and present it to the Commonwealth for review
D-05.02	Effective Date + 90 days	*Transition Management Plan* After review and approval from the Commonwealth, Offeror must create a Detailed Transition Project Plan with major milestones and present it to the Commonwealth for review
D-05.03	Weekly	*Transition Management Plan* Offeror must create a report for the Commonwealth detailing the transition projects on the plan, status, schedule, risks, and the forecasted transition date.
Transition Program Management		
D-05.04	Effective Date + 60 days	*Transition Management Plan* Offeror must present their approach to transition Commonwealth computing assets. The approach must include a roadmap and project plan to successfully transition Commonwealth computing assets using the schedule identified in the RFP
D-05.05	Effective Date + 90 days	*Transition Management Plan* Present and review the transition roadmap and plan to Commonwealth stakeholders.

D-05.06	Effective Date + 60 days	*Transition Management Plan* Establish Interim Contract Management Procedures during the transition of datacenter services. Offeror must describe an interim procedure to monitor and manage service delivery including but not limited to the following; Problem Management, Change Management, Service Level monitoring and reporting, physical and logical security, project management, etc. while the service is transitioned from the Commonwealth to the Offeror.
D-05.07	Effective Date + 60 days	*Transition Management Plan* EDC / Legacy Datacenter Infrastructure Maintenance Strategy – Offeror must document their strategy as it related to providing a solution to the infrastructure maintenance expiration issue at the EDC and any other datacenter that has the same or similar issue.
D-05.08	Effective Date + 60 days	*Transition Management Plan* Offeror must provide the procedure to standup their Transition Management Office
D-05.09	Weekly during transition	*Transition Management Plan* Offeror must provide Transition Status reports, including any schedule variance that cannot be remediated will trigger the escalation procedures outlined in the Transition Plan/Agreement, which will be developed during Transition.
Security Transition Activities		
D-05.10	Effective Date + 60 days	*Transition Management Plan* Offeror must provide their Security Transition Plan
D-05.11	Weekly updates during transition	*Transition Management Plan* Offeror must provide their Security Transition Status Report(s)

D-06 Agency Level DR Plan(s)

The Offeror is required to assist the Commonwealth Agencies with updates to or development of their current DR Plans (DRPs). These Agency Level DR Plans will reflect the Offeror's DR approach and solution for DR testing. The following describes the Offeror's responsibilities regarding the updating of Agency Level DRPs:

- Within six (6) months after the Effective Date, Offeror shall complete the update all existing Agency-specific Disaster Recovery Plans and technical recovery guides to reflect all changes implemented to the Services infrastructure prior to or during the performance of Transition Services.
- For Applications lacking tested Disaster Recovery Plans, Offeror shall work with Commonwealth Agencies to complete a gap analysis of the current Disaster Recovery

Plans and technical recovery guides compared to the requested recovery time objective, as specified in **Schedule J.1 Datacenter Service Level Management**, and update the Disaster Recovery Plans with the results within forty-eight (48) months after the Effective Date.

- For Agencies without a Disaster Recovery Plan, the Offeror shall work with Agencies to develop a basic Disaster Recovery Plan and technical recovery guides within eighteen (18) months after the Effective Date.

DR Planning & Testing		
D-06.01	Monthly	*Agency Level DR Plan* Offeror must provide report(s) describing the schedule of DR test being performed by stakeholders
D-06.02	Monthly	*Agency Level DR Plan* Offeror must provide report(s) describing the results of stakeholder DR test
D-06.03	As requested– Per Agency Critical Application	*Agency Level DR Plan* Offeror must provide DR Test Plans as required

D-07 Security Management Plan

The Security Management Plan will address the overall security management for the planned facility security implementation for the EDC, the Offeror Facilities, software and equipment deployment specifically for data and online security, annual security assessments and other standard security concepts for ensuring the safety, security and confidentiality of Commonwealth Data.

The Security Management Plan shall include a complete description of the personnel security management program. It shall comply with background check requirements specified in the Terms and Conditions and shall provide a methodology for ongoing evaluation and reporting of any change in status of Offeror personnel that would negatively impact their ability to continue to meet Commonwealth or Agency security requirements.

Security Management		
D-07.01	Effective Date + 30 days	*Security Management Plan* Offeror must document their Security Management approach, tool(s) and project plan.
D-07.02	Effective Date +45 days	*Security Management Plan* After review and approval from the Commonwealth, Offeror must review their Security Management approach, tool(s) and project plan with Commonwealth stakeholders.

D-07.03	Quarterly	*Security Management Plan* Offeror must provide the Commonwealth with a report containing the detailed results of the Vulnerability Analyses testing. Include any remediation activities that are required.
D-07.04	Monthly	*Security Management Plan* Offeror must provide the Commonwealth with the detailed monthly Security Log Analysis report. Include any remediation activities that are required.
D-07.05	Ongoing	*Security Management Plan* Offeror must maintain a hardcopy file of all security access changes. The copy will contain the date, time, file changes, access rights applied and the name of the security officer completing the access request.
Security & Firewall		
D-07.06	Effective Date + 30 days	*Security Management Plan* Offeror must document their Security and Firewall approach, tool(s) and project plan.
D-07.07	Effective Date +45 days	*Security Management Plan* After review and approval from the Commonwealth, Offeror must review the Security and Firewall approach, tool(s) and project plan with Commonwealth stakeholders
D-07.08	Monthly	*Security Management Plan* Threat Assessment and Analysis Report. Provide a monthly report detailing the threat assessments, volume and major types of malware detected, volume of SPAM rejected, corrective actions, and recommendations that would improvement security of Commonwealth systems.
D-07.09	Monthly	*Security Management Plan* Offeror must provide SLA reports. Provide a report detailing system availability, SLA attainment, reason for outages, and recommendations for improvements, security incident notification, and security change request intervals and results.
D-07.10	Monthly	*Security Training and On-boarding Status Report* Offeror must provide a monthly Security Training and On-boarding Status Report detailing security training, changes to project personnel, and background check status and results.

D-08 Facilities Management Plan

The Facilities Management Plan will address management for both the EDC facility and the proposed Offeror's facility(s). The Facilities Management Plan should describe the Offeror's plan for providing and managing the physical environment. For example; power and power distribution, cooling and ventilation, fire detection and suppression, building security and access control, and environmental monitoring. Provide an approach for yearly review and self-verification that the datacenters will be managed, maintained and operated at the equivalent of Uptime Institute of Tier 3 rating. The plan should also address how the Offeror will support SSAE-16 compliance audits.

Facilities Architecture / Maintenance		
D-08.01	Effective Date + 60 days	*Facilities Management Plan* Offeror must present their assessment of the EDC and any required facility changes/modification required to upgrade the facility to meet service level objectives. The assessment must include a roadmap and project plan to make any required facility modifications.
D-08.02	Effective Date + 365 days	*Facilities Management Plan* Present results of the SSAE 16 audit of the EDC and all other datacenters used by the Offeror to provide computing services to Commonwealth shareholders.
D-08.03	Monthly	*Facilities Management Plan* Offeror must provide monthly Facilities SLA Report, detailing environmental equipment availability, SLA attainment, and reason for outages.
D-08.04	Quarterly	*Facilities Management Plan* Offeror must provide quarterly Facility service improvement report. Report changes and improvements to the facility or the maintenance of the facilities.
D-08.05	Annual	*Facilities Management Plan* Offeror must provide annual SSAE 16 audit reports for each datacenter facility being used to support the Commonwealth.
Site Operations		
D-08.06	Effective Date + 60 days	*Facilities Management Plan* Offeror must present their assessment of the EDC monitoring and staffing changes/modification required to upgrade the facility to meet Commonwealth service level objectives. The assessment must include a roadmap and project plan to make any required monitoring and staffing modifications.

D-08.07	Effective Date + 90 days	*Facilities Management Plan* Present plan to address the assessment recommendations identified in the EDC monitoring, project plan and staffing report.
D-08.08	Daily, Monthly	*Facilities Management Plan* Offeror must provide daily and monthly SLA report(s), detailing environmental equipment availability, SLA attainment, and reason for outages.
D-08.09	Quarterly	*Facilities Management Plan* Offeror must provide quarterly site operations improvement report. Identify changes or improvements to the site operations that would assist the Offeror in meeting the agreed facility SLAs.

D-09 Security Risk and Vulnerability Assessment Report

The Offeror will execute a Baseline Security Risk and Vulnerability Assessment. The assessment report must include a roadmap and project plan to make any required security modifications prior to final transition of services.

Security Transition Activities		
D-09.01	Effective Date + 60 days	*Security Risk and Vulnerability Assessment Report* Offeror must execute a Baseline Security Risk and Vulnerability Assessment. The assessment must include a roadmap and project plan to make any required security modifications.
D-09.02	Effective Date + 90 days	*Security Risk and Vulnerability Assessment Report* Present results of the Security Risk and Vulnerability assessment along with a Roadmap and Project Plan to address the recommendation identified in the assessment.

D-10 Gap Analysis Report

The Offeror will execute a Data Center Gap Analysis. The analysis report must identify gaps in the current data centers and the Offeror's recommendations and corrective approach.

Gap Analysis Activities		
D-10.01	Effective Date + 120 days	*Gap Analysis Report* Offeror must execute a Data Center Gap Analysis. The analysis must include gaps identified and a roadmap and project plan to institute any recommendations and corrective actions.

D-10.02	Effective Date + 150 days	*Gap Analysis Report* Present results of the Data Center Gap Analysis along with a Roadmap and Project Plan to address the recommendations identified in the analysis.

D-11 Contract Management Plan

The Contract Management Plan will address management for the overall contract. The Contract Management Plan should describe the Offeror's plan to ensure it is adhering to the terms and conditions of the contract and providing the services/products that meet the requirements of the project. The Contract Management Plan must identify the activities to be performed or initiated to manage, track, amend, and close the contract. The Contract Management Plan must include but is not limited to: participants roles and responsibilities, task accomplishment plan, status reports, deliverable management, contact performance management, risk management, and contract closeout.

Contract Management Plan		
D-11.01	Effective Date + 45 days	*Contract Management Plan* Offeror must document its Contract Management approach, tool(s) and project plan.
D-11.02	Effective Date + 60 days	*Contract Management Plan* After review and approval from the Commonwealth, Offeror must review its Contract Management approach, tool(s) and project plan with Commonwealth stakeholders.

Deliverable Acceptance Criteria Matrix

This section is provided for the Offeror to understand the process the Commonwealth will use for acceptance of Deliverables/Milestones that are committed to in the RFP. The Matrix provided below is an example of the template that will be used to capture Deliverables/Milestones and other information related to the acceptance process.

It is critical to the success of the Data Center Computing Services project that the deliverable acceptance process is thorough and that any deficiencies are addressed as early as possible to minimize impacts to the Services. Designated Commonwealth working teams will be reviewing the Deliverables/Milestones throughout the phases of development. The Offeror will solicit input from the Commonwealth team members as the items are developed with the goal of understanding expectations in advance so as to obtain acceptance upon delivery. Feedback and suggestions received from the Commonwealth must be incorporated into the Deliverables/Milestones. The Commonwealth will identify the individuals authorized to provide formal Acceptance Approval / Nonconformance notification to the Offeror for the Deliverables/Milestones. The deliverable acceptance process will comply with the following guidelines and be formally documented in the Commonwealth Computing Procedures Manual (CCPM).

1. The Offeror will give written notice to the Commonwealth that a Deliverable / Milestone is complete.
2. A walk-through review of the Deliverable and/or Milestone will be scheduled by the Offeror seven (7) days following the issuance of the written notice to the Commonwealth. The purpose of the walk-through is to provide a forum for discussion and review of the Transition Deliverable / Milestone with the approver/s. If additional review, physical inspection, on-line access or backup information is required, the Commonwealth will notify the Offeror at this time.
3. The Commonwealth will provide the Offeror with notice that the Deliverable / Milestone is Accepted or notice of Noncompliance no later than seven (7) days after the walk-through, fourteen (14) days after notice of completion.
4. If the Commonwealth does not provide notice to the Offeror of their Acceptance or Nonconformance within fourteen (14) days of notice of completion, the Offeror will give the Commonwealth written notice that the request was not received and the Acceptance Review Period will be extended an additional seven (7) days.
5. The Enterprise Datacenter Services Transition Management Committee will review all Deliverable / Milestones which have not received written notice of Acceptance or Noncompliance within fourteen (14) days after notice of completion. The Enterprise Datacenter Services Transition Management Committee's goal is to determine and document the Commonwealth and Offeror actions necessary to complete the review minimizing any potential delays to the project and addressing any substantive issues.
6. For any Deliverables / Milestones which are found to be Noncompliant, the Offeror will address the nonconformity (and any other problems of which it has knowledge) and redeliver the item to the Commonwealth using the process outlined above.

The status of each Deliverable and any associated issues will be managed through a monthly deliverables review meeting between the Commonwealth and the Offeror. The objective of the meeting is to review the status of all deliverables, communicate deliverable owners and

deliverable recipients for upcoming deliverables, review rejected deliverables and remediation plans for those deliverables.

Example - Deliverable Acceptance Matrix

Reference #	Deliverable / Milestone Name	Due Date	Acceptance Criteria	Monthly Credit
D-01	Datacenter Architecture Plan and Roadmap		➢	
D-02	Commonwealth Computing Procedures Manual (CCPM)		➢	
D-03	Technology Architecture and Refresh Approach		➢	
D-04	IT Service Continuity Architecture and Plan		➢	
D-05	Transition Management Plan		➢	
D-06	Agency Level DR Plan(s)		➢	
D-07	Security Management Plan		➢	
D-08	Facilities Management Plan		➢	
D-09	Security Risk and Vulnerability Assessment Report		➢	
D-10	Gap Analysis Report		➢	
D-11	Contract Management Plan		➢	

UNISYS RESPONSE:

The Commonwealth identified 11 Key Program Deliverables specified within Schedule K with prescriptive Program Deliverables detailing specific timeframes, milestones within the deliverable and criteria to be met for each deliverable to be considered acceptable. This section discusses the approach we will take to comply with the deliverables set forth in Schedule K. The Unisys Team understands that Key Program Deliverables will be subject to deliverable acceptance criteria and Commonwealth approval documented on the Commonwealth Sign-off Matrix. This matrix will be developed prior to the effective date of the contract in the format referenced in Schedule K.

Considering the aggressive timelines associated with key program deliverables, it is important that clarity on acceptance criteria be established early to ensure that completed deliverables meet the needs of the Commonwealth without requiring rework. It is our responsibility to define and agree upon the expectations in advance to provide deliverables that are compliant with Commonwealth anticipated finished products. We will do this through collaboration with the designated Commonwealth working teams to review deliverables and milestones throughout the phases of development.

The Key Program Deliverables provide a strong foundation upon which the Data Center Services Computing Program will be established. These deliverables are critical to the success of our transition and future programs, so tasks associated with their completion have been highlighted in our transition plan. In **Schedule M: Transition Plan**, the Unisys Team provides tasks and milestones that mirror the Commonwealth's Key Program Deliverables within our Transition of Services (ToS) projects. The Transition Plan can be found in **Attachment 9 of Section 3.0 – Schedule M: Transition Plan** of this proposal.

During the ToS project, Unisys, IBM, and Deloitte subject matter experts (SMEs) will work with the Commonwealth to identify the appropriate format, content, and timing as well as deliver the first occurrence of each report or plan as appropriate. During transition, the TPMO will oversee the production of the deliverables. For deliverables intended to be produced periodically throughout the agreement's duration, the Transition SME will review them with the appropriate Commonwealth stakeholder for approval and then with the appropriate steady state resources to provide knowledge transfer of the process, source of data, required timing, and stakeholders. After turnover, the PMO will oversee the production of the deliverables.

The Unisys Team and the Commonwealth will meet on a monthly basis to review the status of each deliverable and any associated issues. In addition to providing status, this meeting will provide the opportunity for direct communication

between deliverable owners and deliverable recipients for upcoming deliverables, and a review of rejected deliverables and remediation plans for those deliverables.

Unisys will work with the Commonwealth to formalize the deliverable acceptance criteria and process. The Commonwealth will identify the individuals authorized to provide formal acceptance approval or nonconformance notification to Unisys following receipt of the deliverable. The deliverable acceptance process will be defined and subsequently documented in the Commonwealth Computing Procedures Manual (CCPM). Minimally, this process will comply with the following Commonwealth guidelines:

- Unisys will give written notice to the Commonwealth that a deliverable or its milestone is complete.
- Unisys will schedule a walk-through review of the deliverables and/or milestones seven days following the issuance of the written notice to the Commonwealth.
- The Commonwealth will provide Unisys with notice that the deliverable and/or milestone has been accepted or does not comply within seven days after the walk-through, 14 days after the Unisys notice of completion.
- If the Commonwealth does not provide notice to Unisys of their acceptance or nonconformance within 14 days of notice of completion, Unisys will provide written notice to the Commonwealth that the request was not received and the acceptance review period will be extended an additional seven days.
- The Enterprise Data Center Services Transition Management Committee will review deliverable/milestones which have not received written notice of acceptance or noncompliance within 14 days after notice of completion. This committee's goal is to determine and document the Commonwealth and Unisys actions necessary to complete the review minimizing any potential delays of the project and addressing any substantial issues.
- For any deliverables/milestones which are found to be noncompliant, Unisys will address the nonconformity and redeliver the item to the Commonwealth using this process.

D-01 – Data Center Architecture Plan and Roadmap

The Data Center Architecture Plan and Roadmap will be developed during the early stages of the Data Center Migration project's planning. This deliverable consists of seven major milestones that are due within the first 30 to 180 days of contract effective date. Specific data centers will be chosen for each application, and detailed plans will be developed to provide for the workloads targeted for each center.

Key to the Data Center Plan will be the use of the Enterprise Data Center (EDC), which will be evaluated for deficiencies that need to be remediated to provide the level of services required by the Commonwealth. The plan's other components will include technical specifications of the target data centers and tools that will be used to support the service levels required.

D-02 – Commonwealth Computing Procedures Manual (CCPM)

The Commonwealth Computing Procedures Manual (CCPM) deliverable consists of 83 milestones to be delivered from 30 to 180 days of contract start, and on a regular basis throughout steady state of the contract. The CCPM will be developed during the Transition of Services project and maintained throughout the agreement's duration as a tool for communicating how the Commonwealth and Unisys Team should interact in specific situations and how Unisys will support your technologies. This document is to be used by each Commonwealth Agency using Data Center Computing Services, all key personnel supporting the operations of the Data Center Computing Services, all Technical Support Services Teams for all platforms, the subcontractors and Small Diverse Business partners and the Bureau of Enterprise Services (BES). For additional details, please refer to **Attachment 7 to Section 3.0 – Schedule H: Commonwealth Computing Procedures Manual (CCPM).**

D-03 – Technology Architecture and Refresh Approach

The Technology Architecture and Refresh Approach is a key program deliverable with nine specific milestones that are due from 30 to 60 days from the start of the contract. This deliverable will enable the Commonwealth to meet the technical requirements of the business and application. This approach will include an ongoing review of the currently implemented technologies and assets to identify and validate when the Commonwealth's Capacity on Demand, Fully Managed, and Managed-Only Services or equipment should be replaced to support new business needs or maintain hardware and software currency and defined service levels. The Senior Enterprise Infrastructure Architect and the Agency Infrastructure Architects will manage the Technology Architecture and Refresh Approach, with recurring scheduled reviews and discussions with the Commonwealth and participating agencies.

The Data Center Technology Roadmap will begin with defining and understanding key Commonwealth business plans and needs. Using the Commonwealth's business plans and needs to define the technical requirements will enable the roadmap to align the technology recommendations, schedules, and retirement with the changes in the Commonwealth's business environment. The roadmap will also include technical recommendations identified in the Continuous Improvement process.

D-04 – IT Service Continuity Architecture and Plan

The IT Service Continuity Architecture and Plan key program deliverable consists of seven major milestones that are due from 30 to 45 days from the effective date of the contract, with a monthly reoccurring requirement. The Unisys Team will design, build, and test a tiered DR solution for the Commonwealth. The architecture for the DR solution will be documented, reviewed with the Commonwealth, and updated based on reviews and DR testing results.

A Unisys IT Risk Manager will coordinate the overall IT Service Continuity across all agencies. This experienced resource will have the responsibility to develop and execute the project plan to test DR plans prior to workload migrations in cases where DR Service is already established. In addition, the scope of the DR plan will include transition of agencies to the requested Tiered DR solution.

To support a cross-agency IT Service Continuity architecture and plan, Unisys provisioned a common Online Disaster Recovery Planning tool that will help agencies identify gaps in IT Service Continuity. We also provisioned an Emergency Notification system that can be tuned to each agency's roster of agency staff that require notifications.

D-05 – Transition Management Plan

The Transition Management Plan key program deliverable consists of 11 major milestones that are due from the initial startup through the first 90 days with reoccurring requirements thereafter. The Commonwealth's Transition Program Management Plan will focus on two primary functions: Transition of Services and Data Center Migrations. Transition of Services activities will concentrate on the implementation and transformation of processes, tools, technology, and people providing support services to the Commonwealth and data centers. Much of this effort will center on the implementation of an ITILV3-based framework that will facilitate continuous improvement in the delivery of services. The Data Center Migration (DCM) activities will center on the design and build out of the technical infrastructure required to provide a secure, highly reliable, and cost-effective environment for the Commonwealth's applications to execute as well as the organization and coordination necessary to migrate the Commonwealth's applications to this new environment. The plan's actual content will follow the Commonwealth's ITIL V3 guidelines for Management Plans, including an explanation of the methodology, staffing, schedule, and specific tasks required to accomplish the transition. Transition deliverables will be documented in the plan as part of Key Deliverable D-05.

D-06 – Agency Level DR Plan(s)

The Agency Level DR Plan key program deliverable consists of three major milestones with monthly recurring requirements. We also understand the importance of protection of critical agency applications from disaster. Unisys will provide assistance to Commonwealth agencies with updating or developing their current disaster recovery plans. Agency

level DR plans will reflect the Unisys DR approach and solution for testing and be modified to include the new technology solution utilized for their application infrastructure in the new data center. We will also work with agencies that do not have disaster recovery plans, but desire protection to develop plans to protect their most critical applications.

D-07 – Security Management Plan

The Security Management Plan key program deliverable consists of 10 major milestones that are due within the first 45 days of the contract. The Security Management Plan will be developed during the Transition of Services project and include a provision for annual security assessments and definition of security controls to address the confidentiality, integrity, and availability of Commonwealth data. It will address procedures for personnel security, including background check requirements as well as a procedure for ongoing personnel status changes that may negatively affect their ability to continue meeting security requirements.

D-08 – Facilities Management Plan

The Facilities Management Plan key program deliverable consists of nine key program deliverables effective within the first year of the contract. The Offeror Facility Management Plan will provide a proven framework for all facility-related environmental systems, including power, cooling, fire detection and suppression, building access control, and environmental monitoring as well as how future project work is to be performed at the EDC facility and the Unisys Team facilities. All facility management work detailed will be subject to the Change Management process.

D-09 – Security Risk and Vulnerability Assessment Report

The initial Security Risk and Vulnerability Report due within the first 90 days of the contract will be developed during the Transition of Services project and will leverage Deloitte's leading practices for assessing security risk and conducting vulnerability assessments to help achieve the Commonwealth's IT security and overriding business objectives in a timely and cost-effective way.

Deloitte's approach is based on deep experience in serving multiple agencies of the Commonwealth and other public sector clients using Deloitte's demonstrated methodology and framework. Deloitte's security vulnerability assessment process is comprised of five phases: Scope and Plan; Conduct vulnerability assessment; Perform penetration testing; Perform security risk assessment and architecture review; and Perform security configuration risk review.

D-10 – Gap Analysis Report

The Gap Analysis Report key program deliverable consists of two major milestones that are due between 120 and 150 days from contract start. Unisys will conduct a data center analysis, and create a report that identifies gaps in the current data centers including Unisys corrective action and approach recommendations.

D-11 – Contract Management Plan

The Contract Management Plan key program deliverable consists of two major milestones due within 60 days of the contract effective date. The Contract Management Plan will be developed to address management procedures for the overall contract. It will describe our plan to remain compliant with the terms and conditions of the contract and provide services and products that meet the requirements of the project. This plan will identify activities to be performed or initiated to track, manage, amend, and close the contract. This plan will include interim contract procedures.

Request for Proposal

RFP # 6100022698

Commonwealth of Pennsylvania
Office of Administration
Office for Information Technology
Data Center Computing Services

Schedule J.3

Data Center SLA Definitions

CONTENTS

1. OFFEROR GUIDELINES....4

1.1. Offeror Instructions....4

1.2. Service Level Class Definitions....4

2. SERVICE LEVEL DETAILS....4

SL01 Application Infrastructure Availability – Platinum....5

SL02 Application Infrastructure Availability – Gold....9

SL03 Application Infrastructure Availability – Silver....13

SL04 Application Infrastructure Availability – Bronze....17

SL05 Application Infrastructure Availability – Basic....21

SL06 Resolution Time - Severity Level 1 Incidents....25

SL07 Resolution Time - Severity Level 2....30

SL08 Resolution Time - Severity Level 3/4....35

SL09 Solution Request Fulfillment....40

SL10 Standard Service Request Fulfillment....43

SL11 Completion of Project/Solution Phase....46

SL12 Solution and Procurement Proposals Delivered....49

SL13 CMDB Content Accuracy and Timeliness....53

SL14 Software License Renewal Timeliness....56

SL15 Successful Backups....59

SL16 Successful Recoveries....62

SL17 Security Incident Notification Timeliness....65

SL18 Security Update Timeliness....68

SL19 Incident Management Communication – for Severity 1 Incidents....70

SL20 Root Cause Analysis Delivery....72

SL21 Chronic Problems....75

SL22 High Risk Security Patch Updates....78

SL23 Change Management Effectiveness....81

SL24 Service Desk – Call Answer Time....84

SL25 Service Desk – Abandon Rate....86
SL26 Incident Ticket Quality....88
SL27 Service Desk – Customer Satisfaction....91
SL28 Batch Scheduling Launched on Time....94
SL29 Batch Processing Completed Successfully....96
SL30 Reports Delivered On Time....98
SL31 Off-Site Media Management....100
SLXX Name (Template)....102

3. NOTES....103

4. ADDITIONAL DEFINITIONS....103

1. Offeror Guidelines

This Schedule contains specific service level requirements that the Offeror must meet in order to perform the requested Services. The Offeror must respond to the requirements contained in this Schedule according to the instructions provided below.

1.1. Offeror Instructions

- The Offeror's response to the RFP should reflect and comply with the information contained in this Schedule.
- The Offeror will complete the following sections in each of the Critical Measurements and Key Measurements:
  - Collection Process – identify how the measurement data will be collected
  - Reporting Tools – identify any tools, automated or manual, that will be used
  - Raw Data Storage (Archives) – identify where data will be stored and accessible by the Commonwealth for further analysis
  - Reporting Format/s – identify the proposed reporting format

1.2. Service Level Class Definitions

There are two classes of Service Level performance metrics used, Critical Measurements (CMs) and Key Measurements (KMs).

- **Critical Measurements (CMs)** are performance measurements defined for the most important service areas. CMs will have associated fees, e.g. Performance Credits, payable by the Offeror to Commonwealth for missed CMs according to the terms of the negotiated contract.

- **Key Measurements (KMs)** are performance target measurements for non-critical service areas. KMs are not eligible for Performance Credits. Key Measures cover less critical service deliverables, sub processes or interim activities that are related to CM performance, and are reflective of overall effective and efficient service performance management. Based on periodic contractual SLA reviews, adjustments may be negotiable and KMs may be promoted to CMs.

Service Level measurement and reporting normally begins immediately following the Service Commencement Date. However, to allow for stabilization where appropriate, application of Performance Credits may be reduced or waived for some period of time (to be negotiated) after the Service Commencement Date.

2. Service Level Details

The following pages describe each Service Level, its calculation, and other details relevant to the Service Level.

SL01 Application Infrastructure Availability – Platinum

Service Level Reference	Description
Application Infrastructure Availability– Platinum	
Service Category	Availability
Metric Description	This Service Level measures the percentage of time the Applications are Available during the applicable Measurement Window. This measurement is by application, not by server instance. Availability is defined by whether the application residing on any of the associated server instances is available to users. Targeted Applications will be determined by the Commonwealth based on the critical nature of the Agency Application.
Metric Inclusions	Server Instances and related CIs supporting Targeted Applications are identified in the CMDB. Scheduled hours of operations and maintenance windows for each infrastructure element related to the Targeted Applications will be maintained in the Commonwealth Computing Procedures Manual.
Metric Exclusions	• All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** The Service Level calculation for "Targeted Applications Infrastructure Availability" is the sum of Actual Uptime for the individual Applications divided by the sum of expected, scheduled Uptime for the Applications, with the result expressed as a percentage. • = 1 – ((Sum of Minutes the Application is not Available) / ((1440 Minutes Per Day) X (Calendar Days In Month))) expressed as a percentage
Collection Process	Unisys will work with the Commonwealth to establish the processes for collecting appropriate data for infrastructure availability measurements for the required Commonwealth Application(s). These metrics will be established when the Commonwealth selects the Unisys proposed Enterprise Services Catalog for mapping Configuration Items (CI's) for each Commonwealth Application. As part of this service, Unisys can show the relevant metrics that can be collected by the BMC Service Level Management (SLM) Application. This data is used to setup service targets against incident tickets affecting availability for each mapped Commonwealth Application CI. The SLM Application will compute the availability for supporting mapped CI's, as outlined above, for the Commonwealth Application(s). Inputs: • CMDB (mapped CI's to application)

	• Incident Tickets
Reporting Tools / Data Source(s)	The SL01 compliance will be recorded in the BMC ITSM Service Level Management Application and displayed on the real-time dashboard for all stakeholders to view and access. Data Sources: • BMC ITSM Incident Tickets • BMC ITSM Configuration Management Database Reporting Tools: • BMC Service Level Management Module • Real-time Dashboard • BMC Analytics Reporting Outputs: • Notifications through email generated from BMC ITSM SLM module for SL01 violations • SLA compliance will be displayed on Real-time Dashboard • BMC Analytics SLA Monthly Report
Data Storage (Archives)	13 months – Online Tape Backup – Life of Contract
Reporting Format/s	The SLA dashboard format will be determined during transition for display on the Real-time Dashboard. **Figure J-1** provides a dashboard example:

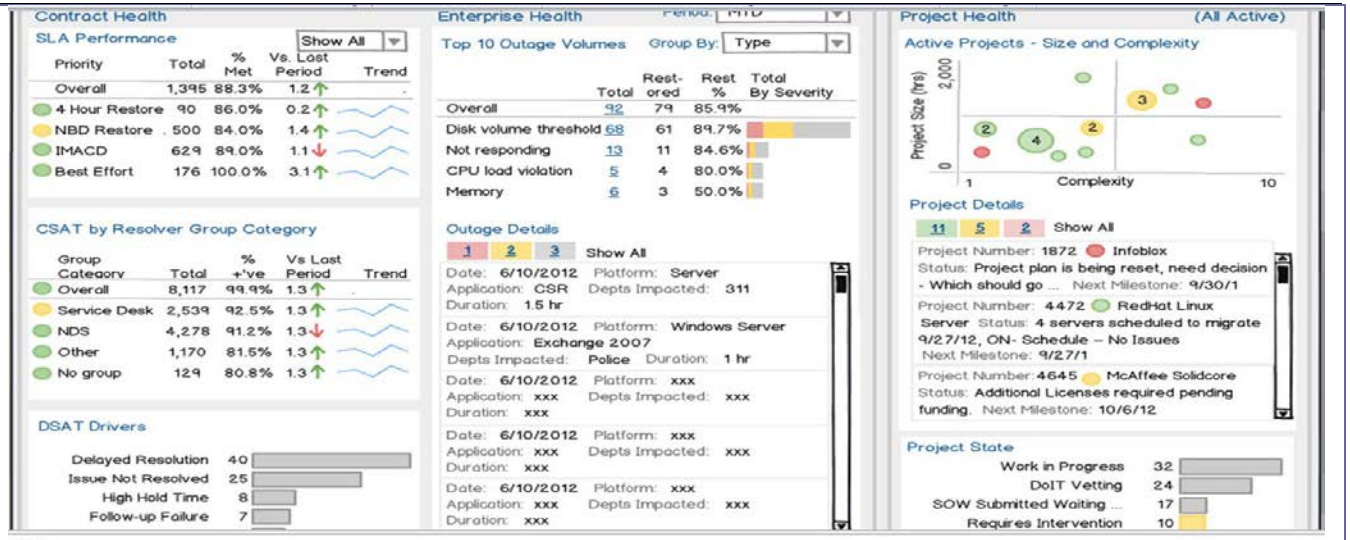


Figure J-1. SL01 Real-time Dashboard

The SLA Reporting format will be determined during transition for reporting using BMC Analytics Reporting. **Figure J-2** is an example of reports [redacted] This format will continue to be used until a new format is deployed:

Environment	Component		Allowed Minutes	Minutes Down					Remaining Minutes
		SLA	March	w/e 3/3	w/e 3/10	w/e 3/17	w/e 3/24	w/e 3/31	
DPW HSH-A	System	99.90%	45	0					45
	TIP	99.90%	45	0					45
	WEBTS	99.70%	134	0					134
	WEBTWO	99.70%	134	0					134
	OLTP	99.90%	45	0					45
DPW HSH-C	System	99.90%	45	28					17
	TIP	99.90%	45	0					45
	MAPPER	99.90%	45	0					45
	APPMAP	99.90%	45	0					45
	OLTP	99.90%	45	0					45
DPW HSH-F	System	99.90%	45	0					45
	TIP	99.90%	45	0					45
PSP	System	99.90%	45	0					45
	TIP	99.87%	58	0					58
	MAPPER	99.90%	45	0					45
GAME	System	99.90%	45	0					45
	COMS	99.90%	45	0					45
DOS L2K	System	99.90%	30	0					30
	SQL Server	99.90%	30	0					30
DOS SURE	System	99.80%	35	0					35
	SQL Server	99.90%	30	0					30
	SRS Application System	99.90%	45	0					45
	SRS SQL System	99.90%	45	0					45
	Virtual Citrix Print Servers	99.50%	223	0					223
DOI Web Envir	System	99.90%	20	0					20
	IIS	99.70%	59	0					59
DOI	System	99.70%	61	0					61

Figure J-2. SL01 BMC Analytics Reporting

Service Level Reporting Window	Monthly

SL02 Application Infrastructure Availability – Gold

Service Level Reference	Description
Application Infrastructure Availability – Gold	
Service Category	Availability
Metric Description	This Service Level measures the percentage of time the Applications are Available during the applicable Measurement Window. This measurement is by application, not by server instance. Availability is defined by whether the application residing on any of the associated server instances is available to users. Targeted Applications will be determined by the Commonwealth based on the critical nature of the Agency Application.
Metric Inclusions	Server Instances and related CIs supporting Targeted Applications are identified in the CMDB. Scheduled hours of operations and maintenance windows for each infrastructure element related to the Targeted Applications will be maintained in the Commonwealth Computing Procedures Manual.
Metric Exclusions	• All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** The Service Level calculation for "Targeted Applications Infrastructure Availability" is the sum of Actual Uptime for the individual Applications divided by the sum of expected, scheduled Uptime for the Applications, with the result expressed as a percentage. • = 1 – ((Sum of Minutes the Application is not Available) / ((1440 Minutes Per Day) X (Calendar Days In Month))) expressed as a percentage
Collection Process	Unisys will configure the collection for infrastructure availability measurements for selected Commonwealth Application(s) when the Commonwealth selects the Unisys proposed Enterprise Services Catalog for mapping Configuration Items (CIs) for each Commonwealth Application. As part of this service, the BMC Service Level Management (SLM) Application will setup service targets against incident tickets affecting availability for each mapped Commonwealth Application CI. The SLM Application will compute the availability for supporting mapped CIs, as outlined above, for the Commonwealth Application(s). Inputs: • CMDB (mapped CIs to application)

	• Incident Tickets
Reporting Tools / Data Source(s)	The SL02 compliance will be recorded in the BMC ITSM Service Level Management Application and displayed on the Real-time Dashboard for all stakeholders to view and access. Data Sources: • BMC ITSM Incident Tickets • BMC ITSM Configuration Management Database Reporting Tools: • BMC Service Level Management Module • Real-time Dashboard • BMC Analytics Reporting Outputs: • Notifications through email generated from BMC ITSM SLM module for SL02 violations • SLA compliance will be displayed on Real-time Dashboard • BMC Analytics SLA Monthly Report
Data Storage (Archives)	13 months – Online Tape Backup – Life of Contract
Reporting Format/s	The SLA dashboard format will be determined during transition for display on the Real-time Dashboard. **Figure J-3** provides a dashboard example:

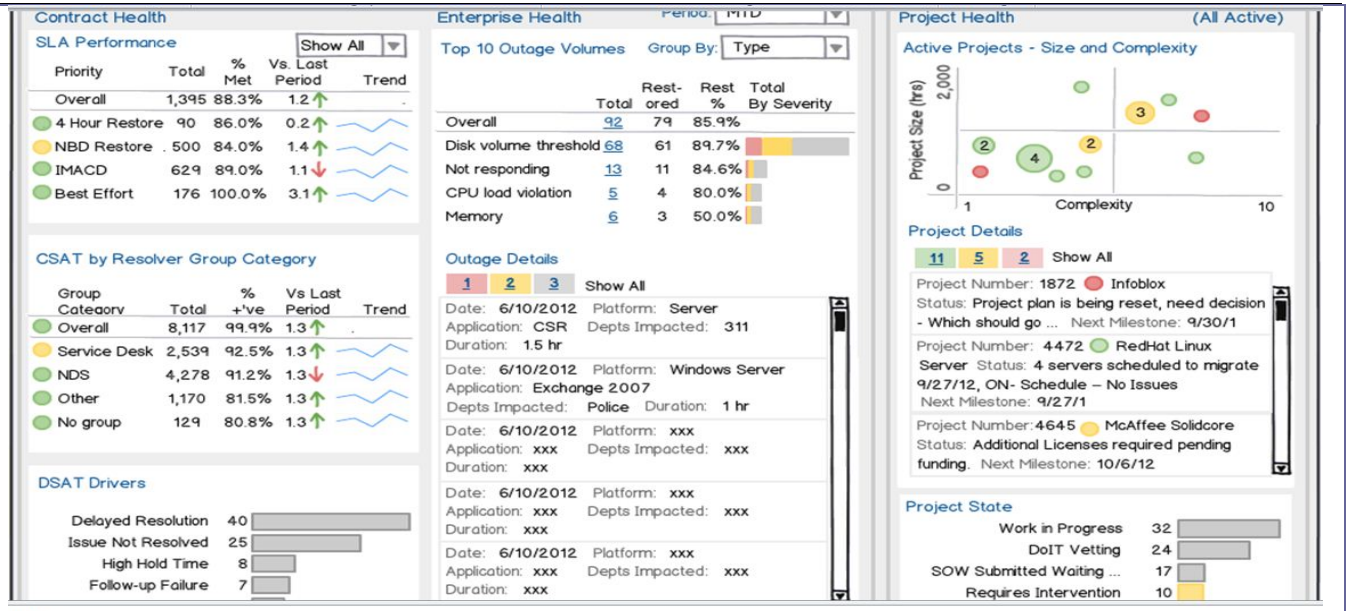


Figure J-3. SL02 Real-time Dashboard

The SLA Reporting format will be determined during transition for reporting using BMC Analytics Reporting. **Figure J-4** is an example of reports [redacted] This format will continue to be used until a new format is deployed

Environment	Component		Allowed Minutes	Minutes Down					Remaining Minutes
		SLA	March	w/e 3/3	w/e 3/10	w/e 3/17	w/e 3/24	w/e 3/31	
DPW HSH-A	System	99.90%	45	0					45
	TIP	99.90%	45	0					45
	WEBTS	99.70%	134	0					134
	WEBTWO	99.70%	134	0					134
	OLTP	99.90%	45	0					45
DPW HSH-C	System	99.90%	45	28					17
	TIP	99.90%	45	0					45
	MAPPER	99.90%	45	0					45
	APPMAP	99.90%	45	0					45
	OLTP	99.90%	45	0					45
DPW HSH-F	System	99.90%	45	0					45
	TIP	99.90%	45	0					45
PSP	System	99.90%	45	0					45
	TIP	99.87%	58	0					58
	MAPPER	99.90%	45	0					45
GAME	System	99.90%	45	0					45
	COMS	99.90%	45	0					45
DOS L2K	System	99.90%	30	0					30
	SQL Server	99.90%	30	0					30
DOS SURE	System	99.80%	35	0					35
	SQL Server	99.90%	30	0					30
	SRS Application System	99.90%	45	0					45
	SRS SQL System	99.90%	45	0					45
	Virtual Citrix Print Servers	99.50%	223	0					223
DOI Web Envir	System	99.90%	20	0					20
	IIS	99.70%	59	0					59
DOI	System	99.70%	61	0					61

Figure J-4. SL02 BMC Analytics Reporting

Service Level Reporting Window	Monthly

SL03 Application Infrastructure Availability – Silver

Service Level Reference	Description
Application Infrastructure Availability– Silver	
Service Category	Availability
Metric Description	This Service Level measures the percentage of time the Applications are Available during the applicable Measurement Window. This measurement is by application, not by server instance. Availability is defined by whether the application residing on any of the associated server instances is available to users. Targeted Applications will be determined by the Commonwealth based on the critical nature of the Agency Application.
Metric Inclusions	Server Instances and related CIs supporting Targeted Applications are identified in the CMDB. Scheduled hours of operations and maintenance windows for each infrastructure element related to the Targeted Applications will be maintained in the Commonwealth Computing Procedures Manual.
Metric Exclusions	• All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** The Service Level calculation for "Targeted Applications Infrastructure Availability" is the sum of Actual Uptime for the individual Applications divided by the sum of expected, scheduled Uptime for the Applications, with the result expressed as a percentage. • = 1 – ((Sum of Minutes the Application is not Available) / ((1440 Minutes Per Day) X (Calendar Days In Month))) expressed as a percentage
Collection Process	The Unisys Team will work with the Commonwealth to establish the processes for collecting appropriate data for infrastructure availability measurements for the required Commonwealth Application(s). These metrics will be established when the Commonwealth selects the Unisys proposed Enterprise Services Catalog for mapping Configuration Items (CIs) for each Commonwealth Application. As part of this service, Unisys can show the relevant metrics that can be collected by the BMC Service Level Management (SLM) Application. This data will be used to setup service targets against incident tickets affecting availability for each mapped Commonwealth Application CI. The SLM Application will compute the availability for supporting mapped CIs, as outlined above, for the Commonwealth Application(s). Inputs: • CMDB (mapped CIs to application)

	• Incident Tickets
Reporting Tools / Data Source(s)	The SL03 compliance will be recorded in the BMC ITSM Service Level Management Application and displayed on the Real-time Dashboard for all stakeholders to view and access. Data Sources: • BMC ITSM Incident Tickets • BMC ITSM Configuration Management Database Reporting Tools: • BMC Service Level Management Module • Real-time Dashboard • BMC Analytics Reporting Outputs: • Notifications through email generated from BMC ITSM SLM module for SL03 violations • SLA compliance will be displayed on Real-time Dashboard • BMC Analytics SLA Monthly Report
Data Storage (Archives)	13 months – Online Tape Backup – Life of Contract
Reporting Format/s	The SLA dashboard format will be determined during transition for display on the Real-time Dashboard. **Figure J-5** provides a dashboard example:

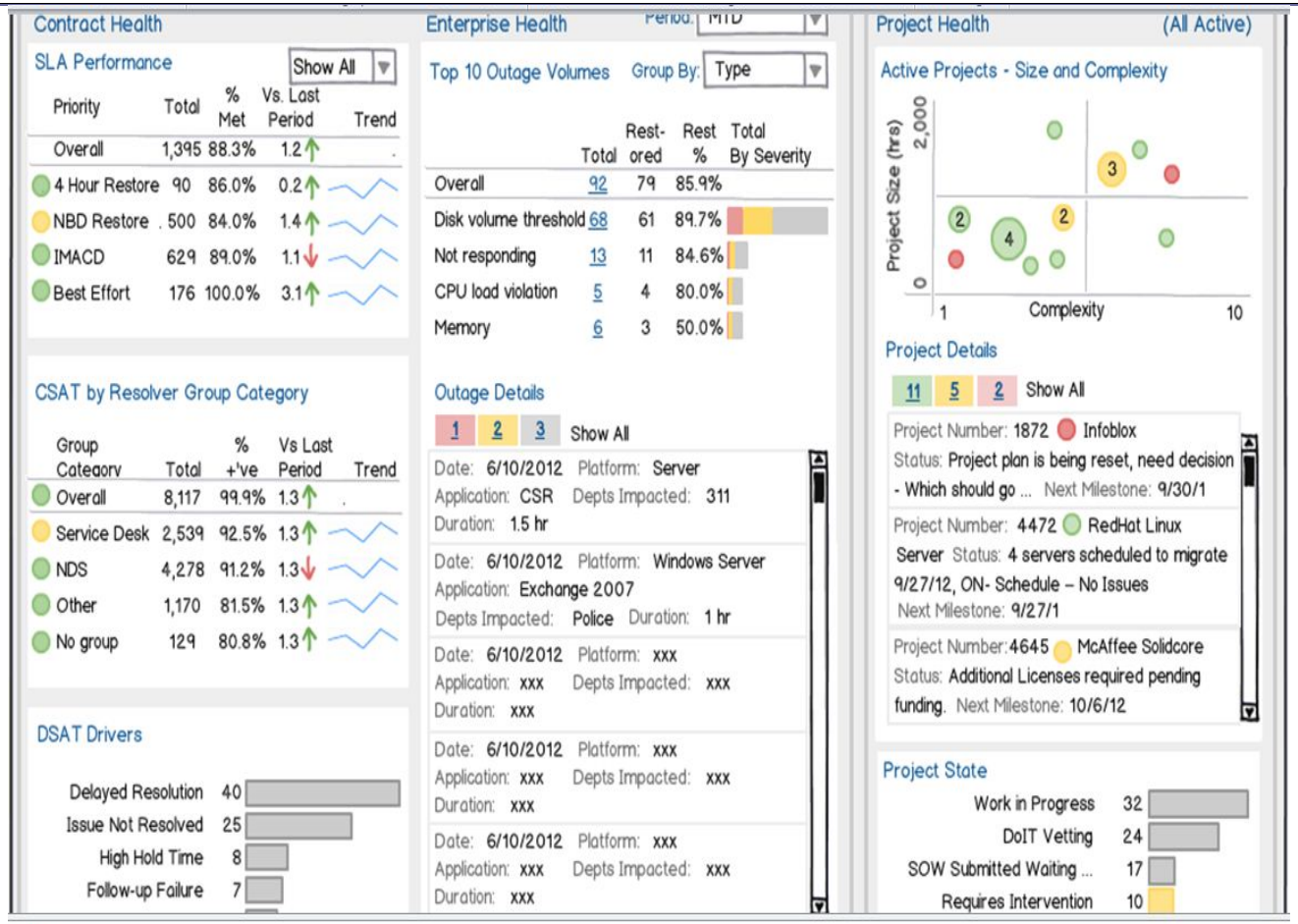


Figure J-5. SL03 Real-time Dashboard

The SLA Reporting format will be determined during transition for reporting using BMC Analytics Reporting. **Figure J-6** is an example of reports [redacted] This format will continue to be used until a new format is deployed

Environment	Component	SLA	Allowed Minutes March	Minutes Down w/e 3/3	w/e 3/10	w/e 3/17	w/e 3/24	w/e 3/31	Remaining Minutes
DPW HSH-A	System	99.90%	45	0					45
	TIP	99.90%	45	0					45
	WEBTS	99.70%	134	0					134
	WEBTWO	99.70%	134	0					134
	OLTP	99.90%	45	0					45
DPW HSH-C	System	99.90%	45	28					17
	TIP	99.90%	45	0					45
	MAPPER	99.90%	45	0					45
	APPMAP	99.90%	45	0					45
	OLTP	99.90%	45	0					45
DPW HSH-F	System	99.90%	45	0					45
	TIP	99.90%	45	0					45
PSP	System	99.90%	45	0					45
	TIP	99.87%	58	0					58
	MAPPER	99.90%	45	0					45
GAME	System	99.90%	45	0					45
	COMS	99.90%	45	0					45
DOS L2K	System	99.90%	30	0					30
	SQL Server	99.90%	30	0					30
DOS SURE	System	99.80%	35	0					35
	SQL Server	99.90%	30	0					30
	SRS Application System	99.90%	45	0					45
	SRS SQL System	99.90%	45	0					45
	Virtual Citrix Print Servers	99.50%	223	0					223
DOI Web Envir	System	99.90%	20	0					20
	IIS	99.70%	59	0					59
DOI	System	99.70%	61	0					61

Figure J-6. SL03 BMC Analytics Reporting

Service Level Reporting Window	Monthly

SL04 Application Infrastructure Availability – Bronze

Service Level Reference	Description
Application Infrastructure Availability– Bronze	
Service Category	Availability
Metric Description	This Service Level measures the percentage of time the Applications are Available during the applicable Measurement Window. This measurement is by application, not by server instance. Availability is defined by whether the application residing on any of the associated server instances is available to users. Targeted Applications will be determined by the Commonwealth based on the critical nature of the Agency Application.
Metric Inclusions	Server Instances and related CIs supporting Targeted Applications are identified in the CMDB. Scheduled hours of operations and maintenance windows for each infrastructure element related to the Targeted Applications will be maintained in the Commonwealth Computing Procedures Manual.
Metric Exclusions	• All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** The Service Level calculation for "Targeted Applications Infrastructure Availability" is the sum of Actual Uptime for the individual Applications divided by the sum of expected, scheduled Uptime for the Applications, with the result expressed as a percentage. • = 1 – ((Sum of Minutes the Application is not Available) / ((1440 Minutes Per Day) X (Calendar Days In Month))) expressed as a percentage
Collection Process	Unisys will work with the Commonwealth to establish the processes for collecting appropriate data for infrastructure availability measurements for the required Commonwealth Application(s). These metrics will be established when the Commonwealth selects the Unisys proposed Enterprise Services Catalog for mapping Configuration Items (CIs) for each Commonwealth Application. As part of this service, Unisys can show the relevant metrics that can be collected by the BMC Service Level Management (SLM) Application. This data will be used to setup service targets against incident tickets affecting availability for each mapped Commonwealth Application CI. The SLM Application will compute the availability for supporting mapped CIs, as outlined above, for the Commonwealth Application(s). Inputs: • CMDB (mapped CIs to application)

	• Incident Tickets
Reporting Tools / Data Source(s)	The SL04 compliance will be recorded in the BMC ITSM Service Level Management Application and displayed on the Real-time Dashboard for all stakeholders to view and access. Data Sources: • BMC ITSM Incident Tickets • BMC ITSM Configuration Management Database Reporting Tools: • BMC Service Level Management Module • Real-time Dashboard • BMC Analytics Reporting Outputs: • Notifications through email generated from BMC ITSM SLM module for SL04 violations • SLA compliance will be displayed on Real-time Dashboard • BMC Analytics SLA Monthly Report
Data Storage (Archives)	13 months – Online Tape Backup – Life of Contract
Reporting Format/s	The SLA dashboard format will be determined during transition for display on the Real-time Dashboard. **Figure J-7** provides a dashboard example:

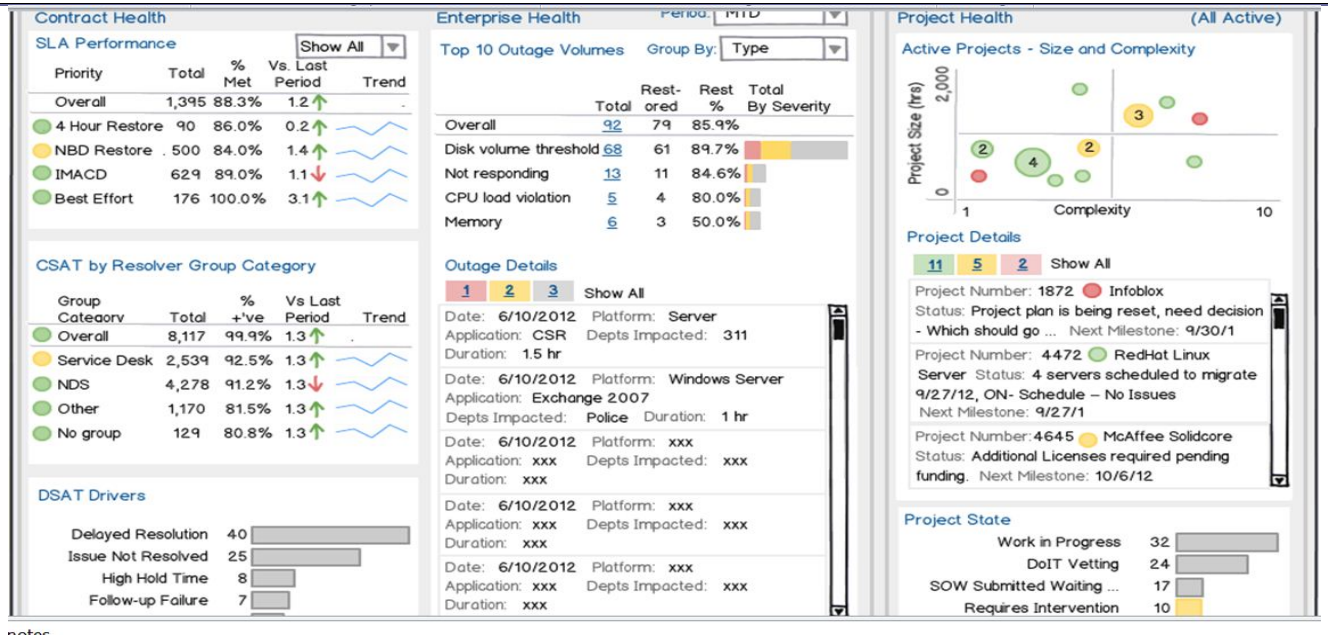


Figure J-7. SL04 Real-time Dashboard

The SLA Reporting format will be determined during transition for reporting using BMC Analytics Reporting. **Figure J-8** is an example of reports [redacted] This format will continue to be used until a new format is deployed

Environment	Component		Allowed Minutes	Minutes Down					Remaining Minutes
		SLA	March	w/e 3/3	w/e 3/10	w/e 3/17	w/e 3/24	w/e 3/31	
DPW HSH-A	System	99.90%	45	0					45
	TIP	99.90%	45	0					45
	WEBTS	99.70%	134	0					134
	WEBTWO	99.70%	134	0					134
	OLTP	99.90%	45	0					45
DPW HSH-C	System	99.90%	45	28					17
	TIP	99.90%	45	0					45
	MAPPER	99.90%	45	0					45
	APPMAP	99.90%	45	0					45
	OLTP	99.90%	45	0					45
DPW HSH-F	System	99.90%	45	0					45
	TIP	99.90%	45	0					45
PSP	System	99.90%	45	0					45
	TIP	99.87%	58	0					58
	MAPPER	99.90%	45	0					45
GAME	System	99.90%	45	0					45
	COMS	99.90%	45	0					45
DOS L2K	System	99.90%	30	0					30
	SQL Server	99.90%	30	0					30
DOS SURE	System	99.80%	35	0					35
	SQL Server	99.90%	30	0					30
	SRS Application System	99.90%	45	0					45
	SRS SQL System	99.90%	45	0					45
	Virtual Citrix Print Servers	99.50%	223	0					223
DOI Web Envir	System	99.90%	20	0					20
	IIS	99.70%	59	0					59
DOI	System	99.70%	61	0					61

Figure J-8. SL04 BMC Analytics Reporting

Service Level Reporting Window	Monthly

SL05 Application Infrastructure Availability – Basic

Service Level Reference	Description
Application Infrastructure Availability - Basic	
Service Category	Availability
Metric Description	This Service Level measures the percentage of time the Applications are Available during the applicable Measurement Window. This measurement is by application, not by server instance. Availability is defined by whether the application residing on any of the associated server instances is available to users. Targeted Applications will be determined by the Commonwealth based on the critical nature of the Agency Application.
Metric Inclusions	Server Instances and related CIs supporting Targeted Applications are identified in the CMDB. Scheduled hours of operations and maintenance windows for each infrastructure element related to the Targeted Applications will be maintained in the Commonwealth Computing Procedures Manual.
Metric Exclusions	• All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** The Service Level calculation for "Targeted Applications Infrastructure Availability" is the sum of Actual Uptime for the individual Applications divided by the sum of expected, scheduled Uptime for the Applications, with the result expressed as a percentage. • = 1 – ((Sum of Minutes the Application is not Available) / ((1440 Minutes Per Day) X (Calendar Days In Month))) expressed as a percentage
Collection Process	Unisys will work with the Commonwealth to establish the processes for collecting appropriate data for infrastructure availability measurements for the required Commonwealth Application(s). These metrics will be established when the Commonwealth selects the Unisys proposed Enterprise Services Catalog for mapping Configuration Items (CIs) for each Commonwealth Application. As part of this service, Unisys can show the relevant metrics that can be collected by the BMC Service Level Management (SLM) Application. This data will be used to setup service targets against incident tickets affecting availability for each mapped Commonwealth Application CI. The SLM Application will compute the availability for supporting mapped CIs, as outlined above, for the Commonwealth Application(s). Inputs: • CMDB (mapped CIs to application)

	• Incident Tickets
Reporting Tools / Data Source(s)	The SL05 compliance will be recorded in the BMC ITSM Service Level Management Application and displayed on the Real-time Dashboard for all stakeholders to view and access. Data Sources: • BMC ITSM Incident Tickets • BMC ITSM Configuration Management Database Reporting Tools: • BMC Service Level Management Module • Real-time Dashboard • BMC Analytics Reporting Outputs: • Notifications through email generated from BMC ITSM SLM module for SL05 violations • SLA compliance will be displayed on Real-time Dashboard • BMC Analytics SLA Monthly Report
Data Storage (Archives)	13 months – Online Tape Backup – Life of Contract
Reporting Format/s	The SLA dashboard format will be determined during transition for display on the Real-time Dashboard. **Figure J-9** provides a dashboard example:

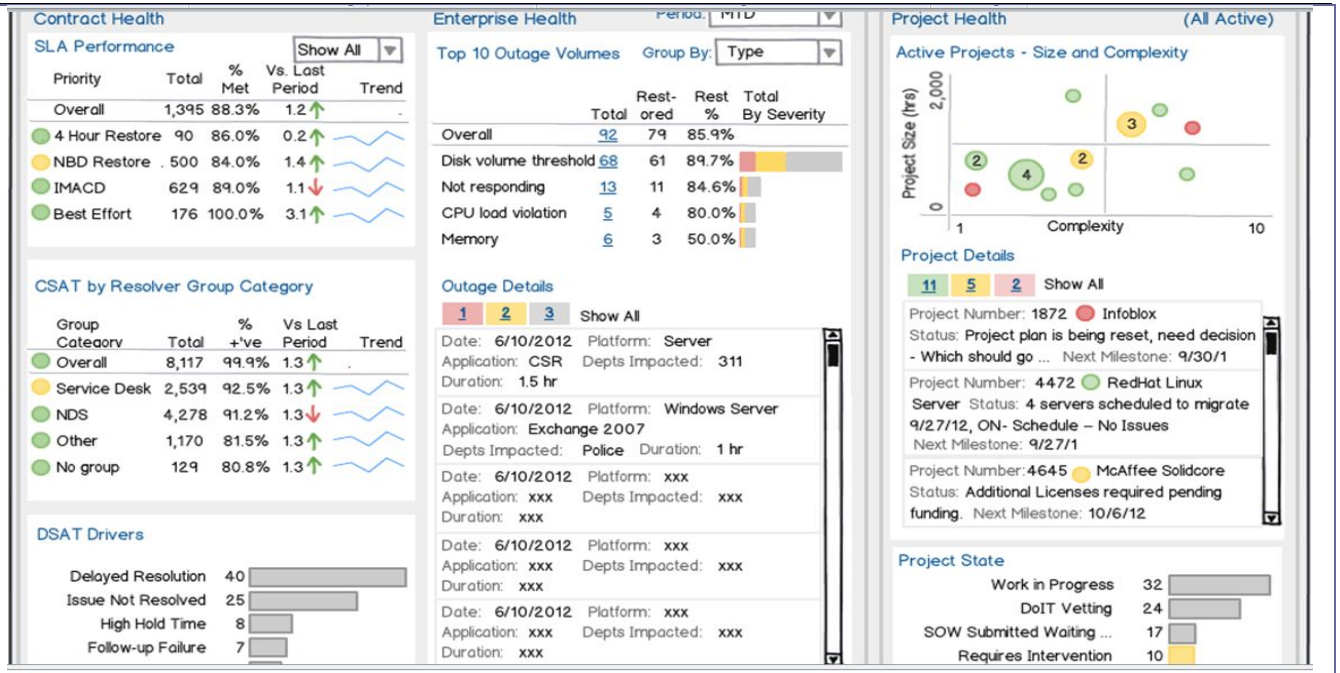


Figure J-9. SL05 Real-time Dashboard

The SLA Reporting format will be determined during transition for reporting using BMC Analytics Reporting. **Figure J-10** is an example of reports [redacted] This format will continue to be used until a new format is deployed

Environment	Component		Allowed Minutes	Minutes Down					Remaining Minutes
		SLA	March	w/e 3/3	w/e 3/10	w/e 3/17	w/e 3/24	w/e 3/31	
DPW HSH-A	System	99.90%	45	0					45
	TIP	99.90%	45	0					45
	WEBTS	99.70%	134	0					134
	WEBTWO	99.70%	134	0					134
	OLTP	99.90%	45	0					45
DPW HSH-C	System	99.90%	45	28					17
	TIP	99.90%	45	0					45
	MAPPER	99.90%	45	0					45
	APPMAP	99.90%	45	0					45
	OLTP	99.90%	45	0					45
DPW HSH-F	System	99.90%	45	0					45
	TIP	99.90%	45	0					45
PSP	System	99.90%	45	0					45
	TIP	99.87%	58	0					58
	MAPPER	99.90%	45	0					45
GAME	System	99.90%	45	0					45
	COMS	99.90%	45	0					45
DOS L2K	System	99.90%	30	0					30
	SQL Server	99.90%	30	0					30
DOS SURE	System	99.80%	35	0					35
	SQL Server	99.90%	30	0					30
	SRS Application System	99.90%	45	0					45
	SRS SQL System	99.90%	45	0					45
	Virtual Citrix Print Servers	99.50%	223	0					223
DOI Web Envir	System	99.90%	20	0					20
	IIS	99.70%	59	0					59
DOI	System	99.70%	61	0					61

Figure J-10. SL05 BMC Analytics Reporting

Service Level Reporting Window	Monthly

SL06 Resolution Time - Severity Level 1 Incidents

Service Level Reference	Description
Resolution Time - Severity Level 1 Incidents	
Service Category	Incident and Problem Resolution
Metric Description	This Service Level measures the percentage of time Offeror resolves Severity Level 1 events within the applicable time period. Also known as "Mean Time To Resolve" (MTTR) for Severity Level 1 Incidents.
Metric Inclusions	Includes all Applications Infrastructure components as defined by the CMDB and Severity Level 1 events that are assigned to the appropriate Service Level. The time limits for the resolution of each are as listed below. Time frame for resolution shall be based on the Tier designation for the highest mainframe, server or instance associated with the respective incident. For incidents not associated with a specific Mainframe, Server, or Instance, the resolution timeframe shall be measured as a Silver Tier. Platinum < 90 minutes Gold < 120 minutes Silver < 180 minutes Bronze < 240 Minutes
Metric Exclusions	• All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** The Service Level calculation for "Resolution Time – Severity Level 1" is the total number of Incidents that are or become Severity Level 1 that are Resolved within the relevant Resolution Time specified, divided by the total number of Incidents that are or become Severity Level 1 during the applicable Measurement Window, with the result expressed as a percentage. • = (Number of Severity Level 1 Incidents Resolved within Limit) / (Total Number of Severity Level 1 Incidents) expressed as a percentage
Collection Process	All infrastructure components with a Severity 1 incident ticket resolved during the measurement window will be included for calculation of the SL06 Resolution Time SLA. The CMDB will be used to determine the highest-level incident to be included for the calculation of the SLA. A Service Target

	in the BMC ITSM module will calculate the Mean Time to Resolve (MTTR) for each identified incident ticket using the time stamps of when the incident started and when the service was restored for the Configuration Item identified. The service target in the Service Level Management Module will calculate the compliance of the Severity 1 Incident Ticket(s) according to the SL06 definition. Inputs: • Incident Tickets (Severity 1) • CMDB (hierarchy of CIs and service level for the CI)
Reporting Tools / Data Source(s)	The SL06 compliance will be recorded in the BMC ITSM Service Level Management Application and reported on Real-time Dashboard for all stakeholders to view and access. Outputs: • SLA compliance will be displayed on Real-time Dashboard • SLA reports from BMC Analytics Data Sources: • BMC ITSM Incident Management Module • BMC ITSM Configuration Management Module • BMC ITSM Service Level Management Reporting Tools: • BMC ITSM Service Level Management • Real-time Dashboard • BMC Analytics
Data Storage (Archives)	Data storage is 13 months of history online with offline storage to tape with all supporting details.
Reporting Format/s	The SLA Incident reporting format will be determined during transition for display on the Real-time Dashboard. **Figure J-11** is a sample of an Incident SLA resolution time report. **Figure J-12** provides additional examples of BMC analytics page displaying incident time analysis. **Figure J-13** demonstrates a model we will use to display incident data on the dashboard.

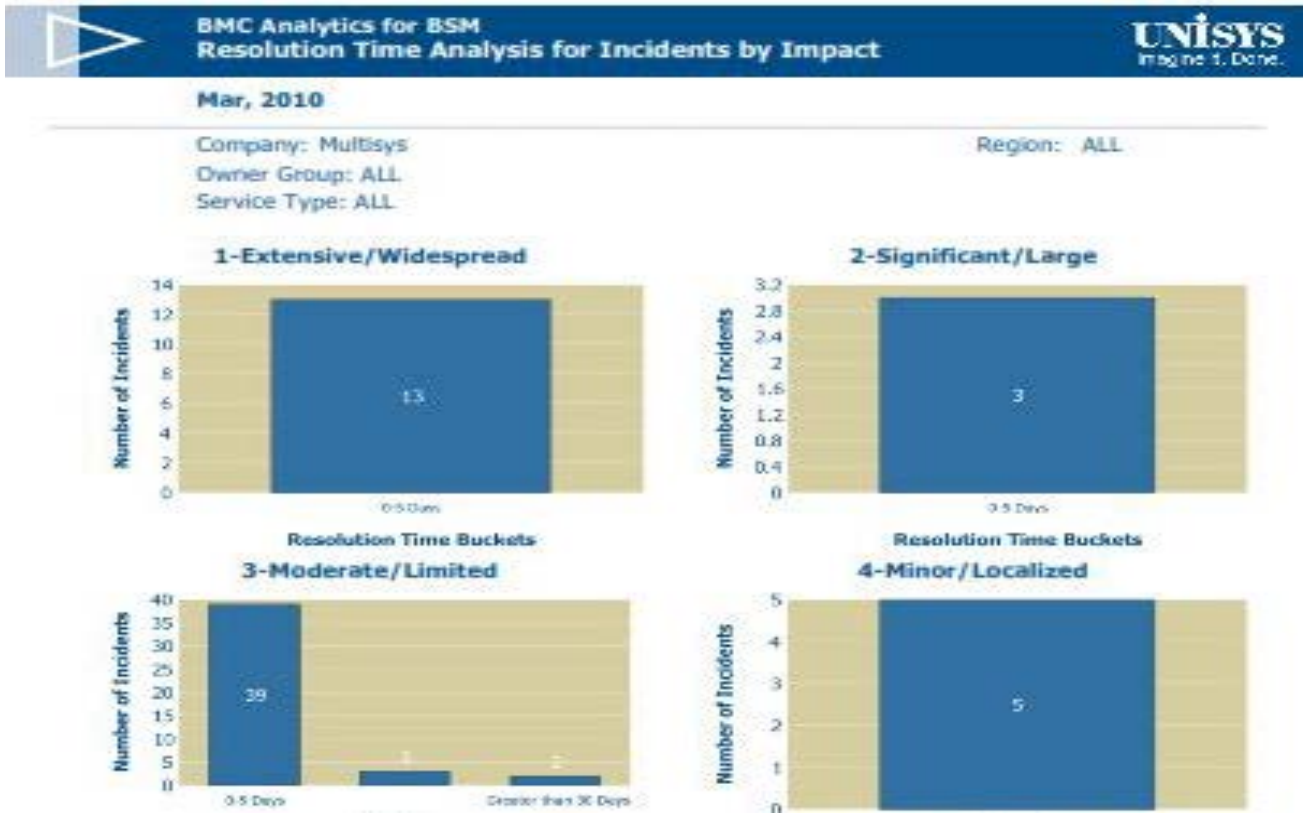


Figure J-11. SL06 SLA Resolution Time Report

BMC Analytics for BSM
Resolution Time Analysis for Incidents by Impact

UNISYS

Mar, 2010

Company: Multisys
Owner Group: ALL
Service Type: ALL

Region: ALL

1-Extensive/Widespread

Incident ID	Summary	Resolution Time in Days	Assigned Group	Incident Reported Date Time	Incident Last Resolved Date Time
INC000001520446	67: <HTTP Port> <HTTP Port> parameter <Port	0-5 Days	MULS-Service Desk-Globa	3/2/2010 10:44:48 AM	3/4/2010 6:21:47 AM
INC000001521189	Test - Multisys - 2/3/2010 - Pls Ignore	0-5 Days	MULS-Service Desk-Globa	3/2/2010 11:18:56 AM	3/2/2010 11:21:43 AM
INC000001528278	Test Multisys Incident Closure - 3/3/2010 - 1	0-5 Days	MULS-Service Desk-Globa	3/3/2010 9:12:30 AM	3/3/2010 9:13:45 AM
INC000001540161	67: <HTTP Port> <HTTP Port> parameter <Port	0-5 Days	MULS-Service Desk-Globa	3/5/2010 9:52:54 AM	3/5/2010 5:25:48 PM
INC000001542193	67: <HTTP Port> <HTTP Port> parameter <Port	0-5 Days	MULS-Service Desk-Globa	3/5/2010 5:25:52 PM	3/9/2010 12:37:46 PM
INC000001554989	67.96.142.194 is DOWN - not responding to ping	0-5 Days	MULS-Service Desk-Globa	3/9/2010 3:37:30 PM	3/9/2010 3:38:29 PM
INC000001563392	Response Time	0-5 Days	MULS-Desktop Resource	3/10/2010 7:41:55 PM	3/10/2010 10:16:47 PM
INC000001608331	67 is DOWN - not responding to ping	0-5 Days	MULS-Service Desk-Globa	3/21/2010 6:59:39 AM	3/22/2010 2:38:35 PM
INC000001608333	67: <HTTP Port> <HTTP Port> parameter <Port	0-5 Days	MULS-Service Desk-Globa	3/21/2010 7:00:09 AM	3/22/2010 2:39:44 PM
INC000001611640	67: <HTTP Port> <HTTP Port> parameter <Port	0-5 Days	MULS-Service Desk-Globa	3/22/2010 3:26:42 PM	3/22/2010 3:34:01 PM
INC000001612453	67 is DOWN - not responding to ping	0-5 Days	MULS-Service Desk-Globa	3/22/2010 6:01:36 PM	3/22/2010 6:09:35 PM
INC000001612455	67: <HTTP Port> <HTTP Port> parameter <Port	0-5 Days	MULS-Service Desk-Globa	3/22/2010 6:01:51 PM	3/22/2010 6:09:44 PM
INC000001643861	Test Multisys - Incident Status	0-5 Days	MULS-Service Desk-Globa	3/29/2010 8:16:50 AM	3/29/2010 8:19:51 AM

Figure J-12. SL06 BMC Analytics

Figure J-13 is a sample of the SLA Dashboard showing Incident Resolution times:

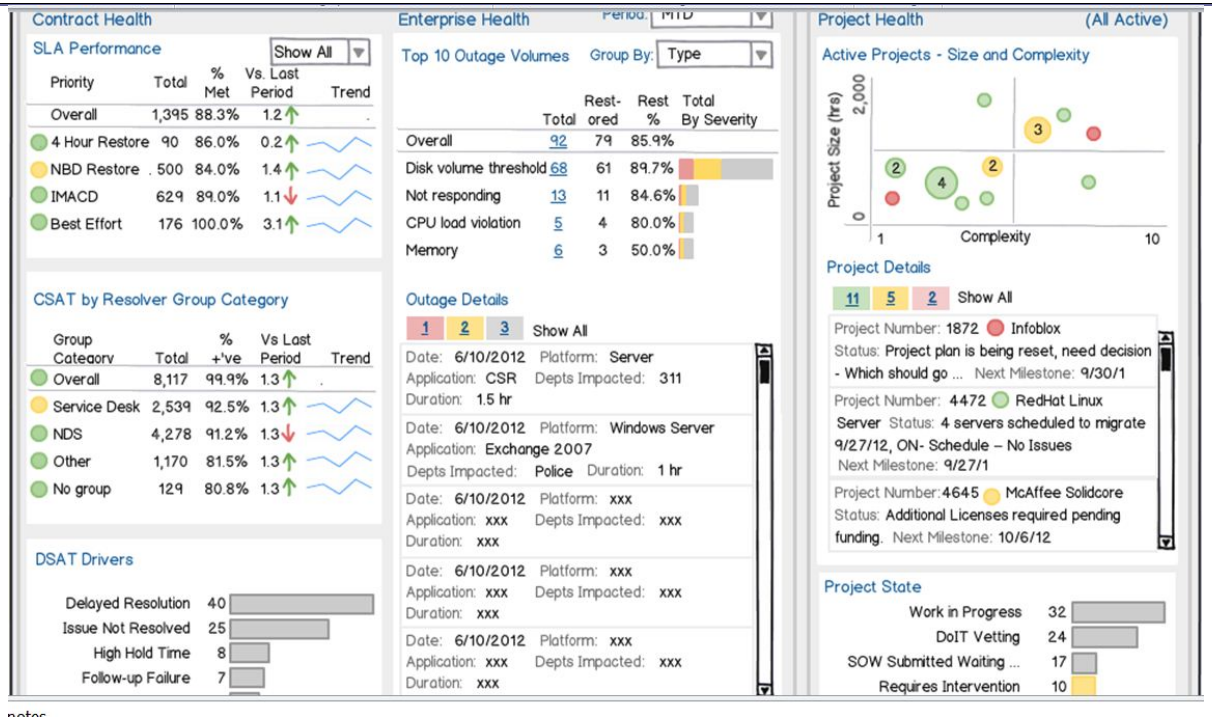


Figure J-13. SL06 Real-time Dashboard Incident Resolution Display

Service Level Reporting Window	Monthly

SL07 Resolution Time - Severity Level 2

Service Level Reference	Description
Resolution Time - Severity Level 2	
Service Category	Incident and Problem Resolution
Metric Description	This Service Level measures the percentage of time Offeror resolves Problems within the applicable time periods. Also known as "Mean Time To Resolve" (MTTR) for Severity Level 2 Incidents.
Metric Inclusions	Includes all Mainframes, Servers, and Instances associated with Targeted Applications and other Severity Level 2 events not associated with Servers or Instances. The time limits for the resolution of each mainframe, server or instance are as listed below. Time frame for resolution shall be based on the Tier designation for the highest mainframe, server or instance associated with the respective incident. For incidents not associated with a Mainframe, Server, or Instance, resolution shall be measured as Silver Tier (< 360 minutes). Platinum < 90 minutes Gold < 180 minutes Silver < 360 minutes Bronze < 960 Minutes
Metric Exclusions	• All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** The Service Level calculation for "Resolution Time – Severity Level 2" is the total number of Incidents that are or become Severity Level 2 that are Resolved within the relevant Resolution Time specified, divided by the total number of Incidents that are or become Severity Level 2 during the applicable Measurement Window, with the result expressed as a percentage. • = (Number of Severity Level 2 Incidents Resolved within Limit) / (Total Number of Severity Level 2 Incidents) expressed as a percentage
Collection Process	All infrastructure components with a Severity 2 incident tickets resolved during the measurement window will be included for calculation of the SL07 Resolution Time SLA. The CMDB will be used to determine the highest-level incident to be included for the calculation of the SLA. A Service Target in the BMC ITSM module will calculate the Mean Time to Resolve (MTTR) for each identified incident ticket using the times stamps of when the incident started and when the service was restored

	for the Configuration Item identified. The service target in the Service Level Management Module will calculate the compliance of the Severity 2 incident ticket(s) according to the SL07 definition. Inputs: • Incident Tickets (Severity 2) • CMDB (hierarchy of CIs and service level for the CI.
Reporting Tools / Data Source(s)	The SL07 compliance will be recorded in the BMC ITSM Service Level Management Application and reported on Real-time Dashboard for all stakeholders to view and access. Outputs: • Notifications through email generated from BMC ITSM with communication status updates per time intervals defined for SL07 • SLA compliance will be displayed on Real-time Dashboard • SLA reports from BMC Analytics Data Sources: • BMC ITSM Incident Management Module • BMC ITSM Configuration Management Module • BMC ITSM Service Level Management Reporting Tools: • BMC ITSM Service Level Management • Real-time Dashboard • BMC Analytics
Data Storage (Archives)	Data storage is 13 months of history online with offline storage to tape with all supporting details.
Reporting Format/s	The SLA incident-reporting format will be determined during transition for display on the Real-time Dashboard. **Figure J-14 and J14a** are samples of an BMC Incident SLA resolution time report:

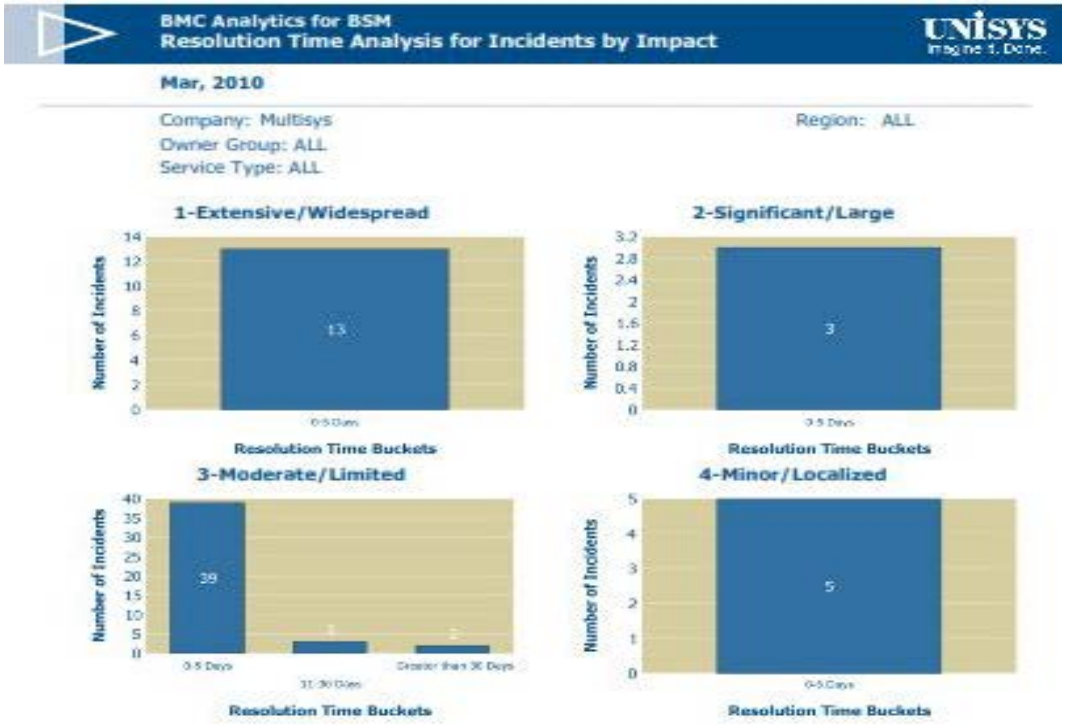


Figure J-14. SL07 Real-time Dashboard

BMC Analytics for BSM
Resolution Time Analysis for Incidents by Impact

UNISYS

Mar, 2010

Company: Multisys
Owner Group: ALL
Service Type: ALL

Region: ALL

2-Significant/Large

Incident ID	Summary	Resolution Time in Days	Assigned Group	Incident Reported Date Time	Incident Last Resolved Date Time
INC000001561707	Hardware Issue	0-5 Days	MULS-FTSS-Global	3/10/2010 3:16:05 PM	3/10/2010 4:33:38 PM
INC000001567516	Performance issue with CSII	0-5 Days	MULS-Incident Managem	3/11/2010 6:53:10 PM	3/11/2010 7:08:12 PM
INC000001651291	Performance issue with CSII	0-5 Days	MULS-Incident Managem	3/30/2010 2:09:03 PM	3/30/2010 2:45:42 PM

3-Moderate/Limited

Incident ID	Summary	Resolution Time in Days	Assigned Group	Incident Reported Date Time	Incident Last Resolved Date Time
INC000001207351	Test	Greater than 30	MULS-TEST	12/9/2009 9:19:03 PM	3/8/2010 2:46:16 PM
INC000001471615	Password Reset	11-30 Days	MULS-TEST	2/18/2010 12:20:06 PM	3/18/2010 10:41:05 AM
INC000001471804	Password Reset	11-30 Days	MULS-TEST	2/18/2010 12:59:34 PM	3/9/2010 5:25:52 PM
INC000001476697	Test for Onsite	11-30 Days	MULS-Desktop Resource	2/19/2010 10:56:12 AM	3/8/2010 2:47:47 PM
INC000001496012	test pls ignore	Greater than 30	MULS-Service Desk-EMEA	2/24/2010 11:48:27 AM	3/29/2010 10:23:01 AM
INC000001530133	Test Ticket, please do not respond	0-5 Days	MULS-TEST	3/3/2010 3:25:01 PM	3/8/2010 2:50:30 PM
INC000001554453	AD Password reset for username	0-5 Days	MULS-TEST	3/9/2010 1:13:51 PM	3/9/2010 1:30:01 PM
INC000001554454	AD password reset for username	0-5 Days	MULS-TEST	3/9/2010 1:14:28 PM	3/9/2010 1:30:36 PM
INC000001554455	AD Password reset for username	0-5 Days	MULS-TEST	3/9/2010 1:12:45 PM	3/9/2010 1:30:01 PM
INC000001554456	AD Password reset for username.	0-5 Days	MULS-TEST	3/9/2010 1:12:50 PM	3/9/2010 1:29:55 PM
INC000001554457	AD password reset for Multest A001	0-5 Days	MULS-TEST	3/9/2010 1:14:21 PM	3/9/2010 1:30:00 PM
INC000001554461	Network account password reset	0-5 Days	MULS-TEST	3/9/2010 1:10:54 PM	3/9/2010 1:30:02 PM

bmcsoftware Generated Apr 26, 2010 12:08:12 PM Page 2 of 5

Figure 14a, SL08 BMC Analytics

Figure J-15 is a sample of the SLA Dashboard showing Incident Resolution times:

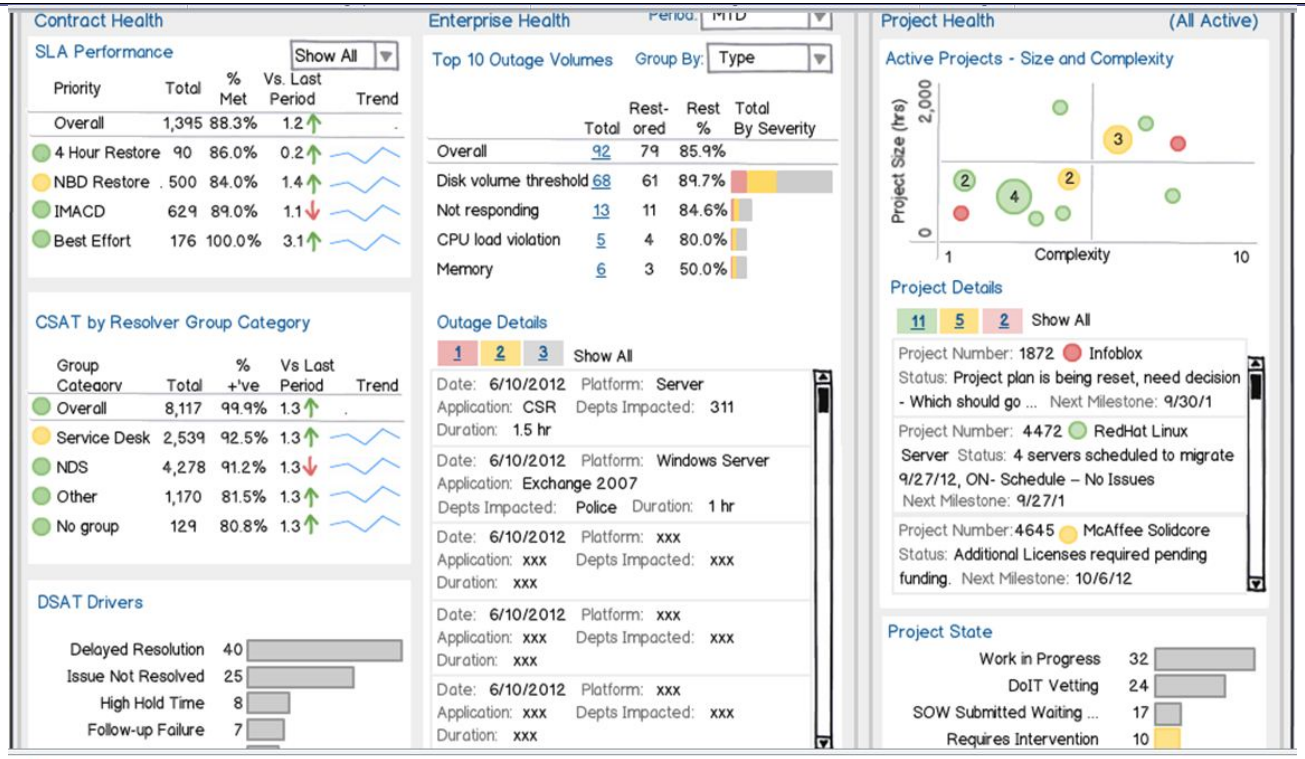


Figure J-15. SL07 Real-time Dashboard Incident Resolution Times

Service Level Reporting Window	Monthly

SL08 Resolution Time - Severity Level 3/4

Service Level Reference	Description
Resolution Time - Severity Level 3/4	
Service Category	Incident and Problem Resolution
Metric Description	This Service Level measures the percentage of time Offeror resolves Incidents within the applicable time periods. Also known as "Mean Time To Resolve" (MTTR) for Severity Level 3 and Severity Level 4 Incidents.
Metric Inclusions	Severity Level 3 - For all Severity Level 3 Incidents , the incident shall be resolved within 3,780 Business Minutes (i.e. 63 hours) Severity Level 4 - For all Severity Level 4 Incidents, the incident shall be resolved within 4,860 Business Minutes (i.e. 81 hours or 9 business days) Total Business Minutes shall be measured during only those minutes between 8:00 AM and 5:00 PM inclusive, Monday through Friday inclusive (1 Business day = 9 Business hours = 540 Business minutes); (1 Business Week = 2,700 minutes)
Metric Exclusions	• All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	8:00AM – 5:00 PM
Days of Measurement	Monday through Friday
Calculation	• **Summary:** The Service Level calculation for "Resolution Time – Severity Level 3/4" is the total number of Incidents that are or become Severity Level 3 or 4 that are Resolved within the relevant Resolution Time specified, divided by the total number of Incidents that are or become Severity Level 3 or 4 during the applicable Measurement Window, with the result expressed as a percentage. • = ((Number of Severity Level 3 Incidents Resolved within Limit) +(Number of Severity Level 4 Incidents Resolved within Limit)) / ((Total Number of Severity Level 3 Incidents) + (Total Number of Severity Level 4 Incidents)) expressed as a percentage
Collection Process	All infrastructure components with a Severity 3 and 4 incident tickets resolved during the measurement window will be included for calculation of the SL08 Resolution Time SLA. A Service Target in the BMC ITSM module will calculate the Mean Time to Resolve (MTTR) for each identified incident ticket using the times stamps of when the incident started and when the service was restored for the Configuration Item identified. The service target in the Service Level Management Module will calculate the compliance of the Severity 3 and 4 incident ticket(s) according to the SL08 definition.

	Inputs: • Incident Tickets (Severity 3 and 4)
Reporting Tools / Data Source(s)	The SL08 compliance will be recorded in the BMC ITSM Service Level Management Application and reported on Real-time Dashboard for all stakeholders to view and drill down into details. Outputs: • Notifications through email generated from BMC ITSM with communication status updates per time intervals defined for SL08 • SLA compliance will be displayed on Real-time Dashboard • SLA reports from BMC Analytics Data Sources: • BMC ITSM Incident Management Module • BMC ITSM Service Level Management Reporting Tools: • BMC ITSM Service Level Management • Real-time Dashboard • BMC Analytics
Data Storage (Archives)	Data storage is 13 months of history online with offline storage to tape with all supporting details.
Reporting Format/s	The SLA Incident Resolution Reporting format will be determined during transition. **Figure J-16** is a sample of a BMC Analytics Time Analysis sheet, **Figure J-17** is a BMC incident work sheet, and **Figure J-18** provides a sample view of the dashboard Incident SLA resolution time report:

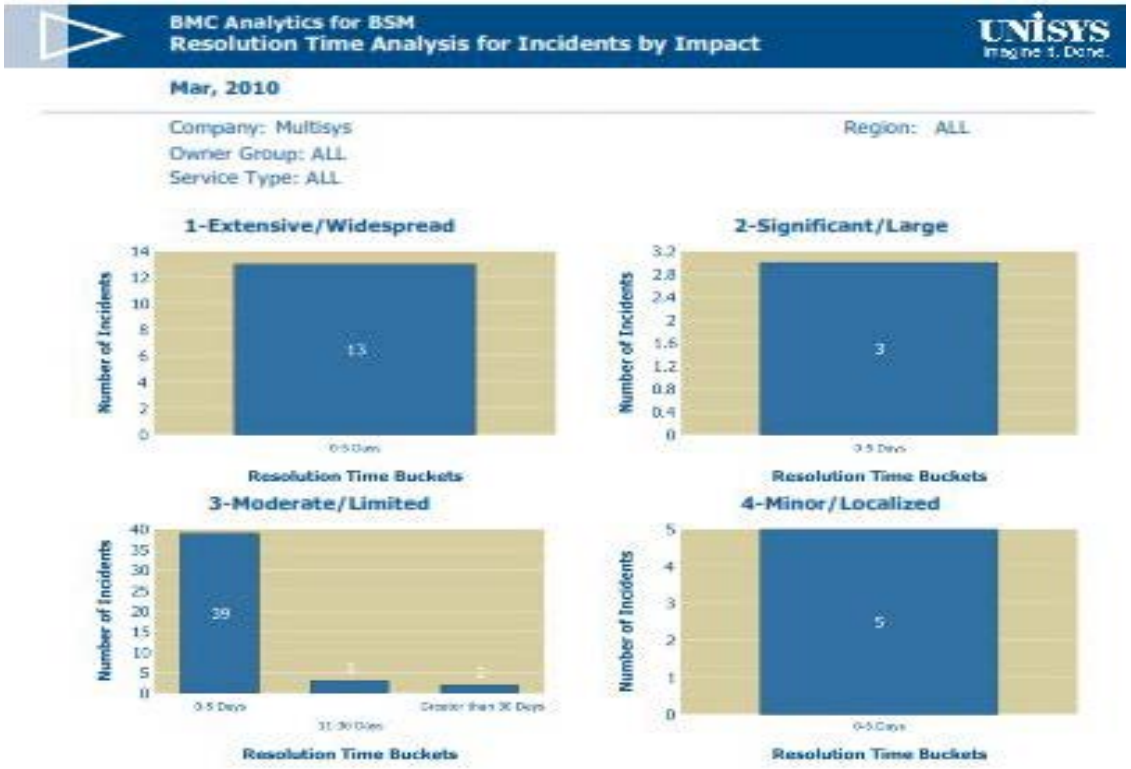


Figure J-16 SL08 BMC Analytics Diagram

3-Moderate/Limited

Incident ID	Summary	Resolution Time in Days	Assigned Group
INC000001207351	Test	Greater than 30	MULS-TEST
INC000001471615	Password Reset	11-30 Days	MULS-TEST
INC000001471804	Password Reset	11-30 Days	MULS-TEST
INC000001476697	Test for Onsite	11-30 Days	MULS-Desktop Resource
INC000001496012	test pls ignore	Greater than 30	MULS-Service Desk-EME/
INC000001530133	Test Ticket, please do not respond	0-5 Days	MULS-TEST
INC000001554453	AD Password reset for username	0-5 Days	MULS-TEST
INC000001554454	AD password reset for username	0-5 Days	MULS-TEST
INC000001554455	AD Password reset for username	0-5 Days	MULS-TEST
INC000001554456	AD Password reset for username.	0-5 Days	MULS-TEST
INC000001554457	AD password reset for Multest A001	0-5 Days	MULS-TEST
INC000001554461	Network account password reset	0-5 Days	MULS-TEST

bmcsoftware Generated Apr 26, 2010 12:08:12 PM

Figure J-17. SL08 BMC Analytics Table

Figure J-18 is a sample of the SLA Dashboard showing Incident Resolution times:

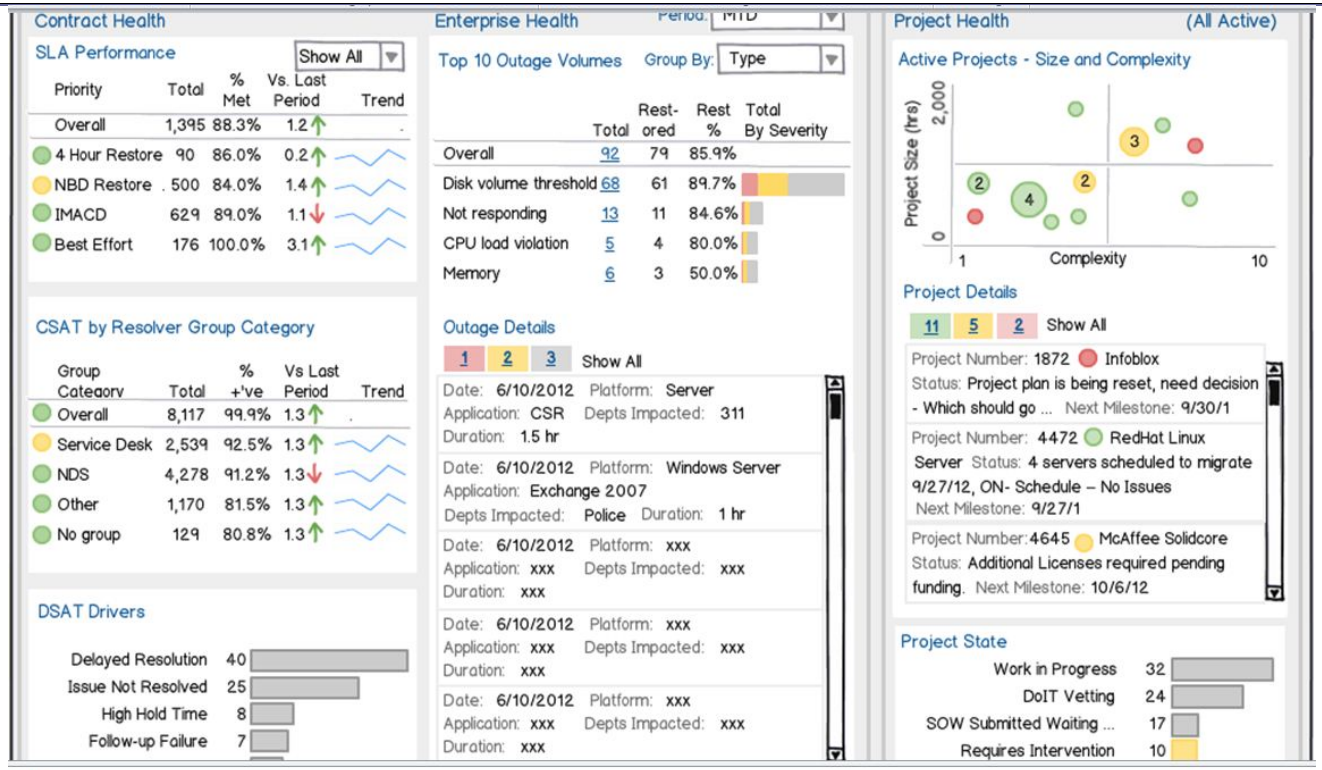


Figure J-18. SL08 Real-time Dashboard Incident Response Time Example

Service Level Reporting Window	Monthly

SL09 Solution Request Fulfillment

Service Level Reference	Description
Solution Request Fulfillment	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the percentage of time Offeror successfully implements a Solution Request within the timeframe committed to the requester as measured in the applicable Measurement Window. All phases of the Solution implementation process from the Commonwealth Customer approval of the Solution Proposal through implementation and the Commonwealth Customer acceptance into production are included in this measure.
Metric Inclusions	For purposes of calculating this Service Level, only those requests which require a solution proposal that has been accepted by the State will be included in the calculation. Solution Requests without a production date established by the time the order is received will be counted as a "missed" expectation.
Metric Exclusions	None
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is the total number of projects that are successfully completed during the applicable Measurement Window on are before the due date specified in the applicable Solution Proposal and/or a subsequent project plan, divided by the total number of projects that should have been completed during the applicable Measurement Window, with the result expressed as a percentage. • = (Number of Solution Requests Completed within Limit) / (Total Number of Solution Requests) expressed as a percentage
Collection Process	To support the Commonwealth Service Level for Solution Request Fulfillment, approved solution requests requiring a project plan will be tracked. The approved project completion date following the review of the documented project plan will be used to provide the tracked due date. The due dates will be added to the service request within the service request tracking tool and added to the project status reports. The reporting and calculations for the service level will occur based upon the data recorded in within the Service Request tracking tool and validated by the Project Status Reports. Input: • Approved Solution Request requiring a project plan • Approved Project Plan with Completion Date

Reporting Tools / Data Source(s)	Data Sources: • Project Plan • Service Request Tracking Tool • ITSM Change Management Reporting Tools: • Project Management Status Reports • Service Request Tracking Reports • Real-time Dashboards
Data Storage (Archives)	Online Storage – 13 months Tape Backups – Life of the Contract
Reporting Format/s	The Project Management Status reports will be generated using MS Project and MS Excel, the exact format and content will be determined through collaborative meetings with the Commonwealth during transition. The content and format of the Service Request tracking form will be determined through collaborative meeting with the Commonwealth during the transition. The SLA dashboard format will be determined during transition for display on the Real-time Dashboard. See **Figure J-19** for an example of the Real-time Dashboard.

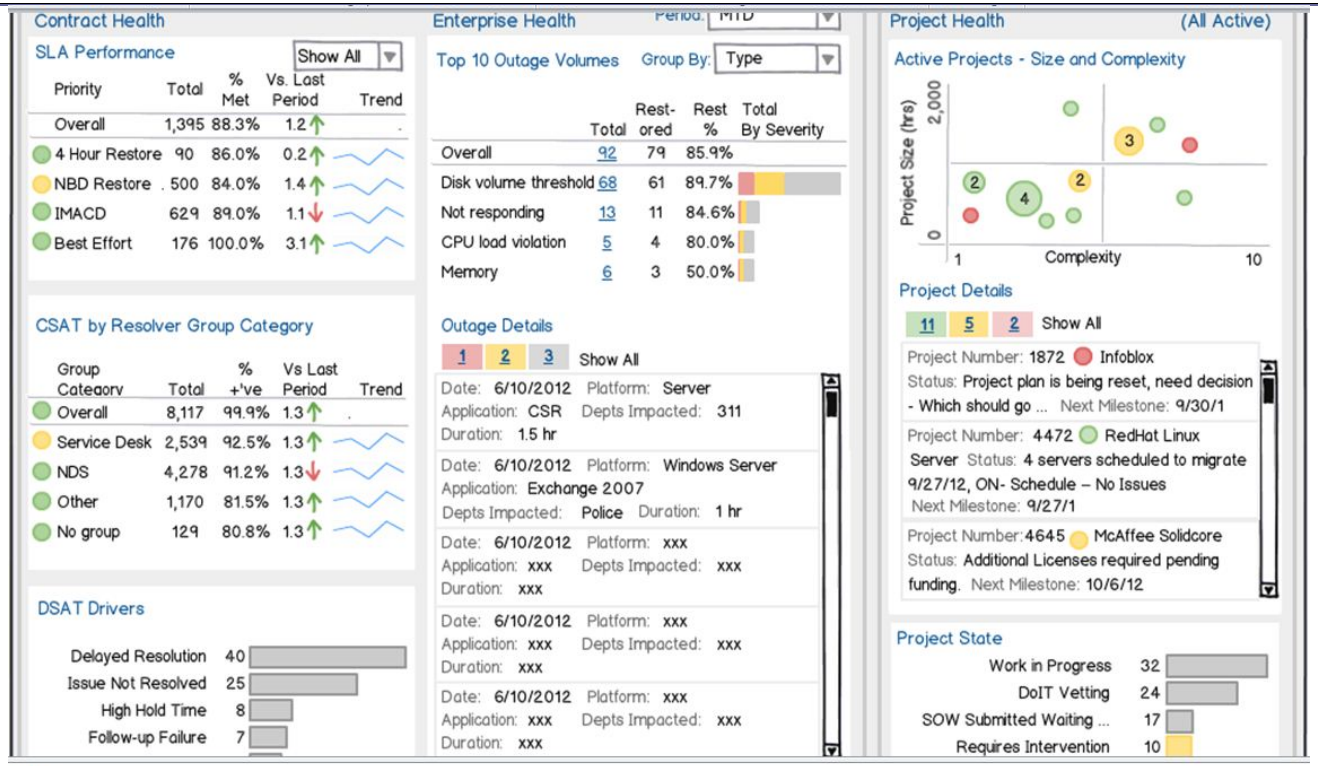


Figure J-19. SL03 Real-time Dashboard

Service Level Reporting Window	Monthly

SL10 Standard Service Request Fulfillment

Service Level Reference	Description
Standard Service Request Fulfillment	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the percentage of time Offeror successfully completes Standard Service Requests that do not require a purchase or a solution proposal to be approved by the State. Specific target timeframes are either established in the CCPM or a specific commitment date outside of the standard timeframe may be established at the State's discretion. Examples of these types of requests are provision of ID access, upgrade to a new OS version, run a special batch job, etc.
Metric Inclusions	Included as Standard Service Requests shall be an agreed upon set of service requests as specified in the Commonwealth Computing Procedures Manual.
Metric Exclusions	• Elapsed time waiting for the Commonwealth or a Commonwealth Customer's required approval or hold shall be excluded. • All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is the total number of Standard Service Requests successfully completed by Offeror during the applicable Measurement Window and within the required timeframes specified in Commonwealth Compute Procedure Manual (CCPM) or other agreed to date, divided by the number of Standard Service Requests that should have been completed by Offeror during the applicable Measurement Window, with the result expressed as a percentage. • = (Number of Standard Requests Completed within Limit) / (Total Number of Standard Requests) expressed as a percentage
Collection Process	To support the Commonwealth Service Level for Standard Service Request Fulfillment, standard service requests will be entered into the service request tool with date submitted and date completed. The type of service request will be identified in the service request record. This data will be used to calculate the SL10 calculations for reporting. The Commonwealth's standard service requests will be documented within the CCPM and include a description of the service, the tasks to be performed, and the timeframe for the service request's

	implementation. The tracking for each service request will begin with the submittal of the requests within the Service Request tool and end with its completion and acceptance update within the tool. Inputs: • Standard Service Requests
Reporting Tools / Data Source(s)	Data Sources: • Standard Service Requests Reporting Tools • Service Request tool • ITSM Change Management Modules • Real-time Dashboards
Data Storage (Archives)	Online Storage – 13 Months Tape Backups – Life of Contract
Reporting Format/s	The Change Management report format and content, and the Service Request tracking form, will be determined through collaborative meetings with the Commonwealth during transition. The SLA dashboard format will be determined during transition for display on the Real-time Dashboard. Real-time Dashboard is shown below in **Figure J-20**

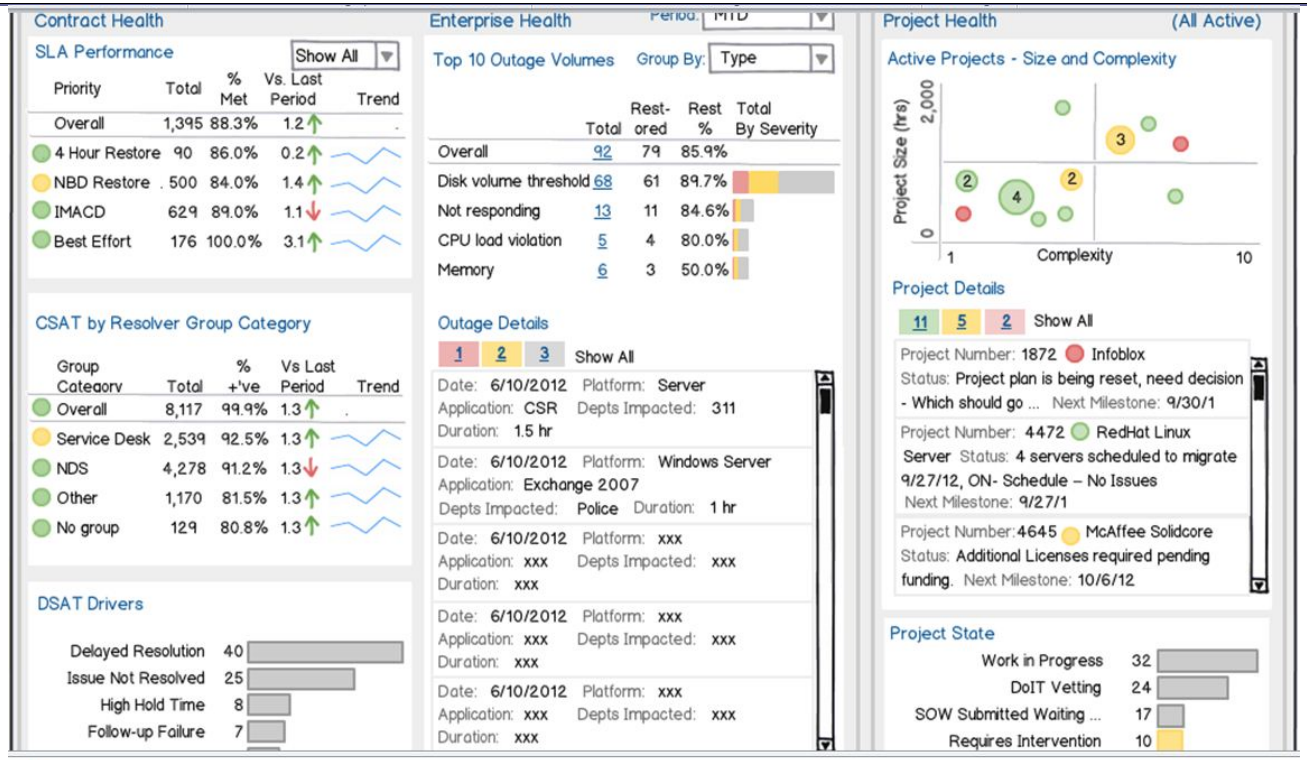


Figure J-20. SL10 Real-time Dashboard

Service Level Reporting Window	Monthly

SL11 Completion of Project/Solution Phase

Service Level Reference	Description
Completion of Project/Solution Phase	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the percentage of time Offeror successfully completes a phase (e.g. procurement, floor prep, network prep, physical install, turn-up and test, production) milestone no later than the committed timeframe. All phases of the Solution implementation process following the Commonwealth Customer approval of the Solution Proposal through implementation and the Commonwealth Customer acceptance into production are included in this measure.
Metric Inclusions	For purposes of calculating this Service Level, only those requests which require a solution proposal or project plan that has been accepted by the State and a production date established will be included in the calculation. If a milestone is missed, the rescheduled milestone will also be included in the measurement
Metric Exclusions	All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is the total number of Project or Solution Requests successfully completed by Offeror during the applicable Measurement Window and within the required timeframes specified in Commonwealth Compute Procedure Manual (CCPM) or other agreed to date, divided by the number of Project and Solution Requests that should have been completed by Offeror during the applicable Measurement Window, with the result expressed as a percentage • = (Number of Project/Solution Requests Completed within Limit) / (Total Number of Project/Solution Requests) expressed as a percentage
Collection Process	To maintain on time delivery of projects and support the Commonwealth's business operations, the Service Level for Project/Solution Phase Completion, approved solution requests requiring projects with multiple phases will be tracked. Each phase's due date, including the project's completion date, will be reviewed with the Commonwealth and, upon approval, recorded within the Service Request tool and documented in the Project Management Status Report for the individual service requests. As phases are performed and completed, the status will be recorded in the project plan, Service Request Tracking tool and the Project Status Reports. The reporting and calculations for the service level will occur based upon the data recorded within the Service Request Tracking tool and validated by the

	Project Status reports. Inputs • Approved Solution Requests requiring Project Plans with multiple Phases • Project Plan with approved dates for multiple phases.
Reporting Tools / Data Source(s)	Data Sources • Approved Project Plans with multiple phases • Approved Service Requests requiring project plans with multiple phases • Service Request Tracking Tool Reporting Tools: • Project Management Status Reports • Service Request Tracking Tool • Real-time Dashboard
Data Storage (Archives)	Online Storage – 13 months Tape Backups – Life of Contract
Reporting Format/s	The Project Management Status reports will be generated using MS Project and MS Excel, the exact format and content will be determined through collaborative meetings with the Commonwealth during transition. The content and format of the Service Request tracking form will be determined through collaborative meetings with the Commonwealth during the transition. The SLA dashboard format will be determined during transition for display on the Real-time Dashboard. **Figure J-21** is an example of the CIO Dashboard for SLA's:

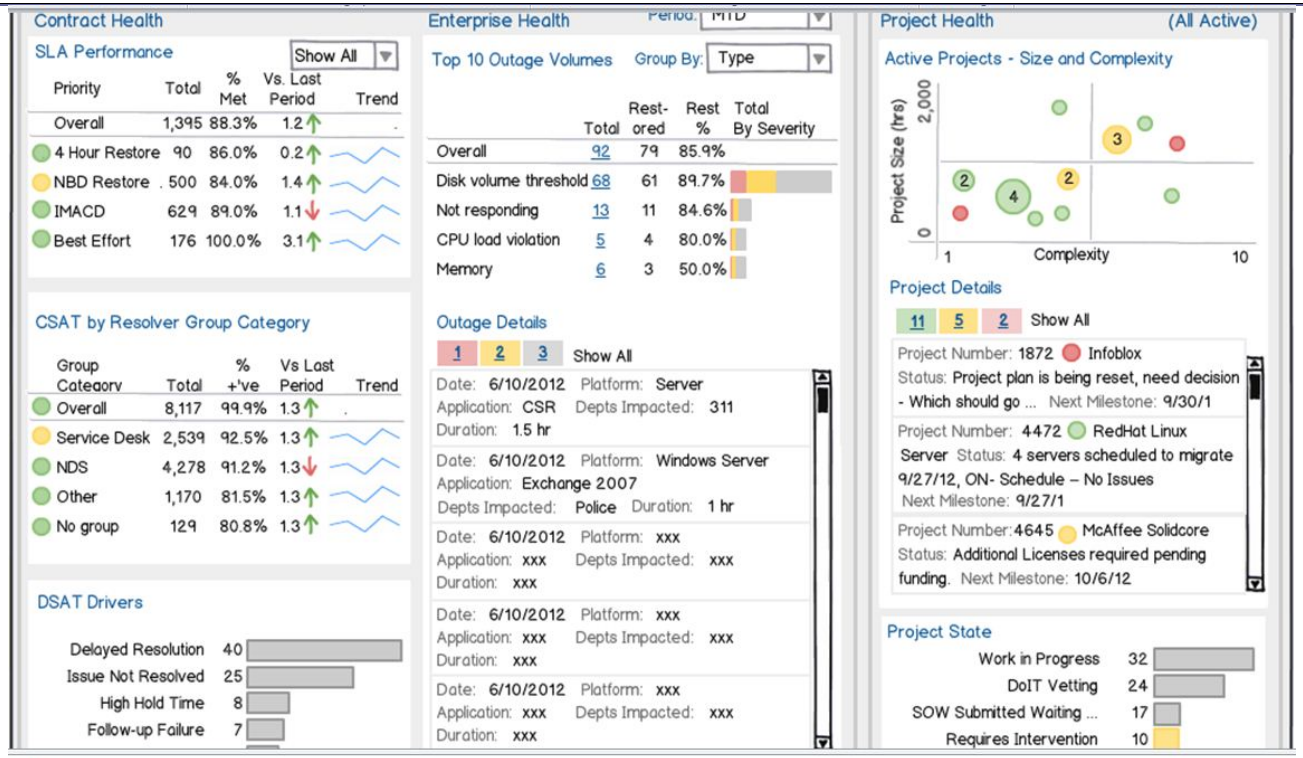


Figure J-21. SL11 Real-time Dashboard

Service Level Reporting Window	Monthly

SL12 Solution and Procurement Proposals Delivered

Service Level Reference	Description
Solution and Procurement Proposals Delivered	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the percentage of time Offeror provides a viable proposal to the State, in response to a solution or procurement request, within the timeframe established in the Commonwealth Computing Procedures Manual for commodity and standard requests or a jointly agreed to commitment date for custom requests.
Metric Inclusions	Each proposal submitted to the State will be considered a measurable event. If there are multiple proposals for one request due to requirements changes then subsequent iterations will be counted as another event. Each will count as an event and an opportunity to succeed or fail.
Metric Exclusions	• All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is the total number of viable proposals submitted to the State during the applicable Measurement Window on or before the due date determined from the Commonwealth Computing Procedures Manual for Standard and Commodity Requests or jointly agreed for custom requests, divided by the total number of proposals that should have been submitted during the applicable Measurement Window, with the result expressed as a percentage. • = (Number of Solution and Procurement Proposal Requests Completed within interval) / (Total Number of Solution and Procurement Proposal Requests) expressed as a percentage
Collection Process	As the Commonwealth's business needs continues to change, new solutions and procurement requests will be submitted to request support for the new requirements and to provide new and additional services or technology. The Service Level for the Delivery of Solution and Procurement Proposals will support multiple types of requests with several dates tracked within the Service request tool. The Commonwealth has identified several types of solution requests, which will require solutions or procurement activity and which will be tracked as part of this service level. 1) Statement of Objectives: Request covering multiple functional areas with additional procurement requirements or new services to be added to the Enterprise Services Catalog. 2) Work Order: Request covering multiple functional areas with no additional procurement

requirements and all services are within the existing Enterprise Services Catalog.

3) Service Requests: Request covering a single functional area with no additional procurement requirements and the services are within the existing Enterprise Services Catalog

4) Request for Technical Analysis: Technical Solution Research requests on possible solutions

5) Cost-Benefit Analysis: Research request to identify the cost benefit of new technologies and services

6) Conceptualization: Research request to identify possible technical options to fulfill an objective.

7) High Level Estimates: Research request to develop a rough order of magnitude cost quote

8) Technical Opinions: Research request to analyze technologies for technical merits and suitability within the Commonwealth environment

All Solution requests will be entered into the Service Request Tracking Tool and tracked until the request has been approved for implementation. The actual fulfillment of an approved solution will not be tracked by this Service Level, but will be tracked by SL09 (Solution Request Fulfillment) and SL11 (Completion of Project/Solution Phase).

To maintain the quality and timeliness of the solutions, the Service Level may include the time to collect, review and approve the requirements, but the final date for the delivery of the solution will not be established until after the requirements are agreed to with the Commonwealth. The SLA tracking will begin after the Requirements approval by the requesting Agency. If new requirements are received at any time after the requirements are approved by the Agency, the Service Level time measurement will be reset after the additional Agency review and updated date for the solution is submitted and approved.

The solution review's approval with the Commonwealth will be considered the final tracking item for this Service Level SL12. This date will be captured in the service request for custom solution requests.

Inputs

- Solution Request, including the type of service request
- Requester requirements confirmation
- Solution plan delivery date

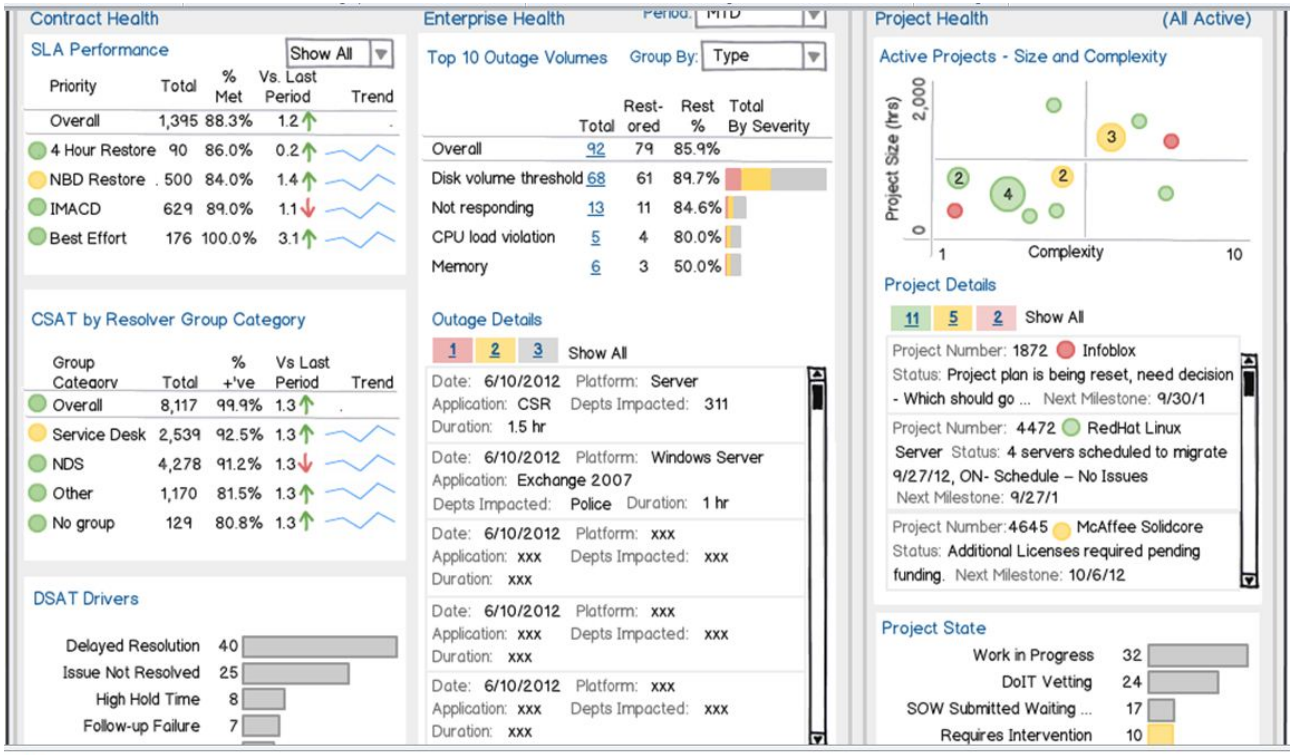
Reporting Tools / Data Source(s)	Data Sources • Service Request Tracking Tool Reporting Tools • Real-time Dashboard • Service Request Tracking Tool
Data Storage (Archives)	Online Storage – 13 months Backups – Life of Contract Completed Solutions – Knowledge Management Database and /or SharePoint
Reporting Format/s	The content and format of the Service Request tracking form will be determined through collaborative meetings with the Commonwealth during the transition. The SLA dashboard format will be determined during transition for display on the Real-time Dashboard. **Figure J-22** provides an example of the format we plan to use for SLA 12. 

	Figure J-22. SL12 Real-time Dashboard
Service Level Reporting Window	Monthly

SL13 CMDB Content Accuracy and Timeliness

Service Level Reference	Description
CMDB Content Accuracy and Timeliness	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the percentage of an audited statistically valid sample of Inventory Records (as defined below) during the Measurement Window that is determined to be Accurate (as defined below) by such audits.
Metric Inclusions	The audited sample for this Service Level must contain a number of randomly selected CMDB Inventory Records that is reasonably acceptable to the Commonwealth. The random selection shall be a statistically significant stratified random sampling representing all Commonwealth Customers each month. **Definitions for purposes of this Service Level:** "Accurate" means all Critical Inventory Attributes are correctly and completely populated in the CMDB Inventory of Record. "Critical Inventory Attributes" means those database fields in an Inventory Record that are essential for Offeror's successful delivery of Service and necessary for CoPA's successful performance of retained responsibilities, including architecture, IT planning, and reconciliation of invoices. Critical Inventory Attributes that shall be audited are set out in Commonwealth Computing Procedures Manual and may be modified over time in accordance with the Commonwealth Computing Procedures Manual. "CMDB Inventory of Record" means the inventory of CIs, including all Equipment and Software, to be created and maintained by Offeror in accordance with the CCPM. "Inventory Record" means the record for a single item of Equipment or Software in the Inventory of Record, including all of the Critical Inventory Attributes for that item.
Metric Exclusions	• All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is the total number of CMDB Inventory Records that are audited during the applicable Measurement Window and that are Accurate, divided by the total number of Inventory Records that are audited during the applicable Measurement Window, with the result expressed as a percentage.

	• = ((Number of Valid Records Found) / (Total Number of Records Audited)) expressed as a percentage
Collection Process	The Commonwealth will supply a list of Configuration Items (CIs) to be audited on the agreed monthly cycle. The CIs will be reviewed together with the Commonwealth to determine which attributes of the CIs are to be audited and the approach to auditing. The audit results will be recorded in a spreadsheet. The spreadsheet will contain the random sample CI description, location and the CMDB configuration attribute information extracted from the CMDB. The discovered or audited value for each CI and attribute will be recorded in the same spreadsheet and compared to the CMDB values. Any discrepancies will be noted and researched. The spreadsheet will calculate the SL13 compliance metrics to be reported.
Reporting Tools / Data Source(s)	The reporting tool will be Real-time Dashboard to display the SLA compliance calculation. The spreadsheet will be used to calculate the SLA compliance and to populate the SL13 Real-time dashboard. The details recorded in the spreadsheet will be used for analysis and a PowerPoint Presentation summarizing the results, analysis and recommendations for change will be created on a monthly basis.
Data Storage (Archives)	The spreadsheet and PowerPoint for summary review of results will be locked after analysis is completed and stored in the Services Portal for future access and review.
Reporting Format/s	The content and format of the SLA Compliance tracking will be determined through collaborative meetings with the Commonwealth during the transition. Formats for reporting audit results will be agreed to in transition for the PowerPoint audit results and spreadsheet detail formats. **Figure J-23** provides an example of how the SL13 results will be shown in the Real-time Dashboard.

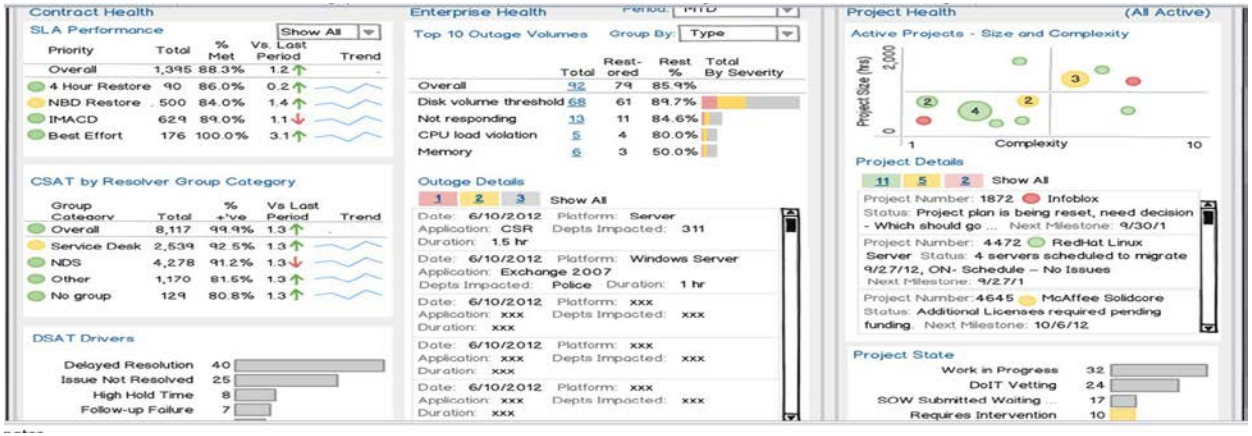


Figure J-23. SL13 Real-time Dashboard

Service Level Reporting Window	Monthly

SL14 Software License Renewal Timeliness

Service Level Reference	Description
Software License Renewal Timeliness	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the timeliness of all license and maintenance renewals for software managed by Offeror.
Metric Inclusions	This SLA includes the renewal of software licenses included in the Agreement and hardware maintenance agreements included in Hardware Service Charges (HSC) to a the Commonwealth Customer (e.g. renewal of SSL certificates, Application Utility software, custom solution hardware (covered by a maintenance agreement) charged to the Commonwealth Customer through the HSC).
Metric Exclusions	• Renewals for software or maintenance purchased outside of this contract by the Commonwealth or the Commonwealth Customers and not included in Offeror's charges to the Commonwealth are excluded. • All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	This Service Level measures the timeliness of all license and maintenance renewals for software managed by Offeror.
Days of Measurement	N/A
Calculation	• **Summary:** Renewals are routinely expected to be installed ten (10) or more Business Days prior to the renewal due date for the item or service. (Renewal due date is the date when the current license or maintenance contract expires.) The Service Level calculation for "Software License Renewal Timeliness" is a percentage derived from the total number of all renewals processed divided by the total number due for the month that were renewed before the renewal expiration date without disruption in service. • = ((Successful Software Renewals implemented within Time Frame) / (Total Software License Renewals Completed)) expressed as a percentage
Collection Process	To support the Commonwealth Service Level for the timeliness of Software maintenance renewals, the hardware and software maintenance renewals for the components used to support the services provided and the maintenance renewals for software licenses from Exhibits B.4 and B.10 will be tracked. The software and hardware used by the Unisys team or hosted using our services will be tracked within the ITSM Asset Management module. As maintenance renewal cycles occur, the License

	Manager will use the data stored within the Asset Management module to identify the software and hardware to renew prior to the required renewal date. The updated expiration dates will be added to the Asset Management data. Within a set timeframe defined within the CCPM, an email will be generated by the ITSM Asset Management and Notification system and sent to authorized Commonwealth and Unisys staff to communicate when renewals are required. As additional software and hardware is added into the service, the additional maintenance renewal requirements will be added into the Asset Management module. For software which is removed from active service, the Asset Management data will be updated to reuse the software or hardware or, upon retirement, the Asset Management data will be updated to document the actual retirement. SL14 will be calculated by the Service Level Management Application utilizing maintenance renewal target date and updates for completed renewals for software and hardware maintenance contract renewal requirements compared to the SLA requirement of all renewals completed 10 days prior to expiration. Inputs: BMC Asset data for : • Software License and Hardware Maintenance contract begin and end dates • Software Licensing certificates • SSL certificate Purchase and Expiration dates
Reporting Tools / Data Source(s)	Data Sources: ITSM Remedy Asset and Service Level Management Applications Reporting Tools: • Real-time Dashboard • BMC ITSM Remedy • BMC ITSM Remedy email notification for maintenance renewals
Data Storage (Archives)	Online – 13 months Tape Backups – Life of Contract
Reporting Format/s	The SLA dashboard format will be determined during transition for display on the Real-time Dashboard. **Figure J-24** provides an example of the Real-time Dashboard:

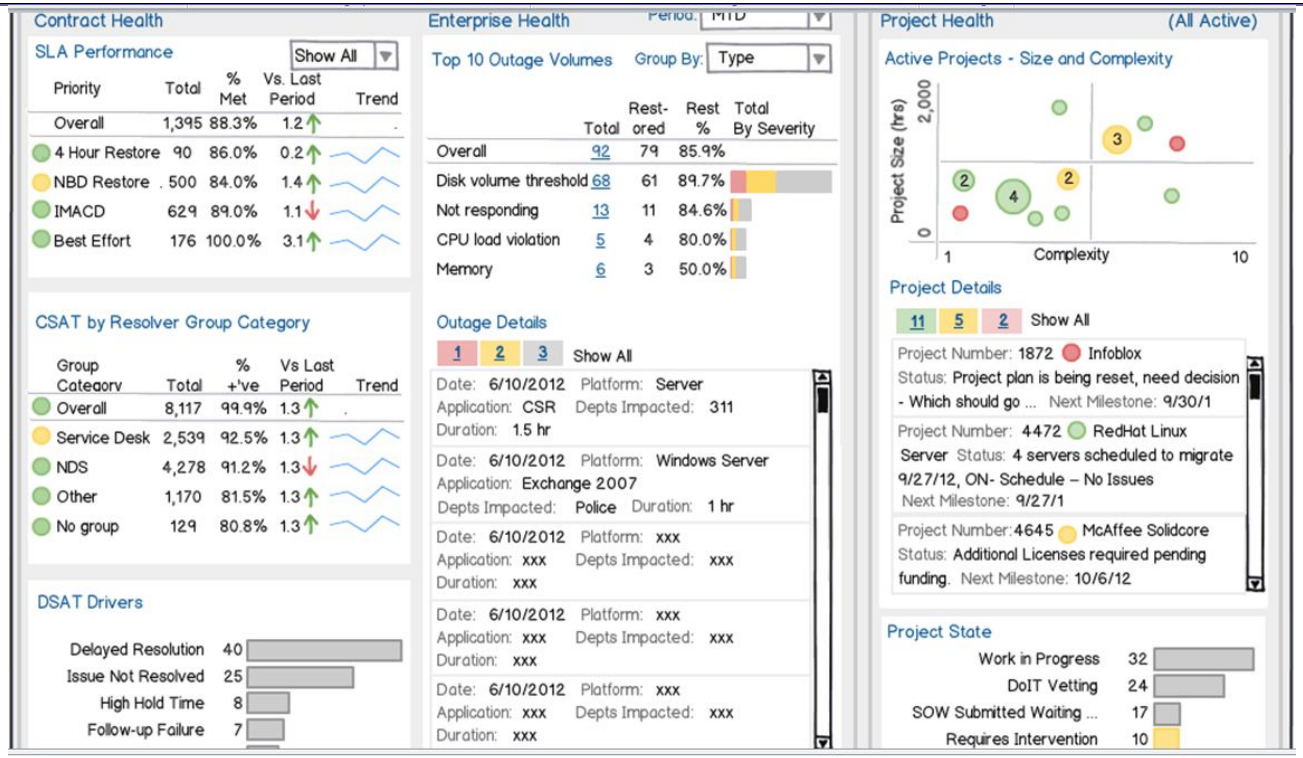


Figure J-24. SL14 Real-time Dashboard

Service Level Reporting Window	Monthly

SL15 Successful Backups

Service Level Reference	Description
Successful Backups	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the percentage of time Offeror completes backup jobs successfully during the applicable Measurement Window in accordance with the relevant criteria specified in the Commonwealth Computing Procedures Manual.
Metric Inclusions	Backup jobs include all registered backup clients (including but not limited to all file systems, databases, application files, operating systems, applications and respective data).
Metric Exclusions	• If there is an appropriate tool available and in use that captures open files, then the backup of open files are included as part of the backup. If there is not an appropriate tool available and in use for the capture of open files, then open files are skipped and not counted against this Service Level. Any batch jobs related to infrastructure backups, or other functionality exclusively for Offeror would be excluded. • All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level is the sum of the number of times Offeror completes backup jobs successfully and complete on time during the applicable Measurement Window divided by the of the sum of the number of times Offeror began or should have begun backup jobs within the applicable measurement window, with the result expressed as a percentage. • = ((Number of Successful Backups) / (Total Number of Backups Attempted)) expressed as a percentage
Collection Process	Success/failure data from the CommVault tool used to backup data will be used to calculate the SLA. Backup failures will be captured in the ITSM system. Count of successful and total backups can be exported out of CommVault. The SLA will be displayed in the SLA dashboard and reported monthly as part of the BMC Analytics SLA Summary Report. Inputs: • CommVault success/failure data
Reporting Tools / Data Source(s)	The SL15 compliance will be recorded in the BMC ITSM Service Level Management Application and

	displayed on the Real-time Dashboard for all stakeholders to view and drill down into details. Data Sources: • CommVault Reporting Tools: • BMC Service Level Management Module • Real-time Dashboard • BMC Analytics Reporting Outputs: • SLA compliance will be displayed on Real-time Dashboard • BMC Analytics SLA Monthly Report
Data Storage (Archives)	Data storage is 13 months of history online with offline storage to tape with all supporting details `
Reporting Format/s	The SLA dashboard format will be determined during transition for display on the Real-time Dashboard. **Figure J-25** is a dashboard (back page) example:

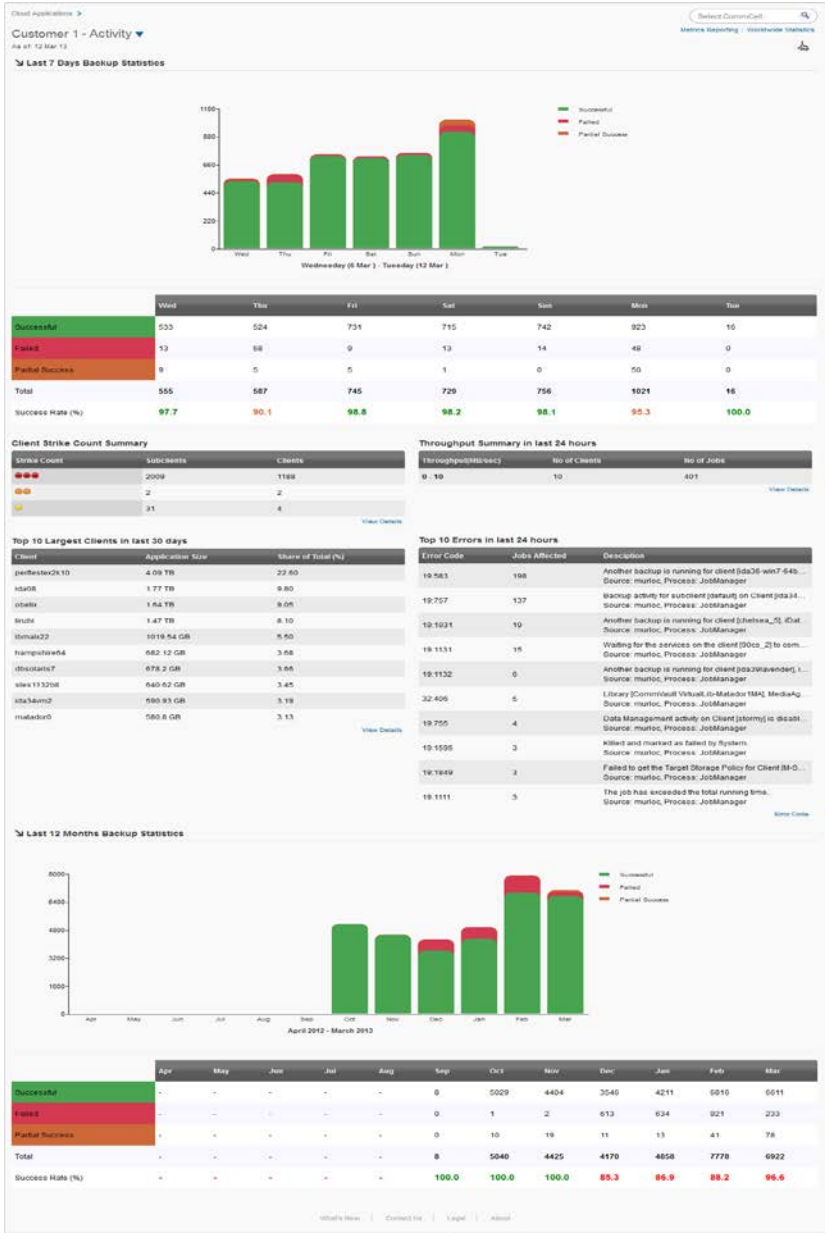


Figure J-25. SL03 Real-time Dashboard

Service Level Reporting Window	Monthly

SL16 Successful Recoveries

Service Level Reference	Description
Successful Recoveries	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the percentage of time Offeror completes data recoveries successfully and on time during the applicable Measurement Window in accordance with the relevant criteria specified in the Commonwealth Computing Procedures Manual.
Metric Inclusions	Recoveries include all registered recovery clients (including but not limited to all file systems, databases, application files, operating systems, applications and respective data).
Metric Exclusions	• Any batch jobs related to infrastructure recoveries, or other functionality exclusive for the Offeror would be excluded. • All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is the total number of data recovery jobs that are completed successfully and on time in accordance with the relevant criteria set forth in the Commonwealth Computing Procedures Manual during the applicable Measurement Window, divided by the total number of data recovery jobs that were attempted or scheduled to be completed during the applicable Measurement Window, with the result expressed as a percentage. • = ((Number of Successful Recoveries) / (Total Number of Recoveries Attempted)) expressed as a percentage
Collection Process	A service request ticket for data restore jobs will be updated with success/failures outcomes according to the defined CCPM procedure for calculating SL16. The service request ticket will be updated manually with the success/failure data from the procedure and CommVault Tool used to restore data. The Service Level Management Module will be used to calculate the SLA from the service request tickets for data restores by examining the success/failure status of the tickets. The SLA will be displayed in the SLA dashboard and reported monthly as part of the BMC Analytics SLA Summary Report. Inputs: • Service Request Tickets (for data restores) • CommVault success/failure data

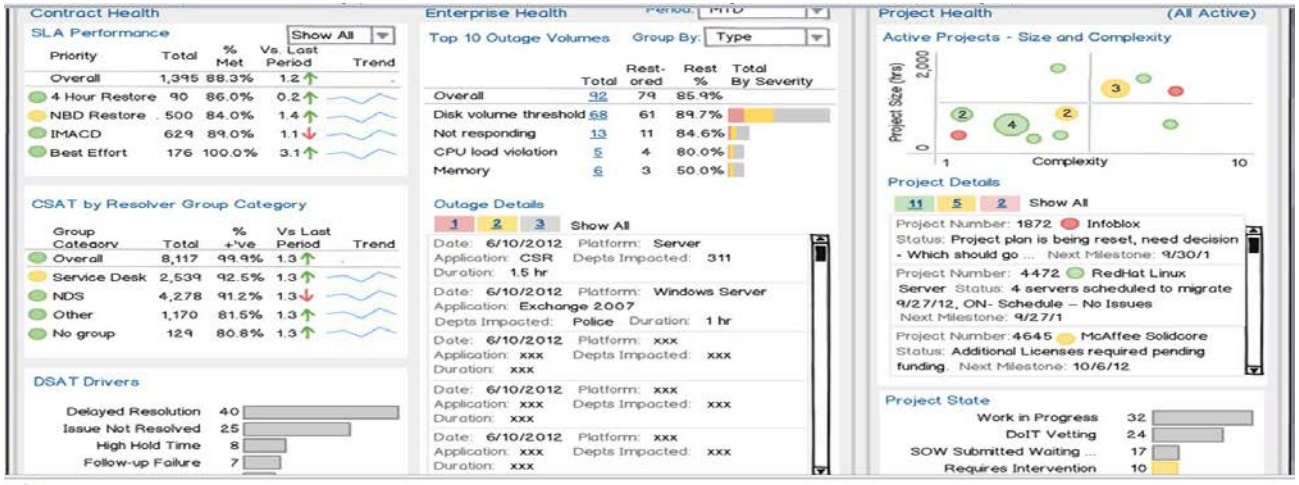
Reporting Tools / Data Source(s)	The BMC Service Level Management Application will be configured with service targets to calculate SL16 for data restore service requests. The SLA will be displayed on the Real-time Dashboard for all stakeholders to view and drill down into details. Outputs: • SLA compliance will be displayed on Real-time Dashboard • SLA reports from BMC Analytics Data Sources: • Service Request Tickets Reporting Tools: • Real-time Dashboard • BMC Analytics Monthly Summary SLA Report
Data Storage (Archives)	Data storage is 13 months of history online with offline storage to tape with all supporting details.
Reporting Format/s	The SLA dashboard format will be determined during transition for display on the Real-time Dashboard. **Figure J-26** is an dashboard (back page) example:

Figure J-26. SL16 Real-time Dashboard

Service Level Reporting Window	Monthly

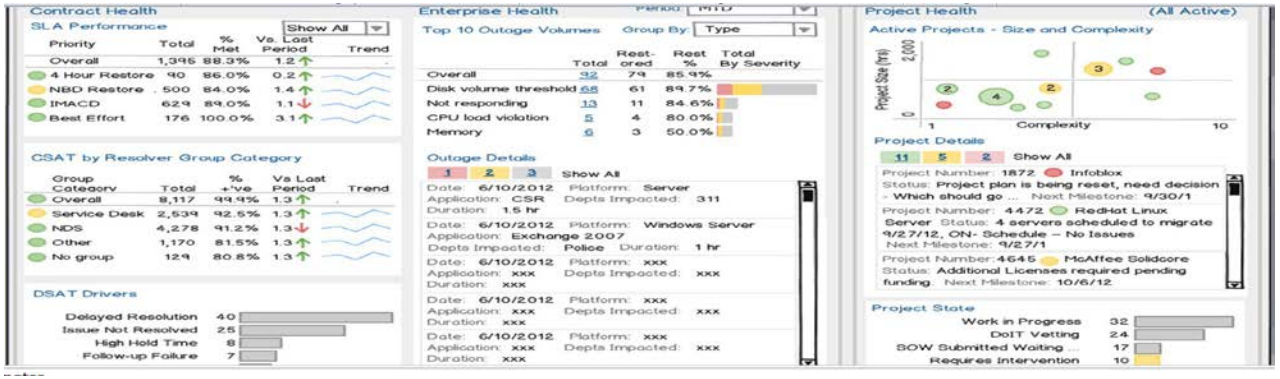
SL17 Security Incident Notification Timeliness

Service Level Reference	Description
Security Incident Notification Timeliness	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the percentage of time Offeror completes identifying and notifying CoPA of detected security incidents in accordance with ITB-SEC024.
Metric Inclusions	Time required receiving and analyzing reactive and/or proactive incidents from any and all managed sources including, but not limited to, firewalls, intrusion detection/prevention devices, VPN appliances, switches, routers, and all other equipment over which Commonwealth traffic traverses. Time required contacting CoPA and reporting the incident in accordance with ITB-SEC024.
Metric Exclusions	• All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is the total number of Security Incidents reported in accordance with ITB SEC-024 using the procedure set forth in the Commonwealth Computing Procedures Manual, divided by the total number of detected security incidents, with the result expressed as a percentage. • = [(number of incidents reported in accordance with ITB SEC-024) / number of detected incidents)] expressed as a percentage
Collection Process	All detected security incidents will be collected in the ArcSight tool from any and all managed sources including, but not limited to, firewalls, intrusion detection/prevention devices, VPN appliances, switches, routers, and all other equipment over which Commonwealth traffic traverses and will be forwarded and recorded in the BMC ITSM toolset. The ArcSight tool will set a data field on the incident record forwarded to BMC ITSM that indicates the incident is in accordance with ITB SEC-024. This flag will be used by the BMC ITSM Service Level Management (SLM) Application to calculate the SLA. The Commonwealth will be notified through email for every recorded security incident following the incident management process and in accordance with ITB SEC-024. The SLA will be calculated and recorded. Input: • Detected Security Incident

	• Recorded Incident in BMC ITSM Toolset
Reporting Tools / Data Source(s)	SL17 compliance will be recorded in the BMC ITSM Service Level Management Application and reported on Real-time Dashboard for all stakeholders to view and drill down into details. Output: • SLA compliance will be displayed on Real-time Dashboard • SLA reports from BMC Analytics Reporting Tools • Real-time Dashboard • BMC Analytics for SL17 Summary Report Data Sources • ArcSight database for security events and incidents • BMC ITSM database for security incidents and service level targets
Data Storage (Archives)	Data storage is 13 months of history online with offline storage to tape with all supporting details.
Reporting Format/s	The reporting format will be determined during transition for display on the Real-time Dashboard. **Figure J-27** is a dashboard example:  **Figure J-27. SL03 Real-time Dashboard**
Service Level Reporting Window	Monthly

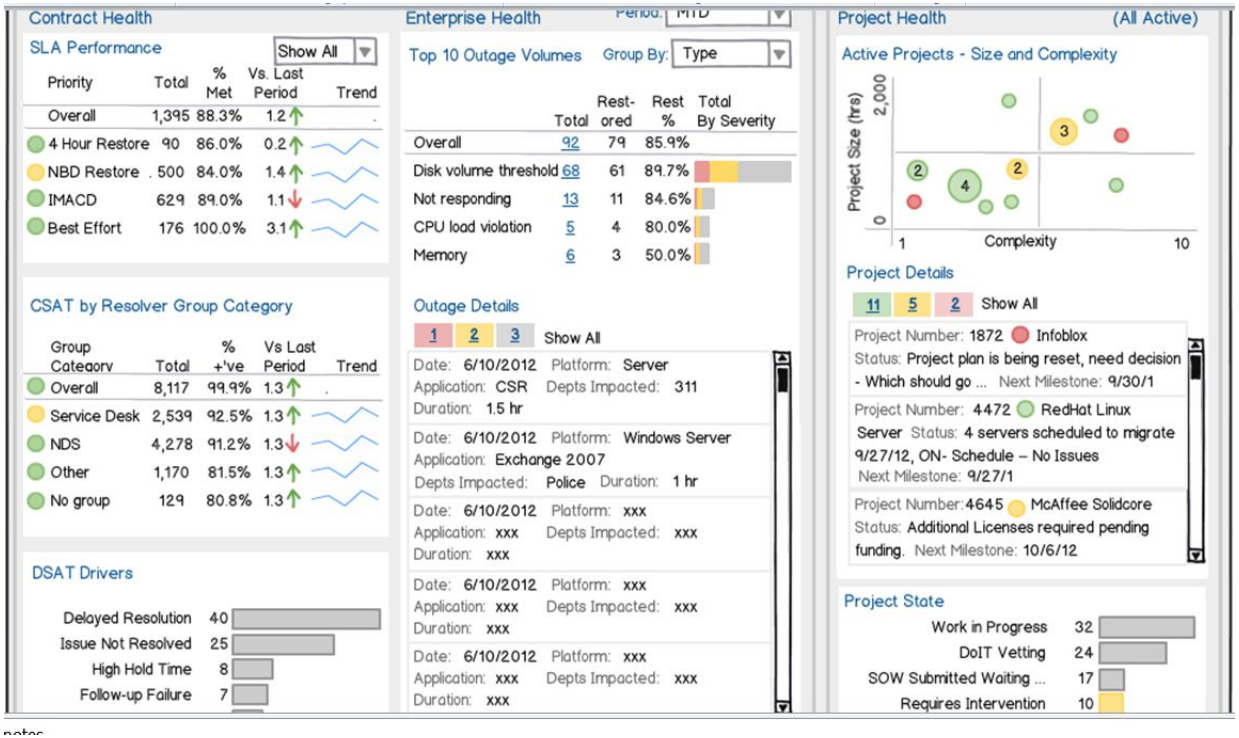
SL18 Security Update Timeliness

Service Level Reference	Description
Security Update Timeliness	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the percentage of time Offeror completes Security Updates successfully and on time during the applicable Measurement Window in accordance with the relevant criteria specified in the Commonwealth Computing Procedures Manual.
Metric Inclusions	Security Updates include all updates and changes designated as a Security Update at the time or request/order. These updates includes, but are not limited to, Security Patches, Firewall configuration changes, Proxy updates and changes, and Identity Management Changes.
Metric Exclusions	• Any batch jobs related to infrastructure recoveries, or other functionality exclusive for the Offeror would be excluded. • All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is the total number of Security update requests that are completed successfully and on time in accordance with the relevant criteria set forth in the Commonwealth Computing Procedures Manual during the applicable Measurement Window, divided by the total number of Security update requests that were requested to be completed during the applicable Measurement Window, with the result expressed as a percentage. • = ((Number of Security Updates) / (Total Number of Requested Security Updates)) expressed as a percentage
Collection Process	After a determination has been made by the security team that a security update is needed, a change request is created to be implemented during the appropriate security change window. Priority and schedule for the SLA will be determined based on the CCPM and recorded in the change request. The change request will include the implementation date of the security update and the SLA will be calculated. Input: • Security team determination of a security update requirement • A change request

	• Implementation date of the change
Reporting Tools / Data Source(s)	The SL 18 compliance will be recorded in the BMC ITSM Service Level Management Application and reported on Real-time Dashboard for all stakeholders to view and drill down into details. Output: • SLA compliance will be displayed on Real-time Dashboard • SLA reports from BMC Analytics Reporting Tools: • Real-time Dashboard • BMC Analytics Data Sources: • BMC ITSM data including Change tickets and SLM targets
Data Storage (Archives)	Data storage is 13 months of history online with offline storage to tape with all supporting details.
Reporting Format/s	The reporting format will be determined during transition for display on the Real-time Dashboard. **Figure J-28** is a dashboard example:  **Figure J-28. SL18 Real-time Dashboard**
Service Level Reporting Window	Monthly

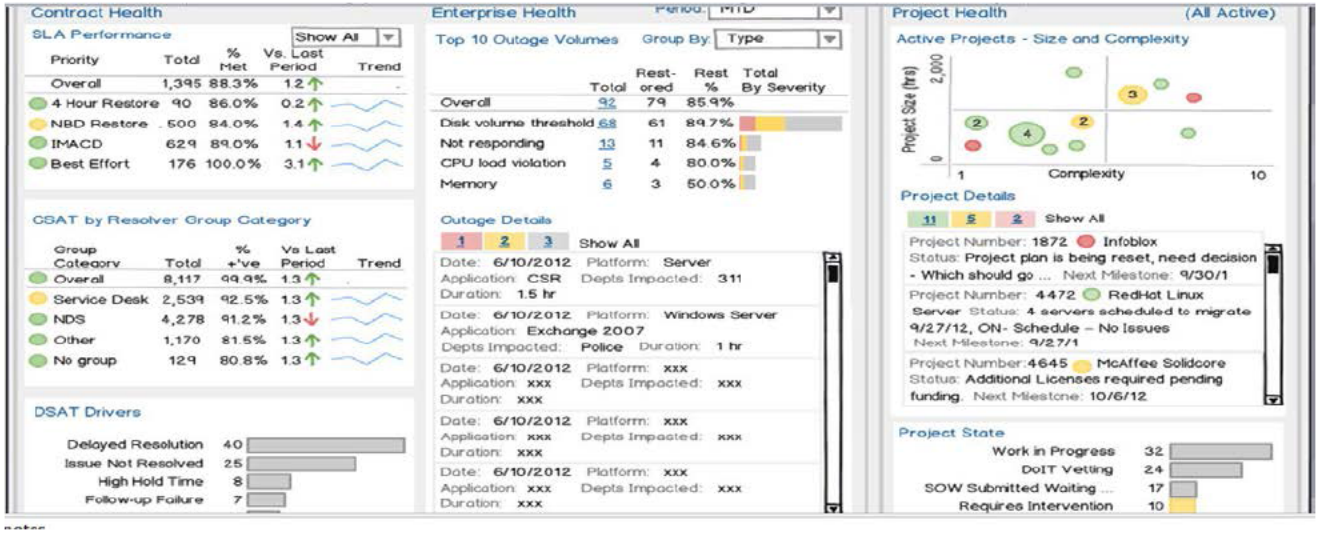
SL19 Incident Management Communication – for Severity 1 Incidents

Service Level Reference	Description
Incident Management Communication – for Severity 1 Incidents	
Service Category	Incident & Problem Resolution
Metric Description	This Service Level measures the percentage of time the Offeror provides the notices to the applicable Authorized Users within the following timeframes with respect to Incidents that are or become Severity 1 Incidents and that are not Resolved in less than one (1) hour from the Start Time for such Incident. •□ First notice: Within one hour of incident ticket creation •□ Subsequent notices: every 30 minutes A "notice" is defined as : •□ Verbal communication to Authorized User, as documented in the ticket •□ Bridge call including Authorized User, as documented in the ticket •□ Email to Authorized User, as documented in the ticket Such notices shall not be deemed to have been provided unless (a) the Authorized User that reported the Incident has been contacted by the Offeror and such notice of status has been provided or (b) Offeror has left a voice mail (or if not possible because the Authorized User does not have a voice mail box, sent an email or attempted some other reasonable means of communication) for the Authorized User.
Metric Inclusions	Includes all Priority 1 Incidents
Metric Exclusions	•□ Priority 2, 3 and 4 Incidents •□ Duplicate Incident Reports for the incident •□ All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	•□ **Summary:** This Service Level calculation is the total number of Incidents that are or become Severity 1 Incidents, that have Start Times during the applicable Measurement Window, that have actual Resolution Times of greater than one (1) hour and for which Offeror provided the applicable Authorized User the required notice(s) within the required timeframe(s) as set forth in this Section, divided by the total number of Incidents that are or become Severity 1 Incidents, that have Start Times during the applicable Measurement Window and that have actual Resolution Times of

	greater than one (1) hour, with the result expressed as a percentage. •□ = ((Number of Incidents with Communications within Established Intervals) / (Total Number of Severity 1 Incidents)) expressed as a percentage
Collection Process	All communications to authorized users in the Commonwealth for Priority tickets will be recorded on the incident ticket (priority 1 only) with a time stamp until the incident ticket is resolved with a restored service. A service target in the Service Level Management Module will calculate the compliance of communication on the Priority 1 incident ticket according to the definition of SL19.
Reporting Tools / Data Source(s)	The SL19 compliance will be recorded in the BMC ITSM Service Level Management Application and reported on Real-time Dashboard for all stakeholders to view and drill down into details as configured.
Data Storage (Archives)	Data Storage is 13 months of history online with offline storage to tape with all supporting details.
Reporting Format/s	The reporting format will be determined during transition for display on the Real-time Dashboard. **Figure J-29** is an example:  **Figure J-29. SL19 Real-time Dashboard**
Service Level Reporting Window	Monthly

SL20 Root Cause Analysis Delivery

Service Level Reference	Description
Root Cause Analysis Delivery	
Service Category	Incident & Problem Resolution
Metric Description	This Service Level measures the percentage of time Offeror reports the results of a Formal Root Cause Analyses for Service Restoral Incidents within the timeframes below during the Measurement Window: • RCA's due within ten (10) Business Days from the request of the RCA.
Metric Inclusions	An Authorized User may request a Formal RCA for incidents that require more in-depth analysis than required with the "normal" Root Cause Analysis process. The Formal RCA is documented and tracked within the Problem Management process, and upon completion, is presented by the Offeror Problem Management Team to the affected the Commonwealth Customer and the Commonwealth for review and approval. Offeror shall perform a "Formal" Root Cause Analysis with respect to any Service Restoral Incident, if requested by the Commonwealth, and that has a Start Time during the applicable Measurement Window.
Metric Exclusions	• Those Service Restoral Incidents for which the Commonwealth or the Commonwealth's Customer does not request a "Formal" Root Cause Analysis. • Duplicate Requests • All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is the total number of written Formal Root Cause Analyses that are delivered to the Commonwealth within the timeframes specified in this Section during the applicable Measurement Window, divided by the total number of written Formal Root Cause Analyses that should have been delivered to the Commonwealth during the applicable Measurement Window, with the result expressed as a percentage. • = ((Number of Formal Root Cause Analyses Delivered within Established Interval) / (Total Number of Formal Root Cause Analyses Due)) expressed as a percentage
Collection Process	The Commonwealth will request a formal RCA for selected problems. The request will be recorded within the problem ticket. A service target from the Service Level Management (SLM) application in

	Remedy ITSM will monitor and calculate the time it takes to issue a formal RCA that will also be recorded in the problem ticket. The SLM application will alert when there is an SLA violation in the Real-time dashboard, when the RCA report has not been completed within 10 days and report SL20 compliance in the SLA Monthly Summary Report.
Reporting Tools / Data Source(s)	The SL20 compliance will be recorded in the BMC ITSM Service Level Management Application and reported on Real-time dashboard for all stakeholders to view and drill down into details as configured. SL20 compliance will also be reported in the SLA Monthly Summary Report.
Data Storage (Archives)	Data Storage is 13 months of history online with offline storage to tape with all supporting details.
Reporting Format/s	The SLA dashboard format will be determined during transition for display on the Real-time Dashboard. **Figure J-30** is a dashboard example:  **Figure J-30. SL20 Real-time Dashboard** The SLA Reporting format will be determined during transition for reporting using BMC Analytics Reporting. **Figure J-31** is an example [redacted]

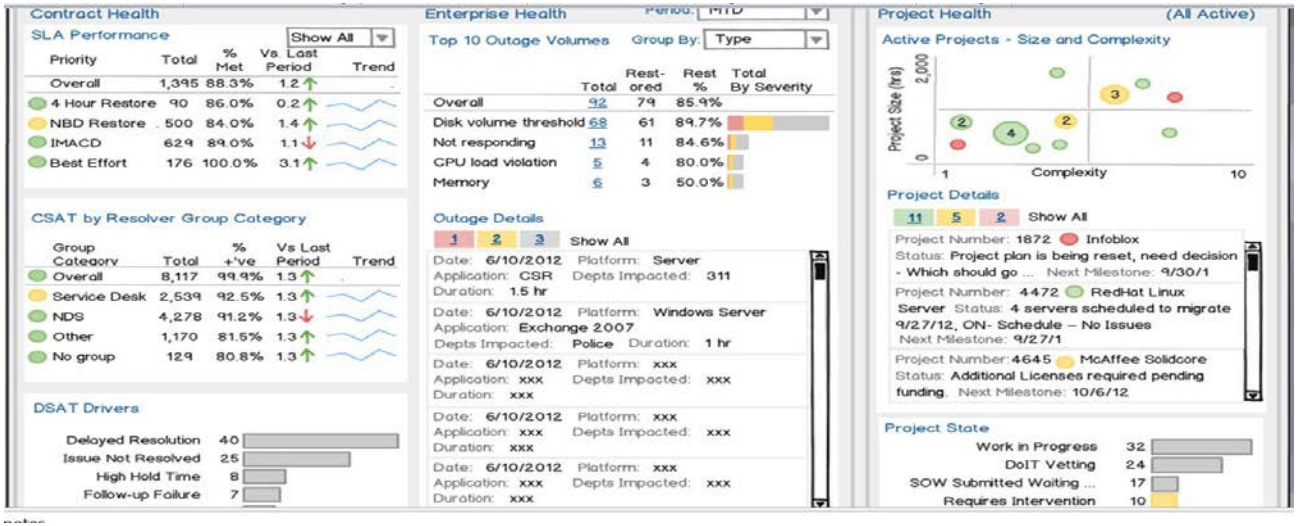
Environment	Component	SLA	Allowed Minutes March	Minutes Down w/e 3/3	w/e 3/10	w/e 3/17	w/e 3/24	w/e 3/31	Remaining Minutes
DPW HSH-A	System	99.90%	45	0					45
	TIP	99.90%	45	0					45
	WEBTS	99.70%	134	0					134
	WEBTWO	99.70%	134	0					134
	OLTP	99.90%	45	0					45
DPW HSH-C	System	99.90%	45	28					17
	TIP	99.90%	45	0					45
	MAPPER	99.90%	45	0					45
	APPMAP	99.90%	45	0					45
	OLTP	99.90%	45	0					45
DPW HSH-F	System	99.90%	45	0					45
	TIP	99.90%	45	0					45
PSP	System	99.90%	45	0					45
	TIP	99.87%	58	0					58
	MAPPER	99.90%	45	0					45
GAME	System	99.90%	45	0					45
	COMS	99.90%	45	0					45
DOS L2K	System	99.90%	30	0					30
	SQL Server	99.90%	30	0					30
DOS SURE	System	99.80%	35	0					35
	SQL Server	99.90%	30	0					30
	SRS Application System	99.90%	45	0					45
	SRS SQL System	99.90%	45	0					45
	Virtual Citrix Print Servers	99.50%	223	0					223
DOI Web Envir	System	99.90%	20	0					20
	IIS	99.70%	59	0					59
DOI	System	99.70%	61	0					61

Figure J-31. SL20 BMC Analytics Reporting

Service Level Reporting Window	Monthly

SL21 Chronic Problems

Service Level Reference	Description
Chronic Problems	
Service Category	Incident & Problem Resolution
Metric Description	A "Chronic Problem" means a problem which meets any of the following criteria: 1. The existence two or more incidents with the same root cause for the same software, service, process, or hardware for which Offeror, the Commonwealth, or the Commonwealth Customer, have designated as a problem requiring a Root Cause Analysis with a Corrective Action Plan. 2. The existence of three or more service failures or outages for the same software, service, process, or hardware within the same month for any two (2) months within any rolling six (6) months. 3. The existence of three (3) or more service failures or outages for the same software, service, process, or hardware within any rolling six (6) month period for which no root cause has been determined. Multiple Incidents that are opened contemporaneously for the same software, service, process, or hardware due to the same root cause shall be deemed to be a single incident for purposes of this Service Level.
Metric Inclusions	All incidents and Problem Investigation reports for all services covered by any service level metric.
Metric Exclusions	• Problems which have a published Root Cause Analysis with an associated action plan approved by the Commonwealth Customers and which has all agreed corrective actions on schedule (not exceeding their completion dates) and have had no reoccurrences of the same failure may be excluded at the Offeror's request and the Commonwealth's approval. • All items defined in Note 2 at the bottom of this Schedule J.3 • Duplicate Incident Reports for the same Incident
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** Offeror's performance shall be measured by determining the total number of Problem that are or become Chronic Problem during the applicable Measurement Window. • ((the number of Chronic Problems) / (the total number of problems)) expressed as a percentage
Collection Process	The collection process requires the Service Level Management (SLM) application in Remedy ITSM to be configured for service targets to identify, track and record Chronic Problems as defined above. The

	collection process will calculate SL21 using the number of identified Chronic Problems identified and the total number of problem records for the appropriate timeframe to report SL21.
Reporting Tools / Data Source(s)	The SLM application will alert when there is an SLA violation in the Real-time dashboard, when the Chronic Problem threshold has been exceeded and report SL21 compliance in the SLA Monthly Summary Report.
Data Storage (Archives)	Data Storage is 13 months of history online with offline storage to tape with all supporting details.
Reporting Format/s	The SLA dashboard format will be determined during transition for display on the Real-time Dashboard. **Figure J-32** is an example:  **Figure J-32. SL21 Real-time Dashboard** The SLA Reporting format will be determined during transition for reporting using BMC Analytics Reporting. **Figure J-33** is an example [redacted]:

Environment	Component		Allowed Minutes	Minutes Down					Remaining Minutes
		SLA	March	w/e 3/3	w/e 3/10	w/e 3/17	w/e 3/24	w/e 3/31	
DPW HSH-A	System	99.90%	45	0					45
	TIP	99.90%	45	0					45
	WEBTS	99.70%	134	0					134
	WEBTWO	99.70%	134	0					134
	OLTP	99.90%	45	0					45
DPW HSH-C	System	99.90%	45	28					17
	TIP	99.90%	45	0					45
	MAPPER	99.90%	45	0					45
	APPMAP	99.90%	45	0					45
	OLTP	99.90%	45	0					45
DPW HSH-F	System	99.90%	45	0					45
	TIP	99.90%	45	0					45
PSP	System	99.90%	45	0					45
	TIP	99.87%	58	0					58
	MAPPER	99.90%	45	0					45
GAME	System	99.90%	45	0					45
	COMS	99.90%	45	0					45
DOS L2K	System	99.90%	30	0					30
	SQL Server	99.90%	30	0					30
DOS SURE	System	99.80%	35	0					35
	SQL Server	99.90%	30	0					30
	SRS Application System	99.90%	45	0					45
	SRS SQL System	99.90%	45	0					45
	Virtual Citrix Print Servers	99.50%	223	0					223
DOI Web Envir	System	99.90%	20	0					20
	IIS	99.70%	59	0					59
DOI	System	99.70%	61	0					61

Figure J-33. SL21 BMC Analytics Reporting

Service Level Reporting Window	Monthly

SL22 High Risk Security Patch Updates

Service Level Reference	Description
High Risk Security Patch Updates	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the timeliness in which high-risk security patches are applied. All high risk security patches must be applied within five (5) Business Days from the date the software vendor or applicable industry guiding entity provides notice to the Offeror or other date as agreed to by the Commonwealth or the Commonwealth Customer.
Metric Inclusions	Includes those security patches for which the vendor or applicable industry guiding entity indicates is "high" risk.
Metric Exclusions	• Excludes low and medium risk patches • All items defined in Note 2 at the bottom of this Schedule J.J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is the total number of high risk security patches released five (5) Business Days prior to the beginning and end of the measurement window that were installed within five (5) Business Days divided by the total number of high risk security patches released five (5) Business Days prior to the beginning and end of the measurement window, with the result expressed as a percentage. • = ((Number of High Risk Intrusion Protection Updates Installed within Established Interval) / (Total Number of High Risk Intrusion Protection Updates Installed)) expressed as a percentage
Collection Process	A change request will be opened upon notification from the Commonwealth of the need to apply high-risk security patches. The change request will include the implementation date of the high-risk security patch and the SLA will be calculated. Input: • Notification from Commonwealth of a high-risk security patch requirement • A change request • Implementation date of the change
Reporting Tools / Data Source(s)	The SL 22 compliance will be recorded in the BMC ITSM Service Level Management Application and reported on Real-time Dashboard for all stakeholders to view and drill down into details.

	Output: • SLA compliance will be displayed on Real-time Dashboard • SLA reports from BMC Analytics Reporting Tools: • Real-time Dashboard • BMC Analytics for SL22 Summary Report Data Sources • BMC ITSM Change Request Records • BMC ITSM SLM service targets
Data Storage (Archives)	Data storage is 13 months of history online with offline storage to tape with all supporting details.
Reporting Format/s	The reporting format will be determined during transition for display on the Real-time Dashboard. **Figure J-34** provides a dashboard example; **Figure J-35** provides an example of a BMC analytics summary report that could define the SL 22 Summary Report format.

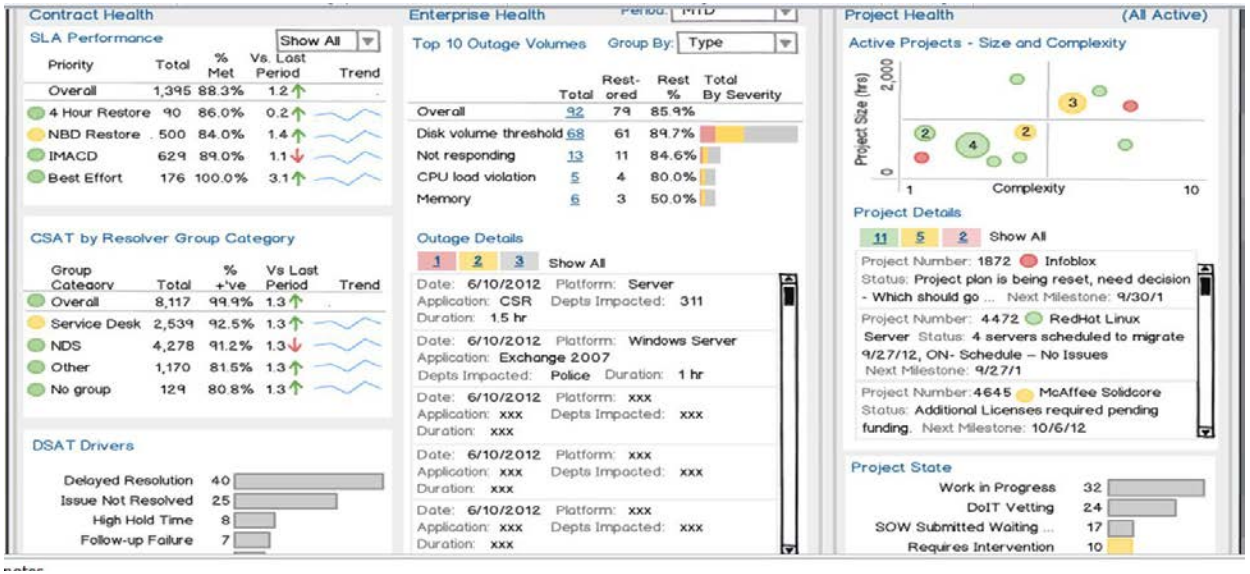
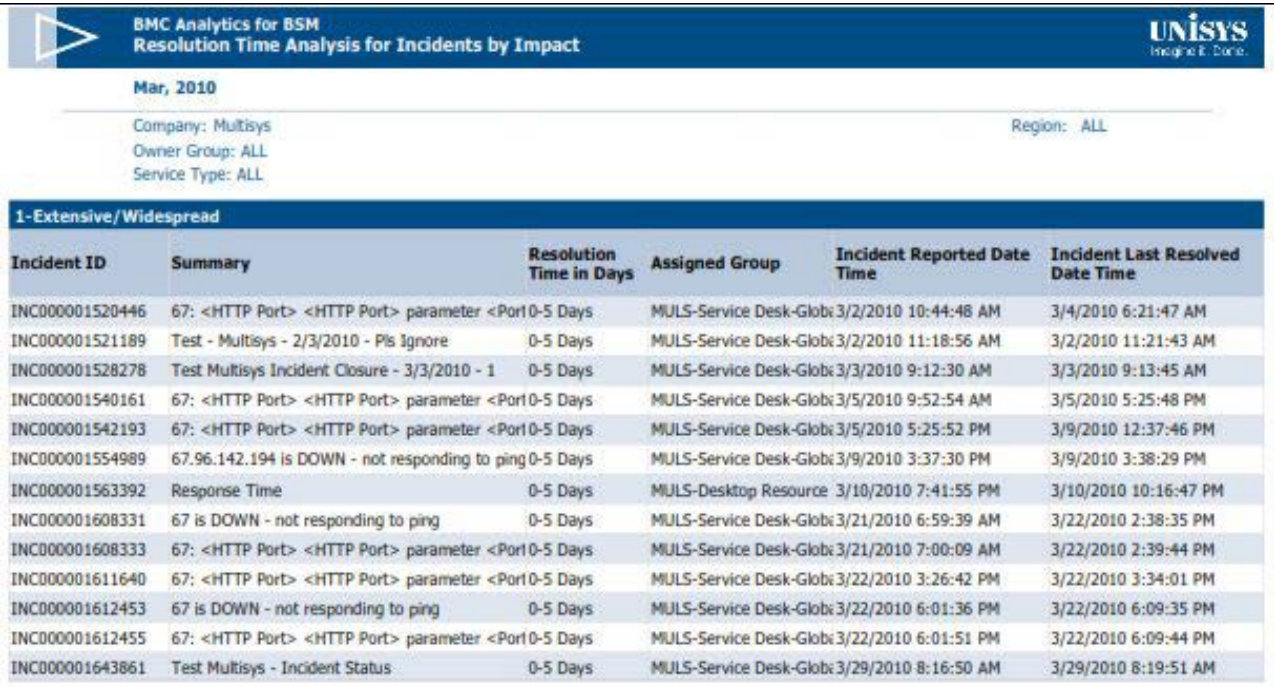


Figure J-34. SL22 Real-time Dashboard



BMC Analytics for BSM
Resolution Time Analysis for Incidents by Impact

UNISYS

Mar, 2010

Company: Multisys
Owner Group: ALL
Service Type: ALL

Region: ALL

1-Extensive/Widespread

Incident ID	Summary	Resolution Time in Days	Assigned Group	Incident Reported Date Time	Incident Last Resolved Date Time
INC000001520446	67: <HTTP Port> <HTTP Port> parameter <Port	0-5 Days	MULS-Service Desk-Globa	3/2/2010 10:44:48 AM	3/4/2010 6:21:47 AM
INC000001521189	Test - Multisys - 2/3/2010 - Pls Ignore	0-5 Days	MULS-Service Desk-Globa	3/2/2010 11:18:56 AM	3/2/2010 11:21:43 AM
INC000001528278	Test Multisys Incident Closure - 3/3/2010 - 1	0-5 Days	MULS-Service Desk-Globa	3/3/2010 9:12:30 AM	3/3/2010 9:13:45 AM
INC000001540161	67: <HTTP Port> <HTTP Port> parameter <Port	0-5 Days	MULS-Service Desk-Globa	3/5/2010 9:52:54 AM	3/5/2010 5:25:48 PM
INC000001542193	67: <HTTP Port> <HTTP Port> parameter <Port	0-5 Days	MULS-Service Desk-Globa	3/5/2010 5:25:52 PM	3/9/2010 12:37:46 PM
INC000001554989	67.96.142.194 is DOWN - not responding to ping	0-5 Days	MULS-Service Desk-Globa	3/9/2010 3:37:30 PM	3/9/2010 3:38:29 PM
INC000001563392	Response Time	0-5 Days	MULS-Desktop Resource	3/10/2010 7:41:55 PM	3/10/2010 10:16:47 PM
INC000001608331	67 is DOWN - not responding to ping	0-5 Days	MULS-Service Desk-Globa	3/21/2010 6:59:39 AM	3/22/2010 2:38:35 PM
INC000001608333	67: <HTTP Port> <HTTP Port> parameter <Port	0-5 Days	MULS-Service Desk-Globa	3/21/2010 7:00:09 AM	3/22/2010 2:39:44 PM
INC000001611640	67: <HTTP Port> <HTTP Port> parameter <Port	0-5 Days	MULS-Service Desk-Globa	3/22/2010 3:26:42 PM	3/22/2010 3:34:01 PM
INC000001612453	67 is DOWN - not responding to ping	0-5 Days	MULS-Service Desk-Globa	3/22/2010 6:01:36 PM	3/22/2010 6:09:35 PM
INC000001612455	67: <HTTP Port> <HTTP Port> parameter <Port	0-5 Days	MULS-Service Desk-Globa	3/22/2010 6:01:51 PM	3/22/2010 6:09:44 PM
INC000001643861	Test Multisys - Incident Status	0-5 Days	MULS-Service Desk-Globa	3/29/2010 8:16:50 AM	3/29/2010 8:19:51 AM

Figure J-35. SL06 BMC Analytics.

Service Level Reporting Window	Monthly

SL23 Change Management Effectiveness

Service Level Reference	Description
Change Management Effectiveness	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the percentage of time Offeror successfully implements Changes to the Services.
Metric Inclusions	Changes are not successfully implemented if they: (i) do not comply with the Change Management procedures (including the Change Control Process), (ii) do not comply with the Change Management procedures detailed within the Commonwealth Computing Procedures Manual, (iii) cause Severity 1 Incidents or Severity 2 Incidents, within 168 hours of implementing the change, (iv) exceeds the reserved implementation or maintenance window as approved within the ITSM Change Request, or (v) are backed out.
Metric Exclusions	• Severity Level 1 and Severity Level 2 incidents that occur during the implementation window for the change and are resolved before the Implementation or Maintenance window ends. • All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is the number of changes that are successfully implemented by Offeror during the applicable Measurement Window, divided by the number of changes that should have been implemented by Offeror during the applicable Measurement Window, with the result expressed as a percentage. • = ((Number of Successful Change Management Requests) / (Total Number of Change Management Requests Scheduled during the period)) expressed as a percentage
Collection Process	All conditions that are related to an unsuccessful change below will be attached or documented in the change ticket including: (i) Changes that do not comply with the Change Management procedures (including the

	Change Control Process) (ii) Changes that do not comply with the Change Management procedures detailed within the Commonwealth Computing Procedures Manual (iii) Severity 1 Incidents or Severity 2 Incidents will be related to a change ticket. The service target within the SLM application will determine an SLA violation if a new incident occurred within 168 hours of the change being deployed (iv) Change tickets that are deployed that are not completed within the reserved maintenance window approved, or are backed out will be identified as an SLA violation The data in the change record will be used by the Service Level Management service targets setup to identify these unsuccessful changes and calculate SL23 accordingly.
Reporting Tools / Data Source(s)	SL23 results will be published in the Real-time Dashboard utilizing the service target data and calculations from the BMC ITSM Service Level Management Application. Real-time Dashboard will display the SL23 results with drill down capability to review change record details supporting the SL19 calculation.
Data Storage (Archives)	13 months online in Real-time Dashboard and ITSM SLM with a rotation to archive tape backup
Reporting Format/s	The SLA reporting format will be determined during transition for Real-time Dashboard and will resemble the format in **Figure J-36**:

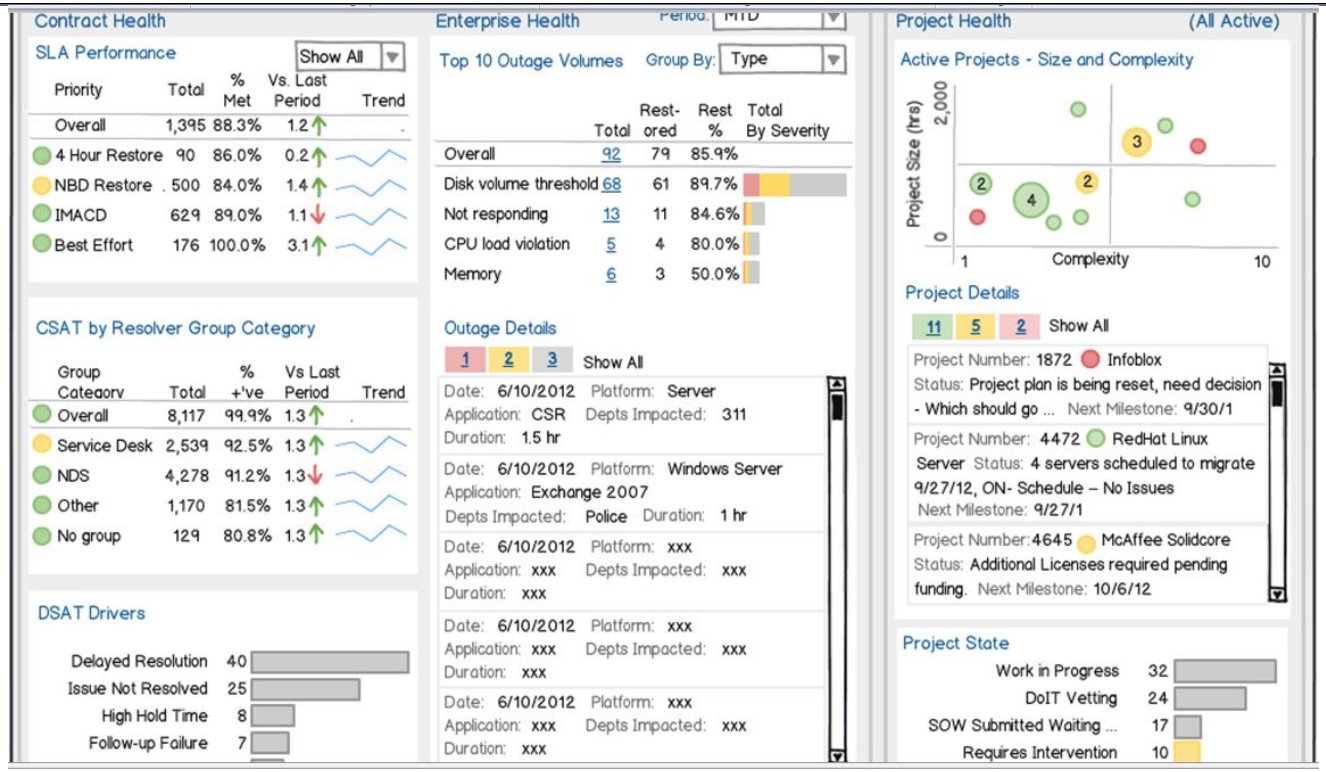


Figure J-36. SL23 Real-time Dashboard

Service Level Reporting Window	Monthly

SL24 Service Desk – Call Answer Time

Service Level Reference	Description
Service Desk – Call Answer Time	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the elapsed time an Authorized User is placed on hold after leaving the Interactive Voice Response or Automatic Call Distribution System to the time the phone call is answered by a live support technician.
Metric Inclusions	All phone calls to the Service Desk shall be included in the calculation of this Service Level with no exceptions for phone calls to the Service Desk during any period of Downtime.
Metric Exclusions	• All items defined in Note 2 at the bottom of this Schedule J.3 • Excludes the time a caller is listening to a Menu of choices before being routed to a helpdesk agent.
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is the total number of seconds, for all phone calls to the Service Desk during the applicable Measurement Window, between the time the phone caller first selects a menu option on the IVR or Automatic Call Distribution System for assistance by a live support technician to the time the phone call is verbally answered by a live support technician ready to start working on the phone call, divided by the total number of all phone calls to the Service Desk during the applicable Measurement Window. • = (Average Time a Call takes to be answered by Service Desk Agent) expressed in seconds
Collection Process	Input • Unisys ACD captures all inbound call data including arrival time, as well as agent answer time or abandon time. Process • Call is time stamped on arrival and again at agent answer in the ACD system. The Service Desk team will pull data from an ACD Call Answer report monthly for use in the SLA calculation as required. Output • SLA reports from ACD – MS Excel format

Reporting Tools / Data Source(s)	SL24 compliance will be recorded in the MS Excel spreadsheet and reported on SharePoint for all stakeholders to view and drill down into details.
Data Storage (Archives)	Avaya ACD data stored online for 13 months of history with offline storage to tape for all call history with all supporting details.
Reporting Format/s	SL24 compliance is reported in MS Excel format, the details for the format will be worked out with the Commonwealth during the transition. A two day excerpt from a sample ACD report is shown in **Figure J-37:**
Service Level Reporting Window	Monthly

Global Day	Target	3/19/2013	3/20/2013

Figure J-37. SL24 Sample ACD Report

SL25 Service Desk – Abandon Rate

Service Level Reference	Description
Service Desk – Abandon Rate	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the percentage of phone calls to the Service Desk that are abandoned by the Authorized User after the Authorized User selected a service option and prior to a live support technician answering the phone call.
Metric Inclusions	All phone calls to the Service Desk shall be included in the calculation of this Service Level with no exceptions for phone calls to the Service Desk during any period of Downtime.
Metric Exclusions	• Calls disconnected prior to an automated voice response system completing the Menu of choices for callers are not counted as abandoned. • All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is the total number of phone calls to the Service Desk during the applicable Measurement Window that are abandoned by the Authorized User (prior to an automated voice response system answers), divided by the total number of phone calls to the Service Desk during the applicable Measurement Window, with the result expressed as a percentage. • = ((Number Of Abandoned Telephone Calls) / (Total Number Of Telephone Calls)) expressed as a percentage
Collection Process	Input • Unisys ACD captures all inbound call data including arrival time, as well as agent answer time or abandon time. Process • Call is time stamped on arrival and again at agent answer. All calls that are dropped by the caller after the 30-second SLA threshold will be considered Abandoned. The Service Desk team will pull an ACD Abandon report monthly for use in the SLA calculation as required. Output • SLA MS Excel report from ACD

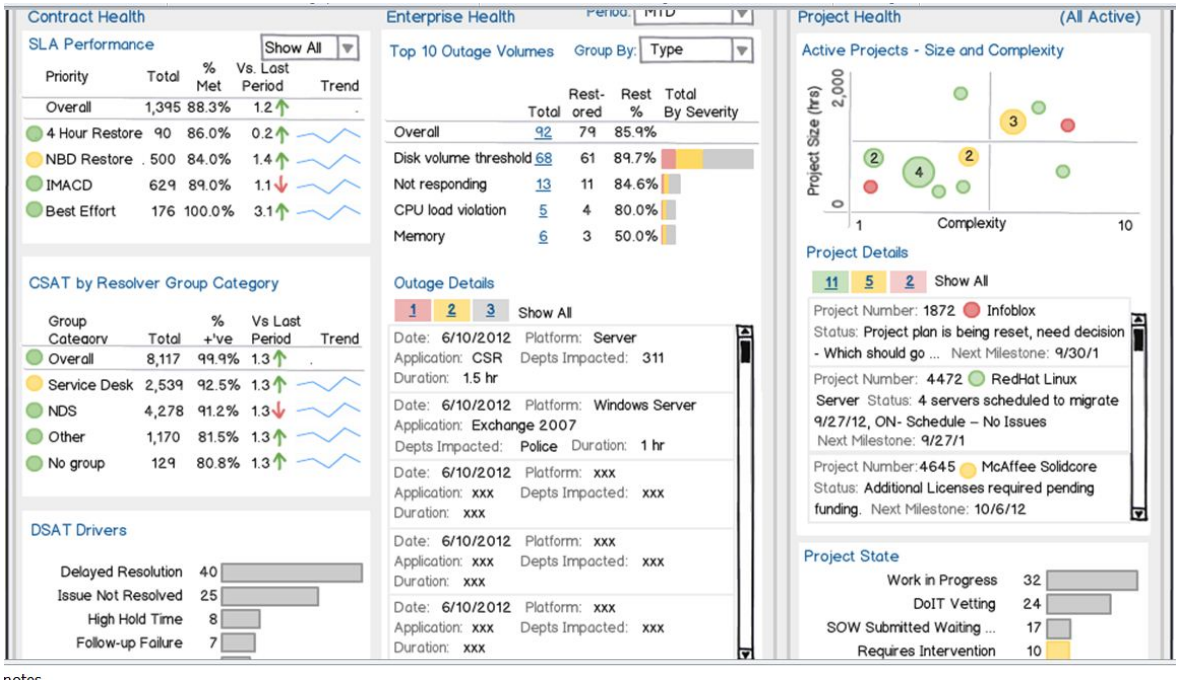
Reporting Tools / Data Source(s)	SL25 compliance will be recorded in the MS Excel spreadsheet and reported on SharePoint for review and analysis.
Data Storage (Archives)	Avaya ACD data stored to tape on archive schedule.
Reporting Format/s	SL25 compliance is reported in MS Excel format, the details for the format will be worked out with the Commonwealth during the transition. A two day excerpt from a sample ACD report is shown in **Figure J-38**:
Service Level Reporting Window	Monthly

Global Day	Target	3/19/2013	3/20/2013
		289	296
		286	291
		0	1
		3	4
		0	1
	5%	0.0%	0.3%

Figure J-38. SL25 ACD Report Excerpt

SL26 Incident Ticket Quality

Service Level Reference	Description
Incident Ticket Quality	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the quality and timeliness of the Offeror's incident management and communication of incident management activities (as defined in the Commonwealth Computing Procedures Manual Commonwealth Computing Procedures Manual). Offeror must update the incident tickets at a minimum on the following frequencies: **Service Restorals**: P1: every 15 minutes; P2: 30 minutes; P3: daily; P4: weekly **Service Requests**: P1: Daily; P2: Weekly; P3: every 2 weeks; P4: Monthly
Metric Inclusions	Includes a statistically valid random sample of Service Restorals and Service Requests closed during the Measurement Window, all priorities.
Metric Exclusions	• Excludes Change Requests (CRQ), Solution Requests (REQ), and Problem Management (PBI) • All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is the number of sampled tickets in the Measurement Window which meet the defined quality and communication frequency criteria divided by the total number of sampled tickets in the Measurement Window, with the result expressed as a percentage. • ((Number of service restorals and requests that met the interval) / (the total number of service restorals and requests)) expressed as a percentage
Collection Process	Input • Responsible Resolver and/or Incident Manager manually updates ticket in ITSM Process • ITSM tracks the time each ticket is updated, as well as updates to the ticket status and work log that were made by the Incident Managers.

	P1/P2 - Incident Managers interact with designated P1 / P2 Escalation Team and responsible Resolvers - manually update ticket in ITSM. P3/P4 - Incident Managers interact with responsible Resolvers to obtain incident status. Resolver must manually update ticket status in ITSM. If SLA threshold is close to being reached, an Incident Manager will contact the Resolver for status and will update the ticket status themself. Output • SLA metric reported on SLA dashboard on agreed periodic timeframe
Reporting Tools / Data Source(s)	SL26 compliance will be recorded in the MS Excel spreadsheet and reported on Real-time Dashboard for all stakeholders to view and drill down into details. The reporting format will be determined during transition for display on the Real-time Dashboard. **Figure J-39** is an example of the dashboard:  **Figure J-39. SL26 Real-time Dashboard.**
Data Storage (Archives)	13 months – Online Tape Backup – Life of Contract

Reporting Format/s	The reporting format will be determined during transition for display on the Real-time Dashboard. **Figure J-40** is an example of the dashboard:
Service Level Reporting Window	Monthly

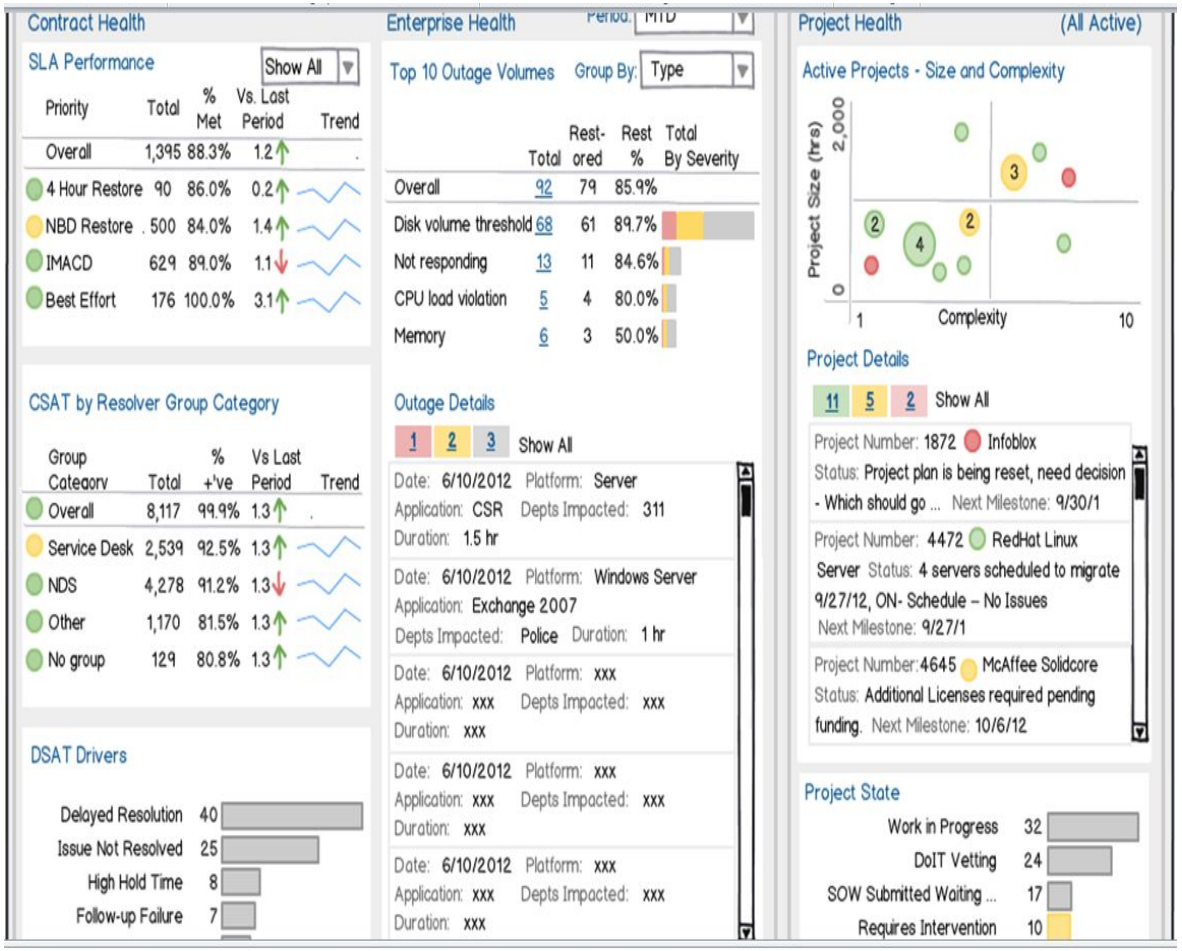


Figure J-40. SL26 Real-time Dashboard

SL27 Service Desk – Customer Satisfaction

Service Level Reference	Description
Service Desk – Customer Satisfaction	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the average scores of the customer satisfaction surveys taken on a random statistical sample of customers that had a service contact with the Offeror during the measurement period. The surveys will be conducted in accordance with the Commonwealth Computing Procedures Manual.
Metric Inclusions	Survey responses shall be on a five (5) point scale (with five (5) being the most satisfied) or shall reflect such other satisfaction criteria established pursuant to the survey design process.
Metric Exclusions	• All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** At the Commencement Date, This Service Level calculation is the sum of all scores for each response (question answered) for the Point of Service surveys that are returned during the applicable Measurement Window, divided by the total number of responses for all Point of Service surveys that are returned during the applicable Measurement Window. • = (Average Score of Surveys)
Collection Process	Input • Email-based survey responses from Service Desk users. Process • Unisys sends a request to complete a Customer Satisfaction Survey by e-mail to users who recently reported an incident to our Service Desk. The e-mail contains a hyperlink that takes a user to a Web site to enter his or her responses on an HTML form. Responses are delivered back to our Service Desk by e-mail and collected in a database. Unisys will use the information collected in our Customer Satisfaction Survey as a basis for continuous improvement of service delivery. To calculate customer satisfaction, we take the sum of all scores for all surveys performed in a month and divide it by the total number of surveys performed in that month. To conduct Customer Satisfaction Surveys, Unisys uses an automated survey system process and a set of questions that ask the end user to rate our service on a scale of 1 to 5:

	5—Very Satisfied 4—Satisfied 3—Neither Satisfied nor Dissatisfied 2—Dissatisfied 1—Very Dissatisfied. For questions the end user rates with a 1 or a 2, Unisys asks him or her to provide supporting detail; we record this detail in the survey record and escalate customer satisfaction issues that require follow-up electronically to the Unisys Service Manager or the appropriate management representative Output • Spreadsheet with survey results compared to SLA targets • SLA metric imported into SLA Real-time Dashboard on agreed periodic timeframe.
Reporting Tools / Data Source(s)	SL27 compliance will be recorded in the MS Excel spreadsheet and reported on Real-time Dashboard for all stakeholders to view and drill down into details.
Data Storage (Archives)	ITSM data stored to tape on archive schedule
Reporting Format/s	SLA Report is formatted in MS Excel. An excerpt from a sample report is shown in **Figure J-41**:

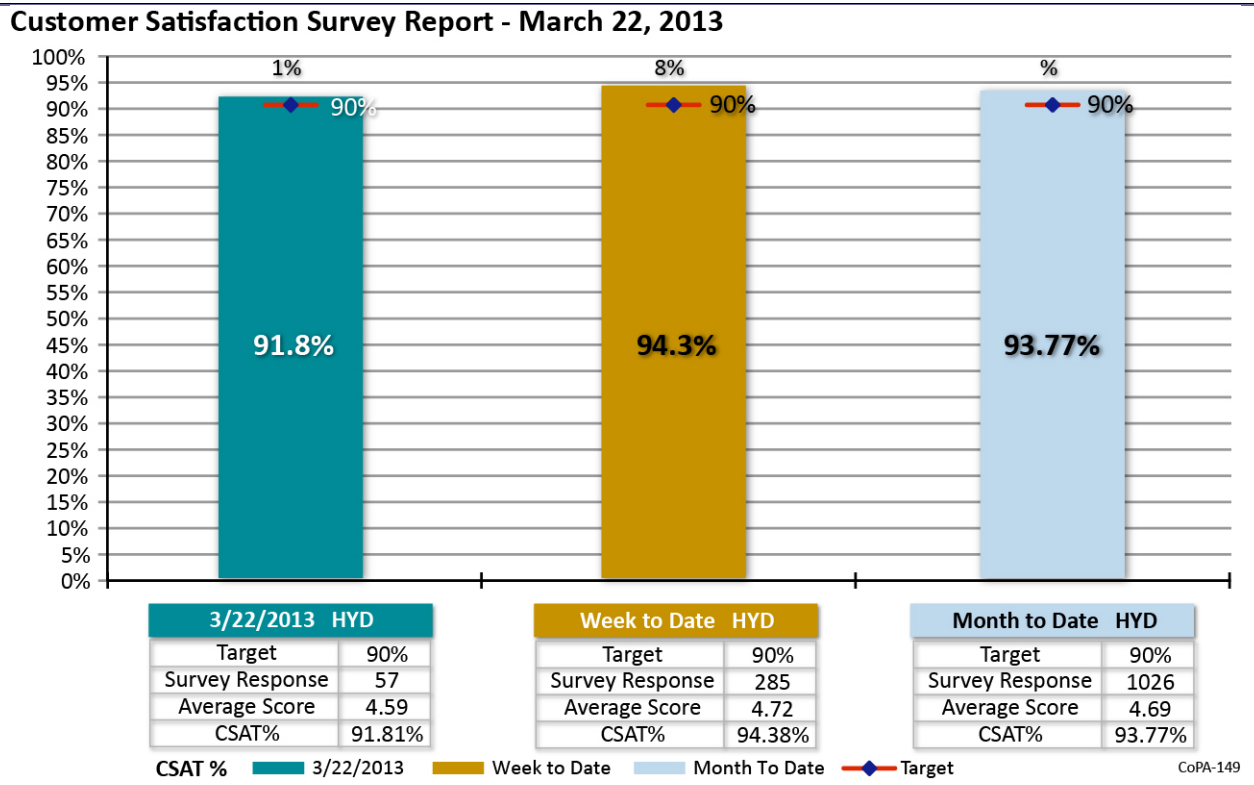
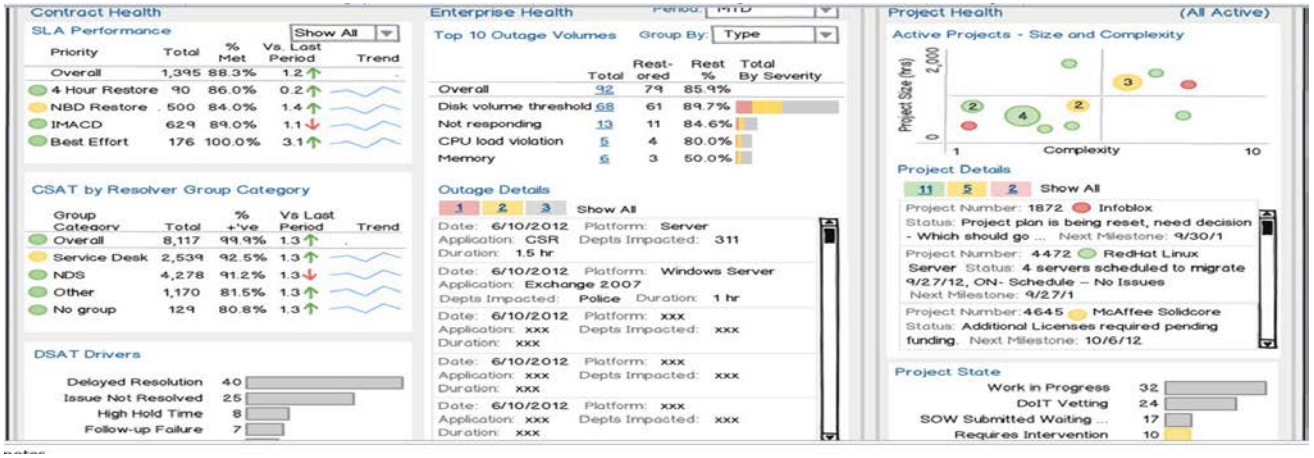


Figure J-41 – SL27 Sample SLA Report

Service Level Reporting Window	Monthly

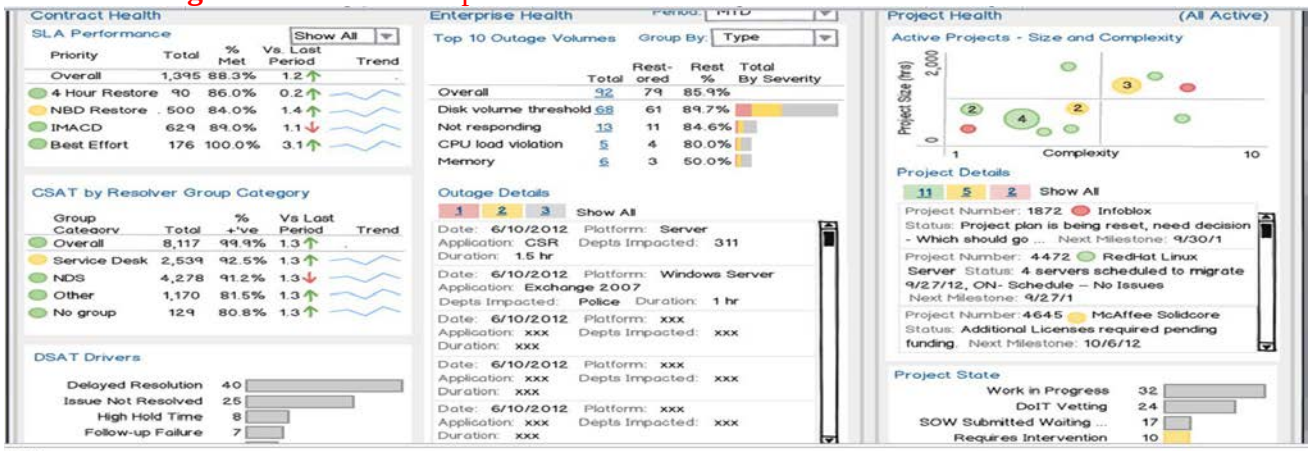
SL28 Batch Scheduling Launched on Time

Service Level Reference	Description
Batch Scheduling Launched on Time	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the percentage of time Offeror starts the Batch job schedules defined in the standard scheduling tool or manually scheduled at the established start time associated with such schedules specified in the Commonwealth Computing Procedures Manual.
Metric Inclusions	Scheduled Batch jobs include normally scheduled and recurring production jobs, as well as production jobs that are run on an as-needed basis.
Metric Exclusions	• Any batch jobs related to infrastructure backups, or other functionality exclusive for Offeror would be excluded. • All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is the total number of Batch job schedules defined in the standard scheduling tool that are started during the applicable Measurement Window at the established start time associated with such schedules as set forth in the Commonwealth Computing Procedures Manual, divided by the total number of Batch job schedules that should have been started during the applicable Measurement Window, with the result expressed as a percentage. • = (Number Of Batches Launched On Time) / (Total Number Of Batches Scheduled) expressed as a percentage
Collection Process	Input • Scheduled Jobs launched time compared to scheduled launch time in BMC Control M Process • Calculate SL28 Batch Scheduling Launched on Time SLA = = (Number Of Batches Launched On Time) / (Total Number Of Batches Scheduled) expressed as a percentage Output • SLA metric reported on SLA CIO Real-time Dashboard • BMC Control M Monthly summary report for SL28
Reporting Tools / Data Source(s)	Real-time Dashboard and BMC Control M reports.

Data Storage (Archives)	13 months – Online Tape Backup – Life of Contract
Reporting Format/s	The SLA dashboard format will be determined during transition for display on the Real-time Dashboard. See **Figure J-42** for an example of a Real-time Dashboard snapshot.  **Figure J-42. SL28 Real-time Dashboard**
Service Level Reporting Window	Monthly

SL29 Batch Processing Completed Successfully

Service Level Reference	Description
Batch Processing Completed Successfully	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the percentage of time Offeror completes Batch jobs successfully and on time during the applicable Measurement Window in accordance with the relevant specifications located in the Commonwealth Computing Procedures Manual.
Metric Inclusions	Batch jobs include normally scheduled and recurring production jobs, as well as production jobs that are run on an as-needed basis. To be considered Successful the Batch must complete within the schedule window for that particular Batch Job.
Metric Exclusions	• Any batch jobs related to infrastructure backups, or other functionality exclusive for Offeror would be excluded. • All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is the total number of Batch jobs that are completed successfully and on time in accordance with the relevant criteria set forth in the Online CCPM repository during the applicable Measurement Window, divided by the total number of Batch jobs that should have been completed during the applicable Measurement Window, with the result expressed as a percentage. • = ((Number Of Successful Batches) / (Total Number Of Batches Scheduled)) expressed as a percentage
Collection Process	Input • Batch jobs scheduled in Batch Scheduling and Management Tool BMC Control-M • Acceptable time to complete batch job (CCPM) Process • SLA 29 Batch Processing Completed Successfully = ((Number Of Successful Batches) / (Total Number Of Batches Scheduled)) expressed as a percentage Output

	• SLA 29 Batch Processing Completed Successfully reported in Real-time Dashboard • Monthly SL 29 Summary Report of batches completed and batches not completed on time
Reporting Tools / Data Source(s)	Real-time Dashboard and BMC Control M
Data Storage (Archives)	13 months – Online Tape Backup – Life of Contract
Reporting Format/s	The SLA dashboard format will be determined during transition for display on the Real-time Dashboard. **Figure J-43** is an example:  **Figure J-43. SL29 Real-time Dashboard**
Service Level Reporting Window	Monthly

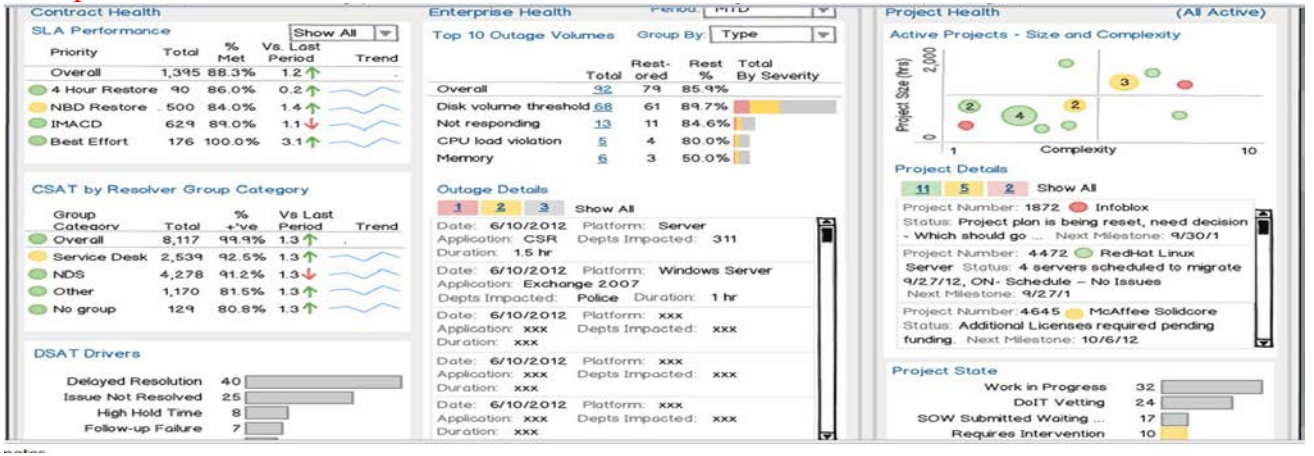
SL30 Reports Delivered On Time

Service Level Reference	Description
Reports Delivered On Time	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level for Reports delivered on time as outlined in Schedule K - Reports measures the percentage of time Offeror delivers the Reports on time in accordance with the requirements. Each Report provided with respect to a Critical Service Level or Key Measurement shall be deemed an individual Report for the purposes of calculating this Service Level.
Metric Inclusions	Schedules as set forth in the Commonwealth Computing Procedures Manual.
Metric Exclusions	• Any reports identified as Critical Monthly Reports in the Commonwealth Computing Procedures Manual and measured in Critical Service Levels. • All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is a count of the total number of Reports that were not successfully delivered (i.e. on time and in compliance with content and format requirements) during the applicable Measurement Window. • = ((Number Of Reports Delivered On Time) / (Total Number Of Reports Scheduled To Be Delivered)) expressed as a percentage
Collection Process	Input: • Collection inputs will be the scheduled ITSM reports outlined in Schedule K by Commonwealth Agency and time period Process • Process will be to setup a SLA service target for collecting the ITSM reports delivered to the appropriate output medium (Real-time Dashboard) on time at agreed interval to agreed medium. Output • SLA 30 Report Delivered on Time Metric in SLA Dashboard • SLA 30 Report of Reports Delivered on Time and Reports not Delivered on Time
Reporting Tools / Data Source(s)	Remedy Report (Analytics)

	Real-time Dashboard
Data Storage (Archives)	13 months – Online Tape Backup – Life of Contract
Reporting Format/s	The SLA dashboard format will be determined during transition for display on the Real-time Dashboard. **Figure J-44** is an example: **Figure J-44 SL30 Real-time Dashboard**
Service Level Reporting Window	Monthly

SL31 Off-Site Media Management

Service Level Reference	Description
Off-Site Media Management	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the accuracy of the Offeror's management of off-site media, specifically the physical location and electronic tracking accuracy of off-site media. The measure is intended to sample one-twelfth of the universe of off-site media such that each the Commonwealth Customer's complete environment is sampled at least once per year.
Metric Inclusions	All media for which Offeror receives an off-site storage resource unit charge.
Metric Exclusions	• Virtual tapes and tapes retained in the Consolidated Data Centers or Non-Consolidated Service Locations. • All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	N/A
Days of Measurement	N/A
Calculation	• **Summary:** This Service Level calculation is based on a statistically valid random sample representing one-twelfth of the universe of off-site media and is the sum of the number of times a tape is either physically in the correct location or electronically listed in the correct location divided by the total number of tapes in the random sample, with the result expressed as a percentage. • = ((Number Of Correct Audits) / (Total Number Of Audits))expressed as a percentage
Collection Process	Tape media personnel will conduct monthly audits of 1/12th of the off-site media against the record locations stored in media management tools (e.g., CommVault). The results will be recorded in a spreadsheet for SLA calculation and reporting. Inputs: • Audit results • CommVault data records
Reporting Tools / Data Source(s)	The MS Excel spreadsheet will be used for comparing audit results to media tools location records, and for calculating the off-site media accuracy SL31. The MS Excel spreadsheet will also contain the details to be used for reporting. Outputs: • MS Excel Spreadsheet with off-site media audit results and details

	Data Sources: • CommVault • Mainframe media management tools Reporting Tools: • Real-time Dashboard • MS Excel Summary SL31 Report
Data Storage (Archives)	13 months – Online Tape Backup – Life of Contract
Reporting Format/s	The Off-site Media SLA Report will be developed during the transition period, we will engage in discussions with the Commonwealth to define the exact content of the report. The SLA dashboard format will be determined during transition for display on the Real-time Dashboard. **Figure J-45** is an example:  **Figure J-45. SL31 Real-time Dashboard**
Service Level Reporting Window	Monthly

SLXX Name (Template)

Service Level Reference	Description
SLA Name (Template)	
Service Category	
Metric Description	
Metric Inclusions	
Metric Exclusions	
Hours of Measurement	
Days of Measurement	
Calculation	
Collection Process	
Reporting Tools / Data Source(s)	
Data Storage (Archives)	
Reporting Format/s	
Service Level Reporting Window	

3. Notes

Note 1: Offeror's failure to achieve any Service Level will not constitute a Service Level Default or accrue toward a Service Level Termination Event to the extent such failure is directly attributable to any Force Majeure events as (as defined in Paragraph 65 of the Contract.

Note 2: Offeror's failure to achieve any Service Level will not constitute a Service Level Default or accrue toward a Service Level Termination Event to the extent such failure is directly attributable to any of the following:

(i) the failure or unavailability of equipment or other resources for which the Commonwealth is operationally and managerially responsible pursuant to the Contract,

(ii) changes made to the environment by the Commonwealth that were not communicated in accordance with the Change Control Procedure or other method agreed upon by the Parties, and

(iii) scheduled and approved maintenance windows.

4. Additional Definitions

1. "Accurate" means all Inventory Attributes are correctly and completely populated in the CMDB Inventory of Record.
2. "Bronze" is defined as a level of service that has a specific Availability value or Response time interval requirement.
3. "CMDB Inventory of Record" means the inventory of CIs, including all Equipment and Software, to be created and maintained by Offeror in accordance with the CCPM.
4. "Commonwealth Computing Procedures Manual" means the established procedural manual related to services offered within this procurement.
5. "Configuration Management Database" (CMDB) is defined as the complete database of all Hardware and software items that make up a service.
6. "Customer Request Date" means the customer requested due date (CRDD) in the Offeror's service management platform (SMP).
7. "Emergency Downtime" means downtime agreed by the Parties to enable maintenance and break fix
   i. necessary to address Service issues stemming from Force Majeure causes or
   ii. Otherwise agreed by the Commonwealth pursuant to the Emergency provisions of the Change Control Procedures.
8. "Gold" is defined as a level of service that has a specific Availability value or Response time interval requirement.
9. "Hold Time" or "Customer Time" is defined as a period of time when Offeror is prevented from progressing the investigation or repair of an incident (outage or degradation) due to Commonwealth required decisions or actions. Examples of this include, but are not limited to:

i. Not providing physical access to a facility pursuant to the Contract so that equipment can be tested or replaced

ii. Not releasing a Application or Server for testing

iii. Not providing accurate or complete information when opening an incident resulting in a Offeror inability to progress the resolution of the logged incident

iv. Not responding with necessary additional information upon request to enable the effective investigation or repair of a logged Service ID

v. related incident

vi. Commonwealth requested delays in the installation of required patches and/or upgrades

vii. Failure of user authentication services, unique end-user VPN client software issues, or other components managed by the Commonwealth. In every case in which Offeror intends to place an incident or ticket on Hold Time or Customer Time, Offeror will make the appropriate prior notification to the Commonwealth. Valid Hold Time and Customer Time is excluded as outage time in calculations of Service Level Availability and Time to Restore.

10. "Inventory Attributes" means those database fields in an Inventory Record that are essential for Offeror's successful delivery of Service and necessary for The Commonwealth's successful performance of retained responsibilities, including architecture, IT planning, and reconciliation of invoices. Inventory Attributes that shall be audited are set out in Commonwealth Computing Procedures Manual and may be modified over time in accordance with the Commonwealth Computing Procedures Manual.

11. "Inventory Record" means the record for a single item of Equipment or Software in the Inventory of Record, including all of the Inventory Attributes for that item.

12. "Major Degradation of Service" means a Service that tests as fully operational but is degraded below user expectations across a significant segment of the user population as determined by the Commonwealth.

13. "Non-Excluded Outage Minutes" is defined as a Minutes that are not considered Customer Time, Hold Time, Scheduled Downtime as defined within this Schedule J.3

14. "Resolution" is defined as removing a fault or degradation from the Commonwealth operational environment. Resolution is followed by notification to the Commonwealth and either performing further joint testing or receiving an approval to place the affected Service or Service ID back in operation.

15. "Response" or "Respond" is defined as Offeror taking and logging meaningful action to progress the testing and restoration of any Service ID, or, as the case may be, Security Services, that has an active Incident ticket opened in the Incident Management System as defined by the Incident and Problem Management Process which is part of the Process and Procedures Manual.

Examples of meaningful response actions include the following, all pursuant to the Policies and Procedures Manual:

- Calling the Commonwealth to obtain additional information to help progress the testing and restoration of the logged incident
- Requesting access to a facility
- Requesting release of a Service ID for testing

- Requesting contact information required to progress the incident management process
- Escalating the incident to technical support for additional testing and analysis

16. "Scheduled Availability" means 24/7/365, unless otherwise specified in a Service Level, minus Scheduled Downtime, Customer Time, Hold Time, and Emergency Downtime.

17. "Scheduled Downtime" means downtime expected and agreed by the Parties, expressed monthly, for which the underlying systems were taken off- line for routine or scheduled maintenance during the Measurement Window.

18. "Service ID" means the unique identifier assigned to a service by Offeror.

19. "Service Level Availability" shall mean the actual availability of access and all functionality of the Services described in a Service Level expressed as percentage of the Scheduled Availability for such Services.

20. "Severity Level" means a priority setting assigned to an incident or change that represents the impact the event has on service for the customer. This level is set by the person reporting the incident or requesting the change and may be adjusted by authorized personnel at the Commonwealth.

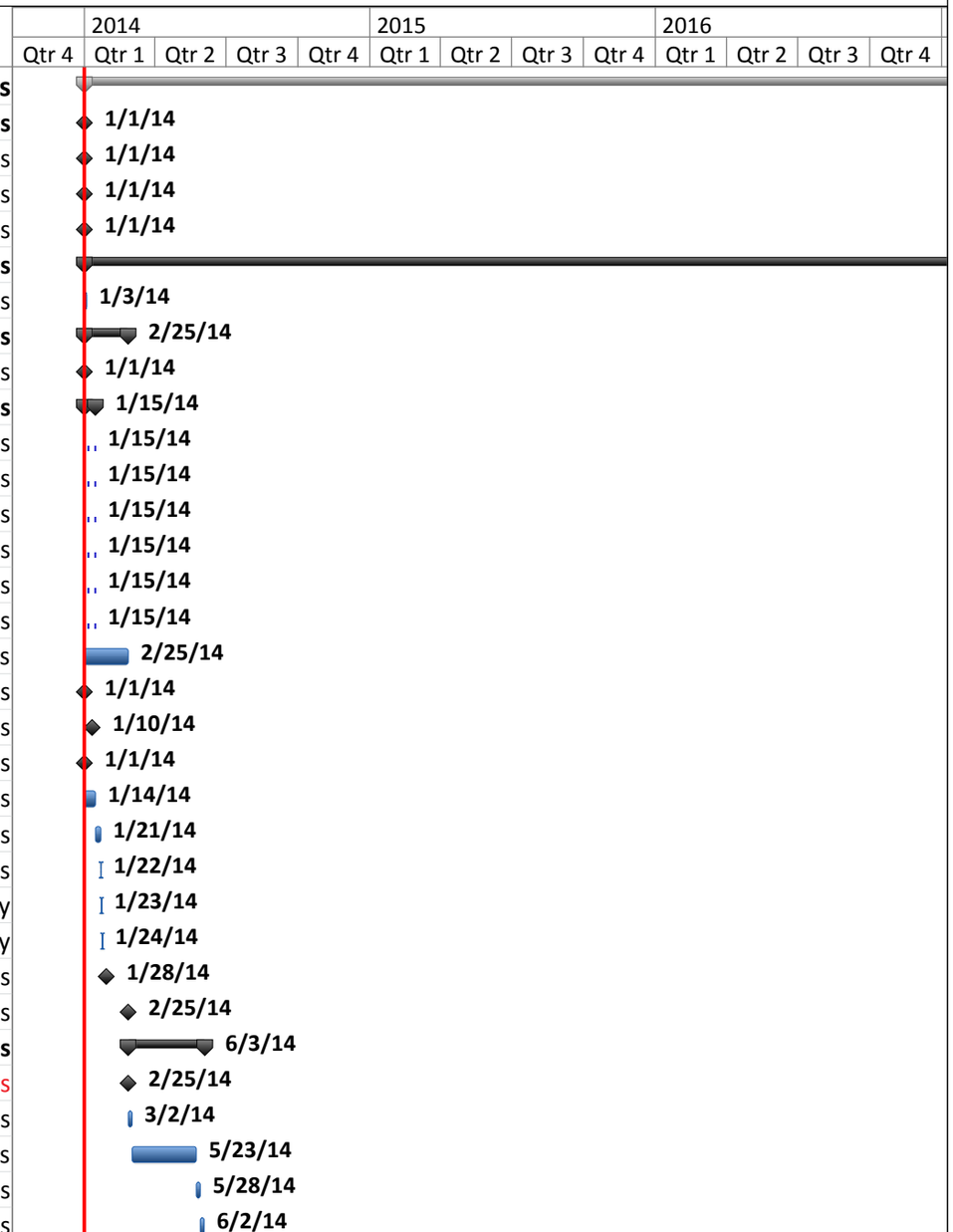
21. "Silver" is defined as a level of service that has a specific Availability value or Response time interval requirement.

22. "Standard Service Interval" means the corresponding period of time in the Standard Service Intervals in the Policy and Procedures Manual, including procedures regarding accuracy, completeness and changes to previously accepted orders. As of the Execution Date, the Standard Service Intervals are set forth in the document provided by the Offeror to the Commonwealth labeled [***to be completed by Offeror***].

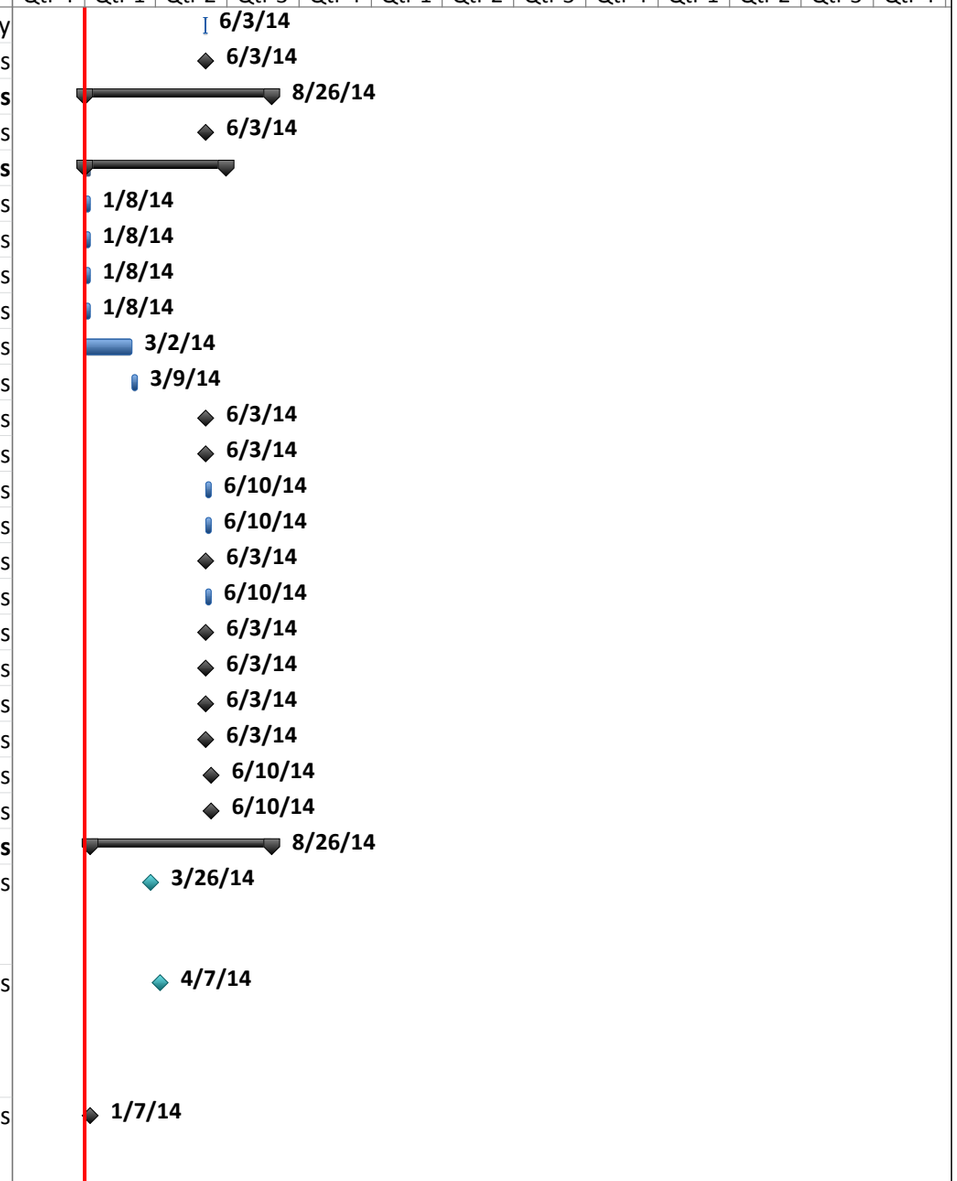
23. For purposes of This Service Level Matrix, a "day" means a 24 hours period from the trigger for the measurement. For example, if a ticket is logged at 9:15am on Tuesday the 14th, a "day" ends at 9:15am on Wednesday day the 15th.

Commonwealth of Pennsylvania Data Center Computing Service Proposed Work Plan

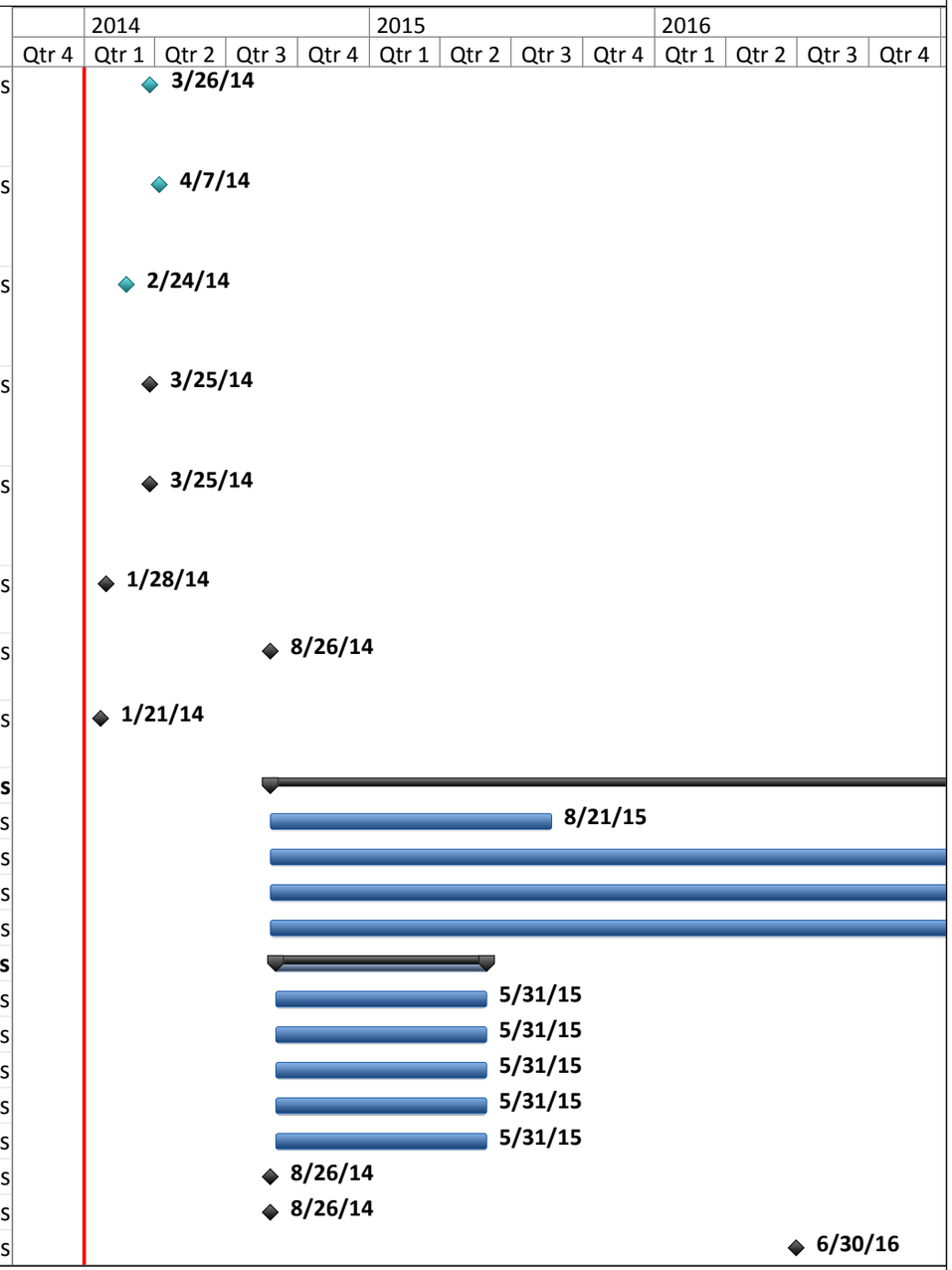
ID	Task Name	Start	Finish	Duration
0	**CoPA Transition Program**	**1/1/14**	**12/31/24**	**2870 days**
1	**1 Key Program Start Dates**	**1/1/14**	**1/1/14**	**0 days**
2	1.1 MS - Unisys Sign DC Contract with New Datacenters as required	1/1/14	1/1/14	0 days
3	1.2 MS - Unisys Approval to begin	1/1/14	1/1/14	0 days
4	1.3 MS - Contract Effective Date	1/1/14	1/1/14	0 days
5	**2 Program Management Tasks**	**1/1/14**	**10/16/18**	**1250 days**
6	2.1 MS - Unisys Team Program Kickoff Meeting	1/1/14	1/3/14	3 days
7	**2.2 Plan Program**	**1/1/14**	**2/25/14**	**40 days**
8	2.2.1 Plan Tasks Started	1/1/14	1/1/14	0 days
9	**2.2.2 Update Project Plans**	**1/1/14**	**1/15/14**	**10 days**
10	2.2.2.1 Update Transition Governance Plan	1/1/14	1/15/14	14 edays
11	2.2.2.2 Update the Initial Transition MPP	1/1/14	1/15/14	14 edays
12	2.2.2.3 Update the Transition Communications Plan	1/1/14	1/15/14	14 edays
13	2.2.2.4 Develop Project Logs (RAID)	1/1/14	1/15/14	14 edays
14	2.2.2.5 Plan Change and Quality Management	1/1/14	1/15/14	14 edays
15	2.2.2.6 Plan Acceptance Criteria	1/1/14	1/15/14	14 edays
16	2.2.3 Setup Transition QA Program	1/1/14	2/25/14	2 mons
17	2.2.4 Obtain the Transition Logistics	1/1/14	1/1/14	0 edays
18	2.2.5 Conduct Internal Transition Kickoff Meetings	1/10/14	1/10/14	0 days
19	2.2.6 Complete Pursuit to Transition Handover and Knowledge Transfer	1/1/14	1/1/14	0 days
20	2.2.7 Schedule and Hold CoPA Kickoff Sessions	1/1/14	1/14/14	10 days
21	2.2.8 Baseline the Transition MPP	1/14/14	1/21/14	7 edays
22	2.2.9 Conduct Checkpoint Quality Review	1/22/14	1/22/14	4 hrs
23	2.2.10 Update Project Logs (RAID)	1/22/14	1/23/14	1 day
24	2.2.11 Perform Internal Status Requirements	1/23/14	1/24/14	1 day
25	2.2.12 PMS-5 - Detailed Transition Plan Completed	1/28/14	1/28/14	0 days
26	2.2.13 MS - Plan Tasks Completed	2/25/14	2/25/14	0 days
27	**2.3 Assess Program**	**2/25/14**	**6/3/14**	**70 days**
28	2.3.1 MS - Start Assess Tasks	2/25/14	2/25/14	0 days
29	2.3.2 Coordinate Assessment Process Review Meeting with Client	2/25/14	3/2/14	5 edays
30	2.3.3 Conduct Customer Assessment Meeting and Data Gathering	3/3/14	5/23/14	3 mons
31	2.3.4 Conduct Internal Review of Workstream Assessment Package	5/23/14	5/28/14	5 edays
32	2.3.5 Gain Client Agreement on Mitigation Plan for Assessment Gaps	5/28/14	6/2/14	5 edays



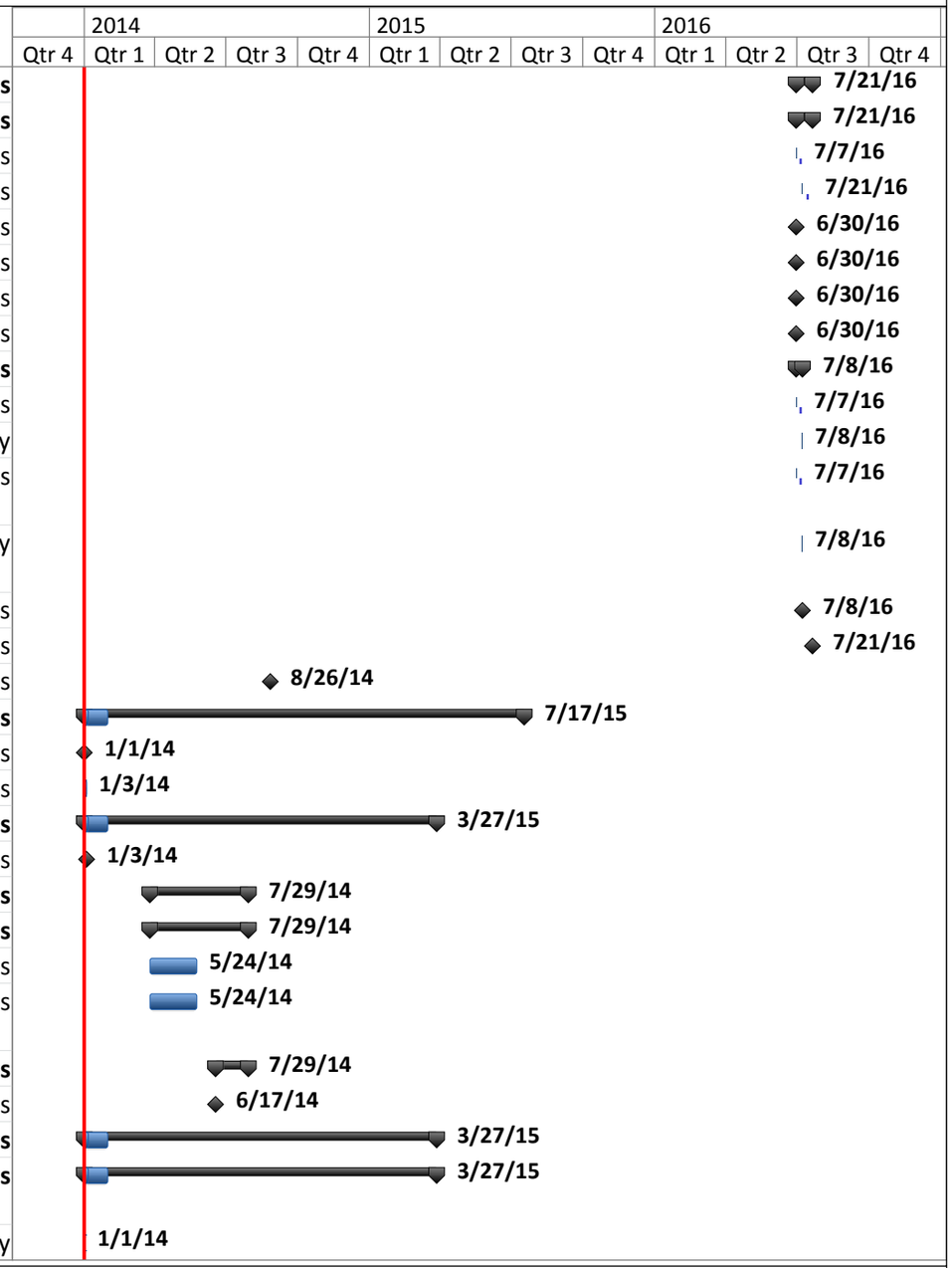
ID	Task Name	Start	Finish	Duration
33	2.3.6 Obtain Workstream Assessment Package Sign Off from Client	6/3/14	6/3/14	1 day
34	2.3.7 Assess Tasks Completed	6/3/14	6/3/14	0 days
35	**2.4 Design Program**	**1/1/14**	**8/26/14**	**170 days**
36	2.4.1 MS - Start Design Tasks	6/3/14	6/3/14	0 days
37	**2.4.2 Develop Program Master Plan**	**1/1/14**	**6/30/14**	**180 edays**
38	2.4.2.1 Governance Plan	1/1/14	1/8/14	7 edays
39	2.4.2.2 Risk Plan	1/1/14	1/8/14	7 edays
40	2.4.2.3 Data Gathering	1/1/14	1/8/14	7 edays
41	2.4.2.4 Operational Readiness Plan	1/1/14	1/8/14	7 edays
42	2.4.3 Complete Transition Program Schedule	1/1/14	3/2/14	60 edays
43	2.4.4 Review and Gain Approval of Program Schedule from Commonwealth	3/2/14	3/9/14	7 edays
44	2.4.5 Complete Solution Design Documents (SDD) for Each Workstream	6/3/14	6/3/14	0 days
45	2.4.6 Refine the Customer Communication Plan	6/3/14	6/3/14	0 edays
46	2.4.7 Gain Client Agreement on Design Gap Mitigation	6/3/14	6/10/14	7 edays
47	2.4.8 Conduct Internal Program Plan Review	6/3/14	6/10/14	7 edays
48	2.4.9 Review Transition Status Report Templates with Client	6/3/14	6/3/14	0 edays
49	2.4.10 Finalize ITSM Operating Processes and Procedures	6/3/14	6/10/14	7 edays
50	2.4.11 Address Procurement	6/3/14	6/3/14	0 edays
51	2.4.12 Develop Procedures For Each Workstream	6/3/14	6/3/14	0 edays
52	2.4.13 Develop the Program Performance Reporting Plan	6/3/14	6/3/14	0 edays
53	2.4.14 Perform Internal Design Review	6/3/14	6/3/14	0 edays
54	2.4.15 Complete the Customer Design Review	6/10/14	6/10/14	0 edays
55	2.4.16 Complete Design Tasks	6/10/14	6/10/14	0 days
56	**2.4.17 D-05 - Transition Management Plan**	**1/7/14**	**8/26/14**	**165 days**
57	2.4.17.1 D-05.01 - Transition Management Plan - New Customer/Service - Create Transition Roadmap with major milestones and present to the Commonwealth	3/26/14	3/26/14	0 days
58	2.4.17.2 D-05.02 - Transition Management Plan - New Customer/Service - Create a Detailed Transition Project Plan with major milestones and present it to the Commonwealth	4/7/14	4/7/14	0 days
59	2.4.17.3 D-05.03 - Transition Management Plan - New Customer/Service First of weekly Transition Status Report	1/7/14	1/7/14	0 days



ID	Task Name	Start	Finish	Duration
60	2.4.17.4 D-05.04 - Transition Management Plan - Present approach to transition Commonwealth computing assets. Includes Roadmap and project plans	3/26/14	3/26/14	0 days
61	2.4.17.5 D-05.05 - Transition Management Plan - Present transition roadmap and plan to Commonwealth stakeholders	4/7/14	4/7/14	0 days
62	2.4.17.6 D-05.06 - Transition Management Plan - Establish Interim Contract Management Procedures during the transition of datacenter services	2/24/14	2/24/14	0 days
63	2.4.17.7 D-05.07 - Transition Management Plan - Document EDC/Legacy Datacenter Infrastructure Maintenance Strategy	3/25/14	3/25/14	0 days
64	2.4.17.8 D-05.08 - Transition Management Plan - Document procedure to standup the Transition Management Office	3/25/14	3/25/14	0 days
65	2.4.17.9 D-05.09 - Transition Management Plan - Provide the first of the weekly Transition Status Reports	1/28/14	1/28/14	0 days
66	2.4.17.10 D-05.10 - Security Transition Activities - Provide Security Transition Plan	8/26/14	8/26/14	0 days
67	2.4.17.11 D-05.11 - Transition Management Plan - Provide the first of the weekly Security Transition Status Reports	1/21/14	1/21/14	0 days
68	**2.5 Deploy Program**	**8/26/14**	**10/16/18**	**1080 days**
69	2.5.1 Start Deploy Tasks	8/26/14	8/21/15	12 emons
70	2.5.2 Manage Transition of Services	8/27/14	10/16/18	1080 days
71	2.5.3 Manage Tools Implementation Project	8/27/14	10/16/18	1080 days
72	2.5.4 Manage Operational Readiness Project	8/27/14	10/16/18	1080 days
73	**2.5.5 Manage DPH Migration**	**9/3/14**	**5/31/15**	**9 emons**
74	2.5.5.1 Manage DPH Move Group 1	9/3/14	5/31/15	9 emons
75	2.5.5.2 Manage DPH Move Group 2	9/3/14	5/31/15	9 emons
76	2.5.5.3 Manage DPH Move Group 3	9/3/14	5/31/15	9 emons
77	2.5.5.4 Manage DPH Move Group 4	9/3/14	5/31/15	9 emons
78	2.5.5.5 Manage DPH Move Group 5	9/3/14	5/31/15	9 emons
79	2.5.6 Conduct Deployment Checkpoint Review	8/26/14	8/26/14	0 days
80	2.5.7 Hold the Services Operational Readiness Review (ORR)	8/26/14	8/26/14	0 days
81	2.5.8 Final Go-Live (Cutover)	6/30/16	6/30/16	0 days

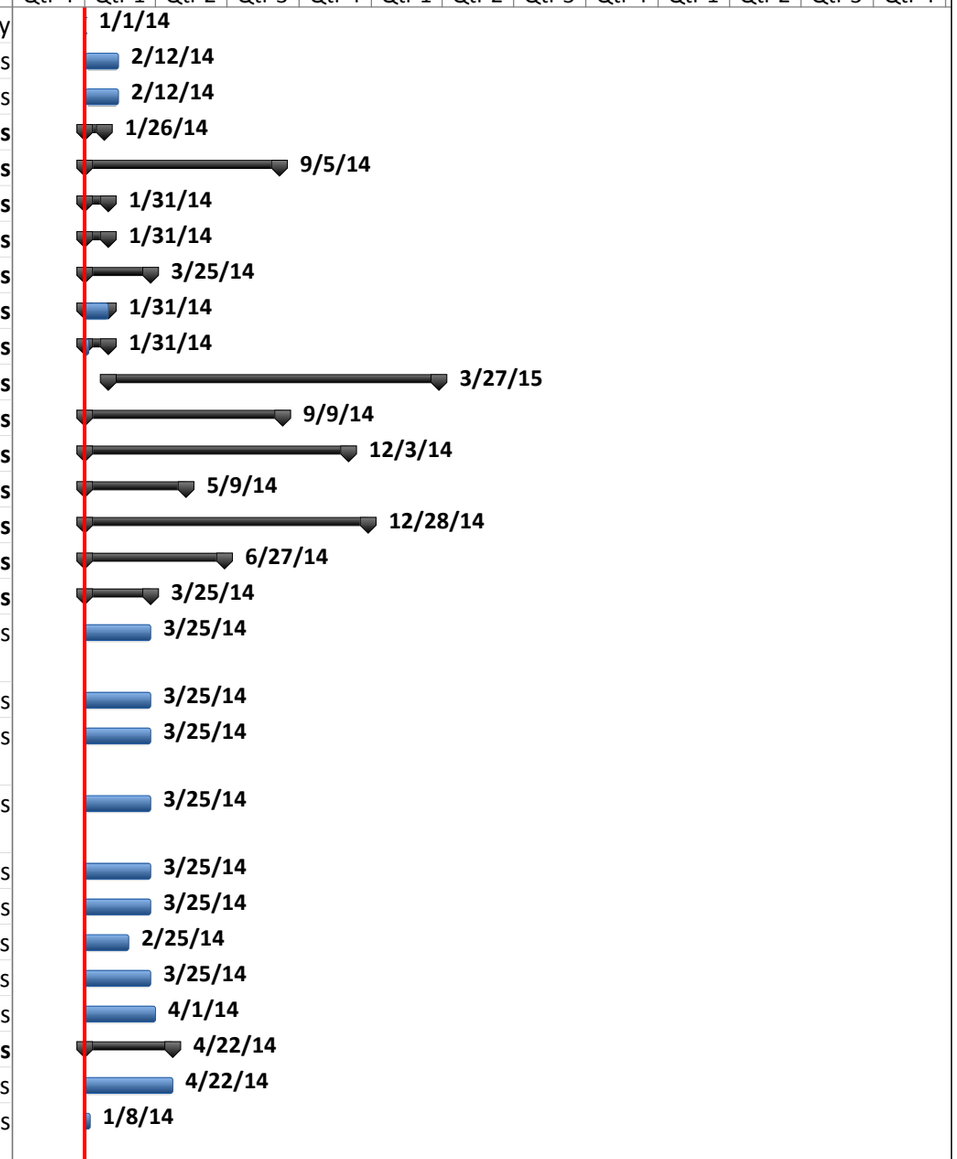


ID	Task Name	Start	Finish	Duration
82	**2.6 Handover and Close to Steady State**	**6/30/16**	**7/21/16**	**15 days**
83	**2.6.1 Transition Feedback**	**6/30/16**	**7/21/16**	**15 days**
84	2.6.1.1 Prepare to Seek Transition Feedback	6/30/16	7/7/16	7 edays
85	2.6.1.2 Gather and Submit Transition Feedback	7/7/16	7/21/16	14 edays
86	2.6.2 Review Initial Operational Reports with Client	6/30/16	6/30/16	0 edays
87	2.6.3 Customer Close-Out Transition	6/30/16	6/30/16	0 edays
88	2.6.4 Hand Off Out of Scope Opportunities to Account Project Office	6/30/16	6/30/16	0 edays
89	2.6.5 Handover to Service Delivery	6/30/16	6/30/16	0 edays
90	**2.6.6 Finalize and Manage Lessons Learned**	**6/30/16**	**7/8/16**	**6 days**
91	2.6.6.1 Finalize and Submit Transition Management Phase Lessons Learned	6/30/16	7/7/16	7 edays
92	2.6.6.2 Identify Vital Few Deals and Communicate Accordingly	7/7/16	7/8/16	1 eday
93	2.6.6.3 Prepare for Lessons Learned Review for Transition Management Phase	6/30/16	7/7/16	7 edays
94	2.6.6.4 Schedule and Conduct Lessons Learned Review Transition Management Phase	7/7/16	7/8/16	1 eday
95	2.6.6.5 Drive Lessons Learned Action Items	7/8/16	7/8/16	0 hrs
96	2.7 MS - Program Management Tasks Complete	7/21/16	7/21/16	0 days
97	2.8 PMS-6 - Detailed Transition Plan Complete	8/26/14	8/26/14	0 days
98	**3 CoPA Transition**	**1/1/14**	**7/17/15**	**403 days**
99	3.1 MS - Transition Start	1/1/14	1/1/14	0 days
100	3.2 Conduct Transition of Services Project Kickoff Meeting	1/1/14	1/3/14	3 days
101	**3.3 Transition of Services Project (Enable Common Service Portfolio)**	**1/1/14**	**3/27/15**	**323 days**
102	3.3.1 MS - TOS Start	1/3/14	1/3/14	0 days
103	**3.3.2 Assess CoPA Current Environments**	**3/25/14**	**7/29/14**	**90 days**
104	**3.3.2.1 Knowledge Transfer activities**	**3/25/14**	**7/29/14**	**90 days**
105	3.3.2.1.1 Review ADDM Results EDC and DPH	3/25/14	5/24/14	60 edays
106	3.3.2.1.2 Review ADDM results DOR, DLI, DPW, DOH, PSP	3/25/14	5/24/14	60 edays
107	**3.3.2.1.3 D-10 - Gap Analysis Report**	**6/17/14**	**7/29/14**	**30 days**
110	3.3.2.2 PMS-5 - Data Gathering	6/17/14	6/17/14	0 days
111	**3.3.3 Setup the Account Team**	**1/1/14**	**3/27/15**	**323 days**
112	**3.3.3.1 Organizational Change Control Components - Program and Services Management**	**1/1/14**	**3/27/15**	**323 days**
113	3.3.3.1.1 Townhall to announce Agreement	1/1/14	1/1/14	1 day

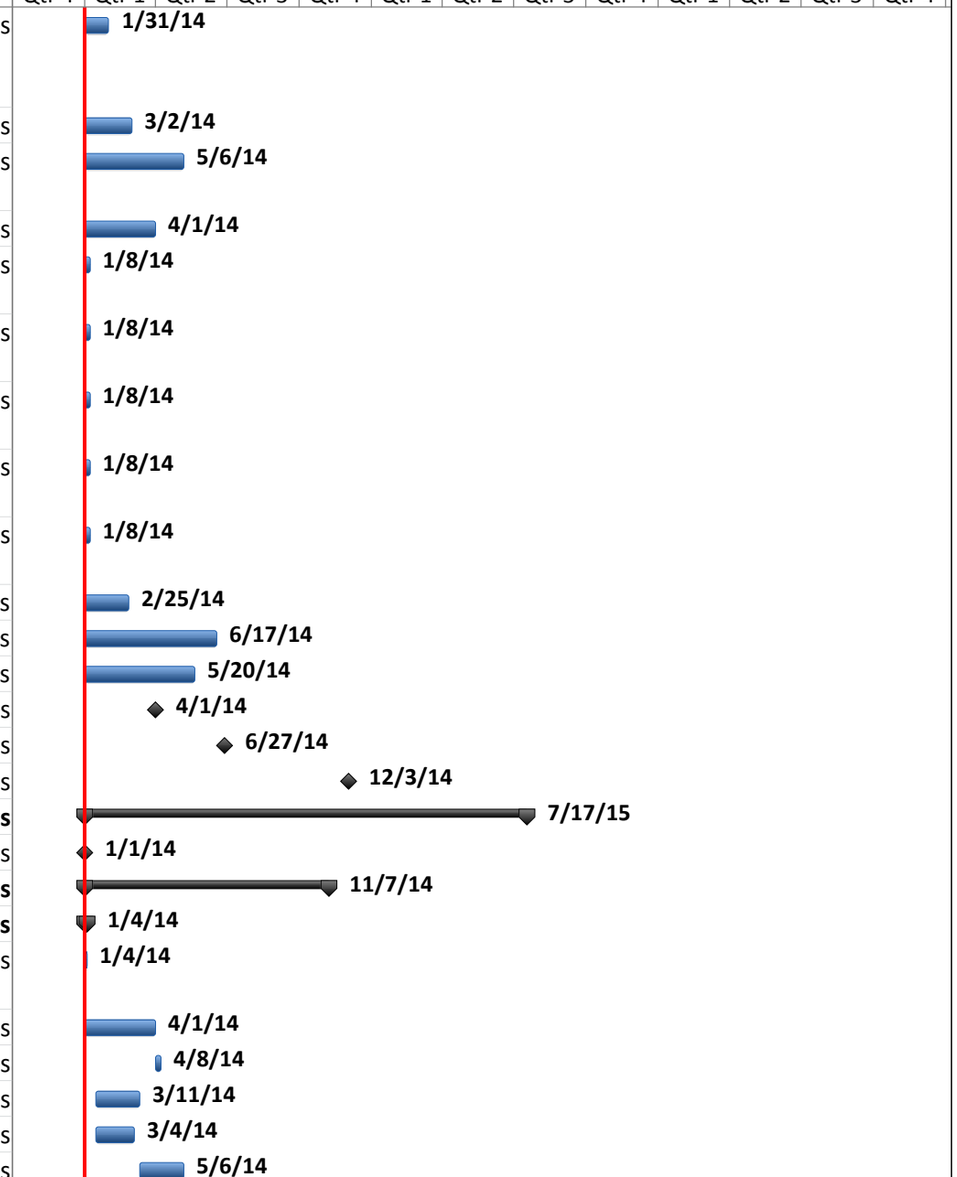


Commonwealth of Pennsylvania Data Center Computing Service Proposed Work Plan

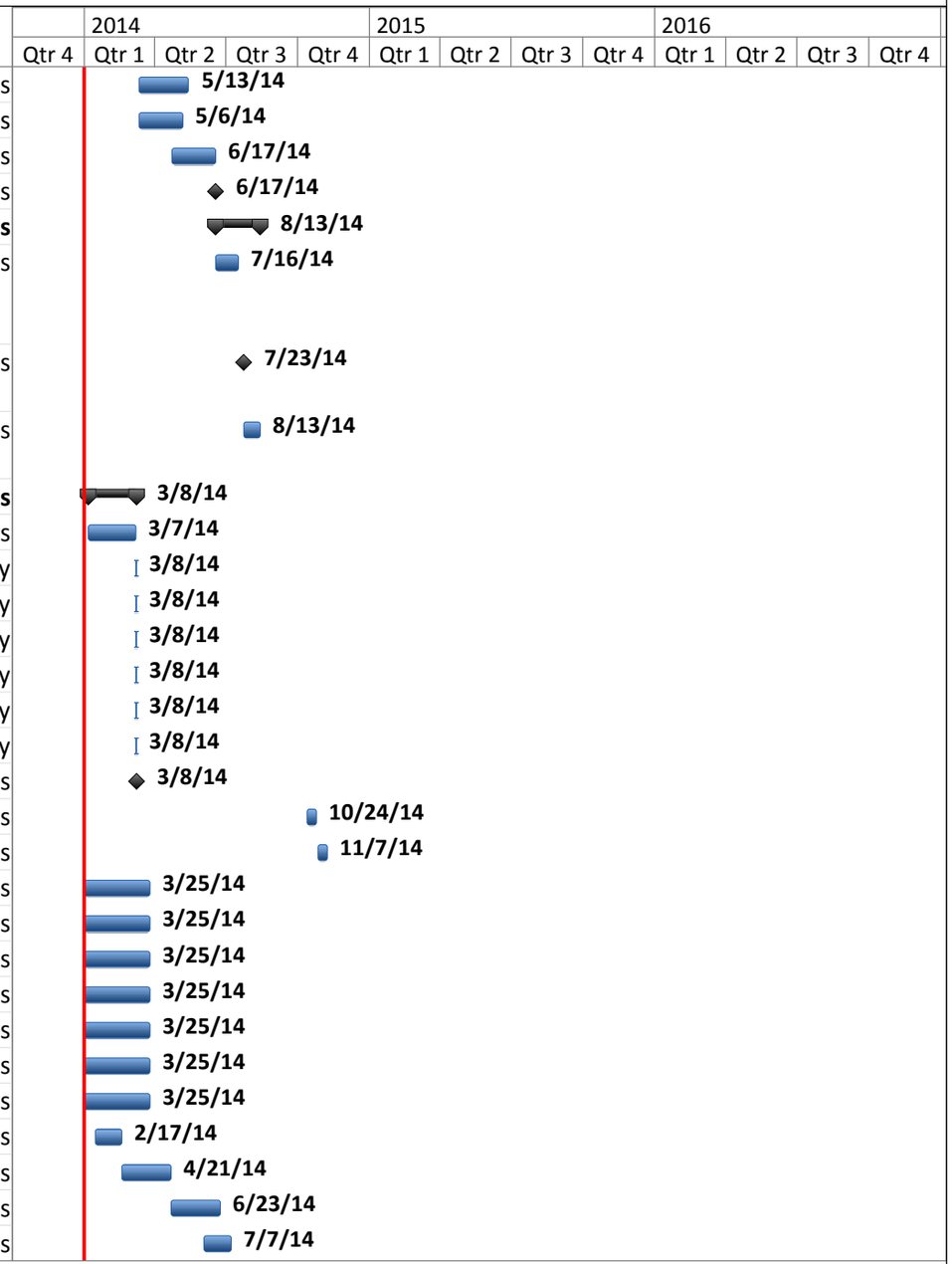
ID	Task Name	Start	Finish	Duration
114	3.3.3.1.2 Team Meetings to discuss what this "means to me"	1/1/14	1/1/14	1 day
115	3.3.3.1.3 Re-Organize Account Staff to new model	1/2/14	2/12/14	30 days
116	3.3.3.1.4 Establish PMO Guidelines and Processes	1/2/14	2/12/14	30 days
117	**3.3.3.1.5 Establish Vendor and Subcontractor Management**	**1/1/14**	**1/26/14**	**18 days**
121	**3.3.3.1.6 Staff Account**	**1/1/14**	**9/5/14**	**178 days**
143	**3.3.3.1.7 Establish PMO Leadership Team**	**1/1/14**	**1/31/14**	**22 days**
146	**3.3.3.1.8 Establish Project Management Team - TPMO and Steady State**	**1/1/14**	**1/31/14**	**22 days**
148	**3.3.3.1.9 Establish Contract Management Team**	**1/1/14**	**3/25/14**	**60 days**
157	**3.3.3.1.10 Establish Agency Account Management Team**	**1/1/14**	**1/31/14**	**22 days**
160	**3.3.3.1.11 Establish Enterprise Architecture Team**	**1/1/14**	**1/31/14**	**22 days**
163	**3.3.3.1.12 Establish Service Excellence Office (SEO)**	**1/31/14**	**3/27/15**	**301 days**
264	**3.3.3.1.13 Establish Financial Management Team Processes**	**1/1/14**	**9/9/14**	**180 days**
272	**3.3.3.1.14 Establish Service Delivery Teams - Processes and Procedures**	**1/1/14**	**12/3/14**	**240 days**
381	**3.3.3.1.15 Training**	**1/1/14**	**5/9/14**	**93 days**
398	**3.3.3.1.16 Relocate Account Team**	**1/1/14**	**12/28/14**	**258 days**
405	**3.4 Enterprise Data Center to Managed Services Model**	**1/1/14**	**6/27/14**	**128 days**
406	**3.4.1 Perform EDC Assessment**	**1/1/14**	**3/25/14**	**60 days**
407	3.4.1.1 Identify Required Security Updates/Upgrades	1/1/14	3/25/14	60 days
408	3.4.1.2 Identify HVAC and power upgrades	1/1/14	3/25/14	60 days
409	3.4.1.3 Identify physical access required for facility	1/1/14	3/25/14	60 days
410	3.4.1.4 Review BMS System quality and information	1/1/14	3/25/14	60 days
411	3.4.2 Integrate Building Management System to BMC BEM	1/1/14	3/25/14	60 days
412	3.4.3 Integrate DCIMI to BMC BEM	1/1/14	3/25/14	60 days
413	3.4.4 Implement Rackwise	1/1/14	2/25/14	2 mons
414	3.4.5 Install Electrical SubMetering	1/1/14	3/25/14	3 mons
415	3.4.6 SSAE 16 Audit of EDC	1/1/14	4/1/14	90 edays
416	**3.4.7 Knowledge Transfer activities**	**1/1/14**	**4/22/14**	**80 days**
417	3.4.7.1 Create/update Runbooks	1/1/14	4/22/14	4 mons
418	3.4.7.2 Verify CMDB contains EDC assets and Cis	1/1/14	1/8/14	7 edays



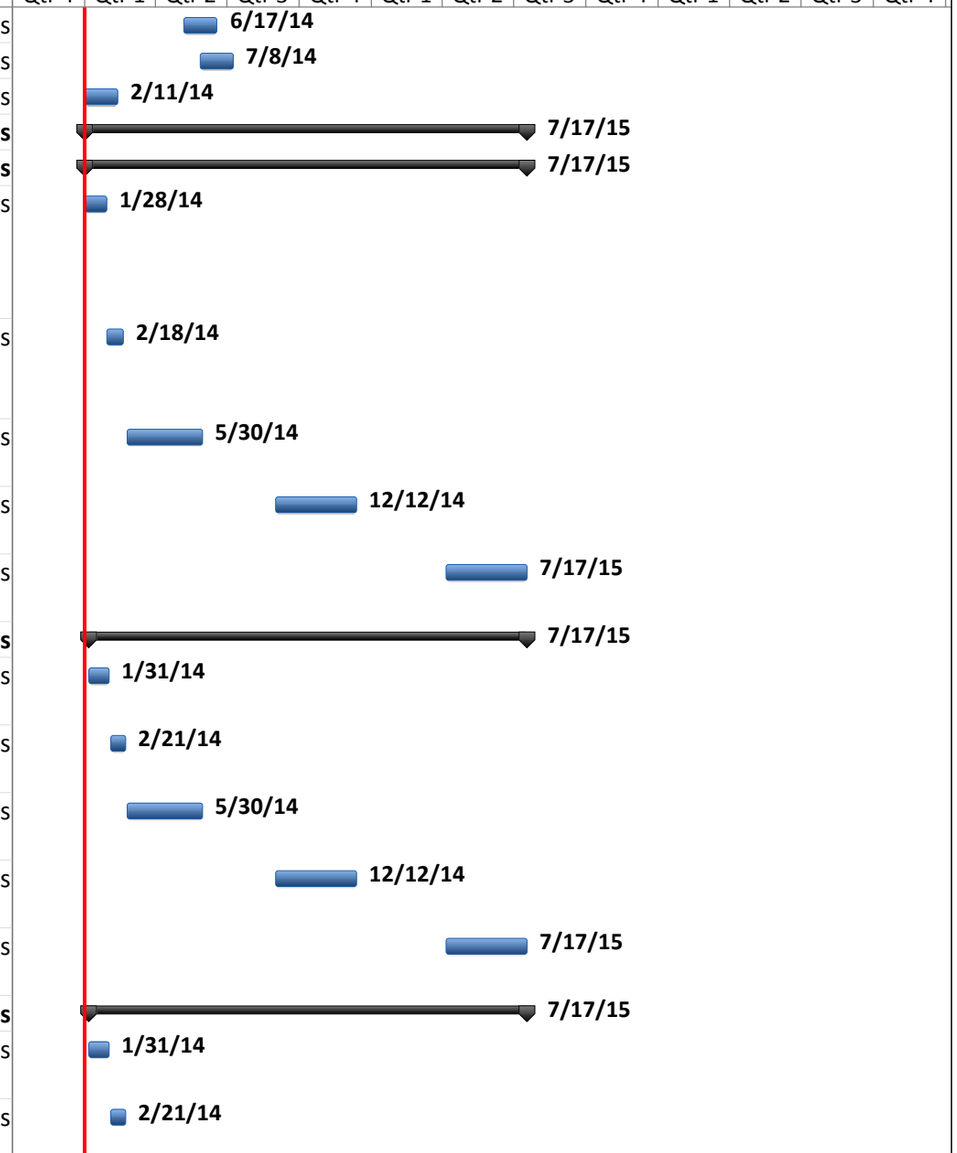
ID	Task Name	Start	Finish	Duration
419	3.4.7.3 Document current Service Catalogs, processes and procedures are transitioned	1/1/14	1/31/14	30 edays
420	3.4.8 Multi-environments/instances are available for identified systems	1/1/14	3/2/14	60 edays
421	3.4.9 Verify High Availability, backup and DR are operational for identified system	1/1/14	5/6/14	90 days
422	3.4.10 Verify specific details for CCPM are in KMP	1/1/14	4/1/14	90 edays
423	3.4.11 Verify Operational dashboards are in place to report on status and alerts	1/1/14	1/8/14	7 edays
424	3.4.12 Verify Service Level agreements have been identified and supporting metrics are in place	1/1/14	1/8/14	7 edays
425	3.4.13 Verify system is Operational for scheduling and tracking of ticket-based tasks and incidents (ITSM/Remedy)	1/1/14	1/8/14	7 edays
426	3.4.14 Verify system is is operational to begin data collection in order to produce Configuration, monitoring and management status reports	1/1/14	1/8/14	7 edays
427	3.4.15 Verify all Transition Orders are completed and accepted by the Commonwealth	1/1/14	1/8/14	7 edays
428	3.4.16 Implement ITIL Processes	1/1/14	2/25/14	2 mons
429	3.4.17 Complete Staffing	1/1/14	6/17/14	6 mons
430	3.4.18 Implement Tools	1/1/14	5/20/14	5 mons
431	3.4.19 PMS-13 - SSAE 16 Audit of EDC Completed	4/1/14	4/1/14	0 days
432	3.4.20 PMS-15 - EDC Transition Completed	6/27/14	6/27/14	0 days
433	3.5 MS-ToS Complete	12/3/14	12/3/14	0 days
434	**3.6 Tools Implementation Project**	**1/1/14**	**7/17/15**	**403 days**
435	3.6.1 MS - Tools Implementation Project Start	1/1/14	1/1/14	0 days
436	**3.6.2 Install BMC ITSM**	**1/1/14**	**11/7/14**	**223 days**
437	**3.6.2.1 Prepare Foundation Data**	**1/1/14**	**1/4/14**	**3 days**
438	3.6.2.1.1 Host Workshops for ITSM / SEO Process Development - Data Gathering	1/1/14	1/4/14	3 edays
439	3.6.2.2 Gather ITSM Data from Commonwealth	1/1/14	4/1/14	90 edays
440	3.6.2.3 Gain approval from Commonwealth on B2B interface	4/1/14	4/8/14	7 edays
441	3.6.2.4 Configure Incident Management	1/15/14	3/11/14	40 days
442	3.6.2.5 Configure Problem Management	1/15/14	3/4/14	35 days
443	3.6.2.6 Configure Change Management	3/12/14	5/6/14	40 days



ID	Task Name	Start	Finish	Duration
444	3.6.2.7 Configure CFG Management	3/12/14	5/13/14	45 days
445	3.6.2.8 Configure Release Management	3/12/14	5/6/14	40 days
446	3.6.2.9 Configure Service Level Management	4/23/14	6/17/14	40 days
447	3.6.2.10 MS - ITSM Configured and Tested	6/17/14	6/17/14	0 days
448	**3.6.2.11 CCPM Approach & Reviews with COPA**	**6/18/14**	**8/13/14**	**41 days**
449	3.6.2.11.1 Prep SD,SLM,CHG&Release, Performance & Capacity Mgt, Configuration Mgt + Software License MgtApproach CCPM	6/18/14	7/16/14	21 days
450	3.6.2.11.2 Review SD,SLM,CHG & Release, Performance & Capacity Mgt, Configuration Mgt + Software License MgtApproach CCPM	7/23/14	7/23/14	0 days
451	3.6.2.11.3 Change and Asset Mgt Procedures Delivered to CCPM KM	7/24/14	8/13/14	15 days
452	**3.6.2.12 DSO - Remedy Sync**	**1/6/14**	**3/8/14**	**45 days**
453	3.6.2.12.1 Configure DSO - Remedy Sync	1/6/14	3/7/14	45 days
454	3.6.2.12.2 Test Incident Connectivity	3/7/14	3/8/14	1 eday
455	3.6.2.12.3 Problem Connectivity	3/7/14	3/8/14	1 eday
456	3.6.2.12.4 Change Request Connectivity	3/7/14	3/8/14	1 eday
457	3.6.2.12.5 Configuration items reconciliation	3/7/14	3/8/14	1 eday
458	3.6.2.12.6 Invoices processed through ITSM to Commonwealth AP	3/7/14	3/8/14	1 eday
459	3.6.2.12.7 Reporting from Unisys ITSM is available in Commonwealth's ITSM	3/7/14	3/8/14	1 eday
460	3.6.2.13 PMS-9 - ITSM Systems Integration Completed	3/8/14	3/8/14	0 days
461	3.6.2.14 Install and Configure Knowledge Management	10/13/14	10/24/14	10 days
462	3.6.2.15 Load KM ITSM Procedures, SC, Contract Pricing	10/27/14	11/7/14	10 days
463	3.6.2.16 Install & Configure EDC & DPH ADDM Discovery	1/1/14	3/25/14	60 days
464	3.6.2.17 Install & Configure DOR ADDM Discovery	1/1/14	3/25/14	60 days
465	3.6.2.18 Install & Configure DLI ADDM Discovery	1/1/14	3/25/14	60 days
466	3.6.2.19 Install & Configure DOH ADDM Discovery	1/1/14	3/25/14	60 days
467	3.6.2.20 Install & Configure DPW ADDM Discovery	1/1/14	3/25/14	60 days
468	3.6.2.21 Install & Configure PSP ADDM Discovery	1/1/14	3/25/14	60 days
469	3.6.2.22 Install BPPM/BEM/SIM Monitoring & Integration	1/1/14	3/25/14	60 days
470	3.6.2.23 Configure Availability Management	1/15/14	2/17/14	24 days
471	3.6.2.24 Configure Capacity Management	2/18/14	4/21/14	45 days
472	3.6.2.25 Install and Configure BladeLogic for Servers (EDC)	4/22/14	6/23/14	45 days
473	3.6.2.26 Install and Configure BladeLogic for Network	6/3/14	7/7/14	25 days

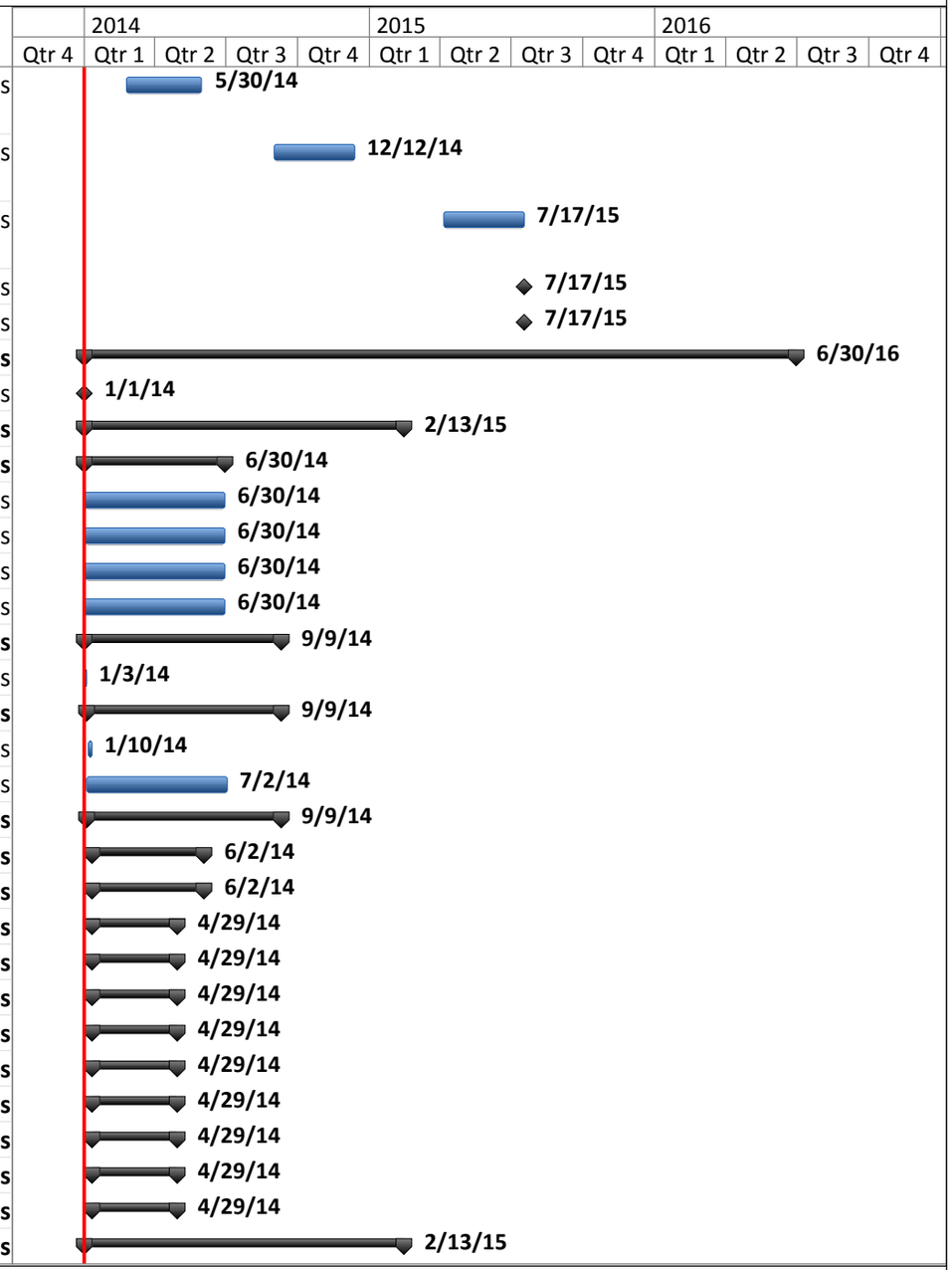


ID	Task Name	Start	Finish	Duration
474	3.6.2.27 Configure Standard Reporting BMC	5/7/14	6/17/14	30 days
475	3.6.2.28 Configure Pureshare Dashboards	5/28/14	7/8/14	30 days
476	3.6.2.29 Configure PMG - Service Catalog	1/1/14	2/11/14	30 days
477	**3.6.3 Security Tools**	**1/1/14**	**7/17/15**	**403 days**
478	**3.6.3.1 Data Loss Prevention**	**1/1/14**	**7/17/15**	**403 days**
479	3.6.3.1.1 Perform requirements gathering and design the data center DLP solution to monitor the datacenter egress points	1/1/14	1/28/14	20 days
480	3.6.3.1.2 Implement pilot solution and configure DLP policy on one egress point	1/29/14	2/18/14	15 days
481	3.6.3.1.3 Implement DLP solution for DCM Phase 1	2/24/14	5/30/14	70 days
482	3.6.3.1.4 Implement DLP solution for DCM Phase 2	9/1/14	12/12/14	75 days
483	3.6.3.1.5 Implement DLP solution for DCM Phase 3	4/6/15	7/17/15	75 days
484	**3.6.3.2 Database Firewall (DBFW)**	**1/6/14**	**7/17/15**	**400 days**
485	3.6.3.2.1 Perform requirements gathering and design the data center DBFW	1/6/14	1/31/14	20 days
486	3.6.3.2.2 Implement pilot solution and configure DBFW	2/3/14	2/21/14	15 days
487	3.6.3.2.3 Implement DBFW solution for DCM Phase 1	2/24/14	5/30/14	70 days
488	3.6.3.2.4 Implement DBFW solution for DCM Phase 2	9/1/14	12/12/14	75 days
489	3.6.3.2.5 Implement DBFW solution for DCM Phase 3	4/6/15	7/17/15	75 days
490	**3.6.3.3 Web Application Firewall (WAF)**	**1/6/14**	**7/17/15**	**400 days**
491	3.6.3.3.1 Perform requirements gathering and design the data center WAF	1/6/14	1/31/14	20 days
492	3.6.3.3.2 Implement pilot solution and configure WAF	2/3/14	2/21/14	15 days



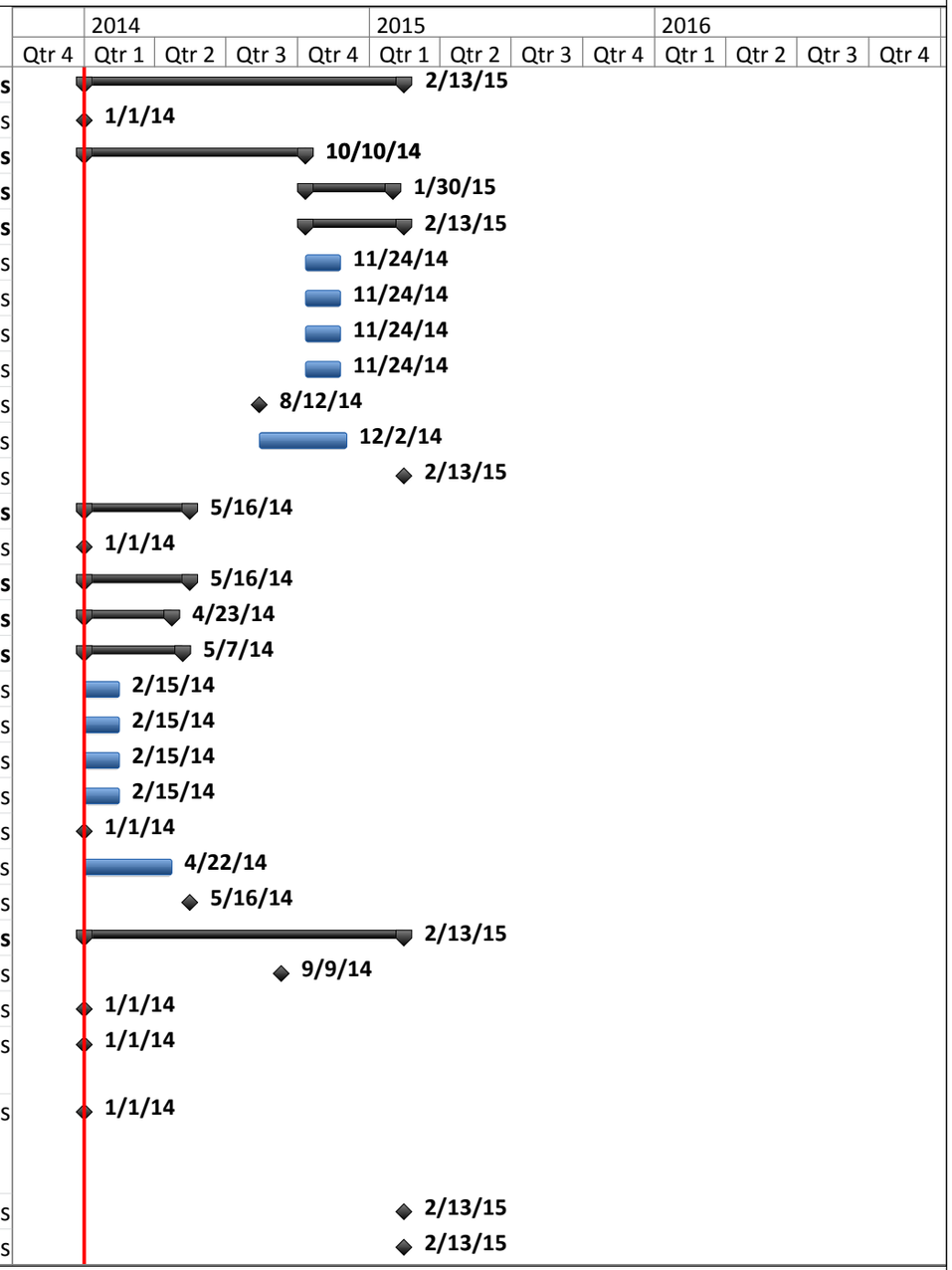
Commonwealth of Pennsylvania Data Center Computing Service Proposed Work Plan

ID	Task Name	Start	Finish	Duration
493	3.6.3.3.3 Implement DBFW solution for WAF Phase 1	2/24/14	5/30/14	70 days
494	3.6.3.3.4 Implement DBFW solution for WAF Phase 2	9/1/14	12/12/14	75 days
495	3.6.3.3.5 Implement DBFW solution for WAF Phase 3	4/6/15	7/17/15	75 days
496	3.6.4 MS - Tools Implementation Project Complete	7/17/15	7/17/15	0 days
497	3.6.5 MS - CoPA Transition of Services Complete	7/17/15	7/17/15	0 days
498	**4 CoPA Application Workload Migration**	**1/1/14**	**6/30/16**	**651 days**
499	4.1 MS - CoPA Datacenter Migration Start	1/1/14	1/1/14	0 days
500	**4.2 Infrastructure Readiness Project**	**1/1/14**	**2/13/15**	**293 days**
501	**4.2.1 Project Management Tasks**	**1/1/14**	**6/30/14**	**128 days**
502	4.2.1.1 Refine Governance Plan	1/1/14	6/30/14	180 edays
503	4.2.1.2 Develop and maintain Risk Plan (RAID)	1/1/14	6/30/14	180 edays
504	4.2.1.3 Validate Data Gathering Timeline	1/1/14	6/30/14	180 edays
505	4.2.1.4 Develop Configuration/Test Plan	1/1/14	6/30/14	180 edays
506	**4.2.2 Data Center Architecture Design and Planning Tasks**	**1/1/14**	**9/9/14**	**180 days**
507	4.2.2.1 Data Center Planning Kickoff Meeting	1/1/14	1/3/14	3 days
508	**4.2.2.2 Refine Data Center Plan**	**1/3/14**	**9/9/14**	**177 days**
509	4.2.2.2.1 Finalize DC Seed and Critical Gear plan	1/6/14	1/10/14	5 days
510	4.2.2.2.2 Develop Operational Readiness Plan	1/3/14	7/2/14	180 edays
511	**4.2.2.2.3 Create Architecture Diagrams**	**1/3/14**	**9/9/14**	**177 days**
555	**4.2.2.3 Order Long Lead/Seed Items**	**1/10/14**	**6/2/14**	**101 days**
556	**4.2.2.3.1 WAN**	**1/10/14**	**6/2/14**	**101 days**
562	**4.2.2.3.2 LAN**	**1/10/14**	**4/29/14**	**77 days**
567	**4.2.2.3.3 x86 Seed**	**1/10/14**	**4/29/14**	**77 days**
572	**4.2.2.3.4 x86 ITSM Environment**	**1/10/14**	**4/29/14**	**77 days**
577	**4.2.2.3.5 Storage Seed**	**1/10/14**	**4/29/14**	**77 days**
582	**4.2.2.3.6 Storage ITSM**	**1/10/14**	**4/29/14**	**77 days**
587	**4.2.2.3.7 IBM MF**	**1/10/14**	**4/29/14**	**77 days**
592	**4.2.2.3.8 Unisys MF**	**1/10/14**	**4/29/14**	**77 days**
597	**4.2.2.3.9 IBM P-Series**	**1/10/14**	**4/29/14**	**77 days**
602	**4.2.2.3.10 IBM AIX**	**1/10/14**	**4/29/14**	**77 days**
607	**4.2.3 Data Center Buildout**	**1/1/14**	**2/13/15**	**293 days**



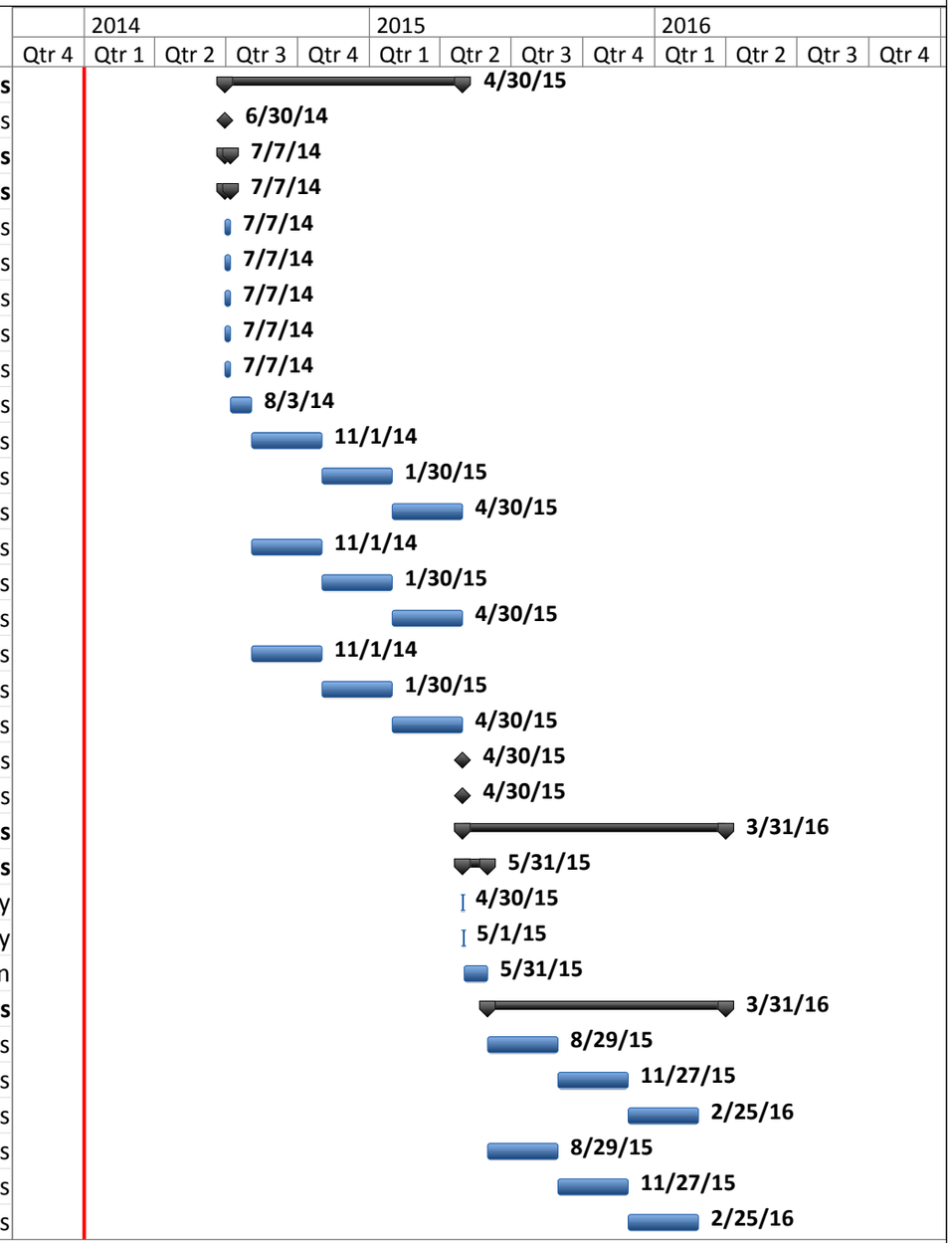
Commonwealth of Pennsylvania Data Center Computing Service Proposed Work Plan

ID	Task Name	Start	Finish	Duration
608	**4.2.3.1 DC1 - Buildout - MP0**	**1/1/14**	**2/13/15**	**293 days**
609	4.2.3.1.1 MS - Begin DC1 - Buildout	1/1/14	1/1/14	0 days
610	**4.2.3.1.2 DC1 - Network Buildout**	**1/1/14**	**10/10/14**	**203 days**
625	**4.2.3.1.3 DC1 - Storage Buildout**	**10/10/14**	**1/30/15**	**80 days**
632	**4.2.3.1.4 DC1 - x86 Buildout**	**10/10/14**	**2/13/15**	**90 days**
640	4.2.3.1.5 DC1 - Backup Buildout	10/10/14	11/24/14	45 edays
641	4.2.3.1.6 DC1 - IBM MF Buildout	10/10/14	11/24/14	45 edays
642	4.2.3.1.7 DC1 - AIX Buildout	10/10/14	11/24/14	45 edays
643	4.2.3.1.8 DC1 - Monitoring Buildout	10/10/14	11/24/14	45 edays
644	4.2.3.1.9 Initiate SSAE 16 Audit for DC1	8/12/14	8/12/14	0 days
645	4.2.3.1.10 Execute SSAE 16 Audit for DC1	8/13/14	12/2/14	4 mons
646	4.2.3.1.11 MS - DC1 - Buildout - MP0 - COMPLETED	2/13/15	2/13/15	0 days
647	**4.2.3.2 DC2 - Buildout - MP0**	**1/1/14**	**5/16/14**	**97 days**
648	4.2.3.2.1 MS - Begin DC2 - Buildout	1/1/14	1/1/14	0 days
649	**4.2.3.2.2 DC2 - Network Buildout**	**1/1/14**	**5/16/14**	**97 days**
664	**4.2.3.2.3 DC2 - Storage Buildout**	**1/1/14**	**4/23/14**	**80 days**
671	**4.2.3.2.4 DC2 - x86 Buildout**	**1/1/14**	**5/7/14**	**90 days**
679	4.2.3.2.5 DC2 - Backup Buildout	1/1/14	2/15/14	45 edays
680	4.2.3.2.6 DC2 - IBM MF Buildout	1/1/14	2/15/14	45 edays
681	4.2.3.2.7 DC2 - AIX Buildout	1/1/14	2/15/14	45 edays
682	4.2.3.2.8 DC2 - Monitoring Buildout	1/1/14	2/15/14	45 edays
683	4.2.3.2.9 Initiate SSAE 16 Audit for DC2	1/1/14	1/1/14	0 days
684	4.2.3.2.10 Execute SSAE 16 Audit for DC2	1/1/14	4/22/14	4 mons
685	4.2.3.2.11 MS - DC2 - Buildout - MP0 - COMPLETED	5/16/14	5/16/14	0 days
686	**4.2.3.3 Prepare Operational Readiness Report**	**1/1/14**	**2/13/15**	**293 days**
687	4.2.3.3.1 Deliverables D-01 (01,02, 03,04,05,06,07) Completed	9/9/14	9/9/14	0 days
688	4.2.3.3.2 Transition Project Office established	1/1/14	1/1/14	0 days
689	4.2.3.3.3 Transition Program Plan and architecture developed and approved	1/1/14	1/1/14	0 days
690	4.2.3.3.4 Processes and tools implemented to support the transition change control, schedule, quality, communications, risk and issues management (Project Logs established)	1/1/14	1/1/14	0 days
691	4.2.3.3.5 Datacenter environment configured, tested and accepted	2/13/15	2/13/15	0 days
692	4.2.3.4 PMS-12 - Operational Readiness	2/13/15	2/13/15	0 days

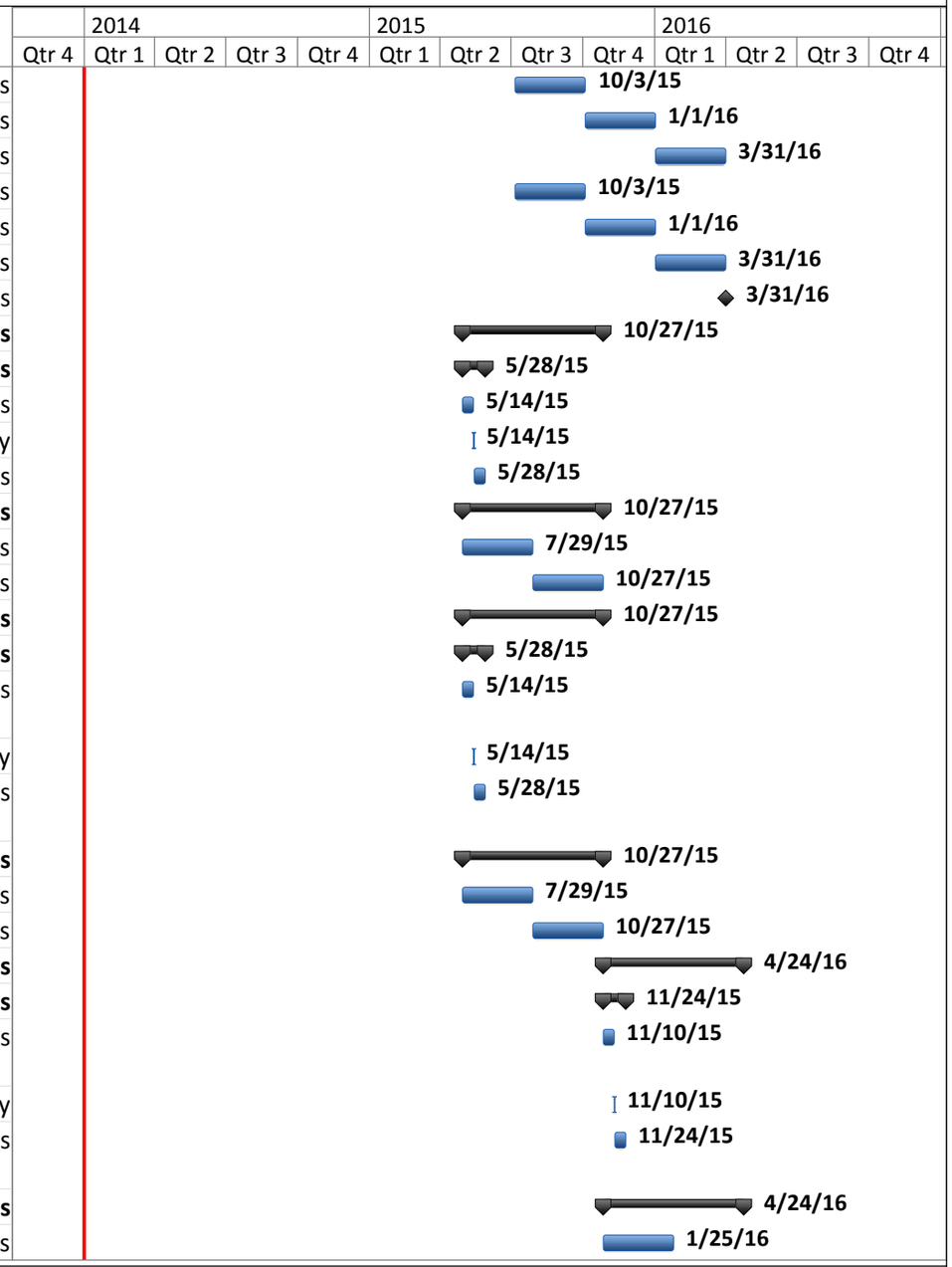


Commonwealth of Pennsylvania Data Center Computing Service Proposed Work Plan

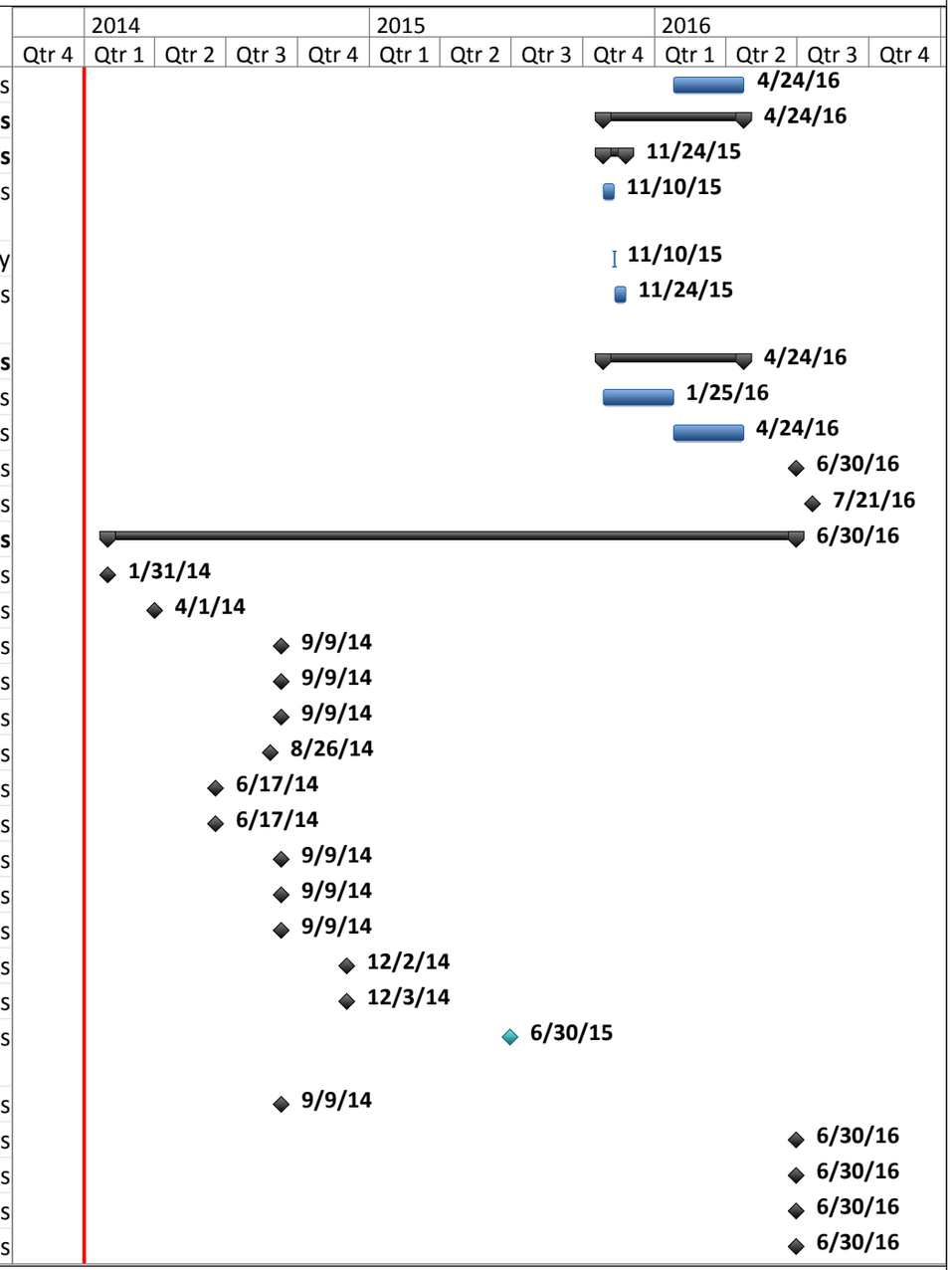
ID	Task Name	Start	Finish	Duration
693	**4.3 DPH Application Workload Migration**	**6/30/14**	**4/30/15**	**218 days**
694	4.3.1 DPH Start	6/30/14	6/30/14	0 days
695	**4.3.2 Project Management Tasks**	**6/30/14**	**7/7/14**	**5 days**
696	**4.3.2.1 Develop Agency centric plans**	**6/30/14**	**7/7/14**	**5 days**
697	4.3.2.1.1 Governance Plan	6/30/14	7/7/14	7 edays
698	4.3.2.1.2 Risk Plan	6/30/14	7/7/14	7 edays
699	4.3.2.1.3 Validate Data Gathering Timeline	6/30/14	7/7/14	7 edays
700	4.3.2.1.4 Configuration/Test Plan	6/30/14	7/7/14	7 edays
701	4.3.2.1.5 Operational Readiness Plan	6/30/14	7/7/14	7 edays
702	4.3.3 DPH Planning and Review of high level move groups	7/7/14	8/3/14	27 edays
703	4.3.4 DPH-DPW Move Package #1	8/3/14	11/1/14	3 emons
704	4.3.5 DPH-DPW Move Package #2	11/1/14	1/30/15	3 emons
705	4.3.6 DPH-DPW & DOI Move Package #3	1/30/15	4/30/15	3 emons
706	4.3.7 DPH-PSER/PUC/Sungard DR Move Package	8/3/14	11/1/14	3 emons
707	4.3.8 DPH-PSP/PGC Move Package	11/1/14	1/30/15	3 emons
708	4.3.9 DPH-DOH/DOS/DEP Move Package	1/30/15	4/30/15	3 emons
709	4.3.10 DPH-PLCB Move Package	8/3/14	11/1/14	3 emons
710	4.3.11 DPH-IES Move Package	11/1/14	1/30/15	3 emons
711	4.3.12 DPH-DOR Move Package	1/30/15	4/30/15	3 emons
712	4.3.13 MS-DPH Applications Migrated	4/30/15	4/30/15	0 days
713	4.3.14 PMS-13 - DPH DCM Complete	4/30/15	4/30/15	0 days
714	**4.4 DLI Application Workload Migration**	**4/30/15**	**3/31/16**	**241 days**
715	**4.4.1 Plan DLI Workload Migration**	**4/30/15**	**5/31/15**	**22 days**
716	4.4.1.1 Send Application Questionnaires to Application Owners	4/30/15	4/30/15	1 day
717	4.4.1.2 Kickoff Meeting - L&I Application Workload Migration	5/1/15	5/1/15	1 day
718	4.4.1.3 Perform Detailed planning of Move Package	5/1/15	5/31/15	1 emon
719	**4.4.2 Execute DLI Moves**	**5/31/15**	**3/31/16**	**219 days**
720	4.4.2.1 DLI -1 Move Package	5/31/15	8/29/15	3 emons
721	4.4.2.2 DLI -2 Move Package	8/29/15	11/27/15	3 emons
722	4.4.2.3 DLI -3 Move Package	11/27/15	2/25/16	3 emons
723	4.4.2.4 DLI -4 Move Package	5/31/15	8/29/15	3 emons
724	4.4.2.5 DLI -5 Move Package	8/29/15	11/27/15	3 emons
725	4.4.2.6 DLI -6 Move Package	11/27/15	2/25/16	3 emons



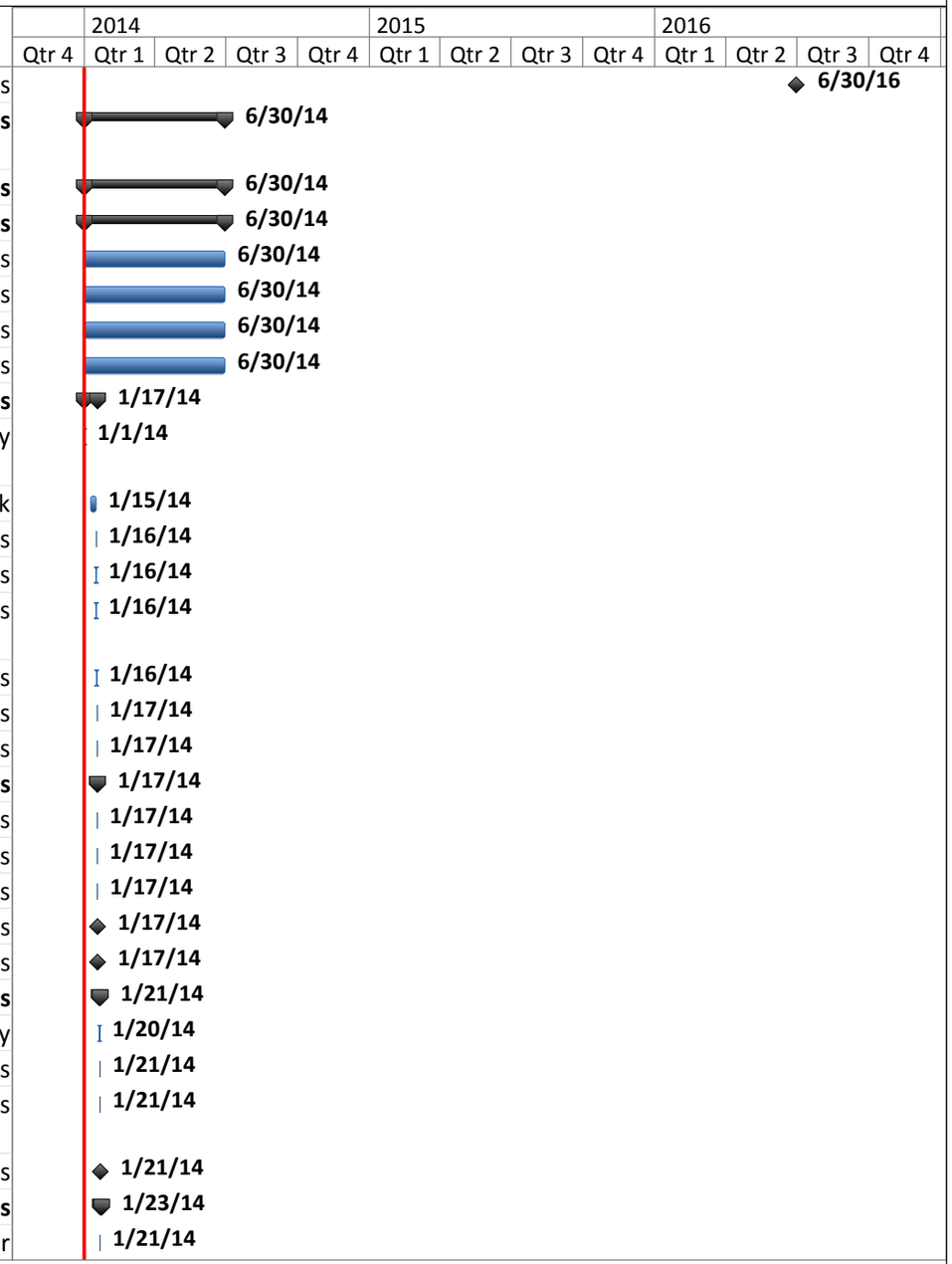
ID	Task Name	Start	Finish	Duration
726	4.4.2.7 DLI -7 Move Package	7/5/15	10/3/15	3 emons
727	4.4.2.8 DLI -8 Move Package	10/3/15	1/1/16	3 emons
728	4.4.2.9 DLI -9 Move Package	1/1/16	3/31/16	3 emons
729	4.4.2.10 DLI -10 Move Package	7/5/15	10/3/15	3 emons
730	4.4.2.11 DLI -11 Move Package	10/3/15	1/1/16	3 emons
731	4.4.2.12 DLI -12 Move Package	1/1/16	3/31/16	3 emons
732	4.4.2.13 MS-DLI Application Workload Migration Complete	3/31/16	3/31/16	0 days
733	**4.5 DOR Application Workload Migration**	**4/30/15**	**10/27/15**	**128 days**
734	**4.5.1 Plan DOR Workload Migration**	**4/30/15**	**5/28/15**	**21 days**
735	4.5.1.1 Send Application Questionnaires to Application Owners	4/30/15	5/14/15	14 edays
736	4.5.1.2 Kickoff Meeting - DOR Application Workload Migration	5/14/15	5/14/15	1 day
737	4.5.1.3 Perform Detailed planning of Move Package	5/14/15	5/28/15	14 edays
738	**4.5.2 Execute DOR Moves**	**4/30/15**	**10/27/15**	**128 days**
739	4.5.2.1 Execute DOR Move Group 1	4/30/15	7/29/15	3 emons
740	4.5.2.2 Execute DOR Move Group 2	7/29/15	10/27/15	3 emons
741	**4.6 DPW Application Workload Migration**	**4/30/15**	**10/27/15**	**128 days**
742	**4.6.1 Plan DPW Workload Migration**	**4/30/15**	**5/28/15**	**21 days**
743	4.6.1.1 Send Application Questionnaires to Application Owners	4/30/15	5/14/15	14 edays
744	4.6.1.2 Kickoff Meeting - DPW Application Workload Migration	5/14/15	5/14/15	1 day
745	4.6.1.3 Perform Detailed planning of Move Package	5/14/15	5/28/15	14 edays
746	**4.6.2 Execute DPW Moves**	**4/30/15**	**10/27/15**	**128 days**
747	4.6.2.1 Execute DPW Move Group 1	4/30/15	7/29/15	3 emons
748	4.6.2.2 Execute DPW Move Group 2	7/29/15	10/27/15	3 emons
749	**4.7 PSP Application Workload Migration**	**10/27/15**	**4/24/16**	**129 days**
750	**4.7.1 Plan PSP Workload Migration**	**10/27/15**	**11/24/15**	**21 days**
751	4.7.1.1 Send Application Questionnaires to Application Owners	10/27/15	11/10/15	14 edays
752	4.7.1.2 Kickoff Meeting - PSP Application Workload Migration	11/10/15	11/10/15	1 day
753	4.7.1.3 Perform Detailed planning of Move Package	11/10/15	11/24/15	14 edays
754	**4.7.2 Execute PSP Moves**	**10/27/15**	**4/24/16**	**129 days**
755	4.7.2.1 Execute PSP Move Group 1	10/27/15	1/25/16	3 emons



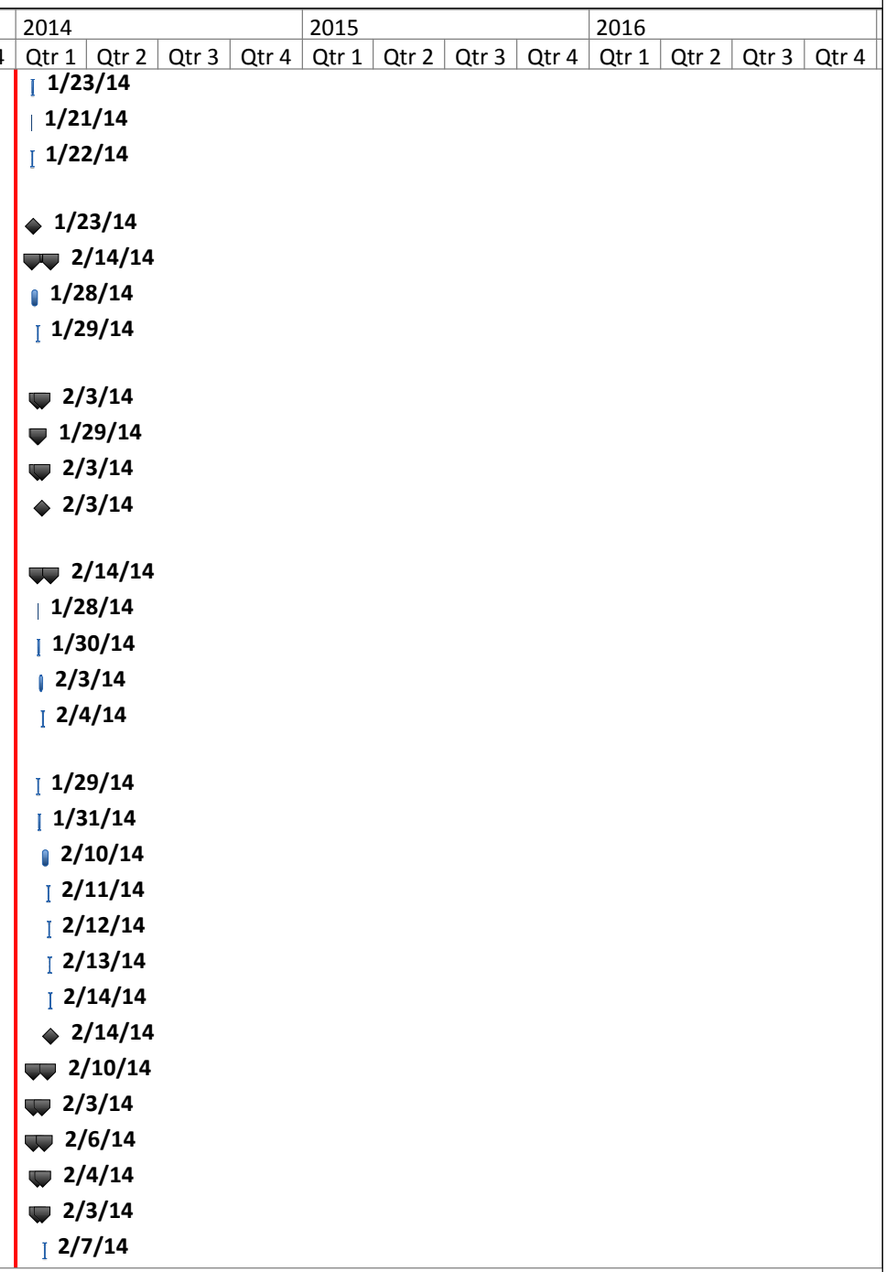
ID	Task Name	Start	Finish	Duration
756	4.7.2.2 Execute PSP Move Group 2	1/25/16	4/24/16	3 emons
757	**4.8 DOH Application Workload Migration**	**10/27/15**	**4/24/16**	**129 days**
758	**4.8.1 Plan DOH Workload Migration**	**10/27/15**	**11/24/15**	**21 days**
759	4.8.1.1 Send Application Questionnaires to Application Owners	10/27/15	11/10/15	14 edays
760	4.8.1.2 Kickoff Meeting - DOH Application Workload Migration	11/10/15	11/10/15	1 day
761	4.8.1.3 Perform Detailed planning of Move Package	11/10/15	11/24/15	14 edays
762	**4.8.2 Execute DOH Moves**	**10/27/15**	**4/24/16**	**129 days**
763	4.8.2.1 Execute DOH Move Group 1	10/27/15	1/25/16	3 emons
764	4.8.2.2 Execute DOH Move Group 2	1/25/16	4/24/16	3 emons
765	4.9 MS-CoPA Application Workload Migration Completed	6/30/16	6/30/16	0 days
766	5 MS-CoPA Transition Program Complete	7/21/16	7/21/16	0 days
767	**6 Contract Milestones**	**1/31/14**	**6/30/16**	**629 days**
768	6.1 CM-1 - Key Staffing Completed	1/31/14	1/31/14	0 days
769	6.2 CM-2 - Contract Management Plan	4/1/14	4/1/14	0 days
770	6.3 CM-3 - Staffing Completed	9/9/14	9/9/14	0 days
771	6.4 CM-4 - Data Center Architecture Complete	9/9/14	9/9/14	0 days
772	6.5 CM-5 - Data Gathering Completed	9/9/14	9/9/14	0 days
773	6.6 CM-6 - Detailed Transition Plan Completed	8/26/14	8/26/14	0 days
774	6.7 CM-7 - Commonwealth Compute Procs Manual (CCPM) Completed	6/17/14	6/17/14	0 days
775	6.8 CM-8 - Network Connectivity Completed	6/17/14	6/17/14	0 days
776	6.9 CM-9 - Security Arch, Soln, Policies and Procedures Completed	9/9/14	9/9/14	0 days
777	6.10 CM-10 - ITSM Systems Integration Completed	9/9/14	9/9/14	0 days
778	6.11 CM-11 - Financial Management Complete	9/9/14	9/9/14	0 days
779	6.12 CM-12 - Operational Readiness	12/2/14	12/2/14	0 days
780	6.13 CM-13 - SSAE 16 Audit of EDC Complete	12/3/14	12/3/14	0 days
781	6.14 CM-14 - DPH DCM Completed	6/30/15	6/30/15	0 days
782	6.15 CM-15 - EDC Transition Completed	9/9/14	9/9/14	0 days
783	6.16 CM-16 - L&I DCM Completed	6/30/16	6/30/16	0 days
784	6.17 CM-17 - DOR DCM Completed	6/30/16	6/30/16	0 days
785	6.18 CM-18 - PSP DCM Completed	6/30/16	6/30/16	0 days
786	6.19 CM-19 - DPW DCM Completed	6/30/16	6/30/16	0 days



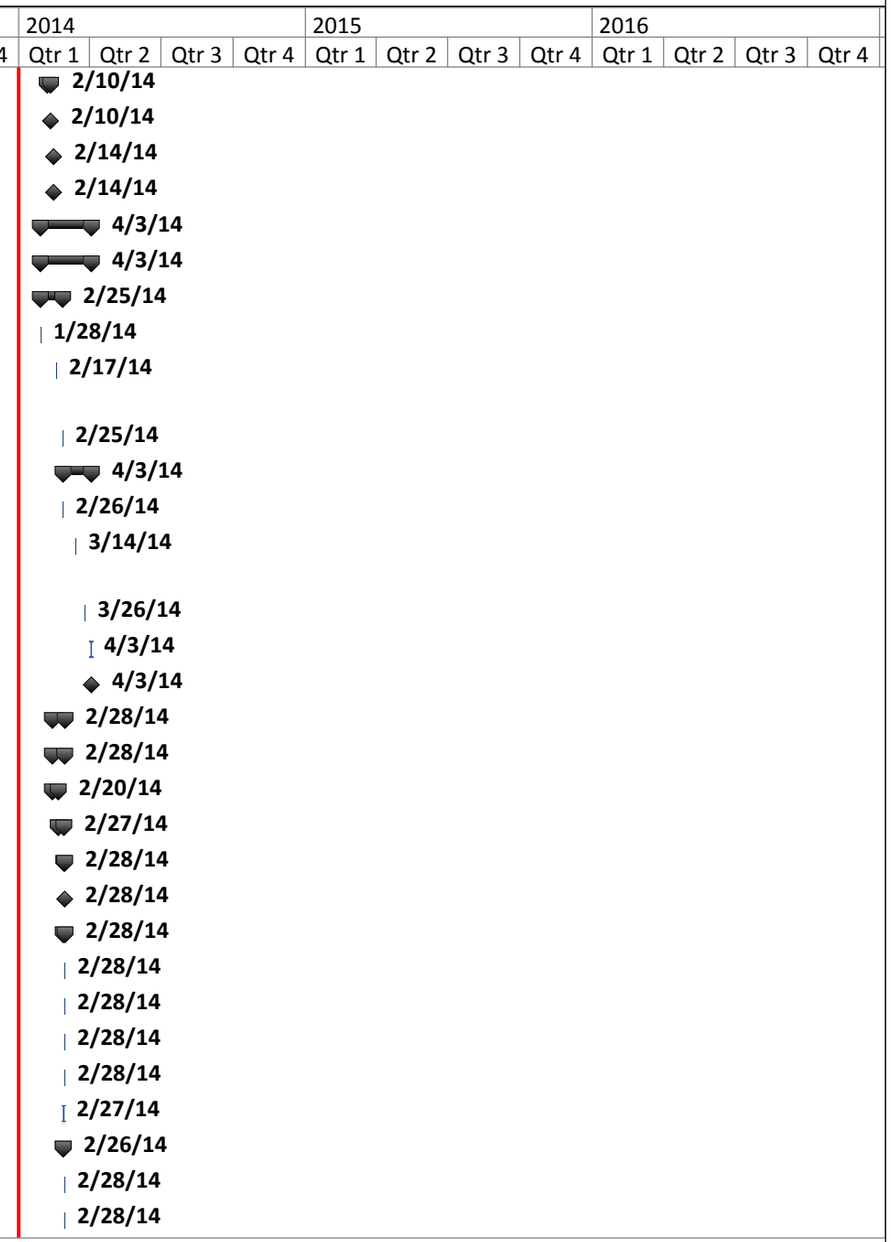
ID	Task Name	Start	Finish	Duration
787	6.20 CM-20 - DOH DCM Completed	6/30/16	6/30/16	0 days
788	**7 - Sample MOVE PACKAGE Schedule (to be replicated and modified as required by Move Package)**	**1/1/14**	**6/30/14**	**128 days**
789	**7.1 DCM_MP - PLAN MIGRATION**	**1/1/14**	**6/30/14**	**128 days**
790	**7.1.1 Project Management Tasks**	**1/1/14**	**6/30/14**	**128 days**
791	7.1.1.1 Governance Plan	1/1/14	6/30/14	180 edays
792	7.1.1.2 Risk Plan	1/1/14	6/30/14	180 edays
793	7.1.1.3 Validate Data Gathering Timeline	1/1/14	6/30/14	180 edays
794	7.1.1.4 Configuration/Test Plan	1/1/14	6/30/14	180 edays
795	**7.1.2 DCM_MP - MOVE STRATEGY/IDENTIFY SERVERS**	**1/1/14**	**1/17/14**	**13 days**
796	7.1.2.1 Schedule Individual Application Meetings and Distribute Questionnaire	1/1/14	1/1/14	1 day
797	7.1.2.2 Conduct One-on-One Application Owner Meetings	1/9/14	1/15/14	1 wk
798	7.1.2.3 Conduct Internal Planning Meeting/Review Overall Approach	1/16/14	1/16/14	2 hrs
799	7.1.2.4 Identify In-Scope P2P, V2V, Forklift Server/Application	1/16/14	1/16/14	4 hrs
800	7.1.2.5 Validate Move Strategy & Initial Logistics Assessment (Virtual & Forklift)	1/16/14	1/16/14	4 hrs
801	7.1.2.6 Validate Out-of-Warranty Servers	1/16/14	1/16/14	4 hrs
802	7.1.2.7 Determine HA, backup and DR requirements for each application	1/17/14	1/17/14	4 hrs
803	7.1.2.8 Refine MP Move Baseline (Unix and Intel) with DCM Team Review	1/17/14	1/17/14	4 hrs
804	**7.1.2.9 DCM_MP - CODE FREEZE**	**1/17/14**	**1/17/14**	**0.5 days**
805	7.1.2.9.1 Initiate MP Server Baseline Inventory Freeze	1/17/14	1/17/14	0.5 hrs
806	7.1.2.9.2 Initiate MP Code Freeze for all the Related Applications	1/17/14	1/17/14	0.5 hrs
807	7.1.2.9.3 Remove any remaining hard coded IP s from the applications	1/17/14	1/17/14	4 hrs
808	7.1.2.9.4 COMPLETED: DCM_MP - CODE FREEZE	1/17/14	1/17/14	0 days
809	7.1.2.10 COMPLETED: DCM_MP - MOVE STRATEGY / IDENTIFY SERVERS	1/17/14	1/17/14	0 days
810	**7.1.3 DCM_MP - MOVE STRATEGY SIGNOFF**	**1/20/14**	**1/21/14**	**1.5 days**
811	7.1.3.1 Review Move Package Contents and Strategy with	1/20/14	1/20/14	1 day
812	7.1.3.2 Provide Move Package Contents and Strategy to for Approval	1/21/14	1/21/14	2 hrs
813	7.1.3.3 Receive Move Package Content and Strategy Approval to Proceed from	1/21/14	1/21/14	2 hrs
814	7.1.3.4 COMPLETED: MP - MOVE PACKAGE STRATEGY SIGNOFF	1/21/14	1/21/14	0 days
815	**7.1.4 DCM_MP - DUE DILIGENCE PLANNING**	**1/21/14**	**1/23/14**	**1.63 days**
816	7.1.4.1 Schedule, Prepare, Perform MP Kickoff Meeting	1/21/14	1/21/14	1 hr



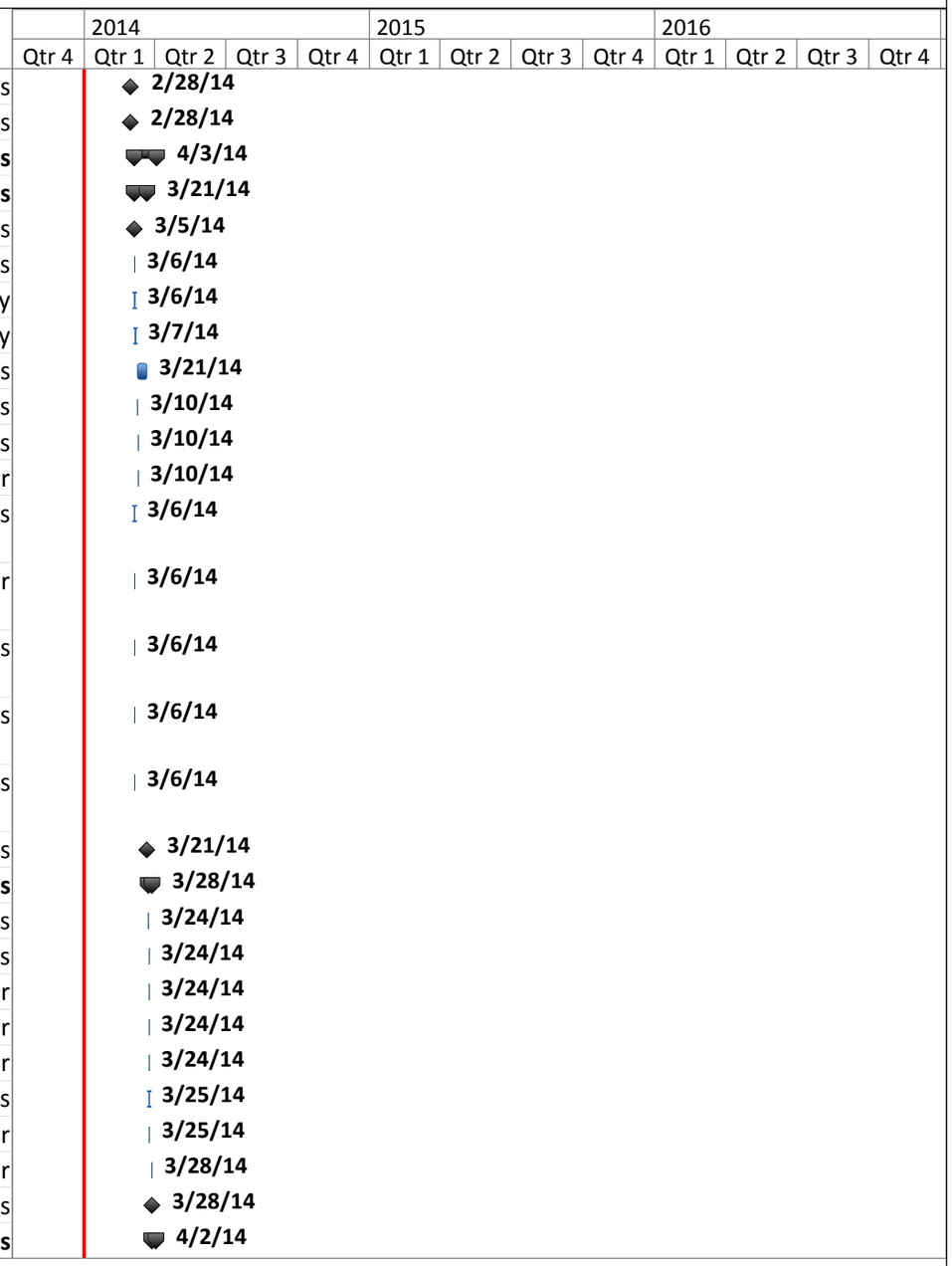
ID	Task Name	Start	Finish	Duration
817	7.1.4.2 Establish Weekly Meetings with App Owners and Technical Team	1/21/14	1/23/14	1.5 days
818	7.1.4.3 Schedule WAN Analysis (optional)	1/21/14	1/21/14	0.06 days
819	7.1.4.4 Check if WAN Analysis is completed & remediation implemented (optional)	1/21/14	1/22/14	0.5 days
820	7.1.4.5 COMPLETED: DCM_MP - DUE DILIGENCE PLANNING	1/23/14	1/23/14	0 days
821	**7.1.5 DCM_MP - CREATE WORKBOOK**	**1/21/14**	**2/14/14**	**18 days**
822	7.1.5.1 Initiate Workbook for Move	1/21/14	1/28/14	1 wk
823	7.1.5.2 Assess MP in-flight projects, determine status and establish a plan for completion	1/28/14	1/29/14	1 day
824	**7.1.5.3 DCM_MP - DEVELOP RISK MANAGEMENT PLAN FOR MOVE**	**1/28/14**	**2/3/14**	**4 days**
825	**7.1.5.3.1 MP_RISK - RISK MITIGATION**	**1/28/14**	**1/29/14**	**1 day**
828	**7.1.5.3.2 MP_RISK - CONTINGENCY PLANNING**	**1/28/14**	**2/3/14**	**4 days**
834	7.1.5.3.3 COMPLETED: DCM_MP_PM - DEVELOP RISK MANAGEMENT PLAN FOR MOVE	2/3/14	2/3/14	0 days
835	**7.1.5.4 MP_APPS - DEVELOP TEST PLANS**	**1/28/14**	**2/14/14**	**13 days**
836	7.1.5.4.1 Review Initial Test Plan Template with the Application Test Lead	1/28/14	1/28/14	4 hrs
837	7.1.5.4.2 Identify Applications to be Tested	1/29/14	1/30/14	16 hrs
838	7.1.5.4.3 Identify Application Testers	1/31/14	2/3/14	16 hrs
839	7.1.5.4.4 Commit to Re-IP Planned Outage Window + Receive Email Approval from App Owners	2/4/14	2/4/14	8 hrs
840	7.1.5.4.5 Work with Application Test Lead to Create the Test Plan	1/29/14	1/29/14	8 hrs
841	7.1.5.4.6 Develop the High Level Test Plan (HLTP)	1/30/14	1/31/14	16 hrs
842	7.1.5.4.7 Create Test Cases / Scripts	2/4/14	2/10/14	5 days
843	7.1.5.4.8 Finalize Test Plan	2/11/14	2/11/14	8 hrs
844	7.1.5.4.9 Execute Dry Run of Test Cases and Scripts (Baseline)	2/12/14	2/12/14	8 hrs
845	7.1.5.4.10 Establish Success Criteria Statement for DCM Event	2/13/14	2/13/14	4 hrs
846	7.1.5.4.11 Receive Written Approval of Test Plan and Success Criteria from	2/13/14	2/14/14	1 day
847	7.1.5.4.12 COMPLETED: MP_APPS - DEVELOP TEST PLANS	2/14/14	2/14/14	0 days
848	**7.1.5.5 DCM_MP - SITE PREPARATION**	**1/23/14**	**2/10/14**	**12.13 days**
849	**7.1.5.5.1 DCM_MP_SP - SERVER IP REQUIREMENTS**	**1/23/14**	**2/3/14**	**7.25 days**
859	**7.1.5.5.2 DCM_MP_SP - FIREWALL RULE REQUIREMENTS**	**1/23/14**	**2/6/14**	**10 days**
866	**7.1.5.5.3 DCM_MP_SP - WINTEL SERVICE REQUESTS**	**1/28/14**	**2/4/14**	**4.38 days**
879	**7.1.5.5.4 DCM_MP_SP - UNIX SERVICE REQUESTS**	**1/28/14**	**2/3/14**	**3.75 days**
904	7.1.5.5.5 DCM_MP_SP - Confirm SAN Setup	2/6/14	2/7/14	1 day



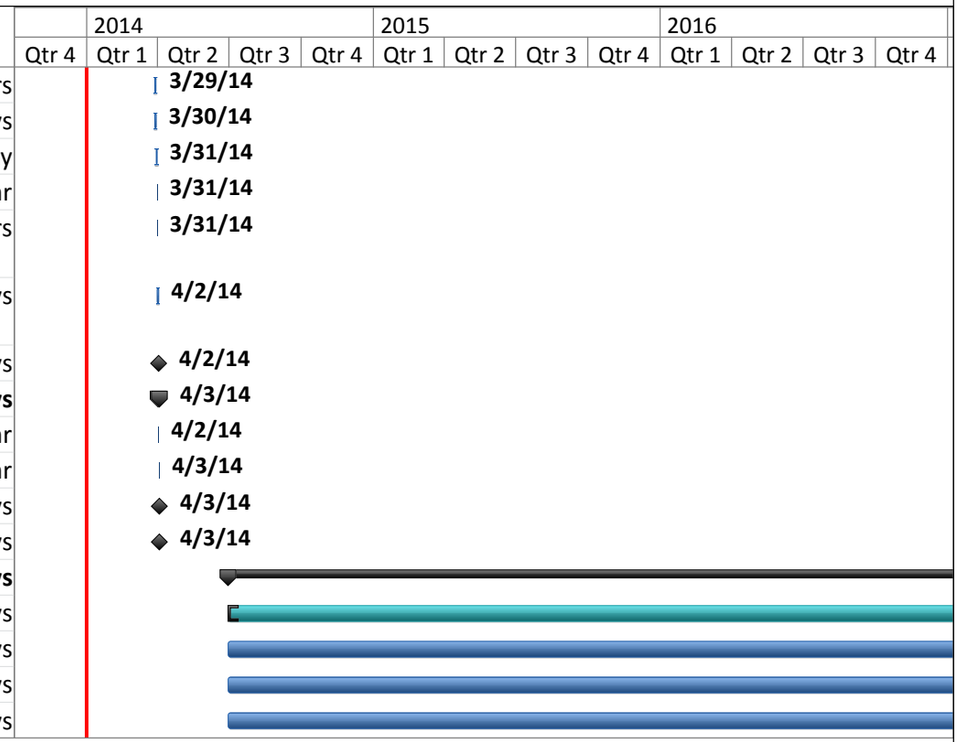
ID	Task Name	Start	Finish	Duration
905	**7.1.5.5.6 MP_APPS - FIREWALL SERVICE REQUEST**	**2/6/14**	**2/10/14**	**2.13 days**
912	7.1.5.5.7 COMPLETED: DCM_MP_SP - SITE PREPARATION	2/10/14	2/10/14	0 days
913	7.1.5.6 COMPLETED: DCM_MP - CREATE WORKBOOK	2/14/14	2/14/14	0 days
914	7.1.6 COMPLETED: DCM_MP - PLAN MIGRATION	2/14/14	2/14/14	0 days
915	**7.2 DCM_MP - MIGRATION TO DC1**	**1/28/14**	**4/3/14**	**46.75 days**
916	**7.2.1 DCM_MP - REVIEW AUDITS AND DCM NOTIFICATIONS**	**1/28/14**	**4/3/14**	**46.75 days**
917	**7.2.1.1 Pre-Re-IP Notifications**	**1/28/14**	**2/25/14**	**20.5 days**
918	7.2.1.1.1 Prepare & Send 30 Day Pre-Re-IP Planned Outage Notice	1/28/14	1/28/14	4 hrs
919	7.2.1.1.2 Prepare & Send 7 Day Pre-Re-IP Planned Outage Notice	2/17/14	2/17/14	0.5 days
920	7.2.1.1.3 Prepare & Send 2 Day Pre-Re-IP Planned Outage Notice	2/25/14	2/25/14	4 hrs
921	**7.2.1.2 Pre-DCM Notifications**	**2/26/14**	**4/3/14**	**25.88 days**
922	7.2.1.2.1 Prepare & Send 30 Day Pre-DCM Planned Outage Notice	2/26/14	2/26/14	4 hrs
923	7.2.1.2.2 Prepare & Send 7 Day Pre-DCM Planned Outage Notice	3/14/14	3/14/14	4 hrs
924	7.2.1.2.3 Prepare & Send 2 Day Pre-DCM Planned Outage Notice	3/26/14	3/26/14	4 hrs
925	7.2.1.2.4 Completion Notification (3 days post-move)	4/3/14	4/3/14	2 hrs
926	7.2.1.3 COMPLETED: DCM_MP REVIEW AUDITS AND DCM NOTIFICATIONS	4/3/14	4/3/14	0 days
927	**7.2.2 DCM_MP - Re-IP/Mock Move EVENT**	**2/13/14**	**2/28/14**	**12 days**
928	**7.2.2.1 DCM_MP_Re-IP - EXECUTION**	**2/13/14**	**2/28/14**	**11.5 days**
929	**7.2.2.1.1 MP_Re-IP - PREPARE APPLICATIONS**	**2/13/14**	**2/20/14**	**5.25 days**
947	**7.2.2.1.2 MP_Re-IP - GO/NO-GO DECISION**	**2/20/14**	**2/27/14**	**5.25 days**
956	**7.2.2.1.3 MP_Re-IP - EXECUTE Re-IP EVENT**	**2/27/14**	**2/28/14**	**1 day**
961	7.2.2.1.4 COMPLETED: DCM_MP_Re-IP - EXECUTION	2/28/14	2/28/14	0 days
962	**7.2.2.2 DCM_MP_Re-IP - POST RE-IP ACTIVITIES**	**2/26/14**	**2/28/14**	**2.25 days**
963	7.2.2.2.1 Update/Verify new IP Addresses for All Servers in Baseline	2/28/14	2/28/14	4 hrs
964	7.2.2.2.2 Commit to Move Package Planned Outage Window	2/28/14	2/28/14	2 hrs
965	7.2.2.2.3 Make Initial Move Logistics Arrangements	2/28/14	2/28/14	2 hrs
966	7.2.2.2.4 Install any required data transfer hardware or software agents (opt	2/28/14	2/28/14	2 hrs
967	7.2.2.2.5 Develop/Distribute Move Hr-By-Hr Plan (Draft)	2/26/14	2/27/14	7 hrs
968	**7.2.2.2.6 Submit CRQ Numbers to PM for Move**	**2/26/14**	**2/26/14**	**0.13 days**
977	7.2.2.2.7 Reserve War Room (Conference Rooms) for Move event	2/28/14	2/28/14	2 hrs
978	7.2.2.2.8 Arrange Site Access for Move Event	2/28/14	2/28/14	2 hrs



ID	Task Name	Start	Finish	Duration
979	7.2.2.2.9 COMPLETED: DCM_MP_Re-IP - POST RE-IP ACTIVITIES	2/28/14	2/28/14	0 days
980	7.2.2.3 COMPLETED: DCM_MP - Re-IP EVENT	2/28/14	2/28/14	0 days
981	**7.2.3 DCM_MP - MOVE PACKAGE MIGRATION EVENT**	**3/5/14**	**4/3/14**	**20.25 days**
982	**7.2.3.1 DCM_MP_MOVE - PERFORM FINAL LOGISTICS TASKS**	**3/5/14**	**3/21/14**	**12 days**
983	7.2.3.1.1 Submit Final Logistics Request Form to Logistics Manager	3/5/14	3/5/14	0 days
984	7.2.3.1.2 Request ISSA Approval to ship systems	3/6/14	3/6/14	0.5 hrs
985	7.2.3.1.3 Provide Logistics Quote & Shipping Plan to Project Manager for App	3/6/14	3/6/14	1 day
986	7.2.3.1.4 Receive Approved Logistics Quote & Shipping Plan from Project Ma	3/7/14	3/7/14	1 day
987	7.2.3.1.5 Initiate Logistics Plan & Coordinate with Shipping Vendors	3/10/14	3/21/14	10 days
988	7.2.3.1.6 Confirm DC Physical Security Arrangements (Guards are Notified)	3/10/14	3/10/14	2 hrs
989	7.2.3.1.7 Confirm security access arrangements for source locations	3/10/14	3/10/14	2 hrs
990	7.2.3.1.8 Submit Change Request for Move Event	3/10/14	3/10/14	1 hr
991	7.2.3.1.9 AC-Verify CCPM contains specific details for apps within Move Package	3/6/14	3/6/14	4 hrs
992	7.2.3.1.10 AC-Validate Monitoring is in place for Move Package Apps - will appear on dashboards	3/6/14	3/6/14	1 hr
993	7.2.3.1.11 AC-Confirm SLAs are in place for Move Package Apps	3/6/14	3/6/14	0.13 days
994	7.2.3.1.12 AC-Confirm ITSM ready to receive information regarding Move Package Apps	3/6/14	3/6/14	0.13 days
995	7.2.3.1.13 AC-Verify DR plans and test scheduled as appropriate	3/6/14	3/6/14	0.13 days
996	7.2.3.1.14 COMPLETED: DCM_MP_MOVE - PERFORM FINAL LOGISTICS TASK	3/21/14	3/21/14	0 days
997	**7.2.3.2 DCM_MP_MOVE - GO/NO-GO DECISION**	**3/24/14**	**3/28/14**	**4.38 days**
998	7.2.3.2.1 Finalize the Move Hr-By-Hr Plan Schedule	3/24/14	3/24/14	2 hrs
999	7.2.3.2.2 Prepare for Move GO/NO-GO Conference Call	3/24/14	3/24/14	2 hrs
1000	7.2.3.2.3 Review Final Move Package Risks with	3/24/14	3/24/14	1 hr
1001	7.2.3.2.4 Validate and Approve Move Package Success Criteria with	3/24/14	3/24/14	1 hr
1002	7.2.3.2.5 Submit Supplemental CMDB Updates for Migration (if needed)	3/24/14	3/24/14	1 hr
1003	7.2.3.2.6 Final Receiving Site(s) Walk-Thru Inspection	3/24/14	3/25/14	2 hrs
1004	7.2.3.2.7 Conduct Internal Move GO/NO-GO Decision	3/25/14	3/25/14	1 hr
1005	7.2.3.2.8 Conduct Formal Move GO/NO-GO Decision	3/28/14	3/28/14	1 hr
1006	7.2.3.2.9 COMPLETED: DCM_MP_MOVE - GO/NO-GO DECISION	3/28/14	3/28/14	0 days
1007	**7.2.3.3 DCM_MP_MOVE - EXECUTE MOVE EVENT ACTIVITIES**	**3/28/14**	**4/2/14**	**3.25 days**



ID	Task Name	Start	Finish	Duration
1008	7.2.3.3.1 Relocate Equipment (Forklift)	3/28/14	3/29/14	30 ehrs
1009	7.2.3.3.2 Migration Activities (See Move Hr-By-Hr Plan for Full Details)	3/28/14	3/30/14	2 edays
1010	7.2.3.3.3 Conduct Move Application Testing	3/30/14	3/31/14	1 eday
1011	7.2.3.3.4 Final Conf Call and Verbal approvals	3/31/14	3/31/14	1 ehr
1012	7.2.3.3.5 AC-Provide MP Completion Documentation to Steady State and receive signoff	3/31/14	3/31/14	2 ehrs
1013	7.2.3.3.6 AC-Received Approved MP Completion Documentation from App Owners	3/31/14	4/2/14	2 days
1014	7.2.3.3.7 COMPLETED: DCM_MP_MOVE - EXECUTE MOVE EVENT ACTIVITIES	4/2/14	4/2/14	0 days
1015	**7.2.3.4 DCM_MP_POST-MOVE LESSONS LEARNED**	**4/2/14**	**4/3/14**	**1.25 days**
1016	7.2.3.4.1 MP_Post- Move Lessons Learned - Internal Team	4/2/14	4/2/14	1 hr
1017	7.2.3.4.2 MP_Post- Move Lessons Learned - Full Team	4/3/14	4/3/14	1 hr
1018	7.2.3.4.3 COMPLETED: DCM_MP_POST-MOVE LESSONS LEARNED	4/3/14	4/3/14	0 days
1019	7.2.3.5 COMPLETED: DCM_MP - MOVE PACKAGE MIGRATION EVENT	4/3/14	4/3/14	0 days
1020	**8 Steady State Operations and Continuous Improvement**	**6/30/14**	**12/31/24**	**2742 days**
1021	8.1 Operations Monitoring	6/30/14	12/31/24	2742 days
1022	8.2 Service Request Management	6/30/14	12/31/24	2742 days
1023	8.3 Disaster Recovery Testing	6/30/14	12/31/24	2742 days
1024	8.4 Security Testing	6/30/14	12/31/24	2742 days



4.0 Prior Experience

4. PRIOR EXPERIENCE 4-3

4.1 OVERALL 4-3
4.1.1 Team Introduction and Prior Experience 4-4
4.1.2 IBM, Key Partner 4-5
4.1.3 Deloitte, Key Partner 4-5
4.1.4 Teaming Approach 4-5
4.1.5 Small Diverse Business Partners 4-6
4.1.6 Why this Team 4-7
4.1.7 Experience and Services Relative to this RFP 4-10
4.1.8 Team Qualifications 4-11
4.1.9 Service Levels 4-16
4.1.10 Quality of Comparable Services 4-16
4.1.11 References and Length of Service 4-17
4.2 UNISYS CORPORATE INFORMATION 4-19
4.2.1 History and Background 4-19
4.2.2 Current Services 4-19
4.2.3 Client Focus 4-20
4.2.4 Services, Global Outsourcing is a Unisys Key Strategy 4-20
4.2.5 Global Footprint 4-22
4.2.6 Technology Agnostic and Committed to Strategic Partnerships 4-23
4.2.7 Corporate Organization 4-24
4.3 UNISYS STRATEGIC DIRECTION 4-27
4.3.1 Unisys Corporate Mission 4-27
4.3.2 Corporate Strategy 4-28
4.3.3 Innovation 4-31
4.3.4 Hybrid Enterprise – Building the Data Center of the Future 4-36
4.3.5 Platform Strategy 4-41
4.3.6 Service Management Strategy 4-43
4.3.7 Impact on the Commonwealth 4-45
4.3.8 Summary Unisys Strategic Direction 4-48
4.4 UNISYS DEDICATION TO QUALITY 4-51
4.4.1 Approach to Measuring & Maintaining High Quality Services 4-52
4.4.2 Industry-recognized Quality Standards and Awards 4-58
4.4.3 External Quality Certification 4-60
4.4.4 Detailed Approach and Quality Plan 4-64
4.4.5 Summary of the Unisys Dedication to Quality 4-73
4.5 CLIENT REFERENCES 4-75
4.5.1 Project References (RFP Appendix C) 4-75
4.5.2 Unisys Project References 4-79
4.5.2 IBM Project References 4-106
4.5.3 Deloitte LLP Project References 4-115

4.5.4 Acclaim Systems, Inc. Project References 4-126
4.5.5 American Personnel Managers and Consultants, Inc. Project References 4-132
4.5.6 Credo Technology Solutions, Inc. Project References 4-144
4.5.7 Domino Technologies, Inc. Project References 4-150
4.5.8 e&e IT Consulting Services, Inc. Project References 4-157
4.5.9 Info-Matrix Corporation Project References 4-163
4.5.10 Innovative Business Concepts, Inc. Project References 4-169
4.5.11 PC Network, Inc. Project References 4-176
4.5.12 Pierson Computing Connection, Inc. Project References 4-184
4.6 SUBCONTRACTORS AND SUPPLIERS 4-189
4.6.1 Unisys Subcontractors and Suppliers Capabilities Table 4-189
Schedule L – Unisys List of Subcontractors 4-190

4. Prior Experience

RFP	*Requirement*
	Overall *The Offeror must provide information describing its background, services, experience, and qualifications relative to the scope of this RFP. Information that will be considered includes the length of the service, service levels, references, and quality of comparable services provided to other clients. The Offeror should also indicate any additional information that will be helpful to the Commonwealth's evaluation.*

4.1 Overall

Unisys, the Prime Contractor

Unisys, serving as the prime contractor, will be the single point of contact for the Commonwealth. As demonstrated under our existing Data PowerHouse (DPH) contract, Unisys will continue to lead and take full responsibility and accountability for contract execution, subcontractor performance, and all related issues.

"Unisys…has built its own infrastructure of systems and people ready and able to meet customer needs on a global basis. In recent years, Unisys has demonstrated it understands the power of partnerships and exploited this understanding to become one of the premier service organizations in the market."
—Gartner

This engagement is personal to Unisys since we are a Pennsylvania-based company that depends on many Commonwealth services. That is one reason we have worked so hard when awarded Commonwealth contracts.

We believe deeply that our clients must become our partners and we do everything possible to strengthen the relationships by doing whatever is necessary to meet their high expectations of service and quality.

Unisys has worked with many State, Local, Federal, and foreign government clients for more than 50 years. As a result, we have a deep appreciation and understanding of providing mission critical, innovative solutions in the public sector. For many of these 50 years, we have provided services to Commonwealth agencies. In fact, some of our global best practices were created as a result of our work with the Commonwealth.

Our knowledge of the thousands of Commonwealth applications, a thorough understanding of your technical architecture, and an appreciation for and commitment to the needs and

expectations of state agencies, are extremely important to successfully transform the Commonwealth's computing environment.

Unisys believes that one of our most important differentiators is the experience and strength of our entire team. As part of providing background related to our prior experience, we want to start by introducing the Commonwealth to our team.

When combining the like extensive Commonwealth experience of our key partners, IBM and Deloitte, no other service provider will be able to mitigate risk and delivery cost effective on-demand computing capacity better than our knowledgeable team.

4.1.1 Team Introduction and Prior Experience

In anticipation of the release of the Data Center Computing Services Request for Proposal (RFP), one of the first tasks Unisys undertook was an analysis of what partnerships would add the most value and strengthen the already strong Unisys and IBM team serving the Commonwealth. After making the initial partner decisions, we validated our selections against the requirements outlined in the Request for Information (RFI) and then in the RFP issued by the Commonwealth. Finally, after twice validating the requirements, we solidified a core "best of class" team to serve the Commonwealth and to bring a fresh perspective and innovative ideas. Our team members were carefully selected to significantly reduce risk and to deliver this initiative on time and on budget and to provide high quality cost effective ongoing services. This knowledge and experience is a key differentiator between the Unisys Team and others that may claim they have the necessary Commonwealth experience to transition the Commonwealth's most important business systems.

Local Resources

*In **Pennsylvania**, Unisys, IBM, and Deloitte **employ 6,962 people** with over **900 people in Metropolitan Harrisburg area***

Given the RFP requirements, especially for the transition and transformation to an On-Demand infrastructure Private Cloud Model, Unisys formed our consortium under a very specific premise that our strategic partners have an extensive resume of proven experience delivering outsourced compute services as well as specific long-term business experience with the Commonwealth. Entrusting such an important initiative to those with limited exposure to the Commonwealth, increases risk of failure. This is not an environment conductive to implementation by trial and error.

To put it simply, the Commonwealth is looking for a trusted partner to lead a proven consortium of service providers in managing the compute services that supports the Commonwealth's mission and non-mission critical business application systems.

While providing a more transparent and cost effective, On-Demand services model is important, we also understand that this initiative revolves around the Commonwealth's

business application systems. Therefore, beyond just managing the hardware and software and related infrastructure we sought the best possible team to support the agency business applications.

4.1.2 IBM, Key Partner

One of our key determining factors in forming our consortium is **that Unisys and IBM invented or supplied the technology infrastructure that hosts nearly all of the Commonwealth's critical business application systems.**

Another key determining factor is that Unisys and IBM developed a significant portion of the system software infrastructure supporting the Commonwealth's most mission critical business applications.

Also, IBM has been a valued partner with the current DPH project, and therefore has gained valuable long-term experience with the Commonwealth. This experience is extremely important to the success of this project. We are excited to have IBM as a key partner.

As a result of choosing IBM, the two companies (IBM and Unisys) that have successfully provided DPH services for the past 14 years will again work together to best serve the Commonwealth.

4.1.3 Deloitte, Key Partner

Although both Unisys and IBM have more than 50 years of working knowledge of the Commonwealth's business application systems and the underlying technology, we will enhance our team with additional services from Deloitte. Deloitte represents the largest, most experienced applications integrator, developer, and application maintenance provider to support the Commonwealth's business application systems. This experience will be extremely valuable.

Unisys

IBM and Deloitte

No other team possesses the collective knowledge, experience, and track record of this core team in providing managed infrastructure security and application services to the Commonwealth

Also, Deloitte currently provides the Commonwealth with a number of security services. In fact, Deloitte is the largest provider of these services to the Commonwealth. Security is extremely important to this engagement's success and is another important reason Deloitte was selected as a Key Partner.

4.1.4 Teaming Approach

We combined our respective Unisys and IBM management and technical talent, along with Deloitte resources, into a single team. This approach will provide the Commonwealth with

significant experience, and a very detailed understanding of the Commonwealth, its agencies and the specific challenges of implementing such a complex project. Having such a wealth of knowledge gained over decades of working with the Commonwealth and its agencies will be invaluable and frankly is the major differentiator between our team and the competition.

Unisys, IBM, and Deloitte form the core of a "best-of-class" team to deliver compute services to the Commonwealth efficiently and securely.

Figure 4-1 are the key factors in our selection of IBM and Deloitte as key Unisys partners for this engagement:

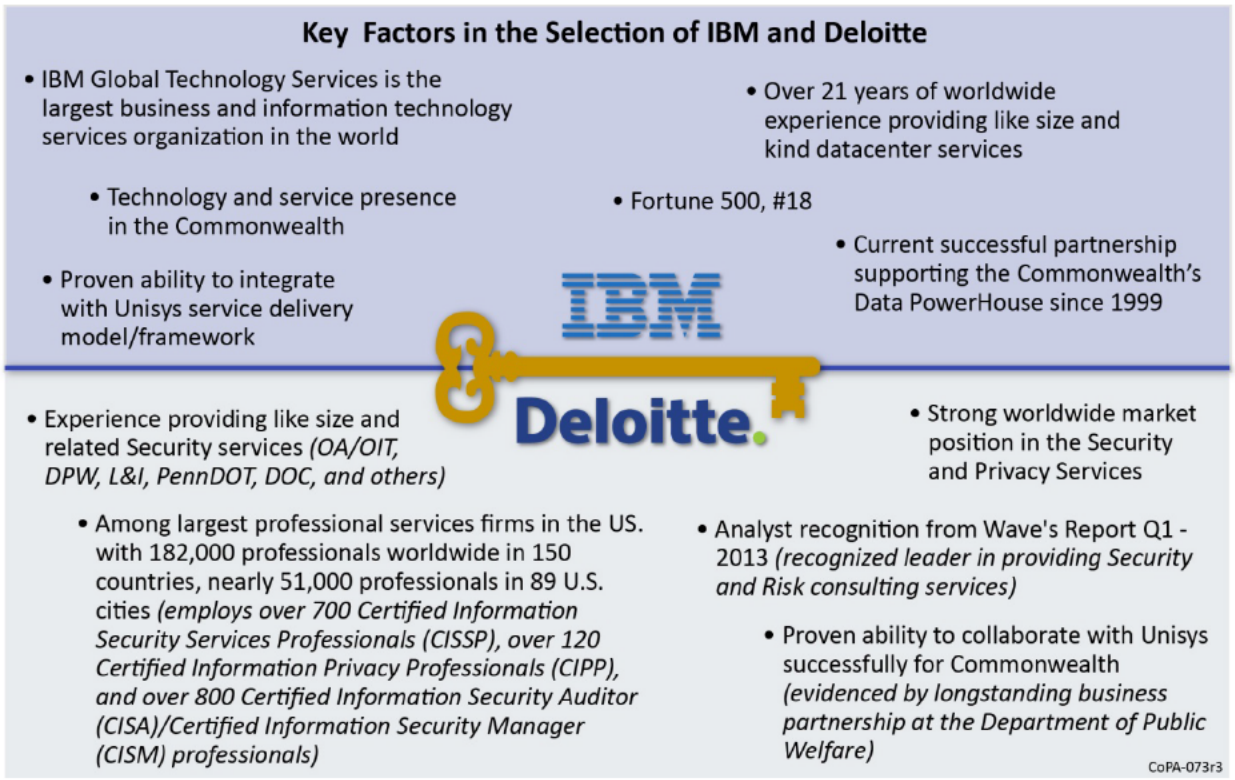


Figure 4-1. Key Factors in the Selection of IBM and Deloitte.

4.1.5 Small Diverse Business Partners

We understand the importance and value of having talented small businesses join our team. Several Small Diverse Businesses (SDBs) have joined as partners. We selected them specifically for their direct experience in providing like services to the Commonwealth. They represent the very best of small businesses in Pennsylvania, and we are proud to have them on our team.

In line with Governor Corbett's support for small business development and expansion, we will be using SDB qualified businesses, including Acclaim Systems, e&e Consulting, Info-

Matrix Corporation, Domino Technologies, American Personnel Management Consultants (APMC), PCN-Network, Innovative Business Concepts (IBC), Credo Technologies, Latus Commercial realty, and Pierson Computing Connection to help us achieve your vision. It is important to note these are ALL—all Pennsylvania-based small businesses. Our selection criteria verified each of these businesses has specific expertise in the areas such as application and infrastructure support service management, help desk, transition services, media management, staffing, cultural change management, and other areas as defined in our proposal.

4.1.6 Why this Team

It is clear….. **No other team possesses the collective knowledge and experience of Commonwealth compute services than the Unisys consortium.**

Also our consortium has a proven record of success over many years of service delivery to Commonwealth agencies. Therefore we offer the lowest risk and virtually no learning curve. That means a much greater probability that your vision will be achieved on time, within budget and fully meeting your expectations. This will be extremely beneficial given this engagement's nature and the need for consistency in affecting the transition and transformation to a new Commonwealth data center operating model. Bottom line—we formed the team that combines the best management disciplines with the experience and expertise to deliver the highest levels of client service, at the lowest risk to the Commonwealth.

Table 4-1 showcases our team and the value they bring to the Commonwealth.

Table 4-1. The Unisys Team

Company	Description
UNISYS	Unisys is an industry leader providing information technology (IT) services and technologies for governments around the globe as well as the world's top banks and other financial services companies. At the Commonwealth of Pennsylvania, we have more than 50 years of demonstrated successful delivery on mission critical systems and programs. We assembled a team of highly qualified information technology professionals who all have extensive Commonwealth-specific knowledge. Our team will be leveraging their experience supporting the Commonwealth's IT environments while meeting the Commonwealth's requirements. As the prime contractor, Unisys will be solely accountable for overall program performance.
IBM	International Business Machines Corporation (IBM) provides IT products and services worldwide. Its Global Technology Services segment provides IT infrastructure and business process services, including strategic outsourcing, process, integrated technology, and maintenance services, as well as technology-based support services. IBM will provide mainframe hardware/software support including installations, upgrades, and support. IBM has more than 50 years of providing like services to the Commonwealth. IBM will be providing technology products and managed services for IBM zSeries mainframes and IBM pSeries AIX mid-range based systems, including disaster recovery and capacity-on-demand services to the project.

Company	Description
Deloitte.	In the United States, Deloitte LLP and its subsidiaries have 57,000 professionals with a single focus: serving their clients and helping them solve their toughest problems. They work in four key business areas: audit, financial advisory, tax, and consulting. Deloitte has significant experience in supporting the Commonwealth of Pennsylvania with some of its most complex projects. Deloitte will be providing technical security services and database management support services to the project.
acclaim SYSTEMS	Acclaim Systems is a leading software solution company offering a multitude of comprehensive and customized services. Acclaim Systems is committed to maintaining client relationships by effectively aligning technology and consulting resources with clients' dynamic business requirements. Acclaim Systems succeeds by investing in the professional fulfillment of their employees. Consistent delivery of high-quality solutions results from employee empowerment. Acclaim Systems, a Pennsylvania certified Small Diverse Business, has extensive experience in providing like services to the Commonwealth. Acclaim Systems will be providing technical and project management support resources to the project.
AMERICAN PERSONNEL MANAGERS and CONSULTANTS, INC.	American Personnel Managers & Consultants, Inc. is a superior human resource management and recruiting firm, staffing and project management company with more than 70 years of experience in staffing and 13 years of experience with staffing, the Pennsylvania Data PowerHouse (DPH) project. APMC is a Pennsylvania-certified Small Diverse Business. APMC will be providing technical support resources to the project.
CREDO TECHNOLOGY SOLUTIONS	Credo is a Pennsylvania-certified Small Diverse Business that has built a tight cadre of team members focused on consistently delivering services that help clients meet their IT challenges. Credo's staff and strategic partners are able to offer business and technology solutions as well as project management offerings. Credo Technology Solutions will be providing technical and project management support resources to the project.
Domino Technologies, Inc.	Since its founding in 1996, Domino Technologies, Inc. has built a solid record of performance working with clients in both the private sector and government. Domino Technologies had consistently delivered innovative business solutions, using the latest technology to fulfill the Commonwealth's goals. Domino Technologies, a Pennsylvania-certified Small Diverse Business, has extensive experience in providing infrastructure-managed services to the Commonwealth. Domino Technologies will be providing technical and project management support resources to the project.
e&e IT Consulting Services, Inc.	e&e IT Consulting Services, Inc. is a Pennsylvania-certified certified Small Diverse Business technology services firm providing staffing in Pennsylvania, Virginia, New Jersey, and the City of Philadelphia. e&e provides all levels of skilled IT professionals to clients in Central Pennsylvania and surrounding areas. e&e is recognized for the sixth consecutive year as one of the Top 50 Fastest Growing Companies in Central Pennsylvania, making significant contributions to the growth, strength, and success of the Central Pennsylvania region. e&e will be providing technical and project management support resources to the project.
INFO-MATRIX CORPORATION	Info-Matrix is a private, woman-owned information technology consulting firm based in Lemoyne, Pennsylvania. Since 1996, Info-Matrix has focused largely on the government sector, with an emphasis on human services IT projects, including Medicaid eligibility, welfare case management, and child support enforcement systems. From Texas to Alaska, Info-Matrix has broad experience at the federal, state, and local levels with hiring experienced professionals with an average of 15 years of IT experience who have distinguished themselves by successfully implementing complex government IT projects mainly at the Commonwealth of Pennsylvania.

Company	Description
	Info-Matrix will be providing technical and project management support resources to the project.
Innovative Business Concepts, Inc.	Since 1989, Innovative Business Concepts, Inc. (IBC) has been a Pennsylvania-certified Woman-Owned Business empowering customers to maximize productivity, efficiency, and cost savings by deploying the best people, practices, and knowledge in the technology industry. IBC provides excellent IT personnel, products, and services. IBC will be providing technical and project management staff to the project.
PCCi Pierson Computing Connection Inc	Pierson Computing Connection, Inc. (PCCi), a Pennsylvania-certified Women's Business Enterprise, is headquartered in Mechanicsburg, Pennsylvania and central to the Harrisburg Regional Technology Corridor Enterprise Zone. The 40-member PCCi team is dedicated to providing computer services with unsurpassed quality, uncommon honesty, and amazing customer satisfaction throughout every aspect of our project management, consulting, and installation services. PCCi has extensive experience in Pennsylvania performing infrastructure installations and setup as well as project management and IT project staffing. PCCI will be supplying infrastructure hardware, installation services, and project management services to the project.
PCN	PC Network (PCN) is a growing, woman-owned IT services company based in Center City Philadelphia that works with enterprises, prime contract partners, and the public sector. PCN provides affordable solutions for the many complex problems facing business today. PCN's customers span the commercial, transportation, defense, and government sectors. Founded in 1988, PCN has evolved from its traditional systems integrator roots to provide a broad range of IT consulting services. PCN has a strong focus on quality with ISO 9001 and TL9000 quality programs and is ISO 27000 compliant. PCN will be providing Customer Satisfaction Survey support, IPV6 Strategy Services, Service Desk staff, and technical/Project management staff to the project.
Harrisburg University Government Technology Institute	Harrisburg University is the first science- and technology-focused, non-profit, comprehensive university to be established in Pennsylvania in more than 100 years. Founded to address the Capital Region's need for increased educational opportunities in science, technology, engineering and mathematics (STEM) careers, Harrisburg University represents a major step to attract, educate, and retain Pennsylvania's diverse 21st century knowledge-based workforce. The University operates several applied centers which are a means of outreach and service to various industries. One of these centers is the Government Technology Institute (GTI), of which Unisys is a Founding Member. Harrisburg University will partner with Unisys Corporation in the delivery of training to Commonwealth of Pennsylvania. A Harrisburg University training coordinator will work closely with the Unisys project team to ensure that all training sessions are planned and delivered in a quality manner. For large training events, sessions will be hosted at the Harrisburg University campus in downtown Harrisburg. In addition, HU will record sessions which will be cataloged and made available for on-demand playback for Commonwealth personnel.

Figure 4-2 graphically represents the Unisys Team.

Figure 4-2. The Unisys Team

4.1.7 Experience and Services Relative to this RFP

Collectively, Unisys and IBM have the experience of hundreds of outsourced managed services implementations, many as large and complex as that of the Commonwealth. The outsourcing services performed by Unisys and IBM at the Commonwealth are great examples of our capabilities in state government. Beyond the Commonwealth, both companies have significant managed services experience in the public sector. For example, Unisys has provided managed outsourcing services to a number of public sector institutions, including the cities of Chicago, Minneapolis, and Santa Clara; California State University; the Metropolitan Police in London, England; the U.S. Department of Agriculture; and the State of Texas. IBM also has significant outsourcing services experience in the public sector providing outsourcing services to organizations such as the states of Georgia and Washington. Recently, IBM was awarded the opportunity from the State of Ohio, to modernize their State Computing Center (SOCC) and the development of a private cloud computing environment.

> ***Experience***
>
> *Where will other teams find all of the necessary experienced staff to support this project?*
>
> *This team will provide highly experienced and qualified candidates primarily sourced from our current local engagements leveraging unique Commonwealth knowledge.*

Also, many of the Fortune 500 corporate giants use our outsourcing services to support their domestic needs and use the global reach of Unisys and IBM to support the needs of the marketplace worldwide.

Likewise, Deloitte one of the world's largest professional services firms, brings knowledgeable and talented staff to this engagement. It also supports many other public sector organizations in addition to the important work it currently does for the Commonwealth.

For example, the State of South Carolina selected Deloitte & Touche LLP ("Deloitte) in March 2013 to assist with the implementation of their Information Security (INFOSEC) Program. The massive data breach that the State suffered in October 2012 and subsequent Governor level involvement in the remediation efforts led to the RFP to implement the INFOSEC program. The Deloitte team started work in March 2013 and the first major set of deliverables were completed on time and budget by May 1st, and included a publicly available report of the initial recommendations.

Beyond our security and managed services experience, our team of Unisys, IBM, and Deloitte, employs more than 638,000 IT professionals in a variety of disciplines, and have significant financial resources associated with more than $140 billion in annual revenue.

In Pennsylvania, Unisys, IBM, and Deloitte employ 6,962 people with more than 900 people in the Harrisburg area alone. That number of local resources not only brings growth and revenue to the Commonwealth, but also provides a wealth of local and very qualified resources to support this opportunity.

4.1.8 Team Qualifications

Unisys

Outsourcing Awards and Credentials

An example of the many Unisys qualifications is the fact that all industry evaluators generally recognize Unisys as a leading performer of Information Technology Outsourcing (ITO) and related services over an extensive period, as evidenced by the recognition and the ratings in **Figure 4-3**.

Figure 4-3. Unisys Outsourcing Awards and Credentials

As previously noted, this section is an introduction to our team and will focus primarily on our key partner's qualifications. The extensive list of other Unisys qualifications is highlighted throughout Section 4.2, Unisys Corporate Information, Section 4.3, Unisys Strategic Direction, and Section 4.4, Unisys Dedication to Quality.

IBM, Key Partner Qualifications

IBM Global Technology Services, part of IBM Global Services, is the largest business and information technology services organization in the world, generating $60.2 billion of revenue in 2011.

As it relates to this RFP, IBM Global Technology Services will provide the Services and has over 21 years of experience in the outsourcing marketplace.

IBM Certifications

An overview of industry-recognized certifications supported by IBM, and applicable to our solution are listed in **Table 4-2**.

Table 4-2. IBM Certifications

Certification	Date	Description	Focus Area
IBM Quality Standards and Frameworks			
ITIL	Since early 1980s	IBM is a funding sponsor, author, reviewer, developer and user of the IT Infrastructure Library. ISO 20000 is a standard for IT service management that enables compliance to ITIL requirements, and IBM holds multiple ISO 20000 certifications throughout the world. IBM as a whole has approximately 11,855 ITIL-certifications across all disciplines and serving multiple industries (as of 1/2/2013). Moreover, all delivery professionals are trained in ITIL compliance.	Best Practices Framework
Six Sigma Lean Sigma	1986 2005	IBM has a long history working with Six Sigma initiatives and has incorporated the defined processes for quality, process measurement and improvement in our IT services. Renewed focus of IBM Process Excellence effort and led to the establishment of their global delivery methodology.	Process Management Methodology
COBIT	–	IBM is a global sponsor of COBIT and offers products and services related to IT Governance and Controls Management that are based on this valuable set of internationally recognized best practices.	IT Governance Framework
PMI	–	IBM Project Managers are required to obtain PMI certification as part of their IBM career advancement.	Staged Maturity Model
IBM ISO Certifications			
ISO 9001:	Since 04/2001 Latest Renewal 12/2011	IBM Corporation, certificate # 82346	Quality Management
ISO 14001	Since 10/2003 Latest Renewal 02/2011	IBM Corporation, certificate # 48320	Environmental Management
ISO 20000	12/10	IBM holds multiple ISO 20000 and BS15000 certifications throughout the world. IBM also achieved ISO 20000 global certification at 18 of their global delivery centers in 22 locations IBM Corporation, certificate #10-02-00-00/ITMS/AD	Service Management/ ITIL Standards

IBM Awards

IBM has received a significant amount of recognition for their products, services, quality, customer satisfaction, and community involvement. Relevant to our solution, the recent notable examples include the following:

SAP

- 2012 SAP Pinnacle Awards
  - Technology Award: Global Technology Partner of the Year
  - Service Award: Transformational Award - Rapid Time to Value

For 40 years, IBM and SAP have helped clients formulate and execute winning strategies. Since the SAP Pinnacle Awards began in 2002, IBM has won 25 awards—more than any other SAP partner. Once again for 2012, IBM has been recognized as the Global Technology Partner of the Year in the annual SAP Pinnacle Awards. It is the second time in three years IBM has captured this coveted title for superior joint engagements to achieving client success enabled by innovative technology.

IBM Industry Analyst Awards

- **Gartner**
  - Gartner Inc. has positioned IBM as a Leader in the Magic Quadrant for Data Center Outsourcing and Infrastructure Utility Services, North America
  - IBM is positioned in the Leaders Quadrant of Gartner, Inc.'s Magic Quadrant for Help Desk Outsourcing, North America
  - IBM is positioned in the Leaders Quadrant of Gartner, Inc.'s Magic Quadrant for Desktop Outsourcing Services, North America
- **Forrester**
  - IBM was positioned as a leader in the Forrester Wave™: Global IT Infrastructure Outsourcing, Q1 2011
  - Information Security Consulting Services, Q1 2011.

Deloitte, Key Partner Qualifications

As it relates to this RFP, Deloitte will bring professionals from Deloitte Consulting LLP and Deloitte & Touche LLP – collectively referred to as "Deloitte", to provide technology and information security services respectively.

Deloitte has nearly 51,000 professionals in 89 U.S. cities, and is one of the largest professional services firms in the United States. Deloitte's portfolio of clients includes many of the nation's largest and most prominent organizations in every sector of the economy.

Deloitte Certifications

Deloitte not only encourages and supports their practitioners obtaining relevant security certifications, but require relevant certifications as a prerequisite for the growth of their practitioners in their firm. Their emphasis on the certifications has enabled Deloitte to be the leading provider of security services with more than 1,000 certified security professionals. This is the largest pool of certified security professionals in the country, including

- More than 700 professionals with the Certified Information Security Services Professional (CISSP) certification
- More than 120 Certified Information Privacy Professionals (CIPP)
- More than 800 professionals with the Certified Information Security Auditor (CISA)/Certified Information Security Manager (CISM) certification.

Deloitte Awards

Deloitte has received a significant amount of recognition for their services, quality, customer satisfaction, and community involvement. Relevant to our solution, the recent notable examples include the following:

SAP

- SAP Pinnacle Quality Award Partner of the Year
- SAP North America Partner Excellence Award: Top Services Partner – Strategic Industries
- SAP Pinnacle Award for Analytics Impact: includes BI, GRC and Financials

Oracle

- Oracle Excellence Awards for Specialized Partner of the Year-North America: Global SI Applications Momentum

CA Technologies

- Security Partner of the Year

Deloitte Industry Analyst Awards

- **Forrester Research**
  - Deloitte named a leader in information security, and receives high marks for client focus and mature offering by Forrester Research, Forrester Wave ™: Information Security Consulting Services Q1 2013", Ed Ferrara and Andrew Rose, February 1, 2013
  - "Deloitte shines when tackling large-scale challenges at mature, complex organizations. Customers facing such issues and looking for a vendor that will marry deep technical capabilities with strong business processes should look to Deloitte."

- "Deloitte maintained its position in the Leaders category thanks to exceptional client feedback and comprehensive, sophisticated, and mature service offerings, with notable strengths in BC/DR and network strategy and design."

- **Gartner**
  - Based on Gartner estimates, Deloitte is the world's largest IT consulting firm, as well as the largest security consulting services firm.
  - The company has established solid branding around its Center for Security & Privacy Solutions, which helps it engage and brand itself with corporate clients.
  - One reason Deloitte succeeds against the four other top firms is that its global delivery network is the largest and most mature compared with those firms.

  Source: Gartner Research: Market Share Analysis: Security Consulting, Worldwide, 2012

4.1.9 Service Levels

The best example of our team's future ability to meet the very demanding service levels required in this RFP is to review our past performance at the DPH. To put it simply —**we are exceeding all service levels and have done so for the last 14 years. Our level of service received an overall average of 8.8 (on a scale of 1 to 10) in the most recent Commonwealth agency survey conducted in October 2012**. Our DPH record speaks volumes about our future performance.

We recognize the need for revised processes and tools to support new, more demanding service levels. Our solution includes the necessary tools, processes, and training to provide the service levels requested.

4.1.10 Quality of Comparable Services

As shown in **Figure 4-4**, Unisys IT services and clients reach across all industries including a large number of Public Sector Clients similar to the scope and size of this RFP. Additional detail on Unisys and our team's quality of comparable services are found throughout this entire section.

Market	Scope	Rationale	Sample Clients
Large Global Organizations	Multi-Sourcing or Selective Sourcing Environments >$75 million Total Contract Value (TCV)	• Provides best-in-class end user services that enable common global processes and tools • Leverage global capabilities and global footprint for data centers • Recent wins validated competitiveness	• Microsoft • UnitedHealth Group • American Red Cross • Eli Lilly • Starbucks
Mid-Cap Multi-Nationals	Full Scope – enterprise computing, applications support, end user services, application outsourcing, Mobile device support $20 to $75 million TCV	• Enables clients to drive common global processes and controls in their organization • Leverage full-line capabilities of Unisys	• Ameriprise • Piper Jaffray • Quest Diagnostics • BlackRock • Imation • 7-Eleven/NEC • Flowserve
Tier 1 Nationals/ Public Sector	Full Scope – enterprise computing, application support, end user services $10 to $1.5 billion TCV	• Leverage brand recognition in key markets • Provides *national* clients with benefits of *global* solutions and best practices • Leverage full-line capabilities of Unisys	• Commonwealth of Pennsylvania • County of Los Angeles • US Federal GSA Catalog • Internal Revenue Service • City of Minneapolis • Defense Information Systems Agency • London Metropolitan Police • California State University System • Texas Workforce Commission
OEMs (PLS)	Global End User Services $75 million TCV	• Provides best-in-class end user services that enable common global processes and tools • Leverage global capabilities and footprint • Recent global wins validate competitiveness	• Dell • Lenovo • Alcatel Lucent • BT

Figure 4-4. Unisys Primary Industries and Markets Served are Similar to the Commonwealth of Pennsylvania's Compute Services Requirements

4.1.11 References and Length of Service

Please see the Client References in Section 4.5 for additional information on Unisys and our team's references and length of services provided to like clients.

This page intentionally left blank.

4.2 Unisys Corporate Information

RFP	*Requirement*
	Corporate Information *The Offeror must provide a narrative describing its background, history, services, and corporate organization. A general overview of the corporate organization is appropriate. If the Offeror is a subsidiary or division of a larger company, this section should concentrate on the operating history of the subsidiary or division which will provide the Services.*

4.2.1 History and Background

In addition to our extensive experience with supporting the Commonwealth's IT infrastructure on our DPH and EDC engagements, Unisys has had a formative role in the IT industry and has a broad base of experience relevant to the Commonwealth of Pennsylvania and the RFP requirements.

Unisys has been a technology leader for more than 140 years. Our predecessor companies include Burroughs—inventors of the world's first commercial calculator, and Sperry—famous for its document retrieval machines, gyroscopes, and ENIAC—the world's first commercially available computer system and first with core memory, virtual memory, and multiprocessing system—are among our other innovations. ENIAC's roots are traced to the University of Pennsylvania, where it was designed in the 1940s. For decades Unisys "wrote the code" for airline reservations systems and check processing. Since the 1990s, we transformed to become services led. More than 85 percent of our current revenue is from services (Refer to **Figure 4-5**).

With precision thinking and relentless execution, our more than 22,000 employees drive our clients' business visions forward. We help thousands of clients in more than 100 countries quickly and efficiently achieve success by delivering the right solutions backed by the right technology. Unisys staff integrate and deliver the solutions, services, platforms, and network infrastructure governments and businesses require to transform their organizations for success in this new era.

4.2.2 Current Services

Unisys provides solutions to 50,000 clients around the world. In 2012, our personnel achieved total worldwide revenue of $3.71 billion attributable to a portfolio of services, systems, and support, helping clients manage information for tangible business results. Of the more than 22,000 employees at Unisys, about 14,000 are in technical delivery roles. Our success is built on combining technical expertise with an in-depth knowledge of the

industry trends and business challenges facing clients. Additionally, we draw upon the resources of an extensive network of third-party alliances. Service and solution delivery that helps clients apply and support technology to improve their business performance accounts for more than 80 percent of Unisys revenue today.

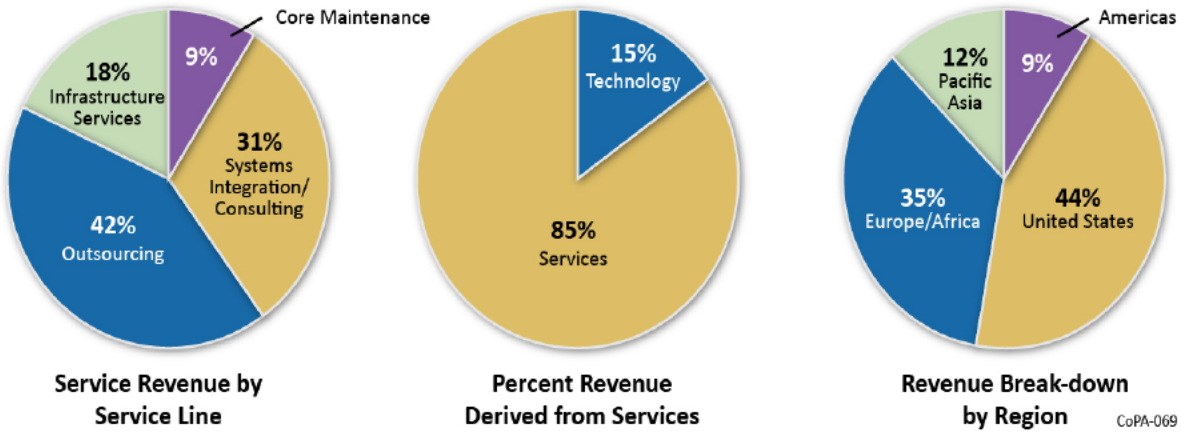


Figure 4-5. Unisys Revenue

4.2.3 Client Focus

As previously stated, this engagement is personal to Unisys since we are a Pennsylvania-based company. It is one reason we have worked so hard when awarded Commonwealth contracts.

We believe deeply that our clients must become our partners. We strengthen our client relationships by doing whatever is necessary to meet their high expectations. This is not only a belief, but applies to our many engagements.

As demonstrated with our joint DPH project, Unisys develops true partnerships with our clients, enabling us to align with each client's culture and business objectives. We complement each client's core business with an IT support structure that promotes excellence and flexibility.

The Unisys business strategy is built on our strength in delivering secure, mission-critical IT operations with a particular focus on areas that are strategic to our clients, such as data center outsourcing operations.

4.2.4 Services, Global Outsourcing is a Unisys Key Strategy

Globally, Unisys is a leader in the IT infrastructure support and managed services market, as evidenced by consistent recognition from independent third party consultants such as Gartner, Forrester, and the Black Book of Outsourcing.

Unisys has deep expertise in outsourcing and provides a wide range of infrastructure services to clients **Figure 4-6** provides a "selected client" summary and evolution graphic that gives an overview of Unisys' outsourcing relationships. This client overview emphasizes our outsourcing approach and represents a client selection with a variety of industry backgrounds, enterprise sizes, and regions. It also shows our commitment to Global Outsourcing Services.

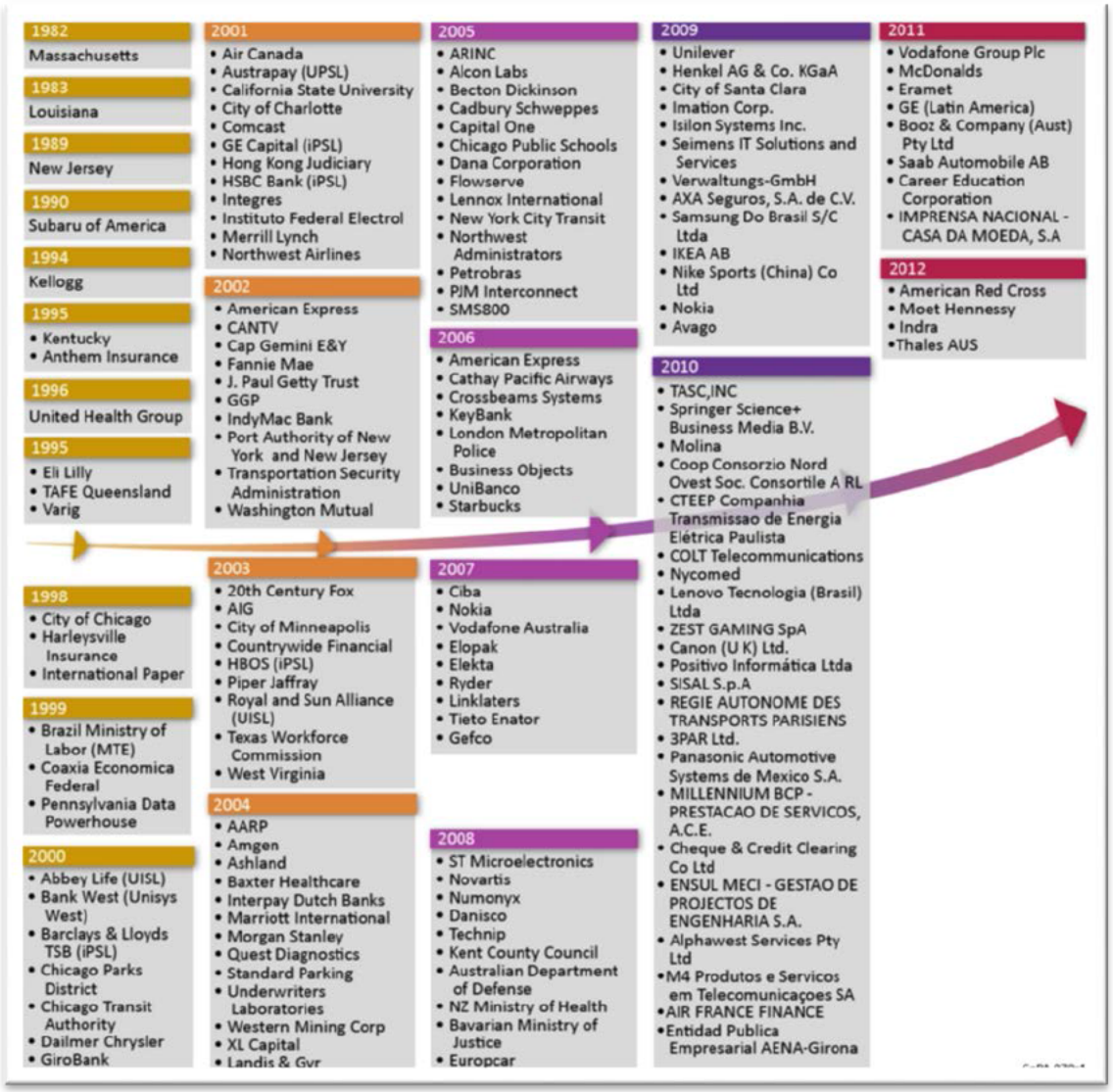


Figure 4-6. Selected Client List

4.2.5 Global Footprint

Our strategy includes the ability to deliver cost-efficient, high quality, and state-of-the art IT outsourcing services. Unisys implemented global sourcing capabilities not just in the United States, but also in Eastern Europe, China, India, South America, and New Zealand.

All services to meet the requirements for the Commonwealth will be hosted and provided from within the United States

Unisys has made strategic investments in system infrastructure, processes, tools, training, and people to build our global delivery model. **Figure 4-7** represents some of our corporate domestic, near shore, and offshore resource strengths in the areas of data center footprints

Figure 4-7. Global Services Footprint

For worldwide volumes, global reach, and market position for services delivered similar to the Commonwealth of Pennsylvania, please see **Figure 4-8**.

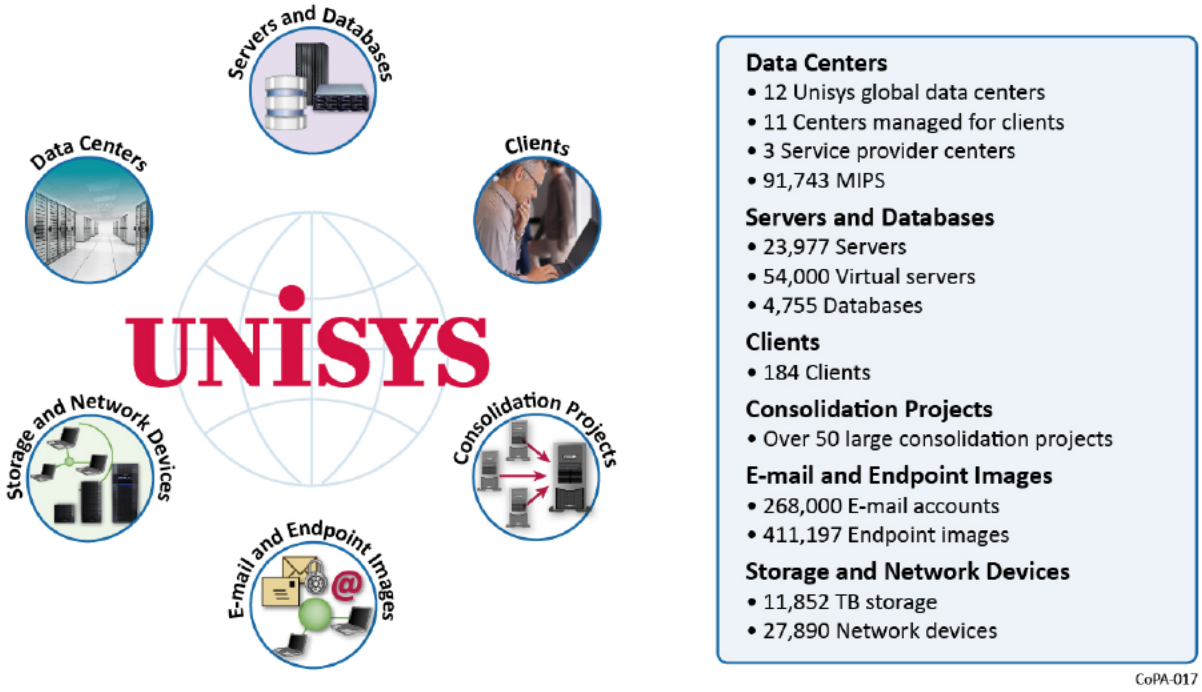


Figure 4-8. Global Services and Worldwide Volumes

4.2.6 Technology Agnostic and Committed to Strategic Partnerships

In addition to our strategic technology partnership with IBM, Unisys maintains strategic alliances with technology front-runners, including Dell, EMC, Intel, Microsoft, Oracle, and VCE, as reflected **in Figure 4-9**.

Figure 4-9. Global Alliances

Strong alliances with industry-leading companies allow Unisys to move quickly and confidently across a full range of advanced services and technologies, allowing our clients to achieve exceptional performance, control costs, have competitive advantage, and effectively manage risk. Strong alliances are instrumental to our ability to deliver solutions for secure business operations. We focus on alliances with proven success to help meet our clients' specific needs.

Unisys plays a leadership role in various market segments, in setting industry standards, and in charting the direction of industry practices and technology. Many of our employees participate in industry standards groups.

4.2.7 Corporate Organization

Demonstrating our commitment to the Commonwealth of Pennsylvania, Mr. Ed Coleman, Unisys Chairman and CEO is the Executive Sponsor of this engagement. Mr. Coleman will personally promote our company's complete commitment to the project's success. Our corporate organization is shown in **Figure 4-10**.

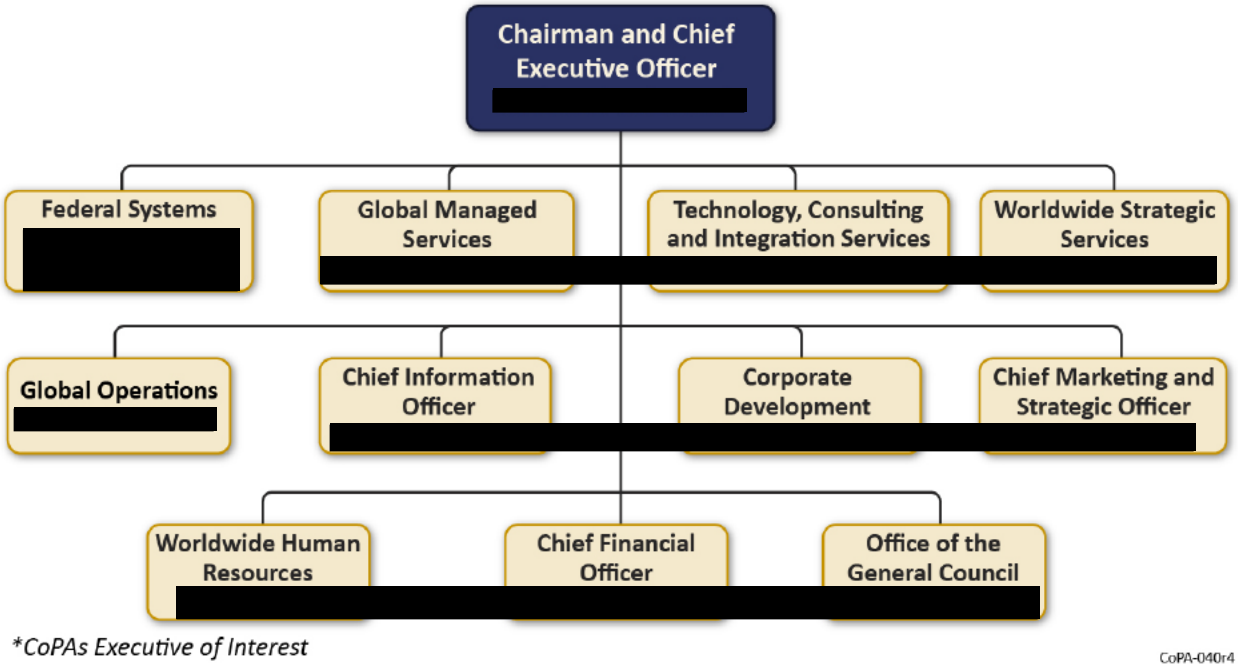


Figure 4-10. Unisys Executive Committee

Executive Leadership Committee

In addition to Ed Coleman's role as Executive Sponsor Unisys has established an Executive Leadership Committee to support the efforts of the Harrisburg-based leadership team. This committee consists of very senior Service Delivery Executives from Unisys, IBM, and Deloitte. This Executive Leadership Committee has been established to provide direct project visibility into the Corporate Executives at all three firms to make sure we meet our commitments to the Commonwealth, during both transition and steady state operations. The committee will also be leveraged to resolve any significant issues during the engagement. This committee will also be part of the formal transition and steady-state governance model that is implemented for this engagement. **Figure 4-11** identifies the members of the Executive Committee.

Figure 4-11. Unisys Executive Leadership Committee

4.3 Unisys Strategic Direction

RFP	*Requirement*
	Strategic Direction *The Commonwealth places strong emphasis on the need for a long-term strategy. The Offeror should describe its strategic direction, and the implications of that strategy for the Commonwealth.*

4.3.1 Unisys Corporate Mission

Unisys is a global information technology service delivery company whose purpose is to deliver mission-critical IT solutions and services that solve our clients' most demanding IT challenges, such as those being delivered by Unisys and our team to the Commonwealth for the past 14 years at the DPH. We differentiate ourselves by the topmost levels of high-quality service and measure success by our customer satisfaction.

Our software, services, and technology offerings are designed from the ground up to operate in the most critical environments, and cost effectively exceed the reliability, scalability, and security requirements needed to achieve our clients' strategic missions.

We define "mission critical" as secure, reliable, scalable computing and processing environments that support our clients' "front office" (i.e., activities that directly impact our clients' customers).

Key Elements of Our Mission

- *Mission-Critical Computing Focus*
- *Delivery Quality is our first priority*
- *Success measured by the highest degree of Customer Satisfaction*

Our mission and the mission of the Commonwealth are clearly aligned. The Commonwealth's "front office" is the 12.6 million citizens who depend on "mission critical services" delivered by the technology and infrastructure in scope of this procurement's scope. The Commonwealth's commitment to deliver these services in a secure, reliable, scalable, and efficient way has been and will remain our commitment as well.

To meet these requirements we are dedicated to six key principles of service delivery designed to make sure our solutions adapt and deliver against the most difficult client challenges and deliver the highest customer satisfaction.

Our six key principles of service delivery are:

1. **First and foremost,** we use our deep, longstanding technical expertise to engineer **mission-critical capabilities** into every market offering.

2. **Second,** we establish a **culture of collaboration**: both externally with our clients and internally at Unisys.

3. **Third,** we engineer consistency into our global service delivery organization, ensuring best practices are propagated quickly, and drive the most **cost effective solution delivery** approach.

4. **Fourth,** we continuously invest in skills to maintain our mission-critical edge; and apply those skills effectively ensuring **global accessibility**.

5. **Fifth,** our innovation focus is to invest heavily to rapidly bring **disruptive technologies** into our portfolio and to our clients through our **continuous innovation** processes

6. **Last and most critically,** we never lose the focus on our existing **clients and their priorities.** We measure our success by the highest **customer satisfaction**.

4.3.2 Corporate Strategy

Our strategy is centered on delivering mission critical solutions in four areas of our clients' IT operations: security infrastructure; data center transformation and outsourcing; end user outsourcing and support; and application modernization and outsourcing.

Our deep knowledge and decades of experience in each of these areas directly and favorably influences the services we deliver to the Commonwealth. The requisites for a secure infrastructure, an understanding of the end user experience and expertise in application performance in a multiple-platform environment are integrated into the services we currently provide to the Commonwealth. Data center transformation is a welcomed addition and something strongly supported by our corporate strategy.

We are highly attuned to a range of IT trends that affect our clients' business and provide opportunities for innovation in how we deliver those solutions. Disruptive IT trends of focus include cloud computing, cyber security, consumerization of IT, mobility, big data, and smart computing, social computing, and IT appliances. These emerging technologies offer many important advantages to our clients. Through collaboration, we will determine which of these technologies will work best and help implement them. Our strategy, related to these disruptive technologies, is to invest and integrate them into the solutions with our four areas of strength to make sure our clients benefit from the latest technology and Unisys intellectual property.

Our Four Areas of Strength

Unisys is a worldwide, world-class services and solutions provider that prides itself on its collaborative approach, inventive solutions, and committed people (**Figure 4-12**). We know the world is changing rapidly—from the consumerization of IT to the convergence of physical and IT security—and it is important that we choose to focus on areas that best address the changing marketplace and our clients' most mission-critical needs.

Figure 4-12. Unisys Areas of Strength and Innovation Focus on Disruptive Trends

Data Center Transformation and Outsourcing—Our standard Data Center solutions enable our clients to update their operations to meet the ever-increasing demands for increased efficiency. We help optimize infrastructure through virtualization techniques. We build and deploy secure, scalable, reliable computing platforms. We help clients think through and implement outsourcing computing requirements, which may or may not include a private or public "Cloud". With our practical engineering expertise, we remove the mystery of the "Cloud" and focus instead on solving business issues. Our heritage in the data center combined with our independent thinking, innovative infrastructure and sourcing capabilities deliver solutions that are more secure, more productive, and more reliable. Our corporate focus and strength in Data Center Outsourcing and distinctive Pennsylvania outsourcing experience, uniquely qualifies Unisys for this opportunity.

Security—Security is an integral part of an IT infrastructure. Our offerings are designed to secure people, assets, systems and data for governments and businesses with no room for

error. We integrate physical and digital security technology. Our solutions protect borders, airports, data centers, financial information and classified data and are integral to many national defense systems. Security is in our DNA and permeates our extensive experience with defense, security, and law enforcement agencies around the world. From creating biometrically enabled national ID cards and sophisticated border control systems to developing national police command and control systems and cyber security operations solutions — we provide mission critical security solutions globally. We will leverage this corporate strength in security to protect the Commonwealth's valuable assets.

Application Modernization and Outsourcing—The application layer in many ways is the core of most mission-critical applications. We deliver industry-specific systems for governments and the financial, transportation and telecommunications sectors using our engineering experience to help our clients modernize their applications. This may involve rewriting applications in a more modern language, creating new features and functions, or integrating various applications into a whole to achieve the desired business outcome. Unisys has more than 30 years of application modernization and outsourcing experience across most industries and government sectors, including 200 million voicemail users worldwide, 600 airports, 22 of the top 25 banks, and 1,500 government agencies. Combining our corporate focus on application modernization with our local application knowledge of key agencies business systems again uniquely qualifies Unisys for this outsourcing initiative.

Unisys Application Modernization and Outsourcing Services (AMOS) enable clients to regain control of their application suite. Historically, enterprises built and integrated their applications in silos. Today, it is cost-prohibitive to maintain them, and the employees who have the knowledge to do so are retiring. In a time of limited resources and global economic pressures, our capabilities extend the life of our clients' current assets, enhancing our clients' productivity and competitive position by modernizing and outsourcing their mission-critical applications.

End User Outsourcing and Support Services—Our services provide anywhere, anytime support for our clients' end users with a one-call global model that increases user satisfaction while driving down support costs. With the rapid increase of knowledge workers, and the fundamental dependency on laptops and mobile devices, providing service to end users takes on a level of importance rising to mission critical. Our services, tools, and methods are designed to support the global enterprise 24 hours a day, 7 days a week with the perfect mix of remote and onsite services designed to keep our clients' operations running. We are differentiated by our ability to leverage the combination of our global ITIL-based Resolution Optimization Model, network of 31 ITO Operations Centers, and 6,000-person strong field force to deliver measurable cost reductions, improved satisfaction levels and faster time to incident resolution.

In summary, we add value to our clients as a "mission-critical" IT solutions provider focused in our four areas of strength, based on a strategy rooted in our traditional engineering expertise, practical innovations and continuous improvement of our service delivery efficiencies. Throughout our history, one constant has remained true—our dedication to delivering mission-critical IT products and services.

4.3.3 Innovation

Our Approach to Continuous Innovation with Our Clients

Though many of our competitors provide informal, disconnected innovation tools and approaches, the Unisys Strategic Innovation Program provides a systematic, cohesive, globally coordinated program. We deliver innovative ideas, solutions, and outcomes for our clients, leveraging a highly structured, yet flexible approach. We will leverage our corporation approach to improve continuous innovation through our dedicated continuous innovation project office assigned to this major initiative.

Three Tenets of our Innovation Approach

- *Identification of key disruptive technologies and trends*
- *Investment and integration into our Portfolio Areas of Strength*
- *"Continuous Innovation" approach to deliver innovation to customers*

Key elements of our innovation approach include identification of the latest disruptive technologies and trends that have strategic benefit to our clients, investing to integrate them into our four portfolio Areas of Strength, and then delivering "continuous innovation" with our clients via our programmatic approach, including our highly collaborative Innovation Workshops.

Transformation with Disruptive Technology Trends

Disruptive technology trends are those that have the potential to rapidly disrupt "business as usual" through compelling combinations of cost improvement, enhanced productivity, and new business capabilities. They provide the opportunity for transformational change (i.e. "*faster-better-cheaper*"), which alters the IT delivery model.

Unisys is investing in technologies around six key disruptive IT trends: cloud computing, mobile computing, social computing, big data, IT appliances, and cyber security, as reflected in **Figure 4-13**.

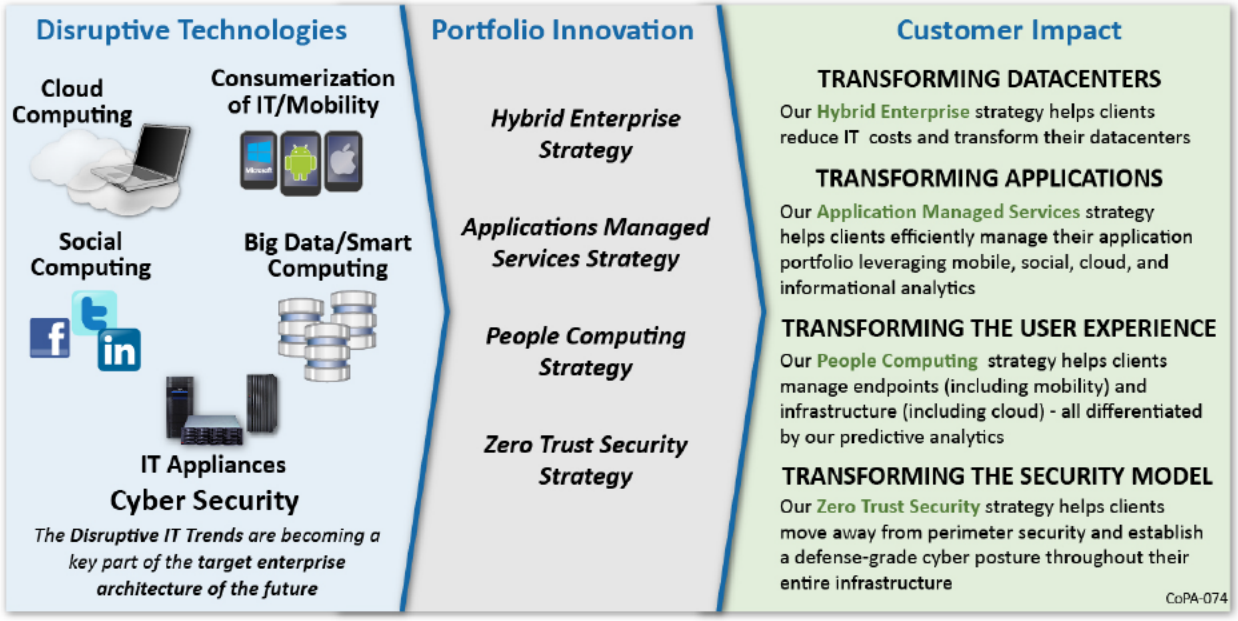


Figure 4-13. Our innovation with the Disruptive Trends is focused on helping clients transform their data centers, applications, and the user experience.

These trends are creating new opportunities for IT to deliver business value and increased productivity through new styles of interaction, automation, and service delivery.

Beyond the individual trends, the seamless "combination" of these trends is becoming ever more critical because it represents an agile new IT fabric for applications, data centers and, most important, the user experience. Mobile and social-enabled applications, deployed from the cloud, with superior information analytics are now the target architecture of the future. Cyber security is critical across all elements. The question is how to achieve this transformation on a production scale across their entire IT architecture.

The Unisys strategy aims to address this client challenge by innovating with the disruptive trends across our four areas of strength — addressing the user experience, applications, and the data center in a holistic manner — and helping our clients move to this desired end state IT architecture of the future.

Innovation in our Portfolio

*A key part of the Unisys strategy is to bring the industry innovation occurring within the **Disruptive Trends** into our **four portfolio areas of strength**. This ensures our clients gain the **operational benefits** of our mission-critical computing focus coupled with the **transformational benefits** of the next generation IT architecture represented by these trends.*

- **Transforming the User Experience** – Our innovation related to **mobility** helps clients transform the end user experience for their constituents, support Bring-Your-Own-Device (BYOD) initiatives driven by the consumerization of IT, and manage this heterogeneous environment across all end points. Our portfolio innovation related to **big data** and **predictive analytics** helps to detect potential issues before they occur and identify opportunity areas for improvement in enterprise service management.
- **Transforming Applications** – Our innovation focus is to help clients modernize their enterprise applications, not just for Web and mobile enablement, but to embrace the collaborative benefits of **social business** platforms and the economic and agility benefits of **cloud development and delivery** from software-as-a-service.
- **Transforming the Data Center** – Our innovation related to **cloud computing** and **cyber security** helps clients move to the desirable end state of the data center of the future, where application deployment options span from public cloud, to internal and hosted private cloud, to traditional and outsourced models, all managed and governed seamlessly in a highly virtualized and secure environment.

Key Unisys Investments for Transforming the Data Center

We clearly understand that an important intent of the RFP is transforming the Commonwealth's traditional data center approach to one that maximizes the latest in technologies, processes and knowledge gained from supporting global IT organizations and operations. Our commitment is to focus all of our knowledge and resources on moving the Commonwealth to a higher level of performance and expanded on-demand service offerings. Also, our corporate strategy will continue to invest in those on-demand service activities to keep the Commonwealth current with industry best practices. Some key areas of investment are as outlined below.

Future IT architecture transformation must occur at the user experience and application level and also designed into the data center of the future. Efficient management of the future data center must occur across all application deployment options from public cloud, to hosted internal-private cloud, to traditional and outsourced environments. On-Demand, **smart computing** and **intelligent analytics** will be increasingly used to optimize data center resources including placement of applications and workloads (e.g. public cloud or private cloud), policy-based optimization (e.g. business rules for decisions related to virtual

machines and cloud service brokering), and management of physical variables such as space, power and cooling.

The key disruptive technologies converging in the data center will clearly be **cloud, cyber security**, and **big data analytics** with **mobile-** and **social-enabled** applications either hosted in the data center or delivered from the cloud. Cloud-based software development will become increasingly important to free developers from tedious infrastructure procurement and setup, thereby reducing cycle times and allowing more time for creative development related to compelling new business models and user experiences. **Cyber Security** will be increasingly important in the data center because of its continued virtualization (e.g. software defined data centers) and highly distributed nature.

In light of our vision for the target enterprise, IT architecture and data center of the future, some of the key Unisys investments in our Data Center Transformation and Outsourcing portfolio include the following initiatives. These corporate investments will bring innovation and cost efficiencies to the Commonwealth:

- **Hybrid Enterprise –** Our investments in **cloud** help clients transform their data centers to support and seamlessly manage all traditional, outsourced and cloud deployment environments from a unified service view.
- **Platform Innovation** – Our investments in **next generation mission-critical computing** provide clients with a game-changing approach to supporting mission-critical workloads on highly cost-effective, industry-standard Xeon processors with support for Windows and Linux operating systems. Also, as part of our platform strategy, we are investing in **big data analytics** with support for Apache Hadoop to allow our clients to identify patterns and insights for competitive advantage from their massive amounts of data.
- **Service Management** – Our investments in **intelligent analytics** allow us to optimize enterprise service management delivery for our clients using predictive analytics from Lean Six Sigma methods to identify opportunities for improvement.
- **Cyber Security** - Our investments in **cyber security** help clients confirm their sensitive data is protected in and across their data centers with industry-leading, military-grade data protection solutions to provide data encryption for regional isolation and targeted communities of interest.
- **Big Data & Intelligent Analytics** – Our investments in **big data readiness** help clients prepare their information infrastructures with solutions that support automated storage resource analysis and optimization. Equally, big data extends to IT Service Management to bring unstructured service data from multiple processes into a structure view to identified continuous improvement efforts to optimize the IT operating environment.
- **IT Appliances** – Our investments in **IT appliances** help clients rapidly deploy highly-optimized functions such as Web and mobile extensions to their enterprise applications.

"Continuous Innovation" with our Clients

In order to optimize performance for the Commonwealth there needs to be an ongoing program of improvement. We developed and used a methodology that has worked well for our clients and we propose its use with the Commonwealth. The premise is collaboration and we know from experience that the Commonwealth wants to actively participate in bringing positive change to its data center operations. The RFP is evidence of the Commonwealth's intention for improved data center performance. Therefore, this process for continual improvement should be highly effective when adopted by the Commonwealth.

Rather than an ad hoc compilation of capabilities, tools and methods, our Strategic Innovation Program provides Unisys with a continuous and systematic way to deliver innovative outcomes for our clients leveraging a highly structured, yet flexible approach. Two key elements include our Continuous Service Improvement and Innovation Program (CSIIP) and Innovation Workshops (**Figure 4-14**).

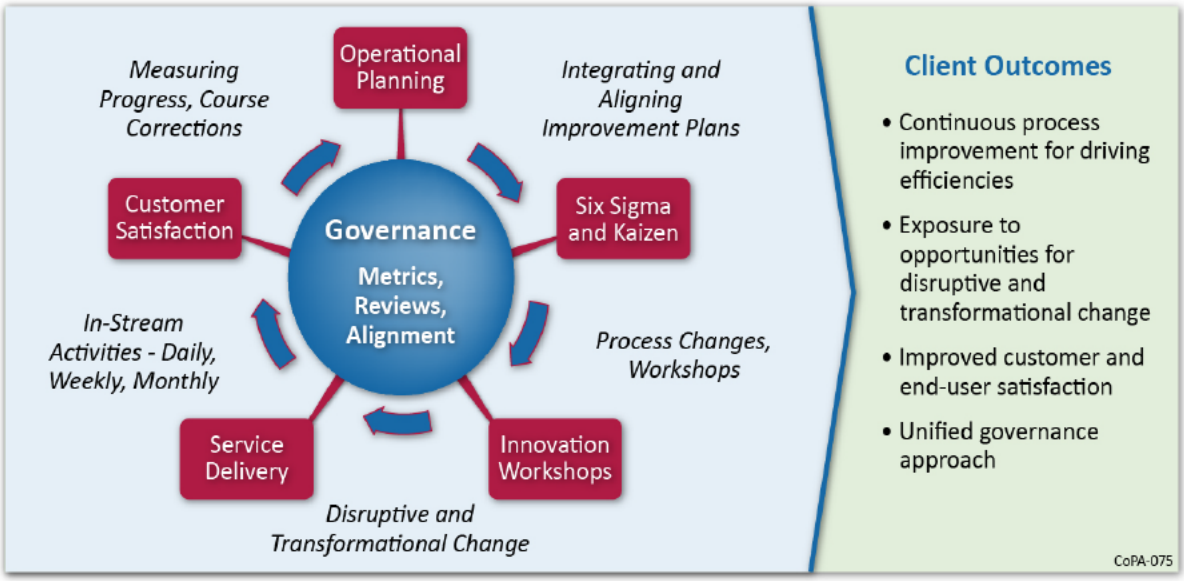


Figure 4-14. Continual Service Improvement and Innovation Program (CSIIP)

CSIIP encourages the proactive identification and introduction of measurable improvements in a specific work area and introduces "innovation in context" to those areas. Our well-defined methodology is an outcome of our Six Sigma Lean practice and supported by a trained team of Black Belts. These resources assist our clients to create a single structure for collaboratively managing issues, opportunities, and subsequent improvement programs.

One of the major features of our CSIIP program is the ability to consolidate and analyze the many inputs required for effective development of an innovation and improvement plan. This provides our clients with the necessary information to make informed decisions based

on relative cost/benefit, alignment with strategy and ROI for various actions, of varying scale from incremental through to truly "breakthrough" initiatives.

Unisys Innovation Workshops are a key part of our "continuous innovation" approach with clients and truly differentiate us as a highly collaborative and trusted advisor. These workshops are internal, client-facing workshops that focus on innovation identification, categorization, and prioritization of innovation opportunities and then the development of high-level business cases and implementation roadmaps for the most promising opportunities identified. We use a global pool of trained facilitators and conduct workshops across a wide range of industry verticals in North America, Latin America, Europe, and Asia Pacific.

Innovation Workshops

Unisys Innovation Workshops are collaborative workshops with our clients designed to explore opportunities for disruptive and transformational change. We expose our clients to the latest disruptive technologies and trends and collaboratively examine opportunities for strategic business benefit.

4.3.4 Hybrid Enterprise – Building the Data Center of the Future

The Hybrid Enterprise is our strategy by which we leverage cloud computing, IT appliances, big data/analytics, and cyber security in our portfolio to enable clients to transform their data centers from a traditional service model to a ***hybrid service oriented organization*** *based on a new utility model that balances costs, service and agility.*

We differentiate with our Integrated Service Management environment for complete visibility, control and accountability across all assets, creating a unified service view to the business.

Cloud computing enables the agility required by organizations to be leaders in today's dynamic economic conditions. It is accelerating time to market for new products and services while reducing costs to design, build, deploy, and support them. The past couple of years have proven that the properties of clouds – elasticity, pay-per-use, standardization, and automation – enable cloud providers and users alike to benefit from economies of scale, faster provisioning times, and reduced runtime costs. The Commonwealth's vision for the future data center aligns very closely with the Unisys Hybrid Enterprise strategy. This alignment will facilitate an improved transformation to the Commonwealth new data center model.

The Hybrid Enterprise is the Unisys approach to transforming the Data Center

Because enterprise IT workloads have highly varying requirements—some suited to cloud, others to traditional deployments in the data center and outsourced—Unisys believes that the data center of the future will need to operate not solely in a cloud model or in a model comprised of multiple cloud entities (hybrid cloud), but in a Hybrid Enterprise model. This hybrid model consists of internal and external infrastructure—some deployed as clouds and others more traditionally operated with a mix of general-purpose and specialized functions.

Our corporate strategy for the Hybrid Enterprise will provide the most flexibility to the Commonwealth as we move forward together.

Unisys Vision for the Hybrid Enterprise

Like the Commonwealth's vision for new compute services, Unisys believes that the data center environment will gradually transform to a virtual data center with no boundaries where IT organizations will manage aggregated virtual capacity and not islands of technology. In general, the data center will transition from a supplier-driven model to a service provider relationship model in which IT is managed in a holistic capacity model driven by attributes such as self-service automation, automated capacity provisioning, service catalogs, and other orchestration tools and processes.

These end states of virtualized data center environments are agile, flexible, and cost-effective and will have the ability to scale up or down according to business demands. Also, organizations will effectively manage the various environments in this virtualized data center, leveraging the Unisys Hybrid Enterprise framework, tools, and processes.

Key Attributes of the Data Center of the Future

- *Highly-virtualized and automated to maximize efficiency*
- *Service oriented*
- *Utility model balances costs, service and agility*
- *Mission-critical security*
- *Seamless management for visibility, control and accountability across all environments*

The Unisys Hybrid Enterprise framework (**Figure 4-15)** is a composition of cloud, non-cloud, internal and external IT service delivery models, that remain unique entities. These entities are bound together by an integrated service management environment, common technology, processes, and policies that optimize agility, enable data and application portability, and reduce risk. Hybrid Enterprise is a holistic approach to transform the data center from a traditional service model to a **hybrid service oriented organization** based on a new utility model that balances costs, service and agility.

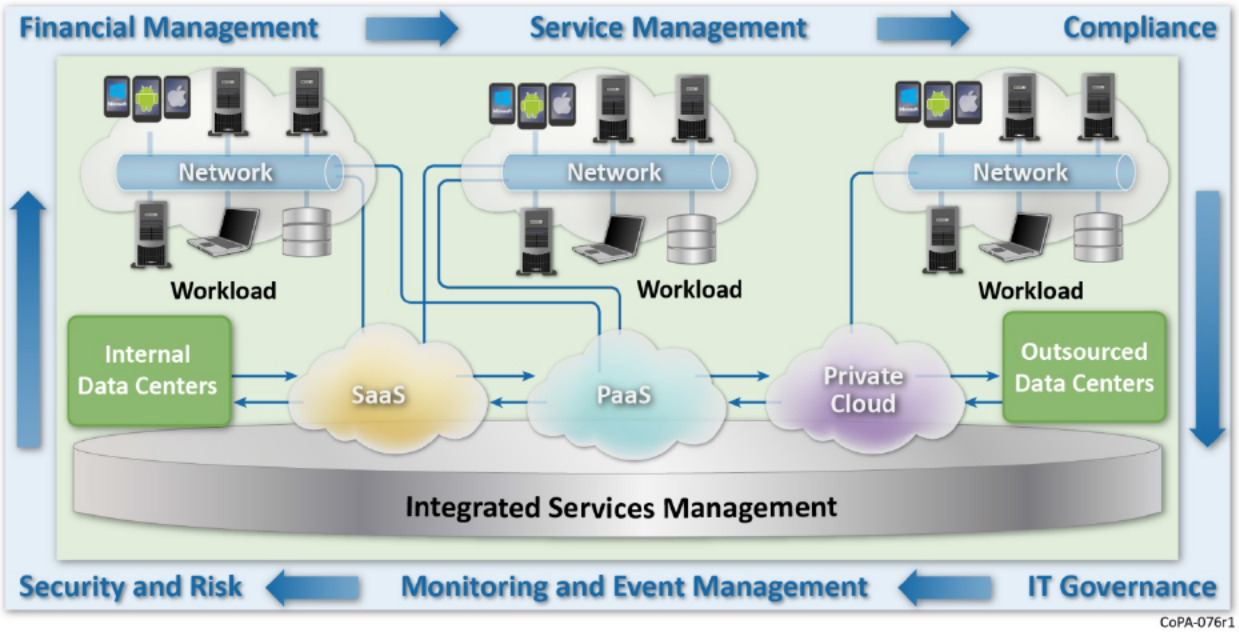


Figure 4-15. Unisys Vision for the Hybrid Enterprise. *An integrated single service view encompassing traditional, cloud, internal, and external IT service delivery models that is borderless, virtual, automated and secure.*

Unisys Hybrid Enterprise Strategy – Addressing Applications, Data Centers, and Management

The Hybrid Enterprise strategy comprehensively addresses strategic considerations across applications, data centers, and management. In this framework, a workload placement decision model is required to characterize applications and drive placement decisions so workloads can run on the optimal infrastructure. A consistent approach is required for building and evaluating data center characteristics, one that meshes with the application demands and optimizes the data center footprint across cloud and non-cloud delivery models while minimizing complexity. Finally, a single unified management environment is required that provides a set of controls to manage governance, risk, compliance, services and costs across all infrastructure types.

To this end, our Hybrid Enterprise strategy focuses on three core areas of the Commonwealth's IT operations:

- **Applications** – We apply a formalized "fit-for-purpose" approach to confirm that workloads – mission-critical and otherwise – are analyzed and placed in the most appropriate environments (i.e. public cloud, private cloud, hybrid cloud, and traditional IT, etc.). The goal is to balance the workloads and maintain optimal performance.
- **Data Centers** – Our consistent methodology and tools for building and evaluating data center characteristics integrates with application modeling processes and optimizes the data center footprint across delivery models—minimizing complexity without compromising processes. These tools and methodology help automate and

self-provision our clients' infrastructure consisting of various environments, including private, public, hybrid cloud and traditional IT.

- **Management** – We employ a comprehensive approach that unifies the management of the virtual data center with a mix of environments and consistently addresses key process areas for all traditional and cloud delivery models. The key attributes of this unified management capability include features such as seamless and integrated monitoring, event management, service management, financial management and compliance.

To help maximize the value of the Hybrid Enterprise, we work closely with our clients to establish a roadmap tailored to their organization's specific business needs and desired outcomes. We bolster this approach with a perspective that manages the cloud transformation across people, processes, policies, and technologies – enabling our clients to confidently maintain control, manage governance and compliance, reduce IT costs, and address both current and emerging operational requirements.

Accelerating the Journey to the Hybrid Enterprise

Our data center strategy allows clients to enter the journey to the Hybrid Enterprise at any point in their life cycle according to their specific business needs. Typical starting points for CIOs are outlined below and supported by our unique set of services across applications, data centers, and management:

Applications

- **Application Alignment** – We create an actionable plan that efficiently migrates workloads to an optimal delivery model (cloud, public, or private) by taking a detailed approach to understanding business goals and objectives while aligning technical capabilities that constitute a business workload. The result is an intuitive migration roadmap that accelerates migrations to a "fit-for-purpose" destination.
- **Workplace Virtualization** – We help our clients centralize some or all of the components of their traditional desktop environment—effectively relocating pieces of the end user computing environment to a data center. This enables clients to increase security, governance and compliance, improve manageability and productivity, deliver a consistent user experience, and reduce management and support costs.

Data Centers

- **Cloud Building and Internal Private Cloud Deployment** – We provide a comprehensive series of consulting, integration and support activities to help clients successfully deploy their cloud environments while maintaining operational compatibility and transforming their existing infrastructure for the delivery of an agile IT-as-a-Service model. We provide a pre integrated, internal private cloud that transforms data center operations to an agile, efficient, and highly automated infrastructure. This helps clients obtain transparency and agility in their operations,

enabling them to deliver services just in time, reducing wait times for resources, and lowering their capital and operating expenditures.

- **Cloud Brokering** – We enable clients to manage multiple private and public clouds from multiple providers in a brokering model that provides a simple "one-stop" service for cloud procurement and management.
- **Hosted Private Cloud Services** – We provide hosted private cloud services which enable accelerated cloud adoption, optimized IT infrastructure, flexible and agile resources, simplified cloud management, and enhanced cloud security. Cloud capabilities are ISO 20000 certified ITIL V3 compliant and can be remotely managed and quickly implemented while ensuring business continuity and higher productivity.

Management

- **Integrated Service Management** – We provide ITIL (V3)-based IT Service Management and Enterprise Systems Management system that is designed to help businesses solve service-related problems by deploying integrated remote monitoring and management capabilities for a range of IT assets and towers. The system converges and unifies event monitoring based on business priorities and co-ordinates service responses across an organization's IT estate, towers, third-party service providers and internal IT teams.

The Unisys approach to address these steps in the journey to the Hybrid Enterprise as illustrated in **Figure 4-16**.

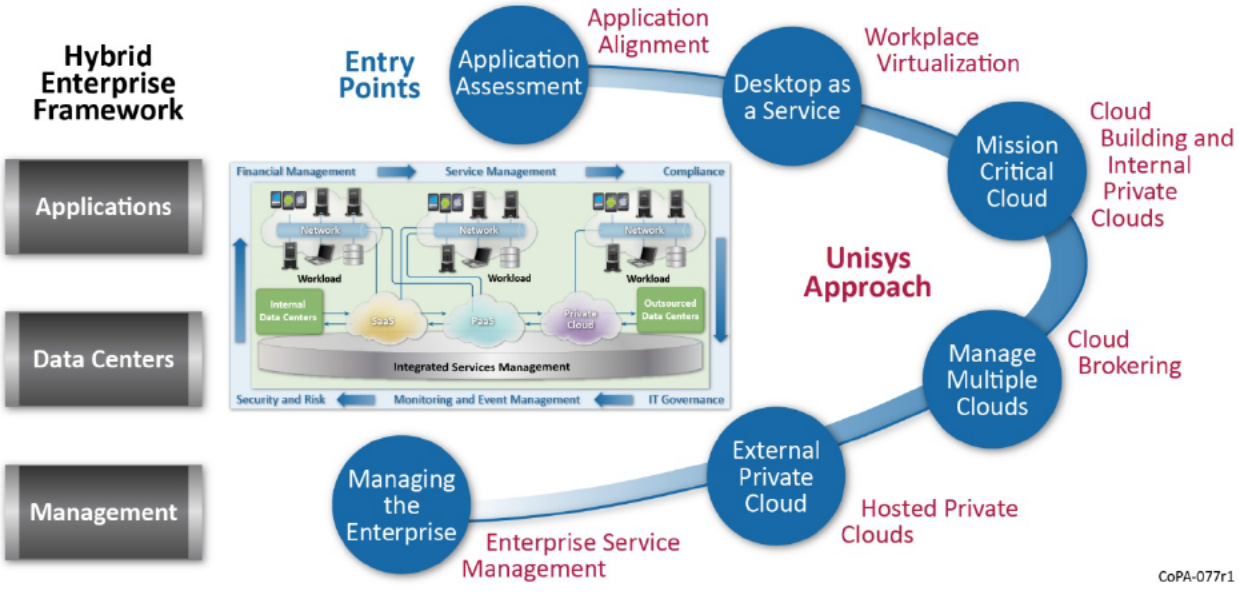


Figure 4-16. The comprehensive Unisys approach to support the journey to the Hybrid Enterprise.

4.3.5 Platform Strategy

We have adopted a heterogeneous platform strategy targeted at cost-effectively optimizing our clients' infrastructure platforms. Our differentiation comes from our mission-critical fabric computing platform which is capable of cost-effectively running ClearPath, Windows and Linux operating systems.

Our vision for the Hybrid Enterprise and the data center of the future is underpinned by our platform strategy that provides a mission-critical and highly cost-effective compute foundation. The Unisys platform strategy is to deliver a highly available and reliable computing experience using advanced fabric technologies and industry-leading Xeon-based processor technology combined with industry standard virtualization; proprietary, standards-based secure partitioning, security, and management software and technologies. Our heritage in mission critical mainframe-class computing uniquely positions us to deliver an inexpensive Xeon-based mission critical computing experience.

"The genius of what Unisys has done is that it has created layers of virtualization and hardware emulation for the OS 2200 and MCP platforms that let it run binary code, unmodified and unrecompiled, that is moved from its own mainframe engines over onto the Xeon engines."

—Timothy Morgan
The UK register

Unisys uses a single, consistent, architecture to support both ClearPath and our Open Systems initiatives. We employ a layered architecture to bring a consistent compute experience to clients. The layers include the infrastructure layer, which combines the platform itself, a system interconnect or fabric, partitioning, and management. A data foundation layer and a solutions layer ride on top of the platform to deliver a "software-defined everything" architecture.

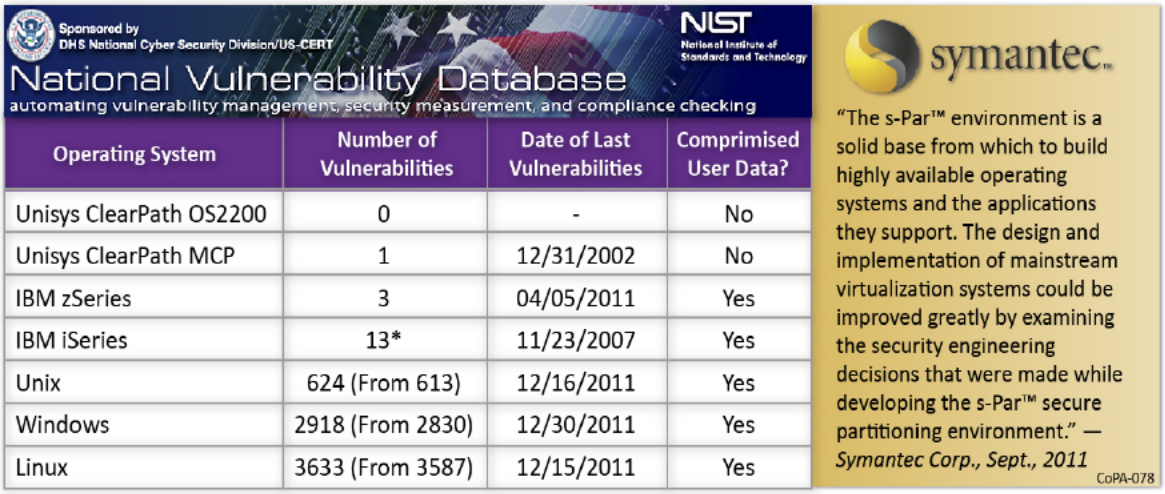
The architecture takes the best from the industry's converged infrastructure plays, but implements it using a single processor architecture, Intel's Xeon. These processors are housed in a multi-socket enclosure designed for high availability and high performance platform. Unisys' partitioning technology allows multiple operating systems and their value stacks to be deployed. These include Unisys' own enterprise class stacks – OS2200 and MCP—along with Windows and Linux and their native tools, applications, databases and transaction environments.

Tenets of our Platform Strategy

- *Mission-Critical Attributes: Security, Scalability, Reliability*
- *Cost effectiveness via standardization*
- *Multiple-platform support for ClearPath, Windows and Linux*
- *"Software defined everything" architecture*
- *Industry leading security and manageability*

A high-speed, low-latency, media-independent fabric interconnects processing platforms, or nodes, providing uniform inter-partition services between partitions in different processing nodes. These secure services allow the software stacks to communicate with each other and the outside world over a software-defined network using dedicated secure virtual circuits and secure virtual switches. Specialized Unisys intellectual property called the Secure Partitioning layer, or s-Par, guarantees

predictable performance, security, and isolation of one partition from another to contain errors **(Figure 4-17)**.



Operating System	Number of Vulnerabilities	Date of Last Vulnerabilities	Comprimised User Data?
Unisys ClearPath OS2200	0	-	No
Unisys ClearPath MCP	1	12/31/2002	No
IBM zSeries	3	04/05/2011	Yes
IBM iSeries	13*	11/23/2007	Yes
Unix	624 (From 613)	12/16/2011	Yes
Windows	2918 (From 2830)	12/30/2011	Yes
Linux	3633 (From 3587)	12/15/2011	Yes

Figure 4-17. NIST National Vulnerability Database showing ClearPath industry leadership

The distributed and elastic nature of this computing complex enables the true Hybrid Enterprise. Our clients can own as much or as little of the complex as they desire, with the balance available in a Platform-as-a-Service (PaaS) arrangement. The architecture also supports advanced business continuance and disaster recovery models because it is inherently disaster resilient. The architecture's flexible nature is enabled by its fabric backbone, which allows owned assets to be distributed over distance and allows easy integration of PaaS resources.

The reliance on a single processor architecture enables our clients to fully use the entire complex, no matter which software solution stacks are required over time - thereby providing a future-proof architecture. As business needs evolve, and the need for one solution stack diminishes and another grows, all hardware assets can be re-provisioned with no waste. This is unique to our converged infrastructure and as a result delivers unprecedented investment protection and flexibility.

4.3.6 Service Management Strategy

Unisys Corporation is a world-class service provider with deep expertise in IT Service Management (ITSM). Our expertise and ITSM service portfolio spans multiple technologies and includes a series of service model archetypes that are unparalleled in the industry. Our client base and expertise includes nearly every commercial and public sector industry vertical. This positions Unisys with expertise that extends far beyond industry best practice.

Integrated Service Management

To achieve the high levels of performance expected and needed to support the Commonwealth's critical services, we recognize the importance of quality service management. In fact, the Commonwealth already took positive steps to bring ITIL best practices, to its operations. Likewise, the entire Unisys Team supporting the current DPH operation is certified in ITIL V3 Foundation.

At Unisys, we made substantial investments in our ITSM Service Portfolio and partnered with key technology suppliers to bring a total solution to our client base. Our ISM practice has some of the most highly skilled ITSM resources in the industry. The team's expertise, which collectively exceeds 1,000 years, spans every discipline of IT with a concentration of BMC Remedy skill sets.

The entire practice is anchored by international standards and industry best practice frameworks such as ITIL, TOGAF, eTOM, COBIT, and ISO. The practice works with our world class deployment team to deliver ITSM services that are unparalleled in the industry.

Unisys BMC has acknowledged as the leading implementer of BMC Remedy ITSM with more than 82 customer migrations to our global multitenant 7.6.04 system as well as dedicated instances.

Value Proposition of Unisys Integrated Service Management

- *World's most comprehensive service management platform*
- *Unified Service view across cloud and traditional environments*
- *Accelerated time to value in upgrading and optimizing service support operations*
- *Ability to right-size costs by moving to a service model for operational improvements*

Service Asset and Configuration Management (SACM) has been a complex area for clients throughout the ITSM community. Our dedicated team is continually feeding years of consulting and industry expertise to implementation guidance. These inputs have helped our clients realize the return on investment that CMDB and SACM have promised for many years.

These examples are representative of what is possible with the optimized architecture we assembled to deliver service management solutions across all IT requirements. All of these are customizable to support client business needs, from management of mobility options to service catalogs and visualization of data across the enterprise.

Integrated Service Management Platform

The Unisys Integrated Service Management (ISM) Environment in **Figure 4-18**, builds the functionality provided in the ITIL IT Service Management framework and provides additional functionality for modular proactive problem management, change management, asset and configuration management, service level management, service request management, and additional dashboard and reporting capabilities.

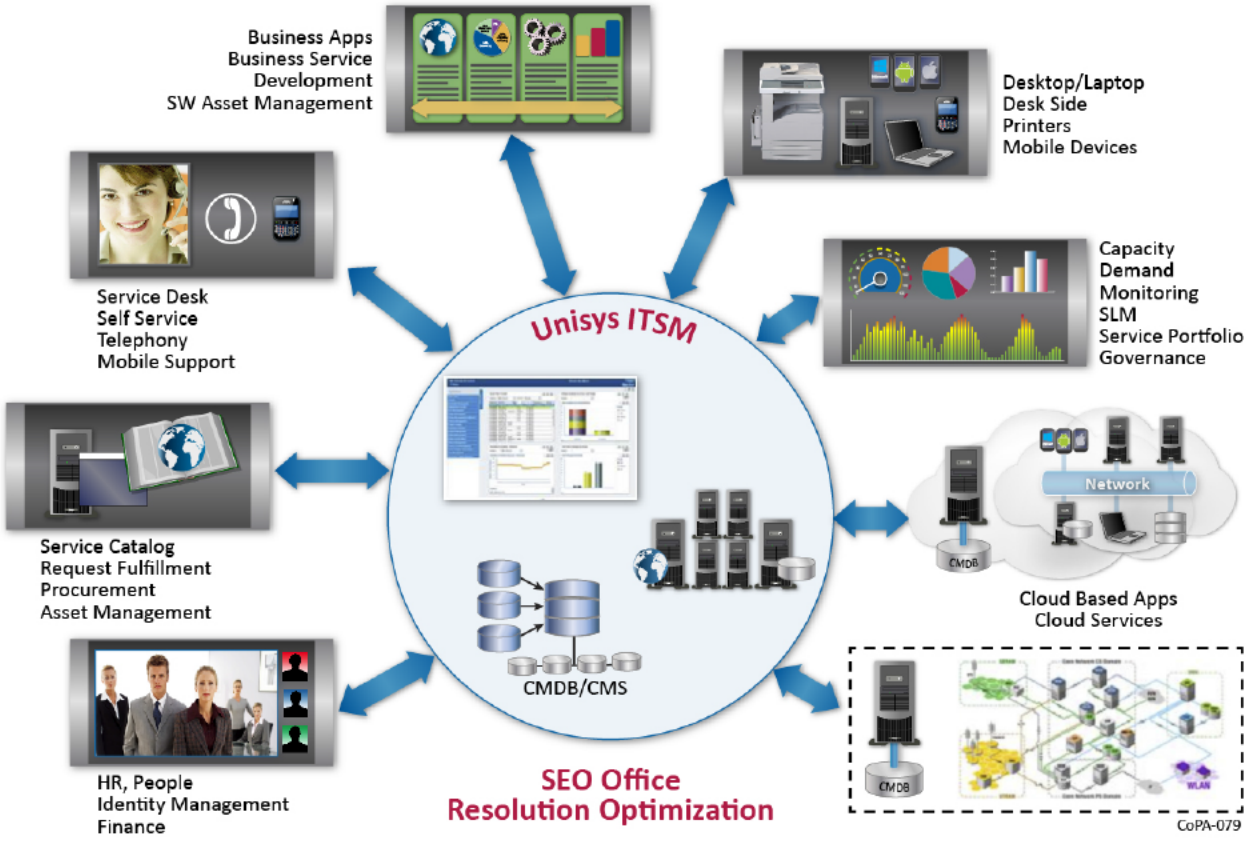


Figure 4-18. The comprehensive Unisys Integrated Service Management Environment

The Unisys ISM platform is made up of the following six services:

1. **Proactive Problem Management:** Helps clients bring IT out of a reactive mode to a predictive mode. This is accomplished by collecting, analyzing and base-lining the current behavior of applications and IT infrastructure, proactively analyzing data to provide recommendations for change management; automatically pinpointing probable cause across technology silos, and initiating standardized problem resolution processes.

2. **Incident Management:** Manages identified incidents resulting from degradation of service or a service outage reported by monitoring systems or user contacts to the Service Desk. Provides full end-to-end management from registration of the incident, through analysis and resolution, to closure and review or a subset of these activities in which the client can perform and track the resolution.
3. **Change Management:** Manages change across the entire IT infrastructure – according to ITIL best practices and organizational policy. Provides better visibility, transparency, and control across the organization. It brings together the process, implementation, and verification components of deploying IT changes through cross-silo integration based on a factory-architected, ITIL-based CMDB.
4. **Service Asset & Configuration Management (SACM):** A set of tools and processes that manages service assets to support the other Service Management processes. SACM discovers and maintains information about infrastructure components (including software, hardware, physical and virtual assets) and integrates it into the service delivery process, leading to efficient and optimized resource allocation.
5. **Service Level Management & Reporting:** Enables real-time, proactive SLA management. Helps to manage the entire range of Service Level Agreements (SLA), from predefined SLAs and monitoring compliance to collecting and analyzing Key Performance Indicator (KPI) data, addressing problem areas, and continually refining the services offered. Analytics provides point-and-click analysis and interactive customizable reports for Incident Management, Problem Management, Asset Management, and CMDB.
6. **Service Reporting:** Provides custom reports and access to data on dashboards. Dashboards enable the linking of critical IT processes to a consolidated view that provides aggregated performance indicators in a single pane of glass. It provides a consolidated, graphical interface of best practice IT metrics for incident, problem, change, and service impact management.

4.3.7 Impact on the Commonwealth

By following our Corporate Strategy, our "best-of-class" team will provide the Commonwealth with the following major benefits:

Cost Efficiencies

Some of the major financial challenges that the Commonwealth is facing include high costs of maintaining its decentralized infrastructure residing in two enterprise data centers and five individual agency data centers. Also, refreshing the Commonwealth's technology on a preplanned basis to limit failures and realizing savings from improved

Key Business Benefits for the Commonwealth

- *Cost Efficiencies and conversion of CAPEX to OPEX*
- *Transformation to Service Orientation and agile IT-as-a-Service*
- *Agility, Flexibility and Scalability benefits of the Cloud Computing model*
- *Mission-Critical Security*
- *Continuous Innovation*

performance is cost prohibitive in these challenging economic times.

To combat these challenges, Unisys recommends a competitive capacity on-demand compute model (private cloud), coupled with full control over fine-grained characteristics of virtual infrastructures, to enable agencies to achieve significant savings in ongoing operating expenses. By leveraging such a competitive subscription model, the Commonwealth will have consistent and predictable pricing to facilitate accurate and timely budget projections.

Also, by freeing up resources currently performing tasks that are easily automated, and by adopting a "factory" model for service delivery, IT organizations can reallocate staff to more productive uses that improve the Commonwealth's ability to meet business goals sooner or more effectively. This proposal fully supports the needs of participants to offload activities to automated environments available in the cloud computing ecosystem.

Service Orientation

Along with cost efficiencies, another key business benefit in terms of the impact to the Commonwealth is service orientation and the ability to move to an IT-as-a-Service model. As previously outlined, this service orientation is reflected across all of the Unisys data center transformation and outsourcing solutions

For example, **CloudBuild Services** enable clients to successfully deploy a cloud while maintaining operational compatibility and transforming their existing infrastructure for the delivery of an agile IT-as-a-Service model.

Agility, Flexibility and Scalability

The Unisys objective is to provide an agile, flexible, scalable, reliable and robust IT infrastructure to support the Commonwealth's transformation to an information-focused organization.

Our Hybrid Enterprise approach that includes cloud building, deployment of internal secure private clouds, cloud brokering, and management of hosted private clouds, coupled with our mission-critical platform technology, will support rapid provisioning of services (in minutes instead of days or weeks in many IT environments), flexibility to scale up or down as business needs dictate, and unprecedented scalability.

Automation in a modern data center environment enables users to have complete control over the timing and availability of IT resources. The productivity gained by being able to provision services rapidly enables users to respond to changing conditions and new requirements quickly, without sacrificing service delivery quality.

Unisys' **Secure Private Cloud** provides improved automation, self-diagnostics, server utilization, compliance and ease of management in the data center environment. Also, Unisys provides the following services that help in seamless integration:

- Enterprise Virtualization Design and Implementation
- Secure Private Cloud Plan, Design, and Implementation
- Full set of Unisys Infrastructure Management Suite (IMS), including Plan, Design, and Implementation
- Training and Mentoring Services
- A master cloud architecture and roadmap

The implementation of Secure Private Cloud computing along with the Unisys IMS suite will enable the Commonwealth to address issues such as the need for cost savings, operational efficiency, capacity flexibility and support for transitioning to a new business model.

Security

Our platform strategy, coupled with our "zero trust" security approach and unique, defense-grade data protection technologies, will enable the Commonwealth to operate in a mission-critical environment that allows the full benefits of cloud computing to be realized without compromising sensitive data.

We provide a secure, durable technology platform with industry-recognized certifications and audits, including PCI DSS Level 1, ISO 27001, FISMA Moderate, HIPAA, and SSAE 16. Our services and data centers have multiple layers of operational and physical security to confirm the integrity and safety of Commonwealth data.

Unisys' **Stealth Solution Suite** – A defense grade enterprise-wide security innovation that makes data communication end points invisible on the network and therefore removed as targets from hackers. Also, Stealth reduces costs through consolidation and virtualization of networks as well as end user and multitenant cloud architectures and will be implemented as part of our solution.

In addition to using Stealth for this engagement, we have combined our corporate strengths in security with Deloitte's local security expertise and knowledge of the Commonwealth, to provide a "best-in-class" security solution and architecture.

Continuous Innovation

Leveraging the innovation in our Hybrid Enterprise framework will provide the Commonwealth with a highly virtualized data center architecture to support current and future capacity and service level demands. Our integration services will consolidate the enterprise and agency data centers to save costs, reduce energy consumption, use space optimally, and improve IT asset utilization.

One of the key advantages of the Unisys Cloud Provisioning System is the ability to seamlessly integrate these hybrid delivery models. This will allow the Commonwealth to have a single model for seamlessly managing all delivery models while allowing the selection of the most effective provider for a given application or workload. We maintain

strong relationships with key partners to meet a wide variety of cloud applications and supporting services.

Commitment to Process, Tools and Automation

A key differentiator of Unisys is our focus on process excellence and automated tooling to optimize efficiencies both on our consulting and systems integration projects and in our production operations. Our history of innovation and intellectual property in this area will make sure that we maximize the business benefits delivered throughout this engagement and throughout the ongoing operations.

4.3.8 Summary Unisys Strategic Direction

Unisys is a global information technology company whose purpose is to deliver **mission-critical** IT solutions that solve our clients' most demanding IT problems. We differentiate ourselves on the highest levels of **service quality** and measure success by our **customer satisfaction**. We have proven our commitment to both service quality and customer satisfaction by providing very similar services to the Commonwealth since 1999. Our quality, as measured by SLAs, and our customer satisfaction, measured by regular surveys of our agency clients, evidences that our corporate strategy is to make our customers highly satisfied with our services. That commitment is unchanged. In fact, our most senior corporate executive, Ed Coleman, has personally affirmed that commitment.

As you can see, our focus areas are well aligned with the Commonwealth's requirements. The Hybrid Enterprise is our comprehensive data center strategy that defines the data center of the future and provides the tools, technologies, and services to successfully navigate the transition. Our heterogeneous platform strategy is targeted at cost-effectively optimizing our clients' infrastructure platforms and is differentiated by our mission critical, fabric computing platform capable of cost-effectively running ClearPath, Windows and Linux operating systems.

To bring this innovation to our clients, the key elements of our approach include: identification of the latest disruptive technologies and trends that have strategic benefit to our clients; investing heavily to integrate them into our portfolio and our four Areas of Strength, and then delivering continuous innovation with our clients in our programmatic approach, including our highly collaborative Innovation Workshops.

In this way, we can bring the industry innovation occurring in the disruptive trends – including cloud computing, mobile computing, social computing, and big data/analytics - into our four portfolio areas of strength so that clients gain the **operational benefits** of our mission-critical computing focus coupled with the **transformational benefits** of the next generation IT architecture enabled by these technologies and trends.

The net result is that we are ideally poised to help the Commonwealth leverage the latest technology trends coupled with our mission critical solutions in a **systematic way** making

sure **real and measurable business value to your many constituents is derived.** We also commit that our team and the technology proposed will help enable that the 12.6 million Pennsylvanians to receive critical services they need and expect.

This page intentionally left blank.

4.4 Unisys Dedication to Quality

RFP	*Requirement*
	Dedication to Quality *The Offeror must provide details of its approach to measuring and maintaining high quality services. The Offeror should provide details of any industry-recognized quality standard to which it is, or will become, compliant (including a timeframe for compliance, if not already achieved), as well as any awards received over the past 18 months. Indicate all quality programs that are externally measured (e.g., Six Sigma, ISO 9001:2000) and how such certifications would directly benefit the Commonwealth. A detailed approach and quality plan should be included in the response to this section.*

High-quality Services

Unisys—Local Quality Commitment to the Commonwealth

The cornerstone of the Unisys Team's approach to quality for the Commonwealth are conformance to ITIL standards in everything we do for service management and the complete implementation of our Continuous Improvement and Innovation Program (CSIIP), which is run and supported by the Unisys Six Sigma Lean (SSL) organization.

ITIL Foundation V3

All Unisys staff supporting the EDC and the DPH are ITIL V3 certified.

Unisys is a recognized IT Infrastructure support and managed services partner in the Commonwealth through our engagements at the Enterprise Data Center (EDC) and the Data PowerHouse (DPH). At the EDC, since May 2000 Unisys resources have provided a variety of IT support services to the Commonwealth's EDC which hosts approximately 3,900 servers, 700 Web-based applications, 97,000 e-mail users, 900 TB of data storage, and 2,000 databases. For the past 13 years, Unisys has provided outsourced operations and technical support services at the DPH for most of the mission-critical systems under the jurisdiction of the Governor's Office.

Just one example of our current commitment to maintaining high-quality services for the Commonwealth is the fact that all operations and technical support staff currently providing services at both the EDC and the DPH are certified in ITIL V3 Foundation. Also, all Unisys senior staff managing both the EDC and DPH are certified in ITIL V3 Foundation.

4.4.1 Approach to Measuring & Maintaining High Quality Services

Unisys approaches the delivery of quality and innovation through an integrated set of programs, processes and standards that will be greatly enhanced and begin with a dedicated, project-level, and local Service Excellence Office (SEO)

Service Excellence Office (SEO)

Measuring and maintaining high-quality services begins with having an organization focused on quality and service excellence. Unisys views quality and continuous service improvement as a critical success factor in driving customer satisfaction for the Commonwealth IT infrastructure. We are establishing a dedicated and local project-level SEO to proactively manage quality, continuous service improvement, ITIL process management, and Customer Satisfaction through a comprehensive Quality Plan that specifically addresses all of these areas. We believe this is a key differentiator in our partnership with the Commonwealth. The SEO will define and oversee of all ITIL process management and analysis functions including Change Management, Release Management, Incident Management, Problem Management, Asset Management, Configuration and CMDB Management, Availability Management, and Service Level Management. More information on our SEO is in our detailed Approach and Quality Plan in Section 4.4.

Dedicated Service Excellence Office (SEO)

A local and dedicated SEO will proactively manage Quality, Continuous Service Improvement, ITIL Process Management, and Client Satisfaction via a comprehensive Quality Plan for this project.

Conformance to IT Standards and Best Practices

Measuring and maintaining high-quality services requires discipline and adherence to industry standards. For the Commonwealth, Unisys will implement a sound service delivery framework and methodology based on industry standards: ITIL and best practices. The Commonwealth seeks a service provider that has significant experience with ITIL and with providing managed services and support to large institutions with highly complex multiplatform applications and technology. Unisys will not just provide staff to the Commonwealth; we will deliver managed services and delivery resources supported by a proven ITIL compliant service delivery framework and a global service and support infrastructure. We are a global managed services provider with a wealth of knowledge and experience in implementing and supporting large, complex IT environments in which we repeatedly conform to ITIL standards, leverage best practices and implement continuous improvement programs for our clients.

The managed services that the Unisys Team provides will be based on the globally accepted ITIL framework providing end-to-end Service Management for the Commonwealth. The ITIL framework, illustrated in **Figure 4-19**, focuses on industry best practices for providing

consistent, reliable, well-defined processes and procedures for delivering IT Service Management. Unisys will also incorporate the Control Objectives for Information and related Technology (CobIT), linking control and Six Sigma defect-reduction practices (measuring and responding to quality issues) to our service delivery methodology, adding this expertise to improve the Commonwealth's IT processes. Our mature practices will lead to world-class service delivery offer the Commonwealth better quality, spend predictability, containment, and reduced complexity across the entire infrastructure.

ITIL Service Management Model

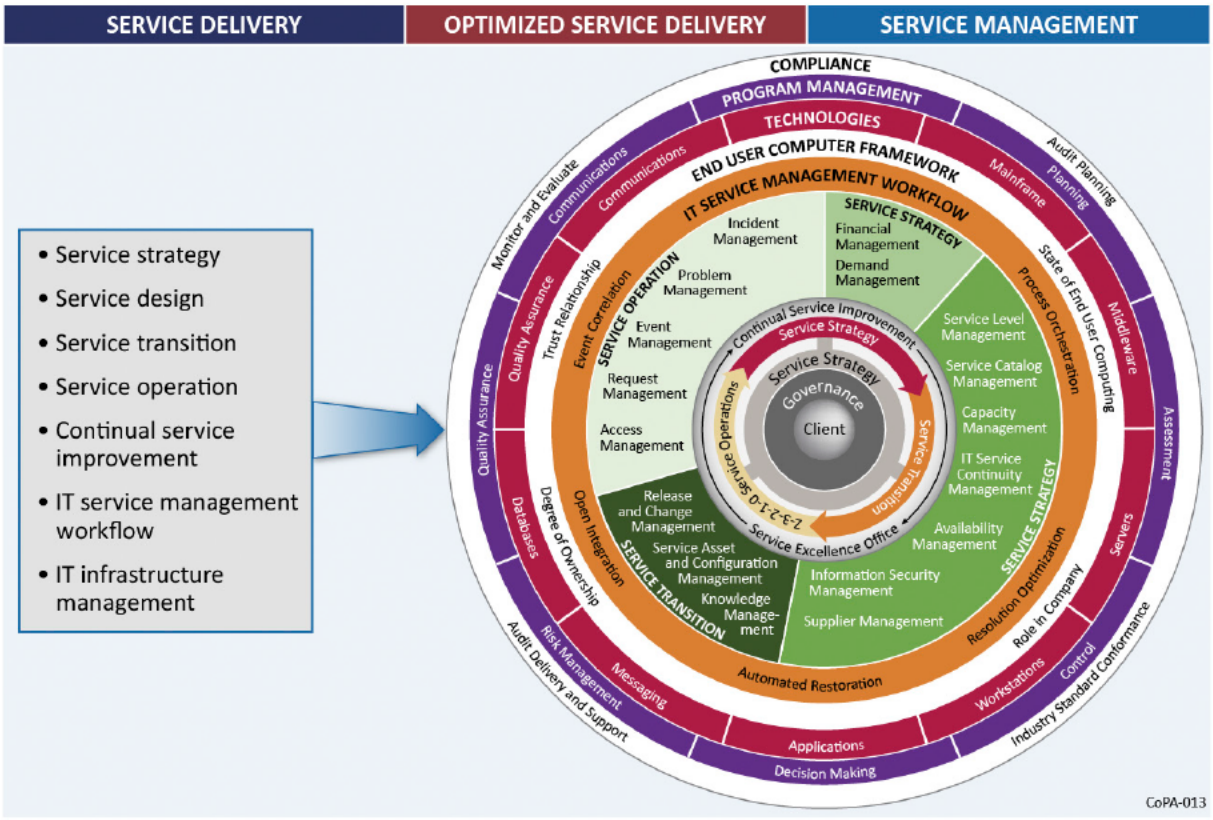


Figure 4-19. ITIL Service Management Model

By embracing this framework, Unisys will provide the Commonwealth with a consistent level of service across the infrastructure, increasing problem resolution times and decreasing downtime to provide a stable, high-performing infrastructure environment and increased agency satisfaction. The Unisys Service Delivery Framework offers the right skills, infrastructure, and best practice processes to provide a cost-effective, flexible, single-source solution for ongoing management of the Commonwealth's infrastructure.

Unisys follows many of the ITIL components today on our engagements at the EDC and the DPH. The Unisys Quality framework at the Commonwealth has introduced operational

efficiencies to improve the mean time to resolve issues and incidents for both the EDC and DPH projects. At the DPH, Unisys deployed our advanced tool suite in which we employed software instrumentation and artificial intelligence techniques to provide automated monitoring, response, notification, and wherever possible, instant corrective action. Our proven Service Delivery Framework, also based on ITIL, has dramatically improved the consistency and predictability of operations and mean time to repair while also improving the overall efficiency of operations at the DPH.

Unisys will implement our proven Service Delivery Framework across all the Commonwealth agencies to provide best-in-class quality solutions.

Quality Measurement Tools, SLAs, SLOs, and KPIs

The ITIL framework contains Industry tools that measure and monitor the IT infrastructure across its life cycle. Unisys has leveraged industry best practices, ITIL V3, and ISO 20000 standards to develop an automated framework that provides a systematic means for our Commonwealth project team to follow and gauge success. By standardizing on mutually accepted key performance indicators and measurements (SLAs, SLOs, and KPIs) we can evaluate the project's effectiveness, the quality of the products, and collect historical data points for trending comparisons. This will provide tracking and guidance for Unisys to promote a continuous state of quality improvement, while providing the Commonwealth with key data points to track the environment's performance and historical reports for trending. Some of the Key Enterprise System Management Tools being provided to the Commonwealth are outlined in **Figure 4-20.**

Enterprise System Management Tools

Scope and Tasks

- Events monitoring and notification
- First level triage and remiediation
- Change management
- Support of production job/scheduling
- Vendor coordinator and management
- Request Management
- Maintenance window coordination

Technologies

- Wintel Servers
- Unisys Mainframes (MCP/2200)
- IBM Mainframe z-Series
- Storage and backup
- Unix servers
- Network devices
- Security (Firewalls/Security Devices)

Tools	
Ticketing	• Remedy 6.0 • ITSM Remedy 7.1 and 7.6 • Service Center
Monitoring	• BMC Impact Explorer (BEM) • NAGIOS • SCOM • Xymon • SPO/Opcon Web • Control M/Opcon XPS • SolarWinds • Mainframe Consoles • Dell Open Manage IT Assistant • HP Open View • SMARTS
Others	• Citrix • LifeRay (Portal and KM) • Microsoft RDP • Telnet • VNC Viewer • Tonysoft • Dell Remote Assistant Console (DRAC)

CoPA-195

Figure 4-20. Enterprise System Management Tools

Quality Measurement Processes—Client Satisfaction Program, Six Sigma Lean Processes, Continuous Service Improvement & Innovation Process and Internal Audit Processes

Unisys will continually align and realign IT services with the changing business needs of the Commonwealth agencies by identifying and implementing improvements to IT services that support business processes, across the entire IT life cycle. We will leverage proven process methodologies to drive improved quality and continuous service improvement for the Commonwealth. These key processes are outlined in **Figure 4-21.**

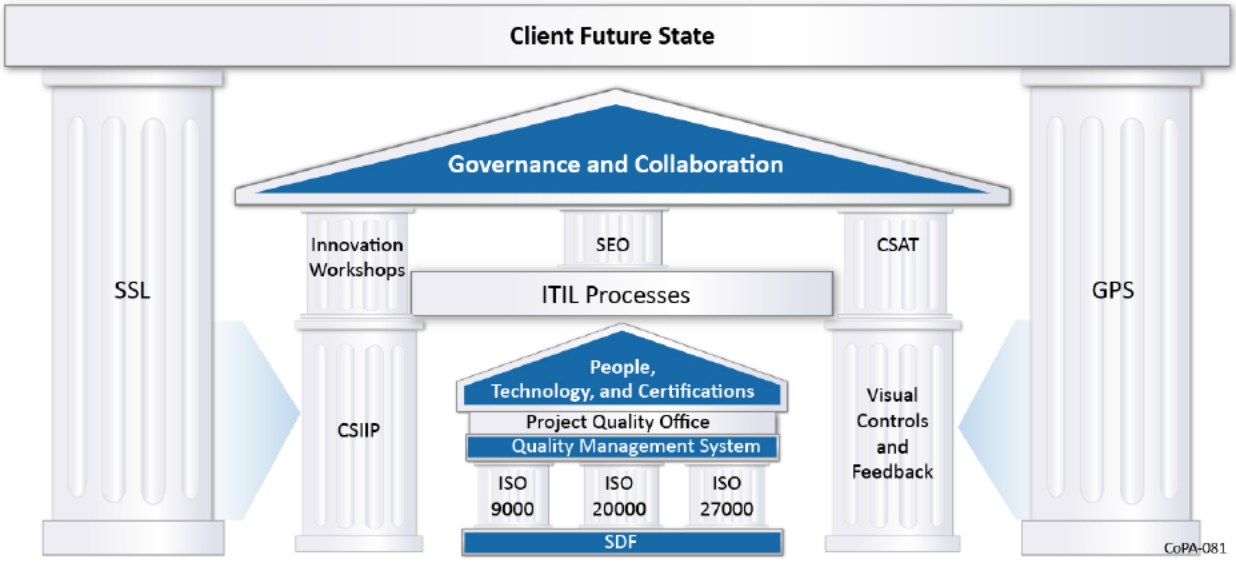


Figure 4-21. Continuous Improvement

Client Satisfaction Program (CSAT)

Providing best-in-class ITIL based IT Service Management and driving excellent Client Satisfaction is extremely important to Unisys and a key focus in our IT Solution. Our SEO will manage a multipronged approach to Client Satisfaction. Our SEO will collect data across multiple levels to gain a clear understanding of the Commonwealth's satisfaction with the IT Services being provided. Our Service Desk will randomly survey Commonwealth customers who call the Service Desk with a request or change that needs to be completed or an incident that needs to be resolved. We will develop a Knowledge Management Portal to allow for direct feedback from Commonwealth agencies. Additional details on the local project implementation of our CSAT program are in our Detailed Approach and Quality Plan in Section 4.4.4.

Global CSAT Auditing

From a corporate perspective, our local CSAT program is a strategic, action-oriented program initiated and followed monthly by the Unisys CEO, Ed Coleman and is a regular agenda item in the CEO's monthly Executive Committee meetings. It supports the Unisys goal of regular, open communication and associated remediation when needed.

Six Sigma Lean (SSL)

Since 2005, Unisys has adopted the Six Sigma Lean methodology and embedded the methodologies and skills across our organization. Our CSIIP process and the SEO activities are supported by Six Sigma Lean methods and techniques. Specifically, our RCA methodologies (such as those for defect reduction) follow the PDCA Cycle and use Six Sigma Lean tools such as the fishbone diagram, graphical analysis, mistake proofing, hypothesis testing, correlation/regression, value stream mapping, and Failure Mode and Effect Analysis (FMEA). Also, key leaders in the Unisys Project Management Office are all trained in Six Sigma Lean and when appropriate will have access to Six Sigma Black Belt level resources. Our Black Belts are trained as facilitators for collaborative events such as Kaizen and Innovation Workshops.

Our Six Sigma efforts focus on improving client satisfaction, operational excellence, and overall efficiency of operations that reduce cost. Unisys has a comprehensive Six Sigma Lean training curriculum with both instructor-led and self-paced classes on topics such as DMAIC, statistical analysis, Lean thinking, Kaizen methods and A3 problem-solving at Yellow Belt, Green Belt and Black Belt levels.

Continuous Service Improvement and Innovation Program

Unisys established our Continuous Service Improvement and Innovation Program (CSIIP) as our standard framework for aligning our improvement focus on our clients' strategic priorities. This has delivered impressive results for multiple Unisys clients around the globe.

The mainly goal of CSIIP is to create an ongoing formal program that encourages the proactive identification and introduction of measurable improvements in a specific work area or work process, and to introduce "innovation in context" to those areas. One of this program's major features is its ability to consolidate and analyze the many inputs required to effectively develop an innovation and improvement plan. These inputs include:

- Executive management objectives
- Key Provider Technology Roadmaps
- Customer Satisfaction Surveys and the Voice of the Customer
- Business and Technology Risk Registers
- Unisys Thought Leadership and Best Practices
- Problem Management analysis from the Unisys Service Excellence Office
- Agent feedback and suggestions

The CSIIP process uses a structured approach to gathering and analyzing these important factors to build a comprehensive roadmap to cover remediation, improvement and innovation opportunities. This will provide the Commonwealth with the necessary information to make informed decisions based on relative cost/benefit, alignment with strategy and return on investment for various actions, of varying scale from incremental through to truly 'breakthrough'.

For additional details of our implementation of Unisys CSIIP, please see our detailed Approach and Quality Plan in Section 4.4.4.

Unisys Corporate Innovation

Unisys Innovation Workshops are collaborative workshops with our clients designed to explore opportunities for disruptive and transformational change. We expose our clients to the latest disruptive technologies and trends and collaboratively examine opportunities for strategic business benefit. **Unisys Global Portfolio Services (GPS)** community monitors industry trends and technology changes. When combined with feedback from the Commonwealth with all of our Client results, this monitoring will help us shape our corporate products and solutions. GPS is also integral and augments the delivery of innovation to our local SEO, which will then advise the Commonwealth on the applicability of technology in its environment.

Unisys Global Infrastructure for Enterprise Computing

For continuous improvement, the local Service Excellence Office will be supported by the corporate Enterprise Computing Program which conducts regular initiatives to drive year-on-year productivity improvements for all Client accounts such as creating command centers and redistributing workload to create more efficient delivery models. An example of this is the introduction of automated runbooks that replaced manual help files at the DPH to bring more knowledge in context' to Level 1 teams.

Internal Audit Processes

Project Quality Office (PQO)

The Unisys PQO is the independent organization at Unisys chartered as the key quality advisor to the operating groups on deal structures, risk management, and project performance. Our PQO reviews and evaluates all aspects of proposals and project engagements with the goal to minimize risk while maximizing client satisfaction over the entire life cycle

The Unisys PQO conducts two types of project reviews—Project Readiness Reviews (PRRs) and Quality Assurance Reviews (QARs)—to identify any potential problems or gaps

- PRRs are designed to confirm that the:
  - Project is properly planned
  - Project plans are sufficiently adequate, accurate and detailed

- Project's contracted solution can be delivered on time and on budget
- Appropriate risk management is included (identify approaches to manage/mitigate risks)

- QARs will be performed periodically by independent reviewers who are not part of the Unisys local account team. This process provides a second level of quality and risk review using individuals who are independent of the Unisys client serving team. This process also provides an unbiased view of engagement progress, risk management actions, client satisfaction, and advice on solving problems and making improvements. The client interview is part of the QAR process.

The Unisys Quality Policy Statement

From a corporate standpoint, Unisys drives client value activities and business excellence initiatives to make our company a world-class provider of choice, Unisys continually improves our client relationships in order to achieve world-class business relationships and client advocacy. Our employees have both internal and external clients and must maintain regular communication with them to clearly understand and meet their changing requirements and expectations. Units at Unisys are required to set measurable quality objectives to continually improve the effectiveness of their processes. We are required to confirm that the applicable statutory and regulatory requirements are met for our products and services. We acknowledge that our people are critical to the success of our Quality Improvement Process and we therefore provide in their development so that they can contribute to this process effectively.

4.4.2 Industry-recognized Quality Standards and Awards

Unisys has consistently achieved top rankings in critical IT managed services and outsourcing evaluations conducted by key market influencers. Unisys is consistently rated in Gartner's Leader Quadrant for Outsourcing Services. We are also a recognized leader in Secure Outsourcing Solutions. These industry-leading awards clearly demonstrate our commitment to provide best in class, high-quality services to the Commonwealth. Please see **Figure 4-22.**

SQM	2011 SQM first Call Resolution Improvement Award for Marriott. Unisys is the only service provider to have received this award. Marriott is recognizes by SQM in the "Call Center World Class Call Certification"
Gartner	• 2012 Leader Quadrant for North America Help Desk Outsourcing • 2012 Challenger Quadrant for North America Data Center Outsourcing • 2012 Challenger Quadrant for North America Desktop Outsourcing Services • 2012 Challenger Quadrant for Europe Help Desk Outsourcing • 2012 Challenger Quadrant for Europe Desktop Outsourcing Services
FORRESTER®	• 2011 Strong Performer: The Forrester Wave™:Global IT Infrastructure Outsourcing Q1 2011 • 2010 Strong Performer: The Forrester Wave™: Managed Security Services 2010
GLOBAL 100 SERVICES	2012 and 2011 Global Services Top 100 Service providers of the Year; Multiple Categories: Top Global Diversified Outsourcing Vendors, Top Global ITO Vendors, Top ADM Vendors, Top IM Vendors
	Computerworld Honors Program, 2011 Laureates Class (Multiple Clients)
sson	• 2011 Excellence in People and Communications - Winner • 2011 Excellence in Culture Creation - Finalist
IAOP	Leaders category for the 2011 and 2012 Global Outsourcing 100® service provider list
tpi	2011 ANZ Service Provider Excellence Award

CoPA-071

Figure 4-22. Industry Recognitions

Unisys also receives numerous Partner Awards from our IT Managed Services clients. Microsoft, Amgen, Dell, and Starbucks have all recognized Unisys for our Service excellence, quality, and commitment to success. Please see **Figure 4-23.**

Figure 4-23. Partnership Awards

4.4.3 External Quality Certification

Unisys takes pride in industry certifications that show our dedication to technology, quality, and process excellence. We hold more than 30 certifications for quality management and assurance from the prestigious International Organization for Standardization (ISO). All Unisys Data Centers are ISO 27001, ISO 9001, and ISO 20000 certified. A combination of these three certifications makes certain that Unisys is capable in maintaining quality, security, and a true service management system throughout our entire global operation.

Quality Enhancement

Unisys ISO 9001 certified quality assurance (QA) will be provided as part of our PMO, where our QA function is located, and will interact with our global quality assurance team, which will enable the Commonwealth benefits from the leveraged QA program that is deployed throughout Unisys. Our QA function will interact closely with our global Service Delivery Manager and Service Control Managers to make sure that any irregularities to the services will be handled and avoided by realigning processes and resources for better quality delivery. Our QA office will also perform audits to verify that operations documentation is kept up to date and adheres to the highest quality. Documentation will be produced by the service streams and integrated by our global service delivery organization. Unisys developed and is continually aligning operational procedures; the Commonwealth

benefits from them as these are released to production by the service development functions at Unisys.

An example of a typical quality enhancement initiative is the work done with a major US-based retail organization that needed enhanced service delivery (more than originally contracted). Unisys worked with the Commonwealth on the design and implementation of a new process using replacement units with pre-deployed inventory to reduce end user downtime

The following tables reflect Unisys External Quality Compliance, Unisys External Certifications, and Unisys External Certifications for our Staff:

Unisys Compliancy

Certification and Standards	How they Apply at Unisys
ISO 27001 and ISO 27002	To support our clients globally, Unisys uses our Data Centers and Managed Services Centers in the United States, the Netherlands, Hungary, India, China, Brazil, and Colombia. All these locations are ISO 27001 certified. The DPH is certified in ISO 27001 and regularly passes SSAE 16 audits.
ISO 14001	Unisys has two production facilities in the United States; both are ISO 14001 certified.
SSAE 16 Type II and ISAE 3402	Unisys Data Centers and Managed Services Centers in the United Kingdom, the Netherlands, Hungary, India, and China are compliant with SSAE 16 Type II and ISAE 3402.
Specific Data Center Standards	Unisys Data Center operations are based on industry standards certified by ISO. All Unisys Data Centers are ISO 27001, ISO 9001, and ISO 20000 certified. A combination of these three certifications confirms that Unisys can maintain quality, security, and a true Service Management system throughout all of our global operations.
Quality Assurance Methodology	All Unisys operations, countries, and locations operate according to the Unisys Quality System, which is accredited by ISO 9001.
ITIL V3	ITIL (the IT Infrastructure Library) is the most widely accepted approach to IT Service Management in the world. ITIL provides a cohesive set of best practices drawn from the public and private sectors worldwide. It is supported by a comprehensive qualifications program, accredited training organizations, and implementation and assessment tools. Best practice processes are promoted in ITIL support and supported by ISO 20000. Unisys is proud to be a truly global ITIL V3 compliant service provider—we can provide one global service delivery experience throughout all our Managed Services Centers and Data Centers. Fifty five Unisys resources dedicated to the Commonwealth are ITIL V3 certifications
Unisys IT Service Mgmt (ITSM)	The Unisys IT Service Management (ITSM) practice was assessed by Underwriters Laboratories, Inc., which found that the practice is in compliance with that ISO/IEC 20000-1:2005, resulting in a 3-year certification. Unisys was the eighth company to be certified in the United States and the first company to receive certification for its global operations.

Certification and Standards	How they Apply at Unisys
ISO 27001 and ISO 27002	To support our clients globally, Unisys uses our Data Centers and Managed Services Centers in the United States, the Netherlands, Hungary, India, China, Brazil, and Colombia. All these locations are ISO 27001 certified. The DPH is certified in ISO 27001 and regularly passes SSAE 16 audits.
Unisys Desktop Services	Unisys Desktop Services, portal and electronic interfaces, service request management, service supply chain, and maintenance and time and materials billing comply with ISO 9001:2000 and TickIT standards.
Unisys Maintenance, Installation, and Project Management Services	Unisys Maintenance, Installation, and Project Management Services are ISO 9002 certified for operations in Australia, Canada, Europe, Hong Kong, Latin America, Singapore, Taiwan, and the USA
Regulatory Compliance	Unisys service locations meet all FDIC, FFIEC, OCC, NIST, and HIPAA requirements

Unisys Certifications

Certification	Certification Date	Description
ITIL/ITSM-certified service delivery personnel	Date not applicable	All the service delivery personnel assigned to support the Commonwealth are certified to use the Unisys global ITSM platform, which was developed from BMC Remedy 7.6. All our service delivery personnel completed their ITIL V3 Foundation training.
CISSP-certified service security personnel	Date not applicable	Unisys has 135 CISSP-certified services personnel.
PMI-certified service delivery personnel	Date not applicable	Unisys has 170 PMI-certified Project Management resources. Project Management resources assigned to the Commonwealth will be PMI certified.
ISO 9001	Managed Services Center	Quality - 100 percent certification of our global Managed Services Centers (MSCs) providing Enterprise Compute Services.
ISO 9001	Global Supply Chain	Certification for multivendor parts delivery, product distribution, and network integration operations. Unisys is the only company to hold global ISO 9001 certification for multivendor parts delivery, product distribution, and network integration operations.
ISO 17799	Not applicable	Unisys manages to the ISO 27001 standard.
ISO 27001	Managed Services Center	Security - a global standard for best practices in Information Security Management achieved by all 22 major Unisys Data Centers and Managed Services Centers providing Enterprise Compute Services.
ISO 20000	Managed Services Center	ITIL - Certification service for event and service desk management. Desktop services, portal and electronic interfaces, service request management, service supply chain, and maintenance/T&M billing comply with ISO 9001:2000 and TickIT standards.
CMMI	Application Support Center	Capability Maturity Model Integration (CMMI) Level 5 for our primary Application Support Centers and Regional Centers are at least at Level 3.
Sarbanes-Oxley Act	Annual	Global MSCs providing Enterprise Compute Services.
SSAE 16 SOC 1 Type II Audit	Annual	Global MSCs providing Enterprise Compute Services.

Unisys Employee Certifications (as of January 2013)

Certification	Number of Employees
Management Discipline	
Program Management	324
ISO 9000 Internal Auditors/Quality Trainers	69
Six Sigma	
Master Black Belts (MBBs)	9
Black Belts	86
Green Belts	581
Lean Practitioners	150
White Belts	22,000
Representative DBMS and Language Types	
Oracle/Oracle tools	1,228
Java and Java tools	1,174
C, C++	1,484
Rational tools	871
Security	
Certified Information Systems Security Professional (CISSP)	61
Cleared employees:	2,074
Secret	749
Interim Secret	92
Top Secret	1,001
Interim Top Secret	41
SCI	191
Technology	
Microsoft	
Microsoft Certified Professional (MCP)	845
Microsoft Certified Professional + Internet (MCP+I)	220
Microsoft Certified Solution Developer (MCSD)	35
Microsoft Certified Solution Developer (MCSD)	35
Microsoft Certified Systems Engineer (MCSE)	826
Microsoft Certified Systems Engineer + Internet (MCSE+I)	48
Microsoft Certified Trainer (MCT)	37
A+ computer technician certification	2,061

Certification	Number of Employees
Novell	
Certified Novell Engineer (CNE)	199
Certified Novell Administrator (CNA)	148
Cisco	
Cisco Certified Network Associate (CCNA)	357
Cisco Certified Internetwork Expert (CCIE)	41
Cisco Certified Design Associate (CCDA)	53
Oracle	
Oracle 7 DBA Certification	10
Oracle 8 DBA Certification	26
Oracle 9i Certified Professional DBA	21
Oracle Certified Professional	18
Oracle Masters Certificate	10

4.4.4 Detailed Approach and Quality Plan

Quality, continuous service improvement, and client satisfaction all begin with the voice of the Commonwealth. Unisys recognizes the voice of the Commonwealth and the significant importance of quality and continuous service improvement to reduce risk, improve service quality, improve client satisfaction, and confirm service transparency through a continuous cycle of evaluation and improvement in an IT infrastructure. We view quality and continuous service improvement as a Critical Success factor in driving client satisfaction for the Commonwealth IT infrastructure. Unisys is establishing a dedicated and local project level Service Excellence Office that will proactively manage quality, continuous service improvement, ITIL process management, and customer satisfaction through a comprehensive Quality Plan that specifically addresses all of these areas. We believe this is a key differentiator in our partnership with the Commonwealth. Unisys will develop, implement, manage, and govern two detailed Quality Plans. The initial Quality Plan will be a Transition Quality Plan to make sure that quality is a primary focus in the critical Transition of the Commonwealth agencies to the new IT Services contract. Unisys will then develop and manage the IT Services Management Quality Plan, for steady state ongoing operations. These plans will be documented, updated, and governed through the Commonwealth Computer Procedures Manual (CCPM). Through this new organization and these quality plans, Unisys will drive best in class services and the highest customer satisfaction experience throughout the Commonwealth.

Service Excellence Office

Out Transition Quality Plan begins with the Service Excellence Office (SEO). As shown in **Figure 4-24**, the SEO defines and oversees all ITIL process management and analysis functions, including Change Management, Release Management, Incident Management,

Problem Management, Asset Management, Configuration and CMDB Management, Availability Management, and Service Level Management. Process managers and analysts' responsibilities in the SEO include process effectiveness audits, confirm service delivery teams' comply with proper process execution, and analyze process trends for anomalies. The SEO will manage Continuous Service Improvement programs in collaboration with Commonwealth agencies.

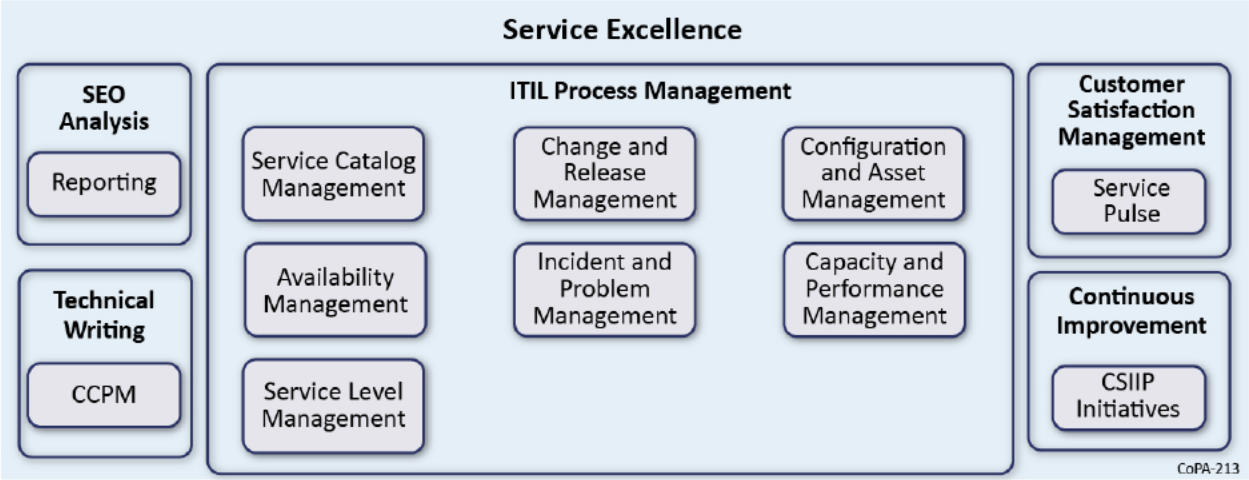


Figure 4-24. Service Excellence and Oversight of ITIL Process Management

The SEO manages and drives quality across the Commonwealth's multidimensional, complex, and matrixed IT service delivery organizations. The SEO will standardize quality across Commonwealth agencies, Unisys, and partner organizations, as well as across all IT service processes, IT monitoring and automation tools, and client satisfaction surveys and processes. Unisys will leverage the ITIL framework, ISO Certifications, Six Sigma Lean tools, and our Continuous Service Improvement and Innovation Program (CSIIP) to proactively make certain the highest-quality IT services are being provided. Please refer to Schedule F, Section 3.2.1.1.6 for organizational details on the SEO.

ITIL Service Delivery Framework – Driving Standardization and Service Excellence

The ITIL Process Management function is at the core of service excellence. This function effectively designs the management practices, processes, functions, roles, knowledge, and skills that the Unisys Team will use to enable us to deliver services that create value to the Commonwealth. Through IT Service Management, processes are developed and executed to facilitate the implementation and management of quality IT services that meet the Commonwealth's needs. This discipline is essential to verify we consistently produce quality services in a timely and cost-effective way.

Unisys engages in quality planning activities to confirm that changes are planned, documented, accomplished and evaluated. Our quality planning process establishes quality goals and objectives that are appropriate to meet the Commonwealth's requirements.

Quality planning provides a framework to guide the evolution and continuous improvement of the Quality Plans through the Plan-Do-Check-Act (PDCA) continuous improvement cycle **Figure 4-25**.

PLAN - Who will do what by when? What materials are needed?

DO - Implement the plan

CHECK - Evaluate the effort and results

ACT - Identify actions that need to be taken

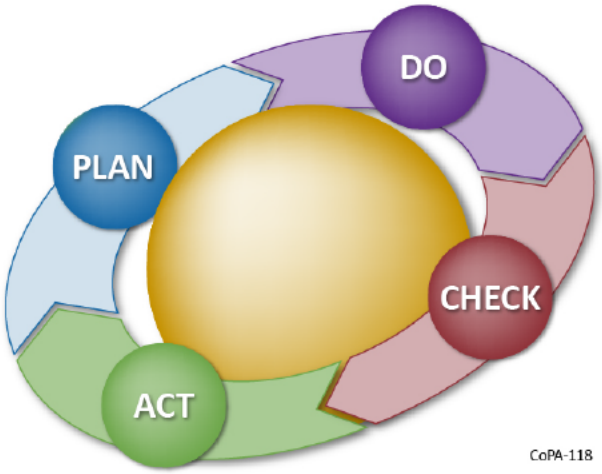


Figure 4-25. Plan-Do-Check-Art Cycle

The quality planning PDCA cycle requires input from each of the highly matrixed organizations and processes in the Commonwealth IT Infrastructure. Input will be proactively obtained from the Commonwealth agencies; Unisys; third-party partners; and from the ITIL management processes: Service Request, capacity and performance, incident and problem, change and release, availability, Service Level management; monitoring and automation tools; and CSAT surveys. The outputs of each phase of the PDCA cycle provide the inputs to the subsequent phase. The SEO will proactively manage this PDCA during transition as well as through the Steady State IT Service Delivery processes.

Continuous Service Improvement

Continuous service improvement and quality will be the key objectives of the SEO. The SEO's objectives will be to focus on increasing efficiency, maximizing effectiveness, and optimizing the cost of Commonwealth IT services and the underlying IT Service Management processes while maximizing customer satisfaction. Unisys will continually align and realign IT services with the changing business needs of the Commonwealth agencies by identifying and implementing improvements to IT services that support business processes. The SEO reviews, analyzes, and makes recommendations on improvement opportunities in each ITIL life cycle phase. These reviews, analyses, and recommendations will also leverage Six Sigma Lean methodologies to drive specific,

measurable results. We identify and implement individual activities to improve IT service quality and improve efficiency and effectiveness of the ITIL processes. Quality standardization will be a major objective for the SEO. This will improve the cost-effectiveness of delivering IT services to the Commonwealth while driving service excellence and maximizing customer satisfaction.

We will accomplish these Continuous Service Improvement objectives by listening to the voice of the customer, building effective relationships, learning each agencies business goals and priorities, leading and proactively managing ITIL processes, and delivering high-quality services to the Commonwealth, while leveraging ISO-certified processes as well as best in class industry tools and methodologies. The SEO will manage key Continuous Service Improvement activities to make sure Unisys is meeting the Commonwealth's IT service objectives, and driving quality and client satisfaction in each Commonwealth agency and its clients. The SEO will review management information and trends to verify that services meet agreed service levels and to make certain that the output of the ITSM processes achieve the desired results. Unisys will leverage Six Sigma Lean practices to drive definitive results. Conducting maturity assessments against the process activities and roles to highlight areas of improvement or concern also will be a key focus, along with internal audits to verify compliance. Six Sigma Lean, Kaizen workshops will be periodically conducted to identify and prioritize Continuous Service Improvement opportunities, analyze data, and present recommendations to senior management to make sure that Unisys is hearing the voice of the customer and meeting the Commonwealth's expectations. We will conduct Quality Management Reviews to consistently drive value to the Commonwealth, through improved services, quality, client satisfaction, customer value, and return on investment, while lowering overall IT costs.

The Unisys Resolution Optimization Model in **Figure 4-26** provides a clear example of how Unisys will provide Continuous Service Improvement to the Commonwealth. The Unisys SEO organization will proactively manage IT incidents, problems, and changes through ITIL Service Management processes and operations. We will leverage ISO-certified processes and Six Sigma Lean tools to drive quality as well as client satisfaction. The quality management processes will be standardized and integrated across all IT domains, the Commonwealth agencies, Unisys, IBM, Deloitte, and the Small Diverse Businesses.

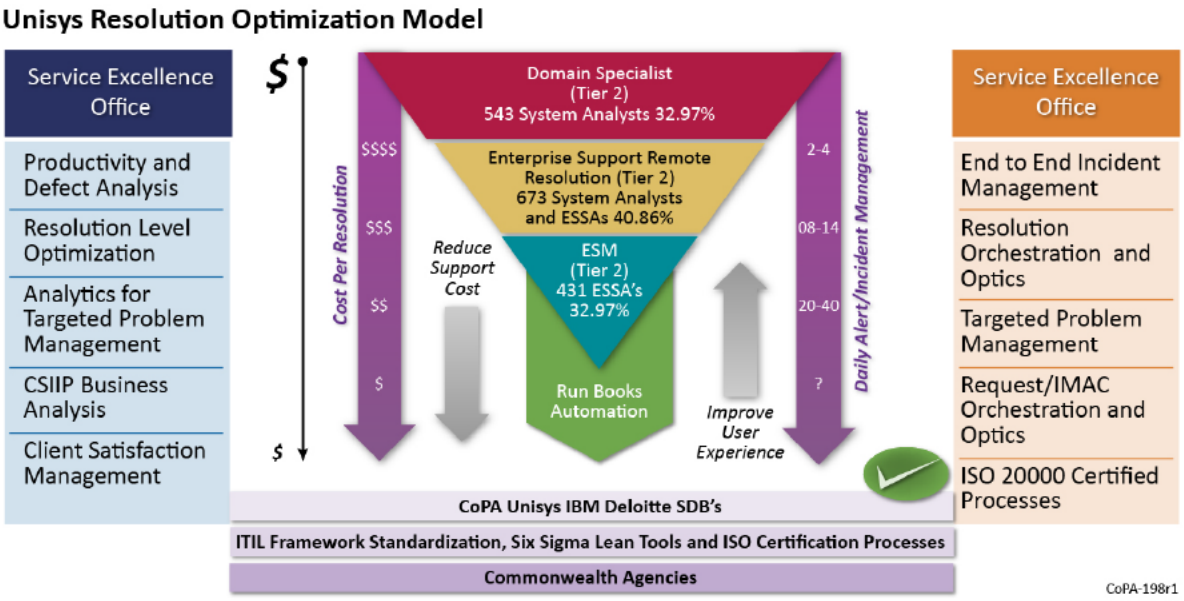


Figure 4-26. Unisys Resolution Optimization Model

A CSIIP SharePoint portal will be created and maintained to include all improvement and innovation actions. This CSIIP portal will be accessible to all the Commonwealth agencies, and will drive transparency for the Commonwealth. The SEO and SSL team will also support innovation activities managed through Innovation Workshops that collaborate with the Commonwealth agencies to plan and develop the future IT strategies and IT solutions. This governance, transparency, and innovation will drive lower cost of ownership and are outlined in **Figure 4-27** and **Figure 4-28**.

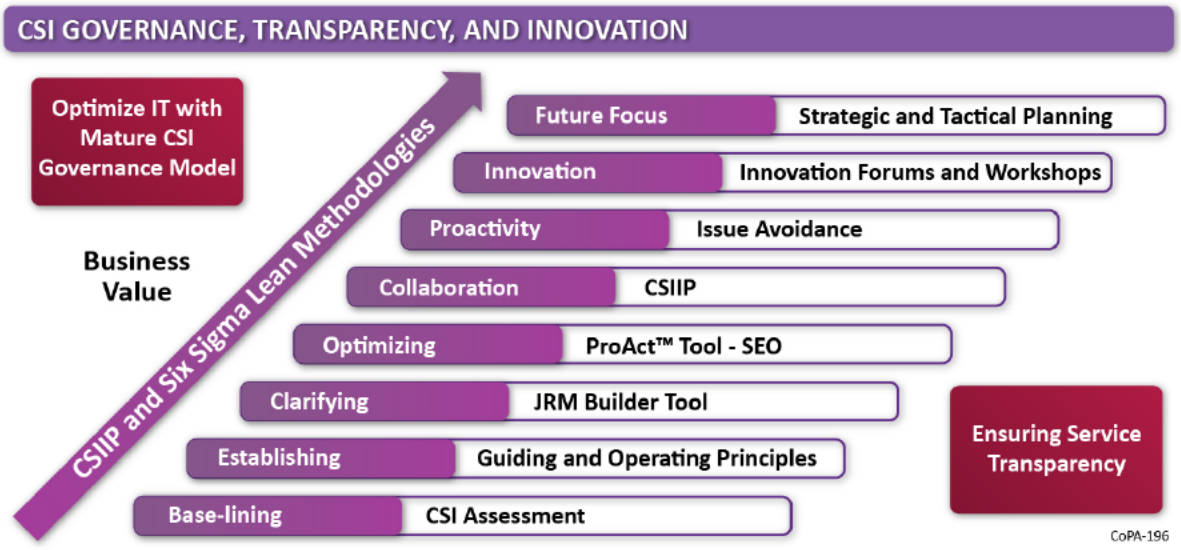


Figure 4-27. Continuous Service Imporvement Governance, Transparency, and Innovation

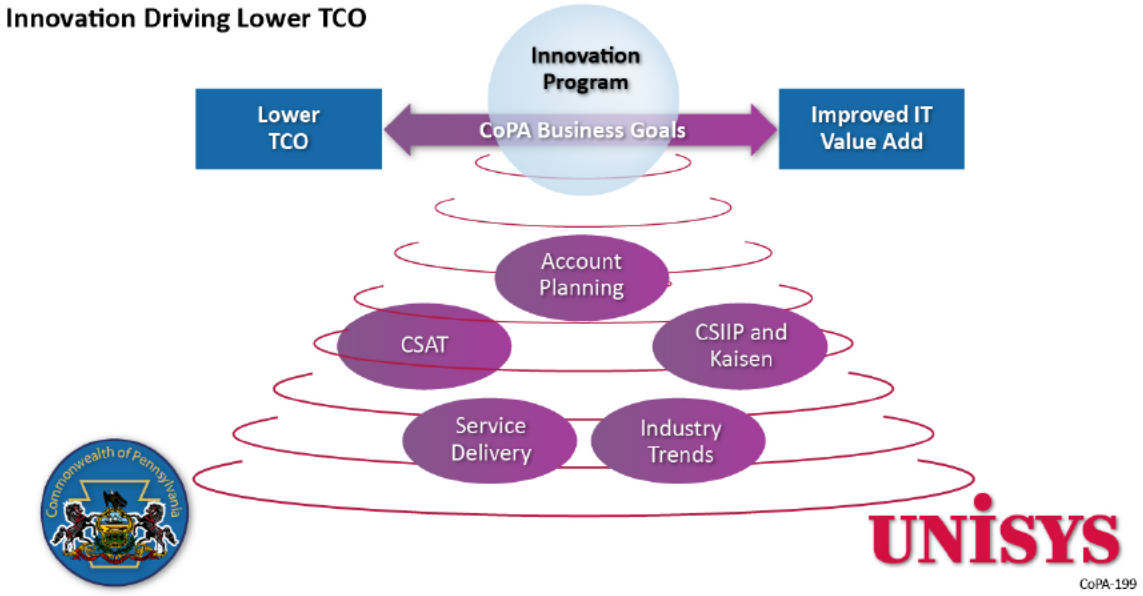


Figure 4-28. Innovation Driving Governance, Transparency, and Innovation

Risk Management and Independent Quality Audits, and Business Continuity Management

Risk management, independent quality audits, and business continuity management are integral Quality Management processes. Unisys is committed to managing risks and making sure that business objectives are achievable and that these processes are followed. Risk mitigation occurs through the implementation of tight quality controls: standard policies, procedures, roles, and Risks, Assumptions, Issues, and Definitions (RAID). Unisys will manage multiple risk registers for large projects, changes, implementations, and transitions. We also will manage an overall Program Risk Register. The risk types, tools, analyses, and processes are outlined in **Figure 4-29**.

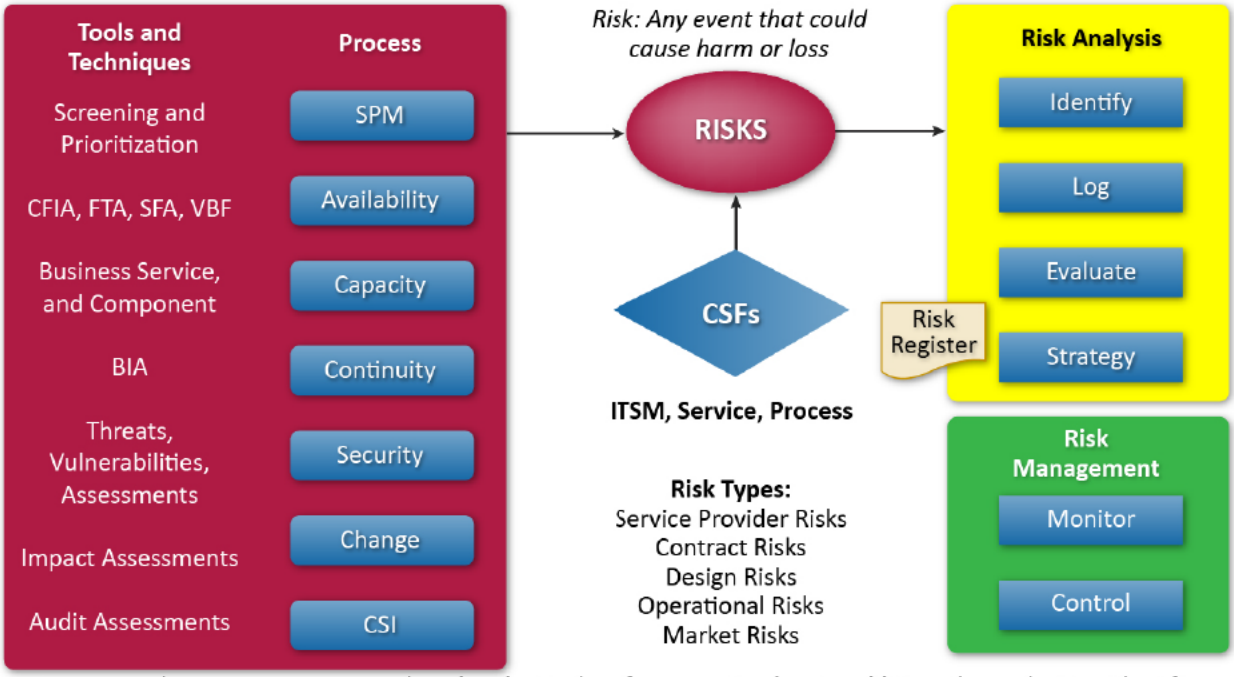


Figure 4-29. Risk Types, Tools, Analyses, and Processes

The Project Quality Office (PQO) is the independent organization at Unisys chartered as the key quality advisor to the operating groups on deal structures, risk management, and project performance. The PQO reviews and evaluates all aspects of proposals and project engagements with the goal to minimize risk while maximizing client satisfaction over the entire life cycle.

Unisys will work with the Commonwealth to conduct two types of project reviews—Project Readiness Reviews (PRRs) and Quality Assurance Reviews (QARs) to identify any potential problems or gaps.

The PRR is designed to confirm that the project is properly planned; the project plans are sufficiently adequate, accurate, and detailed; the project's contracted solution can be delivered on time and on budget; and the appropriate risk management is included (identify approaches to manage or mitigate risks). Unisys will conduct these reviews during major project implementations. Conduct of PRRs will occur specifically during transition to confirm providing a high-quality solution and implementation.

Unisys will also work with the Commonwealth to conduct QARs. They will be performed periodically by independent reviewers who are not part of the Unisys account team. This process provides a second level of quality and risk review using individuals who are independent of the Unisys client-serving team. This process also provides an unbiased view

of engagement progress, risk management actions, client satisfaction, and advice on solving problems and making improvements. The client interview is part of the QAR process.

Business Continuity Management (BCM) is an integral aspect of Corporate Governance and Unisys Quality Solution. BCM includes key areas of disaster recovery, facilities, risk, HRM, supply chain, quality, health and safety, knowledge, emergency, Security Management, crisis communication and public relations. Unisys provides for three levels of business continuity — basic, custom, and emergency. We will work with the Commonwealth to confirm that we provide comprehensive BCM program management; maintain a suitable BCM policy; confirm that decisions are made based on Business Impact Analysis (BIA); and create a Business Continuity Plan, and a Crisis Management Plan, and a Resource Recovery and Solution Plan. The implementation of Recovery Plans will follow a defined and approved risk assessment methodology. Every Business Continuity Plan, Resource Recovery and Solution Plan, and Crisis Management Plan will be tested at least once a year.

Risk management, independent program quality office audit reviews, and business continuity planning are key programs that Unisys will provide and manage in order to minimize risk throughout the ITIL lifecycle phases.

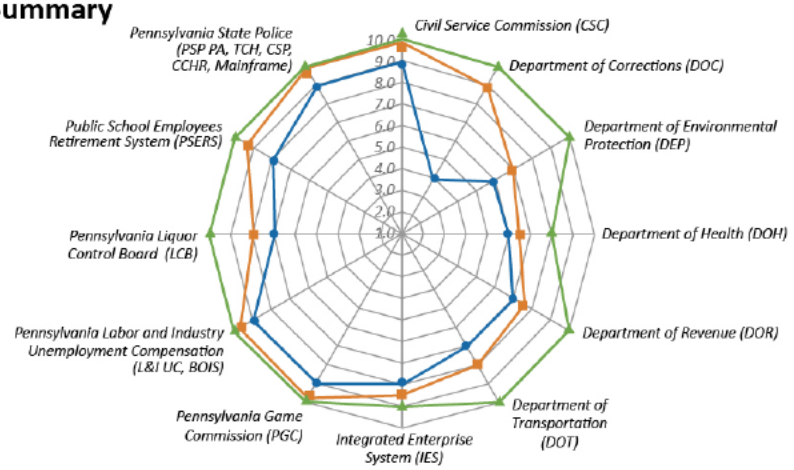
Client Satisfaction

Providing best-in-class ITIL-based IT service management and driving excellent client satisfaction is extremely important to Unisys and a key focus in our IT solution. The SEO will manage a multipronged approach to client satisfaction. We will gather data across multiple levels to gain a clear understanding of the Commonwealth's satisfaction with the IT services being provided. The Service Desk will randomly survey Commonwealth customers who call to the Service Desk with a request or change that needs to be completed or an incident that needs to be resolved. A Knowledge Management Portal will be developed to allow for direct feedback from Commonwealth agencies. A formal Customer Satisfaction Survey will be conducted quarterly to clearly understand the customer satisfaction of each agency and all of the ITIL service management operations areas. Unisys is currently providing these results to the Commonwealth. An example of these CSAT Survey summaries by agency and operational area are shown in **Figure 4-30**. Client-facing Leadership meetings between the Commonwealth CSAT Director and the Service Excellence Officer will be conducted quarterly to review this summary and the corresponding results from the multipronged input gathered in this robust CSAT process. Specific CSAT Action Plans will be documented and implemented to drive rapid service improvement if a remediation plan is required. This detailed CSAT process, analysis, and proactive communication will drive improved quality and greater transparency, while significantly improving the customer experience.

DPH Agency Satisfaction Survey Summary

Overall Agency Satisfaction 2012

Agency	Average
Civil Service (CSC)	9.9
Game Commission (PGC)	9.9
State Police (PSP)	9.9
Labor and Industry	9.8
Retirement System (PSERS)	9.5
Correction (DOC)	8.7
Revenue (DOR)	8.6
Integrated Enterprise System (IES)	8.4
Liquor Control Board (LCB)	8.3
Transportation (DOT)	8.2
Environmental Protection (DEP)	7.8
Health (DOH)	6.5
Agency Overall Satisfaction Rating	***8.8***



Satisfaction by Service 2012

Service Area	Average
System Availability	9.4
Communications	9.1
Technical Support	9.0
Online Subsystem Availability	8.9
ITIL/ITSM7	8.8
Project Management	8.8
Batch Processing	8.8
Disaster Recovery	8.6
Responsiveness	8.6
Capacity Planning	8.6
RFS Change Order Process	8.4
Help Desk	8.4
Agency Overall Satisfaction Rating	***8.8***

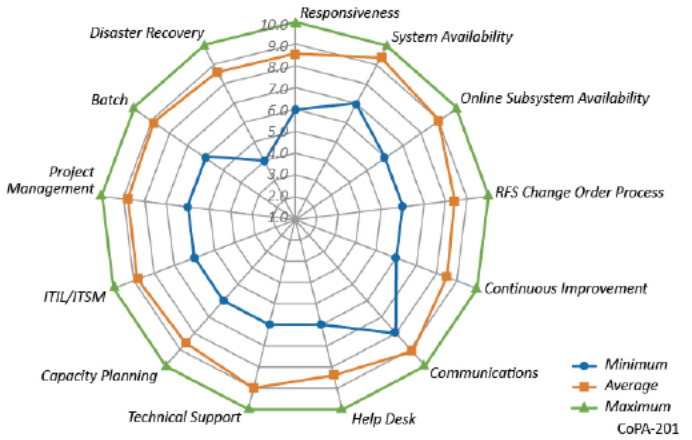


Figure 4-30. Current DPH Agency Satisfaction Survey Summary

Reduced Cost

Unisys is committed to providing the Commonwealth with best in class IT Services managed and driven by a dedicated SEO. The SEO will drive Continuous Service Improvement throughout the ITIL lifecycle. Standardization of ITIL frameworks, along with leveraging ISO-certified processes and Six Sigma Lean tools will drive Continuous Service Improvements. Governance, Transparency, and Innovation Workshops will make sure that the Commonwealth agencies plan and develop their future IT strategies and IT solutions. Risk management, independent quality audits, and business continuity planning will minimize risk throughout the ITIL lifecycle phases. Our multipronged Customer Satisfaction processes will confirm that Unisys clearly understands the voice of the customer and will drive high-quality continuous improvement actions based on collaborative feedback. All of this collectively represents the Unisys Integrated Quality Plan for the Commonwealth. This plan will provide the Commonwealth with the highest client satisfaction experience, best-in-class high-quality IT services and ITIL processes, and a significant lower total cost of ownership, as reflected in **Figure 4-31**.

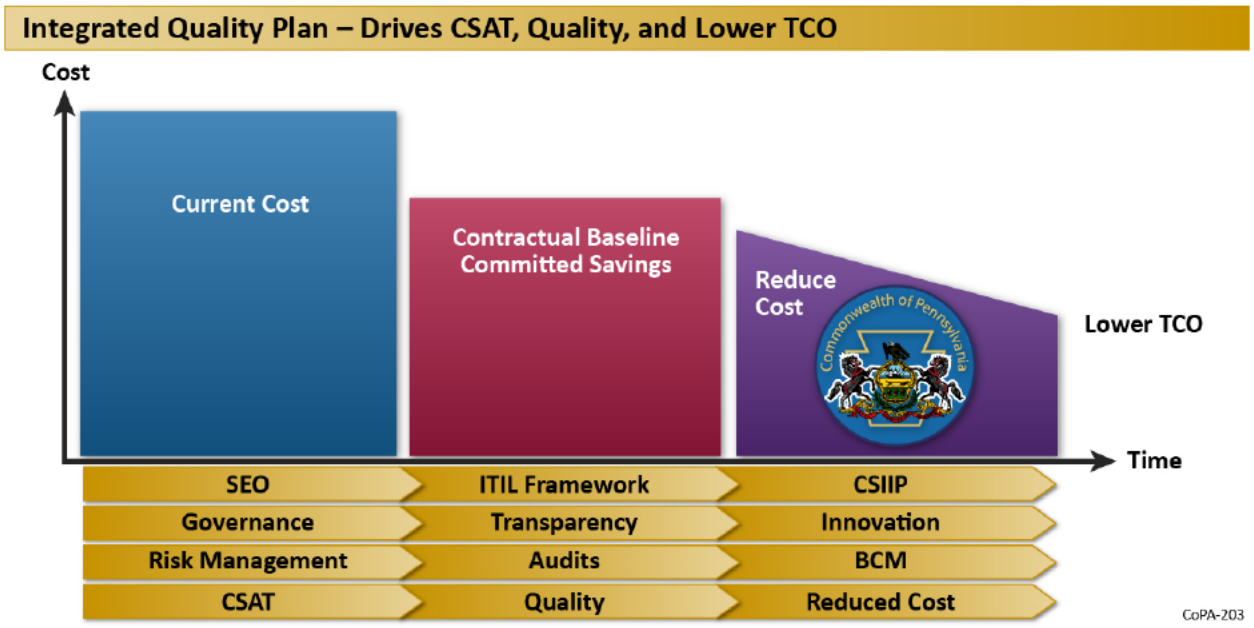


Figure 4-31. Risk Types, Tools, Analyses, and Processes

4.4.5 Summary of the Unisys Dedication to Quality

Unisys is joined by a premier team of experienced companies that were selected in accordance with the requirements of the RFP. Our selection criterion was to assemble a "best-of-class" team to meet all the requirements of the Commonwealth.

Unisys, headquartered in Pennsylvania, plays a leadership role in various market segments, in setting industry standards, and in charting the direction of industry practices and technology. More than 300 of our employees participate in industry standards groups

The ability to sustain quality of service while continually innovating and introducing cost and operational efficiencies is crucial for IT outsourcing providers. The acknowledgement Unisys has received demonstrates our clients' and the market's recognition that Unisys is in the front rank in delivering those benefits consistently around the world.

We believe the combination of the expertise of our local Harrisburg staff, our experience on similar projects (including our engagements at the Commonwealth Enterprise Data Center and Data PowerHouse), and Unisys proven processes and procedures founded on ITIL process and standards form a solid foundation for a partnership with the Commonwealth and differentiate Unisys from all other potential service providers.

Unisys looks forward to partnering with the Commonwealth on this very important opportunity. Our experience as a recognized global leader in designing, installing, and

managing IT infrastructure combined with the Commonwealth's vision, guidance and oversight will further maximize network and system availability achieving the Commonwealth's primary mission of ensuring a seamless delivery of all IT services to the citizens of Pennsylvania.

4.5 Client References

RFP	*Requirement*
	The Offeror must provide at least three (3) customer references for projects similar to this Project using Appendix C – Project References. If the Offeror is using subcontractors to provide a significant portion of services, each subcontractor must also provide at least three (3) references. To the extent possible, references should be selected to represent projects of similar size and complexity to the project described in this RFP. The Commonwealth at its sole discretion may request references from any or all proposed subcontractors.

4.5.1 Project References (RFP Appendix C)

Unisys provides the Commonwealth with at least three customer references and each of our proposed subcontractors are presented using the format outlined in RFP Appendix C – Project References. The customer references presented here are for projects of similar size and complexity to the Commonwealth of Pennsylvania's Data Center Computing Services Project as described in the RFP. **Table 4-3** provides details at a glance of the experience Unisys and our proposed key business partners have as it relates to the requirements of the Commonwealth.

Table 4-3. Unisys Team Experience

		Unisys							Deloitte			IBM		
		CoPA DPH	Defense Information Systems Agency	California State University	Internal Revenue Service	City of Minneapolis	American Red Cross	London Metropolitan Police	CoPA DPW	State of Utah	Commonwealth of Massachusetts	CoPA DPH (Unisys)	State of Georgia	State of Washington
Users -->		73,000	250,000	490,000	50,000	3,600	20,000	33,000	300,000			73,000	45,000	5,000
Additional Technical Services	Capacity On Demand	X	X	X	X	X	X	X				X	X	X
DR Infrastructure on Demand	Capacity On Demand	X		X		X							X	
Server Capacity on Demand	Capacity On Demand	X	X	X								X	X	X
Storage Capacity on Demand	Capacity On Demand	X	X	X	X	X	X					X	X	

		Unisys							Deloitte			IBM		
		CoPA DPH	Defense Information Systems Agency	California State University	Internal Revenue Service	City of Minneapolis	American Red Cross	London Metropolitan Police	CoPA DPW	State of Utah	Commonwealth of Massachusetts	CoPA DPH (Unisys)	State of Georgia	State of Washington
Datacenter Architecture and Technology	Datacenter Architecture and Technology		X	X		X	X				X	X	X	X
Facilities Architecture/ Maintenance	Facilities Management	X	X	X		X	X	X						
Site Operations	Facilities Management	X	X	X		X	X	X				X	X	X
Database Management Services	Managed Hosting Services	X	X	X		X		X	X			X	X	X
ERP Hosting - SAP / Oracle	Managed Hosting Services	X	X	X		X		X				X	X	
Limited Use Collocation Services	Managed Hosting Services		X				X	X						
Mainframe Services	Managed Hosting Services	X	X		X			X				X	X	X
Security and Firewall	Managed Hosting Services	X	X	X		X	X		X				X	X
Storage Management	Managed Hosting Services	X	X	X	X	X	X	X				X	X	X
UNIX Support - AIX / Linux	Managed Hosting Services	X	X			X	X	X				X	X	X
Windows Support	Managed Hosting Services		X	X		X	X	X					X	
Multi Datacenter Environment	Multi Datacenter Environment		X	X	X	X	X	X						
Data Protection	Network and Security Architecture	X	X	X			X	X	X		X		X	
Network and Security Architecture	Network and Security Architecture	X	X	X		X	X	X	X		X		X	
Third party License Management	Program and Service Management	X	X	X	X			X				X	X	X
Account Management	Program and Service Management	X	X	X		X	X	X				X	X	X
Additional Planning Services	Program and Service Management	X	X	X	X	X	X	X				X	X	X

		Unisys							Deloitte			IBM		
		CoPA DPH	Defense Information Systems Agency	California State University	Internal Revenue Service	City of Minneapolis	American Red Cross	London Metropolitan Police	CoPA DPW	State of Utah	Commonwealth of Massachusetts	CoPA DPH (Unisys)	State of Georgia	State of Washington
Availability / SLA Management	Program and Service Management	X	X	X	X	X	X	X				X	X	X
Business Partner Management	Program and Service Management	X		X		X							X	
Change and Release Management	Program and Service Management	X	X	X		X	X	X				X	X	X
Configuration Management	Program and Service Management		X	X		X	X	X	X			X	X	X
Continual Service Improvement	Program and Service Management	X	X	X		X		X	X			X	X	X
Financial Management	Program and Service Management	X	X	X		X	X	X			X	X	X	X
Governance and Policy Compliance	Program and Service Management	X	X	X	X	X	X	X			X	X	X	X
IT Service Continuity Architecture	Program and Service Management	X	X	X		X	X	X					X	
PMO and Contract Maintenance	Program and Service Management	X	X	X	X	X	X	X	X	X	X	X	X	X
Service Desk	Program and Service Management	X	X	X	X	X	X						X	
Subcontractor Management	Program and Service Management	X	X	X	X	X		X				X	X	X
Technical Architecture	Program and Service Management	X	X	X		X		X				X	X	X
Technology Refresh	Program and Service Management	X	X	X	X	X	X	X	X			X	X	X
Capacity Management	Technical Services	X	X	X		X	X	X				X	X	X
DR Planning and Testing	Technical Services	X	X	X		x	X	X				X	X	X
Infrastructure Architecture	Technical Services	X	X	X		X		X	X		X	X	X	X

		Unisys							Deloitte			IBM		
		CoPA DPH	Defense Information Systems Agency	California State University	Internal Revenue Service	City of Minneapolis	American Red Cross	London Metropolitan Police	CoPA DPW	State of Utah	Commonwealth of Massachusetts	CoPA DPH (Unisys)	State of Georgia	State of Washington
Performance Monitoring and Management	Technical Services	X	X	X		X	X	X	X			X	X	X
Security Management	Technical Services	X	X	X		X	X	X	X	X	X		X	X
Transition Management (new customer and or services)	Technical Services	X	X	X	X	X	X	X				X	X	X
Security Transaction Activities	Transition	X	X	X			X	X	X	X			X	X
Transition Program Management	Transition	X	X	X		X	X					X	X	

4.5.2 Unisys Project References

Unisys Project Reference 1: Commonwealth of Pennsylvania

Name of Client & Project Title	Commonwealth of Pennsylvania – Data PowerHouse (DPH) Outsourcing Agreement
Contract Value	$1.4 billion
Nature and Scope of Project:	**Project Description** In 1997, Governor Tom Ridge pressed forward to improve the delivery of public services through the strategic use of information technology. The Governor's Office of Administration initiated a data center consolidation contract for Commonwealth agencies titled Data PowerHouse (DPH). Unisys has provided the Commonwealth with data center computing services for the DPH and application support services for the Enterprise Data Center (EDC) since 1999. This effort consolidated and outsourced the operations and technical support of 17 formerly separate state agency Data Centers. The DPH, managed by a consortium of 10 companies, led by Pennsylvania-based Unisys, replaced these 17 separate state-run data centers. Unisys uses Information Technology Infrastructure Library (ITIL) standards in the DPH. All Unisys staff that work on the DPH contract are familiar with the key elements, concepts, and terminology used in the ITIL Service Lifecycle and have achieved (at a minimum) ITIL V3 Foundation certification. **Program Management Office (PMO) and Service Management** **Project/Contract Management –** Ann Kirwan-Orner, Unisys Client Account Executive, is responsible for the overall program, projects, and contract elements associated with the DPH contract. Operating under Ann's direction, the Unisys executive management team maintains an active working relationship with the Commonwealth's project team. Unisys hosts a Monthly Service Performance Management Meeting that provides the Commonwealth with an opportunity to review and discuss project performance and on-going initiatives. The Request for Service (RFS) / Change Order (CO) system used by Unisys was developed in conjunction with the Commonwealth and has been customized over time to meet its evolving needs. The process begins with an RFS initiated by the agency though their assigned Unisys Service Delivery Manager (SDM) and OA Enterprise Services Representative (ESR). The SDM schedules a meeting to gather requirements. After the meeting, a RFS document is created and submitted to the agency for review. Unisys creates the supporting documentation and cost information after the requirements have been finalized by the agency. After the agency, OA ESR, and Unisys SDM have approved the final RFS and associated cost a change order is generated. Upon approval of the change order by OA Contract Compliance, Unisys moves forward to implement the required change. **Availability/SLA Management –** Under the DPH contract, each month Unisys reports to the Commonwealth on 445 Service Level Agreements (SLAs). Unisys provides multiple service tiers (i.e. Gold, Silver, and Bronze) and associated service levels within each service offering. This has provided the Commonwealth with the ability to contain costs by selecting the appropriate level of service that meets its specific needs. Unisys employs a quality and process improvement program that focuses on both meeting and exceeding targeted SLA requirements. In the event that an SLA is missed, Unisys investigates the

Name of Client & Project Title	Commonwealth of Pennsylvania – Data PowerHouse (DPH) Outsourcing Agreement

problem to determine the root cause and takes action to implement changes to correct the underlying issue.

Change and Release Management – Unisys works in partnership with the Commonwealth to manage all changes that occur in the DPH. Each Unisys SDM holds regular change management meetings with the designated representatives of their assigned agency. In addition, Unisys reviews major changes during the monthly Service Management Meeting attended by OA/OIT and the agencies. Unisys uses the BMC Remedy IT Service Management (ITSM) application to track and manage changes and releases in the DPH. All changes in the DPH require approval by the appropriate authorized Commonwealth representatives prior to implementation. Authorized Commonwealth staff members have direct access into the BMC Remedy ITSM 7.6.4 application maintained by Unisys.

Service Desk – Unisys provides a service desk to the Commonwealth to assist appropriate authorized Commonwealth users in determining, tracking and resolving questions regarding the services we provide. Unisys uses the Incident Management, Problem Management, Change Management, Asset Management, and Change Project modules of the BMC Remedy ITSM 7.6.4 application to support service desk business processes. Unisys developed, updates, and maintains documentation of service desk policies and procedures. The service desk is staffed by individuals with knowledge of the systems that support the Commonwealth's mission critical business applications.

Technical Architecture – Unisys provides the Commonwealth of Pennsylvania with dedicated Technical Architects that oversee the ongoing design of the various computing platforms that support the Commonwealth's existing computing topologies. These Technical Architects understand the unique business and technical needs of each Commonwealth agency. Their understanding of available technology provides them with the knowledge they need to recommend technology changes that result in cost effective solutions that provide increased performance on behalf of the Commonwealth.

Account Management – Unisys has assigned a Service Delivery Manager (SDM) to each of the Commonwealth agencies that receive services in the DPH. The SDM works with the agency and OA/OIT to coordinate projects and address contract questions. The average Unisys SDM has more than 5 years experience supporting the Commonwealth.

Configuration Management – Unisys employs a robust Configuration Management system that ensures complete and accurate recordkeeping relative to datacenter assets (e.g. hardware, operating system software, firmware, and network) contained in the DPH.

Third Party License Management – Unisys provides the Commonwealth with Third Party License Management services related to the numerous hardware and software platforms and products required to support the DPH infrastructure. Our services ensure accurate inventory and licensing compliance for almost 60,000 individual machine or user licenses for more than 100 distinct infrastructure software products. Unisys proactive third Party License Management has resulted in cost savings and credits to the Commonwealth in the amount of $537,382 since 2011.

Technology Services

Transition Management – Beginning in 1999, Unisys successfully consolidated 19 individual Commonwealth owned Data Centers serving 17 agencies into the DPH. This was accomplished within the timelines established by the Commonwealth and with no unplanned disruptions to the agencies involved. In 2008, Unisys commenced with a comprehensive technology refresh initiative to provide updated computing, storage, and

Name of Client & Project Title	Commonwealth of Pennsylvania – Data PowerHouse (DPH) Outsourcing Agreement

networking platforms as a result of the Commonwealth extending the DPH contract. This transition involved detailed planning for procurement, infrastructure build out, testing, and workload migration affecting every Commonwealth agency within the project. Unisys demonstrated strong transition management experience utilizing a Project Executive and several Project Managers to work closely with the agency to minimize the business impact of each workload transition. The only major issue encountered during the transition project was a mainframe configuration setting that affected workload performance for the DOT partition. Unisys conducted research to identify the root cause of the problem and implemented corrective action. After action, reviews were conducted to capture lessons learned.

Infrastructure Management – Unisys IT infrastructure services include system engineering, network management and support, data center operations, data storage/archiving, information security engineering, application hosting, disaster recover (DR) services, and systems certification and accreditation.

Capacity Management – Unisys uses automated tools to continuously monitor resource utilization in the DPH. DPH capacity utilization for each agency is reported to the Commonwealth on a monthly basis. These reports show usage, trends, capacity forecasts, and provides recommendations for upgrades when necessary. Reports are segmented by platform (e.g. IBM/Unisys Mainframe, IBM iSeries, etc). Unisys works in conjunction with the Commonwealth to produce a comprehensive capacity planning report on an annual basis. This report includes input gathered from the agencies regarding changes in business requirements that may drive the need for additional or reduced capacity in the future.

Disaster Recovery Planning & Testing – Unisys worked with the Commonwealth to plan and implement a backup/disaster recovery (DR) plan to protect critical IT resources from disasters. Unisys provides the Commonwealth with a 2,900 sq. ft. DR site in southeastern Pennsylvania. Each agency is able to receive DR services specific to its individual needs. Unisys works closely with each agency that receives DR services to coordinate and conduct regular DR testing to ensure that everything will work smoothly in the event of an actual disaster.

Security Management – The information security management system Unisys employs on behalf of the Commonwealth on the DPH project has been ISO/IEC 27001:2005 certified continuously since 2009. Unisys conducts annual audits of the DPH and reports the results to the Commonwealth. Unisys recently moved from using the SAS 70 auditing standard to using the more comprehensive and expansive SSAE 16 standard. Unisys complies with applicable Commonwealth IT policies and directives as well as applicable federal and Commonwealth laws, regulations and policies. All Unisys staff assigned to the DPH attends mandatory security training on an annual basis. This includes training to address the specific security and compliance needs of the Commonwealth.

Performance Management & Monitoring – Unisys monitors systems environments in the DPH on a 24X7X365 basis using industry standard tools (e.g. MS SCOM, nWorks, SightLine, TeamQuest, and Tivoli) to ensure availability and capacity is adequate for the workload. These tools provide the critical input needed to calculate SLAs, and for associated monthly evaluation and reporting needs.

Facilities Management

Facilities Maintenance – Unisys maintains two geographically dispersed data centers to provide the Commonwealth with protection from regional disruptions such as weather, power or other emergencies. The DPH is the primary data center and is a 21,980 sq. ft.,

Name of Client & Project Title	Commonwealth of Pennsylvania – Data PowerHouse (DPH) Outsourcing Agreement

tier 2 rated facility based on the current standard established by the Uptime Institute. As managed by Unisys, the DPH has been consistently performing at a tier 3 level. The DPH houses a separate dual-homed network interconnection. Unisys has upgraded intra-facility power distribution, battery backup systems, air conditioning, fire suppression, and security in the DPH. In addition to the DPH, Unisys provides the Commonwealth with agency specific Disaster Recovery capabilities needed to maintain mission critical data processing for 14 agencies' requirements through dedicated space established with SunGard at their Philadelphia site.

Site Operations – Unisys provides the datacenter operations staff and management required to operate and monitor the IT computing equipment and Services being provided in the DPH. Perry Pritchard, Unisys Data Center Manager, is responsible for the DPH and has been in this role for over 14 years. Mr. Pritchard and other Unisys staff regularly interface with Commonwealth staff to institute best practice datacenter services. Unisys datacenter operations in the DPH includes management of the computing platforms, storage, local area networking, security firewall, tape backup, and offsite tape rotation systems.

Managed Hosting Services

Windows Support – Unisys provides hosting, operations, and support services for Microsoft Windows based servers located in the DPH. This includes support for approximately 500 physical servers and 325 virtual servers that utilize virtualization technology from VMware and Microsoft's Hyper-V. All MS Windows servers, network devices, etc. are actively monitored on a 24X7X365 basis using industry standard tools such as MS System Center Operations Manager (SCOM) 2012. The Unisys staff that supports the MS Windows environment in the DPH hold industry recognized certifications from Microsoft, VMware, and Cisco among others. Unisys staff ensures that operating systems are maintained and that current patch levels are applied in accordance with agency requirements. If a service disruption occurs, Commonwealth users are notified and regularly updated via text message and e-mail.

Storage Management – Unisys manages over 1.6 petabytes (PB) of storage in the DPH on behalf of the Commonwealth. This includes management of storage technology from vendors such as EMC and IBM. Unisys provides trained staff members that hold manufacturer certifications from EMC, IBM, and Brocade.

ERP Hosting SAP/Oracle – The Commonwealth was one of the first states to fully integrate business processes in an SAP Enterprise Resource Planning (ERP) system across all state agencies. First implemented in 2002, the SAP ERP system efficiently and securely supports more than 53 state agencies and processes millions of finance, budget, procurement, supplier relationship, plant maintenance, payroll, travel, human resource and employee self service transactions monthly. The Commonwealth's Bureau of Integrated Enterprise System (IES) migrated the SAP ERP system to the DPH in 2010 and has entrusted Unisys with the care of its supporting infrastructure since that time.

UNIX Support AIX/Linux – Unisys provides hosting, operations, and support services for UNIX (i.e. AIX/Linux) based servers located in the DPH. This includes support for 147 virtual AIX images on 8 physical frames as well as 17 physical and 4 virtual Linux servers. All UNIX servers, network devices, etc. are actively monitored on a 24X7X365 basis using industry standard tools such as MS SCOM 2012. The Unisys staff that supports the UNIX environment in the DPH hold industry recognized certifications that include IBM Certified Expert, LINUX, and Oracle among others. Unisys staff ensures that UNIX operating systems are maintained and that current patch levels are applied in accordance with

Name of Client & Project Title	Commonwealth of Pennsylvania – Data PowerHouse (DPH) Outsourcing Agreement	
	agency requirements. If a service disruption occurs, Commonwealth users are notified and regularly updated via text message and e-mail. **Mainframe Services IBM/Unisys –** Unisys provides the Commonwealth with hosting and operational support services for both IBM and Unisys mainframe systems located in the DPH and SunGard. Support for five (5) Unisys Mainframe partitions in the DPH and three partitions at SunGard are provided directly by Unisys. Support for IBM Mainframe and IBM Midrange (i.e. IBM iSeries) partitions are provided by IBM under contract with Unisys. **Security & Firewall –** Unisys provides the Commonwealth with hosting and operational support services for security products and firewalls located in the DPH. **Database Services –** Unisys provides the Commonwealth with Database Management Services for the Unisys Mainframes located in the DPH. Mainframe Database services include mainframe software product line to manage database integrity and availability. Unisys also works with the agencies Data Base Administrators to back-up and restore critical Oracle databases. Early in the contract, Unisys also provided Oracle and MS SQL Database Services for various Commonwealth agencies located in the DPH. The Commonwealth subsequently made the decision to move these Database Management Services back in-house. **Capacity on Demand and Additional Services** **Exchange as a Service –** In 2008, as part of our ongoing Enterprise Exchange Management contract with the Commonwealth, Unisys transitioned the Commonwealth's messaging environment from centralized MS Exchange 2000 to Exchange 2007 for 85,000 users supporting 45 state agencies—an upgrade for 60,000 initial end users (which grew to 85,000 users). This transition created one of the largest state-hosted MS Exchange systems in North America. Unisys worked with MS in validating the migration effort. The complexity of this project included the complete messaging migration, on an agency-by-agency basis, from an earlier MS Exchange technology platform to Exchange 2007. Unisys installed all servers, implementing the MS Exchange environment. When the systems and servers went operational, Unisys successfully bid to support the MS Exchange system for the entire Commonwealth. During the migration to Exchange 2007, Unisys assessed all enterprise messaging infrastructure and technology at the Commonwealth's Enterprise Data Center (EDC) facility. We provided the required enterprise-wide utilization reports, including BlackBerry, MS Exchange, network, server (CPU, physical memory, disk utilization, and virtual memory), and MS Outlook Web Access. Unisys also provided weekly spam and antivirus detection reports as well as SAN utilization, storage allocation per cluster, and daily data backup reports. Unisys consultants are currently onsite managing and supporting the Commonwealth's Windows 2008 Active Directory, MS Exchange, BlackBerry, and Enterprise Data Center network and providing Tier 2 support to the agencies.	
Project Duration:	**Start Date Year:** 1999	**End Date Year:** 2014
Nature of the Client:	With more than $1 billion in information technology investments annually, the Commonwealth of Pennsylvania is the equivalent of a Fortune 20 organization providing a diverse portfolio of IT services and solutions to its 12.7 million citizens and business customers. The DPH project is managed by the Office of Administration, Office for Information Technology.	

Name of Client & Project Title	Commonwealth of Pennsylvania – Data PowerHouse (DPH) Outsourcing Agreement
Nature of Client Audience:	Employees and citizens of the Commonwealth of Pennsylvania
Number of Users:	73,000+ Commonwealth employees; 12.7 million citizens
# & Composition of Vendor Employees & Consultants Assigned:	**Vendor Project Manager/Key Consultant on Project Team:** Ann Kirwan, Client Account Executive Unisys provides a total staff of 99 dedicated staff members in support of the DPH. This dedicated staff is broken into 86 (on-site) and 13 (off-site) and is down approximately 30% from peak level. Unisys provides a total staff of 39 dedicated staff members in support of the EDC.
Client Contact Information:	**Reference Contacts:** **Name:** [redacted] **Title:** [redacted] **Department:** PA Office of Administration, Bureau of Enterprise Services **Full Address:** [redacted] **Telephone:** [redacted] **E-mail** [redacted] **Relation/Role to Project:** Mr. Salvaggio is currently the Service Portfolio and Quality Manager for the Bureau of Enterprise Services for the Governor's Office of Administration and has been in the role since May 2011. His role includes responsibility for interfacing with the Unisys management team in support of the Commonwealth's DPH contract to ensure service quality issues are addressed and that communication with agency customers are handled in timely and professional manner. **Name:** [redacted] **Title:** [redacted] **Department:** County of Franklin, Pennsylvania **Full Address:** 218 N Second Street, Chambersburg, PA 17201 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** [redacted] His role included responsibility for oversight of the Commonwealth's DPH contract with Unisys.

Unisys Project Reference 2: Defense Information Systems Agency (DISA)

Name of Client & Project Title	Defense Information Systems Agency (DISA) – Enterprise Services Directorate (ESD) ClearPath Managed Services, Mainframe and Mid-tier Technical and Application Support Services
Contract Value	$200+ million
Nature and Scope of Project:	**Project Description:** DISA's Enterprise Services Directorate provides excellent processing capability, systems management, communications and storage in support of Department of Defense services, agencies, and combatant commands. Located in 13 secure facilities strategically located throughout the world; Enterprise Services support more than three million users of more than 2,800 applications utilizing more than 25 petabytes of storage. Under the DISA Managed Services contract, Unisys provides all the required capacity and technical services to support DISA's Unisys ClearPath based workloads. The Managed Service includes Unisys ClearPath mainframes, EMC disk storage, DSI Virtual Tape, hardware maintenance, software licenses, software maintenance, and technical support. The DISA Mainframe and Mid-tier support contract requires contractor support to optimize Defense Enterprise Computing Center (DECC) Ogden operations, enhance customer support and ensure continuity of service. The scope encompasses all aspects of technical, application and operational support required by DISA DECC Ogden to include Unisys, IBM, and Server computer system hardware and software (system and functional application) management, system analysis, long-range capacity planning, problem resolution, disk and tape systems management and customer support. Unisys complies with all applicable DoD-approved architectures, programs, standards and guidelines. **Program Management Office and Service Management** **Project/Contract Management –** The Unisys Team established an accountable, integrated program management organization, staffed by experienced, quality personnel focused on supporting the DISA mission. Unisys implemented a Program Management Office (PMO) to coordinate all program efforts, leverage resources, and provide control and visibility of efforts. The Unisys approach to managing a task order is built on Program/Project Management disciplines that are blueprinted within the Unisys Services and Solutions Delivery Framework (SDF). The Unisys SDF Program Management methodology is designed as a framework to ensure that complex business needs are managed, governed and achieved. The tools and processes are designed to help effectively manage change and realize business benefits. With our Program Management framework, teams improve and control business assets through more effective governance of distributed teams and heterogeneous environments. **Availability/SLA Management –** Unisys provides a semi-annual Program Review to evaluate our service level agreements and provide our availability rates – our last availability rate (as of May 2013) was 99.998 percent. Unisys maintains a flexible, responsive, and supportive environment, engages appropriate stakeholders, provide DISA management with necessary insights, and provide the functions needed to support day-to-day and high-priority managed services objectives. **Change & Release Management –** Unisys has established a Quality Assurance organization at the Montgomery Support Center (MSC) to provide unit, regression, and

Name of Client & Project Title	Defense Information Systems Agency (DISA) – Enterprise Services Directorate (ESD) ClearPath Managed Services, Mainframe and Mid-tier Technical and Application Support Services

integration testing of all managed service components prior to deploying (releasing) to the production sites. A test environment mirroring the infrastructure of a production site is used at the MSC to conduct all unit, regression, and integration testing. Test plans are developed and are exercised for every major software component prior to release to the field. DISA customer applications and data are captured and loaded in the test environment to facilitate integration testing. Before any software updates are released to the field, the quality assurance group exercises the customer applications through automated scripts utilizing the Mercury LoadRunner tool to ensure compatibility with the fielded workloads eliminating any possible related update delays or downtime. Our release control maintains copy of every release made to our client.

Service Desk – Unisys customer service/operations support staff provide technical guidance, training, and hands-on problem resolution in resolving ITSM incidents assigned to the Service Desk. We analyze, troubleshoot, and resolve incidents that negatively affect production processing. We escalate incidents and report notifications of interruptions in accordance with documented procedures. We update incident status, track problems for turnover, and make appropriate entries into the Known Error Database for faster resolution in the future. We also assist with automated batch scheduling using both OpCon and Control M.

Technical Architecture – Unisys staff performs overall technical coordination support for the Ogden EPC and Defense DPS environments. We support the consolidation planning, system design, preparation, installation, and testing necessary to ensure minimal disruption to the overall EPC and DPS customer services. Additionally, the Unisys team supports the ongoing operational requirements such as maintenance windows and service recovery or restoration.

Account Management – Unisys provides a Customer Account Manager to oversee and support DISA Enterprise Computing Services. This position ensures the following functions are performed by the appropriate staff: Analyzing customer requirements; staffing technical solutions; preparing business case proposals to include preparing final costs, procurement, acceptance and delivery; and assisting project managers in the successful implementation of their projects.

Configuration Management – Unisys employs a Configuration Management (CM) Office that maintains copies of every product released. Unisys follows the CM standards set forth in ITIL V3 standards.

Technology Services

Transition Management – Unisys has executed transition plans at several locations with no unplanned disruption. Recently Unisys joined with DECC Ogden staff and another vendor to transition employees and workload without disruption and exceeded client expectations.

Infrastructure Management – The Unisys system administration team provides all system administrator functions for SUN Solaris and HP-UX servers maintained by DECC OKC. We support workstations and Entry-Level servers to Midframe/Midrange servers as well as High-End Servers like HP Itanium. Unisys Linux technical staff has multi-platform environment experience with the installation, configuration, and IA compliance of Linux. We support communication protocols used between IBM, Sun, and HP OEs, and the Web servers, network switches, routers, and NIPRNet WAN

Name of Client & Project Title	Defense Information Systems Agency (DISA) – Enterprise Services Directorate (ESD) ClearPath Managed Services, Mainframe and Mid-tier Technical and Application Support Services

connectivity and disaster recovery. We use the Tivoli Enterprise Management software, including Framework, Monitoring, Provisioning Manager, Netcool/OMNIbus, Enterprise Console, and Business Service Manager

Capacity Management – Unisys staff performs overall technical coordination support for the OKC Data Center environment and consolidation planning, design, preparation, installation and testing necessary to ensure DISA activities are accomplished with minimal disruption to the overall DECC OKC customer services. For example, we supported the implementation of the Defense Enterprise E-mail system, which has more than 1 million e-mail accounts and is saving the DOD millions of dollars by leveraging buying power for the entire DOD. Unisys performs sizing and capacity management to ensure DECC OKC can fulfill customer requirement in processing and storage capacity.

Disaster Recovery Planning & Testing – Critical to the operational readiness of the DECC Oklahoma City Unisys ClearPath based workloads, our team manages and address issues related to the data replication (SRDF and RecoverPoint) of ClearPath production data from Oklahoma City to the backup site in St. Louis and perform remote administration on the St. Louis COOP platforms. Unisys assists in planning and development of the Disaster Recovery (DR) process. Unisys personnel participate in the semi-annual DR testing by relocating to the St Louis site to perform touch labor as well remote system access. The Unisys System Administration team has direct access to Unisys Corporate resources, which ensures any situation that might affect ClearPath workload processing receives the appropriate attention by Unisys and our support vendors.

Security Management – The Unisys team provides IA support for the DECC Ogden environment consisting of OS2200 ClearPath, UNIX/Linux, and Windows servers, automated tape libraries, disk farms and SANs. We provide the IA Officer role for the OS2200 Dorado. Our constant oversight and IA maintenance has resulted in a spotless security record. Unisys personnel focus primarily on the security posture of the DECC Ogden Windows environment. This team was recently recognized for a clean SAE 16 audit opinion. Our seasoned professionals provide technical support for Windows XP and 2003/2008 Servers. Our IA team assists with the setup and necessary STIG application to prepare Windows servers for Enclave Connection Authority.

Performance Management & Monitoring – Unisys system management staff (one with TS/SCI) operates and administers the Unisys OS2200 mainframe processing environment. Our team designed and deployed the Automated Message System (AMS/SMART) decision support rules that automate console operations and eliminated human intervention requirements. We also design, construct, deploy, and manage configurations for the Dorado Single Point Operations environment. Unisys supports long-range capacity planning to assess hardware limitations and capabilities for new or increased workloads. Unisys provides hardware configuration and implementation for IBM, Server, and Unisys Dorado OEs that include modeling, sizing, and interpreting data produced by TORCH software.

Facilities Management – Unisys has been supporting DISA Defense Enterprise Computing Center (DECC) Ogden since 1992 and providing centralized information system processing services to DISA's diverse and geographically dispersed DoD customer base. Working under the terms of HC1028-08-D-2027-03, our Unisys Team provides support for all types of DoD customer requirements across Unisys, IBM, HPUX, Solaris, Linux, and Windows operating environments (OEs) and the backend

Name of Client & Project Title	Defense Information Systems Agency (DISA) – Enterprise Services Directorate (ESD) ClearPath Managed Services, Mainframe and Mid-tier Technical and Application Support Services

databases they drive. Our Unisys team provides the full and comprehensive range of technical services including all aspects of system design, configuration, deployment, administration and capacity planning. Our team provides DISA and DISA's customers with 24x7x365 response to their complex technical concerns.

Managed Hosting Services

Windows Support – Unisys provides Windows system administration staff supporting performance tuning, Veritas backup solutions, and RAID implementation using fiber channel storage mediums and SANs for enterprise scale networks. We verify that DECC Ogden assets comply with all IA requirements within their scope of responsibility

Storage Management – Unisys provides support for implementation and daily maintenance of large scale Storage Area Networks (SAN) and Backup capabilities in a secure environment for all sites assigned to DECC OKC. We maintain the SAN for the assigned sites/projects in a Hitachi centric environment and provide guidance to government staff in the effective management of large-scale SANs. We work with government personnel through the use of in-place Change Management (CM) processes for all modifications to the SAN infrastructure, both hardware and software and coordinate with maintenance personnel for modifications to all components of the SAN. Unisys assists in development of Logical Unit Number (LUN) presentations and all SAN troubleshooting efforts. We make all required changes to the SAN fabric using existing CM processes and assist vendor personnel in the maintenance or interruptions of the SAN fabric. Unisys monitor on a daily basis all backup activities for all responsible sites and correct all backup processing anomalies or notify SA personnel of all unresolved problems encountered with backup processing. We provide various modifications, as required, to backup routines and provide reports of those activities. Unisys performs complete and accurate weekly vaulting runs and maintains backup software catalogs. Unisys works with other technicians performing technical refresh in the backup processing environment.

ERP Hosting SAP/Oracle – Unisys supports Level 2 applications and Sustainment Liaison for SAP, BW, CRM, Portal, Crystal Enterprise, and Netegrity SiteMinder. We coordinate between development and production for releases and system changes. Unisys conducts daily application checks - perform follow-up tasks as needed. We maintain alert and event management configuration and respond to event management alerts. We monitor and respond, as appropriate, to problem management and service requests through the problem management and service request systems. Unisys provides consultative assistance related to system level activities. Unisys develops and maintains requisite documentation and standard operating instructions. Unisys monitors products within a SAP/Manugistics environment using system monitors such as Windows Event logs, log files. We monitor products within the Citrix environment using software tools, monitors, and products within the ERP environment. Report any irregularities to the TAO. Unisys personnel performs on call functions as required and be available during such periods 24x7.

UNIX Support AIX/Linux – Our UNIX system administrators (one with TS/SCI) provide all standard system administration functions for Sun Solaris/HP-UX servers maintained by DECC Ogden. The Unisys team includes recognized SMEs in both the HPUX and Solaris that represent DECC Ogden on the Server Technical Advisory Group and

Name of Client & Project Title	Defense Information Systems Agency (DISA) – Enterprise Services Directorate (ESD) ClearPath Managed Services, Mainframe and Mid-tier Technical and Application Support Services

support the most difficult issues. Our Solaris SME authored scripts that allow Service Desk personnel to correct issues without engaging technical support. Additionally, scripts were written for the high availability function saving $25,000 in software costs.

Mainframe Services – Under the DISA Mainframe and Mid-tier support contract, Unisys supports the DECC Ogden operations, enhance customer support and ensure continuity of service of the Unisys Mainframe environment. This includes support for the Unisys ClearPath and Dorado mainframe systems. Our Unisys team provides the full and comprehensive range of technical services including all aspects of system design, configuration, deployment, administration and capacity planning. Our team provides DISA and DISA's customers with 24x7x365 response to their complex technical concerns.

Security & Firewall – Unisys has provided the DECC Montgomery Consolidated Communications Center (CCC) network firewall and security support since its inception in 2003. The CCC is provides network management for DISA. Unisys remotely manages many sites throughout the US and abroad. Our duties include managing, maintaining, and troubleshooting end-to-end connectivity in a secure communications environment for all DISA supported sites, their customers, and their applications. The CCC provides 24/7/365 support for DISA and its customers. Unisys network specialists install, configure, manage, monitor, and troubleshoot all aspects of switch/router, firewall and security device. Unisys supports administration of the following devices:

- All models of Cisco switches L2 and L3 including MSFC and Sup 720.
- All models of Cisco routers including 7200 series.
- Juniper routers including VPNs.
- Cisco content switches.
- F5 Load Balancers.
- Cisco VPN routers.
- Use of Sniffer Distributed, Sniffer InfiniStream, Ethereal (Wireshark) to collect and decode network captures.

Database Services – Unisys Database Administrators support Oracle, Sybase, and MS SQL Server databases. In February 2013, we completed a major database migration to the Test, Production, and Continuity of Operations (COOP) environments without a disruption. Unisys ensures all database software components are loaded and operational for existing and new customer use. We perform pre- and post-release steps, and review, coordinate, install and trouble-shoot all application software releases with minimal disruption to the production environment. We provide system administration, system restoration backups, and COOP backups.

Capacity on Demand and Additional Services

Storage Capacity on Demand – The Capacity Services solution provides a modernized baseline of EMC VMAX disk storage capacity capable of supporting DISA's existing Unisys storage requirements. Additionally, the Capacity Services provides the capability to adapt to DISA's changing requirements. The Capacity Services solution provides DISA's Unisys environment EMC's Symmetrix V-Max series Direct Access Storage Devices (DASD). Unisys delivers a Symmetrix V-Max array to DECC Oklahoma City. Unisys provides the DECC Oklahoma City test and development environment a Symmetrix V-Max array configuration that is robust enough to support the necessary cross-boots to all supported operating environments. Unisys supports the

Name of Client & Project Title	Defense Information Systems Agency (DISA) – Enterprise Services Directorate (ESD) ClearPath Managed Services, Mainframe and Mid-tier Technical and Application Support Services
	DECC St. Louis disaster recovery environment with a Symmetrix V-Max array that supports the replicated data from DECC Oklahoma City. Unisys supports dual Symmetrix V-Max arrays to the Montgomery Support Center. This configuration provides a much-needed data replication testing capability that eliminates the need to test microcode on production systems. This environment also provides the ability to evaluate new methods of replication and their subsequent impact to DISA's environment. Each Symmetrix V-Max array includes enough storage to support the Virtual Tape Library solution.
Project Duration:	**Start Date Year:** 1983 (USAF) – Transitioned to DISA 1994 / **End Date Year:** On-going
Nature of the Client:	DISA provides information technology (IT) and communications support services.
Nature of Client Audience:	United States Armed Services, Defense Agencies, and the Office of the Secretary of Defense
Number of Users:	250,000
# & Composition of Vendor Employees & Consultants Assigned:	**Vendor Project Manager/Key Consultant on Project Team:** William Wright, DOD Account Manager Unisys provides approximately 30 FTE's and no consultants. A Unisys Vice President is committed 50%, Senior Manager 100%
Client Contact Information:	Note: The contact details provided for the individuals listed below will change prior to the time that reference contacts are made by the Commonwealth. Please contact Reed Laughlin via phone at (717) 526-1187 or e-mail to edward.laughlin@unisys.com to obtain the latest contact information. **Reference Contacts:** **Name:** [redacted] **Title:** [redacted] **Department:** DECC Oklahoma City, OK **Full Address:** 8705 Industrial Blvd., Tinker AFB, OK 73145 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** Direct oversight of the ClearPath Operations. **Name:** [redacted] **Title:** [redacted] **Department:** Systems Support Organization **Full Address:** 401 E. Moore Dr, Building 834 Maxwell AFB-Gunter Annex, Montgomery, AL 36114 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** Provides daily oversight of the technical support for the ClearPath systems.

Unisys Project Reference 3: California State University (CSU)

Name of Client & Project Title	California State University (CSU) – Data Center Hosting Services
Contract Value	$38 Million
Nature and Scope of Project:	**Project Description** This Data Center (DC) Hosting Services contract supported the CSU Chancellor Office and 23 campuses with PeopleSoft Higher Education Applications and Oracle Databases. DC is located in Salt Lake City, Utah. Data Center Services encompasses; DC Operations, DC Technical Support, Service Desk, Change Management, Incident Management, Network, Security, PMO, Capacity and Performance Management, cRIM (converged remote infrastructure monitoring), Print Support Services, Data Backup and Support, and Disaster Recovery Services - Eagan DC. The contract was forged when the University was faced with the impact of the California Budget Crisis resulting in the need to reduce Information Technology (IT) spending while demonstrating continuous improvement in service delivery. This contract included reassessing IT support to use emerging technologies and to make certain that their IT Infrastructure would support their aggressive software roadmap. **Client Quote** *"With a strong partnership built over the last ten years, Unisys understands our unique needs and requirements. They have given us agility to cost effectively leverage new technologies though Cloud computing and application outsourcing."* [redacted], *California State University* **Services Management** Implemented improvements for Disaster Recovery through the use of images vs. servers reducing recovery point objectives (RPOs) and recovery time objectives (RTOs). Developed a partnership to ensure existing, consistent, effective, and efficient services while also looking towards the future bringing forward new solution opportunities through a mutually beneficial Governance process. **Technical Services** Agility to handle the demand of academic semester/ and quarterly course scheduling peaks throughout the year with flexible computing resources and cost models. Contract provides for a baseline (fixed amount) of compute and storage resources at a fixed price, yet at the same time the flexibility to burst through the cloud services and utilize additional compute and storage resources for variable rates and variable periods of time. **Managed Hosting Services** Delivered flexible Unisys Cloud services (server/storage); scaled up/down for campus registration peaks, year–end processing cycles, and Disaster Recovery.

Name of Client & Project Title	California State University (CSU) – Data Center Hosting Services	
	Unisys is hosting the applications and databases supporting CSU's Oracle/PeopleSoft Higher Education suite.	
Project Duration:	**Start Date Year:** 2001	**End Date Year:** 2016
Nature of the Client:	Largest Public University System in the United States	
Nature of Client Audience:	Students, Faculty, and Administration Staff	
Number of Users:	450,000 Students and 40,000 Employees	
# & Composition of Vendor Employees & Consultants Assigned:	**Vendor Project Manager/Key Consultant on Project Team:** Connie Vaughan, Unisys Client Account Director **Dedicated staff:** 9 (on-site); 35 (off-site)	
Client Contact Information:	**Reference Contacts:** **Name:** [redacted] **Title:** [redacted] **Department:** Common Management System Technical Support **Full Address:** CSU Chancellor's Office, Information Technology Services (ITS) 401 Golden Shore, 3rd Floor, Long Beach, CA 90802 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** [redacted]. Has direct management contact for Unisys Outsourcing Contract. **Name:** [redacted] **Title:** [redacted] **Department:** Contract Services & Procurement **Full Address:** CSU Chancellor's Office, Contract Services & Procurement 401 Golden Shore, 5th Floor, Long Beach, CA 90802 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** Contract Officer that negotiated contract on behalf of CSU and provides ongoing contractual support for amendments and change orders.	

Unisys Project Reference 4: Internal Revenue Service (IRS)

Name of Client & Project Title	Internal Revenue Service (IRS) Service Center Support System (SCSS)
Contract Value	$500+ million
Nature and Scope of Project:	**Project Description:** Under the Service Center Support System (SCSS) contract, Unisys provides maintenance and enhancement of the IRS Tier 1 (mainframe) computing environment. These systems support: (1) integrated computer systems and databases; (2) nationwide access to taxpayer information; (3) online updates to taxpayer information; and (4) authoritative data access to support ongoing case processing. These are the core systems used by the IRS to process the collection of more than two trillion dollars annually. Unisys role as the prime contractor is to provide full systems life cycle maintenance and upgrade of system capabilities in response to evolving IRS processing requirements and the availability of new innovative technology. Over the past 17 years, Unisys has supported the IRS in maintaining and enhancing their mainframe-processing environment. This includes 3 IBM Mainframes (25 images) and 2 Unisys Mainframes (8 images), at the main Computing Centers in Martinsburg, WV and Memphis TN. These platforms host the Integrated Data Retrieval System, providing IRS employees with instantaneous access to taxpayer accounts. This facilitates better, faster, more responsive and more personal service to the taxpayer. The platforms also host the Security and Communications Systems, which provides identification, authorization and audit to prevent unauthorized disclosure of taxpayer information as well as unauthorized access, inspection, and changes. The Computer Assisted Publishing System also runs on the IRS Tier 1 platforms providing the computer resources to maintain the central publishing and distribution capability for IRS published materials. In conjunction with the IRS, we have implemented more than 140 System/Service Initiatives (S/SIs), improving the mainframe hardware and software capabilities with greater security, capacity, and efficiency. We have tailored our maintenance processes to meet the demands of the IRS tax processing seasons and provided highly qualified staff and consultant support. Over the years, our relationships with IRS, IBM, and OEM vendors have grown to facilitate better communications and coordination to meet evolving mission requirements. **Technical Services** Unisys provides support services for the Unisys and IBM environments and storage solutions from IBM, ViON/Hitachi, Oracle, and EMC. Support is also provided for computer room operations, systems operations, configuration management, inter-computer communications, performance monitoring and tuning, system backup and recovery, database management, storage management, data protection, disaster recovery test support, and information security. We have provided the required onsite support with 24x7x365 availability as required. **Facilities Management** Although Unisys does not have direct responsibility for IRS facilities management, we work very closely with the IRS team to make sure that proper planning is conducted to address power and HVAC requirements when implementing new solutions

Name of Client & Project Title	Internal Revenue Service (IRS) Service Center Support System (SCSS)	
	Capacity on Demand and Additional Services Throughout the contract, Unisys has proposed improvements to the SCSS operating environment. These improvements have been for technology enhancement, technology renewal, to satisfy increased requirements or to introduce cost effective innovation. Unisys has worked with the IRS to deliver more than 140 SSIs. These have ranged from the major mainframe consolidation to peripheral device integrations. Recently, these have included storage upgrades to allow virtual tape sharing between the IBM and Unisys platforms, and high volume inter-computer communications that have been tested to support up to 1,500 transactions per second. **Data Center Architecture** Our maintenance support includes apprising the IRS of the mainframe systems technology roadmaps and new capabilities. A major task executed under this vehicle resulted in the consolidation of more than 60 mainframes in 10 IRS Service Centers to 8 mainframes in three Computing Centers. Subsequent consolidation has the pipeline processing workload running on five mainframe systems in two Computing Centers. The enterprise consolidation resulted in hundreds of millions of dollars in cost savings over the life on the contract.	
Project Duration:	**Start Date Year: 1995**	**End Date Year:** On-going
Nature of the Client:	IRS Tier 1 (mainframe) operations	
Nature of Client Audience:	IRS IBM and Unisys Mainframe Branch and the Integrated Data Retrieval System end users	
Number of Users:	50,000	
# & Composition of Vendor Employees & Consultants Assigned:	The team composition varies depending on the number and scope of System /Service Initiatives in progress. During steady state operations, six Unisys employees and six consultants are assigned to the program. Staff are assigned as required to meet delivery commitments. At the peak of consolidation, more than 75 employees and 50 subcontractors were actively engaged in delivering solutions.	
Client Contact Information:	**Reference Contacts:** **Name:** [redacted] **Title:** [redacted] **Department:** Internal Revenue Service **Full Address:** 6009 Oxon Hill Road Oxon Hill, MD 20745 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** [redacted]	

Name of Client & Project Title	Internal Revenue Service (IRS) Service Center Support System (SCSS)
	Name: [redacted] **Title:** [redacted] **Department:** Internal Revenue Service **Full Address:** 6009 Oxon Hill Road Oxon Hill, MD 20745 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** [redacted]

Unisys Project Reference 5: City of Minneapolis

Name of Client & Project Title	City of Minneapolis – Information Technology (IT) Infrastructure Outsourcing
Contract Value	$130 million
Nature and Scope of Project:	**Project Description** In January 2003, the City of Minneapolis awarded Unisys Corporation a seven-year Information Technology (IT) outsourcing contract to manage the City's complete IT infrastructure, from the data center to desktops and mobile devices. Under the contract, Unisys supports multiple city agencies, including the Mayor's Office, City Council, Police, Fire Departments, and the Office of Public Works. In 2011, tech-savvy employees wanted to start using mobile devices in the workplace, the City consulted Unisys for assistance in building a mobility solution to support, govern, and secure wireless devices. The first phase of the mobility initiative—branded Mobility 1.0—completed in 3 months and focused on delivering services specific to the Apple iOS platform with immediate emphasis on iPads and iPad access to the City's infrastructure through VPN clients. The City of Minneapolis determined it was spending too much time and money on routine IT infrastructure management, remedial maintenance, network management, and desktop tasks. The City's IT department found itself being diverted from its core mission of providing information services and planning for better use of e-government systems for all users. Like many businesses, the City faced the challenge of finding new ways to support constituents, achieve cost and efficiency savings, while being able to plan strategically for the future across a multitude of departments. In 2011, the City consulted with Unisys to advance its mobility goals while proactively addressing security risks, management issues, and standards for use that arise when workers introduce mobile devices into city government offices. **Client Quote** *"Our outsourcing relationship with Unisys has enabled city government to realize significant operational efficiencies at a reduced IT cost."* *"We appreciate Unisys flexibility, cost consciousness and IT expertise. Unisys is working closely with the city as we unfold mobile application standards and develop use cases for mobility, such as mobile access to city services by citizens and partners."* [redacted] **Program Management Office and Service Management** A dedicated Unisys Program Management Office coordinates delivery of the services. This single-point-of-contact approach streamlines all service requests, based on Unisys' ITIL/Six Sigma framework, and is a key best practice that Unisys brings to the project. • Data center administration and management • Network and systems monitoring and management

Name of Client & Project Title	City of Minneapolis – Information Technology (IT) Infrastructure Outsourcing

In addition to the initial base services offered, Unisys is also responsible for the managed services to support the City's 311 (non-emergency) and Computer Aided Dispatch 911 (emergency) environment

Technology Services

Technologies supported include, Windows, UNIX, Unisys, EMC, Oracle, and the Windows Office Suite.

- Desktop support services, including desktops, laptops, peripherals; and iPads
- Service Desk services
- Security Analytics and vulnerability services
- Disaster Recovery services
- Technology refresh of laptops, desktops, and servers

Recent secure mobility solutions continue to provide benefits to the city that includes:

- **Time:** Met aggressive timeline for phasing in mobility services
- **Cost:** Leveraged the city's existing LAN infrastructure and current internet wireless provider; a safer, more efficient wireless network at a competitive price; automated management and support services that scale with device numbers; streamlined device deployment through certificate gateway and affordable application deployment via the Apple Volume Purchase Plan
- **Productivity:** Synchronization of mobile devices with desktops through ActiveSync, iPad access to shared drives, upgraded Cisco VPN solution to support roaming workers
- **Security:** Policy management through the service desk and MDM platform system, VPNs and wireless connectivity backed by Cisco security

Capacity on Demand & Additional Services

Unisys delivered Private Secure Cloud Computing and Virtual Storage. This scalable solution provided on-shore support for 85 iPads with ability to accommodate an unlimited number of devices as City of Minneapolis workers begin exploiting mobility-related workflow changes. The city was expecting 10 percent of the municipal workforce to go mobile within the next two years.

Managed Hosting Services

Unisys took ownership of the City's existing servers, storage, PCs and printers. The servers and storage were moved to the Unisys IT Outsourcing Service Centers in Eagan, Minnesota and Roseville, Minnesota. This hardened data center facility provides 24x7x365 availability and application support in a secure, high performance, highly-scalable environment. This transition was accomplished in a record 10 months instead of the projected 18 to 24 months.

Today, Unisys manages and supports over 200 servers and 3,000 desktops for the City. Included among the systems being hosted are the servers supporting the City's Web development and client-facing production Web services servers. Unisys provides full managed hosting services for these servers.

Name of Client & Project Title	City of Minneapolis – Information Technology (IT) Infrastructure Outsourcing	
	Benefits Independent Audit of Unisys Performance: Excipio, a third party consulting firm, was hired by the City to provide an external benchmark of the City's IT department and its contract with Unisys. Excipio reported the following: • The City's contract with Unisys provided the City with an estimated savings of $18.2 million over the contract life • On its own, the City could not have advanced to its current IT state. The City is in a much better place with a more secure IT environment for having outsourced to Unisys • Overall IT process and performance have improved as a result of working with Unisys. There is now an ITIL framework, service level management, stabilized infrastructure, continued innovation, and new tools are introduced on a regular basis. • Outsourcing to Unisys has freed the City's internal IT staff to concentrate on strategic initiatives to better serve city employees and constituents. For example, the deployment of a wireless network that covers all 59 square miles of Minneapolis, providing residents, businesses, and visitors with wireless broadband access anywhere in the city. Additionally, the City is now an aligned organization that drives innovation through technology	
Project Duration:	**Start Date Year:** 2003	**End Date Year:** On-going
Nature of the Client:	The City of Minneapolis is a multi-stakeholder client with a clear vision: to be a world-class virtual city with public services available 24x7x365. Minneapolis and its surrounding cities make up the 16th largest metropolitan area in the country. Its thriving downtown area is home to several Fortune 500 companies.	
Nature of Client Audience:	City of Minneapolis employees	
Number of Users:	3,600 employees at all levels of City of Minneapolis municipal government that provide services to 382,000 citizens	
# & Composition of Vendor Employees & Consultants Assigned:	**Vendor Project Manager/Key Consultant on Project Team:** Jeff Wilke, Unisys Client Account Executive Total staff during start-up was approximately 70 people, approximately 60 staff at operational peak, and ongoing current staff level of 30. This dedicated staff is broken into 15 (on-site) and 15 (off-site).	
Client Contact Information:	**Reference Contacts:** **Name:** [redacted] **Title:** [redacted] **Department:** City of Minneapolis Information Technology Department **Full Address:** Flour Exchange Building, 310 4th Ave South, Suite 400, Minneapolis, MN 55415 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** [redacted]	

Name of Client & Project Title	City of Minneapolis – Information Technology (IT) Infrastructure Outsourcing
	Name: [redacted] **Title:** [redacted] **Department:** City of Minneapolis Information Technology Department **Full Address:** Flour Exchange Building, 310 4th Ave South, Suite 400, Minneapolis, MN 55415 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** [redacted]

Unisys Project Reference 6: American Red Cross (ARC)

Name of Client & Project Title	American Red Cross – Information Technology Infrastructure Outsourcing, End User Outsourcing, and Support Services
Contract Value	$80 million
Nature and Scope of Project:	**Project Description** The American Red Cross (ARC) has entrusted to Unisys its complete IT infrastructure for management, service desk, and customer support from the desktop and mobile devices up through and including transition of Data Center operations, applications and systems from the ARC located in the Chicago area into the Unisys Eagan Data Center facility. Disaster recovery is also being provided facilitated out of the Unisys Data Center located in Salt Lake City UT. Operational standards are based upon an ITIL V3 framework. ITSM is used for Cross Functional coordination and ITIL process management and includes Asset Management. Unisys is also responsible for mobility and distributed computing for ARC end user personnel and their devices. American Red Cross sought full Information Technology Operations (ITO) support for their field operations including Incident, Change and Problem Management, Asset and Configuration Management, Service Desk, End User Services (EUS) / Field Services, and Quality Systems Management. Unisys mission is to provide consistent, efficient, and reliable global delivery capabilities for Information Technology (IT) managed services that support the Red Cross's humanitarian mission and assist Red Cross workers in providing rapid, efficient response to people in need. **Client Quote** *"With Unisys as our services partner, we look forward to gaining efficiencies that reduce operating costs and bring new tools and technologies to our end users," said Doug Greene, vice president for Enterprise Technology of the American Red Cross. "This partnership also puts into place the foundation for us to leverage cloud services, which is in line with our strategic direction."* **Service Management** Unisys provides a full range of customer support and data center managed services to support approximately 20,000 Red Cross workers throughout the United States and Puerto Rico. The contract includes on-site services, IT asset management, and service desk support delivered through Unisys Managed Services Centers in Salt Lake City, Utah, Eagan, Minnesota, and Rochester, New York. Unisys delivers these end-user services in an integrated IT services management (ITSM) environment that enables Red Cross workers to use the most convenient channel to obtain support, including telephone, instant messaging, e-mail and the Web. **Technical Services** Unisys provides data center services from its facility in Eagan, Minnesota, with disaster recovery backup in Salt Lake City, Utah. The technical services provided included transition of services, applications and servers from the ARC datacenter located near Chicago into the Unisys data center in Eagan. This also included the implementation of Unisys remote infrastructure management services, that use automated capabilities to monitor and correlate events across all segments of the managed infrastructure – from servers to

Name of Client & Project Title	American Red Cross – Information Technology Infrastructure Outsourcing, End User Outsourcing, and Support Services

mobile devices - to orchestrate both pre-emptive and preventive action against potential IT faults.

Unisys provides enterprise-wide support to Red Cross in the following major areas: Customer Support Services, Data Center, Quality Management, and Cross Functional Services. All services are monitored under negotiated SLAs and reported on monthly.

North American AIX Center of Expertise:

The ARC team was able to leverage best practice, transition knowledge and lessons learned through interaction with the Commonwealth's AIX support team all of whom are members of Unisys NA AIX Center of expertise. The Commonwealth's AIX team shared valuable AIX best practice based in part from lessons learn from the IES AIX Transition.

Customer Support Services

Service Desk

- In June 2012, Unisys took over operations of Red Cross service desk activities and has implemented the BMC Remedy IT Service Management (ITSM) platform for support of non-regulated service desk incidents.
- Unisys also operates the Red Cross' internal Clarify service desk platform for reporting regulated incidents.

Desktop Support Services

- Desktop image management, packaging, and remote implementation.
- Patching for all desktops and servers
- Dispatch and DC HQ onsite Break/fix services HQ desktops (3,000)
- Install, Move, Add, Change, and Disposal.

Data Center

- Unisys hosts Red Cross' data center at its Eagan Minnesota data center facility.
- Unisys provides operations and management for:
  - Servers
  - Storage
  - Local Area Network.
  - Firewalls
  - Content switches
  - Tape Backup Facilities
- Cross Functional Services
  - Availability Reporting
  - Capacity Management, Trend Analysis, and Forecasting (currently in implementation phase)
  - Backup and Restore
  - OS Maintenance
  - Tape Library management
- Key Applications Platforms
  - Microsoft Office, SQL Server, SharePoint, specialized Biomedical applications for Blood Manufacturing, Donor Management, and Blood drive Campaigns
  - Operating Platform:

Name of Client & Project Title	American Red Cross – Information Technology Infrastructure Outsourcing, End User Outsourcing, and Support Services	
	▪ Windows XP, 7 ▪ Windows Server 2000, 2003, 2008 ▪ AIX 4.x, 5.x, 6.x, 7.x ▪ HP/UX (3000 & 4000) ▪ Sun Solaris ▪ SCO UNIX ▪ Oracle Grid ▪ SQL Server ▪ EMC SAN platforms (Clarion & DMX) ▪ Cisco Networking **Quality Management** • Qualified Biomedical Supplier to Red Cross • Quality Management program and support systems • Supports Red Cross regulated systems and infrastructure under Red Cross Quality oversight. • Training Management • Document Management **Cross Functional Services** • Asset Management and Configuration Management • Change Management and Reporting **Other Services** • Major Incident Management • Problem Management	
Project Duration:	**Start Date Year:** 2012	**End Date Year:** on-going
Nature of the Client:	The American Red Cross is a humanitarian organization that provides emergency assistance, disaster relief, lifesaving blood, and health and safety services inside the United States. The project is managed by the Enterprise Technology branch of the American Red Cross' IT department.	
Nature of Client Audience:	American Red Cross Employees	
Number of Users:	20,000	
# & Composition of Vendor Employees & Consultants Assigned:	**Vendor Project Manager/Key Consultant on Project Team:** **Dedicated staff:** 8 (on-site); 115 (off-site)	

Name of Client & Project Title	American Red Cross – Information Technology Infrastructure Outsourcing, End User Outsourcing, and Support Services
Client Contact Information:	**Reference Contacts:** **Name:** [redacted] **Title:** [redacted] **Department:** American Red Cross **Full Address:** 2025 E Street, Washington, DC 20006 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** [redacted] **Name:** [redacted] **Title:** [redacted] **Department:** American Red Cross **Full Address:** 2025 E Street, Washington, DC 20006 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** [redacted]

Unisys Project Reference 7: London Metropolitan Police

Name of Client & Project Title	London Metropolitan Police Service – Information, Communication and Technology (ICT) Contract
Contract Value	$34 million (approximately)
Nature and Scope of Project:	**Project Description** The Metropolitan Police Service (MPS) employs over 40,000 police officers and staff to police the 7.2 million residents of London's 620 square miles. The MPS ICT contract was awarded in December 2005 to Capgemini, with Unisys and BT as key partners. The contract was for 7 years, and has subsequently been extended a further 3 years until 2015. • Applications Management • Hosting (CRIS) and DR services • Break/ fix • Installations, moves, additions & changes • Managed data center space The Unisys applications teams are responsible for managing all application related incidents reported through the Capgemini service desk, managing the third party product suppliers, user acceptance testing, release management and pro active monitoring of all applications services. The team supports over 60 applications and handles some 2,000 incidents per month. Most of the applications are provided by third parties, with the exception of CRIS, CEC, SAP and a few others. Unisys is responsible for managing the incidents and problems passed to third parties, including the relationship with all third parties. The key application areas are Crime recording, Intelligence and all SAP landscapes. The CRIS (Crime recording Information System) application is used to hold details of all crimes committed in London and capabilities to analyze the data for operational business reasons. The Intelligence applications are used for proactive crime analysis and prevention, and for operational deployment. The SAP services are for back office functions and cater to finance management, procurement, invoicing and purchase orders with a data warehouse for analysis needs. The break fix element of the contract includes all hardware maintenance and IMAC services across the entire MPS estate, which includes over 35,000 desktops/laptops, over 2,000 servers, and a quantity of printers and multi-functional devices (MFDs). As part of the overall service, Unisys also provides a Managed Data Centre service, supporting both live and failover systems on a 24x7 basis. Additionally, as part of ongoing technical refresh activities, Unisys Architects design and implement improved system and data centre architectures in line with emerging technologies. A typical recent example of this, is a complete system update moving to a fully virtualized live and failover capability for the MPS' critical Crime Recording Information System. The above services are all delivered to strict service levels that are consistently met by dedicated teams aligned with each area. In addition to standard delivery, Unisys also provides Project services, which are run and overseen by an integrated PMO function. Under a separate contractual arrangement directly with the Metropolitan Police Service, Unisys provides a complete managed service for the mission critical 24x7 Command and Control (C&C) system. This includes data centre hosting with a full DR capability and a complete technology refresh was performed within the last 5 years. Services provided for C&C range from computer operations and service desk, platform support and system

Name of Client & Project Title	London Metropolitan Police Service – Information, Communication and Technology (ICT) Contract
	software upgrades, through applications support and fault analysis to development of changes and enhancements to the applications, which include Call Handling, Dispatch, GIS and an MIS application. The C&C system serves more than 10,000 users with up to 1,000 concurrent users and provides sub-second response times and availability in excess of 99.9% in a high volume transaction environment. Applications are hosted on a mixture of platforms including Windows, UNIX and Unisys mainframe (ClearPath) with a variety of programming languages ranging from Cobol and Fortran to C, C#, Java and JavaScript. Database management systems include Oracle and SQL Server as well as Unisys proprietary DBMS.
Project Duration:	**Start Date Year:** 2005 — **End Date Year:** 2015
Nature of the Client:	System Integrator working on behalf of Metropolitan Police Service
Nature of Client Audience:	Metropolitan Police officers or civilians employed by the police service
Number of Users:	More than 35,000
# & Composition of Vendor Employees & Consultants Assigned:	**Vendor Project Manager/Key Consultant on Project Team:** Permanently resourced team of technical design, integration, development, test and management resources
Client Contact Information:	**Reference Contacts:** **Name:** [redacted] **Title:** [redacted] **Department:** MPS ICT Account **Full Address:** 95-97 Wandsworth Road, London, SW8 2HG United Kingdom **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** Capgemini is the Prime Contractor delivering large ICT outsource to Met Police, with Unisys as a material Sub-Contractor with total responsibility for the applications management and break fix services [redacted] **Name:** [redacted] **Title:** [redacted] **Department:** Department of Information **Full Address:** Edinburgh House 170 Kennington Lane, London, SE11 5DP, UK **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** [redacted]

4.5.2 IBM Project References

IBM Project Reference 1: Commonwealth of Pennsylvania (Subcontractor to Unisys)

Name of Client & Project Title	Commonwealth of Pennsylvania – Data PowerHouse (Subcontractor to Unisys)
Contract Value	$500 million (Total IBM contract value in excess of since 1999)
Nature and Scope of Project:	**Project Description** In 1999, the Commonwealth contracted a consortium of Information Technology (IT) providers, led by Unisys and supported by IBM, to provide an end-to-end outsourcing solution. The unified IT team consolidated data centers and established the Data PowerHouse (DPH), one centralized data center to support the Commonwealth's agencies. In 2002, the DPH project was named "Most Strategic" by the Outsourcing Journal in its Editor's Choice Awards, and the Commonwealth extended its contract with Unisys and its team of IT providers. In 2008, the Commonwealth still satisfied with the operations of its centralized data center, yet feeling budget pressures, initiated a contract renegotiation. DPH services were modernized, costs reduced and the contract extended as a result of this renegotiation. IBM has been a major subcontractor on the Commonwealth's DPH initiative since 1999. IBM's related competencies and experience from major engagements in the Commonwealth include the following. **Program Management Office and Service Management** IBM has combined leading management disciplines with experience and expertise to deliver high levels of customer service to both the routine and unique needs of the Commonwealth. IBM consistently demonstrated the skills and experience to perform all aspects of the outsourcing services required by the Commonwealth. IBM has made particular efforts to understand and support the Commonwealth's business requirements and culture through long-term retention of account team personnel. **PMO Program Governance –** IBM established a PMO, which interacted with Unisys to provide overall governance of the program. **Managed Services –** IBM provided all managed service responsibility including problem, change and availability management and capacity planning. **Technical Services** IBM was also responsible for Service Level Agreements (SLAs) associated with the technical environment it managed. The technical solution includes 94 Servers configured with AIX and Windows 2000 operating systems and supporting the SAP applications and Oracle databases. **Facilities Management** IBM provided Facilities Management (FM ERP) services for data center operations management of the Commonwealth of Pennsylvania's SAP R/3 infrastructure from 2002 thru 2005 at which time it was migrated over to the Integrated Enterprise System (IES) services described above. IBM services were delivered on customer premises with customer owned hardware and software.

Manage Hosting Services

Under this contract, IBM provides long-term managed services for mainframe and midrange based systems supporting enterprise applications at several major Commonwealth agencies.

IES - IBM provided midrange data center operations services in support of the Commonwealth IES from 2005 through 2010 at which time the services were brought into the DPH. These services supported the IES SAP –ERP environment, which provided budget, finance, payroll, procurement and human resource functions to most of the Commonwealth agencies.

Additional Services

In 1999, at the start of the DPH contract, there were eight (8) agencies running on separate enterprise server platforms in agency operated data centers; IBM successfully transitioned them to a single data center, multiple processor environment and coordinated upgrades as forecasted capacity requirements were needed. The upgrades that brought about innovative changes are highlighted below.

In 2002, two IBM 2064 processors were installed. The Integrated Facility for Linux (IFL) was introduced into the DPH via one of those processors. The IFL is a processor dedicated to Linux workloads on IBM System z servers. The IFL processor enables agencies to add processing capacity exclusively for Linux workloads: consolidations, re-deployments and new deployments. The use of an IFL can improve the IT economics by consolidating, re-deploying existing and deploying new workloads to reduce expenses in the areas of operational efforts, energy, floor space, and software license fees.

DOT began using the IFL in earnest for their Centric application development. Over time the capacity requirements for zLinux on the enterprise server have grown. Today there are a total of five IFLs on the processor, four of which support the application workload and one is dedicated to system/application monitoring environment.

In 2007 the IBM 2094 processor was installed and the z Integrated Information Processor (zIIP) was introduced into the DPH. The zIIP processor, like the IFL is a special purpose processor. It was initially introduced to relieve the general enterprise server central processors (CPs) of specific DB2 processing loads, but currently is used to offload other z/OS workloads. By relieving the general CP of particular workloads, they often lead to a higher workload throughput at reduced license fees. DB2 for z/OS was the first application to exploit the zIIP, but now there are several IBM and non-IBM products and technologies that have taken advantage of that exploitation.

2008 brought about more changes within the DPH, one of those being a consolidation of all remaining agency workload onto single IBM 2097 processor. The Commonwealth received a "technology dividend" from this upgrade in two ways:

1 The IFLs and zIIP carried over to the new processor at zero cost but provided more capacity
2 IBM software allowed for more capacity per measured unit

At this time two other new functions were implemented, Group Capacity settings for the larger agencies and sub-capacity software licensing was implemented where applicable. The changes resulted in additional cost savings for the agencies.

Benefits of the Solution

Following the system virtualization and data center refresh, Unisys expects the Commonwealth to save upwards of $240 million. Additionally, the Worldwide Strategic Outsourcing team's services, combined with the modernized IT environment, will enable

	the Commonwealth's IT staff to focus on strategic tasks and problem solving, instead of application management on a sprawling environment. **Data Center Architecture** IBM's transformation of the infrastructure will help improve performance for the Commonwealth's end users and business operations.	
Project Duration:	**Start Date Year:** 1999	**End Date Year:** 2014
Nature of the Client:	IBM and Unisys have collaborated to provide managed services for the Commonwealth's enterprise computing services since September 1, 1999. During that time we gained valuable experience in delivering quality services while continually seeking out technology improvements and IT cost savings over the life of the contract.	
Nature of Client Audience:	Commonwealth of Pennsylvania agencies who participate in the DPH and the constituents of the Commonwealth	
Number of Users:	8 million Commonwealth constituents	
# & Composition of Vendor Employees & Consultants Assigned:	The services provided with approximately 64 Full Time Equivalent (FTE) personnel, primarily located in the Commonwealth. During start-up and peak times, the level of effort was up to 135 FTEs.	
Client Contact Information:	Note: IBM is a direct subcontractor to Unisys for the DPH project. Because of this unique relationship, Mrs. Kirwan-Orner can provide direct information related to the relationship between IBM and Unisys under the DPH project. Mr. Crager can provide background perspective as it relates to the services IBM and Unisys provided to the Commonwealth of Pennsylvania under the DPH project. **Reference Contacts:** **Name:** [redacted] **Title:** [redacted] **Department:** Unisys Corporation, Global Managed Services **Full Address:** 4750 Lindle Road, 3rd Floor, Harrisburg, PA 17111-2428 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** [redacted] is has operational and contractual responsibility for the contract that Unisys has with IBM. **Name:** [redacted] **Title:** [redacted] **Department:** County of Franklin, Pennsylvania **Full Address:** 218 N Second Street, Chambersburg, PA 17201 **Telephone:** [redacted] **E-mail** [redacted] **Relation/Role to Project** [redacted] his included work done by IBM under that contract.	

IBM Project Reference 2: State of Georgia

Name of Client & Project Title	State of Georgia – Georgia Technology Authority
Contract Value	$1 billion (over 10 years – 8 base and 2 option years)
Nature and Scope of Project:	**Project Description** The Georgia Technology Authority (GTA) was established on July 1, 2000 to provide the delivery of IT infrastructure services to the state's 85 Executive Branch agencies. In 2007, the State of Georgia conducted a third-party assessment of the state's IT operations and documented serious and chronic problems throughout state government which included aging infrastructure, the inability to meet minimum industry standards, the lack of processes and skills, little coordination of spending, and deficiencies in disaster recovery. Georgia determined that their most efficient method for addressing their challenges was to partner with private-sector leaders in technology service delivery. The State awarded an 8-year contract for IT Infrastructure Services to IBM. The contract includes mainframes; distributed computing servers and associated storage; tape; network connectivity and security; print; service desk; end-user computing and disaster recovery. The result translated into saving money, staying current with modern technology and ensuring that confidential data remains safe and secure from outside threats. IBM provides a scope of service to the State of Georgia that is very similar to that desired by the Commonwealth of Pennsylvania and includes. **Program Management Office and Management Service** Common Information Technology Infrastructure Library (ITIL) based systems management services including incident and problem management, performance management, and capacity management: • Physical database support of Oracle, SQL Server, MySQL, DB2 • Support of AD, eDirectory • Messaging software including MS Exchange, Novell GroupWise and Blackberry. • Web middleware support including WAS, IIS, Net Framework, IBM HTTP Server, and Sun One Web Server. • High-availability cluster services • Server virtualization. • Build and harden server security according to agreed-upon security standards and audit compliance posture. • Manage backup recovery, tape (on/off site) and disaster recovery. • Manage SAN storage area networks (IBM, EMC, and NAS). • Implement standard monitoring tools and provide 24x7 monitoring. **Technology Services** IBM provides mainframe support of UNIX/Windows servers. This includes lifecycle management (acquisition, installation, de-installation, and disposal) and ongoing support (OS patching and hardware break/fix). Operating systems supported include UNIX, Solaris, AIX, Linux, Novell, and Windows 2000, 2003, 2008, and Vista On transformation, systems consolidated into a State of Georgia data center supported by IBM.

Name of Client & Project Title	State of Georgia – Georgia Technology Authority	
Project Duration:	**Start Date Year:** 2009	**End Date Year:** Ongoing
Nature of the Client:	Georgia Technology Authority (GTA) provides the delivery of IT infrastructure services to the state's 85 executive branch agencies.	
Nature of Client Audience:	The clients are the Chief Information Officers and Chief Technology Officers (CIOs/CTOs) of the agencies, their IT staff and end users.	
Number of Users:	There are approximately 45,000 end users of the environment in 20 participating agencies.	
# & Composition of Vendor Employees & Consultants Assigned:	IBM has a team of more than 500 full-time equivalents supporting the services. We partner with Dell for end user support, AT&T for network support, and Xerox for managed print services. All other services are provided directly by IBM. IBM has completed transition and is approximately 50 percent complete with transformation. Completion of transformation is targeted for 2014. Transformation includes standardization of e-mail systems, implementation of AD, file server and application server, and other activities. IBM supported or supports the legacy environment prior to its transformation and supports the transformed environment.	
Client Contact Information:	Note: The Georgia Technology Authority has requested that all reference request contacts be coordinated through their IBM account representative. Please contact one of the following individuals to facilitate a reference discussion with the Georgia Technology Authority. **Reference Contacts:** **Name:** [redacted] **Title:** [redacted] **Department:** IBM Global Technology Services **Full Address:** 47 Trinity Ave., Atlanta, Georgia 30334 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** Overall responsibility for the project and client relationship **Name:** [redacted] **Title:** [redacted] **Department:** IBM Global Technology Services **Full Address:** 47 Trinity Ave, Atlanta, Georgia 30334 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** Business office management	

IBM Project Reference 3: State of Washington

Name of Client & Project Title	State of Washington, Automated Client Eligibility System (ACES) Maintenance and Operations
Contract Value	$20 million (annually)
Nature and Scope of Project:	**Project Description** The Automated Client Eligibility System (ACES) is a statewide application used to determine eligibility and issue benefits for social service (cash/food/ medical) recipients in the state of Washington. IBM developed and implemented ACES based on an existing system transferred from another state. ACES has been in production statewide since April of 1996. Since the initial install, ACES has had many enhancements and innovations. Web-based development was introduced in phases. Migrating to a Web-based approach has become a priority, and projects are being defined that will move existing legacy-based functions to the Web more quickly. A new client-facing portal was installed in 2010. It provides "am I eligible" preliminary calculations, applications, and access to a client benefit account with result details. IBM is responsible for three primary service areas covered by this contract. They are Application Development and Maintenance (ADM) for legacy systems, ADM for the ACES Web environment and Technical Support, which is responsible for the hardware and software infrastructure that support the ACES legacy components and the ACES online Web components. For both the core legacy system and the Web environment, IBM delivers 24x7 Production Control coverage for the ACES system running overnight batch jobs, coordinates printed output, and coordinates input/output to interfacing agencies, including Spell out first use EBT and EFT, The ACES system, supported by IBM, has a dedicated mainframe environment and a Web multi-server environment housed at the State of Washington Consolidated Technical Services (CTS) facility. The scope of this contract for the State of Washington is very similar to the scope desired by the Commonwealth of Pennsylvania, for example, both contracts include: • Mainframe support • Support of z/OS and Linux servers: • Life cycle management — acquisition, installation, de-installation, and disposal • Ongoing support: OS patching, hardware break/fix • Operating Systems supported include z/OS and, SUSE Linux. • Common ITIL-based systems management services including incident and problem management, performance management and capacity management. • Physical database support of IMS and DB2 • Support of RACF security and LDAP • Messaging software including MQ • Web middleware support including WAS, IBM HTTP Server, and ITCAMS for monitoring • High-availability cluster services • Server virtualization • Build and harden server security according to agreed-upon security standards and audit compliance posture

Name of Client & Project Title	State of Washington, Automated Client Eligibility System (ACES) Maintenance and Operations

- Manage backup recovery, tape (on/off site) and disaster recovery.
- Manage storage.
- Implement standard monitoring tools and provide monitoring.

Program Management Office and Service Management:

The IBM team is integrated with state teams to provide the technical focused skills of the development life cycle. Mature processes have been defined to manage the content of the quarterly release of the application. IBM also provides several Project Managers to oversee large work efforts and special projects. The base contract is performance based and includes Service Level Agreements (SLAs) for availability, response times, completion of batch jobs and attention to Sev1 Problems.

Technical Services

IBM supports a dedicated Mainframe environment for the account. Capacity reports and trending are provided on a monthly basis and IBM works with the customer to define and recommend architecture changes to meet future needs and strategy.

Facilities Management

The ACES Mainframe environment is located at a facility that is managed by a centralized state agency, Consolidated CTS. The IBM team works closely with CTS when environment changes are required. CTS also provides other hardware operations, including printer services and handling of any tape cartridges.

Managed Hosting Services

IBM manages the Mainframe, which includes a z/OS and z/VM Linux platform. The legacy functions of the application run in z/OS and Web-based functions run in Linux. Services include currency of all system software, installation and configuration. The operation environment is monitored and problems are diagnosed and resolved. The IBM team also manages infrastructure running in WINTEL, but the state is responsible for the hardware and base OS.

Capacity on Demand and Additional Services

This application has a dedicated environment and consistent growth patterns. IBM tracks system usage, plans future capacity, and makes recommendations around budget cycles. We have seen significant growth and need for Linux servers, but the virtual definition can be handled quickly to meet demand. Storage needs are also planned in advance and usage is tracked closely.

Although we recruit and build skills on the team, we have several recent instances where we have turned to Lab services for short-term demand and knowledge transfer. We recently adopted a new approach for data replication between IMS and DB2 that includes an ETL layer using Information Server DataStage. We brought in a replication and DataStage expert to assist the team. We have also turned to Lab Services to speed out adoption of Cognos for Business Intelligence needs and WODM (ILOG) for business rules management

Name of Client & Project Title	State of Washington, Automated Client Eligibility System (ACES) Maintenance and Operations
	Data Center Architecture The ACES Mainframe environment is integrated with a state Data Center managed by CTS. CTS also house the WINTEL server farm. The application support includes 24x7 support for a customer facing internet portal (Washington Connection) and will soon include the high availability demands for the Health Benefit Exchange (HBE) eligibility service. IBM and the ACES team participate in semi-annual disaster recovery test that are coordinated by CTS.
Project Duration:	**Start Date Year: 1993** (latest contract started 07/01/11) — **End Date Year:** Ongoing
Nature of the Client:	IBM partners with the IT Solutions unit of the Economic Services Administration to maintain and operate the ACES application. This administration is the largest in the Department of Social and Health Services (DSHS). This organization is responsible for administering benefits for multiple economic assistance programs, including Food Assistance, Cash and Medical Assistance.
Nature of Client Audience:	There are many stakeholders and business partners for this application, but the primary audience includes financial workers in field offices across the state and the citizens receiving benefits.
Number of Users:	5,000 Financial Workers
# & Composition of Vendor Employees & Consultants Assigned:	**Vendor Project Manager/Key Consultant on Project Team:** The initial project to transfer, modify and install the ACES application included several services that are not part of the ongoing steady-state services. The state did not have all the skills and infrastructure in place at that time, so IBM provided an off-site development environment, established the state network, and supported the help desk and testing. All of these functions have transitioned to the state. The current team provides PM, design, development and implementation as part of the development cycle. This is the focus for about 60 of the total 81 headcount provided in the base contract. This includes about a dozen Web (JAVA) developers, BI resources, and architects. The Technical Support team includes a dozen staff that support system software, middleware and DBAs. A third team of 5 staff provides 24x7 production control monitoring and batch cycle operations. The remaining positions are administrative in nature. At this time there are 20 additional staff that are augmenting the team to deliver the system and application changes required for the HBE eligibility service that is part of the federal Affordable Care Act.
Client Contact Information:	**Reference Contacts:** **Name:** [redacted] **Title:** [redacted] **Department:** DSHS ESA IT Solutions **Full Address:** DSHS ESA PO Box 45893 Olympia, WA 98504-5893 **Telephone:** [redacted] **E-mail:** [redacted]

Name of Client & Project Title	State of Washington, Automated Client Eligibility System (ACES) Maintenance and Operations
	Relation/Role to Project: Overall responsibility for the project and contract administrator **Name:** [redacted] **Title:** [redacted] **Department:** DSHS ESA IT Solutions **Full Address:** DSHS ESA PO Box 45893 Olympia, WA 98504-5893 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** Day-to-day administration of business and operations.

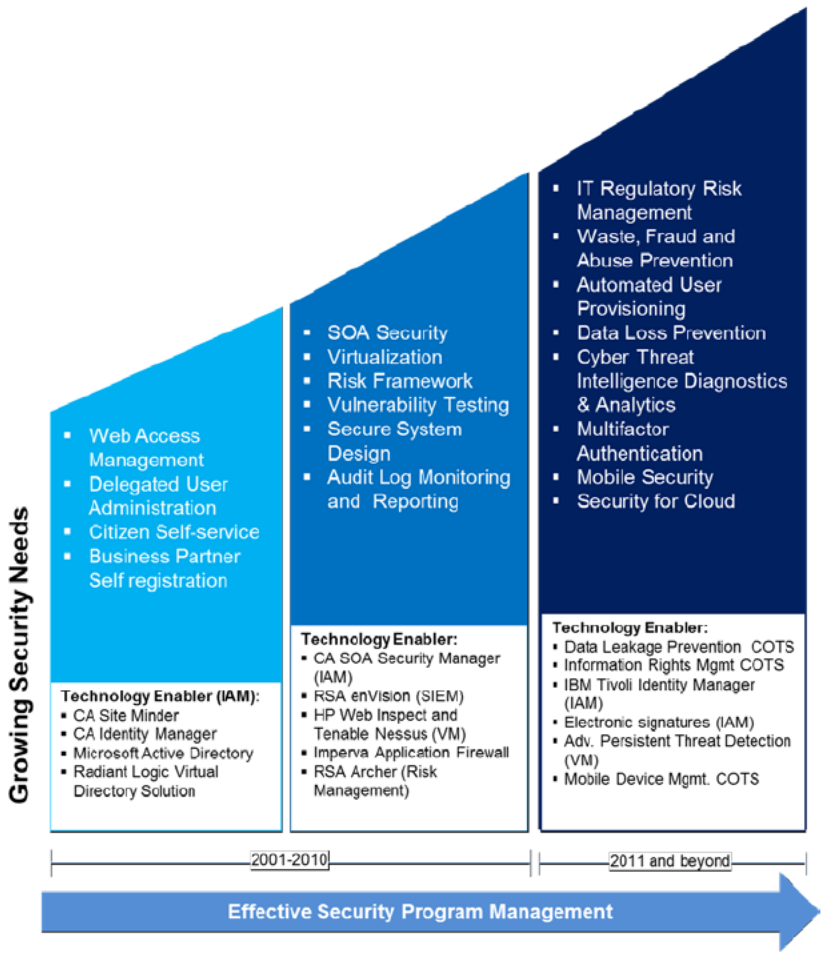
4.5.3 Deloitte LLP Project References

Deloitte Project Preference 1: Commonwealth of Pennsylvania Department of Public Welfare

Name of Client & Project Title	Commonwealth of Pennsylvania, Department of Public Welfare (DPW) – Project: Information Technology Shared Services (ITSS) – Security and Privacy
Contract Value	Part of a larger maintenance and enhancement contract
Nature and Scope of Project:	**Project Description** Security services – advisory and implementation services performed at the Commonwealth of Pennsylvania's largest agency. Deloitte has been providing a broad range of information security services to the Commonwealth for more than 10 years including strategy, design, build/deployment, and operations. This experience positions us to deliver the security services that are required as part of the Pennsylvania's data center project. Our qualifications demonstrate the close working relationships and familiarity with the business applications of key Pennsylvania agencies such as DPW, Office of Administration/Office for Information Technology (OA/OIT), PennDOT, and Labor &Industry (L&I). Deloitte's DPW qualification also demonstrates the ability to positively influence and enable the security program of the largest Commonwealth agency to effect continual improvements, to implement security tools, processes, and measures to stay abreast of a rapidly evolving threat landscape. In addition, Deloitte's knowledge of the Commonwealth security policies, standards–ITBs and certification programs like CA2– will be a key accelerator to help the Commonwealth effectively transition to the new data center operations model and a sustainable security program. Since the late 1990s, DPW has embarked on a program to modernize their enterprise application technologies, which entails a move from tightly controlled, highly isolated mainframe systems towards distributed, publically available and Web-based enterprise applications. While this change enhances the way public welfare programs are administered it also made it critical to provide adequate information security controls in accordance with regulations such as IRS 1075, HIPAA, and the Pennsylvania's Data Breach Notification Act. DPW's technology strategy is to progressively embrace the Services Oriented Architecture (SOA) model along with the appropriate security controls. **Security Services** Deloitte assisted DPW with its security program since 2001, helping DPW with regulatory compliance and keeping up with rapidly evolving security trends and technologies. Deloitte's support to DPW covers the following security and privacy services: 1. Identity and Access Management (IAM) 2. Security Risk Management and Compliance 3. Security Vulnerability Management (VM) 4. Audit Log Monitoring and Reporting using Security Information and Events Monitoring (SIEM) 5. Data Privacy 6. Security Program Management

Name of Client & Project Title	Commonwealth of Pennsylvania, Department of Public Welfare (DPW) – Project: Information Technology Shared Services (ITSS) – Security and Privacy

The following graphic illustrates Deloitte's history in DPW in establishing complex security foundational infrastructure. Some of these foundational security implementations at DPW became the model for many other Commonwealth agencies:



DPW's Security Program. *Deloitte has been an integral part of DPW's security program since 2001, helping DPW keep abreast of the latest security trends and technologies and effectively managing risks in a rapidly evolving threat landscape.*

Following is the summary of each of services delivered by Deloitte to DPW:

Data Center Architecture

Identity and Access Management – Deloitte initially conducted an assessment of DPW's need for a Web-based single sign-on solution. This included assisting DPW to define business requirements and facilitate product selection. In the later phases of the project, Deloitte assisted DPW to architect and implement the IAM system and services based on CA SiteMinder, CA Identity Manager, IBM Tivoli Identity Manager, Radiant Virtual Directory Services and Microsoft Active Directory. During the past ten years, the implementation has evolved into one of the most comprehensive public sector implementations, spanning multiple agencies and disparate users (employee, business partner and citizen users). This effort has enabled employees, citizens and business partners to have seamless and secure access to the services offered by DPW. The IAM fundamentals established at DPW

Name of Client & Project Title	Commonwealth of Pennsylvania, Department of Public Welfare (DPW) – Project: Information Technology Shared Services (ITSS) – Security and Privacy

have expanded to other large agencies, facilitated by OA/OIT. A recent example is the automation of the user provisioning project, facilitated by OA/OIT. DPW was part of the joint pilot with OA/OIT and Deloitte provided implementation services for this successful automation of more than 20 agencies and 50,000 state employees.

Capacity on Demand & Additional Services:

Key Statistics – Deloitte assists DPW's IAM program for over 45 business applications, serving more than 1,500,000 users and several Commonwealth agencies (L&I, PennDOT, Pennsylvania Insurance Department (PID) and the Department of Aging). The complexity of the infrastructure supporting the DPW IAM program is highlighted by more than 60,000 authentications and four million authorizations each business day.

Services Management

Security Risk Management and Compliance – Deloitte assisted DPW to streamline and manage regulatory audit/risk processes by implementing a unified security regulatory risk framework and automated IT Risk Management (ITRM) solution using the RSA Archer product. Deloitte leveraged its accelerator tool, the "Public Sector Security Risk Framework", and augmented it with relevant Commonwealth regulations and standards. Deloitte then used this customized security risk framework to perform a pilot risk assessment to identify potential gaps and suggest appropriate mitigation steps (one time assessment for several applicable regulations).

Deloitte supported DPW to operationalize and streamline their risk management processs using an automated risk management platform, the DPW ITRM solution using RSA Archer. The ITRM solution helps DPW to proactively determine their risk exposure to the department's security standards, Commonwealth policies, and relevant state and federal regulations such as:

- Internal Revenue Service (IRS) publication 1075
- Health Information Privacy and Accountability Act (HIPAA)
- Health Information Technology for Economic and Clinical Health (HITECH) Act
- United States Social Security Administration Act (SSA)

Key Statistics: Through this program, Deloitte supported DPW to support over 10 external audits including IRS, SSA and HIPAA. The ITRM solution's core integrates more than 4,000 applicable regulatory requirements into 350 unique requirements. In addition, OA nominated the DPW ITRM program for the 2012 NASCIO Risk Management Initiatives category. As an operations improvement area, it used to take DPW two months to respond to the IRS audit questionnaire; using the DPW ITRM solution, DPW was able to respond in three weeks. This questionnaire required responses to more than 350 questions from several functional areas within the department.

DPW's implementation of the ITRM processes and tool is being considered by OA/OIT for adoption as the preferred model for the other Commonwealth agencies to perform security assessments and manage the risks.

Security Vulnerability Management – Deloitte assisted DPW to establish secure development lifecycle principles through integration of application vulnerability testing as part of the project lifecycle. The testing was conducted in a lower test environment using automated tools and manual techniques to identify and remediate security vulnerabilities. The automated tools include HP WebInspect, HP SWFScan and HP DevInspect. A conservative estimate is that in just one year DPW has realized approximately $6.8 million in cost avoidance from credit monitoring fees. In addition, Deloitte supports DPW to

Name of Client & Project Title	Commonwealth of Pennsylvania, Department of Public Welfare (DPW) – Project: Information Technology Shared Services (ITSS) – Security and Privacy

perform periodic infrastructure vulnerability assessments and database security assessments. Keeping up with the evolving trends, in 2012 Deloitte conducted a Cyber Threat Intelligence (CTI) diagnostic assessment on selected DPW systems that helped DPW identify and swiftly mitigate presence of malware.

Key Statistics: In 2012 alone, as part of this program Deloitte performed more than 120 vulnerability scans on 20 Web application releases and infrastructure scans on more than 800 systems. In addition to over 15 Commonwealth Application Certification and Accreditation (CA)² submissions. Using CTI diagnostics, Deloitte analyzed up to one Terabyte of audit log data originating from 200 selected hosts for presence of advanced persistent threats within DPW.

Manage Hosting Services

Audit Log Monitoring and Reporting – Deloitte assisted DPW to design, implement and maintain the RSA envision SIEM solution. The DPW SIEM is an enterprise security audit log collection, processing, monitoring and reporting solution, which collects security information from security infrastructure - server and network devices, firewalls, and custom audit logs from several applications.

Key Statistics: On an average, DPW's SIEM solution processes more than 10,000 security events per second and 9.5 million events monthly from over 730 DPW systems.

Data Privacy – Deloitte assists DPW to help determine secure practices to collect and handle Personally Identifiable Information (PII) through the department's intake systems. Deloitte helps DPW to manage their PII catalog that tracks the presence of PII on reports, correspondences and notices. In addition, Deloitte coordinates with the privacy officers of DPW, the Department of Aging and PID to assist in incident response and standards and meet privacy regulatory requirements.

Key Statistics: DPW PII catalog maintains an inventory of PII present on more than 1,000 reports, mailed reports, correspondences and notices.

Information Security Program Management – As DPW continued to evolve their security and privacy program for the past 10 years, Deloitte played a crucial role in elevating and maturing the security program and governance. Deloitte assists in the facilitation of a security and privacy steering team that includes participation of the privacy officers of the DPW, Aging and Insurance agencies.

Awards and Recognition – The security initiatives have helped DPW realize the following recognitions:

- Computerworld Honors Laureate Recognition (IAM), 2007
- Award for "Best Agency Collaboration" at the Pennsylvania Digital Government Summit – for the Identity and Access Implementation that is shared between DPW and the Department of Labor and Industry, 2008
- National Association of State Chief Information Officers (NASCIO) Award for Enterprise Information Technology (IT) Management Initiatives, 2009
- Computerworld Honors Laureate Recognition (Security Vulnerability Testing Shared Service), 2010
- NASCIO Finalist in the Enterprise IT Management Category (OA/OIT Automated User Provisioning project), 2012.

Name of Client & Project Title	Commonwealth of Pennsylvania, Department of Public Welfare (DPW) – Project: Information Technology Shared Services (ITSS) – Security and Privacy
Project Duration:	**Start Date Year:** 2001 — **End Date Year:** On-going
Nature of the Client:	The Department of Public Welfare (DPW) is the largest of the Commonwealth of Pennsylvania's agencies. DPW is responsible for meeting the needs of over two million clients with the assistance of 15,000 support workers, 500,000 providers, and 300,000 employers.
Nature of Client Audience:	DPW: Chief Information Officer (CIO), Chief Technology Officer (CTO), Chief Information Security Officer (CISO), Privacy Officer(s) and the security team
Number of Users:	More than 300,000 users including DPW staff, contractors, business partners and citizen users. Combined DPW and L&I citizen user population exceeds 1.5 million users.
# & Composition of Vendor Employees & Consultants Assigned:	As DPW's program offerings and technology evolve, Deloitte leverages our large pool of highly qualified security professionals to bring the right skill set, in time, to meet DPW needs. Deloitte serves DPW with a team of highly experienced and certified security professionals. Deloitte's current DPW security team includes eight to ten full time practitioners led by Srini Subramanian, Principal, Deloitte & Touche LLP. The team's composition includes: • Senior Security Architect, • Security Architects, • IAM specialists, • VM specialists, and • Risk Management specialist.
Client Contact Information:	**Reference Contacts:** **Name:** [redacted] **Title:** [redacted] **Department:** Department of Public Welfare OA-BIS-Division of Technology Engineering **Full Address:** [redacted] **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** DPW Project Manager **Name:** [redacted] **Title:** [redacted] **Department:** Department of Public Welfare, OA-BIS-Division of Technology Engineering **Full Address:** [redacted] **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** DPW Security Lead

Deloitte Project Preference 2: State of Utah

Name of Client & Project Title	State of Utah – Enterprise Security Assessment
Contract Value	Not available for public disclosure
Nature and Scope of Project:	**Project Description** Deloitte was engaged in May 2012 by the State of Utah to perform security assessments. Deloitte's role was to perform an enterprise-wide security assessment on the information systems and processes that comprise the State's IT security infrastructure services for those agencies managed by Department of Technology Services (DTS). **Security Services** As part of the project, Deloitte's security and privacy professionals worked with the state's Chief Information Officer and other stakeholders to assess security practices and controls of the state agencies against regulatory requirements and industry-standards. Additionally, Deloitte worked with the State to perform technical vulnerability assessments and cyber threat diagnostics for external and internal systems. Deloitte leveraged their accelerator tool, "Public Sector Security Risk Framework", which was augmented with relevant Utah's regulations and standards. The framework was used to assess each in-scope state agency's security policies, processes and controls. **Program Management Office and Service Management** Deloitte provided the state with reports for each in-scope state agency. These reports documented the agency's adherence to the security framework identifying potential risks with the current process or controls. Additionally, Deloitte submitted a statewide report that documented enterprise wide results and trends. Deloitte's reports provided detailed findings and recommendations to address both tactical and strategic security concerns while enhancing current capabilities, elevating maturity levels in protecting information assets and achieving compliance.
Project Duration:	**Start Date Year:** May 2012 | **End Date Year:** December 2012
Nature of the Client:	The State of Utah serves approximately 2.8 million citizens. The executive branch of Utah's government is made up of 35 separate agencies including the Department of Technology Services. In 2005, Governor Jon M. Huntsman Jr established the DTS in response to the Utah Technology Governance Act (H.B.109). Since that time, under the State's Chief Information Officer (CIO), DTS has embarked on an unprecedented transition to consolidate the state's IT resources and services for the State into one department to improve accountability, reduce costs, increase services to taxpayers, and more closely align IT with the business needs of the State. DTS is responsible to manage the State IT infrastructure that includes: • More than 500 servers • More than 20,000 desktops • More than 1,000 online services • More than 890 business applications and more than 250 application projects • More than 15,000 service requests per month • 24/7 continuity of operations for state, local and education entities at the Richfield Data Center

Name of Client & Project Title	State of Utah – Enterprise Security Assessment
Nature of Client Audience:	Not available for public disclosure
Number of Users:	Not available for public disclosure
# & Composition of Vendor Employees & Consultants Assigned:	Deloitte leveraged our large pool of highly qualified security professionals to bring the right skill set, in time, to meet the state's needs. Deloitte served the state with a team of highly experienced and certified security professionals. Deloitte's security team included: • Security risk management specialists • Security vulnerability management specialists • Forensic specialists
Client Contact Information:	**Reference Contacts:** **Name:** [redacted] **Title:** [redacted] **Department:** Office of Fiscal Operations, Department of Health **Full Address:** 288 N. 1460 W. Salt Lake City, UT 84116 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** Project Manager **Name:** [redacted] **Title:** [redacted] **Department:** Department of Technology Services **Full Address:** 1 State Office Building Floor 6 Salt Lake City, UT 84114 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** Steering Committee Member

Deloitte Project Preference 3: Commonwealth of Massachusetts

Name of Client & Project Title	Commonwealth of Massachusetts, Information Technology Division (ITD) – Commonwealth of Massachusetts Data Center Consolidation and MA - Department of Revenue, MASSTAX2
Contract Value	Not available for public disclosure
Nature and Scope of Project:	**Project 1: Commonwealth of Massachusetts Data Center Consolidation – Strategy, Planning, and Implementation assistance.** **Project Description** Deloitte was engaged in 2009/2010 to assist the Commonwealth of Massachusetts with the strategy, planning, road map and implementation assistance for their data center consolidation initiative. The Deloitte team assisted the Commonwealth to scope, plan and implement a statewide IT Consolidation Program for the Commonwealth's central IT Department (ITD) and eight Secretariats. As part of the engagement, Deloitte developed an overarching IT Consolidation vision, strategy, and approach, along with detailed consolidation plans for each of the 8 Secretariats covering 150+ agencies. In Phase 2 of the project, Deloitte provided implementation support that was targeted to result in the Commonwealth achieving 18 percent+ savings in IT operating costs **Program Management Office and Services Management** The Deloitte team assisted the Commonwealth to scope, plan and implement a statewide IT Consolidation Program for the Commonwealth's central IT Department (ITD) and eight Secretariats. As part of the engagement, Deloitte developed an overarching IT Consolidation vision, strategy, and approach, along with detailed consolidation plans for each of the 8 Secretariats covering more than 150 agencies. In Phase 2 of the project, Deloitte provided implementation support that was targeted to result in the Commonwealth achieving 18 percent+ savings in IT operating costs. Deloitte worked closely with the State CIO, Secretariats, and agency CIOs to develop a detailed consolidation plan as part of phase 1, followed by implementation support for Phase 2. The strategy and implementation roadmap developed as part of Phase 1 addressed constraints related to IT Governance, Financial Processes and Chargebacks, IT Workforce Redeployment and Training, and Change Management. In addition, it included the core consolidation activities related to infrastructure and applications. **Data Center Architecture** As part of the project, Deloitte's security and privacy experts helped the Commonwealth with the foundational security architecture and approach required for the future consolidated model. Deloitte's security and privacy professionals worked with the Commonwealth's Chief Information Security Officer and other stakeholders to help design enterprise security architecture for the consolidated data center. **Services Management and Technical Services** During the project's initial phase, the Deloitte team worked with IT leadership from ITD and the agencies to develop a detailed strategy and implementation roadmap to consolidate key IT services, such as Data Centers, Networks, E-mail, Help desk services, Desktop and LAN services, and Web site information architecture and Applications, under a federated model. For each of these threads, the Deloitte team worked collaboratively with

Name of Client & Project Title	Commonwealth of Massachusetts, Information Technology Division (ITD) – Commonwealth of Massachusetts Data Center Consolidation and MA - Department of Revenue, MASSTAX2

stakeholders in the shared services IT organization and at individual Secretariats and agencies to assemble consolidation plans, which included:

- Current state and gaps
- Security assessment to understand current challenges
- Key consolidation requirements
- Future-state vision and targets, including security architecture
- Timeline and activities

In a subsequent planning phase, the team worked to build a detailed executable plan for each area, adding:

- "Playbook" based strategies to perform technology consolidation
- Detailed timelines and consolidation sequencing
- Staffing and organizational impacts and estimates
- Infrastructure estimates
- Detailed dependency analysis

During the implementation phase, the Deloitte team worked with the Commonwealth to:

- Setup a PMO to manage the various threads in an integrated fashion
- Identify risks and manage them effectively to resolution
- Coordinate the activities of the various agencies to meet the overall milestones identified in the implementation roadmap
- Provide industry leading practices to jumpstart activities related to IT service delivery, pricing models and chargebacks, staff consolidation, change management, and communication

To support implementation efforts, the Deloitte team provided advisory services in a number of foundational areas, including security and privacy. In each area, Deloitte SMEs were key participants in client working groups and sub-committees, and helped achieve the outcomes described below:

- **IT Governance.** Implement processes and tools to track consolidation benefits and conduct case study analysis to quantify the benefits of IT consolidation
- **IT Finance –** Develop processes to effectively allocate costs across agencies and identify operational aspects related to federal fund/grant/trust funding
- **HR/Labor/Talent –** Develop processes and tools to plan and transition staff into a shared services model, and train workforce on the ITIL framework
- **Communications –** Provide regular updates and communications to IT employees to involve them in the consolidation process, prepare summary reports for the Governor and other Commonwealth leadership
- **Provide security advisory services –** The team performed an assessment of the state of security, and provided advisory services on the future security architecture in the consolidated data center model.

Name of Client & Project Title	Commonwealth of Massachusetts, Information Technology Division (ITD) – Commonwealth of Massachusetts Data Center Consolidation and MA - Department of Revenue, MASSTAX2	
	Project 2: MA – Department of Revenue, MASSTAX2 **Project Description** In 2011, the Commonwealth awarded a contract to Deloitte Consulting to implement a SAP based state tax and revenue solution. As part of this project, the Deloitte security and privacy team is delivering the following services: • Security risk assessment and compliance with Internal Revenue Service (IRS) publication 1075 requirements • Disaster recovery and business continuity plan development • Implementation of the following security controls: – SAP application security – SAP Governance, Risk, and Compliance (GRC) Access Control (AC) 10.0 – SAP User Experience Monitoring (UEM) – Identity and Access Management system – Data Leakage Prevention (DLP) – Database Activity Monitoring (DAM) – Security Information and Event Monitoring (SIEM) solution.	
Project Duration: (Data Center Consolidation)	**Start Date Year:** March 2009	**End Date Year:** June 2010
Project Duration: (MASSTAX2)	**Start Date Year:** January 2011	**End Date Year:** On-going
Nature of the Client:	**Commonwealth of Massachusetts Information Technology Division** The mission of the Information Technology Division is to support, enable and transform state government through the strategic use of technology to better serve constituents, businesses, and local government. The Information Technology Division (ITD) enables agencies to deliver high quality, efficient and effective services to their customers, by providing a range of centralized IT services; overseeing IT policies, standards and architecture; and promoting cross-agency collaboration and adoption of shared services. The Division is part of the Executive Office of Administration and Finance and is headed by the Commonwealth Chief Information Officer. While the agencies work directly with their customers, ITD works with the agencies as a service provider to ensure their customers' needs are met. Most services offered by ITD are processed through direct chargeback. ITD is structured around seven lines of business: • Applications • Print and Mail • Integration • Unified Communications • Hosting • Data Services • Security	
Nature of Client Audience:	Commonwealth of Massachusetts – CIO, CTO, CISO and agency stakeholders	

Name of Client & Project Title	Commonwealth of Massachusetts, Information Technology Division (ITD) – Commonwealth of Massachusetts Data Center Consolidation and MA - Department of Revenue, MASSTAX2
Number of Users:	Not available for public disclosure
# & Composition of Vendor Employees & Consultants Assigned:	Deloitte leveraged our large pool of highly qualified security professionals to bring the right skill set, in time, to meet the Commonwealth's needs. Deloitte served the Commonwealth with a team of highly experienced and accomplished security professionals. **Deloitte's security team composition includes:** • Senior Security Architect • Security Architect • Risk Management specialist
Client Contact Information:	**Reference Contacts:** **Name:** [redacted] **Title:** [redacted] **Department:** Information Technology Division **Full Address:** 200 Arlington Street, Suite 2100 Chelsea, MA 02050 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** Project Lead (Datacenter Project) **Name:** [redacted] **Title:** [redacted] **Department:** Department of Revenue **Full Address:** 200 Arlington Street Chelsea, MA 02150 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** DOR Security Team Lead (MASSTAX2 Project)

4.5.4 Acclaim Systems, Inc. Project References

Acclaim Systems Inc. Project Preference 1: Pennsylvania Department of State

Name of Client & Project Title	Pennsylvania Department of State – State's Statewide Uniform Registry of Electors (SURE)	
Contract Value	$8.8 million	
Nature and Scope of Project:	**Project Description** Acclaim is responsible for the management, maintenance and enhancements to the SURE system. Project is for 5 years with a contract value of over 8.8M. Project involves Project Management, Maintaining SLAs, Service Management, Technical support, Capacity Planning, Operations Support. We have worked with the Unisys team on this project for Data Center activities. The SURE Election System Manager is the registration system used to administer 8 million Pennsylvania voters across 67 counties in support of the election process. The system handles election setup, voter application processing, precinct management, poll book generation, absentee balloting, reporting, and correspondence generation. These applications support the voter registration process within the Commonwealth of Pennsylvania. **Technical Services** Providing complete Life Cycle Development in the development and implementation of the State's Statewide Uniform Registry of Electors (SURE) system and on-going maintenance and support of the State's Statewide Uniform Registry of Electors (SURE) system.	
Project Duration:	**Start Date Year:** 2009	**End Date Year:** On-going
Nature of the Client:	Pennsylvania Department of State	
Nature of Client Audience:	67 counties	
Number of Users:	More than 8 million	
# & Composition of Vendor Employees & Consultants Assigned:	**Vendor Project Manager/Key Consultant on Project Team:** Cassius Arulkumaran is PM. On an average we have 30 consultants on this project at any time.	
Client Contact Information:	**Reference Contacts:** **Name:** [redacted] **Title:** [redacted] **Department:** Pennsylvania Department of State **Full Address:** 210 North Office Building Harrisburg, PA 17120 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** Project Manager	

Name of Client & Project Title	Pennsylvania Department of State – State's Statewide Uniform Registry of Electors (SURE)
	Name: [redacted] **Title:** [redacted] **Department:** Bureau of Commissions, Elections, and Legislation **Full Address:** 210 North Office Building Harrisburg, PA 17120 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** Client Project Manager

Acclaim Systems Inc. Project Preference 2: Time Warner Cable

Name of Client & Project Title	Time Warner Cable – salesforce.com implementation	
Contract Value	$6 million	
Nature and Scope of Project:	**Project Description** Salesforce.com's CRM (Customer Relationship Management) solution provides support through several applications: Sales, Service & Support, Partner Relationship Management, Marketing, Content, Ideas, and Analytics. This implementation will assist Time Warner Cable in managing their services that pass through more than 26 million U.S. homes serving 13.5 million basic video customers. We provided entire life cycle of salesforce.com solutions—from initial business need assessment to implementation of new capabilities as your business grows and changes. Project is ongoing with a contract value of more than $6 million. Project involved Project Management, Service Management, Technical support, Capacity Planning, Operations Support, and Training. **Program Management Office (PMO) and Service Management** • Discovery, mapping, and modeling of sales or support business processes • Early prototyping of new processes in salesforce.com • Detailed project plan • ROI/TCO analysis in the discovery and project phases • Customization of salesforce.com to enable best practice sales, marketing or support processes • On-site training **Technical Services** • Migration to salesforce.com from legacy on-premise systems and integration with other core systems • IT and business user training and change management • Customized development to extend salesforce.com • Integrating AppExchange applications • Maintenance and support	
Project Duration:	**Start Date Year:** 2009	**End Date Year:** On-going
Nature of the Client:	Time Warner Cable	
Nature of Client Audience:	Time Warner Cable users (commercial, residential)	
Number of Users:	More than 5,000	
# & Composition of Vendor Employees & Consultants Assigned:	**Vendor Project Manager/Key Consultant on Project Team:** Project started with about 10 to 15 consultants and is now down to approximately 7 on average every year. Consultants currently provide architecture, implementation, administration, and support.	

Client Contact Information:	Reference Contacts:
	Name: [redacted] **Title:** [redacted] **Department:** Technical Services Group, Time Warner Cable **Full Address:** 707 Revival Row, Fort Mill SC 29708 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** Project Manager
	Name: [redacted] **Title:** Technology Manager – IT Operations **Department:** IT Operations **Full Address:** 910 Crescent Executive Drive, Charlotte, NC 28217 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** Project Manager

UNISYS

Acclaim Systems Inc. Project Preference 3: Unisys – Pennsylvania Office of Administration

Name of Client & Project Title	Unisys – Pennsylvania Office of Administration (OA) Project	
Contract Value	$1 million	
Nature and Scope of Project:	**Project Description** Acclaim Systems provides administration for multiple servers with SQL Server 2000, SQL Server 2005 and SQL Server 2008 Enterprise (35 Production and 30 Staging and lab Servers in total). These servers support OA's development, test, and production environments. Additionally we administer databases hosted with Oracle 10g RAC and Oracle 9i Fail-safe. Acclaim Systems provides the Office of Administration with database support for Applications on 400 Web servers and for the High Availability SQL Server environment using MS Clustering Technologies (15 servers). • Successfully installed 2-Node Oracle 10g RAC (Real Application Clusters) from scratch with ASM (Automated Storage Management) as the file system controlled Oracle Cluster Services. • Successfully installed and Configured Oracle 10g Grid Control. Installed and configured 10g agents on all the Oracle Servers to maintain them from a single-point. • Successfully implemented Replication (Merge – High availability) between non-trusted domains and the consolidation of servers. • Solid experience on T-SQL programming. • Created and maintain standby environment for Business Critical Applications.	
Project Duration:	**Start Date Year:** 2009	**End Date Year:** On-going
Nature of the Client:	State Government (Pennsylvania) / Unisys, Agency is Office Automation	
Nature of Client Audience:	Government users	
Number of Users:	More than 1,000	
# & Composition of Vendor Employees & Consultants Assigned:	**Vendor Project Manager/Key Consultant on Project Team: What did they do?** Oracle/SQL DBA and Developers	
Client Contact Information:	**Reference Contacts:** **Name:** [redacted] **Title:** [redacted] **Department:** Pennsylvania Office of Administration, Bureau of Infrastructure & Operations **Full Address:** [redacted] **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** Client Side Manager	

Name of Client & Project Title	Unisys – Pennsylvania Office of Administration (OA) Project
	Name: [redacted] **Title:** [redacted] **Department:** PA Office of Administration, Bureau of Infrastructure & Operations **Full Address:** [redacted] **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** Project Manager

4.5.5 American Personnel Managers and Consultants, Inc. Project References

APMC Project Preference 1: Commonwealth of Pennsylvania

Name of Client & Project Title	Commonwealth of Pennsylvania – Data PowerHouse (DPH) (Subcontractor to Unisys)
Contract Value	$8 million
Nature and Scope of Project:	**Project Description** Under a Directive from Governor Tom Ridge in 1997 to improve the delivery of public services through the strategic use of information technology, the Governor's Office of Administration initiated data center consolidation of Commonwealth agencies. Implementing the consolidation and outsourcing operations and technical support functions for 17 formerly separate state agency Data Centers. The Data PowerHouse (DPH), managed by a consortium of 10 companies, led by Pennsylvania-based Unisys, replaced these 17 separate state-run data centers. The services outsourced to Unisys include program management, mainframe and midrange operations systems management, tier-two help desk, related technical support services such as media services, console operations, disaster recovery, application development, and maintenance, desktop management, etc. American Personnel Managers and Consultants also provide: • Recruitment • Retention • Staffing • HR Management for media services, console operators; and administrative staff State agencies participating in the Data PowerHouse include: • Departments of Public Welfare • Revenue Aging • Corrections • Labor and Industry • Health • Transportation • Department of Education • Civil Service Commission • Pennsylvania State Police • Public School Employees' Retirement System • Public Utility Commission • Pennsylvania Game Commission • Liquor Control Board **Program Management Office and Services Management** American Personnel Managers and Consultants Inc. has the breadth and depth of concurrent proficiencies related to the DPH providing more than 13 years' experience as Human Resource/Staffing Managers in the Data Center, specific to overall Data Center Computing Service Staffing that includes media services, console operations, and administrative services. Our Pennsylvania local management team offers more than 90 years of Operations and Management capabilities, with current long-term tenured Management staff working on the DPH as a business partner for both Unisys and IBM.

Name of Client & Project Title	Commonwealth of Pennsylvania – Data PowerHouse (DPH) (Subcontractor to Unisys)

Our entire team provides a depth of knowledge, understanding, and involvement in all phases of our designated scope of work at the DPH that has helped achieve our 13 years of success.

We staff and manage the DPH 365x24 hours, providing full coverage, staff backup and cross training to meet the needs and goals of the DPH project.

Project Management – The primary objective of our Project Manager at the Data Center is to achieve all of the project goals and objectives while adhering to preconceived constraints. The primary constraints are scope, time, quality, and budget. The secondary — and more ambitious — challenge is to optimize the allocation of necessary inputs and integrate them to meet pre-defined objectives as required in our DPH contract. Our team has been very successful in this aspect of the project, never experiencing an SLA in 13 years on the project.

Administrative Support staff (Unisys and IBM) – Project Office Administrator for the Project Office Management Team

Administrator tasks include – but are not limited to:

- Procedural setups (On boarding & Off boarding processing instructions and requests, Quarterly Evaluation Verifications (QEV), Weekly Extract of Linux AD Users Verifications, COPSEC Notes ID Database,
- Prepares and assemble monthly status reports
- Prepares and assemble weekly reports
- Assemble and maintain log of all Annual Renewal Request and Annual Trainings
- Prepare and Maintain Desk Procedures
- Assemble monthly deliverables
- Background & security administration
- Other Administrator tasks as necessary

Services – The following services are provided by APMC employees:

- Oversees tape management systems by operating a computer terminal, maintain control and security of computer tapes
- Verifies, corrects, updates, and deletes information on tape labels, and codes
- Labels and codes newly created tapes based upon content, system, user, creation date, retention date, and number of reels
- Generates media services reports
- Assists in developing, revising, documenting, and implementing media services procedures per client request and specifications
- Controls and coordinates tape flow between the library and security vault
- Maintains an adequate inventory of scratch tapes for the computer room
- Controls the checking of tapes in and out of the automated media services system
- Reviews daily data processing production reports and identifies tape-related production problems, master tapes created, jobs completed, tapes to be reissued, and tapes for vault storage
- Trains new employees in routine library tasks
- Stores tapes and maintains logs according to client classification and retention criteria
- Coordinates the quarterly inventory of the media services and maintenance of the security vault
- Reports processing problems caused by tape errors to supervisors

Name of Client & Project Title	Commonwealth of Pennsylvania – Data PowerHouse (DPH) (Subcontractor to Unisys)

- Works with client to Schedule periodic evaluations of the condition of all tapes in the library and reissues or replaces worn or damaged tapes per client direction
- Orders replacement tapes and enters them into the automated library system
- Maintains records of all tapes issued, replaced, or damaged
- Performs related duties as assigned
- Performs duties related to a computer cataloging system
- Performs General data processing and data control procedures

Recruitment – APMC provides recruiting, interviewing, computerized testing, reference checking, clearance follow-up, and hiring of staff to the Unisys DPH project. We currently supply 22 people to the DPH project that support services in the areas of Media Services, Console Operations, and Administrative staffing. The stages of the recruitment process include: job analysis and developing a 'person' specification; candidate sourcing by networking, advertising, or other search methods; matching candidates to the specific job requirements of the DPH project, and screening individuals using testing (skills or personality assessment); assessment of candidates' motivations and their fit with organizational requirements. Testing tools include the use of interviewing, background checks, and drug testing. The recruitment process also includes the making and finalizing of offers and the induction and on boarding of new employees to the DPH.

Console Ops Recruits, Staffs, Manages, 365x–24hr operation, Console operations and monitoring, Help Desk 1, and Help Desk 2 – Level 2 Help Desk support where our staff interfaces with the Commonwealth's Level 1 Help Desk to provide effective problem communication and resolution. We provide console operators monitoring support for the monitoring centers, experienced, detail oriented staff that are promoted from our seasoned employees in the Media services. We have promoted 10 employees from the Media services to Console ops over the last 4 years, and during the life of the project have provided 50 staff members to IBM and Unisys for console ops positions.

Console operators functions include: On Site Physical staffing and monitoring of 22 Commonwealth agencies, following rigid Commonwealth and Console procedures to monitor and operate Unisys mainframes, Windows/UNIX/AIX servers in a 7x24/365 consolidated Data Center to meet high service delivery requirements for public sector. Staff are responsible for observing multiple monitor screens for alerts, alarms and indicators of abnormal processing for any mainframe or server systems included in the monitored group using manual and automated processes.

Retention – Our ability to retain our key employees has been a critical competitive advantage in today's economy. This has benefited the DPH, Unisys, and American Personnel Managers and Consultants. We have always practiced the belief that key employee retention was critical to the long-term health and success of the contract. Retaining the best employees ensures customer satisfaction, satisfied coworkers, effective succession planning, and deeply imbedded organizational knowledge and learning. Some of our employees have been on this project 10 or more years. Our turnover rate in the past 12 months is 1 percent and more than 2 percent over the past 13 years.

Scheduling – One of the most important tasks is scheduling employees. Creating work schedules to meet the needs of the Data Center, while satisfying the needs of the employees. The monthly schedule is created by our Staffing Manager. This schedule is created to make sure the exact number of employees is always in place to run the Media

services as needed on 24 hours per day, 7 days per week basis. This also entails

Name of Client & Project Title	Commonwealth of Pennsylvania – Data PowerHouse (DPH) (Subcontractor to Unisys)
	rescheduling as needed for employees illnesses, vacations, inclement weather etc. We are on call 24/7 if problems should occur after the normal business day.
Project Duration:	**Start Date Year:** 1999 — **End Date Year:** on-going to 2014
Nature of the Client:	Information Technology
Nature of Client Audience:	Commonwealth agencies
Number of Users:	22 agencies
# & Composition of Vendor Employees & Consultants Assigned:	**Vendor Project Manager/Key Consultant on Project Team:** Pat Gingrich, President Describe start-up, peak, and ongoing level of vendor efforts: 22 staff members: Media Services 12 staff members; Console Ops 3 staff members; Administrative 2 staff members – on site.; Management team 1 member; P. Gingrich 1 president; Staffing Manager 1 staff member; Payroll 1 staff member; Recruiter 1 administrative
Client Contact Information:	**Reference Contacts:** **Name:** [redacted] **Title:** [redacted] **Department:** Global Managed Services **Full Address:** Unisys, 4750 Lindle Road Harrisburg, PA 17111 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** Account Executive **Name:** [redacted] **Title:** [redacted] **Department:** Global Managed Services **Full Address:** Unisys, 4750 Lindle Road Harrisburg, PA 17111 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** IBM Manager **Name:** Jack Roadcap **Title:** ITD - SSO CoPA IBM Data Center

Name of Client & Project Title	Commonwealth of Pennsylvania – Data PowerHouse (DPH) (Subcontractor to Unisys)
	Department: CoPA IBM Data Center **Full Address:** [redacted] **Telephone:** [redacted] **E-mail:** **Relation/Role to Project:** Data Center Manager **Name:** [redacted] **Title:** [redacted] **Department:** N/A **Full Address:** 20 N. Second St, Suite 200, Harrisburg, PA 17101 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** [redacted]

APMC Project Preference 2: Parsons Corporation

Name of Client & Project Title	Parsons Corporation – Call Center Commonwealth of Pennsylvania Department of Transportation
Contract Value	$1.2 million (over 5 years)
Nature and Scope of Project:	**Project Description:** American Personnel Managers and Consultants, Inc. has established a centralized call center for Parsons Corporation, and the Commonwealth of Pennsylvania Department of Transportation. Our call center incorporates inbound teleservices with excellent staff communication and customer service skills including problem solving, pro actively providing the best customer service, continued follow up with customers as needed, providing e-mail response, escalation etc., "as needed". Our commitment to best practices, providing the highest levels of quality, standards of excellence and superior customer services includes working closely with Parsons to insure Commonwealth satisfaction. As call center Project Managers, we utilized our Management and overall business experience to review test, select the best software for this project to meet performance metrics used in the call center. The Commonwealth of Pennsylvania requirements are identical in scope but to a lesser degree or higher degree based on specifications designated by the Commonwealth agency. **Services Management and Staff Augmentation** APMC currently supports the Pennsylvania Drive Clean Emissions call center project Help Desk services. The responsibilities of Managing and Staffing the call center include confirming caller's questions are handled according to specified scope of work. APMC is responsible for Call Center software selection, project oversight and management, day to day operational and HR issues within our scope of work. APMC provides staff and on site project management to: supervise, manage, train, and effectively administer all aspects of the call center. Additionally, our team is responsible for answering calls in the queue within a very specific timeframe; provides responses to caller's questions per Commonwealth standards; and escalate calls if necessary. APMC also provides monthly reports documenting Help Desk activity as approved by the Commonwealth including operational minutes available, outage (or downtime) minutes, and customer wait time in the queue for the previous month. Monthly client meetings, pro-active client goals and objectives achieved, and overall customer satisfaction based on Six Sigma processes. Project scope of staffing is not as complex as Console Operations staffing, but similar in many areas such as project oversight and management; day-to-day operations, Human Resource (HR) issues within our scope of work, and staff training. **Transition Planning** Transition planning follows past project experiences related to HR and Staff Augmentation projects of 500 people transitioned to our team. Our project included staffing and technical services where the end result has met Project expectations. Our Transition Plan identifies all scope of work, out-of scope items, all affected areas and documents, and the overall strategy of transitioning staff. Our Transition Plan starts with a Due Diligence phase with the framework in place. It is very critical for the client to mutually agree on the Transition Plan to prevent any impact during the transition period. Our Transition Plan could have the following items in the Table of Content document – scope, transition strategy, transition schedule, governance covering client and the team along with roles and responsibilities, communication plan, escalation process, progress review meetings, status reporting, milestones clearly identified, risks, and mitigation plan. Our transition strategy includes

Name of Client & Project Title	Parsons Corporation – Call Center Commonwealth of Pennsylvania Department of Transportation	
	transition strategy for each functional area taking into consideration each line of business.	
Project Duration:	**Start Date Year:** Fall 2012	**End Date Year:** Ongoing
Nature of the Client:	Pennsylvania Emissions clean air program – Scope – Call Center/Help Desk APMC has established a state of the art call center at Parsons Corporation Call Center Commonwealth of Pennsylvania Department of Transportation. This call center incorporates inbound teleservices, e-mail response, etc. Our commitment to best practices provides the highest levels of quality, standards of excellence, and superior customer services. Includes software selection and performance metrics used in the call center.	
Nature of Client Audience:	Emissions program – Commonwealth Clean Air	
Number of Users:	Approximately 8000 centers throughout Pennsylvania	
# & Composition of Vendor Employees & Consultants Assigned:	**Vendor Project Manager/Key Consultant on Project Team:** Pat Gingrich, President/CEO – Operations Manager Nancy Griffin, Project Manager (On-site day to day operations) At project start up, American Personnel Managers & Consultants Inc. met regularly with the client preparing for transition from the Verizon contract with the Commonwealth to the Parsons contract award. Our Clear definition of project needs analysis, staff and project requirements; business operation processes, timeline, etc, were outlined and approved. Review , testing and selection of call center "best practices" business services product platforms was completed with approval from Parsons. Go live processes were planned, reviewed, and approved with staff selection and training completed and movement to "readiness" status. With project implementation and project started, calls swelled more than 10 times in the initial few days – technical telephonic system and staff pushed. American Personnel pro-actively addressed both technical teleservices and expansion with positive results adding more staff and telephonic capabilities. Ongoing efforts include continued staff training and system updates as needed, quality assurance goals and objectives, daily customer communication via e-mail or phones, quarterly in person client meetings projected, daily usage and performance reports to clients, and monthly usage and performance reports to client.	

Name of Client & Project Title	Parsons Corporation – Call Center Commonwealth of Pennsylvania Department of Transportation
Client Contact Information:	**Reference Contacts:** Parsons Environment & Infrastructure Group Inc. **Name:** [redacted] **Title:** [redacted] **Department:** Environmental & Infrastructure Group, Inc. **Full Address:** Parsons Corporation 979 East Park Drive Harrisburg, PA 17111 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** Project Operations **Name:** [redacted] **Title:** [redacted] **Department:** Environmental & Infrastructure Group, Inc. **Full Address:** 401 Commerce Park Drive Cranberry Township, PA 16066 **Telephone:** [redacted] **E-mail** [redacted] **Relation/Role to Project:** Manager

APMC Project Preference 3: Pennsylvania Higher Education Assistance Agency

Name of Client & Project Title	Pennsylvania Higher Education Assistance Agency (PHEAA) – Data Domain Implementation
Contract Value	$1 million
Nature and Scope of Project:	**Project Description** APMC is an authorized EMC reseller of products and services and provided Project Management for all phases of the Pennsylvania Higher Education's Data Domain implementation with its subcontractor EMC. APMC's Project Management responsibilities included: regular client meetings; comprehensive understanding review and validation of client requirements, scope of work required, implementation process, services and guarantees needed, with a mutually agreed timeline and final quality review. Additional work was also performed upon completion of the Data Domain implementation project, with a physical move and support services of equipment etc., to an alternate location as designated by PHEAA. Both projects completed on time, and with an excellent quality rating. APMC manages subcontractor functions that are inherent to all contracts and monitors and management of prime and subcontract requirements. EMC's multi faceted experience provided an excellent cornerstone for project success. Project comparisons are based on our ability to independently manage a project thereby meeting overall operational requirements, including quality, cost containment, ongoing customer communication and satisfaction. We provide onsite assistance for day-to-day staff direction, training, supervision, management, and a course of action necessary to retain project success. Those characteristics are representative of this project where we have successfully contained cost, retained staff with less than a 1 percent turnover in the past 12 months, and provide ongoing management support to retain quality and project excellence. The Commonwealth of Pennsylvania requirements in the use of project management and contractor management are similar in function. The project is similar in function where APMC had overall responsibility for the PHEAA project working in a team effort with our subcontractor – EMC to manage the PHEAA project ensuring all facets of the project were delivered on time. Our team defined the scope of work requirements, necessary resources required to perform the project, participated in client communications, meetings, and collaborations to meet all required components of the PHEAA project for quality assurance throughout the project. **Program Management Office (PMO) and Service Management** APMC and the client both assigned a Project Manager to facilitate effective project management controls. Both parties submitted to the other in writing, the name, business address and telephone number of the individual who is designated as their Project Manager during the life cycle of the project. Each manager set up the process and procedures related to reports, measurements and new requirements with on-going communication, focus and project dedication. APMC worked with our management group, EMC technicians, members of the EMC management team and PHEAA managers to provide a requested solution to PHEAA's business needs. Our DeDup solution was selected to address PHEAA'S backup and long-term archive business requirements. We provided PHEAA with necessary information required to make a decision best meeting their solution needs. Additionally, detailed product and service pricing was given to assure requirements were met to fulfill the needs of PHEAA.

Name of Client & Project Title	Pennsylvania Higher Education Assistance Agency (PHEAA) – Data Domain Implementation
	Technical Services Technical Services were always managed by an experienced project manager to insure tasks and schedules were adhered to during the life of the PHEAA project. Such information was reported to the PHEAA project manager to ensure all tasks were met in a timely basis with no impact to the overall project. Management reporting was provided on a timely basis relative to each task. Our technical team worked continuously through project implementation and completion, providing a scalable, cost effective solution for high output and long-term data retention use. We provided the direction, implementation, supervision, management, and course of action for the DeDup solution through project end, with ongoing customer satisfaction requirements project scope
Project Duration:	**Start Date Year:** 2011 — **End Date Year:** 2011
Nature of the Client:	2 phases – Data Domain Implementation & Client equipment relocation, installation etc.
Nature of Client Audience:	Upgrade & New location building facilities
Number of Users:	Not applicable
# & Composition of Vendor Employees & Consultants Assigned:	**Vendor Project Manager/Key Consultant on Project Team:** Pat Gingrich **Start up and ongoing level of APMC team efforts:** Project Employees Included 10 members of our Management team, technical staff, technical support staff, implementation staff, on-site Project Management, administrative support, etc. **Start up:** Initial client management and APMC team meetings were held with the PHEAA Technical Team, Contract Manager. Subsequently, meetings were held for ongoing PHEAA discussions, feedback, review, client applications, solution discussions, overview presentation, client Q&A discussions, APMC Project award, project and management team ramp up, team scope performance, Ongoing Team Performance Review, Ongoing Client review and approval, and Project completion.
Client Contact Information:	**Reference Contacts:** **Name:** [redacted] **Title:** [redacted] **Department:** Contracts **Full Address:** 1200 North 7th Street Harrisburg, PA 17102 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** Contract Officer **Name:** [redacted] **Title:** [redacted] **Department:** Information Technology **Full Address:** Pennsylvania Higher Education Assistance Agency, t/d/b/a American Education Services 1200 North 7th Street Harrisburg, PA 17102 **Telephone:** [redacted] **E-mail** [redacted] **Relation/Role to Project:** Project Manager

APMC Project Preference 4: Commonwealth of Pennsylvania

Name of Client & Project Title	Commonwealth of Pennsylvania (CoPA) and Dell Computers – CoPA Desktop and Laptop Refresh	
Contract Value	$1 million (7 years)	
Nature and Scope of Project:	**Project Description:** American Personnel Managers and Consultants, Inc. was selected as a Dell Partner for the Commonwealth desktop and laptop refresh project more than 8 years ago. As a Team member and subcontractor, we are responsible for a specific SCOPE of work agreed to between Dell and the Commonwealth of Pa. The Dell Project manager designates Commonwealth agency project; Timeline; products; services; etc; with APMC completing all phases of the implementation process. That can include, but may not be limited to; Product confirmation with Agency; review of services, timeline, etc. with the Commonwealth agency. Follow product from Dell location to receiving at our warehouse for detailed internal process validating products etc. Determine agency installation per Dell and agency agreement; provide implementation as required. This Contract was rebid in 2009 **Program Management Office (PMO) and Service Management** APMC assumes all responsibilities of process and service delivery after Dell has provided Commonwealth approval. **Technical Services** Project start up more than 8 years ago was sporadic. Commonwealth agencies were moving from a fragmented system to a one-stop shop, allowing better agency focus and abilities to better use purchasing methods. American Personnel Managers and Consultants, Inc. pro-actively addressed both technical and HR needs as the project has a variety of peaks and valleys associated with Agency budgets, internal requirements and demands for specific software updates, etc. Efforts for 100% satisfaction by Commonwealth agencies remain our number one focus, providing us with a clear path of no SLAs over the last 9 yrs on the project.	
Project Duration:	**Start Date Year:** 2001	**End Date Year:** on-going
Nature of the Client:	2001: CoPA and Dell Corporation – Computer Manufacturer and Commonwealth of Pennsylvania 2009 Rebid: Dell Corporation APMC is responsible for working with Dell corporation to meet Commonwealth hardware requests for every Commonwealth agency under a centralized purchasing system. All Commonwealth agencies refurbish equipment per budget abilities, agency needs and requirements.	
Nature of Client Audience:	2001: Public Officials and Employees project users and audience of all Commonwealth of Pennsylvania agencies 2009 Rebid: Information Technology, Hardware/software updates	

Name of Client & Project Title	Commonwealth of Pennsylvania (CoPA) and Dell Computers – CoPA Desktop and Laptop Refresh
Number of Users:	2001: Number of users- more than 22 Agencies - unknown number of Commonwealth of Pennsylvania Public Employee users 2009 Rebid: All Commonwealth of Pennsylvania employees
# & Composition of Vendor Employees & Consultants Assigned:	**Vendor Project Manager/Key Consultant on Project Team:** Pat Gingrich, President/CEO - Operations Manager Project Manager - Richard Beiber Manager on-site day to day operations 2001: One Project Manager and several staff members "as needed", and two support administrative staff members. This project fluctuates drastically based on Commonwealth Agency needs and requirements throughout the Commonwealth. Startup was somewhat sporadic as Commonwealth agencies changed their business model from a scattered approach to a focused one-stop-shop. Dedicated goal for overall cost savings. Once focus changed, projects moved forward quickly. APMC is responsible for working with Dell Corporation to meet Commonwealth hardware requests for every Commonwealth agency under a centralized purchasing system. All Commonwealth agencies refurbish equipment per budget, agency needs, and requirements. 2009 Rebid: Project start up more than 8 years ago was sporadic. Commonwealth agencies were moving from a fragmented system to a One-stop shop; allowing better agency focus and abilities to better use purchasing methods. American Personnel pro-actively addressed both technical and HR needs as the project has a variety of peaks and valleys associated with Agency budgets; internal requirements and demands for specific software updates, etc. Efforts for 100 percent satisfaction by Commonwealth agencies remain our number one focus, providing us with a clear path of no SLAs over the last 8 years on the project.
Client Contact Information:	**Reference Contacts:** Dell References **Name:** [redacted] **Title:** [redacted] **Department:** Dell Service Delivery Management **Full Address:** Dell Inc., One Dell Way Round Rock, Texas 78682 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** [redacted] **Name:** [redacted] **Title:** [redacted] **Department:** Dell Global Service Delivery **Full Address:** Dell Inc., One Dell Way Round Rock, Texas 78682 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project** [redacted]

4.5.6 Credo Technology Solutions, Inc. Project References

Credo Technologies Solutions, Inc. Reference 1: Pennsylvania Department of Public Welfare

Name of Client & Project Title	Pennsylvania Department of Public Welfare (via Computer Aid) – Technical Support	
Contract Value	$75,000 (annually)	
Nature and Scope of Project:	**Project Description** Credo Technology Solutions delivers a staff augmentation Technical Support Consultant position for the Pennsylvania Department of Public Welfare. Credo's consultant responds to telephone support calls and provides support for networking and desktop issues for all agency users. This role has been in place since June 2010 and is projected to continue for approximately 2 more years. **Technical Services** The Credo consultant participated in installation, configuration, and troubleshooting of customized images on Public Welfare/Office of Medical Assistance Programs personal computers. The consultant also upgraded or installed Windows 2000 or XP, Office XP, McAfee, EPO, SMS, IE 6.0, application and off-the-shelf software packages with service packs and patches as required. The most recent project accomplished by the Credo consultant was to install new personal computer hardware and peripherals, relocate existing equipment to other physical locations, and remove decommissioned personal computers and peripherals from the environment.	
Project Duration:	**Start Date Year:** 2010	**End Date Year:** On-going
Nature of the Client:	Pennsylvania Department of Public Welfare is one of Commonwealth's largest Agencies and they have onsite Technical Support staff to manage their servers and user desktops. Our employee is on this staff and continues to keep our client happy.	
Nature of Client Audience:	The users are mostly State Employees of Department of Public Welfare, along with a few being Consultants.	
Number of Users:	All Agency Personnel and Consultants	
# & Composition of Vendor Employees & Consultants Assigned:	Scott Long-COO/Nathan Houser: Since June 2010, Nathan works 8 hours a day to provide Technical Support to all users in Department of Public Welfare. This is an on-going effort.	
Client Contact Information:	**Reference Contacts:** **Name:** [redacted] **Title:** [redacted] **Department:** Department of Public Welfare **Full Address:** [redacted] **Telephone:** [redacted] **E-mail** [redacted] **Relation/Role to Project:** Approved Nathan's position	

Name of Client & Project Title	Pennsylvania Department of Public Welfare (via Computer Aid) – Technical Support
	Name: [redacted] **Title:** [redacted] **Department:** Bureau of Information Services/ Desktop Infrastructure Management Operations **Full Address:** [redacted] **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** Manages IT Desktop Support

Credo Technologies Solutions, Inc. Reference 2: Pennsylvania Department of Transportation

Name of Client & Project Title	Pennsylvania Dept. of Transportation (PennDOT) – Video Architect Project	
Contract Value	$150,000 (annually)	
Nature and Scope of Project:	**Project Description** The scope was to architect a Video Surveillance Process for PennDOT on Highway Surveillance, managed by the PennDOT Server Farm team. It was Architected and Managed by our employee. This project covers a number of initiatives that include: • PennDOT Traffic Management System which encompasses 11 PennDOT districts • A New Statewide Traffic Management System which involves PennDOT, PEMA, other state agencies and neighboring states **Program Management Office (PMO) and Management Services** • Determine the current configuration and what could be reused for the next generation PennDOT Traffic Management System • Determine how much existing video bandwidth already exists and the associated costs • Determine requirements and Concept of Operations (ConOps) • Use identified requirements and ConOps to determine the delta for needed bandwidth and equipment • Research existing and new technology along with qualified vendors and document findings • Present these findings for best in class technology and vendors for PennDOT consideration and approval • Coordinate with PennDOT approved vendors, PennDOT Telecommunications, and IT services to oversee the successful installation and implementation of the video TMC system • Coordinate with and assist PEMA, PennDOT, and other agencies on the design and construction of the Statewide Traffic Management System (STMC) **Technical Services** Our employee worked with multiple user groups to gather information on the next generation of PennDOT Traffic Management system. The project entailed taking data from Help desk users on issues and requests to improve the system and determine how much usage and bandwidth was consumed in order to make the system more functional and easy to use. .	
Project Duration:	**Start Date Year:** 10/2011	**End Date Year:** 11/2012
Nature of the Client:	PennDOT is one of the Commonwealth's largest Agencies and they have a large Server Farm to service and administer the servers and project related components.	
Nature of Client Audience:	The users are mostly State Employees of PennDOT (Including some consultants)	
Number of Users:	All agency personnel and consultants	

Name of Client & Project Title	Pennsylvania Dept. of Transportation (PennDOT) – Video Architect Project
# & Composition of Vendor Employees & Consultants Assigned:	Scott Long-COO/David Bastarache In October 2011, David was brought into PDOT to Architect and Manage the Video Surveillance Project, which he worked with the Cisco Security team as well.
Client Contact Information:	**Reference Contacts:** **Name:** [redacted] **Title:** [redacted] **Department:** PennDOT Server Farm **Full Address:** [redacted] **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** Managed Project above David Bastarache **Name:** [redacted] **Title:** [redacted] **Department:** PennDOT Server Farm **Full Address:** [redacted] **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** Monitor Project

UNISYS

Credo Technologies Solutions, Inc. Reference 3: Unisys

Name of Client & Project Title	Unisys Corporation – Patch Management Consultant	
Contract Value	$98,000	
Nature and Scope of Project:	**Project Description** The scope of the project is for a senior Patch Management Consultant. It involved complex work on enterprise-wide servers at Enterprise Data Center (EDC). The various environments are in development, staging, and production. The role required strong experience with Microsoft System Center Configuration 2007 (SCCM) in a production server environment preferably a large environment. Credo had to ensure that we identified a senior consultant with strong understanding of the fundamentals of these technologies i.e. Active Directory, Domain Naming Services (DNS), Internet Information Services (IIS) (versions 6 & 7) & Windows server operations (server 2003 and 2008 R2). The additional skill set required includes experience in Linux, PKI/CA/SSL, VMware, Scripting/Development, SQL, .net framework, Citrix, BizTalk, and SharePoint. The core qualifications are strong knowledge and experience in: Microsoft SCCM 2007, IIS 5.0/6.0 and/or SQL 2000/2005 Administration, Active Directory 2000/2003 Administration, MCSE 2000/2003 certification, Microsoft Office SharePoint Server 2007, Microsoft Internet Security and Acceleration Server 2006, Oracle 9i/10G Database, BizTalk Server 2004, Microsoft Operations 2005 & Remedy. The role required for mobile support for infrequent after-hours support and escalations and be part of a 24x7 on-call rotation one week out of every eight weeks **Technical Services** This is an ongoing contract that Credo Technology Solutions has with Unisys. The consultant is a member of an operations team managing a large enterprise Web application hosting environment in Central Pennsylvania. His responsibilities include Patch Management and virus-related Disaster Prevention. This person monitors all relevant security sites for new vulnerabilities; reviews, recommends, and ensures all servers are patched in a timely manner using standard tools. He also handles support tickets and is responsible for troubleshooting Windows, IIS, SQL and application issues. The hosting environment comprises 2000 Wintel servers and 600 Web-facing applications and continues to grow. It is widely recognized for its innovative use of the latest technologies from Microsoft, Cisco, and other leading IT companies. The scope of the project is for a senior Patch Management Consultant. It involved complex work on enterprise-wide servers at Enterprise Data Center (EDC). The various environments are in development, staging, and production. The role required strong experience with Microsoft System Center Configuration 2007 (SCCM) in a production server environment preferably a large environment. Over a year, Credo's strong consultant supported well and was able to handle the role well. Through regular interactions with Unisys and the consultant, Credo managed the expectations and offered exceptional support to the process. This led to a great partnership with Unisys and we are excited about the opportunity.	
Project Duration:	**Start Date Year:** 1-2012	**End Date Year:** On-going
Nature of the Client:	Commonwealth of Pennsylvania, Office of Administration - Bureau of Infrastructure & Operations	

Name of Client & Project Title	Unisys Corporation – Patch Management Consultant
Nature of Client Audience:	Commonwealth's various departments
Number of Users:	All agency personnel and consultants
# & Composition of Vendor Employees & Consultants Assigned:	Scott Long-COO/Prasad Kalluri: In January 2011, Prasad was brought into Pennsylvania Office of Administration, Bureau of Infrastructure & Operations through Unisys to perform patch management.
Client Contact Information:	**Reference Contacts:** **Name:** [redacted] **Title:** [redacted] **Department:** CoPA-Office of Administration **Full Address:** [redacted] **Telephone:** [redacted] **E-mail:** [redacted]m **Relation/Role to Project:** Delivery Manager **Name:** [redacted] **Title:** [redacted] **Department:** PA Office of Administration, Bureau of Infrastructure & Operations **Full Address:** [redacted] **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** Operations Manager

4.5.7 Domino Technologies, Inc. Project References

Domino Technologies Reference 1: Pennsylvania Department of Transportation

Name of Client & Project Title	Pennsylvania Department of Transportation (PennDOT) - Bureau of Infrastructure and Operations – PennDOT Server Farm Operations Support through Department of Public Welfare Staff Augmentation Contract
Contract Value	$7.5+ million (since 2005)
Nature and Scope of Project:	**Project Description** Domino Technologies, Inc. employees have worked at PennDOT server farm through Pennsylvania Staff Augmentation contract providing wide range of Infrastructure and operations support services including • Servers administration • Workstation support • Database administration • Network management services • Application server support We have provided support services at PennDOT server farm including Core Network Infrastructure Support, VMware Infrastructure Support, Desktop Configuration Management, WebSphere Infrastructure Support, FileNet and EMC Infrastructure Support, SharePoint Infrastructure Support, and Infrastructure Architecture Design Services. **Program Management Office (PMO) and Service Management** Technical services are managed by Domino Tech project managers and technical leads with the focus on: • Increasing visibility into projects, programs and operations • Aligning business demand to resource capacity • Identifying early warning indicators to ensure scheduled project delivery **Technical Services** Desktop Configuration Management: • Responsible for System and software deployment across all the 6000+ desktops across PennDOT using Microsoft System Center Configuration Management (SCCM) tool • Designed and implemented Microsoft SCCM 2007 migration from existing SMS 2003 implementation across entire agency • Perform routine maintenance on SCCM servers installed throughout the agency • Develop and maintain collections, packages, advertisements, reports, queries, and site settings for entire SCCM site • Perform database maintenance and optimizations on MS SQL 2005 servers where SCCM databases are maintained FileNet and EMC Infrastructure Support: • The EMC Captiva solution encompasses 20 Production servers, which provide redundant, fail-over functionality. It is part of the Safety EDMS solution within dotcentric, giving Safety Administration users the ability to scan, store and retrieve

Name of Client & Project Title	Pennsylvania Department of Transportation (PennDOT) - Bureau of Infrastructure and Operations – PennDOT Server Farm Operations Support through Department of Public Welfare Staff Augmentation Contract

documents

- Scanning utilizes both OPEX and Web-based solutions, allowing users at DLCs and other state offices the ability to scan from almost any location.
- Scanning volumes range from 75,000 to 100,000 documents per day, with higher numbers at peak periods (This equates to approximately 35 million documents per year currently).
- For the storage of the captured documents, the system leverages existing EDMS FileNet architecture
- At this time, Safety FileNet Image Services is storing more than 12 terabytes of data, with an additional terabyte being added every 3-4 months. For document retrieval and exception correction, users utilize a load-balanced Web front-end
- Applications impacted: Safety EDMS: Scanning, storage, retrieval for Bureaus of Driver Licensing and Motor Vehicles

Manage Hosting Servers

Core Network Infrastructure Support – Troubleshooting of complex Network and Hardware problems on Cisco equipment. Network captures and trace file interpretation for both in house projects and business partners. TMC network design build out and installation of AXIS encoder platform providing video stills of traffic for presentation to the public via Web for situational awareness. Designed and implemented Cisco WAF (Wide Area File system) and WAAS at 30 sites throughout the state of Pennsylvania for PennDOT. PennDOT was experiencing bandwidth saturation at T1 sites and experiencing unsatisfactory response times when retrieving files across the T1s. Additional servers at the remotes sites caused PennDOT to incur additional costs because servers had to be deployed to any site that had a T1

VMware Infrastructure Support – Designed and implemented VMware environment at PennDOT. First ESX servers built in Sept 2006. Currently 600+ VMs on production platform (plus 41 VM workstations). Currently more than 20 hosts in production platform. Responsible for setting up the VM environment at OA ESF co-location facility. They migrated all the servers from Cameron street facility to OA ESF co-location facility

Infrastructure Architecture Design Services

WebSphere Infrastructure Support – Designed and implemented WebSphere 6 infrastructure for Highway administration applications – ECMS2, MPMS, BMS2, JPA, UREDMS, GCEDMS CRS and APRAS. Several of these are mission critical applications that have to be available 24 X 7. Upgraded the WebSphere infrastructure to version 7. Planned and coordinated the upgrade of existing version 6 infrastructures with all the application teams. Installed and managed the WebSphere servers used for eGov – Web-based drivers licensing and vehicle registration system. Total number of servers: 60.

SharePoint Infrastructure Support – Responsible for designing, deploying and operating SharePoint infrastructure at PennDOT. Play a major role in implementing several solutions for PennDOT using SharePoint. Involved in integrating SharePoint with the Commonwealth standard user authentication tool SiteMinder. Work with the application requirements group, application architects and infrastructure subject matter experts to design the infrastructure architecture for new applications at PennDOT. Consultants have designed solutions for PennDOT that are based on standards but at the same time modular, flexible and agile.

Name of Client & Project Title	Pennsylvania Department of Transportation (PennDOT) - Bureau of Infrastructure and Operations – PennDOT Server Farm Operations Support through Department of Public Welfare Staff Augmentation Contract
Project Duration:	**Start Date Year:** 2005 — **End Date Year:** On going
Nature of the Client:	PennDOT provides services to 8.7 million licensed drivers and 11.3 million registered vehicle owners of Pennsylvania. With an annual budget of more than $6 billion in state and federal funds, PennDOT oversees programs and policies affecting highways, urban and rural public transportation, airports, railroads, ports, and waterways
Nature of Client Audience:	PennDOT Server Farm consists of over 800 servers with servers in district offices. Applications running on these servers are used by public and by PennDOT employees in offices all over the state
Number of Users:	9,800
# & Composition of Vendor Employees & Consultants Assigned:	**Vendor Project Manager/Key Consultant on Project Team:** These consultants are involved in the entire life cycle of the implementation and in on-going support efforts • Desktop Configuration Management: Scott Setliff • FileNet and EMC Infrastructure Support: Steve Stutzman, Mohammed Subhani • Core Network Infrastructure Support: Greg Mummert, Greg Mauchamer, Scott LaPlantt • VMware Infrastructure Support: Joseph Seaman, Bryan Cunjak, Kenny Lafromboise • WebSphere Infrastructure Support: Lou Bellman, Venkat Valluru • SharePoint Infrastructure Support: Wann Harris • Infrastructure Architecture Design Services: Nathan Balagopal
Client Contact Information:	**Reference Contacts:** **Name:** [redacted] **Title:** [redacted] **Department:** Server Farm Operations **Full Address:** [redacted] **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** [redacted] **Name:** [redacted] **Title:** [redacted] **Department:** Server Farm Operations **Full Address:** [redacted] **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** [redacted]

Domino Technologies Reference 2: Pennsylvania Game Commission

Name of Client & Project Title	Pennsylvania Game Commission – Information Technology (IT) Operations Support	
Contract Value	$50,000	
Nature and Scope of Project:	**Project Description** Domino Technologies, Inc. employees work at Bureau of Automated Technology Services at Pennsylvania Game Commission providing wide range of Infrastructure and operations support services including: • Server Virtualization • Servers administration • Database Administration We have provided support services at the Pennsylvania Game Commission during past two years that include Server Virtualization Project and Server Administration Support. **Program Management Office and Service Management** Domino Tech project manager is responsible for the three critical tasks of successful project execution: Proper Planning, Smooth Execution, and Effective Project Management & Control. **Technical Services** **Server Virtualization Project –** Setup a new SQL Server environment using VMware guest and migrated databases from physical servers to the new environment. Virtualization improved the availability and IT infrastructure efficiency for Pennsylvania Game Commission. Virtualized environment provides them with flexibility to maintain the infrastructure and ease of management of server resources. Designed and implemented built in business continuity solutions using policy based service level management to avoid service disruptions. **Manage Hosting Services** **Server Administration Support –** Domino Tech consultants provide on-going infrastructure operations support to Bureau of Automated Technology Services. • Consultant upgraded all the servers to Windows Server 2008 R2 from Windows 2003 • Upgraded Microsoft SQL Server from version 2005 to 2008 **Data Center Architecture** **Server Virtualization Project –** Pennsylvania Game Commission had all physical server environments with aging equipment. Our consultants designed virtual server environments using VMware ESXi v5 and IBM hardware. All the servers we migrated from physical to virtual guests in a phased manner without any interruption to business.	
Project Duration:	**Start Date Year:** 2012	**End Date Year:** On-going

Name of Client & Project Title	Pennsylvania Game Commission – Information Technology (IT) Operations Support
Nature of the Client:	For more than 100 years, the Game Commission has managed the Commonwealth's wildlife resources for all Pennsylvanians. With the help of more than 700 full-time employees and thousands of part-timers and volunteers, the agency provides a host of benefits to wildlife, state residents, and visitors.
Nature of Client Audience:	Servers host applications that are used by Game Commission employees from locations all over the state.
Number of Users:	More than 500
# & Composition of Vendor Employees & Consultants Assigned:	**Vendor Project Manager/Key Consultant on Project Team:** Project Manager: Nathan Balagopal Server Virtualization Project: Personnel: David Barlett Server Administration Support: David Barlett, Lou Bellman
Client Contact Information:	**Reference Contacts:** **Name:** [redacted] **Title:** [redacted] **Department:** Bureau of Automated Technology Services **Full Address:** 2001 Elmerton Avenue Harrisburg, PA 17110-9797 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** [redacted] **Name:** [redacted] **Title:** [redacted] **Department:** Bureau of Automated Technology Services **Full Address:** 2001 Elmerton Avenue Harrisburg, PA 17110-9797 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** [redacted]

Domino Technologies Reference 3: Pennsylvania Department of Transportation

Name of Client & Project Title	PennDOT - Bureau of Infrastructure and Operations – PennDOT Infrastructure Architecture Design Services through Pennsylvania Staff Augmentation Contract
Contract Value	$251,141 (more than)
Nature and Scope of Project:	**Project Description:** Domino Technologies, Inc. consultant works with the application requirements group, application architects, and infrastructure subject matter experts to design the infrastructure architecture for new applications at PennDOT. Nathan Balagopal joined the new Infrastructure architecture team at PennDOT in 2011. Nathan is experienced in multiple hardware and software environments and also on complex heterogeneous systems environments in use at PennDOT. Consultant was involved in designing the Infrastructure architecture for the following applications: Applications for which Infrastructure architecture design services were provided: • Information Technology and Service Delivery & Consolidation Project • Gatekeeper Modernization Project • eCAMMS • DOTImage **Program Management Office (PMO) and Service Management** • Analyzed the infrastructure requirements • Analyzed the application requirements • Prepared the ball park estimate to implement the technical solution • Evaluated the different technology solutions that will meet the business requirements • Coordinated workshops with IBM subject matter experts for PennDOT application architects and other infrastructure architects • Researched on the technology solutions that will meet the requirements **Technical Services** • Collaborated with the subject matter experts to design the infrastructure that used standard PennDOT enterprise technologies • Collaborated with PennDOT Subject matter experts, IBM Message Broker product specialists, and DataPower product specialists to design the infrastructure • Designed the infrastructure architecture • Coordinated the design sessions with BIO subject matter experts and application development vendor consultants on – clustering IIS server using App fabric, use of SQL server reporting services, need of separate OLAP database instance for reporting, MQ interface, and use of PennDOT PDIF gateway • Prepared the infrastructure architecture design
Project Duration:	**Start Date Year:** 2011 | **End Date Year:** On going
Nature of the Client:	PennDOT provides services to 8.8 million licensed drivers and 11.4 million registered vehicle owners of Pennsylvania. With an annual budget of more than $6 billion in state and federal funds. PennDOT oversees programs and policies affecting highways, urban and rural public transportation, airports, railroads, ports and waterways. PennDOT is directly responsible for nearly 40,000 miles of highway and roughly 25,000 bridges.

Name of Client & Project Title	PennDOT - Bureau of Infrastructure and Operations – PennDOT Infrastructure Architecture Design Services through Pennsylvania Staff Augmentation Contract
Nature of Client Audience:	PennDOT Server Farm consists of over 800 servers with servers in district offices. Applications running on these servers are used by public and by PennDOT employees in offices all over the state.
Number of Users:	9800 (approximately)
# & Composition of Vendor Employees & Consultants Assigned:	**Vendor Project Manager/Key Consultant on Project Team:** Nathan Balagopal is joined the new Infrastructure architecture team at PennDOT in 2011.
Client Contact Information:	**Reference Contacts:** **Name:** [redacted] **Title:** [redacted] **Department:** PennDOT - Bureau of Infrastructure and Operations **Full Address:** 400 North Street Harrisburg, PA 17120 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** Client Manager **Name:** [redacted] **Title:** [redacted] **Department:** PennDOT - Bureau of Infrastructure and Operations **Full Address:** 400 North Street Harrisburg, PA 17120 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** [redacted]

4.5.8 e&e IT Consulting Services, Inc. Project References

e&e IT Consulting Services Project Reference 1: Pennsylvania Turnpike Commission

Name of Client & Project Title	Pennsylvania Turnpike Commission – SMS and Active Directory staffing resources	
Contract Value	$707,200	
Nature and Scope of Project:	**Project Description** e&e IT Consulting Services provided the Pennsylvania Turnpike Commission (PTC) with two Senior Network Engineers who were responsible for implementing SMS to manage over 1,200 desktops across 250 servers, including development of the implementation plan and the enterprise-wide plan rollout. **Technical Services** The technical skills required were experience managing technical rollouts, hands-on experience implementing and maintaining SMS, experience with Active Directory, experience with MOM, and a current MCSE certification.	
Project Duration:	**Start Date Year:** Jan 2007	**End Date Year:** Dec 2008
Nature of the Client:	PTC manages the Pennsylvania Turnpike	
Nature of Client Audience:	PTC employees across multiple sites in the Commonwealth of Pennsylvania	
Number of Users:	1,200	
# & Composition of Vendor Employees & Consultants Assigned:	e&e IT Consulting Services, Inc. was responsible for providing two Sr. Network Engineers to support SMS and Active Directory related projects and maintenance.	
Client Contact Information:	**Reference Contacts:** **Name:** [redacted] **Title:** [redacted] **Department:** Infrastructure/Networking **Full Address:** 700 South Eisenhower Boulevard Middletown, PA 17057 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** Direct manager **Name:** [redacted] **Title:** [redacted] **Department:** SAP/IT **Full Address:** 700 South Eisenhower Boulevard Middletown, PA 17057 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** Direct manager for e&e consultants providing SQL support	

e&e IT Consulting Services Project Reference 2: Pennsylvania Department of Education

Name of Client & Project Title	Pennsylvania Department of Education – Systems Administrator and Desktop Support
Contract Value	$170,310
Nature and Scope of Project:	**Project Description** Maintain the project servers, files, print capacity, and make certain that backups are performed as appropriate. Perform as a front-line interface to users. Accepts trouble reports and dispatch them to appropriate system administrators. Our team writes scripts in a particular administrative language and has programming experience with applicable languages. Communicate accurate and useful status updates, manage and report time spent on all work activities, and follow quality standards. The e&e IT team is responsible for operating and system software upgrades and for keeping patches current, perform minor debugging, and program modifications. As required, we develop and execute the disaster recovery/back up procedures and archiving procedures, and manage server security. We conduct performance tuning, capacity planning, database administration, and fault management. We understand the design of consistent network-wide file system layouts and maintain strong relationships with employees and various tier two and three support groups. Support is provided for tier two support of the technical infrastructure, and we coordinate efforts with vendors if tier three support is required. Risks are mitigated by ensuring high priority issues are resolved in a timely manner and by identifying and reporting hardware problems. Identify and track issues, risks, and action items and resolve and/or assist in issue resolution **Program Management Office (PMO) and Management Services** Our System Administrator served as the Project Manager for the PDE infrastructure consolidation over to OAIT. He helped facilitate and lead the exercise. He also serves as one of the SMEs for the PDE team in terms of their entire Infrastructure as it presently stands in PDE. He also reviews, prioritizes, and researches service requests and may prepare purchase justifications. Experience permits him to anticipate and quickly resolve team specific issues. Additionally, he determines time estimates, schedules for the team's work, resolve issues that may arise in a timely manner, and manage the daily operations to make sure service levels are being met. Our Systems Administrator manages the systems management team's support issue and backlog, monitors the team's open backlog of support issues and re-assign issues as necessary to verify they are closed per agreed upon service levels. Expectations are managed at all levels—customers, end users, and executive sponsors—while implementing and following quality standards. Our systems administrator manages requirements for technical support and design in an application development environment. Work involves interface with various infrastructure teams and operations providers to identify the strategic direction of systems management activities. Other responsibilities include:

Name of Client & Project Title	Pennsylvania Department of Education – Systems Administrator and Desktop Support
	• Act as the first level of escalation for high priority support issues • Function as the liaison to the various support groups with whom the systems management team interfaces • Develop the technical infrastructure maintenance strategy • Manage the system management resources • Act as a system's management expert • Analyze, determine, and document requirements in terms of system management needs and implement them • Recommends policies on system use and services. **Technical Services** Support more than 90 in-house written Web apps. Deploy support for applications written in house. We provide network support, Cisco configuration, firewall support, network security, snort. network and service availability monitoring, and IBM DS3400 SAN EMC Celerra NAS EMC Avamar Backup with offsite replication node. We build/support/administer the Team Foundation Server, assist the development team with process and procedures to implement continuous integration practices, automated build deploy, IIS Admin, and DNS record management. Our team has a solid understanding of networking/distributed computing environment concepts, understands principles of routing client/server programming, and is responsible for keeping the environment up and running.
Project Duration:	**Start Date Year:** 2007 / **End Date Year:** Ongoing
Nature of the Client:	Executive Department of the state charged with K-12 and adult educational budgeting, management and guidelines.
Nature of Client Audience:	All PDE internal as well as external users logging into the site and using the programs.
Number of Users:	Internally 700 and externally millions.
# & Composition of Vendor Employees & Consultants Assigned:	Two Consultants: one System Administrator and one Desktop Technician
Client Contact Information:	**Reference Contacts:** **Name:** [redacted] **Title:** [redacted] **Department:** Center for Data Quality **Full Address:** Pennsylvania Department of Education 333 Market Street Harrisburg, PA 17126-0333 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** In charge of our 2 Contractors working on site

Name of Client & Project Title	Pennsylvania Department of Education – Systems Administrator and Desktop Support
	Name: [redacted] **Title:** [redacted] **Department:** Center for Data Quality **Full Address:** Pennsylvania Department of Education 333 Market Street Harrisburg, PA 17126-0333 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** Director of Division

e&e IT Consulting Services Project Reference 3: PLCB

Name of Client & Project Title	PLCB – Linux POS Support
Contract Value	$127,899.20
Nature and Scope of Project:	**Project Description** The PLCB has 1,500 registers running SUSE Linux Point-Of-Sale (SLEPOS) supporting its retail business. Ronald Meinsler has primarily been working on automating the configuration of these registers. These registers reside in approximately 615 stores across the state. Ron has also been working on automating the configuration of the SUSE Linux servers that run in each of these stores. These two tasks will provide a quicker deployment turn-around as well as more consistent setups for these devices. He has been a big asset in both of these ventures as well as providing a vast knowledge base for Linux in general. **Technical Services** Support the Point-of-Sale team on all operating system or hardware issues on the PLCB's SUSE Linux based registers • Create/update automated deployment scripts for the registers • Create/update register images • Patch the operating system on the registers on a regular basis • Assist the POS team on developing (scripting) application patches • Assist the POS team with register replacements (DNS, DHCP, LDAP changes) • Provide remote support for the SUSE Linux based (in-)store servers • Place and manage hardware calls for the store servers • Patch the operating system on the store servers on a regular basis • Create/update automated deployment scripts for the Point-of-Sale application on the store servers
Project Duration:	**Start Date Year:** 2012 / **End Date Year:** 2012
Nature of the Client:	Support for the Pennsylvania Liquor Control Board Retail System.
Nature of Client Audience:	Retail clients and users at the 615 Stores throughout Pennsylvania.
Number of Users:	1500 registers x numbers of users of these machines.
# & Composition of Vendor Employees & Consultants Assigned:	1 Vendor employee and 1 PLCB employee.
Client Contact Information:	**Reference Contacts:** **Name:** [redacted] **Title:** Network Administrator 2 **Department:** Office of Information Technology Services Enterprise Infrastructure Division **Full Address:** 210 Northwest Office Bldg | Harrisburg, PA 17124-0001 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** Server Support / Enterprise Infrastructure/ OITS

Name of Client & Project Title	PLCB – Linux POS Support
	Name: [redacted] **Title:** [redacted] **Department:** Office of Information Technology Services Enterprise Infrastructure Division **Full Address:** 210 Northwest Office Building Harrisburg, PA 17124-0001 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** Chief of the Department

4.5.9 Info-Matrix Corporation Project References

Info-Matrix Corporation Project Reference 1: Pennsylvania Counties

Name of Client & Project Title	Pennsylvania Counties - Automated Children and Youth System (ACYS)
Contract Value	$1,800,000
Nature and Scope of Project:	**Project Description** The Commonwealth consists of 67 counties who are responsible for the administration of Child Welfare functions and policies as developed by the Commonwealth of Pennsylvania. Over the years each county had developed separate and independent in-house systems to support these functions and provide statistics to the Commonwealth. Over the last few years the Commonwealth has encouraged the counties to standardize on a software solution, which would facilitate the migration to a statewide system, which is planned for implementation in the future. To meet this requirement Info-Matrix developed the Automated Children and Youth System (ACYS). Development of the system commenced on January of 2003. **PMO and Services Management** Part of this effort includes operating a Project Management Office (PMO) to support the multiple projects under way. This includes a strong service management methodology to support the existing infrastructure, application, and business users. This project also entails a phased development and implementation across multiples counties as well as ongoing maintenance and support of the application and infrastructure. Info-Matrix also operates the Help Desk function as required. In addition, Info-Matrix subject matter experts work with county personnel to assist the counties in their decision in hosting their applications or going to a cloud offering. **Technology Services** Info-Matrix Corporation developed the Automated Children and Youth System (ACYS), a .NET/SQL Web-based Case Management System designed to support the administrative functions of Pennsylvania's County Youth Services Offices. ACYS features a complex SQL Server Database and knowledge of the Unisys ES7000. In addition to design and development, during implementation, we provided data mapping, cleansing, and conversion services from various disparate databases to SQL Server. We also have prior experience with index sequential, hierarchal and inverted list databases. The project included general system design, detail system design, development, testing, implementation, training and documentation. Info-Matrix performs installation, user testing as well as cleansing legacy data. This development effort made extensive use of RAD/JAD development techniques due to the compressed development cycle required by the counties. The project was initiated in June of 2003 and the initial system installation was done within 18 months by January of 2004. ACYS has since been deployed in multiple Commonwealth of Pennsylvania counties including Venango, Bucks, and Montgomery. ACYS as a total system includes approximately 70 function points, 70 tables and numerous programmed reports as well as an extensive ad hoc reporting capability. They system will be utilized by approximately 700 users and caseworkers. The platform utilized for this application was .NET with a SQL Server database. Functionality included in ACYS includes:

Name of Client & Project Title	Pennsylvania Counties - Automated Children and Youth System (ACYS)
	Intake, Allegations, Relationships Disposition, Case Management, Case Decision Case Open/Close, Worker Assignment, Contacts Risk Assessment, Placements, Caseload Tracking To Do List, AFCARS, Adoption Search Capabilities, Provider Maintenance, Worker Maintenance
Project Duration:	**Start Date Year:** 2003 — **End Date Year:** Ongoing
Nature of the Client:	Pennsylvania Counties – Venango, Bucks and Montgomery
Nature of Client Audience:	Office of Children, Family and Youth – Pennsylvania Counties – county users and case workers
Number of Users:	Over 700 county employees and case workers
# & Composition of Vendor Employees & Consultants Assigned:	Numerous Info-Matrix employees over the years
Client Contact Information:	**Reference Contacts:** **Name:** [redacted] **Title:** [redacted] **Full Address:** Venango County Office of Children and Youth 1 Dale Avenue Franklin, PA **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** Project initiator and sponsor **Name:** [redacted] **Title:** [redacted] **Department:** Bucks County Office of Children and Youth **Full Address:** Suite 200, 4259 W. Swamp Road Doylestown, PA 18902 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** Bucks County Project initiator and sponsor

Info-Matrix Corporation Project Reference 2: Pennsylvania Game Commission

Name of Client & Project Title	Pennsylvania Game Commission – Mainframe Conversion Project
Contract Value	$2,500,000
Nature and Scope of Project:	**Project Description** The Pennsylvania Game Commission manages the Commonwealth's wildlife resources, which are considered by many to be a state treasure. Over the years, the Game Commission developed numerous mainframe applications to assist the citizens of Pennsylvania and to aid its employees and volunteers in conducting the business for the Pennsylvania Game Commission. This project included migration of their mainframe applications into a more modern technical platform, while enhancing business functionality and processes. **Program Management Office (PMO) and Service Management** Part of this effort includes operating a Project Management Office (PMO) to support the multiple projects under way. The PMO has a growing portfolio of projects supported by PMP certified project managers from Info-Matrix. The standardized methodology has led to a streamlined management of all projects within the Commission and the ability to track them at the task level and generate management reports. This includes a strong service management methodology to support the existing business applications deployed to the new distributed infrastructure. **Technical Services** At the end of 2011, the Commission selected Info-Matrix to architect and modernize the existing mainframe legacy applications. The modernization effort includes migrating over 17 mainframe applications to a Web-based, distributed environment. The effort includes architecting the solution(s), strong project management, business analysis and solutioning, data conversion, and full life cycle development / deployment. The project started in 2011, with a target completion date in December 2014. This complex project entails a phased development and implementation as well as ongoing maintenance and support of the application and infrastructure. Info-Matrix is skilled at large, complex multi- year projects. This requires a strong team with the ability to develop the new business applications as well as supporting those new applications implemented. **Data Center Architecture** The project entails architecting the technical platforms, transition management, technical support for the infrastructure on which the new applications are housed, data conversion and constant interface with the business users on the functionality of the new business applications. Info-Matrix has much experience with the Enterprise Data Center and the Data PowerHouse, which is critical to architecting and migrating the applications from the Data PowerHouse to the EDC environments. The Info-Matrix Team works closely with staff at the EDC to ensure procedures are followed and the required testing and QA takes place prior to deployment of any application. This includes capacity planning and load testing prior to deployment.

UNISYS

Name of Client & Project Title	Pennsylvania Game Commission – Mainframe Conversion Project	
Project Duration:	**Start Date Year:** 2011	**End Date Year:** Ongoing through 2014
Nature of the Client:	Pennsylvania Game Commission – IT Department (Office of the CIO) Executive Sponsor – Executive Director of the Commission.	
Nature of Client Audience:	The business applications being transformed will affect all of the business users and IT support personnel with the Game Commission and streamline operations for citizens and volunteers.	
Number of Users:	The new business applications will utilized by most of the Pennsylvania Game Commission and numerous volunteers and citizens of the Commonwealth.	
# & Composition of Vendor Employees & Consultants Assigned:	**Vendor Project Manager/Key Consultant on Project Team:** The Info-Matrix project manager has been working with the Pennsylvania Game Commission Information Technology Staff since 2011. The initial project team consisted of three people who did the "as is" review of the applications and architected the plan and solution to move to the distributed environment (including business design, solutioning of infrastructure components. The team has ramped up to 6 full time developers during 2012. Additional personnel are brought in as required for specialized work.	
Client Contact Information:	**Reference Contacts:** **Name:** [redacted] **Title:** [redacted]) **Department:** Information Technology **Full Address:** Pennsylvania Game Commission 2001 Elmerton Avenue Harrisburg, PA 17110 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** Project initiator and sponsor **Name:** [redacted] **Title:** [redacted] **Department:** Information Technology **Full Address:** Pennsylvania Game Commission 2001 Elmerton Avenue Harrisburg, PA 17110 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** Game Commission IT Manager responsible for the mainframe migration	

Info-Matrix Corporation Project Reference 3: Pennsylvania Department of Public Welfare

Name of Client & Project Title	Pennsylvania Department of Public Welfare – Large Contract Support
Contract Value	$45,000,000 (estimated over the last 16 years)
Nature and Scope of Project:	**Project Description** Since 1996, Info-Matrix had been working with the Pennsylvania Department of Public Welfare in numerous support roles from application development, to database design / conversion and infrastructure support. Info-Matrix has performed in the capacity as prime vendor as well as a sub-contractor partnered with Deloitte since 2006. Those initiatives include critical projects and legacy mainframe support such as those outlined below (as well as others): **Low Income Home Energy Assistance Programs (LIHEAP) –** The Low-Income Home Energy Assistance Program, also known as LIHEAP, helps low-income families pay their heating bills. LIHEAP is an application that offers assistance in the form of a cash grant, sent directly to the utility company, or a crisis grant for households in immediate danger of being without heat. Info-Matrix was involved initially with the mainframe development of the application and later the development and conversion to a Web-based solution. The LIHEAP application is used across the Commonwealth to determine eligibility and support for our most vulnerable citizens. **Office of Mental Retardation (2001 – Present) –** The Home and Community Services Information System or "HCSIS" was conceptualized and designed as a Web-based application utilizing the .NET framework. The core system processes standardized Mental Retardation (MR) processes, centralized MR data and introduced quality monitoring and resource budgeting improvements to the mental retardation program. Info-Matrix provided over 38 technical experts to develop the statewide system. Info-Matrix began the development in 2001 and continues to provide quality development and operations support to the project today. Info-Matrix was also successful in transitioning the required skills to the DPW development staff through various methods including Web-based training, mentoring programs and formal training sessions. The overall project required extensive system and end user documentation as well. **Program Management Office (PMO) and Services Management** This effort required Info-Matrix to provide strong Project Management Office components in order to manage and support the multiple projects under way. This included defining the business requirements, development, testing, data conversion and implementation within a specific and defined timeline. This also includes a strong service management methodology to support the existing business processes while implementing the streamlined applications. **Technical Services and Manage Hosting Services** The initiatives above provided applications development support, mainframe migrations, data migrations and legacy mainframe support for mission critical applications for DPW. Info-Matrix provided development activities and support for the applications, which are used across the Commonwealth to provide citizen services. The core system standardized business processes, centralized data and introduced quality monitoring and resource budgeting improvements to DPW's various program offices. Info-

Name of Client & Project Title	Pennsylvania Department of Public Welfare – Large Contract Support	
	Matrix provided technical experts to help develop these statewide systems. The effort includes architecting the solution(s), strong project management, business analysis and solutioning, data conversion, and full life cycle development / deployment. Over the years, Info-Matrix has become quite familiar with the design and software requirements, development standards, procedures and development methodology defined by the Department of Public Welfare. Info-Matrix currently provides many talented and experienced individuals to the Department of Public Welfare for software development and maintenance. Our developers, programmers, project managers and consultants distinguish themselves from other candidates because they possess a great deal of Health and Human Services domain knowledge. The combination of domain knowledge and technical expertise is the hallmark of our consultant staff. Info-Matrix currently provides personnel whose mission is to provide analysis, development and maintenance support to DPW for mission critical applications. Info-Matrix has a history and background of mainframe applications and the Unisys platforms.	
Project Duration:	**Start Date Year:** 1996	**End Date Year:** Ongoing
Nature of the Client:	Pennsylvania Department of Public Welfare providing citizen services	
Nature of Client Audience:	Pennsylvania Department of Public Welfare. The business applications developed are used by DPW employees to streamline business processes and streamline services for Pennsylvania citizens.	
Number of Users:	Citizens requiring Pennsylvania Department of Public Welfare services	
# & Composition of Vendor Employees & Consultants Assigned:	Numerous Info-Matrix employees over the years as a sub to Deloitte – Described above	
Client Contact Information:	**Reference Contacts:** **Name:** [redacted] **Title:** [redacted] **Full Address:** 300 Corporate Center Drive Camp Hill, PA **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** DPW Prime Contractor **Name:** [redacted] **Title:** [redacted] **Department:** Bryn Mawr Alliance LLC **Full Address:** 507 8th Street New Cumberland, PA 17070 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** [redacted]	

4.5.10 Innovative Business Concepts, Inc. Project References

Innovative Business Concepts, Inc. Reference 1: Commonwealth of Pennsylvania

Name of Client & Project Title	Commonwealth of Pennsylvania Data PowerHouse (DPH) Contract
Contract Value	$237,000 per year thru December 2014
Nature and Scope of Project:	**Project Description** Call volume/incident reports: Since 1999, IBC has been providing onsite FTE personnel to support all Unisys mainframe, midrange and technical support functions in accordance with the Commonwealth's Data PowerHouse contract. IBC's Operations Help Desk staff interfaces with the Commonwealth's existing Help Desk infrastructure and performs second level (Level 2) problem determination, resolution, and/or tracking for end users. IBC's staff provides these services on site at the Willow Oak facility in Harrisburg, PA. Service coverage is redundant during prime operating hours, for all Level 2 calls in support of user requirements. Specific IBC Help Desk Staff responsibilities include: • Answer phone, fax, or e-mail inquiries in a timely and professional manner • Utilize problem management tools to document and track status of all problems • Perform single-point-of-contact problem determination and problem source identification (PD/PSI) for all user problems within IBC's scope of responsibility • Resolve/correct problems in a timely manner providing high level of customer satisfaction with problem assistance • Escalating, according to procedures, all unresolved problems in a timely manner to the appropriate next level of support including vendor dispatching if needed • Document all service outage/interruption incidents and initiation of recovery procedures • Notify designated Unisys personnel of systems or equipment failures, or of an emergency, according to the Procedures Manual • Monitor system components (host and network availability, application components/deliverables, etc.) and initiate recovery procedures as appropriate • Monitor and control (start/stop/recycle) all system attached devices and telecommunications lines • Provide system/user id password reset control and assistance • Provide assistance with missing or incorrect reports and other application deliverables • Interface with other operations personnel, programmers, and users/customers as appropriate • Update problem documentation via appropriate problem management process; • Initiate appropriate escalation procedures when required • Follow/develop/maintain work procedures • Report on the status of batch jobs upon request • Manage and monitor daily data transmissions • Maintain and distribute an updated Help Desk telephone number listing as required • Dispatch local carrier for line problems. **Service Management** IBC has been on the Data PowerHouse Project since its inception. During that timeframe they have worked with Unisys, IBM and the Commonwealth of Pennsylvania (The Team) to create a Help Desk, which provides services to the Agencies that have enlisted its help. The Help Desk was created from scratch and has evolved over the years in order to

Name of Client & Project Title	Commonwealth of Pennsylvania Data PowerHouse (DPH) Contract	
	provide meaningful reports and provide data for the overall efficiencies of the service. The Help Desk Staff provides ongoing input in order to streamline functions, play watchdog to open incent tickets, and provide updates to the process and procedures in order to keep up with the changing times. IBC only provides Help Desk services. **Technical Services** Innovative Business Concepts (IBC) is a Pennsylvania IT ITQ-qualified technology vendor. IBC is pre-qualified to provide the following IT ITQ services: • Training • Software Development • IT Consulting Services • Outsourcing Services and Support • Network and Telecommunications Consulting Services • Staff Augmentation	
Project Duration:	**Start Date Year:** 1999	**End Date Year:** On-going through 2014
Nature of the Client:	Agencies of the Commonwealth which use the Data PowerHouse	
Nature of Client Audience:	Agencies of the Commonwealth	
Number of Users:	Agencies of the Commonwealth	
# & Composition of Vendor Employees & Consultants Assigned:	**Vendor Project Manager/Key Consultant on Project Team:** IBC supplies 3.5 FTEs – Help Desk Analyst to support this project. Since the inception, IBC has worked with the Team in order to cover the ebbs and flows of the help desk staffing needs.	
Client Contact Information:	**Reference Contacts:** **Name:** [redacted] **Title:** [redacted] **Department:** CoPA Sales and Account Management **Full Address:** 4750 Lindle Road Harrisburg, PA 17111 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** [redacted] **Name:** [redacted] **Title:** [redacted] **Department:** Data Center **Full Address:** 4750 Lindle Road, Suite 300 Harrisburg, PA 17111 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** [redacted]	

Innovative Business Concepts, Inc. Reference 2: Pennsylvania Department of Transportation

Name of Client & Project Title	PennDOT Computer Aided Drafting and Design (CADD) Support Services
Contract Value	$220,000 per year thru December 2014
Nature and Scope of Project:	**Project Description** **Call volume/incident reports –** For the PennDOT Computer Aided Drafting and Design (CADD) Project, Innovative Business Concepts, Inc. partnered with Intergraph to provide PennDOT with CADD Support Services. Specifically, IBC is supporting the project by providing Project Management, Reporting, and two (2) CADD Expert Level Resident Technicians. The PennDOT CADD project provides statewide expert technical support for the maintenance and development of PennDOT's Computer Aided Drafting and Design (CADD) and Geospatial Systems in fourteen (14) district offices and PennDOT locations throughout the state. Intergraph and IBC provide on-site support to assist PennDOT CADD Support personnel in maintaining the CADD/Geospatial sites in good operating condition and are responsive to the requirements of PennDOT. Support services include software and equipment troubleshooting that result in remedial action and routine site and system maintenance. This project entails the on-site placement of expert-level, technical staff within direct, real-time access of all PennDOT design and engineering locations and domains. As such, the eight-member, Resident Technician (RT) Team must command a high degree of knowledge and experience of the PennDOT CADD and GIS infrastructure; the specific operating procedures and policies used at PennDOT; and the short- and long-term objectives and requirements of the departments. In addition to possessing an in-depth knowledge of PennDOT's applicable CADD/GIS software, each RT must also be able to perform as a highly skilled and experienced troubleshooter of the specialized hardware in use at PennDOT, as well as be able to understand and reliably diagnose complex system and network-related issues. This approach is necessitated by the complexity of the technology used within the PennDOT design and engineering locations, as well as the geographic dispersion of the locations. Dedicated technicians co-located with the sites they support, and specialized in the support of the hardware and software technologies that make PennDOT's engineering team productive, are best able to prevent or quickly resolve productivity impacting IT issues. Proactive and responsive support rendered by technicians deeply invested in the environments they support helps to ensure that PennDOT continues to operate at peak efficiency and meet the goal of 100% on-time bid packages. **Program Management Office (PMO) and Service Management:** **Project Management and Coordination** • Daily – Act as the point of contact for all employees to use to notify of an unplanned absence. Ensure that the technical lead is informed. Using pre-determined criteria, decide whether to request backfill of the absent resource, and if so, send the request to the backfill resource. • Weekly – Track vacation plans for each of the technical resources assigned to the project. Identify when outages will occur and ensure backfill resources are identified and tasked to cover those outages. Identify any situations where multiple personnel are requesting time off at the same time and flag to the Technical Lead to resolve.

Name of Client & Project Title	PennDOT Computer Aided Drafting and Design (CADD) Support Services

- Monthly – Participate in monthly program/project reviews remotely via teleconference. Capture minutes and action items from the review and distribute to Intergraph and to the State.
- Monthly – Based on inputs from the technical team, create the consolidated monthly activity report and distribute to Intergraph and to the State after review and acceptance by the Technical lead. Report on trends of issues, locations and number of issues reported from Field Technicians.
- Monthly – Maintain the skills and certification matrix for the existing staff and also the planned training and certifications. Ensure that the technical lead updates the matrix on a quarterly basis or in response to significant technological changes at Penn DOT.
- Monthly – Maintain a consolidated record of system downtime and equipment failures across all supported sites, based on information provided by the Resident Technician supporting each site.
- Quarterly – Participate in the quarterly WebEx sessions with the State remotely via telecon/WebEx. Capture minutes and action items from the session and distribute to Intergraph and to the State.
- Annually – Prepare the contract activity and status report required by the Contract Administrator, either annually, or upon request of DGS.

Technical Services

IBC provides two CADD Expert Level Resident Technicians for statewide support/ Maintenance and development of PennDOT's CADD and Geospatial Systems in fourteen (14) district offices and PennDOT locations throughout the state.

This project entails the on-site placement of expert-level, technical staff within direct, real-time access of all PennDOT design and engineering locations and domains. As such, the eight-member, Resident Technician (RT) Team must command a high degree of knowledge and experience of the PennDOT CADD and GIS infrastructure; the specific operating procedures and policies used at PennDOT; and the short- and long-term objectives and requirements of the departments. In addition to possessing an in-depth knowledge of PennDOT's applicable CADD/GIS software, each RT must also be able to perform as a highly skilled and experienced troubleshooter of the specialized hardware in use at PennDOT, as well as be able to understand and reliably diagnose complex system and network-related issues.

This approach is necessitated by the complexity of the technology used within the PennDOT design and engineering locations, as well as the geographic dispersion of the locations. Dedicated technicians co-located with the sites they support, and specialized in the support of the hardware and software technologies that make PennDOT's engineering team productive, are best able to prevent or quickly resolve productivity impacting IT issues. Proactive and responsive support rendered by technicians deeply invested in the environments they support helps to ensure that PennDOT continues to operate at peak efficiency and meet the goal of 100% on-time bid packages.

Facilities Management

Provide software and equipment troubleshooting support that result in remedial action and routine site and system maintenance. IBC records issues/incents of the PennDOT IT equipment , tracks warranties , and upgrades and applies software patches as needed and repairs the printers to the 14 District Offices, the Photo Licensing Centers and the "ROC Building in Harrisburg.

Name of Client & Project Title	PennDOT Computer Aided Drafting and Design (CADD) Support Services
	Managed Hosting Services Provide on-site support to assist PennDOT CADD Support Personnel in maintaining operating condition and responsiveness of the CADD/Geospatial sites. **Capacity on Demand and Additional Services:** Proactive and responsive support rendered by technicians deeply invested in the environments they support helps to ensure that PennDOT continues to operate at peak efficiency and meet the goal of 100% on-time bid packages.
Project Duration:	**Start Date Year:** 2011 — **End Date Year:** On-going through 2014
Nature of the Client:	PennDOT's Computer Aided Drafting and Design (CADD) and Geospatial Systems
Nature of Client Audience:	The PennDOT CADD project provides statewide expert technical support for the maintenance and development of PennDOT's Computer Aided Drafting and Design (CADD) and Geospatial Systems in fourteen (14) district offices and PennDOT locations throughout the state.
Number of Users:	PennDOT employees statewide
# & Composition of Vendor Employees & Consultants Assigned:	**Vendor Project Manager/Key Consultant on Project Team:** IBC provides two CADD/Network Technicians and one Project Manager
Client Contact Information:	**Reference Contacts:** **Name:** [redacted] **Department:** Security, Government & Infrastructure (SG&I) Division **Full Address:** Intergraph Corporation 218 Westinghouse Blvd., Suite 204 Charlotte, NC 28273 **Title:** [redacted] **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** Contract Manager **Name:** [redacted] **Department:** Security, Government & Infrastructure (SG&I) Division **Full Address:** Intergraph Corporation Keystone Building, 400 North Street Harrisburg, PA 17120 **Title:** [redacted] **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** Technical Consultant

Innovative Business Concepts, Inc. Reference 3: Commonwealth of Pennsylvania

Name of Client & Project Title	Commonwealth of Pennsylvania, External Quality Review Organization (EQRO) – Department of Public Welfare (DPW) Managed Healthcare	
Contract Value	$117,000 Per Year	
Nature and Scope of Project:	**Project Description** Business Concepts, Inc. has partnered with IPRO on the delivery of the EQRO External Quality Review Organization to deliver a successful project of the Commonwealth of Pennsylvania. Specifically IBC is providing IPRO with building, facilities, network, application development, and administrative assistance in support of the project. As Pennsylvania's EQRO, IPRO has worked with its Medicaid managed care programs that provide physical health (PH) services to mandatory and voluntary populations; behavioral health (BH) services to a mandatory population; Enhanced Primary Care Case Management (EPCCM) services; and Prepaid Inpatient Health Plans (PIHP) long-term care services. On the EQRO project, IPRO and its partners, including Innovative Business Concepts, are tasked by DPW with 20 objectives for assessing the performance of Pennsylvania's managed care entities. To an extent, the scope of work parallels past requirements for the implementation of the three mandatory EQRO protocols and several optional protocols for PHMCOs, BH-MCOs, and Long Term Living (LTL) PIHPs. The DPW and IPRO have partnered to apply the knowledge, practical knowhow, best practices and lessons learned from conducting EQRO and related quality assessment and improvement activities for other states and government agencies. The goal is to improve the quality of managed care in Pennsylvania. The EQRO bring new ideas, a fresh perspective, and creative solutions that have been successful elsewhere to the DPW and to determine their applicability in Pennsylvania. **Technical Services** IPRO and its partners, including Innovative Business Concepts, are tasked by DPW with 20 objectives for assessing the performance of Pennsylvania's managed care entities. To an extent, the scope of work parallels past requirements [How} for the implementation of the three mandatory EQRO protocols and several optional protocols for PHMCOs, BH-MCOs, and Long Term Living (LTL) PIHPs. **Facilities Management** IBC is providing IPRO with building, facilities, network, application development, and administrative assistance in support of the project. IBC has secured and leases a location within the capital region for IPRO to utilized for the state contract. IBC provides all utilities and management/upkeep for this location. IBC maintains all IT equipment and software, telephones, furniture and office supplies for this location.	
Project Duration:	**Start Date Year:** 2012	**End Date Year:** On-going through 2015
Nature of the Client:	Commonwealth of Pennsylvania Department of Public Welfare Managed Healthcare	
Nature of Client Audience:	The goal is to improve the quality of managed care in Pennsylvania. Therefore, potentially, all effected by managed health care in the Commonwealth of Pennsylvania	

Name of Client & Project Title	Commonwealth of Pennsylvania, External Quality Review Organization (EQRO) – Department of Public Welfare (DPW) Managed Healthcare
Number of Users:	This is Quality Management for all of the healthcare participates of the state of Pennsylvania to include but not limited to Medicaid recipients
# & Composition of Vendor Employees & Consultants Assigned:	**Vendor Project Manager/Key Consultant on Project Team:** Two administrative assistants, one programmer and a facilities /project manager. IBC created and maintains and office in the capitol area for IPRO
Client Contact Information:	**Reference Contacts:** **Name:** [redacted] **Title:** [redacted] **Department:** Managed Care **Full Address:** IPRO, 1979 Marcus Avenue Lake Success, NY 11042 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** Contract Manager **Name:** [redacted] **Title:** [redacted] **Department:** Managed Care **Full Address:** 1979 Marcus Avenue Lake Success, NY 11042 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** Manager

4.5.11 PC Network, Inc. Project References

PC Network, Inc. Reference 1: Verizon

Name of Client & Project Title	Verizon – Customer Satisfaction Surveys for the Commonwealth of Pennsylvania Telecommunications Contract	
Contract Value	$2,000,000	
Nature and Scope of Project:	**Project Description** To address a contractual requirement for end user feedback and customer satisfaction surveys, Verizon turned to PC Network, Inc. (PCN) to provide these services in support of the Commonwealth of Pennsylvania's quality management activities surrounding the state telecommunications contract. **Services Management** Feedback is solicited from Commonwealth end users of the Verizon CoPA Service Desk and related telecommunications support services through a survey that is generated for every closed service request in Remedy. In addition, Commonwealth agency stakeholders are surveyed on a quarterly basis to obtain feedback on Verizon's overall performance. Verizon obtains reports on a monthly and quarterly basis, with survey "alerts" set up to provide instantaneous feedback when survey responses exceed predetermined thresholds. Feedback is incorporated into Verizon's continual service improvement plans and subsequent actions. All survey data is accessible via a Web-based portal. Dashboards, views, reports and data queries can be customized to suit data access requirements. This project compares similarly in size, scope and complexity with the requirements for customer satisfaction surveys in the CoPA Data Center Computing Services RFP. Customer satisfaction surveys are a key component of the Commonwealth's overall quality management program. PCN's customer satisfaction surveys have helped Verizon continually improve their performance by identifying areas of improvement provided by Commonwealth end users. Satisfaction measurements have trended upward over time as Verizon continually seeks to raise their overall customer satisfaction scores. PCN currently sends out approximately 1,700 surveys per month, with an average return rate of nearly 10%. During an average month, PCN passes along approximately 15 service alerts to Verizon. A dedicated team quickly addresses each alert through direct customer contact, root cause analysis, corrective actions and other methods to ensure the problem is addressed and complete customer satisfaction attained. This is for customer satisfaction surveys only, which are a requirement of the RFP. The services below are not part of the deliverables associated with customer satisfaction surveys.	
Project Duration:	**Start Date Year:** 2010	**End Date Year:** On-going
Nature of the Client:	The end client included the Commonwealth of Pennsylvania's Office of Information Technology, Office of Administration (OA/OIT), who managed the Verizon contract on behalf of Commonwealth agencies and other organizations.	

Name of Client & Project Title	Verizon – Customer Satisfaction Surveys for the Commonwealth of Pennsylvania Telecommunications Contract
Nature of Client Audience:	The customer for this service included agency end users who opened a service request and received support from Verizon's service desk. In addition, agency IT leadership receives quarterly customer satisfaction surveys to solicit feedback on Verizon's overall contract performance.
Number of Users:	More than 56,000 lines transitioned to-date
# & Composition of Vendor Employees & Consultants Assigned:	PCN's Verizon Client Executive and Customer Satisfaction Survey Practice Manager, Frank Potter, was assigned to the start-up and ongoing maintenance of this project. The start-up period took approximately three months to complete, pending vendor activity that could be measured. Surveys are sent to end users and Commonwealth stakeholders on a monthly and quarterly basis, respectively. Reports are also generated on a monthly (End User Feedback) and quarterly (Customer Satisfaction Surveys) basis.
Client Contact Information:	**Reference Contacts:** **Name:** [redacted] **Title:** [redacted] **Department:** Verizon Enterprise Solutions – CoPA Account **Full Address:** 303 Walnut Street, 8th Floor Harrisburg, PA 17101 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** Third party vendor management **Name:** [redacted] **Title:** [redacted] **Department:** Verizon Enterprise Solutions – CoPA Account **Full Address:** 303 Walnut Street, 8th Floor, Harrisburg, PA 17101 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** Overall program management

PC Network, Inc. Reference 2: Verizon

Name of Client & Project Title	Verizon – DNS, DHCP and IP Address Management (DDI) Managed Services for Nissan	
Contract Value	More than $2,500,000	
Nature and Scope of Project:	**Project Description** PCN's end-to-end IPAM (DNS/DHCP/IP Address Management) Managed Services Solution was selected by Verizon to provide IPAM managed services under a multi-year network management contract for Nissan, a global Japanese automaker. **PMO and Services Management** PCN provided project management support and coordination of all activities from design through implementation. We utilized PMP certified project managers and followed PMBOK best practices to help ensure that the project completed on time and budget. Our project managers excel in complex, multi-vendor environments. **Manage Hosting Services** PCN designed, deployed and currently operates and manages a secure, high availability, highly resilient configuration of network appliances that provide centrally managed IP addressing as well as distributed Microsoft DNS & DHCP servers. PCN's IPAM Solution meets the customer's strict 7x24 SLAs and is delivered from our network operations center in Philadelphia, PA. PCN continuously monitors the customer's network environment for DDI service issues through the development and implementation of our proprietary DDI monitoring system. Strict change control processes have been developed with both Verizon and the end customer, and are followed for all MACDs to ensure accuracy and desired outcomes. In addition to DDI managed services, PCN also provides IPv6 consulting services to assist in IPv6 conversion and compatibility. The Commonwealth's Data Center Computing Services RFP requires vendors to provide an IPv6 enterprise migration plan and be able to support both IPv6 and IPv4 formats. DDI managed services may not be in the current scope of the proposed contract, but could easily be an add-on business opportunity should the Commonwealth wish to outsource this function. With the advent of IPv6, the need for DDI managed services in large enterprises will be mandatory, as managing expanding and more complex network environments cannot be accomplished any longer through manual methods. Properly managing DDI reduces the risk of service outages, improves network security, and enables network administrators to more easily manage the expanding number of IP devices. Expand on DDI, break into proper categories, We are only discussing past performance. It is our job to show through past performance how this supports and benefits the new contract	
Project Duration:	**Start Date Year:** 2010	**End Date Year:** On-going
Nature of the Client:	Nissan's IT network services group provides oversight to Verizon and PCN.	
Nature of Client Audience:	The client audience includes all Nissan users of IP-based technologies	

Name of Client & Project Title	Verizon – DNS, DHCP and IP Address Management (DDI) Managed Services for Nissan
Number of Users:	Thousands of global Nissan employees
# & Composition of Vendor Employees & Consultants Assigned:	PCN's IPAM Practice Manager, Dave Champagne, was the key consultant on the project team. Key Nissan and Verizon stakeholders also participated in the process, which included a takeover of the current environment prior to going live with PCN's DDI managed service.
Client Contact Information:	**Reference Contacts:** **Name:** [redacted] **Title:** [redacted] **Department:** Verizon Enterprise Solutions – Nissan Account **Full Address:** 610 North Morgan Street Tampa, FL 33602 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** Responsible for overall program management **Name:** [redacted] **Title:** [redacted] **Department:** Verizon Enterprise Solutions – Nissan Account **Full Address:** 7000 Weston Parkway Cary, NC 27513 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** Transition Project Manager

PC Network, Inc. Reference 3: Dell

Name of Client & Project Title	Dell – Commonwealth of Pennsylvania and City of Philadelphia Deployment Services
Contract Value	More than $1,000,000
Nature and Scope of Project:	**Project Description** PCN provides technical deployment services and project management services for Dell's customers, including the City of Philadelphia and the Commonwealth of Pennsylvania. PCN collaborates with Dell to schedule and project manage technology refreshes with City and Commonwealth agencies, to pilot technology roll outs, work with Dell in developing images, and to deploy hardware and manage reverse logistics. **Program Management Office (PMO) and Management Services** This project reference describes PCN's ability to successfully manage and implement projects for diverse state and local government entities. PCN also provides ad hoc staff augmentation for 49 technical labor categories. **Technical Services** As one of Dell's premier partners in the Commonwealth, PCN maintains a storage depot at its Philadelphia headquarters where Dell directly ships equipment for preparation prior to implementation. Services include operating system installations, standard image development and copying, network configuration, equipment delivery, installation and other services. PCN technicians provide delivery, installation and support directly at customer sites. PCN provides project management services to coordinate all activities across all involved parties, including Dell, PCN employees and end customers.
Project Duration:	**Start Date Year:** 2010 | **End Date Year:** On-going
Nature of the Client:	Clients served by this service include Commonwealth and City of Philadelphia agencies.
Nature of Client Audience:	The client audience served by PCN includes Commonwealth and City of Philadelphia agency users of Dell technologies.
Number of Users:	Thousands of Commonwealth and City of Philadelphia staff members
# & Composition of Vendor Employees & Consultants Assigned:	PCN deploys a project manager along with a deployment team large enough to handle varying workloads over time, as agency refresh schedules vary along with project implementation timeline windows.
Client Contact Information:	**Reference Contacts:** **Name:** [redacted] **Title:** Manager **Department:** Service Delivery Management **Full Address:** 105 Davis Road Phoenixville, PA 19460 **Telephone:** [redacted] **E-mail:** J[redacted]

Name of Client & Project Title	Dell – Commonwealth of Pennsylvania and City of Philadelphia Deployment Services
	Relation/Role to Project: Client management and project oversight **Name:** [redacted] **Title:** [redacted] **Department:** Major Public Accounts **Full Address:** One Dell Way Round Rock, TX 78682 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** [redacted]

PC Network, Inc. Reference 4: Verizon

Name of Client & Project Title	Verizon – Project Management and Subject Matter Expert Augmentation for the Commonwealth of Pennsylvania Telecommunications Contract	
Contract Value	$7,000,000	
Nature and Scope of Project:	**Project Description** Upon the signing of Verizon's seven plus year, $7,000,000 contract to provide telecommunications, networking and security services for the Commonwealth of Pennsylvania, it became immediately clear that the local team was understaffed to transition from the prior vendor in the timeframes agreed to in the contract. PCN's project managers and technical specialists helped to drive a complex and aggressive transition to completion, while identifying and implementing improved processes for order entry, provisioning, dispatch and implementation. PCN also was able to bring technical expertise no longer available in Verizon's organization, which was specific to the Commonwealth's prior telecommunications environment. **Program Management Office (PMO) and Services Management** Verizon engaged PCN to provide project management and other subject matter experts to assist in the transition of voice, data and internet/security services. In addition to project managers, PCN provided more than security experts, order entry specialists, programmers and other technical experts who worked in short, medium and longer term capacities. **Technical Services** Verizon's contract with the Commonwealth required a complex transition of voice, data and internet/security services from the prior vendor over to Verizon in a very short time frame. Data transitions were completed in a timely fashion, while voice services underwent a transformation through the implementation of a new telecommunications Voice Over IP (VoIP) system. Through the Penn Connect project, Pennsylvania became one of the first states to implement a true Unified Communications (UC) telecommunications system, which integrates voice over IP telephony, instant messaging, video conferencing, e-mail and other information technology communication tools.	
Project Duration:	**Start Date Year:** 2010	**End Date Year:** On-going
Nature of the Client:	The end client included the Commonwealth of Pennsylvania's Office of Information Technology, Office of Administration (OA/OIT), who managed the Verizon contract on behalf of Commonwealth agencies and other organizations.	
Nature of Client Audience:	The customer for this service included agency telecommunications leadership and the agency end users they serve.	
Number of Users:	More than 56,000 lines transitioned to-date	
# & Composition of Vendor Employees & Consultants Assigned:	PCN's Verizon Client Executive Frank Potter managed a team of more than 20 concurrent PCN contractors in support of Verizon's transition over the prior three-year period.	

Name of Client & Project Title	Verizon – Project Management and Subject Matter Expert Augmentation for the Commonwealth of Pennsylvania Telecommunications Contract
Client Contact Information:	**Reference Contacts:** **Name:** [redacted] **Title:** [redacted] **Department:** Verizon Enterprise Solutions – CoPA Account **Full Address:** 303 Walnut Street, 8th Floor, Harrisburg, PA 17101 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** Overall program management **Name:** [redacted] **Title:** [redacted] **Department:** Verizon Enterprise Solutions – CoPA Account **Full Address:** 303 Walnut Street, 8th Floor Harrisburg, PA 17101 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** Third party vendor management

4.5.12 Pierson Computing Connection, Inc. Project References

Pierson Computing Connection, Inc. Reference 1: Commonwealth of Pennsylvania

Name of Client & Project Title	Commonwealth of Pennsylvania – IBM Server-Storage Contract	
Contract Value	$6 million	
Nature and Scope of Project:	**Project Description** Over the past eight years, PCCi has provided project management and implementation services for the IBM Commonwealth of Pennsylvania server and storage contract. Throughout this contract PCCi has managed the implementation of hundreds of IBM Series X, Series P, and Series I servers as well as hundreds of Storage Area Network (SAN) solutions in Commonwealth data centers across Harrisburg. In addition, PCCi has provided deployment of geographically dispersed servers at agency locations throughout the Commonwealth as part of this contract. Throughout the life of this contract, and the prior contract as well, PCCi's team is recognized by Commonwealth agencies for their integrity, customer service and technical knowledge regarding the IBM equipment being implemented. **Program Management Office (PMO) and Service Management** PCCi has managed the Server and Storage contract for services for eight years. PCCi's project managers have performed all customer scheduling, management of resources, and follow up for this contract. **Technical Service** Under this contract PCCi has provided transition management, capacity planning, architecture of agency data center server and SAN resources, backup management, capacity planning, and emergency preparedness planning. **Datacenter Architecture** PCCi has provided services to the agencies that include consulting on use of servers and SANs across multiple data centers, facilitating their use of IBM server and storage technology to perform mirroring, data transfer, data backup and other functions required to keep multiple data centers operating smoothly.	
Project Duration:	**Start Date Year:** 2004	**End Date Year:** On-going
Nature of the Client:	Commonwealth of Pennsylvania, Office of Administration	
Nature of Client Audience:	Commonwealth agencies, particularly IT organizations	
Number of Users:	80,000	

Name of Client & Project Title	Commonwealth of Pennsylvania – IBM Server-Storage Contract
# & Composition of Vendor Employees & Consultants Assigned:	**Vendor Project Manager/Key Consultant on Project Team:** Debra Pierson, President, serves as Project Executive on this project. As the project developed multiple PCCI project managers have been engaged to make certain that client and agency satisfaction is met. Up to twenty technical resources have been available to this project, depending on peak times and agency requirements.
Client Contact Information:	**Reference Contacts:** **Name:** [redacted] **Title:** [redacted] **Department:** PA Office of Administration **Full Address:** 1 Technology Park Harrisburg, PA 17110 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** [redacted] **Name:** [redacted] **Title:** [redacted] **Department:** Server Farm Operations **Full Address:** 651 Boas Street Harrisburg, PA 17121 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** [redacted]

Pierson Computing Connection, Inc. Reference 2: Pennsylvania Department of Labor and Industry

Name of Client & Project Title	Pennsylvania Department of Labor and Industry – Unemployment Compensation Modernization Systems (UCMS)	
Contract Value	$3.1 million	
Nature and Scope of Project:	**Project Description** PCCi provided operational support to IBM and the Department of Labor and Industry for the implementation and operation of the IBM systems that support the Unemployment Compensation Modernization Systems (UCMS) application project development and systems. Responsibilities included building and configuring 45 VMware virtual servers, 42 Blade servers, and 7 System X 3650 servers spread across five different environments. Created server configuration and software installation documentation concerning all servers built for this project. Worked with the customer to optimize management software; supported and maintained servers, collaborated with developers to optimize their individual applications pertaining to this project. Maintained the developers PCs, also installed and troubleshot Rational software. Provide on-going PMO support including administrative staff and project work planner. **Program Management Office (PMO) and Service Management** PCCi manages and maintains the detailed project plan for this multiple release, multiple phase Web development project. PCCi develops, reviews, plans, consolidates and evaluates project plans from all releases and phases. PCCi also provides documentation and project tracking reporting. **Technical Service** PCCi and its subcontractor, the ATS Group, provided initial Technical Architecture and planning services for this project.	
Project Duration:	**Start Date Year:** 2006	**End Date Year:** On-going
Nature of the Client:	Pennsylvania Department of Labor and Industry, Bureau of Unemployment Compensation	
Nature of Client Audience:	Businesses and unemployed individuals throughout Pennsylvania	
Number of Users:	20,000	
# & Composition of Vendor Employees & Consultants Assigned:	**Vendor Project Manager/Key Consultant on Project Team:** Debra Pierson serves as Project Executive for this project. Rick Loffredo serves as Project Manager for PCCi. At its peak, PCCi provided ten resources providing technical support and PMO support for this project.	

Name of Client & Project Title	Pennsylvania Department of Labor and Industry – Unemployment Compensation Modernization Systems (UCMS)
Client Contact Information:	**Reference Contacts:** **Name:** [redacted] **Title:** [redacted] **Department:** Information Technology (IT) **Full Address:** 651 Boas Street Harrisburg, PA 17121 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** [redacted] **Name:** [redacted] **Title:** [redacted] **Department:** UC Division, OIT Bureau of Business Application Development **Full Address:** Department of Labor and Industry 651 Boas Street Harrisburg, PA. 17121 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** [redacted]

Pierson Computing Connection, Inc. Reference 3: Commonwealth of Pennsylvania

Name of Client & Project Title	Commonwealth of Pennsylvania – Data PowerHouse (DPH)	
Contract Value	$365,000	
Nature and Scope of Project:	**Project Description** We support the current Commonwealth of Pennsylvania (CoPA) Data PowerHouse (DPH) outsourcing contract by providing support for Availability Management, Change Management, Problem Management, Incident Management, Service Level Agreement Management, and Root Cause Analysis Management for the IBM agencies (PennDOT, DOR, L&I UC, DOC, AGING, L&I BOIS, SCSC) in the contract. We also provide monthly metric reporting for the IBM agencies in the contract, as well as SAS70/SSAE16 audit support. We have provided this support since 2008. **Program Management Office (PMO) and Service Management** Pierson Computing Connection, Inc. is providing this Commonwealth project with Change Management, Problem Management, Incident Management, Availability Management, Service Level Agreement Management, and Root Cause Analysis Management for the IBM agencies in the contract. We also provide monthly metric reporting for the IBM agencies in the contract, as well as SAS70/SAE16 audit support.	
Project Duration:	**Start Date Year:** 2009	**End Date Year:** On-Going
Nature of the Client:	Commonwealth of Pennsylvania	
Nature of Client Audience:	Information Technology (IT) staff of agencies	
Number of Users:	Commonwealth-wide	
# & Composition of Vendor Employees & Consultants Assigned:	**Vendor Project Manager/Key Consultant on Project Team:** Curtis Wilson, Availability Manager, provides the resources under this contract.	
Client Contact Information:	**Reference Contacts:** **Name:** [redacted] **Title:** [redacted] **Department:** PennDOT **Full Address:** 400 North Street Harrisburg, PA, 17120 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** [redacted] **Name:** [redacted] **Title:** [redacted] Department of Corrections **Department:** Bureau of Information Technology **Full Address:** 1920 Technology Parkway Mechanicsburg, PA, 17050 **Telephone:** [redacted] **E-mail:** [redacted] **Relation/Role to Project:** [redacted]	

4.6 Subcontractors and Suppliers

4.6.1 Unisys Subcontractors and Suppliers Capabilities Table

The nature of the Commonwealth of Pennsylvania Data Center Computing Services Project encompasses aspects that make teaming with subcontractors and suppliers a critical program success factor. Section 4.6.1 provides a summary of key factors used to identify the need for our primary subcontractors and small subcontractors and the type of support they will provide for CoPA. Unisys and these subcontractors make up the "Unisys Team." In addition, key suppliers have been identified to provide resources to support the project. **Table 4-4** provides a summary of the level of support each of our subcontractor and supplier partners will provide the Commonwealth.

Table 4-4. List of Subcontractor and Supplier Capabilities

Subcontractor/Supplier	Small Diverse Business	PMO & Mgt Services	Technical Services	System and Data Security	Facilities Management	Manage Hosting Services	Capacity on Demand & Additional Services	Data Center Architecture / Components
IBM		X	X	X		X	X	X
Deloitte			X	X			X	
Acclaim Systems, Inc.	X		X					
APMC, Inc.	X		X					
Credo TS, Inc	X		X					
Domino Tech, Inc	X		X					
e&e IT Inc	X		X					
Info-Matrix Corp	X		X					
IBC Inc	X		X					
PC Network Inc	X		X					
Suppliers								
Harrisburg University		X						
Latus Commercial Realty	X				X			
Metropolitan Technology Services	X							X
Pierson Computing Connection	X							X

Schedule L – Unisys List of Subcontractors

RFP	Requirement
	The Offeror must provide a list of all proposed subcontractors that will be used as part of the project using Schedule L – Approved Subcontractors.

In the following subtab, Unisys includes Schedule L, which lists our subcontractors on this project.

Request for Proposal

RFP # 6100022698

Commonwealth of Pennsylvania

Office of Administration

Office for Information Technology

Data Center Computing Services

SCHEDULE L

APPROVED SUBCONTRACTORS

(Offeror to provide a list of Offeror's subcontractors within the Schedule)

APPROVED SUBCONTRACTORS

- IBM Corporation
- Deloitte LLP
- Acclaim Systems, Inc.
- American Personnel Managers & Consultants, Inc.
- Credo Technology Solutions, Inc.
- Domino Technologies, Inc.
- e&e IT Consulting Services, Inc.
- Info-Matrix Corporation
- Innovative Business Concepts, Inc.
- PC Network, Inc.

IBM Corporation

IBM Corporation is a globally integrated technology and consulting company headquartered in Armonk, New York. With operations in more than 170 countries, IBM attracts and retains some of the world's most talented people to help solve problems and provide an edge for businesses, governments and non-profits. Innovation is at the core of IBM's strategy. The company develops and sells software and systems hardware and a broad range of infrastructure, cloud, managed hosting services like those and consulting services many of which are very similar to the Commonwealth's requirements.

IBM is focusing on four growth initiatives - business analytics, cloud computing, growth markets, and Smarter Planet. IBM is working with customers around the world to apply the company's business consulting, technology and R&D expertise to build systems that enable dynamic and efficient organizations, better transportation, safer food, cleaner water and healthier populations.

IBM will be providing technology products and managed services for mainframe/mid-range based applications including disaster recovery and capacity on demand services to the project.

Deloitte LLP

In the United States, Deloitte LLP and its subsidiaries have 57,000 professionals with a single focus: serving their clients and helping them solve their toughest problems. They work in four key business areas including audit, financial advisory, tax, and Information Technology consulting. Deloitte has significant experience in supporting the Commonwealth of Pennsylvania with some of their most complex application projects and they perform most of the enterprise security work for the Commonwealth.

Deloitte provides technical security services and database management support services for the project.

Acclaim Systems, Inc.

Acclaim Systems is a leading software solution company offering a multitude of comprehensive and customized services. They are committed to maintaining client relationships by effectively aligning technology and consulting resources with clients' dynamic business requirements. They succeed by investing in the professional fulfillment of their employees, empowering them to deliver high quality solutions. Acclaim has significant experience supporting the Commonwealth and Unisys by providing experienced IT resources for critical development and managed services projects. They are a Pennsylvania verified Small Diverse Business.

Acclaim Systems will be providing technical resources in support of Microsoft and Linux operating systems, and the Microsoft Exchange system. In addition, Acclaim Systems will provide project management resources to the support the Transition plan of the project.

American Personnel Managers & Consultants, Inc.

American Personnel Managers & Consultants, Inc. is a superior Human Resource Management and Recruiting firm, Staffing and Project Management company with more than 70 years of experience in the Staffing arena and 13 years of experience with staffing the Pennsylvania Data PowerHouse project. APMC also has extensive experience in providing project work for many Commonwealth agencies. They are a Pennsylvania verified Small Diverse Business.

A leading innovator in work force staffing solutions, connecting “people potential” to the needs of today’s ever changing business requirements, they provide unparalleled experience, comprehensive capabilities across state & federal government lines, with a collaborative and customized focus on client needs through: On-Site Project Management; Staff Augmentation; outsourcing; short and long term staffing and management.

For this project, APMC will be providing operational support resources to monitor system consoles and will be staffing the media management operation to ensure computer tapes are available for critical data backup and restore operations, inventoried, and stored offsite for data protection in the event of a disaster.

Credo Technology Solutions, Inc.

Credo, a Minority Business Entity (MBE), has built a tight cadre of team members focused on consistently delivering services that help clients meet their IT challenges. By maintaining strong relationships with a variety of leading IT companies, Credo’s staff

and strategic partners are able to offer business and technology solutions, as well as project management offerings. They are a Pennsylvania verified Small Diverse Business.

Credo's portfolio of services includes, but is not limited to:

- Enterprise Resource Planning (ERP)
- PeopleSoft and Oracle Consulting
- Software Application Development
- IT Staffing
- Social Media Consulting
- Service Oriented Architecture

Credo Technology Solutions will be providing technical and project management support resources to the project.

Domino Technologies, Inc.

Since its founding in 1996, Domino Technologies, Inc. has built a solid record of performance working with clients in both the private sector and government. They have consistently delivered innovative solutions, using the latest technology to fulfill clients' goals. The result is an intense focus on resolving precise challenges, leading to a reduction in time required to complete the job and ultimately to increase your company's profits.

Domino Tech will be providing technical and project management support resources to the project. They are a Pennsylvania verified Small Diverse Business.

e&e IT Consulting Services, Inc.

e&e IT Consulting Services is a certified Woman Business Enterprise (WBE) technology services firm providing staffing solutions in Pennsylvania, Virginia, New Jersey, and the City of Philadelphia. e&e IT provides all levels of skilled IT professionals to clients in Central Pennsylvania and surrounding areas. They have been recognized, for the sixth consecutive year, as one of the Top 50 Fastest Growing Companies in Central Pennsylvania, making significant contributions to the growth, strength, and success of the Central Pennsylvania region.

e&e IT will be providing technical and project management support resources to the project. They are a Pennsylvania verified Small Diverse Business.

Info-Matrix Corporation

Info-Matrix is a private, woman-owned information technology consulting firm based in Lemoyne, Pennsylvania. Since 1996, Info-Matrix has focused largely on the government sector, with an emphasis in human services IT projects, including, for example, Medicaid eligibility, welfare case management and child support enforcement systems. From Texas to Alaska, Info-Matrix has broad experience at the federal, state, and local levels hiring experienced professionals with an average of 15 years of IT experience who have distinguished themselves by successfully implementing complex government IT projects.

Info-Matrix will be providing technical and project management support resources to the project. They are a Pennsylvania verified Small Diverse Business.

Innovative Business Concepts, Inc.

Since 1989, Innovative Business Concepts, Inc (IBC) has been a Pennsylvania Certified Woman-Owned Business empowering customers to maximize productivity, efficiency and cost savings by deploying the best people, practices and knowledge in the technology industry. They provide world-class IT personnel, products and services.

Innovative Business Concepts, Inc (IBC) will be providing technical and project management support resources to the project. They are a Pennsylvania verified Small Diverse Business.

PC Network, Inc.

PCN is a growing, woman-owned, IT services company based in Center City Philadelphia. They work with enterprises, prime contract partners, and the public sector to affordably solve the many complex problems facing business today. Their customers span the Commercial, Transportation, Defense, and Government sectors. PCN was founded in 1988; they have evolved from their traditional systems integrator roots to provide a broad range of IT consulting services. PCN has a strong focus on quality with ISO 9001 and TL9000 quality programs. PCN is ISO 27000 Compliant.

The PCN portfolio of services help their customers balance cost and productivity throughout your technology's lifecycle. They deliver technology solutions and skilled IT professionals that optimize your existing infrastructure and provide planning and design support to ensure systems continue to meet emerging business and technological needs. They are a Pennsylvania verified Small Diverse Business.

PCN will be providing the following services for the project:

- Customer Satisfaction Survey Support
- IPV6 Strategy Services
- Service Desk Staffing

This page intentionally left blank.

5.0 Personnel

5. Personnel 5-3

5.1 Current Organizational Structure 5-7
5.2 New Organizational Structure 5-8
5.3 Key Personnel Overview 5-12
5.4 Details of the New Organization 5-13
5.5 Roles and Responsibility – High Level Steady State 5-15
5.6 Roles and Responsibility – High Level Transition (includes Architect, Build) 5-17
5.7 Agency Centric Staffing Approach 5-19
5.8 Interaction with the Commonwealth 5-20
5.9 Transition Staffing Approach 5-23
5.10 Key Personnel Table 5-25
5.11 Subcontractor Key Personnel Table 5-33
5.12 Organizational Function Discussion 5-36
5.13 HR Discussion 5-66
5.13.1 Staff Contingency Plan 5-66
5.13.2 Staff Management 5-67
5.13.3 Training Policies and Procedures 5-69
5.13.4 Staff Retention 5-72

""We understand the importance of providing you the right technology in your data center compute environment to enable your transition to the innovative business model of the future. More importantly, we know that it takes the right complement of expertise on our team to successfully work with you as one team to implement the solution. The team established to support the Commonwealth of Pennsylvania understands and respects the individuality of the agencies, each with its own unique team, priorities, needs and working style. Our team has a rich history of working with you to accomplishment your most critical Information Technology initiatives, and we are looking forward to continuing to be a part of your team building your 'new world' together."

[redacted] ***Unisys Engagement Executive***

".... I felt I needed to send a heartfelt "Thank You" for allowing [redacted Agency Account Manager] to continue supporting DOS. Unisys has always been a great partner to us in providing very competent team members that support us well. [redacted] holds customer service qualities that are second to none. We absolutely enjoy working with her and know she is a great advocate to keeping the Department's applications up and running 24x7. Her personality, knowledge, and skill are enjoyed by the entire DOS team. Thank you again."
—Tim Ruppert, Former Director, Pennsylvania Department of State, Bureau of Management Information Systems

"I will echo Tim's comments. [redacted] is exceptional at customer service and follow through. She not only keeps everything on track within Unisys, she also makes sure that nothing falls through the cracks on our end as well with the change requests. I appreciate [redacted] and her abilities! She is part of our team over here and the team is working well. Thank you very much for allowing her to continue to serve us! It means a lot to this agency!"
—Dave Burgess, Former Deputy Secretary for Planning and Service Delivery, Department of State

This page intentionally left blank.

5. Personnel

RFP	*Requirement*
II-5	*Personnel. Include the number of executive and professional personnel, analysts, auditors, researchers, programmers, consultants, etc., who will be engaged in the work. Show where these personnel will be physically located during the time they are engaged in the Project.* ***Refer to Schedule G - Staffing Plan and Key Positions*** *for key personnel, include the employee's name and, through a resume or similar document, the Project personnel's education and experience in respective Account Role as defined within* ***Schedule G - Staffing Plan and Key Positions****. Indicate the responsibilities each individual will have in this Project and how long each has been with your company. Identify by name any subcontractors you intend to use and the services they will perform.*

As discussed in the Management Summary section of our proposal, given our commitment to the Commonwealth of Pennsylvania it should be noted that [redacted], Unisys Chairman and CEO, is this engagement's executive sponsor and will personally ensure our company's complete commitment to its success in the implementation of a new compute services model at the Commonwealth.

In addition to [redacted] role as Executive Sponsor, Unisys established an Executive Leadership Committee shown in **Figure 5-1** to support the efforts of our Harrisburg-based leadership team. We created this committee to provide direct visibility into senior leadership at Unisys to confirm we meet our commitments to the Commonwealth, during both transition and steady state operations, and to break down the inevitable barriers that arise during engagements of this magnitude.

"Our decades of experience in successfully implementing large, complex initiatives teaches us the importance of selecting the right delivery team and empowering them to make decisions locally based on the client's needs and expectations. [redacted] *are some of the very best in service delivery. They have my full support and are empowered to make the necessary decisions to help ensure success. Their team is complemented by a Unisys Executive Oversight Committee focused on providing whatever additional corporate resources and support are necessary."*

— [redacted]
Commonwealth Executive Sponsor
Chairman & CEO

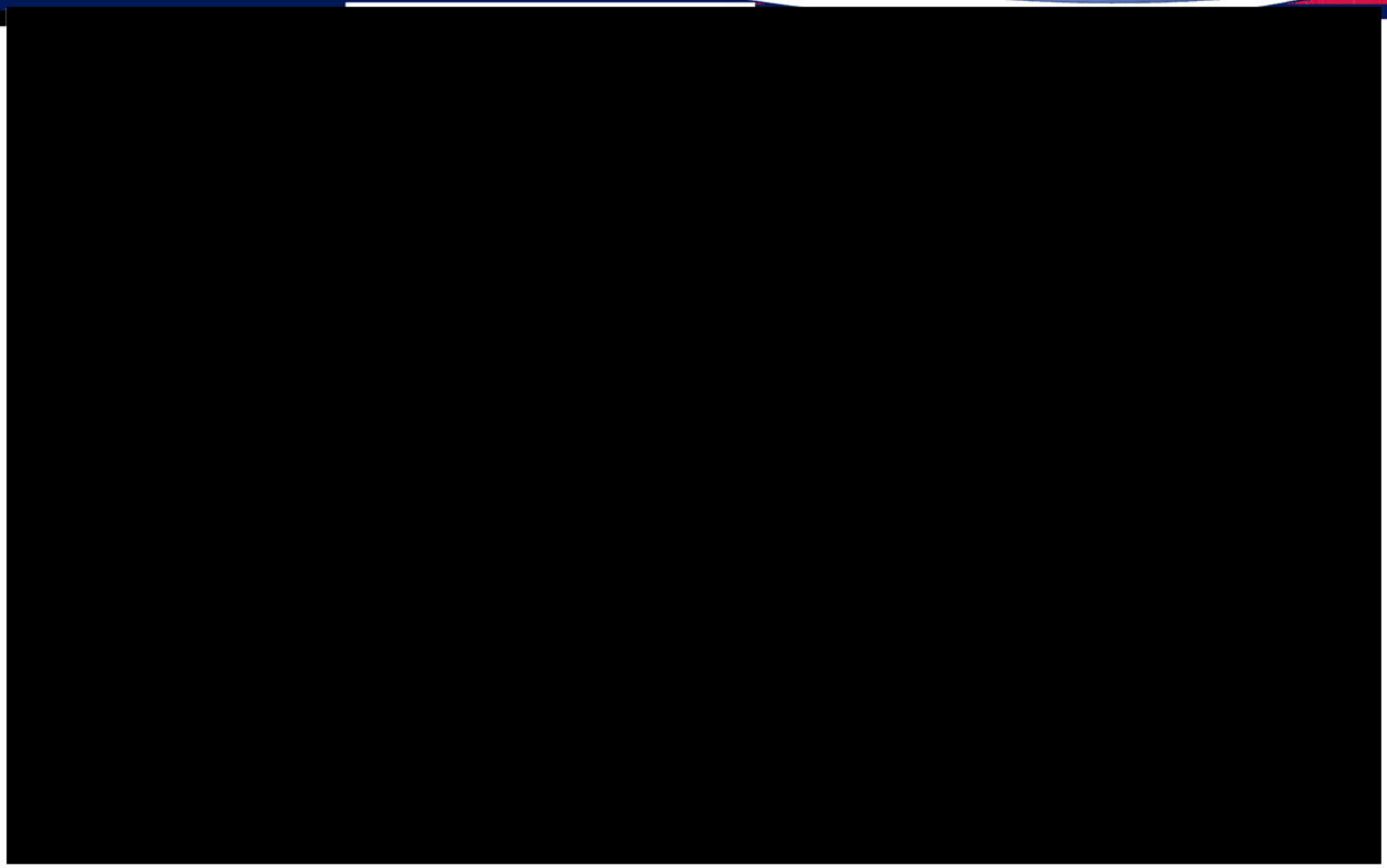


Figure 5-1. Unisys Executive Leadership Committee

Our **Executive Committee consists of:**

- [redacted], Unisys President of Global Service Delivery
- [redacted], Unisys Vice President of Global Service Delivery
- [redacted], IBM Vice President of Global Technology Services
- [redacted], Unisys Vice President of North America Service Delivery
- [redacted], Unisys Vice President and General Manager of North America Service Delivery
- [redacted], Unisys Chief Technology Officer, Technology and Innovation
- [redacted], Unisys Vice President, Commonwealth of Pennsylvania Region
- [redacted], Deloitte Principal, Security and Privacy Services

The Commonwealth's new compute services model will yield many efficiencies but requires a vast, sophisticated, multi-data center operation providing managed services to approximately 50 agencies across nearly 11,000 diverse systems, according to volumetrics data provided in Schedule I. To be successful, it must leverage disciplined processes aligned with ITIL best practices and provides accountability to deliver against stringent SLAs across more than 30 categories. That requires an experienced leader with an extensive background, not only with the associated technologies, tools, and methods, but familiarity with the Commonwealth agencies and their individual needs.

[redacted] will lead a team of 6 extremely capable Unisys executives (based in Harrisburg) who, in turn, will oversee a team of 278 professional, skilled resources to transition and implement the Compute Services Solution described in Section 3.0 of our proposal. Included in the 278 team members are 135 professionals from our subcontractors, IBM, Deloitte, and small diverse businesses.

With Unisys as your prime contractor, [redacted] will continue to be fully empowered and will manage the entire engagement with the Commonwealth. As with the managed services we provide today, [redacted] will take responsibility for all issues and concerns related to our team or infrastructure provided, regardless of the problem's original source. As demonstrated over the past 13 years, we will own and solve problems instead of engaging in the typical finger-pointing and blame game played by many other service providers.

Our Integrated Staffing (Organization) Plan described in this section defines how our new team members will join the transition. At the same time, during transition, we will bring the current data center contract to closure, allowing our skilled team to focus and support the new contract.

We selected a very experienced resource, [redacted], to lead the transition effort. Transition is one of the most important tests of this effort; we wanted a very skilled and experienced leader to help plan and execute the transition. With his experience on similar transitions while working for HP/EDS and Dell/Perot Systems, [redacted] is an excellent choice. We also took great care to select other senior members of our team as well. They are identified further in this section of our proposal.

Table 5-1 lists the location in our proposal where the solution components requested in Schedule G are discussed.

Table 5-1. Location of Solution Components in Proposal

Schedule G Requirement	Location of Discussion
Integrated Staffing Organizational Plan	Sections 5.1 – 5.12
Details of the team – Steady State	Section 5.5
Details of the team – Transition (includes architect, build)	Section 5.6 and 5.9
Proposed use of subcontractors	Sections 5.11 and 5.12
Unisys Expectations of Commonwealth Resources	Sections 5.8 and 5.9
Unisys and Commonwealth resource interaction	Section 5.8

Schedule G Requirement	Location of Discussion
Staffing Plan detailing number of personnel, level, and role	Sections 5.5 and 5.6
Proposed organization chart for Unisys and subcontractors	Section 5.12
Identification of key personnel on organization chart	Section 5.12
Summary of key personnel high level responsibilities	Section 5.12
Offeror Key Personnel Table	Section 5.10,
Subcontractor Key Personnel Table	Section 5.11
Staff Contingency Plan	Section 5.13.1
Staff Management	Section 5.13.2
Training Policies and Procedures	Section 5.13.3
Staff Retention	Section 5.13.4

The Unisys staffing strategy is a critical component of the success of the Commonwealth's Data Center Computing Services (DCCS) initiative. The architecture and technology solution provide a foundation to meet the Commonwealth compute requirements and overall goals. Selecting the right composition for the team to define and execute our strategic plans is paramount to the overall program's success.

The detailed subsections of Section 5 provide the specifics of our Integrated Staffing (Organization) Plan strategy. Because Unisys is the incumbent vendor, our discussion of the overall project organization and approach begins with an overview of the current organization structure, leading to a discussion that introduces the modified high-level organization structure to manage the new contract requirements.

We are in an uncommon position to provide many technology professionals with significant experience and who currently work with the Commonwealth to provide many of the services that will be part of the new contract. This will certainly facilitate a smoother transition because our team has deep knowledge of the existing Commonwealth infrastructure and a respect for how to meet agency expectations, both for the existing services and during the transition to new services.

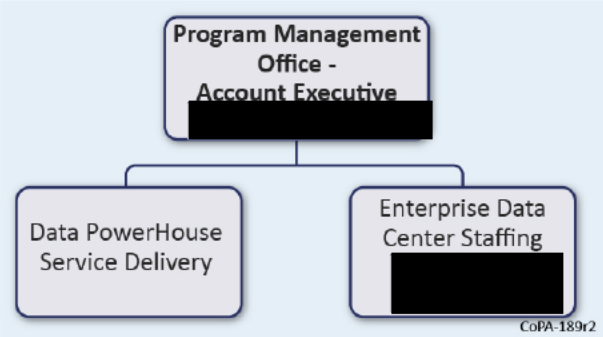
In this section, we introduce you to the key members of our team and provide details on why they were selected, the duties they will perform, and their experience supporting the Commonwealth or like engagements. This includes how we will structure the team, organize their skills, and implement the reporting hierarchy of our team. This includes an important component… how we interface with the Commonwealth team regularly. It also defines reasonable expectations for the assistance and availability of Commonwealth resources.

This discussion is important to help you understand how we will effectively transition from the requirements of the contract we support today to the organization that will enable realization of your vision, and for detailing changes required to facilitate the transformation.

5.1 Current Organizational Structure

A logical starting point for discussing the project organization plan is to review today's organization supporting our current engagements at the DPH and the Enterprise Data Center (EDC). As depicted to the right, the current structure consists of three basic organizations: the Program Management Office, the Data PowerHouse (DPH) Service Delivery Team, and the Enterprise Data Center Team.

This basic organization structure for our current contract has the right level of control to address the needs of the existing DPH contract, supporting managed services in three Service Level Agreement categories for 16 agencies and 1,200 systems from a single data center. Unisys also provides the EDC with staff augmentation in support of 48 agencies and nearly 4,000 systems.



With their historical knowledge and years of experience, the current team forms a strong foundation for the staffing plan of the new DCCS contract and a solid launching point for a number of innovative improvements to the staffing approach for the new contract. The critical enhancements necessary to support the DCCS are detailed throughout Section 5. They cover all the bases and will provide success as we transition to the new services model.

5.2 New Organizational Structure

This section presents a high-level overview of the DCCS future steady state organization structure. Later in this section, we focus on our transition staffing approach, which includes the transition of existing staff supporting the DPH and the EDC to the new organization, and how the new organization will be augmented by a transition team structure that focuses exclusively on mitigating risk and overlays the strong foundation provided by the steady state team. Our current DPH and EDC production staff will be important advisers to the transition team so the transition plan is based on reality that only comes from experience.

The figure below introduces the high-level organizational teams and the executive leaders in our PMO. Key personnel presented in **Figure 5-1** along with other key personnel introduced throughout Section 5 are defined in the abbreviated Key Personnel Table in Section 5.3, and the detailed Key Personnel Tables found in Sections 5.10 and 5.11. Short biographies of key personnel can be found throughout Section 5.12 Organizational Function Discussion.

Key Drivers of New Organizational Structure

- Sheer volume of infrastructure/agencies
- Prominent role in technology strategy
- Transparency of operations/pricing
- Centralized yet flexible communication/governance
- ITIL process alignment/discipline
- Focus on security/compliance
- Agency-centric staffing model

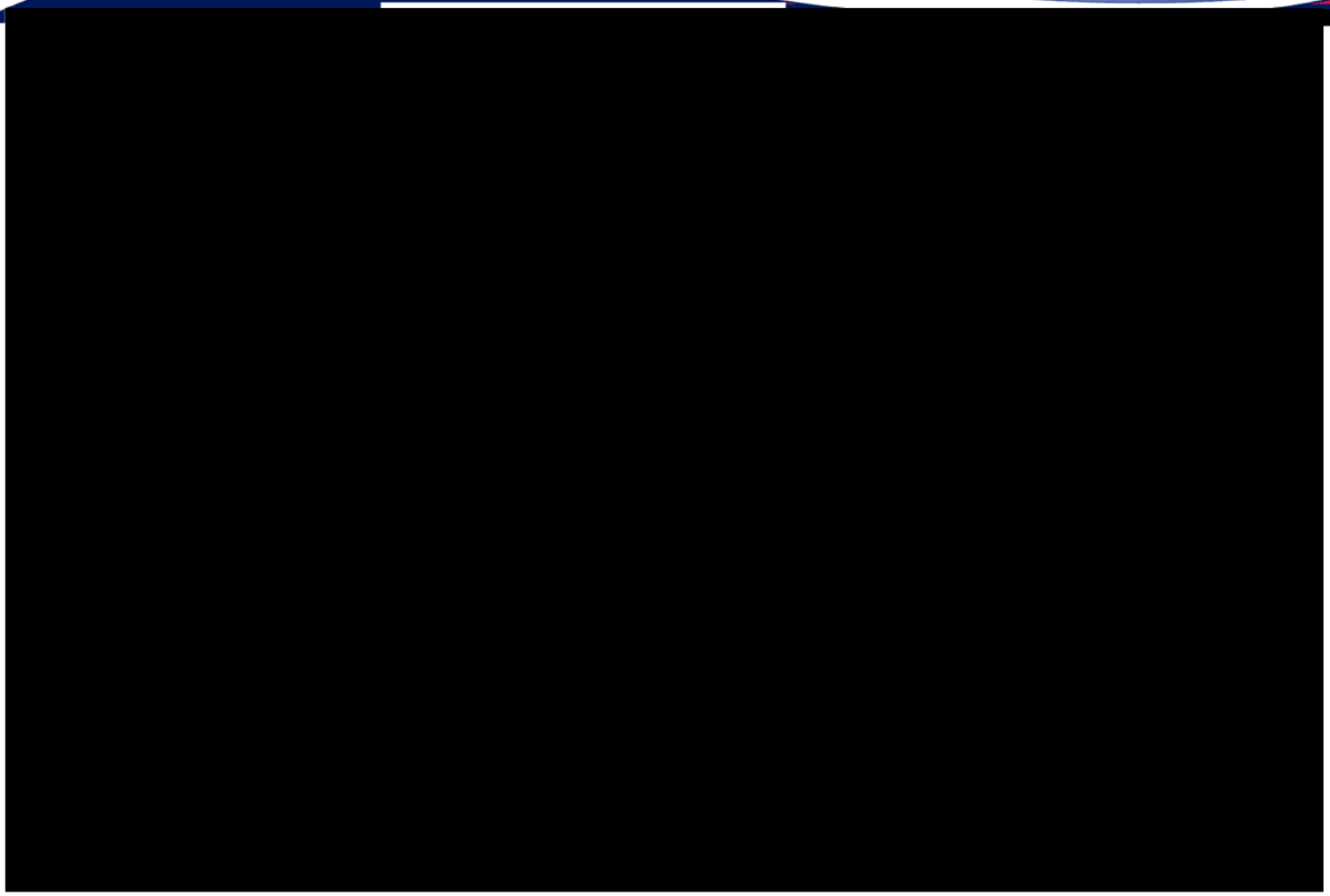


Figure 5-2. Data Center Computing Service Engagement

When contrasted with the current organization already described, the new organization is significantly enhanced by the addition of dedicated teams formed in response to new program goals and to facilitate the Commonwealth's transformation to the new model. **Figure 5-3** provides a high-level description of the functions of each of our seven core teams.

Figure 5-3. Functions of Seven Core Teams

How is the New Organization Different and What are the Benefits?

The paragraphs below highlight the differences and enhancements of the new organization compared with the current organization. A more comprehensive discussion of the overall functions of each of the seven core organizations is covered in Section 5.12.

The **Program Management Office** is an integral part of the current program and has been enhanced to manage the complexities of a much larger and very different DCCS program. This team governs and executes the overall program, projects, and contract elements, and provides ongoing direction and leadership supporting the contract and designated services for the contract's duration. Through the enhanced Financial Management function, this office provides accurate and cost-effective stewardship of IT assets and resources, providing a truly transparent analysis of the Commonwealth's spend on services. Other enhancements include a dedicated focus on subcontractor accountability for performance of services throughout the contract's term along with management of third-party software licensing and all maintenance agreements for hardware and software.

We will be leveraging a sophisticated suite of tools that will automate a number of functions that the **PMO** performs manually today including processing requests for service and approvals for contractual changes around services, hardware and software configurations, and SLAs. We will also automate processing agency level invoices with the level of detail needed to provide transparency, as well as chargeback to particular projects and general ledger codes to track federal funding spend.

The **Agency Account Management** team will be responsible and accountable for supporting each agency participating on this engagement. Unisys realizes that these roles are critical to maintaining a high level of satisfaction with the agencies and will form a dedicated team. Our Agency Account Managers will foster collaboration and are adept at building relationships and pulling teams into action to complete complex initiatives on time, within budget. Through a partnership with agency leadership, each agency account manager engenders a customer-focused culture on the service delivery teams, providing clarity on customer priorities and initiatives.

As with the current contract, **Service Delivery** continues to be at the core of our operation, providing all aspects of technology and infrastructure support to meet the day-to-day needs and to fulfill the contract's service obligations. We believe it is in the Commonwealth's best interest to deviate from an industry standard approach in which technical resources report to technology tower leaders who are typically at remote locations outside Harrisburg and implement a structure of six cross-functional teams supporting multiple technology disciplines (Windows, Network, Storage, and so forth) that report directly to a Harrisburg-based Service Delivery Manager who is directly aligned with an Agency Account Manager supporting a subset of Commonwealth agencies with similar technologies. Each Service Delivery Team led by a Service Delivery Manager has end-to-end responsibility and is fully accountable for providing services for specific agencies and all of their applications.

A significant change to **Service Delivery** relates to enhancement of the Service Desk function, which provides a central point of communication for all Commonwealth approved users and agency staff to report incidents, requests for information, and service requests for all of the services provided. This team also manages the new Knowledge Management Portal providing a central repository for processes and procedures, communication plans, and other documentation to be shared with the Commonwealth. Changes to the Service Desk will facilitate process discipline and consistency, with consistent flow of two-way communication inherent in the process.

The new **Service Excellence Office (SEO)** defines and oversees all ITIL process management and analysis functions, including management and oversight of all processes, maintaining accuracy of the CMDB, auditing process effectiveness to confirm that service delivery teams comply with proper execution of processes, and analyzing process trends for anomalies. This team verifies that all processes are accurately defined and documented in the Commonwealth Computing Procedures Manual (CCPM), and audited on a periodic basis. The SEO manages the Continuous Service Improvement and Innovation Program (CSIIP) and the Customer Satisfaction Program in collaboration with Commonwealth.

Enterprise Architecture is a new team responsible for the development and maintenance of all aspects of the Data Center Architecture Plan and Roadmap and owns the development and management of the technology management program for the compute services delivered. In partnership with Commonwealth agencies, Agency Account Managers, and the rest of the Unisys Team, this function provides leadership in the forecasting and

outlook for new technologies and compute services to be added during the program's term. This group guides IT operations in addition to performing planning, design, build, and transition support on all technical matters.

The **Transition Project Management Office (TPMO)** leverages proven Unisys methodologies to maintain a successful transition from the current Commonwealth Data Center Services model to the new model, and with the same discipline, maintains effective execution of ongoing steady state projects. This new function will include planning and execution of training required to successfully implement all of the program's aspects.

The **Information Security Office** oversees all aspects of the project to confirm compliance with security standards and requirements, develops policies, and performs periodic audits of processes and data to confirm compliance. Information security management's purpose is to align IT security with business security needs and verify that the confidentiality, integrity and availability of the assets, information, data and services match the Commonwealth's. While the current DPH program maintains a strong focus on information security, the new organization works with Commonwealth agencies to plan and implement strategies to bolster information security, taking compliance and protection to the next level.

Because of our past experience with Commonwealth agencies, Unisys believes we structured the new Compute Services Organization with sufficient power and flexibility to properly support the Commonwealth in this new venture. Other potential service providers that lack our level of knowledge and expertise with the Commonwealth may unknowingly significantly underestimate their program organization's size and scope. We did not.

5.3 Key Personnel Overview

Key Personnel

The core of this successful program is comprised of 28 key personnel. They are motivated, seasoned, ITIL V3 Foundations certified and well-educated professionals guided by an executive leader experienced with managing complex IT organizations and projects. The **key personnel** selected by Unisys provide targeted executive focus in key program areas, including program management, service delivery, service excellence and quality, enterprise architecture, transition and steady state project management, information security, and account management.

This organization's key personnel were selected not only for their experience with supporting large, complex customer environments and getting the job done with high success, but also for the collaborative style of their approach. This team of leaders can see the future of the Commonwealth DCCS model with all of its nuances and will create a vision with a roadmap guiding the delivery. They work proactively to prioritize and enable desired outcomes to be achieved to your satisfaction. The key personnel listed in **Table 5–2** have entrusted their faith to Unisys by providing us the exclusive right to represent them

in our proposal to the Commonwealth. Formal certification of that right to represent can be found in the tab behind the Key Personnel Resumes section.

Table 5-2. Key Personnel

Role/Position	Name	Reports to
Engagement Executive	[redacted]	Regional Vice President
Program Manager/Service Delivery	[redacted]	Engagement Executive
PMO Transition Manager 1	[redacted]	Engagement Executive
PMO Transition Manager 2	[redacted]	PMO Transition Manager 1
Security Manager	[redacted]	Engagement Executive
Service Excellence Officer	[redacted]	Engagement Executive
Sr. Enterprise Infrastructure Architect	[redacted]	Engagement Executive
Incident Management Manager	[redacted]	Service Excellence Officer
Availability Manager	[redacted]	Service Excellence Officer
Service Level Management Analyst	[redacted]	Service Excellence Officer
Change Manager	[redacted]	Service Excellence Officer
Change Analyst	[redacted]	Service Excellence Officer
Agency Account Manager 1	[redacted]	Engagement Executive
Agency Account Manager 2	[redacted]	Agency Account Manager 1
Agency Account Manager 3	[redacted]	Agency Account Manager 1
Agency Account Manager 4	[redacted]	Agency Account Manager 1
Agency Account Manager 5	[redacted]	Agency Account Manager 1
Agency Account Manager 6	Unnamed	Agency Account Manager 1
Agency Infrastructure Architect 1	[redacted]	Sr. Enterprise Architect
Agency Infrastructure Architect 2	[redacted]	Sr. Enterprise Architect
Agency Infrastructure Architect 3	[redacted]	Sr. Enterprise Architect
Agency Infrastructure Architect 4	[redacted]	Sr. Enterprise Architect
Agency Infrastructure Architect 5	[redacted]	Sr. Enterprise Architect
Agency Infrastructure Architect 6	[redacted]	Sr. Enterprise Architect
Finance Analyst	[redacted]	Finance Manager
Finance Manager	[redacted]	Engagement Executive
IBM Project Executive	[redacted]	Engagement Executive
IBM Service Delivery Executive	[redacted]	Program Manager

5.4 Details of the New Organization

The Unisys staffing model consists of a diverse, multidiscipline team seeded with professionals experienced in supporting technology initiatives across all compute platforms used by the Commonwealth. Most of our team has specific experience with supporting the compute needs of the Commonwealth's applications developed over the 13 years that Unisys has served the Commonwealth in the DPH. In the aggregate, our team

accumulated more than 1,000 years of experience supporting compute environments for many of the 2,000 or more Commonwealth applications.

Our key leaders and executives introduced in the previous section know that they are only as strong as the team they assemble. The winning team assembled has the right levels of knowledge, experience, and certifications coupled with many years of Commonwealth experience. As we laid out our solution and defined the staffing requirements, we located and added new faces to our team to address the new requirements for certain skills not present among the current staff. This influx of new ideas and strength is a strong demonstration of our agility and commitment to delivery of the right skills for this contract, not just protection of our current employees.

But skills and knowledge quickly lose their advantage if we do not stay current with changes in technology and processes. Therefore, our leadership creates a learning organization that provides opportunities for team members to continually expand their technical and professional skills. In fact, we expect it (as outlined Section 5.13.3 Training Policies and Procedures). Last, and most important, the team of leaders you will see throughout Section 5 are well known for their fervent customer focus, passion for the highest levels of customer satisfaction, and a solid track record of achievement.

Table 5-3 and **Figure 5-4** below provide relevant information about Unisys.

Table 5-3. Facts about the Unisys Team

Topic	Relevance
65% of Our Team has supported the Commonwealth on other engagements	We know how to deliver systems and system change to the Commonwealth
278: The number of team members it takes for a successful program	We have prepared our team for change, added new members to obtain success with the new technology and service delivery concepts.
1000+: Number of years our team members have collectively supported the Commonwealth	Depth, built on successful projects brings assurance we are a low-risk choice.
6.8 years: Average employee tenure of our Harrisburg team	We have solid experience. We bring current skills and motivated people who know how to get things done in the Commonwealth culture.
315+: Number of professional certifications held by our team	Skill demonstrated and substantiated by external sources — some teams say they have skill, we certify the presence of skill.
100%: Percentage of employees with ITIL V3 Foundations Certification that will work on the DCCS team.	Knowing technology is good; knowing how to control the application of technology is better. In fact, it is a key element necessary for success in this contract.

Steady State Staffing

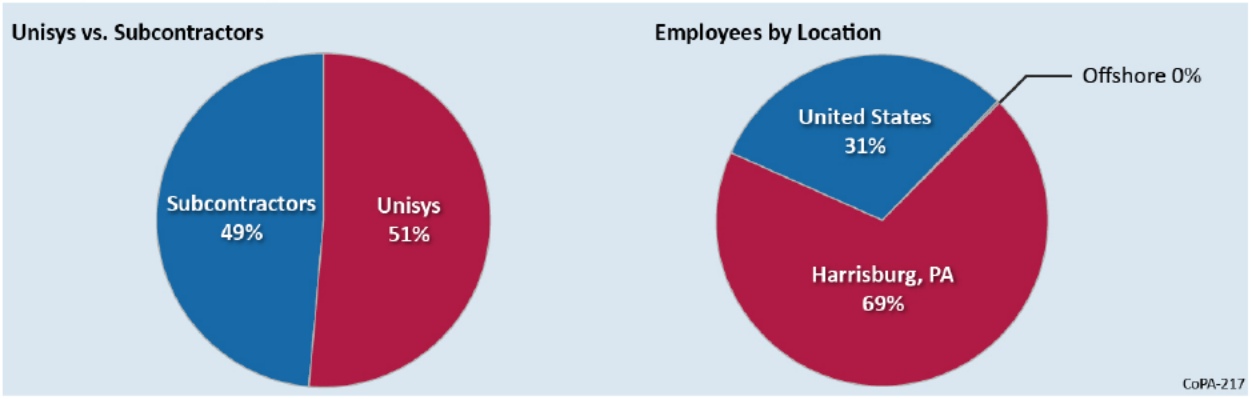


Figure 5-4. Steady State Staffing

5.5 Roles and Responsibility – High Level Steady State

Table 5-4 depicts staffing roles and quantities for each of the seven functional areas of the organization already discussed. This table also provides details on staffing type and quantity that will be provided by our subcontractors, including IBM, Deloitte, and our Small Diverse Business partners. The chart also indicates by staffing role the location of the team members. The Unisys Team will be staffed by a team located throughout the continental United States. Most of this team, including all management, will be located in Harrisburg.

Table 5-4. Staffing Roles and Responsibilities of Seven Functional Areas

Labor Category	Unisys	Subcontractors	Function	Hbg, PA	USA
	Staffing Numbers			Location	
Program Management Office (18)					
Engagement Executive	1		Management	1	
Project Executive (IBM)		1	Management	1	
Finance Manager	1	1	Finance	2	
Finance Analyst	2		Finance	1	1
Contract Manager	1	1	Contracts	2	
Contract Analyst	1	1	Contracts	2	
Subcontractor Manager	1		Third Party Management	1	
Third Party Software Mgt Analyst	2	4	Third Party Management	3	3
PMO Admin		1		1	
Agency Account Management (6)					
Agency Account Manager	5	1	Agency Management	6	

Labor Category	Unisys	Subcontractors	Function	Hbg, PA	USA
	Staffing Numbers			Location	
Service Delivery (203)					
Program Manager (SDE)	1		Management	1	
Service Delivery Manager	6	8	Management	14	
Data Center Manager	1		Facility Management	1	
Media Management		10	Facility Support		10
Space Planner	2		Facility Support		2
Onsite Data Center Supervisor	8		Facility Support	2	6
Automation Manager	1		Automation	1	
ITSM Support	4		Automation		4
ESM Support	9		Automation		9
System Admin – Backup	2	2	Backup and Restore	3	1
System Admin – Linux	13	9	Linux	18	4
System Adm – UIS Mainframe	2		Mainframe	2	
System Adm – IBM Mainframe		13	Mainframe/zLinux	8	5
Computer Operator	5	3	Mainframe	3	5
System Admin – AIX		22	AIX	12	10
System Admin – Network	9		Network	9	
System Admin – Security	1	2	Security	2	1
Service Desk Manager	1		Service Desk	1	
Service Desk Analyst	2		Service Desk	2	
Knowledge Manager	1		Service Desk	1	
Problem Manager	1		Service Desk	1	
Service Desk Agents	2	4	Service Desk	4	2
System Admin – Storage	5	10	Storage	12	3
System Admin – Windows	26	18	Windows	33	11
Service Excellence (26)					
Service Excellence Officer	1		Service Excellence Office	1	
Business Excellence Manager	1		Enterprise Compute Liaison	1	
ITIL Process Manager	4	1	ITIL Process	5	
ITIL Process Analyst	5	5	ITIL Process	8	2

Labor Category	Unisys	Subcontractors	Function	Hbg, PA	USA
	Staffing Numbers			Location	
Service Catalog Analyst	1	1	ITIL Process	1	1
SEO Reporting Analyst	2	2	Reporting	2	2
Technical Writer	2		CCPM and Documentation	2	
Customer Satisfaction Program Manager	1		Customer Satisfaction	1	
Enterprise Architecture (6)					
Senior Enterprise Infrastructure Architect	1		Management	1	
Agency Infrastructure Architect	3	2	Infrastructure Architect	5	
Transition Project Management (5)					
Transition Program Manager	1	1	Transition Management	2	
Steady State Project Manager	2		Project Management	2	
Trainer		1	Training	1	
Security (14)					
Info Security Manager	1		Security Management	1	
Security Analyst		4	Security	3	1
Security Specialist		1	Security	1	
Security Architect		1	Architecture	1	
IT Risk Manager	1	4	Audit/Continuity Management	3	1
DR Planner	1	1	DR Planning	2	

5.6 Roles and Responsibility – High Level Transition (includes Architect, Build)

Table 5-5 depicts the staffing roles and quantities required to support transition activity. Staffing numbers and their fluctuations greatly depend on the timing of each application's migration. During the Transition Planning phase with the Commonwealth, application migration schedules will be established and these numbers will be refined. Many of the staff members will initially join the project to support the transition before supporting the steady state operations. A base of project staff is included in **Table 5-5;** the technical staff is included in the Data Center Architecture stand-up.

Table 5-5. Staffing Roles—Transition Project Team

Labor Category	Quantity
Engagement Executive	1
Finance Manager	1
Finance Analyst	2
Contract Manager	1
Contract Analyst	1
Subcontractor Manager	1
Third Party Software Mgt Analyst	2
Agency Account Manager	5
Program Manager (SDE)	1
Service Delivery Manager	6
Data Center Manager	1
Space Planner	3
Onsite Data Center Supervisor	8
Automation Manager	1
ESM Support	1
System Admin – Backup	2
Service Excellence Officer	1
ITIL Process Manager	4
ITIL Process Analyst	6
SEO Reporting Analyst	1

Labor Category	Quantity
Customer Satisfaction Program Manager	1
Senior Enterprise Infrastructure Architect	1
Agency Infrastructure Architect	4
Transition Program Mgr	2
Project Mgr	6
Trainer	1
Info Security Manager	1
Security Analyst	10
Security Specialist	6
Security Architect	4
DR Planner	1
Data Gathering Architect	6
Business Excellence Manager	1
Transition Master Scheduler	1
Procurement Specialist	1
Communications Specialist	1
Physical Inventory Technician	5
Auxiliary Architect	3
TCIS Director	1
Technical Writer	12

Transition Staff Roles Included in Data Center Architecture Stand-up	
ITSM Support	System Admin – Security
System Admin – Linux	System Admin – Storage
System Adm – UIS Mainframe	System Admin – Windows
System Adm – IBM Mainframe	System Admin – Network
System Admin – AIX	

5.7 Agency Centric Staffing Approach

With our extensive experience supporting the Commonwealth through the DPH and the EDC, combined with a wealth of best practices experience from our national and global outsourcing practices, Unisys knows how to structure the organization that will best support Commonwealth agency needs. Unlike our competitors, we understand that each agency is a unique and distinct client of our compute services. Therefore, the key to success is putting the agency at our model's center. Our model allows the Commonwealth to realize savings from economy of scale without losing the personalized focus on the agencies that could be lost if a model aligned with technology domains were to be implemented. We give you the best of both worlds.

We understand that to an agency a particular compute component is more than just a server or a storage unit, and that outages to such devices can have a major impact to the functioning of an agency's application, and ultimately a negative effect on Commonwealth citizens. The alignment of our agency-centric model facilitates accountability at the agency and application level in contrast with many outsourcing providers that structure around technology components without regard for the customer and applications supported. In those models, you are just a number.

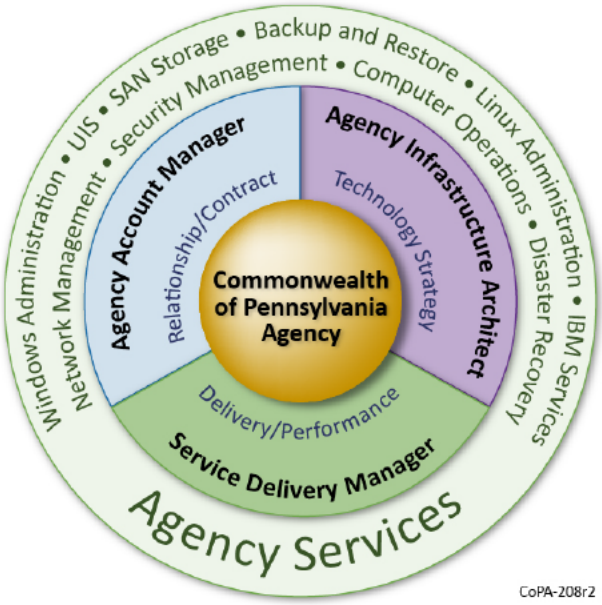
Our Staffing Plan proposes the use of six Service Delivery teams to cover the needs of all the in-scope agencies that will be supported under this contract. Each of the six teams will be directly responsible for providing services to a subset of these in-scope agencies. Determination of agencies to be aligned with each team will be accomplished by evaluating compute services required and the scope of work.

As depicted in **Figure 5-5**, each team has a dedicated management structure that includes an Agency Account Manager who manages the relationship with each agency supported and all aspects of the contract, an Agency Infrastructure Architect who manages the Technology Strategy for assigned agencies, and the Service Delivery Manager who is responsible for end-to-end delivery performance and directly oversees the management of all technicians aligned with the agencies supported by the team. The technical professionals managed by the Service Delivery Manager represent the technology disciplines necessary to provide comprehensive managed compute services to the Commonwealth.

Benefits of using this model include:

- Comprehensive accountability for availability and performance of Commonwealth application infrastructure supporting assigned agencies
- A single team with familiarity at an agency level to implement all projects associated with that agency
- Each team's realization of economy of scale through the support of approximately 1,800 systems per team
- The ability for Service Delivery Managers to leverage delivery resources across teams to cover peak activity.

Figure 5-5. Agency Centric Service Delivery Team Structure



Unisys also realizes there are benefits from a model that aligns staff with technology domains. To that end, we are creating a management role at the Service Excellence Office to function as a liaison between Service Delivery Managers supporting the Commonwealth, and the Unisys global technology domain leaders. This function enables the teams supporting Commonwealth agencies to have access to industry best practices and company standards developed within technology domains. This enables us to leverage supplemental resources throughout the United States that may be needed to support peak activity. This approach truly gives the Commonwealth the best of both worlds.

5.8 Interaction with the Commonwealth

Organized, frequent, and targeted communication is essential to the success of a program of this magnitude. Our team will be located mainly in Harrisburg, close to the locations of Commonwealth agencies that will be using the services to facilitate effective communication and collaboration.

Figure 5-6 provides a high-level graphical depiction of the flow of communication and interactions between our organizations. After working with the Commonwealth for many years, we understand that it is not as simple as one Unisys point of contact for a single Commonwealth counterpart. The Commonwealth organization is multidimensional; each agency has its own management structure and IT support team, and the Office of Administration manages the contract on behalf of the agencies.

In **Figure 5-6**, the Agency column represents the in-scope agencies and their unique roles and staff. Starting at the top, Executive Management level of the organization, the Unisys Engagement Executive who is accountable for the overall Commonwealth business relationship and the project's success interacts directly with agency Chief Information Officers (CIOs) and the CIO of the Office of Administration.

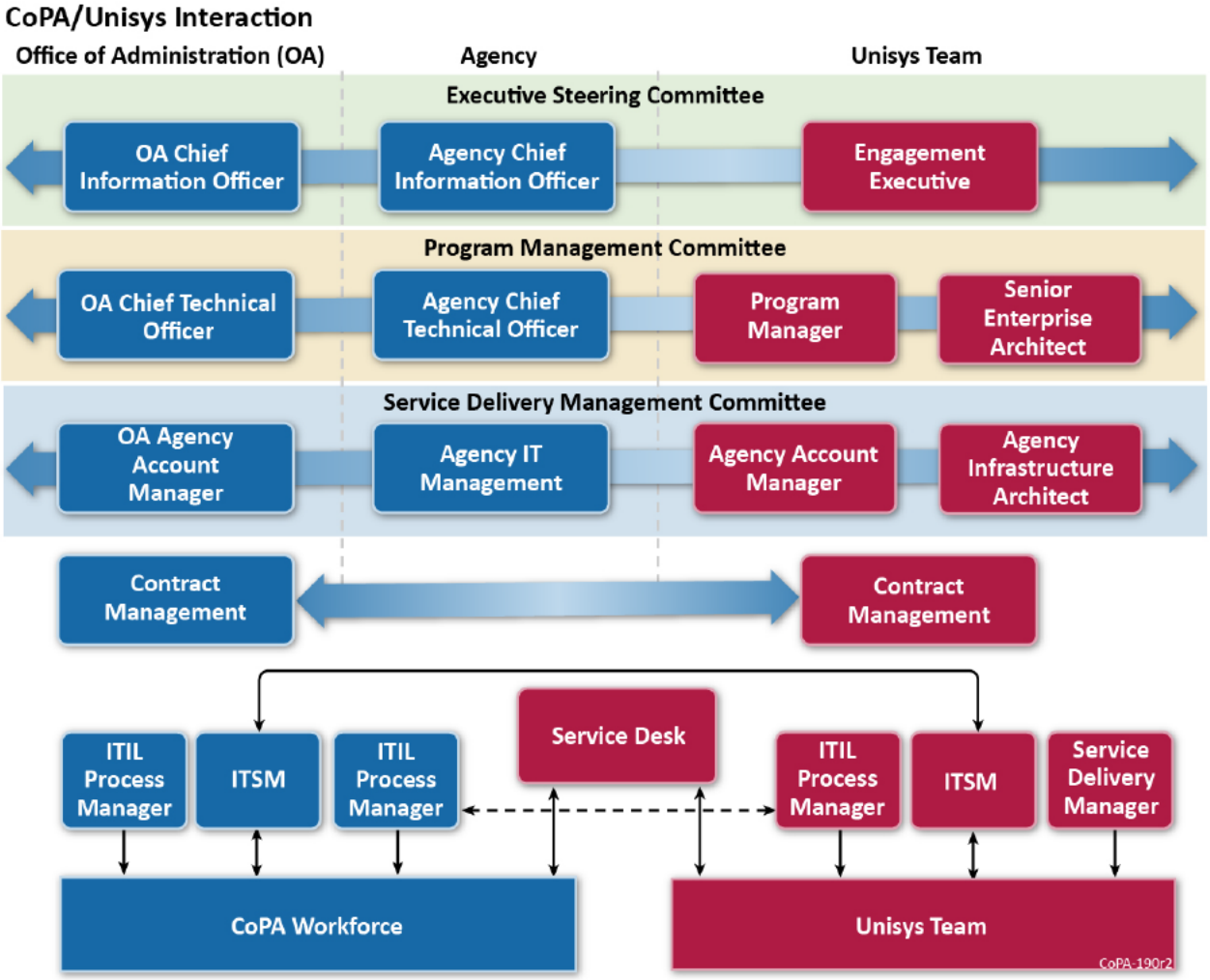


Figure 5-6. Interaction and Communication Flow Between Unisys and CoPA

Together, these individuals set the overall direction to steer the program, maintaining alignment with business objectives for each organization and monitoring the delivery of services to promote continued business value. This level of the organization comprises the Executive Steering Committee previously described in Schedule B, Governance.

At the Program Management level, the Unisys Program Manager and Agency Account Manager interact directly with the Chief Technology Officers and Technology Managers

from the agencies and the Office of Administration. These managers work together to provide the relationship's overall management and the program's delivery, enabling the program to be aligned with the objectives set forth by the Executive Steering Committee. This level of the organization comprises the Program Management Committee previously described in Schedule B, Governance.

At the service delivery level, the Unisys Agency Centric Management team consisting of our Agency Account Manager, our Agency Infrastructure Architect, and our Service Delivery Manager interacts directly with the agency IT management and the Office of Administration counterpart to the Agency Account Manager. This is the level responsible for management of all of the day-to-day delivery streams and confirming attainment of service delivery objectives. This team develops and implements continuous improvement initiatives together with the Service Excellence Office. This level of the organization comprises the Service Delivery Management Committee previously described in Schedule B, Governance.

This contract will be established between Unisys and the Commonwealth's Office of Administration. There will be strong interaction between Contract Management teams from both organizations, enabling communication to pass through the agency to keep it well informed of contractual concerns and changes.

In today's organization on the DPH contract, communication can flow to and from many directions, depending on the topic and the urgency. For the Compute Services contract, formalization and centralization of the flow of communication from the Commonwealth workforce to the Unisys Team through the Unisys Service Desk will greatly simplify interactions, documentation of requests, and tracking of issues in our connected ITSM systems. This quantum step forward will maintain ITIL process compliance with every request. Also, to further strengthen the effective use of communications channels, we are adding ITIL Process Managers who oversee and control key processes such as Change Management, Incident Management, and Service Request Management.

At the bottom of the interaction chart (the working level), the Commonwealth workforce has multiple options for communicating requests and reporting issues to the Unisys Team. They can call the Service Desk, which will receive requests from Commonwealth agencies, document them in the ITSM system, and assign requests to the Unisys Team. Alternatively, the Commonwealth Workforce can enter a request directly into the Commonwealth's ITSM system, and the request will be replicated in the Unisys ITSM system. The Service Desk monitors the queues and confirms that these requests are assigned to the Unisys Team.

Both of our organizations clearly see the benefits of aligning processes with ITIL best practices and made significant investments in the education of our teams. The Unisys process management team consists of key leaders and executives with advanced ITIL certification and education on Six Sigma methodologies. Our Process Managers will work directly with Commonwealth Process Managers to maintain compliance, proper documentation, timely approvals, and participation on joint Advisory Boards.

5.9 Transition Staffing Approach

As the incumbent vendor, Unisys has the singular ability to leverage our diverse, multidiscipline team already serving the Commonwealth in the Data PowerHouse (DPH) and Enterprise Data Center (EDC). We will leverage the talents of existing personnel with experience in supporting the compute needs of the Commonwealth's applications over the past 13 years.

Seeding the team with knowledgeable resources who understand the Commonwealth infrastructure will considerably reduce ramp-up time training staff on basic infrastructure support and each agency's priorities and nuances, enabling us to accelerate our focus on reforming our organizational structure to meet the new model's changing requirements. We will redeploy existing resources to the new contract as workload transitions out of the DPH and hire new Unisys resources as well as support the growth of our strategic partners and Small Diverse Businesses to provide the best complement of professionals and capabilities to the Commonwealth during transition and steady state.

A transition of this magnitude with its complexity and work effort requires extensive thought processes and adherence to the Unisys transition methodologies that have demonstrated proven success. As the incumbent, Unisys has the benefit of a large percentage of our staff already on the ground servicing the same workload that will be migrating to the new Compute Services model. A delicate balance must be maintained whereby staff from the current DPH contract is transitioned in a precise approach that upholds the imperative to provide outstanding service on the current DPH contract. We will work closely with the Commonwealth to verify all requirements of the current contract as well as a timely transition are achieved. The bottom line of our approach—having existing staff participate actively in planning the transition is a huge advantage and significantly reduces risk and project delays.

Our transition staffing approach consists of three main phases. During the first phase from Months 0 through 6, we will fully support the DPH and EDC while working to complete key deliverables before the migration of Data Center workload. The EDC will also transition to a Managed Services model during the first six months, and we will fully transition existing EDC staff to the new contract. During the second phase from Months 7 through 16, we will be migrating workloads from the DPH to the Unisys Data Center. At that time, we will fully transition existing DPH staff to the new contract. The third phase from Months 17 through 26 entails staffing changes to support the migration of outlying Agency Data Centers to the Unisys Data Center.

Figure 5-7 represents how staffing will be trending over time on both the new contract and the existing contract throughout the transition. The red line represents staffing decreasing on the current Computing Services Contract, and the blue line depicts staff increasing on the new contract as project phases progress.

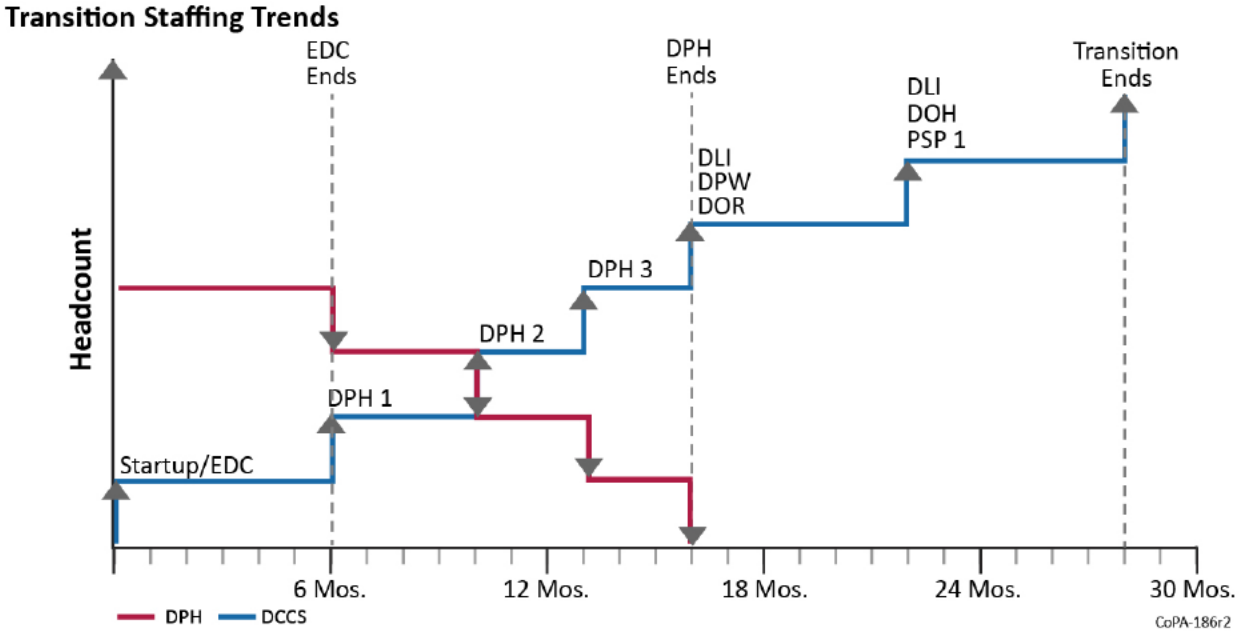


Figure 5-7. Transition Staffing Trends

Transition Phase 1. During Phase 1, we will be ramping up staff to support key deliverables that are prerequisite to workload migrations while maintaining the current quantity of staff on the DPH contract. At that time, we will be on-boarding key personnel who are not currently assigned to the DPH contract along with other personnel required to complete key deliverables. We will also bring on additional technical resources and orient them to Unisys processes and procedures as well as Commonwealth agencies and applications. At this time, we will begin to seed the team with members that are knowledgeable in Commonwealth agency compute environments and applications. The resources reallocated from the DPH contract will be backfilled by resources provided by our network of partners, including Small Diverse Businesses.

During Phase 1, we will establish the framework of our organization, standing up Facilities Management, the Service Excellence Office, the Enterprise Architecture function, and the Transition Project Management Office, and we will begin to restructure our PMO and Service Delivery teams. The EDC will also transition from the current staff augmentation model to a Managed Services model by the end of Month 6. The team of experienced resources working in the EDC will continue to work there and support the workload with further augmentation by additional staff required to effect the change to a managed services model.

Transition Phase 2. During Phase 2, we will be executing migrations of workload from the DPH agencies to the Unisys Data Center. Because agency applications will be moved in migration move packages or waves, you see resource allocation changing in a stair-step way. As agency applications are migrated from the DPH and relocated to the Unisys Data Center, the staff that supports the workload on the current contract will transition with the

work and then support the same application infrastructure under the new contract. As the incumbent, Unisys has the luxury of being able to transition support even at a server level to facilitate stability in Commonwealth services. This capability will be a huge benefit to the Commonwealth during this complex transition because a resource on our team could split time to effectively support his or her current workload regardless of location.

By month 16 at the end of Phase 2, all staff from the current DPH and EDC contracts will have seamlessly transitioned to the new Compute Services contract.

Transition Phase 3. During Phase 3, the outlying Agency Data Center workloads will be migrated to the Unisys Data Center. This is when the Commonwealth will really see the benefits of economy of scale. Unisys will continue to augment staff as workload increases throughout this phase. At this point, augmentation will solely involve the addition of technical staff because our management structure will have been fully established during Phase 2 and the transition. Transition Project Managers who facilitated the Phase 2 migrations will be redeployed to focus on Agency Data Center migrations.

The Commonwealth's participation in the transition process is critical to the project's success. We recommend that the Commonwealth name a counterpart to our Transition Program Manager and that Project Managers at the Commonwealth be aligned with Unisys Transition Project Managers to facilitate agency communication and data gathering to develop an effective plan to transition each agency. In addition to those resources, we recommend that IT staff at the agencies participate in sessions to share information about each application and its infrastructure and to identify agency priorities. We recommend that each agency assess and validate the transition approach proposed by Unisys, including the development and execution of test plans to confirm proper relocation of applications as the transition proceeds.

5.10 Key Personnel Table

The Unisys Team members who were identified to fill key personnel roles will be dedicated to performing that role on the account 100 percent of the time, as required in the RFP. We also plan to fill key personnel positions full time throughout the contract's duration, except for the second PMO Transition Manager that Schedule G clearly specifies. This key staff member will work on the project through the transition's duration. When the transition is complete, support for this key role will no longer be needed. All team members working as key personnel will provide services from the Unisys Harrisburg area office.

The individuals who will perform these functions are project's linchpins. Their performance in the assigned roles will be a determining factor in the program's success.

The key personnel are briefly introduced to you in **Table 5-6**, which is followed by a short summary of each of their responsibilities. Their resumes, including their qualifications for performing their respective roles, are included under the Key Resume tab in Section 5 of our proposal. Key personnel provided by our subcontractors are detailed in **Table 5-7** in Section 5.11.

Table 5-6. Key Personnel

Name	Proposed Account Role	Position in Organization	Experience in Proposed Role (Years)
Role on last 3 projects		**Qualifications for Proposed Role**	
[redacted]	Engagement Executive	Engagement Executive	15 years
• Unisys, DPH Engagement Executive (2 years) DPH Service Delivery Director (2 years) DPH Chief Technologist (1 year) • Cegedigm-Dendrite, Vice President, Technical Services (10 years) • Electronic Data Systems, Operations Manager (11 years)		• 15 years managing high-quality, large-scale outsourcing programs with extremely high SLA achievement and customer satisfaction • ITIL V3 Foundation Certified • Established Commonwealth leader with 5 years of experience managing the DPH contract, including the 2008 Transformation • 26 years managing programs with complex Data Center Services transitions, including data center facility design, consolidations, and physical and logical data center migrations • Laser focused on driving organizations to continually improve service level performance and customer satisfaction	
[redacted]	PMO Transition Manager 1	Transition Director	5 years
• Unisys, Transition Director (1 year) • Dell Services, Transition Management (1 year of responsibility for *all* healthcare transitions and 4 years as a consultant) • Electronic Data Systems, Client Delivery Executive (8 years)		• Provided stellar leadership managing four large-scale data center transitions, migrations, and system upgrades for Dell Services • Exceptional experience with managing accounts, project requirements, and building and leading technical teams • Certifications: ITIL V3 Foundation, Project Management Professional	
[redacted]	Program Manager (Service Delivery Executive)	Program Manager (Service Delivery Executive) as of July 1, 2013	14 Years
• Unisys, DPH Service Delivery Director, effective July 1, 2013 • CSC, Service Delivery Executive (14 years) • Powercom-2000, Global IT Manager (4 years)		• 28 years of experience in senior IT leadership roles, with specialization in large outsourcing engagements • Energetic leader adept at motivating large teams to accomplish goals in fast paced environments • Managed Service Delivery organizations of more than 400 employees through extensive data center consolidation and migration initiatives	

Name	Proposed Account Role	Position in Organization	Experience in Proposed Role (Years)
Role on last 3 projects		**Qualifications for Proposed Role**	
		• Solid track record of process re-engineering to achieve exceptional SLA performance and customer satisfaction • Great communicator with strong emphasis on customer executive relationships	
[redacted]	Service Excellence Officer	Director of Operations, North America	2 years
• Unisys, Operations Management for North America Global Managed Services organization (2 years) • Unisys, Account Process Optimization for DPH and the Commonwealth (2012) • Unisys, ITSM7 Transition Kaizen Workshop for DPH and the Commonwealth (2009)		• More than 30 years of experience in service delivery, with focus on operations, quality, service improvement, and finance • Demonstrated leadership in service excellence, with extensive training and experience in Six Sigma Lean (Black Belt), ITIL, Kaizen facilitation, project and program management • In-depth knowledge of the DPH project, account process, and ITSM7 • Certifications: Six Sigma Lean Black Belt, ITIL V3 Foundation (with ITIL Intermediate Practitioner Service Transition/Change Management certification in progress)	
[redacted]	Senior Enterprise Infrastructure Architect	North American Lead Architect	7 years
• Unisys, Lead Architect (2 years) • IBM, Transformation Integration Architect for the State of Georgia (2 years) • IBM, Transformation Integration Architect for Virgin Mobile (20 months)		• Demonstrated experience and success in leading a large team of architects to develop technical components (server, storage, network, security) to build a multitenant data center to support the State of Georgia's strategic and consolidation plans • Domain expertise in managed hosting services, capacity on demand, data center architecture, system architecture, servers, virtualization, security, and networking • Certifications: IBM IT architect (infrastructure), Open Group Master IT Architect, and ITIL V3 Foundation	
[redacted]	Incident Management Manager	Account Relationship and Service Delivery Manager	6 years
• Unisys, Account Relationship Manager		• More than 6 years of proven ability to direct and deliver new client implementations and steady state	

Name	Proposed Account Role	Position in Organization	Experience in Proposed Role (Years)
Role on last 3 projects		**Qualifications for Proposed Role**	
for a Microsoft Retail store environment (not permitted to name) (1 year) • Unisys, Account Relationship Manager for NEC/7-11 (2 years) • Unisys, Service Delivery Manager, General Growth Properties (2 years)		operations • Skills: Incident, change and problem management; SLA/KPI management; quality improvement program implementation and management; continuous improvement; and new process development and implementation • Training: ITIL V3, Six Sigma Lean Green Belt	
[redacted]	Change Manager	Service Delivery Manager	9 years
• Unisys, IT Service Delivery Manager at the DPH project (7.6 years) • Unisys, IT Resource and Asst. Technical Support Manager at the DPH project (1.6 years) • Endress+Hauser, Advanced Systems Group Manager and LAN Manager (2 years) • U.S. Air Force (22 years); encompassed several Change Management positions		• More than 30 years of IT experience • More than 9 years of experience on the DPH project, largely as a service delivery manager with deep knowledge of all service delivery processes, particularly change management • Proven change management expertise, having led process creation for 13 Commonwealth agencies, focusing on providing change management resource allocation performance reporting, capacity planning, contractual requirements, and incident reporting for data centers. • Demonstrated expertise in delivering advanced technical support to government agencies and meeting their technology needs by monitoring security, updating systems, and troubleshooting. • Certifications: ITIL V3 Foundation (with ITIL Intermediate Practitioner Service Transition/Change Management certification in progress)	
[redacted]	Change Analyst	Change Analyst	10 years
• Unisys, Data Center Analyst for the DPH project (10 years) • Unisys, Computer Operations Supervisor for the DPH project (4 years) • Lockheed Martin, Operations Manager (3 years)		• 27 years of experience providing data center analysis, change analysis, and support • Extensive experience with Remedy IT Services Management, with certifications in change management and resource tracking software • Certification: ITIL V3 Foundation	
[redacted]	Service Level Management Analyst	Service Level Management Analyst (as of July 2013)	11 years
• Unisys, Service Level Management		• 20 years of IT industry experience with primary focus	

Name	Proposed Account Role	Position in Organization	Experience in Proposed Role (Years)
Role on last 3 projects		**Qualifications for Proposed Role**	
Analyst, (as of July 2013) • Comcast, Data Center Services Manager and Data Center Management Tools Program Manager (6 years) • Yellow Book USA, Senior Data Center Operations Manager (11 years)		on data center services, tools and reporting • Built a comprehensive model for capacity metrics and consolidation reporting • Implemented executive reporting summarizing daily processing metrics and current problem status to provide complete transparency; • Defined and negotiated service-level agreements with customers and service partners to improve customer satisfaction	
[redacted]	Finance Manager	Financial Analysis Manager	25 years
• Unisys, Manager, Financial Analysis for the DPH project (14 years) • Unisys, Manager, Business Operations Data Center (7 years) • Unisys, Financial & Asset Control Government Systems (6 years)		• 14 years as a finance manager supporting the DPH project in Harrisburg • In-depth understanding of the DPH billing processes • Designed and implemented many process improvements for the DPH project • Recipient of Unisys Excellence Award • Certification: ITIL V3 Foundation	
[redacted]	Finance Analyst	Senior Project Controller and Financial Analyst	36 years
• Unisys, Project Controller and Financial Analyst for the DPH project (14 years) • AMP, Financial Analyst (2 years) • AMP, Pricing Accountant (14 years)		• 14 years as project controller and financial analyst supporting the DPH project in Harrisburg • Extensive experience with billing and accounts receivables • Supported the creation and improvement of consolidated billing process • Recipient of the Unisys Excellence Award and Silver Recognition Award for Unwavering Customer Commitment • Certification: ITIL V3 Foundation	
[redacted]	Lead Agency Account Manager	Project Manager and Client Service Manager	5 years
• Unisys, Project Manager and Client Service Manager, Pennsylvania Commonwealth Technology Center (5 years) • Unisys, Project Manager and Resource		• More than 10 years of experience working in project management and client service roles in the Commonwealth Technology Center • Proven project management and communications skills and a reputation for bringing commitment and	

Name	Proposed Account Role	Position in Organization	Experience in Proposed Role (Years)
Role on last 3 projects		**Qualifications for Proposed Role**	
Manager (6 years) • Unisys, Portfolio Sales Executive (5 years)		energy to each assignment • A unique blend of project management and sales experience and knowledge of the Commonwealth and its many leaders • Certifications: ITIL V3 Foundation, Project Management Professional	
[redacted]	Agency Account Manager	Service Delivery Manager	6 years
• Unisys, Service Delivery Manager and Operations Architect, Pennsylvania Commonwealth Technology Center (6 years) • Unisys, Operations Architect, Pennsylvania Commonwealth Technology Center (6 years) • Unisys, Team Leader, Pennsylvania Commonwealth Technology Center (2 years)		• More than 14 years at the Commonwealth's EDC ascending from a technical role in 1999 to the current position as Service Delivery Manager, a role that spans responsibilities for customer relations and satisfaction, technology consulting, operations, and account management. • An original member of the EDC and the center's Operations Architect for more than a decade; offers a very deep understanding of all aspects of the EDC and application hosting. • A very distinctive blend of technology, customer service, operations, and communications knowledge, skills, and experience. • Certifications: PMP, ITIL V3 and V2 Foundation, MCSA 2003, MCSE 2000	
[redacted]	Agency Account Manager	Account Business Management and Service Delivery Manager	7 years
• Unisys, DPH Account and Service Delivery Management (7 years) • Computer Aide, Senior Consultant (4 years) • IBM, Principal Consultant (5 years)		• IT Services professional with a demonstrated ability to help customers achieve their IT objectives • 7 years in account and service delivery management supporting the DPH project • Extensive knowledge of the DPH IT infrastructure, processes, deliverables, and personnel • Diverse IT background with proven expertise in consulting, technology, and business development • Education: M.S., Information Systems, Penn State University • Certifications: PMP and ITIL V3 Foundation	
[redacted]	Agency Account Manager	Service Delivery Project	14 years

Name	Proposed Account Role	Position in Organization	Experience in Proposed Role (Years)
Role on last 3 projects		Qualifications for Proposed Role	
[redacted]		Manager	
• Unisys, Service Delivery Manager (5 years) • Affiliated Computer Services, Account Manager, (9 years) • Foundation Health, Program Director (2 years)		• 5 years in account and service delivery management supporting the DPH project • In-depth knowledge of business and service needs for many agencies, including State Police, Department of Environmental Protection, Department of State, and Department of Health • Excellent interpersonal, customer service and general communication skills • Extensive project and program management experience • Certification: ITIL V3 Foundation	
[redacted]	Agency Infrastructure Architect	Client Architect	4 years
• Unisys, Client Architect at the DPH (4 years) • Cegedigm Dendrite, Technical Account Manager and Project Manager (3 years) • Dendrite International, Director of Hardware Services (2 years)		• More than 18 years in technical management and architect roles for government and commercial enterprises • In-depth knowledge of the DPH; worked as key member of the data center transformation project team to transition to a shared enterprise infrastructure model • Proven technical expertise, designing detailed technical data center solutions to support 17 Commonwealth agencies covering mainframe, server, storage, networking, software, and facility components • Strong record of success with data center architecture, management, and relocations • Certification: ITIL V3 Foundation	
[redacted]	Agency Infrastructure Architect	IT Manager	9 years
• Unisys, Manager, OA EDC (3 years) • Unisys, Deployment Consultant, OA EDC (6 years) • Citibank, Consultant (3 months) • Unisys, Consultant, Pennsylvania Department of Public Welfare (2 years)		• More than 14 years of IT experience • 9 years of service and technical excellence at the OA EDC • Proven expertise with TCP/IP Networking, DNS and Name Services; joining Active Directory domains; COM+ applications; IIS Web server and its configuration, administration, and troubleshooting; Access Control; Public Key Infrastructure; CA	

Name	Proposed Account Role	Position in Organization	Experience in Proposed Role (Years)
Role on last 3 projects		Qualifications for Proposed Role	
		SiteMinder; Virtual Directory (RadiantOne); VPN; and Portal Technologies • Broad experience implementing high availability solutions using CSS (Cisco Content Switches), Microsoft Windows Clustering, NLB, and Application Center; hands-on experience with designing and implementing Web publishing solutions using Microsoft ISA Server. • Certifications: CISSP, ITIL V3 Foundation, Windows MCSE	
[redacted]	Agency Infrastructure Architect	Systems Analyst and Project Leader	9 years
• Unisys, Systems Analyst and Project Leader, at the DPH (5 years) • Business Information Group, Network Engineering Consultant (1 year) • Rite Aid Corporation, Systems Administrator and Development (3 years)		• 5 years of experience as a systems analyst at the DPH managing regular upgrades, security enhancements, virtualization deployments, data center consolidations and migrations, and DR design • Through his ingenuity, has implemented a number of Windows and backup technology innovations to gain process efficiencies at the DPH • Expansive knowledge in the following areas: VMware vSphere ESX/ESXi 3.x, 4.x, & 5.x; Windows 2003, 2008, & 2012; Powershell & VB Script; Active Directory; Security Policies; IIS; DHCP; DNS; FTP; IBM Blade Center Servers; Dell and IBM x86 systems; Enterprise Backup/Replication & Disaster Recovery technologies, including Symantec NetBackup, EMC Data Domain, EMC Avamar, Microsoft Failover Clustering, Network Load Balancing, and Microsoft DFS & DFS-R • Certifications: VMware VCP4, VMware VCP5, Microsoft Windows 2008 MCITP: SA, Microsoft Windows 2008 MCA: Virtualization, MCSA: Windows 2012, and ITIL V3 Foundation	
[redacted]	Chief Information Security Officer	Senior Security Architect	4 years
• Unisys, Security Architect and effective Unisys CISO at the Pennsylvania State Police (4 years) • Unisys, Security Architect at the Michigan Department of Human		• 38 years of technical, business, and management experience in the IT and manufacturing automation industries • 6 years supporting the Commonwealth of Pennsylvania, including 4 acting as the Unisys CISO for PSP's CLEAN Services Project	

Name	Proposed Account Role	Position in Organization	Experience in Proposed Role (Years)
Role on last 3 projects		Qualifications for Proposed Role	
Services (2 years) • Unisys, Security Architect at the U.S. Department of Justice (1 year)		• Experienced with security policy and design, consulting, technology assessment, project management, automation, and distributed network architecture • Broad experience with overseeing large, complex projects to verify compliance with both security requirements and security policies and standards • Excellent technical, leadership, and communication skills • Certifications: CISSP (ISC2), GSEC (SANS/GIAC)	

5.11 Subcontractor Key Personnel Table

The Unisys Team subcontractor members who were identified to fill key personnel roles will be dedicated to performing those roles on the account 100 percent of the time with one exception to the benefit of the Commonwealth. The individual who serves as IBM Mainframe Agency Infrastructure Architect will do so on a 50 percent dedicated basis. Because minimal changes are required to the mainframe architecture, the role will be shared by another architect possessing extensive experience with IBM AIX and Windows platforms who also will serve in that role on a 50 percent dedicated basis. This will provide a better blend of skills to support the project's requirements.

Table 5-7. Subcontractor Key Personnel

Name	Proposed Account Role	Position in Organization	Experience in Proposed Role (Years)
Role on last 3 projects		Qualifications for Proposed Role	
[redacted]	PMO Transition Manager 2	Senior Project Manager	3 years
• IBM, DPH Service Delivery Manager (3 years) • IBM, IES Service Delivery Manager (5 years) • IBM, Network Support Project Leader at the Pennsylvania Department of Labor & Industry (7 years)		• Extensive experience in transition leadership, project management, IT infrastructure implementations and IT operations, and services management • Demonstrated performance in leading transition teams comprised of clients, subcontractors, and vendors for implementing data center operations services for mainframe and distributed technologies • More than 14 years of Commonwealth experience • Certifications: Cisco Certified Network Associate, ITIL V3 Foundation, Project Management Professional	

Name	Proposed Account Role	Position in Organization	Experience in Proposed Role (Years)
Role on last 3 projects		Qualifications for Proposed Role	
[redacted]	Availability Manager	Availability Manager	10 years
• IBM, Availability Manager for DPH (3 years) • IBM, Availability and Change Manager for IES (7 years) • IBM, Microsoft Exchange Administrator for Lucent Technologies (1 year)		• 10 years of experience supporting the Commonwealth availability and change process management roles • ITIL V3 Foundations Certification • Adept at process improvement, streamlining, and process control metrics • Team leader for the Remedy ITSM7 and ITIL process implementation	
[redacted]	Agency Account Manager	Service Delivery Manager	11 years
• IBM, Service Delivery Manager for DPH (11 years) • IBM, Disaster Recovery Coordinator Manager for DPH (3 years) • IBM, AS/400 Marketing Specialist (7 years)		• 14 years of service excellence on the DPH project • In-depth knowledge of business and service needs for many agencies, including the Department of Transportation, Department of Labor & Industry, and Department of Corrections • Proven communications skills and ability to build and manage teams • Demonstrated knowledge of IBM platforms and disaster recovery • Extensive experience in managing IT projects	
[redacted]	Agency Infrastructure Architect	Senior Certified IT Architect	17 years
• IBM, IT Architect for Unemployment Compensation Management System and Data Center for Pennsylvania Department of Labor & Industry • IBM, IT Architect for EDC at Commonwealth of Pennsylvania • IBM, IT Architect for Integrated Enterprise System (SAP) for Commonwealth of Pennsylvania		• More than 17 years of IT experience with the Commonwealth of Pennsylvania • More than 34 years of IT experience overall • Proven expertise with the design and implementation of complex infrastructure solutions, including the SAP and Unemployment Compensation infrastructure environments • Certifications: IBM Senior Certified Architect – Infrastructure; ITIL V3 Foundation	
[redacted]	Agency Infrastructure Architect 2	Senior IT Architect	14 years
• IBM, IT Architect, DPH (14 years) • IBM, Systems Engineer (13 years)		• 39 years of IT experience supporting the Commonwealth of Pennsylvania	

Name	Proposed Account Role	Position in Organization	Experience in Proposed Role (Years)
Role on last 3 projects		**Qualifications for Proposed Role**	
• IBM, Operating System Programmer (2 years)		• More than 14 years with the DPH, designing, implementing, and maintaining highly available data center systems and subsystems • Proven expertise in designing and implementing technology infrastructure for complex information systems, including large enterprise systems and mid-range systems	
[redacted]	Agency Infrastructure Architect	Infrastructure Data Center Technical Architect	15 years
• PCN, Solution Architect (5 years) • Business owner and software developer (2 years) • DHL Logistics, Manager IT Architecture (10 years)		• Senior architect with more than 15 years of experience in designing, building, consolidating, and managing data centers and infrastructure • Experience includes consolidating 25 data centers to centralized mega-data centers, building three new data centers, designing six SANs in six data centers, and developing multiple DR solutions • Demonstrated ability to work in a team environment, solid negotiator, quickly learn new data center technologies and embrace change; driven and dedicated person with a passion for information technologies and solutions • Certifications: ITIL, MCP, CheckPoint administration, project management	
[redacted]	IBM Project Executive	IBM Project Executive	15 years
• IBM Project Executive, Unisys DPH contract, Commonwealth of Pennsylvania (6 months) • IBM Deputy Project Executive, Unisys DPH contract, Commonwealth of Pennsylvania (5 years) • IBM Project Executive supporting multiple public sector clients to address governance and contract stabilization (18 months) • IBM Project Executive supporting the MTA New York City Transit Data Center Services contract (5 years)		• More than 30 years of experience in leadership positions at IBM, with the last 15 years focused mainly on providing data center services to multiple large computing service contracts in state and local government, healthcare, insurance, and telecommunications industries • Proven project executive skills and experience with a strong track record for delivery, innovation, and value • Certification: Project Management Professional	

Name	Proposed Account Role	Position in Organization	Experience in Proposed Role (Years)
Role on last 3 projects		Qualifications for Proposed Role	
[redacted]	IBM Delivery Project Executive	IBM Delivery Project Executive	10 years
• IBM Delivery Project Executive, Unisys DPH contract, Commonwealth of Pennsylvania (10 years) • IBM Sr. Delivery Manager/Delivery Project Executive responsible for high-quality delivery of Wintel, UNIX desktop support, UNIX and NT server services, and hardware maintenance for 700 servers and 5,000 end users for a large telecommunications customer (3 years) • IBM Service Delivery Manager managing services to multiple locations for a large telecommunications customer (3 years)		• More than 30 years of experience with IBM demonstrating leadership across a range of positions in quality control, engineering, and management delivering high-quality service and solutions to large IBM accounts • 10+ years of experience and expertise in leading teams to achieve consistent delivery results, providing leadership, experience, and innovation in working through solutions for the Commonwealth • Certification: ITIL V3 Foundation, Project Management Professional	

5.12 Organizational Function Discussion

This section describes the high-level functions performed by each of the seven workgroups. An organizational diagram is provided for each of the workgroups in our organization that depicts all of the functions as rectangular boxes with rounded corners. The role names and quantities of staff that provide that function are listed below each function box. Key personnel are listed in the workgroup and noted by names in red with a key to left of the name. Indentation of roles shows subordinate relationships to the positions above. At the top of each chart, you will see the executive leader and the staffing numbers required for that organization.

Figure 5-8 once again depicts the seven organizations with their basic function, noting key personnel in red. Each of those seven functions is detailed as the following pages.

Figure 5-8. Seven Organizations Staffing Requirements

Program Management Office (PMO)

The PMO serves as a central point of management for the overall program. The Program Management Office is led by the Engagement Executive, [redacted]. All executives responsible for the seven aspects of the program report directly to [redacted] Through the PMO, Unisys will manage continuous cross-organizational collaboration to achieve strategic business goals for the Commonwealth. The PMO organization serves to:

- Provide centralized and coordinated management of all initiatives and projects undertaken to support the data center compute services contract.
- Work in conjunction with Commonwealth leadership to establish a program governance structure.
- Focus on the coordinated planning, prioritization and execution of projects and subprojects that are tied to the Commonwealth's overall business objectives.
- Conduct activity ranging from providing supporting functions such as development of standardized policies and procedures to the direct management

responsibility for achieving business objectives through day-to-day service delivery.

- Act as an integral stakeholder and key decision-maker along with the Commonwealth during the initiation stage of each project/initiative.
- Coordinate effective use of resources and capacity management across all projects and contract activities.
- Provide central point of communication management across projects and throughout agencies.
- Enforce the use of best practices, process standards and project methodology.

Support for the Commonwealth far exceeds the boundaries of the team defined in Section 5. Unisys executives are committed to the Commonwealth's success all the way up to our Chief Executive Officer, [redacted], who serves as the Executive Sponsor for the Commonwealth of Pennsylvania. [redacted] reports directly to [redacted], Regional Vice President who has served the Commonwealth for the past 29 years building long-lasting executive relationships through 5 Commonwealth administrations. The Unisys Executive Leadership Committee discussed at the beginning of Section 5.0 provides far-reaching support for the Harrisburg-based team.

As shown in **Figure 5-9,** the PMO also has supporting staff responsible for the three major functions of Financial Management, Contract Management, and Vendor and Subcontractor Management.

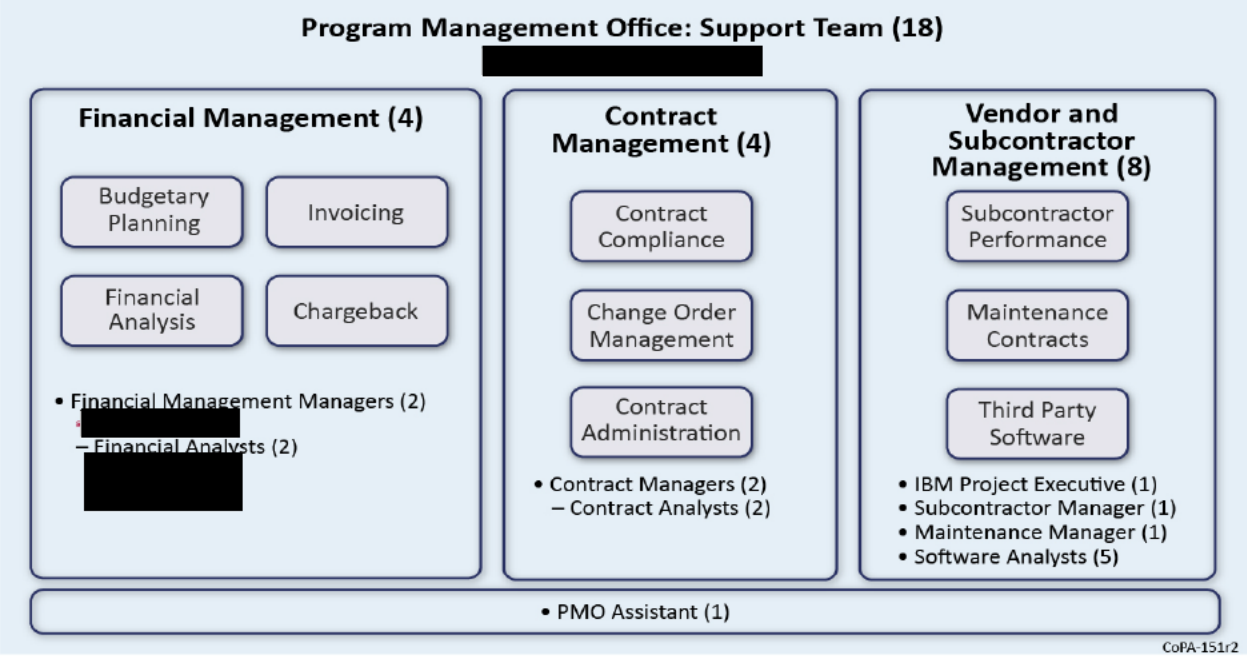


Figure 5-9. Project Management Office Duties and Staffing Requirements

Through the **Financial Management** function, the PMO provides accurate and cost-effective stewardship of IT assets and resources. The PMO plans, controls, and recovers costs expended in providing the services, offering a truly transparent analysis of the Commonwealth's spend on services. Areas of responsibility under Financial Management include:

- **Budgetary Planning:** this function works with the Commonwealth to identify major investments as part of the budgetary planning process.
- **Invoicing:** this function provides clear and transparent invoicing, both for the Commonwealth and for individual agencies, and verifies integrity and accountability of all invoices.
- **Financial Analysis:** this function analyzes efficiency that will be used to create intelligent, metric-based cost reduction strategies.
- **Chargeback**: this function confirms the accurate capture and provision of information on monthly volumes of work, counts, and utilization of specific infrastructure areas to provide the necessary transparency.

Through the **Contract Management** function, the PMO provides the governance and execution of the overall program, projects, and contract elements through its active working relationship with the Commonwealth project team. The Contract Management function provides ongoing direction and leadership supporting the contract and designated services for the contract's duration. Areas of responsibility under Contract Management include:

- **Contract Compliance:** this function confirms that the services provided comply with the requirements outlined by the contract.
- **Change Management:** this function oversees the change control process by which changes to services and approved schedules are requested, confirming that authorized personnel review and approve contract changes.
- **Contract Administration:** this function creates and maintains all contract and change documentation for the contract's duration, confirming that copies are appropriately provided to parties.

The PMO provides overall direction to the Unisys Team, holding subcontractors accountable for performance of services throughout the contract's term. Areas of responsibility under **Subcontractor Management** include:

- **Subcontractor Performance:** managing subcontractor performance is the responsibility of the prime provider of Commonwealth services, enabling high-quality value-added services to be provided and contractual commitments to be met.
- **Maintenance Contracts:** this function confirms that all hardware and software products used in providing the services to the Commonwealth have current and comprehensive maintenance contracts.

- **Third Party Software:** this function confirms accurate inventory and licensing compliance for all Unisys provided infrastructure software products.

The key personnel in the PMO introduced below include the **Engagement Executive,** [redacted]; the **Finance Manager,** [redacted], and the **Finance Analyst,** [redacted] Other key executives are introduced in the section, detailing their area of responsibility.

Engagement Executive Responsibilities and Introduction

- Overall responsibility and accountability for the Commonwealth business relationship and the engagement's success
- Works with Commonwealth executive leadership to set direction on the Unisys Team to meet strategic imperatives of the Commonwealth's executive leadership
- Serves as the primary contact for the management of the Compute Services Contract, assisting Commonwealth executives with all facets of services, promoting delivery of the highest customer service and satisfaction.

The Program Management Office will confirm that the Unisys Team meets all of our requirements for the new contract under the leadership of [redacted] **(based in Harrisburg)**, who has worked closely with Commonwealth executives to manage many aspects of the current DPH Program over the past 5 years. On joining Unisys, [redacted] oversaw the contract, managing commitments and expectations for the major transformation and infrastructure consolidation initiative with the contract's extension in 2008.

During her tenure with Unisys, [redacted] spearheaded a number of innovative technology solutions that reduced cost for the Commonwealth, including server virtualization and the implementation of a shared infrastructure strategy. She also fostered the evolution of the DPH architecture to new technology concepts, including disk-based backup solutions and flexible service offerings. [redacted] has also demonstrated vigilance in customer satisfaction by implementing a number of in-depth survey processes designed to take the customer's pulse at many different levels on all aspects of service. She has held the team accountable to document issues and follow-up actions in collaboration with the agencies. These activities significantly improved customer satisfaction across the board.

[redacted] has 26 years of experience with managing large-scale outsourcing contracts, leading teams of more than 500 staff members to achieve service excellence. She thoroughly **understands the Commonwealth's goals for the Data Center Computing Services engagement and has achieved success with managing similar consolidation and Data Center migration initiatives** as the Vice President, Technical Services at Cegedigm-Dendrite. During her 10 years at the company, [redacted] implemented global data center standards, attained the highest customer satisfaction ratings ever achieved, and grew the operation's scope by more than 900 percent

Under [redacted] direction, her team had many successes, including designing and building a world-class data center from the ground up, then migrating dozens of customers to the

center without disruption. **She provided a vision that led to the adoption of new technologies designed to reduce operational costs and provide customers with increased flexibility.** She established a winning culture and a team that always stepped up to the plate regardless of time pressures or the complexity of projects undertaken. Under her leadership, the reputation of the company's support services was dramatically enhanced.

Finance Manager Responsibilities and Introduction

- Works with Commonwealth financial counterparts to establish procedures to appropriately track funding streams as required by the Commonwealth to secure federal funding.
- Serves as the focal point for pricing of specialized contract changes that are procured outside the Service Catalog.
- Develops a consumption-based pricing model and chargeback mechanism to be deployed for the Commonwealth and develops transparent invoicing that meets Commonwealth needs.

Gary Hoopes will be serving the Commonwealth as the Finance Manager as the Data Center Services contract. He is a tenured Unisys employee who has held various financial management positions for more than 25 years, most recently the past 13 years as the Finance Manager on the Commonwealth of Pennsylvania DPH contract. Gary delivers financial management and billing oversight for several Unisys internal organizations and subcontractors.

Because of his experience with the Commonwealth, Gary has a clear understanding of the Commonwealth's financial processes and requirements for invoicing at the agency level and the tracking of federal funds against grants by project. He has supported restructuring of billing reports into a single Commonwealth invoice with agency-level detail. He is a motivated, conscientious, and diligent professional who takes a meticulous approach to the management of all aspects of finance, including development of financial plans, invoicing and billing activities, change order pricing and processing, and Service Level Agreement tracking.

Finance Analyst Responsibilities and Introduction

- Provides support to the Finance Manager to perform processes associated with documenting and submitting monthly invoicing.
- Develops specific fee schedules for Commonwealth change order processing.
- Responsible for Unisys Controller activities interacting with corporate financial organizations.

[redacted] will be serving the Commonwealth as a Financial Analyst on the Data Center Services contract. He has worked in a variety of financial and accounting roles over the past 30 years, with the past 13 years working for Unisys on the Commonwealth of Pennsylvania DPH contract as the Financial Analyst and Project Controller. In his current

role, [redacted] provides financial reporting and analysis for Unisys management, internal auditors, and external auditors and oversees a wide range of activities, including journal entries, internal billing, external billing, revenue recognition, cash collection, receivables, and asset database entries.

[redacted] has extensive experience with preparing amendments to Commonwealth agency fee schedules together with contract change orders. He developed internal processes to confirm the change order impacts agree with timing used in Commonwealth invoicing programs. [redacted] continually has an eye on process improvement and was recognized with Unisys Excellence and Silver Recognition Awards for his unwavering customer commitment.

Agency Account Management

Agency Account Management is the organization to which all Agency Account Managers report. These six managers serve the critical purpose of providing agencies with a single point of contact to the Unisys Team. These leaders are highly organized, resourceful, and adept at bringing the right resources together to meet customer needs. Each individual selected has extensive experience with managing customer relationships on outsourced data center services engagements with outstanding customer satisfaction.

Each of these team members (**Figure 5-10**) has supported the Commonwealth of Pennsylvania on various engagements for years, understands the importance of dedicated agency focus, and works to accomplish business objectives at the agency level. Their role is essential to confirming that agency leadership understands how to leverage the contract to their benefit, and these leaders act as the agency's advocate on the Unisys Team. Agency Account Management is led by Agency Account Manager, [redacted] who reports directly to [redacted]. The Agency Account Managers are responsible for the four major functions of Contract Liaison, Agency Advocate, Agency IT Planning Sessions, and Monthly Status Reporting. They all have achieved ITIL V3 Foundation certification, and most are PMP certified.

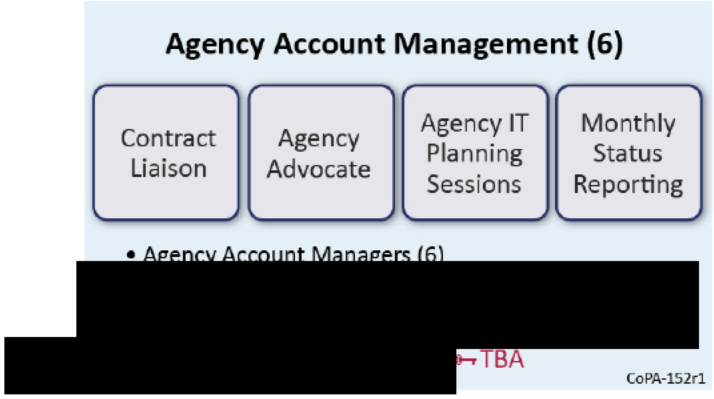


Figure 5-10. Agency Account Management Duties and Staffing Requirements

The **Contract Liaison** function owns the relationship at the agency level, acting as a liaison between agency information technology staff and the Unisys Team. Agency Account Managers are responsible for understanding all Unisys services and guiding the agencies in understanding how to leverage the contract to meet their Data Center needs. They maintain overall responsibility for sales, support, and operations, confirming that all parties finalize and sign agreements.

The **Agency Advocate** function confirms that the Unisys Team understands agencies' needs and requirements and advocates for agency and Commonwealth interests. This function provides the agencies with assistance needed to quickly navigate all facets of the Data Center Services support team.

The **Agency IT Planning Sessions** function, together with Enterprise Architecture, briefs the Commonwealth on new services and technology and is a key function of the agency's planning team.

The **Monthly Status Reporting** function keeps contacts at the agency informed of service level performance. This function meets monthly with the agencies to address problems and provide continuous service improvements. This function creates monthly operational summaries that will address all operational events and issues that occurred during the month that would have affected service level attainments, problems, incidents, and recommendations for changes needed to provide continuous, secure computing services.

The key personnel of the Agency Account Management team consist of five **Agency Account Managers** introduced below: [redacted]

Agency Account Managers' Responsibilities and Introductions

- Overall responsibility and accountability for the Commonwealth agency relationship and meeting agency commitments.
- Serve as the advocate for the agencies on the Unisys Team.
- Understand all of the services provided by the Unisys Team, guide the agencies, and understand their data center business needs.

[redacted] **(based in Harrisburg)** will serve the Commonwealth as an Agency Account Manager under the new contract. He is a 23-year Unisys employee who has worked for the Commonwealth of Pennsylvania since 2002 in a variety of project management and client services management roles supporting numerous Commonwealth organizations. Since 2005, he has worked on site at the Commonwealth Technology Center in very close collaboration with the CTO, CISO, Client Management, EDC, Enterprise Networking and Security, Enterprise Services, GIS, PMO, and many agencies.

[redacted] developed and introduced a customer satisfaction program for the EDC that continues today under the Enterprise Services as an important component of OIT's process for continuous improvement and building strategic relationships. Under this program, he

facilitated regular communications and acted as a liaison for OIT with the CIOs for half of the agencies, describing the center's managed services programs, facility services, and benefits.

Communications, customer service and satisfaction, facilitation, infrastructure, project and program management, and strategic relationship building are common threads for more than a decade working with the Commonwealth and more than 20 years working at Unisys.

[redacted] **(based in Harrisburg)** will serve the Commonwealth as an Agency Account Manager under the new contract. He is a 7-year Unisys employee who has worked for the Commonwealth of Pennsylvania for more than 15 years, providing technology solutions, consulting, and complex project management services. For the past 7 years, [redacted] has served the Commonwealth on the Unisys DPH contract in various Service Delivery and Business Management roles acting as a liaison to the Office of Administration and agencies receiving service.

[redacted] provided exceptional leadership to the DPH team through the alignment with ITIL best practices and the migration to the new ITSM Remedy system. With a service-centric approach, he directed the service delivery organization to support complex solution/design implementation, managed services functions, quality improvement, and cost management activities. He is skilled at contract management and managing vendors and subcontractors, ensuring shared accountability for outcomes.

[redacted] **(based in Harrisburg)** will serve the Commonwealth as an Agency Account Manager under the new contract. She has worked in the IT industry for 14 years and is a 5-year Unisys employee supporting the Commonwealth of Pennsylvania as a Service Delivery Manager on the DPH contract. [redacted] has worked with numerous Commonwealth agencies to develop strong partnerships with agency leadership while aligning Unisys service delivery teams with executing policies and procedures as outlined in the contract with a focus on agency priorities and outstanding customer service.

[redacted] adroitly oversees subcontractors to maintain top-notch service delivery across environments deployed at the DPH. She has managed numerous successful initiatives, including implementations of new systems for the Pennsylvania Liquor Control Board and the Department of Health, along with hardware upgrades for the Department of State. [redacted] is a superb communicator who keeps agency management informed of initiative statuses, and she received numerous accolades from Commonwealth management for her unwavering professionalism and skilled leadership.

[redacted] **(based in Harrisburg)** will serve the Commonwealth as an Agency Account Manager under the new contract. He has held a variety of IT leadership positions since joining IBM in 1976 and has worked with many Commonwealth agencies in the role of Service Delivery Manager for the past 12 years. He has a strong background and proven expertise in many IBM technologies, including zSeries and iSeries technical management, support of the Disaster Recovery process, and relationship management. [redacted] possesses

strong working knowledge of many Commonwealth agencies' business priorities, aligning cost-effective Data Center solutions to meet agency needs.

[redacted] has extensive experience with managing Commonwealth agencies through planning and smooth execution of system migrations and upgrades to new hardware and software product upgrades. He possesses superior knowledge of disaster recovery and business continuity planning demonstrated by creation of the disaster recovery plans supporting all IBM mainframe customers of the DPH and coordination of all disaster recovery tests. [redacted] is highly regarded as an expert in the field and for his knowledge of the Commonwealth, as evidenced by commendable ratings in customer satisfaction surveys during his tenure.

[redacted] **(based in Harrisburg)** will serve the Commonwealth as an Agency Account Manager under the new contract. He has more than 15 years of experience working in the IT industry and has supported the Commonwealth of Pennsylvania since 2000, holding positions of progressive responsibility, including his current role as the Service Delivery Manager at the Commonwealth's EDC. In this role, [redacted] actively collaborates with many Commonwealth agency IT managers to form technology solutions to address business needs with long-term operational strategies that enable real value to be delivered to the Commonwealth. He is well versed with the Commonwealth standards and ITBs and has personally contributed to developing a few of the ITBs.

[redacted] understands the importance of agency participation in major consolidation and migration projects because he played a large role in architecting the e-Government server farm for the Commonwealth to host Web applications for various agencies. On this project, [redacted] leveraged excellent leadership and communication skills to direct a team of technical consultants and to collaborate with more than 40 agencies in their successful application deployment and operation, functioning as a liaison, and moving ideas between the development community and the customer community to confirm the needs of the Commonwealth were represented in the server farm's design and delivery.

Service Delivery Management

Under the direction of the **Service Delivery Executive (Program Manager),** [redacted] who reports to [redacted], the Service Delivery team (**Figure 5-11**)is the heart of the Data Center Compute Services operation, providing all technology and service support functions required to fulfill the contract's service obligations. The six Agency Centric Service Delivery teams previously discussed reside in this organization. In addition to the Service Delivery teams, there are four centralized organizations supporting Facilities Management, Automation Services, IBM Services, and the Service Desk. The major functions of each of these teams are discussed below.

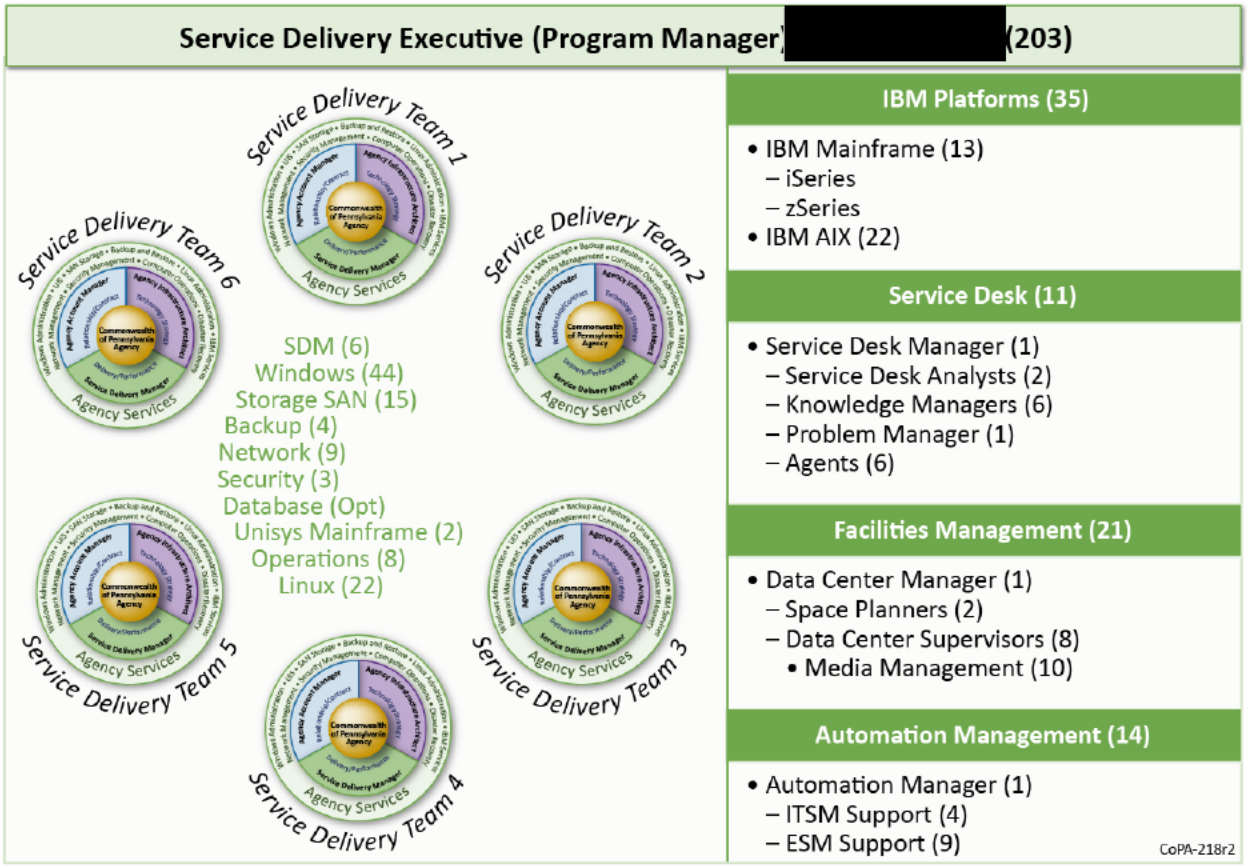


Figure 5-11. Service Delivery Team

We discuss the functions of each of the Service Delivery organizations, starting with cross-functional teams. The major functions of the **Facilities Management** team include Facility Management, Media Management, and Infrastructure Support.

Through the **Facility Management** function, all aspects of providing and managing the physical environment, including power and power distribution, cooling and ventilation, fire detection and suppression, building security and access control, and environmental monitoring, are provided.

The **Media Management** function provides a structured tape management approach for all systems that use tape backup services. This function manages and maintains the tape backup system and services, rotating designated tapes to and from approved off-site storage locations and tracking all tape movement on a detailed audit log.

The **Infrastructure Support** function provides a support team that is on site 24x7 in all of our data centers. This team is responsible for all aspects of data center support that require physical hands-on support in the data center. This team also

coordinates the escorting of vendors performing preventive maintenance tasks and remediating infrastructure components.

Automation Services is a key enabler to the successful implementation of the Commonwealth Data Center Services model. This function manages technologies that facilitate the transformation of resources to valuable services by exploiting the organization's capabilities and toolsets through the automation of repeatable tasks. Through automation, the Unisys Team expands our capabilities to consistently manage higher volumes of work with fewer restrictions than the use of human resources. The major functions of the Automation Services team include IT Service Management (ITSM)/Enterprise System Management (ESM) and Utility Product Support.

The **ITSM/ESM** function provides technology support for the ITSM system and the Enterprise System Management tools. This function configures and manages the ITSM system that serves as a common repository for all process requests supported on the Data Center Compute Services contract. This function also manages customization of ESM tools across all platforms to enable thousands of error messages and anomalous conditions to be trapped by automation and analyzed to prevent issues or escalate impact and notification to appropriate resolvers in real time.

The **Utility Product Support** function manages all other supporting automation products and tools. This function will customize and configure utility products such as the Reports Portal, the Executive Dashboard, the Service Catalog, and the Knowledge Management Portal.

The **IBM Services** team provides hosting and operational support services for platforms supported by our partner, IBM, including IBM zSeries Mainframe and zLinux, IBM iSeries, IBM pSeries, and their associated operating systems.

The **IBM Mainframe** function will support IBM zSeries mainframe systems with senior IBM mainframe engineers who have provided stability and seamless technology migrations to the z10 and z196 processors over the past 5 years. IBM provides our mainframe support on the z/OS and z/VSE platforms, giving us direct access to system programmers who wrote the operating system code and the hardware engineers who designed the hardware in the event of an impact.

The **IBM iSeries** function will support IBM iSeries midrange systems with senior level IBM midrange engineers with expertise on the i/OS platform provided by IBM. Our partner has managed this platform for the Department of Aging, the Department of Labor & Industry, the Civil Service Commission, and the Department of Insurance.

The **IBM pSeries and zLinux** function provides hosting and operational support services for all AIX and zLinux systems. This team is comprised of a blend of industry-certified resources from Unisys and IBM Global Services who possess a

wealth of in-depth platform knowledge and years of experience in supporting critical Commonwealth applications, including ERP systems that are hosted on behalf of the Integrated Enterprise System, the Department of Revenue, and the Pennsylvania Liquor Control Board. This team has a proven track record of success with implementing and migrating these critical environments to new data centers, upgrading hardware platforms, and maintaining a stable operating environment.

The **Database Management** team supports the optional managed database service that includes the database platform hardware and software as well as the ongoing database management administration services. This team is comprised of a mixture of resources from IBM Global Services, Unisys, and Deloitte who are well versed in Oracle, Microsoft SQL, IMS, Sybase, and DB2 database technologies.

The **Service Desk** team provides a central point of communication for all authorized Commonwealth agency staff to report incidents, requests for information, and service requests for all of the services provided in the Catalog of Services. This functional team also manages the Knowledge Management Portal, a central repository for processes and procedures, communications plans, and other documentation to be shared with the Commonwealth.

Six **Service Delivery Teams** are at the core of the Service Delivery organization. Each of the six teams provides end-to-end infrastructure management services to the subset of Commonwealth agencies they are assigned to support. This team is wholly accountable for maintaining application infrastructure availability for all applications needed to support the business of assigned agencies. Many functions are provided by the Service Delivery Team detailed below.

The **Computer Operations and Monitoring** function provides data center operations staff and management to operate and monitor the IT compute equipment and services being provided. This function leverages automated monitoring tools responding to anomalous conditions detected across all infrastructure components.

The **Batch Services** function delivers batch scheduling, execution, and monitoring services. Using a cross-platform system for automated scheduling of batch work and processes, this function processes scheduled batch jobs in the Commonwealth agency-defined windows to achieve maximum performance, enabling required batch completion times to be met.

The **Network Management** function maintains secure and robust, redundant network connections throughout the Data Center architecture. The Network Management team implements and maintains core switching infrastructure comprised of enterprise-level technology designed in a highly redundant configuration.

The **SAN/Storage Management** function provides hosting and operational support services for storage management systems in the data center, including maintaining

system maintenance at current support levels for optimal performance, recoverability, and secure operations.

The **Backup and Restore** functions conduct all system and data backup and restore processing, a key component of the IT Service Continuity Architecture and Plan. This function supports many different technologies that provide disk-based and tape-based backup approaches.

The **Unisys Mainframe** function will continue to be supported by senior Unisys engineers with more than 25 years supporting the Commonwealth systems with specialty in the OS 2200 and MCP operating systems. [redacted] and [redacted] have performed a number of technology refreshes and upgrades over the years, including the most recent migrations to Dorado and Libra technologies with the 2008 Data PowerHouse Transformation project.

The **Windows and Virtualization Platforms** function provides support for both physical and virtual servers across various hardware systems and versions of the Microsoft operating systems and support service software. The Unisys Team has supported virtual and physical Windows environments for the Commonwealth for several years on the DPH contract and implemented the Commonwealth virtualization strategy, using VMware and Microsoft Hyper-V technologies.

The **Linux Support** function provides hosting and operational support services for all Linux systems operating on an x86 platform.

The key personnel of the Service Delivery team include the Service Delivery Executive (Program Manager), [redacted], who reports directly to [redacted].

Service Delivery Executive (Program Manager) Responsibilities and Introduction

- Directly accountable for the success of all aspects and functions of the Service Delivery organization, enabling achievement of contracted Service Levels and meeting all obligations for deliverables under the contract.
- Guides and sets direction for delivery of service to centralized Service Delivery function managers and the six Service Delivery Managers who manage the agency-centric Service Delivery teams.
- Maintains relationships with agency and OA CTOs and actively participates in the Program Management Committee governing body that sets direction for services of the contract.
- Formally reports on the entire program's delivery performance each month.

[redacted] **(based in Harrisburg, PA)** will be serving the Commonwealth as the Service Delivery Executive (Program Manager) under the data center compute services contract. He will be joining the Unisys Team on July 1, 2013. He brings 14 years of experience leading several large Service Delivery organizations supporting outsourced engagements

for Computer Sciences Corporation (CSC). [redacted] will leverage his experience leading a number of large-scale data center delivery teams, including the Textron account where he directed the consolidation of 10 sites with multiple mainframes and over 800 open systems servers, and then managed an ongoing Service Delivery team of 500 employees.

[redacted] is a charismatic, service-driven leader who builds strong performing teams and a winning culture. He has specific management experience with all technologies in use by the Commonwealth. [redacted] has attained ITIL V3 Foundations certification and has a demonstrated track record of success with establishing process discipline and sound metrics that have facilitated performance improvements. For example, his attention to process discipline resulted in improving a 60%-70% SLA achievement to consistently realizing 99.5% or better in two separate major CSC clients in less than a year.

Service Excellence Office

Under the direction of [redacted], who reports to [redacted], the Service Excellence Office (SEO) oversees the execution and performance of the team against all ITIL operational processes with additional focus on continuous improvement and customer satisfaction for the Commonwealth. The SEO (**Figure 5-2**) will monitor and analyze each process in the Unisys service delivery model. The major functions of the SEO include ITIL Process Management, SEO Analysis, Technical Writing, Customer Satisfaction Program Management, and Continuous Improvement.

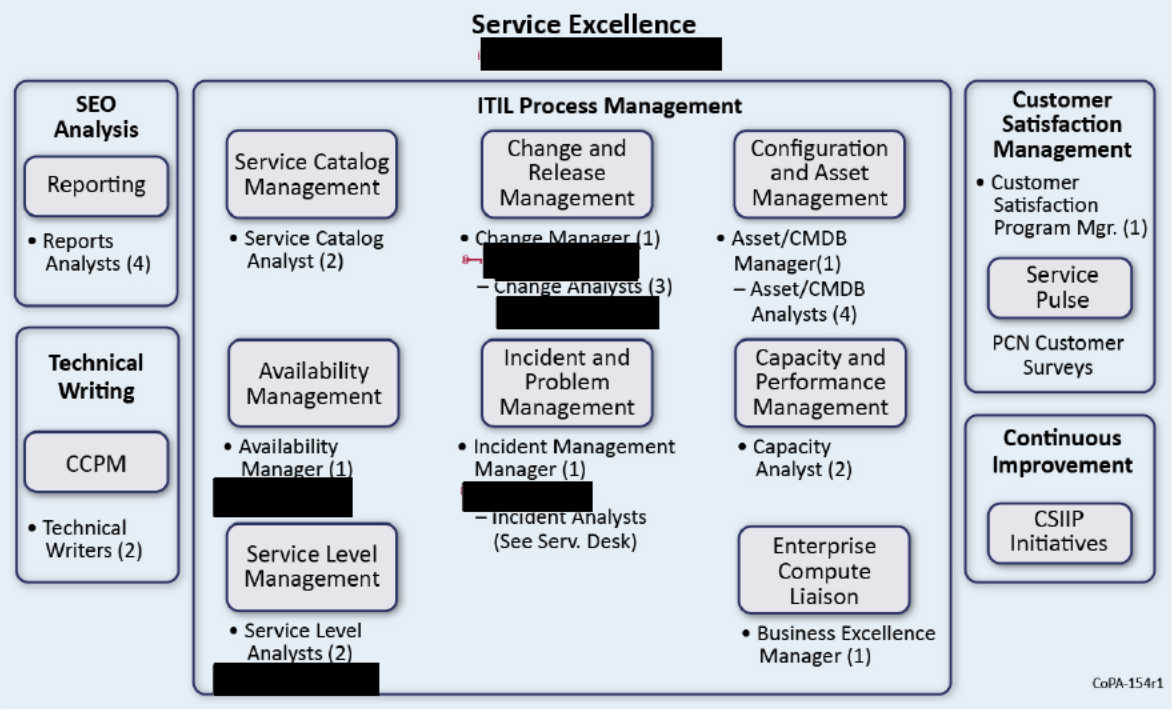


Figure 5-12. Service Excellence Office

The **ITIL Process Management** function is at the core of Service Excellence. This function effectively designs the management practices, processes, functions, roles, knowledge, and skills that the Unisys Team will use to enable us to deliver services that create value to the Commonwealth. Through IT Service Management, processes are developed and executed to facilitate the implementation and management of high-quality IT services that meet the Commonwealth's needs. This discipline is essential to confirm that we consistently produce high-quality services in a timely and cost-effective way. The processes managed by the SEO are listed below.

- **Service Request Management:** this function manages the service catalog containing all current service offerings and those that are planned to deploy soon. This function works closely with Enterprise Architecture to maintain currency of service catalog items and to proactively anticipate the Commonwealth's needs for future Service Catalog offerings.
- **Capacity/Performance Management:** this function conducts the infrastructure Capacity Management planning process to assist the Unisys Team and the Commonwealth in determining current and future capacity requirements, including the elements of hardware, software, environmental systems, and processes as well as the human resources required for successful delivery.
- **Change Management:** across this contract's life cycle phases, significant changes will be required to systems, processes, and infrastructure in response to changing business needs. This functional organization's purpose is to enable these changes to be performed to maximize the benefit to the Commonwealth while minimizing adverse impact on the services delivered.
- **Release Management:** this function is tightly coupled with Change Management. Release and deployment management is the function that delivers new functionality required while protecting the integrity of existing services.
- **Incident Management:** this function's purpose is to restore normal service operation as quickly as possible to minimize any adverse impact on business operations, maintaining agreed levels of service quality. This function defines and oversees the execution of the standardized methods and procedures used for efficient and prompt response, analysis, documentation, ongoing management, and reporting of incidents.
- **Problem Management:** this function focuses on preventing problems and resulting incidents, eliminating recurring incidents, and minimizing the impact of unavoidable incidents by diagnosing the root cause of problems, implementing resolutions with appropriate control processes, and making information on problems, resolutions, and workarounds available in a known error database.
- **Configuration/Asset Management:** this process enables the engagement's service assets (resources and capabilities) to be available and properly controlled, and that accurate, reliable information on the assets to be available when and where it is needed. This function manages every configuration item (including hardware, software, buildings, people, and formal documentation such as SLAs and process documentation) through its complete life cycle, using the CMDB as a repository.

- **Availability Management:** this function's purpose is to perform reactive activities (monitoring and analyzing incidents and events involving unavailability) as well as proactive activities (planning and designing) that improve the availability, reliability, maintainability, and serviceability of the infrastructure provided under this contract.
- **Service Level Management:** achievement of agreed targets for all current and planned services is this function's purpose. It defines, agrees, monitors, and reviews the level of services provided and initiates corrective measures when the service level falls below targeted levels. This function will work closely with Customer Satisfaction Management to improve the overall level of service to the Commonwealth.

The **SEO Analysis** function evaluates available information, placing it in the context of patterns and their implications. This function uses these patterns to give a high level of predictability and reliability on how the data will change over time. This function achieves the reporting of deliverable requirements across all ITIL process areas, technical areas, and the PMO.

The **Technical Writing** function creates and maintains the Commonwealth Computing Procedures Manual (CCPM) as well as all other Standard Operating Procedures (SOPs) and Work Instruction (WI) documentation.

The **Customer Satisfaction Management Program** consistently takes the organization's and customer's service pulse and commissions action plans as needed to improve customer satisfaction and exceed customer expectations.

The **Continuous Improvement** function provides proactive continuous improvement of all processes and functions of service delivery in the Continuous Service Improvement & Innovation Program (CSIIP) methodology.

The key personnel of the Service Excellence Office team include the Service Excellence Officer, [redacted]; the Change Manager, [redacted]; the Incident Management Manager, [redacted]; the Availability Manager, [redacted] **(IBM);** the Change Analyst, [redacted]; and the Service Level Management Analyst, [redacted].

Service Excellence Officer Responsibilities and Introduction

- Has overall responsibility for the quality management functions for the entire Data Center Services program.
- Sets the direction for implementing ITIL best practices throughout the organization to facilitate continuous service improvement programs.
- Is accountable for the creation and timely updates to the Commonwealth Computing Procedures Manual (CCPM) and verifying with the Service Delivery Executive that processes are executed with the discipline defined.

- Has direct responsibility for all ITIL Process Managers, CSIIP initiatives, the Customer Satisfaction Management Program, and all contractually required service level reporting.

[redacted] will serve the Commonwealth as the Service Excellence Officer under the new contract. He is a 32-year Unisys employee who has held a variety of Operations and Quality Management leadership roles supporting numerous Unisys and customer organizations. [redacted] achieved Six Sigma Lean Black Belt Certification and is well versed in Six Sigma and Lean quality principles. He is ITIL V3 2011 Foundation certified. Leveraging this background, [redacted] has facilitated numerous client business planning and continual service improvement workshops for Unisys key accounts. Through his leadership, many Unisys teams reengineered operational processes streamlining operations by 30 percent

[redacted] has conducted multiple Kaizen Process Optimization workshops with the Unisys Team supporting the Commonwealth of Pennsylvania. One of these workshops laid the groundwork to transition the DPH contract from an antiquated Remedy system to the current ITSM 7.6 Remedy system. [redacted] led the team in the identification of process gaps that needed to be addressed to align local processes with ITIL-aligned industry best practices. He will be leveraging an optimized approach refined from numerous past successes with continuous improvement and process management and confirm that metrics and controls are established, analyzed, improved, and maintained to drive Service Excellence and Continuous Improvement.

Change Manager Responsibilities and Introduction

- Sets the direction for the Change Management process for the entire program, enabling changes to be controlled to deliver early realization of benefits with minimum risk and adverse impact.
- Works with the Commonwealth to establish the change management and approval procedures that facilitate processing of requests for change in a formal way with change records that detail configuration items that are affected by the change, implementation procedures, and back out plans.
- Oversees change analysts, enforcing proper staff adherence to the Change Management procedures, including proper documentation in change records.
- Leads the Change Advisory Board (CAB) that is convened to support the authorization of changes and to assist in the assessment, prioritization, and scheduling of changes.

[redacted] **(based in Harrisburg)** will serve the Commonwealth as the Change Manager under the new contract. He is a thorough and results-oriented information technology professional with more than 30 years of experience in delivering advanced technical support to government agencies. [redacted] is a 9-year Unisys employee who has worked for the Commonwealth of Pennsylvania as a Service Delivery Manager on the DPH

contract. In this role, he has worked with numerous Commonwealth agencies, enabling data center needs and services to be met, including managing large-scale technology refresh projects, the capacity planning process, and all details of agency change and incident management processes.

[redacted] is well-known for his ability to achieve results and effectively manage projects as well as his process management diligence. His orientation to detail has effectively confirmed that Commonwealth changes are scheduled and executed by the most qualified resources wherever possible without incident. [redacted] has extensive experience with managing organizations through significant periods of change, including leading the DPH ERP implementations for the Integrated Enterprise System (IES) and the Department of Revenue (DOR).

Incident Management Manager Responsibilities and Introduction

- Sets the direction for the Incident Management process for the entire program, which manages the life cycle of all incidents focusing on restoration of normal service operation as quickly as possible and minimizing the adverse impact on business operations caused by an incident.
- Provides technical and operational escalations, management, and resolution by working with the Service Desk and Service Delivery to oversee escalations.
- Facilitates chronic issue management and resolution; provides resolutions and root cause analyses.
- Manages major incidents and oversees process activities for incident identification, logging and categorization.

[redacted] **(based in Harrisburg)** will serve the Commonwealth as the Incident Management Manager under the new contract. He is an 8-year Unisys employee who has contributed to a number of Unisys outsourcing engagements across multiple service lines, including data center services, managed service desks, and field services. [redacted] is a versatile, results-driven service delivery professional with a proven ability to develop strong client relationships, build teams, and deliver on commitments with a solid emphasis on quality and continuous improvement.

[redacted] has held a number of leadership and process management roles, including oversight of problem, incident, and change management processes for many Unisys clients supported in our multi-client service center in [redacted]. He also monitored and managed services as well as maintained consistent delivery to contracted service level agreements. [redacted] is well-versed in Six Sigma Lean Green Belt and ITIL V3 Foundation methodologies that he consistently applies in the performance of his duties. He will move to Harrisburg at the beginning of the data center services contract.

Availability Manager Responsibilities and Introduction

- Defines and manages the ongoing process of Availability Management covering the design, implementation, measurement, management, and improvement of IT service and component availability.
- Confirms that the level of availability delivered meets the Commonwealth's agreed availability needs in a cost-effective and timely way.
- Works closely with the Incident Management Manager, the Problem Manager, and the Capacity Manager to provide reliability, maintainability, serviceability, performance, and security of configurable items.

[redacted] **(based in Harrisburg)** will serve the Commonwealth as the Availability Manager under the new contract. He is a 13-year IBM employee who has worked in operational leadership roles, including Availability and Change Manager and Data Center Operations Team Lead. Over the past 10 years, [redacted] has served as an IBM Availability and Change Manager for the Commonwealth of Pennsylvania Data PowerHouse project, and for 7 years he managed Data Center Operations for the Commonwealth's Integrated Enterprise System.

[redacted] brings expertise in overseeing processes, including availability management, trend analysis, change control, project planning, implementation, and reporting. He is adept at evaluating processes and applying process improvements, as evidenced by his contributions during our recent implementation of ITIL process standards and the new Remedy ITSM tool. He is well regarded by the Commonwealth and the DPH team for his expertise in the process management area.

Change Analyst Responsibilities and Introduction

- Confirms that information documented on change records is comprehensive and that details such as configuration items affected, procedures for implementing the change, and back out if necessary are included.
- Acts as the steward of the process coordinating and confirming that all change records effectively move through the approval process according to established process timeframes.
- Works closely with the Unisys Team members who create and update change records and with change analysts from the Commonwealth that perform the same function for the Commonwealth workforce.

[redacted] **(based in Harrisburg)** will serve the Commonwealth as a Change Analyst under the new contract. She is a 30-year Unisys employee who has worked to support the Commonwealth for the past 16 years in operational leadership positions, including Change Manager, Help Desk Manager, and Agency Liaison to Data Center Operations.

In her role as Change Manager, [redacted] works with DPH technical teams to process more than 300 data center infrastructure changes per month on average, confirming that all change

requests include required information such as detailed tasks and back out plans. As a true leader, a collaborative approach comes naturally to her when working with the DPH team, and she is diligent in equipping team with process and ITSM product training to successfully execute the change management process.

Service Level Management Analyst Responsibilities and Introduction

- Confirms that all IT service management processes, operational level agreements, and underpinning contracts are appropriate for the agreed service level targets.
- Monitors and reports on service levels, holds regular service reviews with customers, and identifies required improvements.
- Acts as a point of regular contact and communication about service levels to the Commonwealth and Unisys Team managers of the organization.

[redacted] **(based in Harrisburg, PA)** will be serving the Commonwealth as a Service Level Management Analyst under the new contract. She has worked in the IT industry and specifically in large data centers for over 11 years, and will be joining Unisys in July 2013. [redacted] utilizes strong interpersonal skills and a keen attention to detail in order to successfully deliver high-quality, detailed analysis and reporting, which drive cost-effective, quality, IT solutions and continuous service improvement to her clients.

[redacted] has detailed knowledge of IT Service Management and in managing ITIL IT processes: service level management, change management, capacity management, and business continuity management. While working in the IT Industry, [redacted] responsibilities have included: building a comprehensive model for capacity metrics and consolidation reporting; implementing executive reporting summarizing daily processing metrics and current problem status to provide complete transparency; defining and negotiating service-level agreements with customers and service partners to improve customer satisfaction; and managing facility availability activities to 99.99% availability. [redacted] extensive experience, knowledge, and communication skills will confirm that SLAs are effectively managed, analyzed, and communicated to the Commonwealth.

Enterprise Architecture

The Enterprise Architecture organization (**Figure 5-43**) owns the development and management of the technology management program for the Data Center Services delivered. Unisys will establish and maintain this architecture office led by our Senior Enterprise Infrastructure Architect, [redacted] **(based in Harrisburg),** who reports to [redacted]. Reporting to [redacted] will be six dedicated Agency Infrastructure Architects. This organization has direct responsibility for the fulfillment of all architectural requirements of the program. The functions that fall under Enterprise Architecture include meeting Architectural Deliverables, Agency Infrastructure Architecture, Solution Delivery, Innovation Workshops, and Additional Planning Services.

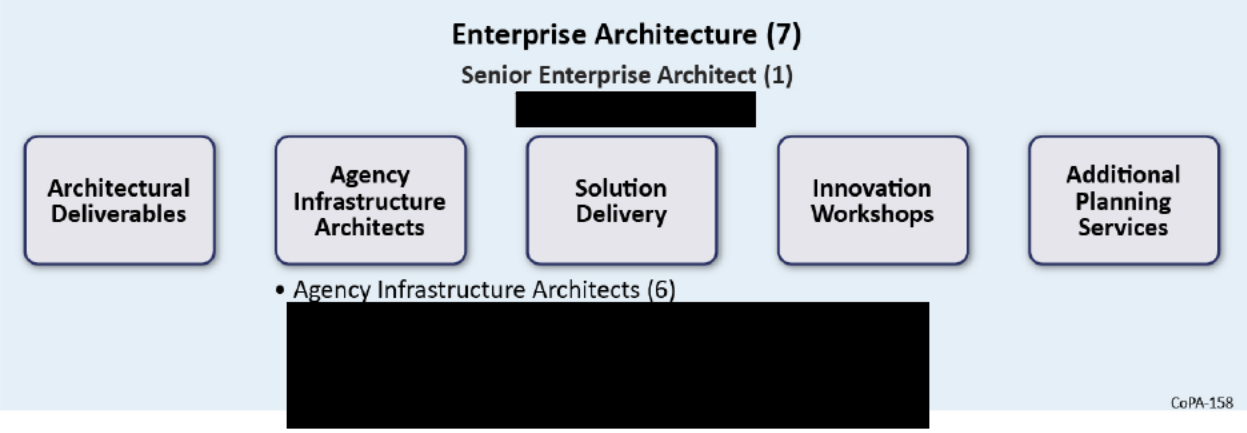


Figure 5-4. Enterprise Architecture Organization

This team is responsible for meeting **Architectural Deliverables,** including:

- **Data Center Architecture Plan and Roadmap,** which includes the 2+ Data Center Architecture, the Data Center Network Architecture, and the Data Center Security Architecture
- **Technology Architecture and Refresh Approach,** which addresses Data Center Technology Refresh and Infrastructure Architecture strategy.

Agency Infrastructure Architecture is comprised of technology architects who bring a wide set of skills and experience that collectively cross all platforms and technologies supported under the Data Center Compute Services contract. Several of our Agency Infrastructure Architects—including [redacted] have provided support to the Commonwealth for as long as 30 years. The architects are aligned with specific agencies and work hand in hand with the Agency Account Managers to enable agency technology needs to be fulfilled. They are responsible for the detailed design engineering of the Commonwealth's specific data center services, design quotes, and coordination of Commonwealth-related requests.

Solution Delivery is responsible for all aspects of the solution delivery, including conducting the requirements definition process with the agencies requesting service, developing a detailed technical solution, quantifying solution costs, and delivering a viable proposal to the Commonwealth within established time frames.

Innovation Workshops are essential to provide the opportunity for collaboration, technical information exchanges, and forums that will address issues, needs, and interests of the Commonwealth team. These Innovation Workshops are a key component of our overall continuous improvement program.

Additional Planning Services provide the Commonwealth with different or additional methods for requesting technical information and support. Depending on the type of request, those methods could include:

- Statement of Objectives (SOO)
- Work Orders
- Service Requests
- Request for Technical Analysis
  - Cost Benefit Analysis
  - Conceptualization
  - High Level Estimate (HLE)
- Technical Opinions.

The **key personnel** of the Enterprise Architecture team include the Senior Enterprise Infrastructure Architect, [redacted], and six Agency Infrastructure Architects, [redacted]

Senior Enterprise Infrastructure Architect Responsibilities and Introduction

- Has overall responsibility and accountability for the fulfillment of all architectural requirements of the contract.
- Works with Commonwealth technology leaders to set overall technology direction and strategy for the program.
- Confirms the engagement of an architecture team focused on agency technology needs that are balanced with the right technical expertise needed to meet the agency's needs.

[redacted] **(based in Harrisburg)** will serve the Commonwealth as the Senior Enterprise Architect under the new contract. He has 16 years of IT industry experience working for IBM in a number of architect roles before joining Unisys in 2011 as the Lead Client Architect managing the North American Client Architect team, which included overseeing the Client Architects supporting the Commonwealth. While working for IBM, [redacted] served as Transformation Integration Architect leading a large team of architects to develop technical components to build a multi-tenant data center to support the State of Georgia's strategic consolidation plans.

[redacted] has served in roles providing strategic technical advice to account directors and state agency CIOs and CISOs, developing consumption-based managed hosting service models, and developing business continuity system architectures to support recovery of critical business applications. Having supported numerous agencies for the State of Georgia, he is well versed on the importance of regulatory compliance and has led architecture teams to integrate federal regulatory guidelines and requirements into technology solutions. [redacted] is an accomplished technologist and excellent communicator who keeps stakeholders informed through a rigorous architecture review process and periodic technology briefings.

Agency Infrastructure Architect Responsibilities and Introductions

- Fully accountable for the end-to-end solution delivery process and the deliverables of all architecture-related requirements.
- Works with the Commonwealth through Innovation Workshops to keep agency leadership abreast of industry and technology trends.
- Provides additional planning services as needed by the Commonwealth to aid in its budgeting and technology planning processes.

[redacted] **(based in Harrisburg)** will serve the Commonwealth as one of our Agency Infrastructure Architects under the new contract. She has worked in various roles supporting the Commonwealth over the past 12 years, starting as a long-term consultant to the Department of Public Welfare providing network security expertise for the installation, configuration, and maintenance of the department's extranet. In her current role, [redacted] provides architecture services and manages the implementation teams supporting the secure integration of agency applications into the EDC.

[redacted] has worked with numerous agencies establishing positive customer relationships and confirming that solutions developed fulfill agency business needs. She has demonstrated superior knowledge across various data center technologies, including Windows server, virtualization, and network. She also attained CISSP certification acknowledging her expertise in security. [redacted] is a strong leader who has skillfully led her team through the implementation of several solutions over the 9 years she has worked in the EDC. This experience enables her to implement solutions that are well thought with successful implementation in mind.

[redacted] **(based in Harrisburg)** will serve the Commonwealth as one of our Agency Infrastructure Architects under the new contract. He has more than 18 years of experience in the IT industry working in data center technical management and architecture roles; for the past 4 years, he has worked as a Client Architect supporting the Commonwealth on the DPH contract. In his role at the DPH, [redacted] designed detailed technical data center solutions for 17 Commonwealth agencies across all technology platforms supported at the DPH.

[redacted] routinely provides guidance and recommendations to Commonwealth agencies on emerging technologies to increase performance, gain functionality, and reduce cost. He has a solid track record of developing highly accurate solutions that are subsequently implemented successfully because of his attention to detail. With a strong background in data center technical management, [redacted] understands the importance of having technical team members participate in the solution development and takes a collaborative approach to fostering accountability on the team, promoting a successful implementation.

[redacted] **(based in Harrisburg)** will serve the Commonwealth as one of our Agency Infrastructure Architects under the new contract. He has more than 39 years of experience in the information technology field supporting the Commonwealth in various positions

demonstrating superb skills in IBM mainframe technologies. [redacted] has supported the Commonwealth for 27 years, the past 14 years as an IT Architect on the DPH contract, and before that spending several years in various systems support roles at the Pennsylvania Department of Transportation.

Throughout his tenure on the DPH contract, [redacted] has continuously developed innovative solutions that improved the IBM mainframe platform performance and resiliency for agencies supported at the DPH. With the DPH transformation in 2008, he consolidated several disparate mainframe platforms onto a single z10 frame that exploited group capacity and sub-capacity software to allow the Commonwealth workloads to gain access to available MIPS beyond their allocated capacity and at the same time not exceeding software licensing limits. This innovation saved the Commonwealth millions of dollars by providing additional capacity to agencies experiencing extraordinary processing requirements for short periods.

[redacted] **(based in Harrisburg)** from our partner IBM will serve the Commonwealth as one of our Agency Infrastructure Architects under the new contract. [redacted] has more than 34 years of information technology experience and has been assigned to the IBM Commonwealth of Pennsylvania team since 1996, when she led the design and implementation of multiple complex IBM infrastructure solutions, including the SAP and Unemployment Compensation infrastructure environments.

[redacted] has supported Commonwealth agencies for the past 17 years, designing and implementing highly available IT systems and subsystems. Using a consultative approach, she works closely with agency IT technical and operations stakeholders to gather their requirements to develop systems management solutions that address needs of the business. Through her solutioning efforts, [redacted] has been instrumental in assisting the Commonwealth with the realization of goals to reduce the number of data centers and servers and to significantly increase server virtualization at the Commonwealth.

[redacted] **(based in Harrisburg)** from PCN will serve the Commonwealth as one of our Agency Infrastructure Architects under the new contract. [redacted] has worked on a variety of assignments crossing diverse technologies and industries, including government agencies and military contracts. He has performed as a Data Center Infrastructure Architect for large organizations for which he has focused on introducing emerging technologies and solutions to the company's vision and leveraging them to enhance capabilities and reduce cost.

Throughout his career, [redacted] has consolidated more than 25 data centers to centralized mega-data centers, built three new data centers, designed six SANs across six data centers, and developed multiple Disaster Recovery solutions including the use of SunGard as well as in house Disaster Recovery solutions using internal infrastructure and data centers. He is skilled in a broad spectrum of data center infrastructure technologies we will be using for the Commonwealth solution.

[redacted] **(based in Harrisburg)** will serve the Commonwealth as one of our Agency Infrastructure Architects under the new contract. He has worked for Unisys supporting many Commonwealth agencies in the DPH over the past 5 years. While at the DPH, [redacted] spearheaded several initiatives that advanced our architecture and support capabilities in Windows and backup technologies, including consolidation of the DPH NetBackup infrastructure that significantly reduced compute and media resources consumed by the backup process.

[redacted] has worked closely with many DPH agencies and took the lead in developing and executing the migration of the Integrated Enterprise Systems Windows platform to the DPH. [redacted] also determined a strategy for using the virtual infrastructure to replicate backup master servers to the disaster recovery site, expediting this component's recovery time from 2.5 hours to 30 minutes. He has consistently applied ingenuity and creativity to developing solutions that solve agency and DPH technology challenges.

Transition and Project Management Office

This office (**Figure 5-5**) is responsible for the deployment of a rigorous project management framework to be used to promote successful agency transitions, data center migrations, and steady state projects. Enabling all aspects of training to be managed consistently is the responsibility of the trainer on this team. Functions of this office include Transition Management, Steady State Project Management, and Training.

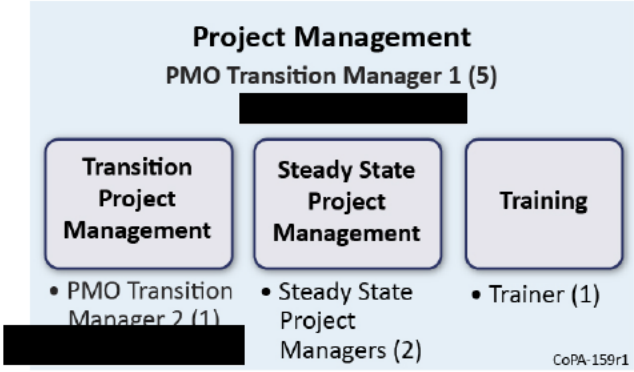


Figure 5-5. Transition and Project Management Office

On the steady state organization chart, there are two key positions for PMO Transition Manager based in Harrisburg. PMO transition Manager 1, [redacted], will lead all of the project management and transition efforts. PMO Transition Manager 2, [redacted] from IBM, will be filling the role of the second transition manager through to the end of transition, when he will be assigned to another service delivery role on the team.

The **Transition Management** function for the Commonwealth will be responsible for all aspects of delivering the transition, including milestones, communications, and the identification and assignment of transition resources. The Transition Managers will

represent the Unisys Team as the single point of contact for agencies supported during the transition, provide oversight and direction, and monitor the transition's overall status.

[redacted] were selected to lead the transition because they are results-driven Transition Managers with many years of experience in managing transitions, transformations, steady state programs, and turnaround initiatives. They are skilled communicators and are diligent about tracking and resolving issues as they arise. They are proficient at managing, designing, and delivering on long-term sustainable complex projects.

For this contract, we plan to have a dedicated **Steady State Project Management** function that confirms that changes to existing Data Center Services are managed using the same procedures and successful methodology used for transition. Having supported the Commonwealth on the DPH contract for the past 14 years, Unisys understands that agencies need to continue to enhance and modify their data center compute environments regularly for several reasons, including changes to legislation, adjusting to volume fluctuations, and refreshing antiquated technology. Two Project Managers will be dedicated for this function, and Unisys will leverage our North American Project Management Organization to support periods of peak activity.

PMO Transition Managers Responsibilities and Introductions

- Provides technical expertise and leadership during the transition of the current state data center services to steady state managed data center services.
- Provides continuing engineering support through the rest of the term for any future transition and transformation needs.
- Develops plans including detailed schedules for the implementation and transition of the Commonwealth from its current contract; obtaining approval and acceptance of the Transition Plan; and identifying the Transition Plan roles, responsibilities, and performance contingencies.

[redacted] **(based in Harrisburg)** will serve the Commonwealth as PMO Transition Manager 1 under the new contract. He brings 27 years of IT delivery experience working for large IT outsourcing firms before joining Unisys at the beginning of this year. As a Transition Management Consultant working for Dell Services/Perot Systems, [redacted] led four large-scale data center transitions, migrations, and system upgrades during his 5-year tenure.

[redacted] has achieved ITIL Foundations V3 and Project Management Professional certifications and applies the strengths of these methodologies to his approach to transition management. He has a long track record of success with building and leading technology teams on new business development initiatives and transformational programs for existing clients. [redacted] is a well-organized, communicative business professional who is proficient at establishing fruitful relationships with clients and Unisys technical teams to create synergistic transition support units.

[redacted] **(based in Harrisburg)** will serve the Commonwealth as PMO Transition Manager 2 under the new contract. He has spent more than 14 years on the IBM Commonwealth delivery team, gaining extensive experience in transition leadership, project management, IT infrastructure implementations, and IT operations and services management. [redacted] has held various leadership roles supporting the DPH, supporting the Integrated Enterprise System ERP contract, and as a project leader with the Department of Labor & Industry.

In October 2005, [redacted] led the transition of the Commonwealth's ERP systems from legacy providers to upgraded systems and network infrastructure on schedule and with no interruption to customer operations or applications. He has been successful on several similar large-scale transitions and projects by designing consistent transition plans with clear team member roles, responsibilities, and deliverables to enable every team member to understand his or her part of the transition. He understands that success relies on working together with the Commonwealth agencies to reach firm agreements on milestones and schedule.

Information Security

The Information Security organization (**Figure 5-6**) oversees all aspects of the project to confirm compliance with security standards and requirements. The main functions that fall under Information Security include IT Risk Management, Security Strategy, and Security Operations.

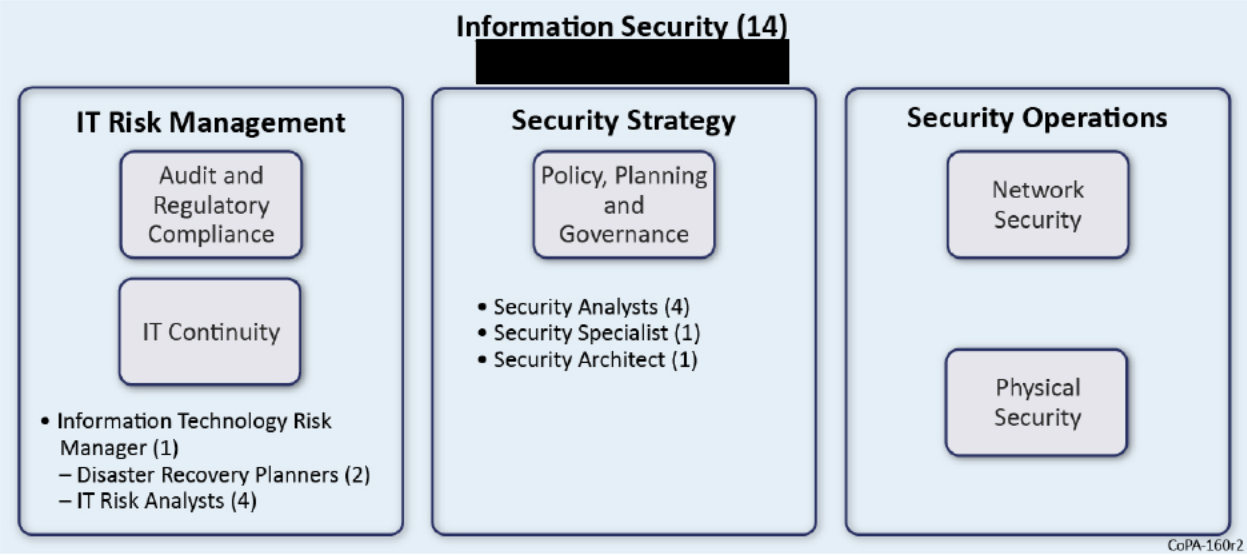


Figure 5-6. Information Security Organization

The **IT Risk Management** function leads efforts associated with continuity of IT business. This function also confirms that all required audits are conducted each year and that the Unisys Team participates as needed in Commonwealth audits.

The **Audit and Regulatory Compliance** function has full accountability for the Unisys Team's compliance with Commonwealth IT policies and directives as well as federal and Commonwealth laws, regulations, and policies. This function works with each agency to understand and confirms compliance with laws, regulations, and policies that pertain to each agency. The responsibility for conducting contractually required audits or arranging for participation in agency audits falls under this function.

The **IT Continuity** function is responsible for strategy and planning associated with continuity of the business as well as disaster recovery. This function leverages a disaster recovery planning tool that is shared with the Commonwealth to document disaster recovery and business continuity plans.

The **Security Strategy** function collaborates with Commonwealth agencies to develop the security plan and roadmap in collaboration with Commonwealth agencies. The **Security Policy, Planning and Governance** function will meet with the Commonwealth's Security teams (OA & agency) to participate in creating a comprehensive Security Program strategy.

The **Security Operations** function oversees all operational security functions including physical security and operational network security. The **Network Security** function provides hosting and operational support services for security products and firewalls at the data centers. The **Physical Security** function provides robust physical security, including biometric access control, video surveillance, and routine security officer patrols, protecting Commonwealth and vendor assets at all times.

The Unisys Information Security team is led by the Security Manager, [redacted], who reports directly to [redacted]. [redacted] is a results-oriented leader with more than 15 years of experience in supporting security product implementations and developing security strategy with Commonwealth CIOs.

Reporting to the Security Manager, [redacted] **IT Risk Manager** oversees all IT continuity functions that include business continuity planning and disaster recovery, including coordinating required staff and resources to execute regular Business Continuity and Disaster Recovery tests and improvements. [redacted] has worked in this role on the DPH contract for the past 4 years, identifying risk areas and establishing plans to mitigate them.

Security Manager Responsibilities and Introduction

- Oversees all aspects of the project to confirm compliance with all security standards and requirements.
- Oversees Network Security, Physical Security, and IT Risk Management operational areas.
- Confirms Commonwealth regulatory compliance on this engagement and leads client projects by developing workable plans, limiting risk, and managing resources.

[redacted] will serve the Commonwealth as the Security Manager under the new contract. He brings more than 38 years of senior technical and management experience, including 6 years with the Commonwealth covering security design, consulting, project management, technology assessment, automation, and distributed network architecture. [redacted] has specialized security expertise throughout a broad range of product sets, including identity management, identification and credentialing, access control, and confirming compliance with security standards.

[redacted] has worked with several federal and state agencies, including the Pennsylvania State Police, where he managed security for the new Commonwealth Law Enforcement Assistance Network (CLEAN) upgrade encompassing security policy; access control by CA SiteMinder; and integration with PSP's RSA Adaptive Authentication using a RadiantOne Virtual Directory Server (VDS) as the user repository. He also collaborated with JNET to most efficiently provide access to CLEAN by JNET users without requiring additional authentication and assisted Commonwealth leadership creating Security ITBs. [redacted] efforts enabled deployment of the new Megan's Law application to its full user base much faster than would have been achievable otherwise, enabling PSP to meet its legislatively mandated deadline.

5.13 HR Discussion

5.13.1 Staff Contingency Plan

RFP	*Requirement*
	The Offeror must provide a contingency plan that shows the ability to add more staff if needed to ensure meeting the Project's due date(s) and milestones as outlined in the Offeror's proposal.

As a global employer and service provider with the processes and capabilities that place the right people, in the right place, at the right time through its various recruiting and staffing functions, including Global Recruiting staff (external candidate sourcing) and Resource Management (internal sourcing), Unisys has the requisite processes in place to support contingent staffing models.

The Unisys dedicated Resource Management and Global Recruiting team's comprehensive staffing approach leverages effective forecasting tools (resource database by skills competencies used as a measure of available internal resources and as a prompt for external recruiting actions) to proactively address staffing needs, including key resources, dedicated and staff augmentation requirement staffing categories, duties and responsibilities, development and training, and succession planning to maximize sourcing for fully qualified staff availability as required throughout the engagement.

Sourcing is comprehensive and includes: evaluating current Unisys employees and service partner resources, using our global Resource Management and internal and external job posting systems; evaluating the current program employees and Unisys preapproved contractors for the engagement during the transition period; employee referrals; the Internet job boards; advertising; job fairs, and agency referrals.

Unisys developed a human resources staffing plan solution that is based on our understanding of the requirements provided. Our proposed contingency plan to address staffing risks includes the following key items:

- Early warning of staffing shortages through continuous review of the project plan to identify late completion of tasks
- Communicating staffing risks and impact to the Commonwealth project manager
- Establishing a standby labor pool of resources with appropriate skills to support the project
- Completing criminal background check for standby resources.

The Unisys contingency staffing approach leverages the use of our internal resources as well as those of our partners and staff augmentation firms. We have employees assigned at

our other U.S.-based data and service centers that can support short-term emergency client support requirements as needed. Our approach enables us to effectively respond to emergencies and special events, extreme weather conditions, and natural disasters, and IT continuity events.

Our Staffing Contingency Plan provides for the injection of additional resources to support transitions, emergencies, and staffing with specialty skills or any other effort in which additional support is required. Proactive planning from our program management leaders, resource management, and global recruiting teams shortens the time to fill by providing dedicated resources focused on the skills required for qualified delivery resource needs supporting the Commonwealth. Enhancing our focus on immediate response to the Commonwealth's needs is our approach to expediting required background investigations as described in the terms and conditions (Appendix A).

Important factors that augment our ability to effectively respond to staffing requirements are (1) keeping teaming partners informed of staffing requirements, (2) keeping ongoing contingency staffing vendors engaged, and (3) maintaining effective communication. This set of adaptable processes are used individually or in any combination to respond to the Commonwealth's staffing needs of varying durations, skills, certifications, and skill levels.

5.13.2 Staff Management

RFP	*Requirement*
	Describe internal standards, policies and procedures regarding hiring, professional development and human resource management.

Unisys is a global employer and service provider with the processes and capabilities that place the right people in the right places at the right time.

Recruiting and Hiring

The first step in the process, and one of the most important, is clearly defining the position's requirements. The detail and clarity of the requirements determine where we will source, and how we will screen and select the final candidates. Unisys uses a Targeted Selection methodology that defines the technical skills, experience, professional competencies, behavioral attributes required.

The Unisys sourcing process is comprehensive and includes:

- Evaluating current Unisys employees and contractors, using our global Resource Management and job posting systems for internal Unisys resources

- Assessing current employees and contractors of the client, service provider, or both for the engagement (if applicable) during the transition period
- Pursuing external candidates from employee referrals, the Internet, candidate sourcing, applicant market research, advertising, job fairs, and agencies.

The screening and selection processes involve our Targeted Selection methodology by evaluating the skills, competencies, and attributes of candidates against the requirements of the roles. We select the candidates, negotiate the salaries, and offer employment to the final candidate.

Internal Standards for Employee Selection

Unisys conducts background checks for all new hires as a condition of employment. Our standard checks include a criminal background check, employment verification, education verification and verification of the right to work in the United States. We accomplish all security procedures required by client service agreements. We also enforce Unisys policies and procedures for a drug-free workplace, security, and client and employee data protection during our recruiting and hiring process.

Professional Development

Professional certifications in the IT services industry demonstrate high standards and validated levels of expertise by the individuals who hold them. As a global service provider, Unisys establishes standards and requirements for our employees to earn, maintain, and add certifications when needed for supporting products and applications as well as for fields of knowledge and proficiency.

Unisys maintains technical and professional certifications and affiliations in many areas. We pursue employees with certifications such as ITIL, Six Sigma, Microsoft (MCSE and so forth), Dell, HP, Cisco, Nortel, Sun, IBM, SSPA, COPC, and HDI. We also pursue employees with technical certifications such as Dell, HP/Compaq, IBM, Unisys, and the industry standard recognized CompTIA A+ Certification.

When applicable, our technical resources attend at least 3 weeks of training a year, much of which leads to certifications. We strive for all Unisys technical resources to have at least one industry certification such as Microsoft MCP NT, Novell CNE, Nortel, Certified Unicenter Engineer (CUE), Microsoft Certified Systems Engineer (MCSE), and Cisco Certified Systems Engineer (CCNA).

Resource Management

Sound human resource management practices are based on mutual respect and trust, shared commitments and following through on them; recognition of each other's abilities and contributions to success, active support for career development, professional behavior, and an openness that invites an exchange of diverse ideas and approaches for delivering

customer and employee satisfaction. Successful working relationships depend on a work environment free from unlawful harassment or coercion.

Internal Standards of Behavior

To build and strengthen those working relationships and improve our chances of business success, we follow simple key practices that define the shared responsibilities between employees and managers:

- Preserve and enhance Unisys reputation
- Know the business and serve your client
- Set work objectives and keep plans on track
- Seek and give feedback and recognition
- Build capable teams
- Develop skills and coach one another
- Discuss accomplishments and rewards.

Getting our human resource management relationships right increases our ability to serve clients, develop the full potential of employees, and build our reputation. Those three elements are essential ingredients for company growth and delivery success to our clients.

5.13.3 Training Policies and Procedures

RFP	*Requirement*
	Describe Offeror's policies and processes for training and ongoing education of its personnel.

Policies and Plans

Unisys formed a partnership with Harrisburg University for Science and Technology (HU) to add real power to our training program. We previously worked together to support of the Government Technology Institute (GTI), which is a joint venture between HU and the Commonwealth that provides technology learning and innovation opportunities for the public sector. Unisys Executive leadership has delivered training and facilitated discussions designed to prepare Commonwealth leaders with information to make informed decisions on the most pertinent information technology challenges plaguing today's technology leaders.

All Unisys Team personnel are trained, competent, and skilled in the performance of their assigned tasks as required for effective performance in service delivery. We provide the Commonwealth with employee training plans, identifying both initial and recurring training. This plan includes any required program or Unisys mandatory training, role-

related technical certifications, and individual (self-directed) development to keep all personnel current in their areas of responsibility. The plan complies with all Privacy Act and other regulations governing personal and private information. All contractor personnel are trained, competent, and skilled in the performance of their assigned work required for effective performance in service support. Our flexible, proactive approach to training uses a variety of training methods.

Unisys created Unisys University (UU) as an internal education and training program. UU offers a range of training, technical certification, and professional development, including about 1,000 computer-based training applications and 2,500 instructor-led courses. UU's rich curriculum covers a variety of subjects, from program management to networking infrastructure and communications. We reimburse employees up to $5,000 a year to acquire career skills and certifications, such as Microsoft Certified Systems Engineer and Project Management Institute PMP, outside the UU network. Leveraging this capability further enhances the experience of our personnel who, in turn, increase their performance for service support to the Commonwealth.

Unisys and our service partners have similar programs to accomplish the goal of providing certified, trained staff that maintain service levels and meet deliverables.

Ongoing Education

Unisys developed a learning approach and methodology to ease the transition for Commonwealth staff from the current model to the new model. Our training approach brings employees substantial benefit that includes three basic pillars:

- Provides rapid access to procedural information relevant to the new contract
- Tailors curricula designed to address specific training needs of individual agency personnel
- Provides a roadmap for the Unisys Team to verify that the team supporting the Commonwealth's new contract is nurturing the skills and knowledge required to be successful from day one.

The Unisys Training program was designed with the following goals:

- Provide professionals who are certified in all aspects of infrastructure technologies supported for the Commonwealth with a subset of advance certifications achieved by the most senior team members
- Deliver annual training to enable our team to understand its responsibility to conduct Unisys business with integrity, to protect confidential information, and to follow security awareness best practices
- Enable 100 percent of the Unisys Team to obtain ITIL Foundation Certification with advanced ITIL certifications for members of the Service Excellence Office
- Provide training for all supporting staff on products and tools used in the data center environment

- Formalize transition preparation, quality assurance, debriefing, and compilation and communication of lessons learned
- Facilitate training on operational procedures and supporting products and tools designed to maintain process compliance.

Table 5-8 provides a high-level view of the training topics for Unisys and subcontractor personnel.

Table 5-8. Training Topics for Unisys and Subcontractor Personnel

Unisys Training Topic	High Level Curriculum Content
Ethics Awareness	Business ethics and public sector requirements
ITIL Process Training	ITIL Foundation certification for all employees, advanced certification for process managers, and detailed procedure training for all employees
Industry Technology and PMP Certifications	Vendor-provided curricula associated with staff technology certifications, as well as basic and advanced project management
Technology Product Training	Training in the installation, configuration, and use of all products and tools used to provide the services
Service Desk Agent Training	Service Desk orientation, operations, customer-specific requirements, and the Knowledge Management Portal
Security and PHI	Security policy awareness and employee responsibilities for protecting of confidential information
Transition Training	Orientation, planning, debriefings, lessons learned, and development of improvement plans

5.13.4 Staff Retention

RFP	Requirement
	Please describe Offeror's process and methodology for retaining Offeror personnel.

Unisys commits to comply with the terms and conditions that key personnel cannot be moved off the program without specific agreement from the Commonwealth on a suitable replacement. This provision enables the Commonwealth to have a solid staffing framework on which to depend to provide program stability and high performance.

Unisys strives to employ and promote the best-qualified person for each position for service delivery to the Commonwealth while valuing and promoting diversity in our workforce. We work hard to provide our employees with an environment that enhances their opportunity to achieve personal, professional, and financial well-being. We believe in providing opportunities that enable our employees to develop to their fullest potential, recognizing they play a key role in their own development. We encourage our employees to take advantage of all training opportunities available to them.

Unisys strives to align compensation to attract and retain individuals who are capable of exceptional performance, dedicated to supporting our company's strategic imperatives, and our delivery objectives to support of the Commonwealth. We maintain a performance-based compensation program. The components of compensation include base pay and depending on the position, short- and long-term incentives and recognition awards.

Hiring and retaining the talented, motivated people the Commonwealth expects requires a total compensation package that competes with those offered by our competitors. The Unisys performance management process includes our total rewards strategy to build a business environment that rewards employees for business and performance success and for the demonstration and development of skills and behaviors needed for effective service delivery to the Commonwealth and business success.

Unisys and our service delivery team employ programs that include a variety of retention incentives and frequent evaluations of employee performance. Because of our previous experience, we know that motivated employees have lower turnover rates and generate higher client satisfaction.

In 2012, the Unisys overall retention rate was 87 percent. This rate compares very favorably with other service providers in the IT Services industry evidencing similar rates. We employ competitive benefit and compensation programs, referral bonuses, extended effort pay, computer-based training, multiple career paths, mentoring, and leadership excellence acceleration programs. As demonstrated today, our excellent retention rate

helps us to minimize service interruption to the Commonwealth by avoiding unnecessary retraining of unskilled staff or constantly introducing new staff unfamiliar with the Commonwealth's agency environments.

Unisys also offers a program of comprehensive benefits including health insurance, income protection for illness, injury, and pregnancy; life insurance, short- and long-term disability insurance, holiday pay; vacation pay; a 401(k) plan, employee discount programs; and other programs that vary on our team.

Each year, Unisys formally evaluates performance of our staff members with a formal midyear review incorporating input gathered from managers, projects, and the Commonwealth. The interim review is structured to provide employees with a sense of how they are doing. Midyear ratings are on track or not on track. They are an overall check on progress against performance, education, and training goals. It is very important for managers to make employees aware of their performance level continually throughout the year. The timing of these reviews varies among team members.

Performance management is an ongoing cycle of planning, implementing, improving, evaluating, and rewarding performance—with continuous coaching and feedback from managers. Effective performance management begins with an understanding of established goals and their connection to individual contributions. Managers assist employees in planning their performance, education, and training by sharing their organizational goals and any role-specific performance expectations that underpin performance. Employees then create performance and education plans. The plans are then reviewed, edited if appropriate, and approved.

Throughout the year, performance and education plans are kept relevant through: (1) ongoing coaching and feedback, (2) performance improvement plans, (3) targeted performance improvement actions to elevate the contributions of low performers, (4) midyear performance discussions to gauge progress and update plans, and (5) project feedback.

As already discussed, the Unisys staffing model consists of a diverse, multi-disciplined team seeded with professionals experienced in supporting technology initiatives across all compute platforms used by the Commonwealth. Most of our team has specific experience with supporting the infrastructure needs of the Commonwealth's applications developed over the 14 years that Unisys has served the Commonwealth in the DPH. In the aggregate, our team accumulated more than 1,000 years of experience supporting infrastructure for many of the Commonwealth's 2,000 applications.

As the incumbent vendor, Unisys has the uncommon ability to leverage our diverse, multi-disciplined team already saving the Commonwealth in the Data PowerHouse and the Enterprise Data Center. We will leverage the talents of existing personnel with experience in supporting the infrastructure needs for the Commonwealth's applications over the past 13 years.

Seeding our team with knowledgeable resources who understand the Commonwealth infrastructure will considerably reduce ramp-up time to train staff on basic infrastructure support and each agency's priorities and, enabling us to accelerate our focus on reforming our organizational structure to meet the new model's changing requirements. We will redeploy existing resources to the new contract as workload transitions out of the DPH and hire as necessary from Unisys and our strategic partners to provide the Commonwealth with the best complement of professionals and capabilities during transition and steady state.

Just as we have over the past 50 years, our Pennsylvania-based team continues to be committed to your goals, and as your long-term partner, we look forward to taking this transitional journey with you that culminates in the realization of your innovative Computing Services vision.

UNISYS

[redacted]

Engagement Executive

Languages

English

Key Skills and Knowledge

Strong Leadership of Complex Organizations

Development of High Performance Teams

Project and Program Management of Large-scale Programs

Expert at Customer Satisfaction Management Developing and Leading Programs

Data Center Migration and Consolidation of Large Scale Implementations

Data Center Facilities Design and Management of Tier 3+ Infrastructures

Data Center and Help Desk Service Management

Quality Improvement Program Implementation and Management

Process and Organizational Reengineering

ERP System Solutions and Migrations

Communications

Incident Management

Business Continuity and Disaster Recovery

Creation of Training Programs

Skills Summary

A dynamic accomplished Program Manager with five years of Commonwealth experience; passionate about service delivery, successful customer relationships, development of high performance operations, and complex project management. Strong track record of reinventing fast-paced organizations and managing them through significant periods of growth and change. Adept at managing financials, quality improvement programs, technology consulting, strategic planning, and performance metrics; well respected by peers and subordinates, sought out by senior vice presidents for the 'tough jobs'.

Employment History and Related Experience

Unisys Client Account Executive

Public Sector, Commonwealth of Pennsylvania 2008 – Present

Client Account Executive, Service Delivery Director and Chief Technologist for the Data PowerHouse (DPH)hosting services contract (based in Harrisburg PA) for the Commonwealth of Pennsylvania's most mission-critical applications since 2008. Delivered full time support for this contract managing client relationships and ensured contract compliance; successfully restructured management of this key program resulting in the highest customer satisfaction levels and Service Level Agreement (SLA) performance in the history of the program.

> [redacted] *goes without saying…but I'll say it anyway…you are doing an excellent job leading: highly communicative, client focused, results driven";*
>
> Bill Bancroft, VP and General Manager, Unisys Global Managed Services

Transformation Solution and Project Management

As Chief Technologist, validated an extensive and highly complicated technology solution, engaged with the Program Management Office supporting the oversight of contract managing commitments, requirements, and expectations; and provided management sponsorship for major transformation and infrastructure consolidation initiative with the contract extension in 2008.

Innovative Service Offering Implementations

Since 2008, spearheaded a number of innovative technology solutions that resulted in cost savings for the Commonwealth of Pennsylvania including server virtualization and the implementation of a shared infrastructure strategy with the 2008 transformation; fostered the evolution of the Data PowerHouse architecture to newer technology concepts including disk-based backup solutions and flexible service offerings.

Worked with subcontractor and Commonwealth leadership to develop an innovative strategy to control unplanned growth and contain cost for IBM mainframe environments; engaged the Program Management Office (PMO) in daily oversight of the effort to contain cost through careful analysis of progress reports, schedule, quality reports, and budget. The implementation of a technology platform upgrade resulted in savings for software licensing costs and creative redeployment of a business class processor. Relocating the Department of Corrections to the business class processor provided remaining mainframe agencies with much-needed capacity to grow their environments. The overall strategy saved the Commonwealth millions of dollars by negating the need for an unplanned capacity upgrade on the mainframe platform.

ERP System Environment Hosting and Migration

Developed the technology solution required to support the Oracle ERP system environment for the Pennsylvania Liquor Control Board, and oversaw the migration of the Oracle ERP system environments from the Northwest Office Building into the Data PowerHouse in 2008. Tracked ERP deliverables; confirmed our team met the project commitments, contract requirements, and customer expectations. The solution provided a solid platform on current technology deployed in a high availability configuration hosted in the hardened Data PowerHouse facility increasing the reliability of the infrastructure supporting this critical Commonwealth business.

Managed the SAP Integrated Enterprise System implementation of a disk to disk backup solution, proactively addressed problems with rapidly growing data requirements, and resolved the massive Commonwealth data backup process that involved as many as 34 tape volumes over several hours. Mitigated the risk associated with reliability of tape media through the implementation of a disk to disk backup configuration. This configuration now supports backup of nearly twice the amount of data than

previously backed up under the tape solution in little more than three hours.

Customer Satisfaction Programs

Developed Customer Service Programs tailored to meet agency needs. Revamped the annual Agency Survey to elicit actionable feedback; shared feedback across the Commonwealth with every Commonwealth Agency; instituted an intensive Service Assessment Process that included a detailed written survey, follow-up analysis, agency interview, and Action Plan to address satisfaction issues. Managed relationship with the Commonwealth, established commitments, requirements, expectations for the Service Assessment process, tracked the required survey deliverables – confirmed that survey events occurred on schedule. Changes to Customer Satisfaction Programs have resulted in higher levels of agency satisfaction through better methods of communication and follow-up on issues impacting the agencies.

Quality Improvement Initiatives

Led the assessment and reengineering of security practices and procedures resulting in achievement of ISO 27001 certification in 2009. Recognizing the importance of alignment to ITIL best practices and completed an initiative to obtain ITIL V3 2011 Foundations certification for all team members supporting the Commonwealth of Pennsylvania. Invested in upgraded Remedy ITSM 7.6 platform with new modules and adopted Unisys global standard processes that facilitate our process alignment to ITIL best practices.

Non-Unisys Project Experience

Dendrite International (Cegedim), Vice President of Technical Services 1996 – 2006

Founded in 1986, Dendrite International now known as Cegedim provides diversified sales, marketing, clinical and compliance solutions to the global life sciences and pharmaceutical industry. As the Vice President of Technical Services and Corporate Officer, leveraged detailed understanding of billing formats, hierarchies, credits, and business structure to strengthen the logistics operations process. Defined organizational standards, Service Levels structure, credits, and service metrics for all outsourced service management organizations including Data Center, Technical Customer Service Center, and Hardware Break fix Logistics Operation providing exceptional service through a staff of more than 500 technicians.

> The Cegedim Chief Technology Officer reported:
>
> *"Ann is an exceptional technology leader. She and her team had many successes including: building a world-class Data Center from the ground up and then migrating dozens of our customers to the center with zero disruption; rapidly expanding our Virginia technical support center supporting thousands of pharmaceutical sales reps; adopting new technologies designed to reduce cost, improve margins and provide our customers with increased flexibility; achieving industry-leading quality standards, and continuously raising the bar on customer satisfaction. Equally important, Ann was able to create a winning culture in Virginia. Her team always stepped up to the plate regardless of time pressures or the complexity of the projects undertaken. Under her leadership the reputation of the company's support services were dramatically enhanced. She was an indispensable part of my senior leadership team and a critical asset to the company."*
>
> Garry Johnson, EVP, Chief Technology Officer at Dendrite International, Inc.

Data Center Design, Consolidation and Migration of United States Data Centers

As a result of strategic acquisitions, Cegedim had multiple data centers in the United States that were not large enough to support the full compute capacity required by the rapidly growing company. Worked with the Hampton Roads Economic Development to negotiate financial incentives and build a new data center in Chesapeake, Virginia. Developed strategy to relocate 50 percent of staff from New Jersey and Pennsylvania, and to recruit the best talent in Virginia to staff the new center. This approach significantly reduced the risk of migrating customer data center workloads by seeding the team with staff experienced in supporting the business that moved with the customer systems.

Designed operational flow and Tier 3 compliant infrastructure architecture, and oversaw construction of 50,000 ft.² data center facility to provide infrastructure hosting of mission critical Sales Force Automation Software Infrastructure for over 40 of the top U.S. pharmaceutical companies. This was one of two facilities within several miles that were able to remain operational during Category 5 Hurricane Isabel.

Worked with customers to collaboratively plan and execute seamless migrations of infrastructure for over 40 pharmaceutical customers in a 17 week period, successfully consolidating all U.S. data center locations into one facility without impact.

Quality Improvement Initiatives

Founding member of Continuous Improvement Council formed to steer company's quality improvement initiative. Developed and implemented Key Performance Indicators for service functions. Established global data center standards and strategy across nine multinational data centers providing hosting services to

many of the world's largest pharmaceutical sales forces. Building this foundation was critical to establishing Cegedim's credibility as the top provider of sales force effectiveness solutions. This strategy was the keystone of success through Cegedim's exponential growth from 1997 through 2006.

Business Continuity During Category 5 Hurricane

Created and invoked Data Center and Customer Service Center Disaster Recovery and Business Continuity plans and led the recovery teams during Hurricane Isabel, a Category 5 hurricane that hit southeastern Virginia resulting in wide-scale power outages in the area for several days. The Data Center's Tier 3 infrastructure sustained business operations for the duration of the storm, and Customer Service Center operations were moved to Norcross, Georgia without impact to pharmaceutical customers.

Service Excellence Grows Business

Streamlined service offerings that leveraged automation technologies; implemented disciplined processes resulting in customer efficiency gains, high customer satisfaction, and competitive pricing of service offerings; grew the company's outsourced technical services business from annual revenues of $2 million per year to over $150 million per year over a nine-year period.

Electronic Data Systems (HP), Operations Manager 1986 – 1996

Provided a broad portfolio of business and technology solutions to help clients worldwide; raised the overall operational tempo and business performance of Electronic Data Systems (EDS) Operations teams. Progressed from computer operations positions to the management of a multi-platform operational team of 60 technicians – developed recurring training to improve quality of operations. Completed numerous strategic initiatives for quality implementation, organizational reengineering, and data center migrations; improved the operational work flow of data centers (improving adherence to scheduled events) in support of several outsourced customer compute environments across many industries including Healthcare Telecomm, Insurance, Financial, and Manufacturing.

Operational Turnaround of High Visibility Data Center Operation

Relocated to Rochelle Park, New Jersey to manage a troubled Data Center Operation that processed critical ATM transactions for over 4,000 financial institutions; standardized multi-platform operational procedures reducing infrastructure management training time by 50percent, and improving operational proficiency and service. Optimized staffing model ensuring skilled resources in key roles and additional training where deficiencies existed. Service turnaround resulted in a 75percent increase in customer satisfaction based upon feedback from client account management surveys, and an employee satisfaction rating that was the second highest of any of the 500 managers in North America.

New Customer Data Center Migrations

Worked on numerous Data Center Migrations to standardize new customers to EDS' processes and tools, and seamlessly migrate their business applications into the shared data center hosting environment. New customers included Meritor Savings Bank, Bethlehem Steel, NASCO and many others Developed several best practices that engaged the migration customer ahead of the start date; ensured the customer was part of the decision process, briefed on status, and involved in the acceptance process as the migration proceeded to closure.

Quality Improvement Initiatives

Designed the Quality Improvement Program for the Camp Hill Information Processing Center and trained 275 employees on Quality Improvement Process concepts based on quality philosophies and practices of Crosby and Deming. Benefits of this initiative included design and automated data collection of Key Performance Indicators, and reengineering and streamlining of batch scheduling and batch execution functions resulting in a 35percent cost savings to the company. Was recognized as a leader in implementing quality improvement programs and worked with numerous EDS' organizations to present our strategy and consult with them on the best approach to their implementation.

Employment History

2008 – Present	Unisys Corporation
1996 – 2006	Dendrite International
1986 – 1996	Electronic Data Systems

Education

Harrisburg Area Community College, Harrisburg, PA: Earned credits toward B.S. Math/Computer Science

Professional Certification

- ITIL V3 2011 Foundations
- Network+

Professional Training

- Project Management Institute: *Project Management Professional (PMP) Certification in progress*
- General Motors Quality Institute: *Professional Certificate in Quality Improvement Process Management*
- Mentor Coach, LLC: Life *Coaching Foundations and Strategic Career Design Coach Certificate Programs*
- International Coaching Academy, Australia: *Certified Professional Coach Program*
- EDS Leading People Program: *Dallas, Texas*
- EDS Operations Development Program: *Dallas, Texas*

Honors and Awards

- *Nominated for* CIO of the Year Award *in Atlanta, Georgia, 2005*
- *Invited Speaker at two* AFCOM Data Center World Conferences, *2004, 2005*
- Outstanding Contribution to Company Award: *Dendrite Morristown, New Jersey, 2000*
- Outstanding Customer Service Award: *EDS Rochelle Park, New Jersey, 1996*

UNISYS

[redacted]

Transition Director

Key Skills and Knowledge

- Project Management
- Data Center Transitions
- Service Level Agreements
- Service Catalog
- Global, Multi-Site Operations
- IT Operations
- Contract Management
- Applications Management
- Business Planning
- Relationship Building
- Operational Transitions
- Business Development
- Portfolio Management, Budgets
- Outsourcing Negotiations.

Skills Summary

IT professional located in Harrisburg with 27 years of exceptional delivery experience improving operations and profitability for well-known companies in diverse industries including Healthcare, Retail, Manufacturing, Communications, Chemical, Gaming/Entertainment, Publishing, Inspection and Testing, Hospitality and Direct Marketing.

Five years of transition experience with a successful record of building and leading technology teams in new business development initiatives and support of an existing base.

Employment History and Related Experience

Unisys Corporation, Transition Director 2012 – Present

Transition Director for the Commonwealth of Pennsylvania located in Harrisburg, Pennsylvania. Provides experience in large transition and migration programs to the solution development team developing schedules and fine tuning processes that will be utilized during the transition and migrations activities.

Dell Services Transition Management Consultant 2008 – 2012

Provided stellar leadership for Dell Services transitions, data center migrations and large scale system upgrades.

Healthcare Data Center Transition

Managed $5,500,000 Data Center Transition Program from data centers in Salt Lake City, Utah to Plano Texas. Provided oversight and leadership of a matrixed team consisting of members from Dell, Intermountain Healthcare Infrastructure and Intermountain Healthcare Applications. This team planned, scheduled, coordinated, and executed legacy upgrade transition of more than 600 servers to Plano, Texas on a very tight schedule. During transition planning, accomplished transition risk assessment forming performance contingencies to address potential issues. The transition was successfully achieved with a robust set of processes, carefully defined roles and responsibilities for the transition team, focused training for the user community, and adherence to strong project management practices.

Data Center Migration

Managed $6,000,000 Data Center Migration Program from data centers in and around Baltimore, Maryland to Plano Texas. Provided oversight and leadership for a team of 30 subject matter experts in disciplines such as Intel Servers, Unix Servers, Storage, Network, Citrix and applications. This team planned, scheduled, and moved more than 500 servers and 50 TB of storage ahead of schedule. Transition planning included, risk assessments, contingency planning, training for transition team member roles and responsibilities, detailed schedule assessments, and daily status meetings. Extensive coordination of transition activities with client eased the operational impacts preparing the user community for the change.

Transition and Data Center Migration Portfolio Oversight

Managed Perot Systems Healthcare Business Unit's portfolio of Transitions and Data Center Migrations (DCM); provided leadership and management oversight to a team of eight Transition Leaders and DCM Project Managers. Guided concurrent projects and programs transitioning operational legacy support of accounts with over $1 billion in total contract value using master schedules and Transition Program Management Office (PMO) processes, and extensive coordination with client during transition planning. Led several Data Center Migrations from client sites to centralized data centers. Delivered all migrations on schedule with successful data conversions, systems ready to support operations, and staff fully trained on new functions. Post transition surveys indicated satisfaction from user community for the seamless transitions for business functions.

Healthcare Transition Portfolio

Managed $7,500,000 Transition of Services Program from an Account based to a Global Leveraged team for the Catholic Healthcare West (CHW) account. Provided oversight and leadership of 14 projects including globalizing a 70 person service desk, a 45 person security provisioning team as well as various other disciplines such as Intel, Unix, Network, and Telecom. This globalization effort enhanced CHWs support by increasing the available staff by approximately 30percent across three additional geographical regions.

EDS Corporation Account Manager – Systems Engineer Manager, 1993 – 2008

Oversaw accounts and system engineering teams in support of Electronic Data Systems (EDS) projects.

SAP Outsourcing Project

Directed a $56,000,000 SAP Hosting outsourcing engagement with client J.Crew, retailer of women's, men's, and children's clothing, shoes and accessories. Led the on-site IT staff at multiple client locations, significantly improved operations and client satisfaction through reengineered legacy processes and better systems communications resulting in a seven year contract extension with a significant increase in scope.

Churchill Downs Implementation

Led sales effort resulting in an outsourcing agreement with Churchill Downs Incorporated worth $6,000,000. Directed account startup activities and on-going support to include hiring and staffing technical delivery team and starting implementation within 30 days of contract signing. Developed and executed plan to implement Customer Relationship Management (CRM) development and production environments within four months allowing Churchill Downs to go-live and benefit from improved CRM activities and marketing for the upcoming Kentucky Derby.

Bethlehem Steel Corporation – Senior Programmer, Programmer 1986 – 1993

Directed $250,000,000 application maintenance and development (AD&M) outsourcing contract with Bethlehem Steel.

Team Leadership

Managed and provided leadership EDS Bethlehem Steel account Information Technology (IT) staff at multiple locations and teams to include advanced technologies, data resource management, human resources, law, finance, and accounting support teams.

Application Enhancements

Delivered wide range of application enhancements that continuously improved client satisfaction resulting in five year contract renewal worth an additional $200,000,000. Significantly increased client employee satisfaction and retention through carefully applied software development and implementation principles. Reduced the anxiety felt by the user community for each software release.

Computer Aid, Inc., –Programmer 1985 – 1986

Provided Application Development and Maintenance support across such platforms as MVS, OS2, Unix, and Windows using COBOL, SAS, Focus, Assembler, C++, and Java programming languages.

Education

- BS, Computer Science – The Pennsylvania State University.
- Stanford University IT Executive Program.
- Harvard/MIT Executive Negotiations Program.

Certifications

- ITIL Foundations V3 Certified
- Project Management Professional (PMP) Certification

UNISYS

IBM

[redacted]

Transition Manager

Key Skills and Knowledge

- Managed pSeries ERP transition
- Led Commonwealth of Pennsylvania SAP transition
- Directed implementation of network upgrades
- 14+years experience supporting the Commonwealth of Pennsylvania
- ITIL Certified
- PMP
- Audit support
- Security focal point.

Skills Summary

Senior Project Manager, located in Harrisburg, Pennsylvania, in the Public Sector Strategic Outsourcing organization of IBM Global Technology Services with more than 14 years of Commonwealth experience. Extensive experience in transition leadership, Project Management, Information Technology (IT) infrastructure implementations and IT operations and services management, and has successfully led transition teams comprised of subcontractors, clients, and IBM resources implementing data center operations services for mainframe and distributed technologies.

Employment History and Related Experience

IBM Corporation – Harrisburg, Pennsylvania 2010 – Present

Data PowerHouse Service Delivery Manager

Manages IT service delivery for the Data PowerHouse outsourcing contract with the Commonwealth of Pennsylvania, overseeing services in the mainframe and distributed systems environments. Successfully managed the transition of the pSeries/AIX systems supporting ERP at agency locations into the Data PowerHouse; developed the transition plan, schedule, contingency options, and coordinated with the Commonwealth; built clearly defined roles and responsibilities for each transition team member to ensure no tasks were overlooked. The project successfully migrated the legacy workloads to new production hardware, physically moved the non-production systems, and was accomplished on schedule.

Effectively maintains customer relationships at the recipient agencies while ensuring positive customer satisfaction; manages service delivery to contract performance standards; supports continuous improvement.

Leads project reviews of compliance process, procedures, and documentation (IBM account security focal point).Manages responses to audit requests and oversees required remediation efforts; leads monthly compliance meetings with to evaluate compliance posture and document security related activities; develops detail project plans and schedules to support biannual multi-agency disaster recovery exercises improving planning, execution, and evaluation for these tests.

IBM Corporation – Harrisburg, Pennsylvania 2005 – 2010

Data PowerHouse Services and Facilities Manager

Led the transition of the Commonwealth's ERP systems from legacy providers to upgraded systems and network infrastructure on schedule with no interruption to customer operations or applications. Designed transition plan with clear team member roles, responsibilities, and deliverables to ensure every team member understood their part of the transition. Developed and coordinated the transition schedule with the Commonwealth to reach firm agreement on dates and to define the points where the Commonwealth would support the transition. The new ERP-SAP environment is critical to the Commonwealth's ability to manage their financial and human resource functions across 53 agencies state-wide. The entire transition was completed on schedule with no unplanned interruption to services.

Managed team of 20+ IT professionals from various technological disciplines to successfully establish service levels, associated system monitoring, disaster recovery plans, and annual testing without financial penalties.

IBM Corporation – Harrisburg, Pennsylvania 1999 – 2005

Commonwealth of Pennsylvania Department of Labor and Industry
Network Support Project Leader

Project Leader for a network support engagement with a large state government agency; support included directing transition activities to upgrade the network infrastructure. He coordinated the transition plan and schedule with Commonwealth stakeholders to ensure the transition workflow integrated properly with the Commonwealth business flow. Mr. DeCecco verified that each transition team member understood their role and responsibility to support the transition. He performed regular transition risk assessments, supported contingency planning, and held regular transition status meetings. The Commonwealth was regularly updated on progress. Project results included decreased system down time, expanded systems management capabilities, and increased throughput.

Mr. DeCecco was responsible for maintaining high network availability and performance for the central office and over 150 remote field office locations.

Mr. DeCecco successfully completed a number of other significant initiatives, including Dynamic Host Configuration Protocol (DHCP) rollout to over 5,000 users, implementation of wireless (802.11 technology) at a Commonwealth-run educational facility and large-scale refresh of network infrastructure for customer local and remote locations. Positive project results and customer satisfaction resulted in multiple contract renewals from the initial one year term.

Directed transition activities to upgrade network infrastructure to decrease system down time, expand management capabilities, and increase throughput; coordinated transition plan schedule between Commonwealth business and work flow; insured each team member understood and performed assigned roles and responsibilities during transition. Performed regular transition risk assessments, supported contingency planning, and held regular transition status meetings while maintaining project status updates with Commonwealth

IBM Software Support Practice – Northeastern U.S. 1995 – 1998

Team Lead Data Networking

Team leader of networking professionals supporting northeastern United States region; provided software support and configuration assistance for IBM Networking products division customers; defined team roles, responsibilities, and processes successfully in order to in order to manage aggressive service level agreements between IBM Networking and customers.

Education

- Bachelor of Science, Trinity College
- Certification in Electronic Engineering, RETS Technical School.

Certifications

- Information Technology Infrastructure Library (ITIL), V3 Foundation Certification, 2010
- Project Management Professional (PMP), Project Management Institute, 2009
- Cisco Certified Network Associate (CCNA), 1999.

UNISYS
IBM

[redacted]
Availability/Change Manager

Languages
- English

Key Skills and Knowledge
- Availibilty Management
- Change Management
- ITSM7
- ITIL Certification
- Service Level Measurements and Incident Reporting
- Focal Point for Aduits

Skills Summary

Currently serving as IBM Availability and Change Manager for the Commonwealth of Pennsylvania (DPH Project); primary responsibilities include providing oversight for change control, project planning, implementation, and reporting; additional responsibilities include monthly measurement and incident reporting, root cause analysis, trend reporting, and process improvement; serves as focal point for internal and customer adults; manages account asset and primary process control metrics; focal lead for ITSM7 tool and ITIL process controls related to incident/problem/change and asset.

Employment History and Related Experience

IDM, Harrisburg, Pennsylvania — September 2010 - Present

Availability/Change Manager

Provides oversight for change control, project planning, implementation and reporting in addition to monthly measurement and incident/RCA, trend reporting and process improvement; IBM focal for all Commonwealth audits; project focal for IBM internal executive processes including CWP (process controls), CHIP (account financial health), GACDW (internal Asset database), and Service Activation/Deactivation process (SA&D); project focal for ITSM7 and ITIL related processes. Managed audit readiness of problem, change, and asset management resulting in zero defects during tenure.

IBM, Harrisburg, Pennsylvania — November 2003 – September 2010

Data Center Operations Team Lead & Availability/Change Manager

Managed Data Center Operations for Commonwealth of Pennsylvania (IES); developed and implemented web based process and procedures specific to costumer computing environment; managed problem and change activity resulting in zero financial penalties during tenure as change coordinator; managed audit readiness of problem, change, and asset management resulting in zero defects during tenure; successfully managed business activity through high turnover of operations staff.

IBM, Allentown, Pennsylvania — November 2002 – November 2003

Microsoft Exchange Administrator

Served as Exchange Administrator supporting Lucent Technologies Global workforce including end user support and exchange server administrative tasks.

IBM, Allentown, Pennsylvania — January 2000 – November 2002

Operations Team Lead

Developed and implemented complete Data Center operation runbooks including processes and procedures specific to the customer's (lucent Technologies) data center environment; supported 1000+ mid-range Wintel and Unix (Solaris) systems; led development and deployment of customized monitoring system (HP Owner) for Data Center operations

Education

- Bachelors of Education in Kinesiology 1999
- University of Kentucky

Professional Certification

- Foundation certified in IT Service Management

UNISYS

[redacted]

Service Level Management Analyst

Key Skills and Knowledge

Leadership & Management
Service Delivery Management
Infrastructure Management
Project Management
Transition Management
Quality Management
Continuous Process Improvement
SLA & KPI Management
Service Delivery Leadership
Team Building Leadership
Governance Leadership

Domain Expertise & Solutions
Reporting & SLA Management
ITIL Capacity Management
ITIL Transition & Implementation
ITIL Change Management
Enterprise Data Center Expert
Data Center Facilities Management
Operations Management
Finance Management (ROI)
Asset Management Audits
Vendor Management
Business Continuity Planning
Disaster Recovery Planning
RFID Technology

Project and Program Management
Microsoft Certified Professional
Business Analysis Professional
ITIL v3 Foundations

Productivity Tools
Microsoft Office
Microsoft Access
Microsoft Project
Microsoft Visio
Adobe
Remedy
Clarity
SharePoint
LDRPS

Skills Summary

An accomplished and innovative professional with hands-on experience in service level agreements, infrastructure management, process improvement, project management, program development, IT Service Management, process/workflow design, new technology review, capacity planning, negotiations, executive reporting, and quality assurance. Strong advocate of business processes, develop service operations process manual to integrate divergent operations concepts into singular flow. Possesses proven leadership strengths in personnel development and team building. Utilizes strong interpersonal skills and keen attention to detail in order to ensure successful delivery of high-quality, cost-effective solutions. A dynamic and dedicated leader with an unwavering commitment to excellence.

Employment History and Related Experience

COMCAST, Senior Manager, Data Center Services, West Chester PA, 2010-2013

Directed data center infrastructure management program, including requirement identification, technical design, service deployment and implementation, project management, and highly customized executive analysis; delivered operational reports, application support, development, data analysis, and quality assurance. Conducted monthly coaching sessions and semi-annual performance reviews and maintained individual development plans for each team member. Designed and implemented end-to-end workflow, documented workflow in an enterprise service operations process manual, minimizing manual data input and employing business and user requirements to reduce process time by more than 30%.

- Evaluated new technology, assessed business justification, and prepared supporting recommendation documents and return-on-investment calculations.
- Collaborated with cross-functional teams to introduce RFID technology into national data centers, automating inventory audits and increasing reporting efficiency by 60%. Analyzed data center audit findings using Microsoft Access to manage large data and queries to identify trends.
- Produced operations reports, departmental productivity metrics, enterprise portfolio capacity metrics, and team performance metrics for customer satisfaction, incident resolution, performance against committed Service Level Agreements, and application availability. Accountable for reporting monthly metrics to senior management, along with explanation of anomalies and significant changes.
- Coordinated project activities and schedules as well as assessed and maintained project plans as appropriate to reflect changing needs and requirements.
- Defined and negotiated service-level agreements with customers and other service-related partners. Maintained adherence to ITIL processes relating to Change Management, Service Level Management, and Problem Management.
- Provided direction and guidance toward identification, development, and delivery of all documentation necessary for related processes and supported applications.
- Managed all aspects of vendor relationships, including contract negotiation, leveraging company buying power to achieve most competitive pricing on purchase agreements, professional services, and annual maintenance.

COMCAST, Program Manager, Data Center Services, West Chester PA, 2008 - 2010

Provided overall program management for national data center computer-aided facilities management initiatives, including oversight of all project management activities from project scope and planning through delivery and acceptance. Presented program status, issues arising, and actionable details regarding future requirements to executive management. Conducted ongoing training for users, ensuring comprehensive understanding and maximizing return on investment for all applications. Built comprehensive model for capacity metrics reporting, reducing completion time by 25%.

YELLOW BOOK USA, Senior Manager, Data Center Operations, King of Prussia, Pennsylvania 2003 - 2008

Led all design, planning, implementation, security, power, cabling, monitoring, capacity planning, migration, forecasting, documentation, vendor management, project management, and change management activities in data centers and LAN rooms company-wide. Built 24/7, geographically dispersed data center support team responsible for racking, cabling, inventory, production processing, enterprise monitoring, systems backups, offsite storage, and tape library management. Evaluated, recommended, implemented, and supported all new data center technology and applications. Maintained all standards, policies, and procedures to ensure 100% compliance with Sarbanes-Oxley.

- Scheduled and tracked maintenance activities for all UPS, diesel generator, HVAC, and fire suppression equipment, resulting in 99.99% uptime.
- Partnered with multiple information technology, real estate, and facilities teams to meet business demands, accomplish project goals, and resolve problems.
- Coordinated multiple engineering and consulting groups to design new 10,000-square-foot, 500KW data center. Managed 250KW critical infrastructure upgrade. Completed upgrade on time, within budget, and with no unplanned downtime.
- Authored comprehensive data center operations manual, standardizing procedures for all production processing, operator monitoring, and support functions and greatly reducing error rates.
- Spearheaded major transition of responsibility for all equipment procurement, racking, cabling, inventory, and documentation to operations, significantly expanding role of team. Implemented flash reporting targeted to senior management summarizing daily processing accomplishments and current problem status, creating complete transparency.
- Earned associate business continuity planner certification while participating in development, implementation, and maintenance of company-wide business continuity and disaster recovery plan

YELLOW BOOK USA, Computer Operator, Data Center Operations, King of Prussia, Pennsylvania 2002

Managed day-to-day offsite data storage program, ensuring disaster recovery capabilities. Monitored technical environment to detect and escalate problems as required. Set up and executed computer processes and procedures as defined by daily, weekly, and monthly schedules. Provided information to data center management and other IT groups relative to normal and abnormal processing activities.

YELLOW BOOK USA, Account Representative, Data Center Operations, York, Pennsylvania 1998 -1994

Managed customer advertising accounts. Developed and presented proposals for directory and internet advertising. Completed corporate sales training program receiving top achievement award for highest dollars sold during training, selling more than 200 new accounts.

Education

- VILLANOVA UNIVERSITY, Online, Master Certificate, Business Analysis, Anticipated 2013
- PENNSYLVANIA STATE UNIVERSITY, Great Valley, Pennsylvania, M.S., Information Science, 2008
- SHIPPENSBURG UNIVERSITY, Shippensburg, Pennsylvania, B.S., International Management, 1993

Certifications

- Microsoft Certified Professional – 2001
- Certified Business Analysis Professional – in progress
- ITIL v3 Foundations Certification – in progress

UNISYS

[redacted] Senior Enterprise Infrastructure Analyst

Languages

English

Key Skills and Knowledge

Domain Expertise & Solutions

- Managed Hosting Services
- Capacity on Demand Services
- Enterprise Service Management
- Networking
- Security
- Data Center Architecture
- System Architecture
- Virtualization.

Project and Program Management

- Services Transition Architecture
- Service Management Deployment.

Hardware

- IBM Servers
- Cisco Networking.

Operating Systems

- Windows (XP, 7)
- Cisco IOS.

Office Productivity Tools

- Microsoft Office
- Microsoft Visio
- Microsoft Project\IBM Rational Requisite Pro.

Skills Summary

Over 16 years of experience with the Information Technology Outsourcing industry focused on Datacenter support. Led a large team of architects to develop technical components (server, storage, and network security) to build a multi-tenant data center to support the State of Georgia's strategic and consolidation plans.

Employment History and Related Experience

Unisys, Lead Client Architect, November 2011 – Present

Realigned strategic Client Architect role; interacted with the client Information Technology (IT) leadership to align technical solutions with the client's current business requirements; reviewed the current technology and services, current business requirements, and future business needs to develop and maintain strategic technical roadmap; provided architectural oversight for services and projects that support the client. Managed North America Client Architect team for the Unisys account teams; nurtured relationships with key client contacts to identify and develop technical solutions to support evolving business requirements for existing Unisys customers; led a business development team to create a strategic technical solution; organized and mapped the technologies and support models to support a consumption based Managed Hosting Services model. Developed a server image rate structure that included hardware, software, and support during the Unisys Self-Provisioning pilot for the Commonwealth; developed a solution architecture document standard to improve Client technical solutions in a consistent manner to include requirements, decisions, technical overview, service components, and associated costs significantly reducing client costs through creative deployment of system components and connectivity elements.

IBM, State of Georgia, January 2010 – November 2011

Transformation Integration Architect

Key technical advisor for the IBM account director; client's director of services, client's director of operations, chief architect and architecture team, agency CIOs and CISOs, and IBM project management team; delivered oversight for on ongoing architecture activity. Implemented problem resolution approach to manage changes within the overall solution; identified additional requirements; developed associated solutions to meet changing business needs during the transition program.

Improved the architecture review process by reviewing current practice with client chief architect and IBM account chief architect; changed the order of the design reviews to enable support staff to review and approve solutions before presentation to client's chief architect and domain team members; changed review process to improve overall quality of solutions presented to client and reduced the review cycle by 5-7 days. Improved architecture review process by separating initial security and regulatory review; created new milestone event as part of architecture review process to enable solution assessments to focus on security concerns while also ensuring regulatory requirements were adequately covered.

Led architecture team to design, document; planed Managed Hosting Services implementations for overall infrastructure transition program to include upgrade; controlled the migration of fourteen agencies to shared enterprise services for Active Directory, Exchange, McAfee Antivirus, IBM Tivoli Storage Manager, IBM Servers, IBM Disk Storage, VMware virtualization, IBM Tivoli Service Management tools, F5 Load Balancers, and Juniper Data Center network. Program comprised data center architecture supporting fourteen agencies with common infrastructure while maintaining separate environments for each agency and introduced a new data center architecture and technology containing shared VMware infrastructure, tape encryption, shared Network Attached Storage, and multi-tenant firewalls

Developed Business Continuity system architecture to support recovery of critical applications at a remote facility; interviewed client chief architect, client architect team, and account manager to interpret requirements; based the application continuity architecture on overall datacenter architecture but the actual components were adjusted to support the smaller application environment for the business continuity tiers each agency requested. Led architecture team to develop branch office common services hosting architecture to replace Netware directory and file servers in Agency branch offices with VMware and Network Attached Storage in order to host Active Directory and File Services with remote backups and disk

encryption to standardized the installation of new servers and storage.

Led architect team to integrate Federal Regulatory guidelines and requirements into technical solutions during the initial architecture activities reducing review time and need to plan and deploy one-off solutions while improving overall solution quality. Established requirements management and architectural decisions reviews with customer's chief architect and IBM architect team; reviewed project plans with agency CIOs and CISOs, IBM project management team, and client architecture team to validate schedules, project dependencies, critical operation time windows, and resource requirements.

IBM, Virgin Mobile, March 2009 – December 2010

Transformation Integration Architect

Introduced and designed a Virtual Desktop Infrastructure (VDI) using VMware virtualization software, Microsoft Windows, Red Hat Linux, IBM Servers, and IBM Disk Storage to support IBM Application Development resources managing and developing mobile services in order to enabled IBM application team to use software development and support team members globally while meeting the client's software licensing obligations in a flexible and cost effective manner. Led architect team to design, document and plan implementation of a new Data Center Architecture to support relocating and consolidating client's business (Active Directory, Exchange, and File Servers) and mobile service applications (SMS, IVR, mobile phone billing, and setup); designed and documented the required infrastructure including a technology hardware refresh to support transition of client application infrastructure using Sun Servers, IBM servers, VMware, and IBM disk storage; designed and documented the data center architecture and provided technical oversight for overall infrastructure deployments including servers, major applications, service management tools, networks, and support functions during the transformation and server relocation programs communicated with technical resources to provide required information and access to meet project requirements and schedules; identified and documented project and technical solution gaps including required changes, associated business requirements, and supported customer technical leads and account management as a technical focal point.

IBM, Hess Corporation September 2008 – March 2009

Transformation Integration Architect

Proposed and designed a standardized VMware virtualization infrastructure using IBM servers and SAN disk storage to support global technology refresh program and new requests for service; communicated with technical resources to provide required information and access to meet project requirements and schedules; designed, documented, and provided technical oversight for overall infrastructure deployment during transformation project including IBM service management tools and support teams; supported customer technical leads and account management as a technical focal point; identified and documented project and technical solution gaps including required changes and associated business requirements.

IBM, Welch Allyn, March 2006 – September 2008

Transformation Integration Architect

Proposed, designed, documented, planned, and implemented a global network upgrade and standardized network architecture using Cisco and Aruba networks technology; developed and deployed a standardized Guest Wireless service for all sites using Aruba networks hardware; proposed, designed, and led the installation of an Infoblox based DNS and DHCP service globally; designed, implemented, and supported a data center network to support email, Active Directory, and a SAP application infrastructure.

IBM, Sandler and Travis' Trade Management System for GM January 2000 – May 2006

Senior Network Architect

Designed a Cisco firewall upgrade to replace end of life IPSEC router; designed, implemented. and managed a Cisco Gigabit network to improve performance, capacity and support updated application requirements; designed, implemented, and managed a Cisco network to replace an end of life Token Ring network and prepare for new servers and application upgrades; trained network support team on new technologies and processes.

IBM, Varian Semiconductor, March 2000 – December 2003

Senior Network Architect,

Designed, implemented, and managed a Cisco Gigabit Ethernet network to replace the IBM ATM network after twenty-four months due to increased performance and management requirements; designed, implemented, and managed an IBM ATM Local Area Network (LAN) to support a SAP application and infrastructure; led network support team to integrate customer's corporate site network with IBM's data center and wide area network (WAN) implementation.

IBM, Senior Network Architect May 1999 – August 2006

Designed, documented, planned, and implemented Cisco Ethernet for a corporate office and data center to replace end of life Token Ring network; designed, documented, planned, and implemented Cisco wireless infrastructure for a corporate office and as testing environment for global standardization; led a national team to support complex projects and problems at all U.S. corporate offices and data centers; developed training presentations and trained the network support team to use new tools, technologies, and processes; developed and documented network support procedures based on contractual requirements.

IBM, Eastman Kodak, August 1996 – May 2006

Senior Network Architect

Designed and implemented new Cisco Gigabit Ethernet Core Network for manufacturing plant to replace an end of life FDDI based core network, improve overall performance, and increase capacity; designed and implemented Cisco router based network using Serial Tunneling to replace obsolete remote Front End processors; evaluated, tested, and deployed new wired and wireless Cisco network technologies in customer production networks to support changing customer and business requirements; evaluated, tested, planned, and managed deployment of two-factor authentication using Cisco ACS with RSA Secure-ID for corporate wireless network. Developed network architectures and project estimates based on Requests for Service and customer requirements; managed and planned projects with network components to ensure proper completion within customer requirements, service level agreements, and approved plans; developed training presentations and trained the network support team to use new tools, technologies, and processes.

Employment History

- Unisys Corporation..... 2011 – Present
- IBM..... 1996 – 2011
- Edgemere Services..... 1995 – 1996

Education

- Salem High School..... 1992
- Rochester Institute of Technology, BS Management Information Systems, 2002

Professional Certification

- ITIL Version 3 (2011 Release) Foundations... 2012
- Open Group Master Certified IT Architect ..... 2008 – Present
- IBM I/T Architect – Infrastructure ..... 2008 – 2011

Professional Development

- ITIL Version 3 (3011 Release)..... 2012

UNISYS

[redacted] Incident Management Manager

Languages - English

Key Skills and Knowledge

Strong Leadership of Complex Organizations

Incident Management

Data Center and Help Desk Service Management

SLA/KPI Management skills

Expert at Customer Satisfaction Management

Development of High Performance Teams

Quality Improvement Program Implementation and Management

Process Development and Organizational Reengineering

Communications

Business Continuity and Disaster Recovery

Continuous Improvement process implementation

Skills Summary

Versatile, results driven and accomplished service delivery professional with the proven ability to direct and deliver new client implementations, steady state IT services including Incident/Change and Problem Management. Strong proven skill with escalation management, incident resolution oversight for technical and operational concerns; delivers ongoing client account management on time, within scope, and with the highest emphasis on meeting the customer's needs.

Project Experience

Microsoft Retail, Unisys Account Relationship Manager, 2012 - Present

Account Relationship Manager for a growing and highly competitive retail store environment. Delivered 24X7X365 Service Desk, Incident Management, and Alert Management Services to manage over 4K contacts per month.

- Provides management for all deliverables agreed to in the Scope of Work as wells as managing financials to ensure we are meeting appropriate margins; facilitates clear linkage and communication between help desks and operations during incident escalation.
- Facilitated progress for this client during their nationwide growth; supported operations increased the supported store count from 17 to over 40 to implementing an Alert monitoring team for data center towers that are supporting the store environment.
- Grew the team from 17 agents to over 40 agents, have been able to meet, and exceed, all deliverables.
- Delivers stable backup support for the Program Manager in areas of incident management, escalation oversight, and resolution tracking.

NEC/7-11, Unisys Account Relationship Manager, 2010 - 2012

Account Relationship Manager responsible for delivering Level 1 and Level 2 Service Desk services, a Level 2 Application support group, and a Level 2 Software/Application/Change Management team to a retail customer operating 7X24X365 with over 7K stores nationwide.

- Processed over 22K inbound calls, 15K outbound calls, and the creation and management of over 16K incidents per month. Our application support team managed real-time issues that preventing the store from selling product, opening/closing related issues, business ownership changes, and issues where store servers failed and needed to be reinstalled and rebuilt to support store operations.
- Identified root causes of chronic problems, worked diligently with Operations to track issues and oversee resolution. Developed improved reviews of SLA performance, confirming delivery compliance with well-defined metrics that clearly demonstrate actual performance, implemented SLA management principles to ensure strong oversight.
- Maneuvered an underperforming account to a well performing account, both in SLA's and financial management; increased the revenue opportunity by identifying an area where a Vendor management service was required.

General Growth Properties, Unisys Service Delivery Manager, 2009 - 2010

Service Delivery Manager responsible for delivering Infrastructure services, Service Desk, and Field Services support; managed all aspects of Problem, Change, Incident, and Release management.

- Implemented new processes to allow for better Incident Management tracking and issue analysis which decreased the resolution times of incidents, which decreased the amount of time user's had to wait for resolution of their issues.
- Implemented a new Change Management process to increase the success of changes while also reducing the number of incidents related to performance of change activities; implemented a Problem Management solution to help quickly drill down to root causes, manage problem areas, and reduce the recurrence of issues. This process led to infrastructure changes being made to reduce failure rates, as well as Service Desk processes being updated to enable better data capture to feed into the process.

Diversey Inc. (JDI), Unisys Service Delivery Manager, – 2007 - 2010

Service Delivery Manager responsible for delivering Service Desk and Field Service support to a global company supporting over 100 countries and 12 languages. Telephone support was provided from 6 different Managed Service Centers located in Brazil, China, India, Netherlands, Hungry, and Columbia. Field Services were provided locally by both dispatched incidents and dedicated onsite support.

- Ensured all SLA's/KPI's are being met, ensuring incidents were being managed to closure, ensuring field services techs had the parts they required to meet the needs, that stocking locations had required inventory, reporting was delivered as per the SOW, and financials were managed to ensure the project's success.
- Implemented new processes that streamlined incident resolution while also ensuring quality was still being delivered. Implemented Incident Management team process to ensure high priority incidents were being managed to resolution while also ensuring the business was receiving communications/updates/statuses.

Quality Improvement Initiatives

Implemented Quality Improvement Programs for NEC/7-11 and Microsoft Retail customers; trained over 100 agents on requirements and proper quality practices. Implementation of this program enabled a better quality product to be delivered both to the end users reporting issues and the groups resolving incidents.

Additional Employment History

- 2005 – 2007 Unisys Corporation
- 2004 – 2005 America Online
- 2002 – 2003 IT Consultant (Self Employed)

Education

- Weber State University, Ogden, Utah: Earned credits toward B.S. in Business Mgmt
- FT Sam Houston Training Center, San Antonio, TX – Earned Certificate of Completion for Army Medical Specialist program

Professional Certification

- ITIL V3 2013 – Expected completion June 2013

Professional Training

- Six Sigma Lean Green Belt

Honors and Awards

- Bronze, Silver, and Gold Achievement awards – Unisys

Military Service

United States Army 1992 – 1994 (Medical Specialist)

UNISYS

[redacted]
Change Manager

Key Skills and Knowledge

- Program Management
- Contract Strategy Analysis
- Change Management
- Service Level Agreement Development and Analysis
- Process Improvement
- Software Support
- Client Relations
- Problem Solving
- Data Operations
- System Upgrade
- Troubleshooting
- Disaster Recovery
- Database Management
- Inventory Control
- LAN and WAN
- Team Leadership

Skills Summary

Results-oriented, thorough Information Technology (IT) professional with30+ years of experience spearheading multifaceted technical business units to meet internal company and client needs. Demonstrated expertise in delivering advanced technical support to government agencies and meeting their technology needs by monitoring security, updating systems, and troubleshooting. Known for delivering projects on time and under budget while leading diverse teams to success.

Employment History and Related Experience

Unisys, Harrisburg, Pennsylvania 2004 – Present

Global provider of consulting, systems integrations, and outsourcing for multiple vertical markets.

Information Technology (IT) Service Delivery Manager 2005 – Present

Support data center technology needs of Commonwealth agencies in project exceeding $1 billion. Allocate and verify delivery of data center resources, including change management, facility services, physical security, hardware services, operational support, software support, disaster recovery, problem management, transitioning, database management, and project management.

Met with agency representatives and multiple internal departments to confirm data center needs and services are met. Used Project Management Professional processes to effectively lead data center projects; developed change management strategies for data centers; accomplished change management planning to implement processes; initiated all agency change management processes from products and services; addressed any agency-supported incidents. Supervised all project personnel; conducted annual disaster recovery tests and lead annual capacity management processes to include items such as budgeting and forecasting for the needs of multiple state agencies. Developed service level agreement (SLA) strategies, co-authored service level agreements, and service level objectives. Managed successful Data PowerHouse (DPH) migration of major Commonwealth agency from legacy system to new system as Project Leader for nine months; spearheaded 20 person team in replacing an outdated agency IBM SAN and correcting a longstanding outage history; led team of 25 employees in replacing multiple open system environments, by moving quickly to replace an average of 14 systems per environment with no impact to current operations; upgraded Commonwealth agencies to Windows 2003, including 16 enterprise servers; provided training to user community, conducted risk assessment of each agency, implemented migration to prevent implementation impacts, and conducted an incident free upgrade; resolved communications gap; confirmed all parties involved in the 2006 – 2008 DPH Capacity Planning initiative received required information and updated processes to make sure that information flow continued for all future planning activities. Directed and championed the effort to sign the first Commonwealth agency, among 21, to add a security baseline of 30+ servers; conducted several successful meetings to tailor security processes to the agency culture; followed up after implementation to gather lessons learned and document best practices for the remaining agencies; shortened the implementation timeline by 15 percent; honored with the 2006 Silver Recognition Quarterly Award for outstanding customer service.

IT Resource Manager 2004 – 2005

Led process creation for 13 Commonwealth agencies, focused on providing change management resource allocation performance reporting, capacity planning, contractual requirements, and incident reporting for data centers. Managed daily technical support team operations, including problem tracking and resolutions. Used Remedy Action Request System Enterprise and HP Open View Management; periodically supervised over 20 employees; recorded baseline data to verify accurate data center service level agreements and objectives; handled contractual obligations, conducted analysis, created problem management procedures, and maintained customer relations;

Improved response times by 25 percent and determined processing deficiencies by conducting agency transaction response time analysis; helped Unisys to pass annual SAS70 inspection by enhancing three SAS70 control objectives; created more shared responsibility and accountability for 23 Commonwealth agencies by revamping a deficient change management system.

ENDRESS+HAUSER, Alexandria, Virginia 2001 – 2003

Supplier of measuring instruments and automation solutions for industrial engineering industry.

Advanced Systems Group Manager and LAN Manager

Delivered advanced technical support for multiple interfacing DESC fuel databases that supported global

fuel transactions; spearheaded team of 12 senior analysts to troubleshoot fuel transactions and process customer issues; coordinated with government officials and provided team guidance; Employed Oracle and Microsoft SQL to troubleshoot and resolve transaction issues; served as Microsoft LAN administrator and supported 15 office personnel and one worldwide training center; provided in-depth analysis while heading the Washington, D.C. office and provided support to government Fuels Automated System clients.

Solved 90percent of advanced technical issue and fielded more than 100 per month; improved services to 15 employees by 40percent by incorporating LAN and private branch exchange telephone system infrastructures; transitioned 10 percent% of unresolved technical issues to software development for resolution.

Upgraded 30 training center desktops from Windows 2K to 2003; chosen as the 2002 subject matter expert from among a team of 20 advanced analysts.

United States Air Force, Various Worldwide Locations 1979-2001

Worldwide military operations – Positions Held

Managed information technology departments; handled software development, maintenance, transaction and batch processing, and scheduled and reports processing; confirmed data security, created and updated databases, and originated corporate systems; programmed in business-oriented language and mainframe proprietary languages; handled multi-domain LAN/WAN. Charged with acquisitions, policy writing, quality assessments, storage and distribution, item management, and asset accounting; verified inventory control, maintained records, and monitored inventory levels; supervised up to 1,200 people; led diverse teams and managed wide-ranging projects.

Served in multiple positions in the ranks of E1-E8, including Logistics Group Computer Support Manager, Squadron First Sergeant, Chief Management and Systems Flight and Chief Computer Operations Element; elected as 1 of 4 1995 NCO Academy Speech Presentation finalists among a field of 150 graduates; received numerous awards, including an Air Force Achievement Medal, two Air Force Commendation Medals, two Air Force Meritorious Service Medals and more.

Career Note

Additional current employment includes 14+ years as an Adjunct Professor (course concentration: Java and C++ programming and introductory computer curriculum) with the University of Maryland University College, Asia Division. Full details available on request.

Education

- Master of Arts in Administrative Management
  - Bowie State University, Mildenhall Air Force Base, England
- Bachelor of Science in Computer Information Systems
  - Chapman University, Orange, California
- Associate of Applied Science in Logistics Management
  - Community College of Air Force, March Air Force Base, California
- Associate of Applied Science in Information Systems Technology
  - Community College of Air Force, Mildenhall Air Force Base, England

Certifications

ITIL V3 Foundations Examination

UNISYS

[redacted]
Change Analyst

Key Skills and Knowledge

- ITIL Foundation Certification (2012)
- Help desk supervisor, customer liaison, change manager, and lead analyst
- Computer Operations for multiple shifts
- Project budget oversight
- Supported the Pennsylvania Child Support Enforcement System
- Generate daily/weekly/monthly operations reports
- Relayed day to day activities of Operations during meeting to senior management
- Prepared work schedules
- Performance reviews for the staff.

Skills Summary

Over 27 years of experience providing data center analysis, change analysis, and support for senior leaders; strong experience with Remedy Information Technology (IT) Services Management, Windows Office suite, Excel, and PowerPoint. Numerous certifications for change management software and resource tracking software; versed in time management and personnel management; ITIL Foundation Certification (2012); multiple certifications and training in job specific computer related skills.

Employment History and Related Experience

Unisys, Harrisburg Pennsylvania 2003 – Present

Data Center Analyst

Data center analyst supporting several projects such as help desk supervisor, customer liaison, change manager, and lead analyst.

Oversaw day to day activities of the Help Desk staff liaison between Unisys and IBC help desk staff while Help Desk Supervisor. Managed active change issues for services; supported change process procedures and updates; provided all training for help desk staff; provided decisions on day to day issues that arise with regards to Help Desk issues; set up reporting procedures to accurately track change processes through closure to make sure the Commonwealth is informed on the status of their changes.

Worked in partnership with agencies to understand and anticipate their business needs as customer/agency liaison; worked closely with the customers to make sure all product concerns and problems are addressed and all daily batch procedures are completed; confirmed operations are informed of all changes of customer product schedules, maintained oversight of change issues, coordinated deployments, and special requests. Held weekly teleconferences with each customer/agency to go over scheduled events, changes, and concerns; examined future plans and coordinated changes with affected parties to mitigate impacts; gathered status on changes that had issues; worked with technical staff and management to resolve issues within 60 days resulting in improved coordination of change and increased accuracy of products; provided configuration and training (including products and services) for members of the Data PowerHouse (DPH) and responsible for and Unisys Global Change Management Process while ITSM7 Change Manager.

Coordinated and recorded all production support staff availability as Lead Analyst; evaluated impact of staffing availability on future production, established mitigations, and coordinated staffing changes with affected organizations; maintained Staff Agency assignments within the Data PowerHouse contract; provided back up to Lead Analyst and agencies for support and expertise as resource management support within Data PowerHouse; maintained reports, conducted meetings, and supported Data PowerHouse Service Delivery Manager.

Unisys Corporation, Harrisburg, Pennsylvania 1999 – 2003

Computer Operations Supervisor,

Supervised computer operations, data control and operations support functions for multiple shifts and planned, coordinated and evaluated the production of staff members

- Responsible for problem/change management as related to Computer Operations procedures and control mechanisms
- Evaluated service and product issues for change implications and oversaw the administration of change issues to confirm coordination of change strategies and change planning
- Monitored Commonwealth systems to verify their processes were running smoothly on their systems. Notified appropriate personnel to investigate the issues that arose to eliminate any down time to the agency
- In charge of advising and coordinating change issues with senior level management for topics such as services provided or products generated
- Work in collaboration with other work units to coordinate work activities, collaborated on procedures, and controlled the implementation of changes to daily operations and services.

Lockheed Martin, Harrisburg Pennsylvania 1997 – 1999

Operations Manager

Responsible for Computer Operations for multiple shifts, maintained the budget for the project, and managed 15 staff members

- Supported the Pennsylvania Child Support Enforcement System implementation team that started the Child Support Enforcement System within the Commonwealth Data PowerHouse.
- Created all documentation needed to verify the system was monitored accurately and efficiently
- Provided daily/weekly/monthly reports of operations to management
- Coordinated day to day plans and activities for operations during meetings with senior management
- Collaborated on business strategies to implement change
- Prepared work schedules and performance reviews for the staff supervised by Ms. Villarreal.

Unisys Corporation, Harrisburg Pennsylvania 1985 – 1999

Order Entry Specialist,

Generated sales orders of equipment for customers, received customer orders from Sales Staff, and reviewed customer orders for pricing accuracy

- Verified orders were received from agencies via tracking shipment and delivery
- Provided daily/weekly/monthly reports of customer orders.

Unisys Corporation, Harrisburg Pennsylvania, 1980 – 1985

Administrative Secretary,

Secretary for customer engineering branch manager; processed and paid department expenses, and balanced financial books for billing.

- Processed local CEs (106) travel expenses (weekly)
- Submitted paychecks to CEs
- Dispatched CEs to service locations
- Ordered Office Supplies
- Supported other miscellaneous duties as assigned

Education and Training

Susquenita High School, Emphasis on Business

Unisys Training courses:

- Remedy
- Change Management
- Personnel Management
- Windows Office suites
- ITIL Certified

Certifications

- ITIL Foundation Certification (2012)

UNISYS

[redacted]
Agency Account Manager

Key Skills and Knowledge

Project and Program Management

- Proposal Development
- Scope Management
- Time Management
- Cost Management
- HR Management
- Communications Management
- Risk Management
- 3rd Party Management
- Procurement Management
- Documentation

Professional Association

- Certified Project Management Professional by Project Management Institute (1279344)
- Member of the Project Management Institute (1080310)
- ITIL V3 Foundation (March 2012)

Awards

2012 Outstanding Leadership and Innovation ("Ollie") award winner for participation on Mobile Video Recorder project for the Pennsylvania State Police

Domain Expertise & Solutions

- Public Sector
- Infrastructure

Security Clearance

Pennsylvania State Police

Skills Summary

Since 2002, working with the Commonwealth Pennsylvania Office of Administration, Office of Information Technology, in Harrisburg, Pennsylvania. Since 2005, working on site at the Commonwealth Technology Center as a project manager and client services manager, often delivering on both roles simultaneously in very close collaboration with the CTO, CISO, Client Management, Enterprise Data Center, Enterprise Networking and Security, Enterprise Services, GIS, PMO, and many agencies. Developed and introduced customer satisfaction program for the Enterprise Data Center that continues today under Enterprise Services as an important component of OIT's process for continuous improvement and building strategic relationships while facilitating regular communications and acted as a liaison for OIT with the CIOs for half of the agencies, including AG, DLI, DOR, and PSP through describing the center's managed services programs, facility services, and benefits.

Worked at Unisys world headquarters in Blue Bell, Pennsylvania, delivering under a range of roles, including corporate communications, marketing, public relations, and sales; directly supported the president of Unisys global customer services division; joined Unisys in 1989 upon graduation from Temple University with Master's degree in Journalism.

Communications, customer service and satisfaction, facilitation, infrastructure, project and program management, and strategic relationship building are common threads for more than a decade working with the Commonwealth and more than 20 years working for Unisys.

Employment History and Related Experience

Commonwealth of Pennsylvania Technology Center. March 2012 – Present

Project Manager

A member of the Commonwealth's Program Management Office (PMO), responsibilities include project management for Enterprise Services, web hosting environment, networking and security, and coordination and stakeholder communications for operational and project activity for select state agencies. All project deliverables and objectives were achieved with high customer satisfaction, one project yielded Commonwealth CIO recognition and an award for leadership (the Ollie award), and other projects culminated with accolades from an agency CIO and other Information Technology (IT) managers.

Commonwealth of Pennsylvania Technology Center Web Hosting June 2008 – March 2012

Client Service Manager

Project responsibilities included management of the client service management program, service management for assigned state agencies, management of assigned projects, and development of monthly reports for the Commonwealth's CTO. Mr. Cavanaugh's work included creating a client satisfaction program – a first for the data center – including establishment of metrics and processes, introduction to agencies, delivery and continued refinement of processes and services. The program has been successful in improving relationships between the data center and agencies, identifying and resolving isolated and programmatic issues, and opening a new line of communications between the Office of Administration Office of Information Technology and the agencies it serves.

Commonwealth of Pennsylvania, Pennsylvania State Police, CLEAN March 2008 – June 2008

Project Coordinator and Documentation Specialist

Project responsibilities were focused primarily on project initiation and execution. Activities included setting up team room and related processes, drafting many of the project documents, including the project management plan and subsidiary plans, and coordinating schedules and resources for testing. The work was instrumental in helping the lead project manager quickly initiate this large and complex project across project teams and resources from Unisys, the customer, and several vendors.

Commonwealth of Pennsylvania, Office of Administration,
Showcase October 2008 – October 2009

Project Manager

Project management responsibilities included project initiating, planning, executing, monitoring, controlling, and closing. Project scope included setting up and executing a media relations program to increase awareness of the Commonwealth's IT initiatives and successes to create a positive public image. The activity resulted in widespread recognition for the Commonwealth, including articles in prominent industry publications and a prestigious award for the Commonwealth's CIO.

Commonwealth of Pennsylvania, Department of Revenue (DOR), Customer Service Planning October 2008 – December 2008

Project Manager

Project management responsibilities included project initiating, planning, executing, monitoring, controlling, and closing. Project scope included the analysis of DOR's customer interaction points with the objective of identifying issues and recommending ways to improve customer service. The project was completed on time with the intended results, providing DOR with visibility on how it can improve customer service.

Commonwealth of Pennsylvania, DLI UCMS Portal
Implementation June 2007 – October 2008

Project Manager

Project management responsibilities included monitoring and controlling project work, managing communications, documenting issues, and coordinating activities between the Office of Administration and OA and Department of Labor and Industry. Project scope included the implementation of a portal (staging and production environments) in OA's Enterprise Server Farm for DLI's new application for unemployment compensation. All project deliverables and objectives were achieved with high customer satisfaction.

Commonwealth of Pennsylvania, Microsoft Exchange 2007
Migration March 2008 – September 2008

Project Manager

Project management responsibilities included monitoring and controlling project work, administering the project plan, and managing stakeholder communications for IT managers at 47 Commonwealth agencies. Project scope included migration of 80,000 mailboxes to a new Microsoft Exchange 2007 messaging infrastructure, the largest such migration in North America at the time. All project deliverables and objectives were achieved with high customer satisfaction.

Unisys Corporation, Bid Capture April 2007 – March 2008

Project Manager

Project management responsibilities included project initiating, planning, executing, monitoring, controlling, and closing relevant to human resource demand planning and responding to client solicitations. The work resulted in producing quality proposals on time and within established budgets.

Commonwealth of Pennsylvania, Enterprise Server Farm, Public Sector, Web Application Hosting and Messaging September/2002 – March 2007

Project and Performance Manager

Project management responsibilities included cost, scope, human resource, and procurement management for 26 full-time resources. The Enterprise Server Farm consisted of more than 600 servers and 200 Web-facing applications. It also included Microsoft Exchange and Active Directory for email and directory services to 80,000 Commonwealth employees and contractors.

Commonwealth of Pennsylvania, Keystone Building Project, Public Sector, Infrastructure Management, April 2004 – March 2007

Project and Performance Manager

Project management responsibilities included project initiating, planning, executing, monitoring, and controlling, with emphasis on integration, scope, cost, quality, human resource, communications, and procurement management. The Keystone Building project included management of a complex switched campus network infrastructure supporting five Commonwealth agencies. The infrastructure included Nortel switches, Cisco routers, Checkpoint/Nokia firewalls, and servers from several manufacturers. The project was transitioned and managed as required by the contract.

Commonwealth of Pennsylvania, State Police, Public Sector, Security Assessment, May 2005 – July 2005

Project Manager

Project management responsibilities included project initiating, planning, executing, monitoring, controlling, and closing with emphasis on integration, scope, time, cost, quality, risk, and communications management. Unisys used manual methods and automated tools to identify known vulnerabilities in the Commonwealth's Police networked environment and recommended strategies to transfer, minimize, accept, and eliminate risk associated with those vulnerabilities. Due to rules associated with federal funding the team was under considerable pressure to complete the project by the end of the fiscal year. Unisys compressed the schedule and added resources to meet the client's deadline. Unisys response to this challenge was recognized at the highest levels of the agency.

Telcove, CP/CPS for Pennsylvania. Office of Administration

Public Sector, Consulting May 2005 – September 2005

Project Manager

Project management responsibilities included project initiating, planning, executing, monitoring, and controlling with emphasis on integration, scope, time, cost, quality, risk, and communications management. Working as a subcontractor to Telcove, the Commonwealth's primary telecommunications supplier, Unisys led a project to develop a Certificate Policy (CP) and Certification Practice Statement (CPS) for the issuance of Verisign Certificates supporting an enterprise VPN solution for Commonwealth employees and contractors.

Unisys, Managed Voting, Public Sector, Managed Voting Services for Pennsylvania Counties March 2005 – November 2005

Program Development Contributor

Unisys developed a services program to assist Pennsylvania counties with compliance to the U.S. Help America Vote Act, which requires a complete replacement of most voting technology in the U.S. by April 2006. Unisys' program included consulting, deployment, outreach, and training services as well as new voting technology solutions from AccuPoll Systems. Responsibilities included the definition of communications and training requirements and development of related solutions, pricing and proposals.

Telcove, VPN Pilot for Pa. Office of Administration

Public Sector, VPN Consulting January 2005 – June 2005

Project Manager

Project management responsibilities included project initiating, planning, executing, monitoring, controlling, and closing with emphasis on integration, scope, time, cost, quality, risk, and communications management. Working as a subcontractor to Telcove, the Commonwealth's primary telecommunications supplier, Unisys provided a suite of services for the implementation of a VPN pilot using Verisign certificates for Pennsylvania's Office of Administration and State Police. The project entailed the configuration and installation of Cisco VPN technology and integration with Commonwealth and Verisign systems for the issuance of certificates for the Pennsylvania State Police VPN users.

Unisys, Commercial, Sales April 1997 – August 2002

Portfolio Sales Executive

Responsibilities included identification, qualification, and winning of new business in the corporate network and desktop services marketplace. Targeted national and multinational companies with 3,000 to 50,000 employees. Leveraged competitive differentiators and industry partnerships to gain competitive advantage. Exceeded annual quotas for revenue, margin, and customer satisfaction.

- 1998 North American Salesman of the Year
- Achieved quota for four consecutive years
- Exceeded 200 percent of quota in 2000

Unisys, Corporate, Marketing June 1994 – March 1997

Manager of Public Relations

Managed U.S. public relations efforts for $2 billion customer services division, supporting new product offerings, customer meetings, and executive communications.

Unisys, Corporate, Marketing October 1989-May 1994

Editor of Marketing Communications

Develop communications plans and create brochures and other marketing materials for

Unisys customer services division. Create, edit, and publish Unisys NewsNet, a daily internal employee newsletter.

Education

Master's Degree, Journalism, Temple University, July 1990

Bachelor's Degree, Liberal Arts, Franklin & Marshall, May 1983

Professional Certification

- □ Project Management Professional
- □ ITIL V3 2011 Foundations

Professional Training

Project Management Professional (PMP) Certification Prep (PMBOK® Guide -Third Edition-aligned)

Project Cost Management (PMBOK® Guide -Third Edition-aligned)

Project Scope Management (PMBOK® Guide - Third Edition-aligned)

Project Integration Management (PMBOK® Guide - Third Edition-aligned)

Project Time Management (PMBOK® Guide - Third Edition-aligned)

Project Management Essentials (PMBOK® Guide - Third Edition-aligned)

Project Risk Management Workshop

Project Feedback Program

ITIL Foundations

Internet Security: An Overview

Unisys Six Sigma Lean White Belt

Financial Requirements and Setup for Project Managers

Project Reporting for Project Managers

Revenue, Invoicing, and Costing Concepts for Project Managers

Introduction to 3D-VE and 3D Blueprinting

3D-VE Infrastructure Modeling and Traceability

Introduction to Business Architecture At Unisys v2.0

Getting Started with Rational(R) RequisitePro(R)

Principles of Modeling

Principles of Rational Unified Process

Getting Started With Rational ClearCase® v2002

Introduction to Business Blueprinting

Managed Services

UNISYS

[redacted]

Agency Account Manager

Key Skills and Knowledge

- 28 years of experience -Fortune 500 Business Process Outsourcing Arrangements
- Technical and non-technical solutions support for CoPA Data PowerHouse.
- Change, Incident and Release Management
- Extensive project/program management experience.
- Large scale Infrastructure Technology (IT) management systems to include ITSM
- Support of operational business process re-engineering, to include go/no go decisions.
- Built strong technical alliances with application support teams for primary, secondary and tertiary software solutions.
- Excellent interpersonal, interviewing, customer service and general communication skills.
- Impact & Gap Analysis, managing issues and risks, and time management.

Communication and Networking

- American Business Women's Association
- Cambridge Business Who's Who in America

Office Productivity Tools

- Microsoft Project Plan
- Microsoft Suite
- Remedy ITSM7.6

Skills Summary

Over 28 years of experience in Fortune 500 business process outsourcing arrangements for both technical and non-technical solutions for the Commonwealth of Pennsylvania; extensive experience in program management, project management, change management, incident and release management, and large scale infrastructure Information Technology (IT) management systems including ITSM; d demonstrated ability to build strong technical alliances with application support teams for various levels of software solutions; Skilled with impact and GAP analysis and risk and time management.

Employment History and Related Experience

Unisys Corporation

Commonwealth of Pennsylvania – Data PowerHouse Project, Harrisburg, Pennsylvania

Provide liaison support to Commonwealth IT Departments as a Service Delivery Manager (SDM) for the following Data PowerHouse (DPH) Agencies: Pennsylvania State Police, Department of Environmental Protection. Department of Health, Pennsylvania Game Commission, Department of State, Pennsylvania Liquor Control Board and the Public Utility Commission. Provide secondary coverage for the following DPH Agencies: Department of Public Welfare, Department of Aging, Department of Insurance, Integrated Enterprise System, and the Department of Revenue – Integrated Tax System.

As a liaison between the DPH and the agency providing data center support for all infrastructure changes, service requests, post release management discussions and incident management resolution. Developed strong partnership with the agency leadership to meet business needs of the agency and balance them with business objectives. Assist organizational units with executing policies and procedures as outlined in the contract, manage policies and procedures through coordination with the Project Management Office.

Identified change order sales opportunities during Business Collaboration Meetings held with the agency; managed the business statement, solution objective, change order presentation, final review, and signing of documentation. Administered change orders sales for the current DPH engagement to include:

- Calendar year 2008 change order sales - $138,500
- Calendar year 2009 change order sales - $6.4 million
- Calendar year 2010 change order sales - $8.6 million
- Calendar year 2011 change order sales - $1.096 million
- Calendar year 2012 change order sales - $570,000.

Currently providing subcontractor oversight for an environment deployed at the DPH. Deployed an Open Systems platform for the Pennsylvania Liquor Control Board, Department of Health, and other hardware upgrades for the Department of State; improved flexibility for application upgrades.

Provide project management coordination to ensure successful planning and implementation of assigned activities; actively collaborates with agency; ensures cost, schedule, and performance metrics are collected, analyzed, and reported.

Special assignments include the management and oversight of the ITSM7.6 application for the DPH. As the liaison for the DPH to the NAEC Team off-shore, coordinate all incident, change, and global modifications to the project team.

Non-Unisys Experience

Affiliated Computer Services, Inc.

Government Health Services Outsourcing

Account Manager for ACS, Inc. contracted with the Department of Public Works (Harrisburg, Pennsylvania) to provide Medicaid Managed Care health maintenance organization enrollment services implemented of the following savings:

- Consolidated Mailroom services with other ACS accounts in the area, realizing a savings $75,000 a year

- Reformatted the Enrollment Broker notification card from a flat rate postage and printing to a post card, realizing a printing and postage savings of over $800,000 per year
- Consolidated the telephone system with a regional Avaya investment, realizing savings in maintenance costs.

Director of Implementation/Special Project for ACS, Inc. (d.b.a.: Texas Medicaid Healthcare Partnership; Austin, TX); contracted with Texas Department of Health and Human Services to provide Medicaid Management Information Systems (MMIS) program management.

- Delivered savings of $1.5 million per year over a five year fixed fee contract, to provide all Texas Medicaid providers with an Explanation of Benefits via a secure website and all Texas Medicaid payments via electronic funds transfer, thus eliminating all printing, envelope, postage, and UPS costs for mailing to over 85,000 providers
- Migrated electronic publications for Texas Medicaid to a secure website; saved the project millions in printing and postage. Accelerated updates of Federal programming information from annual to semi-annual; provided updated information to Texas Medicaid providers in a timely manner
- Improved business processes with the Ambulance, Dental, and Durable Medical Equipment and improved staffing efficiencies and improved relations with these active provider organizations.

Foundation Health, A Texas Health Plan

Government Services

Director of Medicaid and Program Compliance contracted with the Texas Department of Health and Human Services. Supplied a contracted provider network for Medicaid managed care enrollees with primary care providers, specialists, and a viable hospital network.

Austin/Travis County Health and Human Services Department – FQHC

Public Health Department

Business Services Coordinator; integrated public health (W.I.C., V. F.C.) with the Federally Qualified Health Center delivery model; included full service pharmacy, radiology, and basic specialty services.

Employment History

2007 – Present	Unisys Corporation, Harrisburg, Pennsylvania
1998 – 2007	Affiliated Computer Services, Inc., Austin, Texas
1997 – 1998	Foundation Health, A Texas Health Plan, Austin, Texas
1994 – 1997	Austin/Travis County Health Department, Austin, Texas
1988 – 1994	El Rio Health Center, Tucson, Arizona
1987 – 1988	Maxicare HMO Representative, Tucson, Arizona
1986 – 1987	Total Business Systems/Blue Cross – Blue Shield, Albuquerque, New Mexico
1980 – 1986	The Equitable Life Assurance Society, Medicare Part B Administrator, Albuquerque, New Mexico

Education

Business Administration, Business, Tucson University 1994

Certification

ITIL V

UNISYS

[redacted]
Agency Account Manager

Key Skills and Knowledge

- Customer Relationship Mgmt.
- Service Delivery Management
- IT Infrastructure Design
- Enterprise Computing Technology

Project and Program Management
- PMO and Project Management
- Complex project planning
- PMI Certification
- Financial Analysis & Cost Mgmt.
- Procurement & Contract Mgmt.

Service Delivery Operations
- Human Resource Mgmt.
- SSAE-16 Audit
- Service Level Management
- ITIL Foundations Certified
- Process Management
- Security and Compliance

Organization Support
- Research and Analysis
- Management Reporting
- Staffing and Recruiting

Communication and Networking
- Wide area and local area networking, Routers, Switches
- Network Design & Implementation
- Protocol Analysis

Hardware
- Mainframe, Server, Workstation, SANs

Operating Systems
- MVS, Windows Server

Office Productivity Tools
- MS Office
- MS Project
- MS Access and Visio

Skills Summary

A diverse Information Technology (IT) manager and leader with proven consulting, technical, and business development experience who achieves quality results and delivers business value. A certified consultant, project manager, and business professional who consistently accomplishes objectives by leveraging skills in business administration, continuity planning, consultative analysis, enterprise networking, security, systems management and technology infrastructure. Based in Harrisburg, Pennsylvania, Brian has been supporting the Commonwealth of Pennsylvania for over 15 years providing technology solutions, consulting, and complex project management services.

Employment History and Related Experience

Unisys Corporation, Harrisburg, Pennsylvania — May 2006 – Present

Account Management/Service Delivery

Actively supporting a complex IT infrastructure managed services project for the Commonwealth of Pennsylvania government customer in several service delivery and business management roles since 2006, acting as a liaison to the Office of Administration and agencies receiving service. Leverages significant contract management, technical sales, and customer relationship management (CRM) experience to provide high levels of account management support.

Focused on exceptional customer service by leading teams through implementation and practice of ITIL processes and ITSM7 system. Demonstrated experience in new technology solution development and deployment by leveraging design methodologies and project management best practices to support project change orders. Provided direction and leadership for service delivery organization in support of complex solution design, implementation, managed service functions, quality improvement, and cost management activities. Continues to play a leadership role in supporting business development, contract management, and service delivery for the Program Management Office (PMO).

Computer Aid, Inc., Harrisburg, Pennsylvania — 2002 – 2006

Senior Consultant

Developed IT Strategic Plan for a 6000 person government transportation agency to align IT support of the business by focusing on process initiatives, systems and best practices. Created Business Continuity/Disaster Recovery plans for three state government agencies providing over $750K in services revenue.

IBM Global Services, Mt. Laurel, New Jersey/Mechanicsburg, Pennsylvania — 1997 – 2002

Principal Consultant

Led marketing and sales initiatives for professional services offerings through focus on relationship management, solution design, and pricing. Managed staffing, delivery, profitability, and customer satisfaction for $15 million portfolio of IT service contracts for application development, consulting, and systems integration offerings.

Directed team of eight consultants, architects, and IT specialists through full life cycle of complex TCP/IP enterprise network design and implementation for a large Commonwealth of Pennsylvania government agency. Engagement exceeded client expectations and resulted in over $1.6 million of IBM services revenue.

GBC/Globelle, Inc., Berlin, New Jersey — 1995 – 1996

Director of Operations

Supervised five person product management staff in selecting, purchasing, marketing, and managing $4 million networking and midrange computer product inventory. Increased revenue from $6 million to $15 million in nine months by designing and implementing effective asset management, marketing, and sales programs.

Comdisco, Inc., Woodcliff Lake, New Jersey — 1995

Network Consultant

Installed, configured, and tested multi-vendor internetworking infrastructure enhancing campus and enterprise connectivity for a large regional telecommunications carrier.

IBM Corporation, New York, New York 1981 – 1994

Marketing Operations Consultant 1992 – 1994: Conducted market analysis of customer IT expenditures and contributed to development of targeted $5 billion annual business plans for Northeastern region.

Systems Engineering Manager 1990 – 1991: Managed eight person technical team providing quality technical/sales support of IBM products to satisfy the needs of a regional telecommunications carrier, increasing revenues by 10 percent to $35 million.

Lead Systems Engineer 1987 – 1990: Directed technical and marketing activities of 12 systems engineers providing account support for a global financial services company. Developed plan and led team in the installation of $9 million mainframe/storage complex providing 25 percent system capacity growth for application deployment.

Sales Representative 1985 – 1986: Developed and executed sales strategies for midrange, workstation, and communications products resulting in 15 percent increase in revenues and improved customer awareness of product capabilities.

Account Systems Engineer 1981 – 1984 - Led implementation of SNA network protocol conversion project for an international financial services firm reducing line costs by 75 percent while improving transaction response time by 10 percent.

McDonnell Douglas Automation Company, St. Louis, Missouri 1979 – 1981

Network Analyst

Completed installation and testing of IBM terminal and data communications hardware/software systems for national network of 30 communications controllers and 10,000 workstations for aerospace firm.

Education

- M.S., Information Systems, Penn State University, Harrisburg, Pennsylvania – Completion 5/2013
- M.B.A., Marketing, Rutgers University, Newark, New Jersey
- B.A., Computer Science/Economics, State University of New York – Potsdam, New York.

Professional Certifications

- ITIL V3 Foundations Certification
- PMP – Project Management Professional Certification
- IBM Certified Consultant.

UNISYS

IBM

[redacted]

Agency Account Manager

Key Skills and Knowledge

- Project Management for IT projects
- IBM z Series and iSeries technical skills
- Support of Disaster Recovery processes
- 14 years of experience providing services to the Commonwealth of Pennsylvania
- Agency knowledge

Skills Summary

Proven Information Technology (IT) Manager with 14+ years experience with the Commonwealth of Pennsylvania located in Harrisburg, Pennsylvania area. Expertise include z Series and iSeries technical management; support of the Disaster Recovery (DR) process, including the development of DR plans and the coordination of DR exercises and relationship management.

Employment History and Related Experience

IBM Corporation - Harrisburg, Pennsylvania 2002 – Present

Data PowerHouse Service Delivery Manager

Service Delivery Manger on the Data PowerHouse (DPH) contract in Harrisburg worked with agencies of the Commonwealth of Pennsylvania for the past 12 years managing projects to include developing the technical plans, working with major stakeholders to develop time lines and communications plans, coordinating agency and IBM resources in implementing such plans, and performing post-project follow-up and communications.

- Created the disaster recovery plan for IBM-supported agencies at the DPH data center. During the past 12 years, coordinated all of the disaster recovery tests, was responsible for all phases of disaster recovery at PennDot, L&I UC, Department of Revenue, SWIF, L&I BOIS, DOI–MCARE, DOC, and zVM/VSE Liquor Control Board which demonstrated that the systems were recoverable and that the restore point objectives and the recovery time objectives were met in each test.
- Managed system migrations and upgrades to new hardware at PennDot, L&I UC, Department of Health, SWIF, Liquor Control Board, Department of Corrections, L&I BOIS, State Civil Service Commission, and the Department of Aging by creating plans that minimized down time and impact to the agencies. Migrations and upgrades were completed on time, within budget, and with high levels of stakeholder satisfaction.
- Managed resolution of technical issues and software upgrades for zOS, DB/2., CICS, IMS, iOS, zVM, VSE for PennDot, L&I UC, State Workers Insurance Fund, Department of Health, Department of Education, State Civil Service Commission, Department of Aging, and L&I BOIS. Changes were completed successfully within the change window.
- Worked with PennDot in the implementation of a zLINUX environment on their mainframe by developing requirements, providing change orders to acquire appropriate software/hardware/services, and coordinating the IBM technical resources to support the zLINUX environment. At the end of the project, the customer was able to migrate to the new technical environment without incident. The environment has afforded the agency a very stable environment. There have been no service outages since going live with production and has provided a stable platform for additional applications.

Performed as Service Delivery Manager and DPH agency liaison to PennDot, L&I UC, SWIF, Department of Health, Department of Corrections, Department of Education, Liquor Control Board, Department of Aging, State Civil Service Commission, L&I BOIS.

- Provided overall support of the DPH contract and managed the delivery of services to the agencies, which included understanding agency business and technical environments and delivered the appropriate contracted service. Yearly customer satisfaction surveys for agencies managed have exceeded assigned satisfaction targets.
- Worked with agency CIOs to identify opportunities for cost savings or improved agency efficiencies using IBM's latest technology. Projects and solutions included: L&I UC migration from CNT to IP printing solution, Department of Insurance iSeries DR solution, L&I UC contract extension, DOC contract extension, and SWIF contract extension.
- Assisted the agencies with problem management, created solutions to problems, and drove to successful resolution. Over the years, these agencies have in total attained service level commitments.
- Worked with agencies to develop business solutions, created contract change orders, and implemented changes into the technical environment.
- Developed capacity plans to identify requirements, provided hardware solutions for such requirements,

created the contract change order, and implemented the solutions once the contract change order was signed.

IBM Corporation 1976 – 2002

Various Positions

- Disaster Recovery Coordinator Manager for Commonwealth of Pennsylvania DPH contract – Harrisburg, Pennsylvania 1999 – 2002
- AS/400 Marketing Specialist – Central Pennsylvania 1992 – 1999
- Systems Engineering Manager – Central Pennsylvania 1987 – 1991
- Area Information Specialist – Mid Atlantic Area 1985 – 1987
- Systems Engineer – Reading, Pennsylvania 1976 – 1985

Education

- BS Mathematics, Albright College 1971 – 1975
- MBA, Rutgers University 1975 – 1976

UNISYS

[redacted]
Agency Account Manager

Key Skills and Knowledge

- Project Management
- Systems Design & Integration
- Application Development
- ITIL

Domain Expertise & Solutions

- Application/Server Hosting
- Datacenter Management

Project and Program Management

- Requirements Definition
- Systems Implementation
- Application Development and Design

Databases

- SQL Server 2000
- SQL Server 2005
- SQL Server 2008
- Access
- Oracle

Operating Systems

- Windows NT
- Windows 2000
- Windows 2003
- Windows 2008

Programming Languages & Tools

- SQL
- Visual Basic
- VB Script
- JavaScript
- C
- C++
- VC++
- ASP
- VB.Net
- ASP.Net
- XML
- HTML
- ADSI
- LDAP
- CDO
- Biztalk Server
- Application Center

Security Clearance

- PA State Police
- PA Department of Corrections

Located in Harrisburg,

Skills Summary

Over 15 years experience as an Information Technology (IT) professional with experience in project management, project coordination, system study, design, development, and Implementation; held numerous positions of progressive responsibility including programmer and senior technical lead; has a broad understanding of the service catalog offered for the Data Center Modernization contract. Joined Unisys as a consultant in October 2000 with current position as Service Delivery Manager which involves managerial and technical leadership of consulting staff at the Commonwealth of Pennsylvania, including system engineers, network engineer, and developers.

Employment History and Related Experience

Unisys, GMS, Service Delivery Manager 2007 –-Present

Manages all aspects of Enterprise Data Center (EDC) portion of the Commonwealth of Pennsylvania Contract – including Client Relations Management (CRM) (liaison role) and P&L for account valued at over $6 million per year.

- Strong advocate and champion for the use of services as a technology solution. Works with IT and business to form the best approach when selecting services to resolve a business need; responds to Commonwealth strategies with design and architecture solutions to achieve commonwealth objectives.
- Leads and manages Unisys employees and contractors supporting the Data Center projects.
- Designed and implemented the infrastructure for the Pennsylvania State Police Megan's Law application that provides the public information on sexual offenders. Unlike other state's that launched the website earlier, Pennsylvania's public launch by the governor was very successful and the infrastructure was able to support the extremely high load during the initial days of the launch.
- Designed and implemented the infrastructure for the migration of the Pennsylvania Lottery website from an external hosting location resulting in highly reliable hosting with considerable cost savings for the Commonwealth of Pennsylvania.
- Built strong collaborative relationships and idea exchanges to maintain strategic alliances with key members of the Commonwealth.
- Delivered regular briefings for new services and technologies to the Commonwealth to confirm awareness of emerging ideas.
- Reviewed and briefed the Commonwealth of Pennsylvania on managed PKI solutions by Entrust. Implementation resulting in cost savings to the Commonwealth and reduction of manual effort.
- Coordinated with Unisys account team to conduct presentations on BMC ITSM and Secure Private Cloud.
- Key contributor to the success and development of processes and services for the Commonwealth. These processes streamlined and standardized operations and made sure that there was consistent service delivery, proactive problem prevention, and timely incident resolution.
- Gathers together the best of Unisys engineers to develop cost assessments for recommended solutions, define the support required, and develop the long term operational strategies to insure that real value is delivered to the Commonwealth.
- Design and implement data center deployment process that standardized the new applications integration process.
- Design and implement managed services Lite-hosting model. This met and exceeded the customer's expectation of a hosting model where they have control and at the same time benefit from EDC's standard services.
- Track contract adjustments and work orders to verify that agreements are supported, progress, reviewed, discussed, and finalized as all parties come on board and confirms that signatures are in place to solidify the agreement.
- Processed change orders to provide additional resources to meet the Commonwealth of Pennsylvania's staffing requirements for Disaster Recovery project.
- Process change orders to provide skilled resources for the implementation of BMC products procured by the Commonwealth of Pennsylvania.

Pennsylvania

Public Sector, Commonwealth of Pennsylvania, Data Center Hosting 2007 to Present

Operation architect, project manager, customer liaison for Pennsylvania's Enterprise Data Center. Supported strategic relationships and straightforward exchanges of ideas and innovations for the good of the Commonwealth.

- Played a large role in architecting an E-Government data center server farm for the Commonwealth to host web applications for the various agencies. Managed a team of 34+ consultants and collaborated with 40+ agencies in their successful application deployment and operation. Infrastructure data center scope includes more than 4,000 servers and 800 applications and provides a wide range of solutions from various vendors including Microsoft, Linux, Cisco, IBM, and VMware.
- Functioned as liaison, moving ideas between the development community and the customer community to verify the needs of the Commonwealth were represented in the design and delivery of the server farm. The project was a huge success as the data center grew over the years. The Commonwealth of Pennsylvania agencies were able to leverage a centralized team of skilled resources that resulted in reduced duplication and increased cost savings.
- Oversaw the data center's operations and architecture, developed solutions for agency requirements, assisted the client with strategy development, budget management, license management, coordinated deployments of new data center applications, and supervised technical personnel. Daily tasks included managing client, agency, vendor, and team interactions, service deployments, Commonwealth collaboration and liaison activities, and project assignments.
- Accomplished costing estimates to address the value and impact of recommendations for change to existing systems. Developed the entire package including infrastructure, maintenance requirements, implementation tasks, staffing, and then benefit assessment of the project to confirm a strong value for the Commonwealth.
- Implemented various processes including incident management, release management, and change management. Developed Standard Operating Procedures and Rules of Engagement for the various infrastructure service offerings in the server farm. This experience provided a broad base of understanding for the use of services and how they can bring positive impacts to organizations. The processes provided consistent, standard, and reliable delivery of services. The team supports the highest number of exchange mailboxes with the smallest number of staff, while delivering a confirmed high percentage of system availability.
- Actively participated and contributed to the development and enforcement of various IT data center product and process standards of the Commonwealth. Designed a DR solution for critical applications in the data center. Confirmed high availability of all applications running within the data center and achieved a high level of client satisfaction.
- Significant contributor to multi-million dollar contract extension and expansion.
- Key contributor to the success of the client as a pioneer of various IT initiatives in the public sector including standardization, consolidation, and virtualization. The consolidation initiative constituted the consolidation of the IT services of multiple Commonwealth agencies into the data center. This consolidation eliminated duplication, increased consistency, and security and resulted in cost savings. The virtualization of server hardware using VMware increased system availability and flexibility, reduced the server foot print and power utilization and also resulted in quicker deployments and overall cost savings. The customer satisfaction based on periodic customer surveys was consistently greater than 90 percent.

Public Sector, Commonwealth of Pennsylvania, Data Center Hosting 2000 – 2001

Team leader and Commonwealth liaison for the operations team of Pennsylvania E-Government/Enterprise Data Center Server Farm.

- Role involved data center infrastructure design, implementation, and support of the server farm including database and web server administration. Responsible for brief services recommendations and implementation of new technologies in the Commonwealth. Regularly coordinated and collaborated with third parties and vendors to achieve successful data center results
- Architected and implemented Microsoft Active Directory, Application Center 2000, Biztalk Server 2000, and SQL Server 2000

Public Sector, Commonwealth of Pennsylvania, Application Development 1999 – 2000

Lead developer for the Commonwealth Connect project that allowed migrating all Commonwealth's Government agencies to a centralized NT Domain and MS Exchange mail system.

- Designed and developed work flow systems and scripts to automate administration of NT–and later Windows 2000–and Exchange servers using VB, VB Script, COM, CDO, ADSI, and LDAP

Commercial, Goldwire SoftWeb, Application Development, Chennai, India 1997 – 1998

Technical lead for the Software Design and Development team. Responsible for design and development of various Migration tools and products. Flash 2VB was one of the major products developed that converts FoxPro code to a Visual Basic Project. Successfully acted as project manager for many turnkey client projects. Participated in pre-sales that included demonstrating the product in various Microsoft events in India. Responsibilities included requirements analysis, architectural design, development, and implementation of projects.

Education

- Birla Institute of Technology and Science, Pilani, India, 1997
- Bachelor of Engineering (Honors) in Chemical Engineering.

Professional Certification

- Project Management Professional (PMP)
- Information Technology Infrastructure Library (ITIL) Fondations V3
- Information Technology Infrastructure Library (ITIL) Fondations V2
- Microsoft Certified Systems Administrator (MCSA) 2003
- Microsoft Certified Systems Engineer (MCSE) 2000.

Professional Training

- Project Estimating Workshop
- Project Risk Management Workshop
- Introduction to Business Architecture at Unisys
- Project Requirements Management Workshop
- Foundations of Practice Economics
- Ethics Awareness
- Essential Consulting Skills
- ITIL Foundations V2 and V3.

Volunteer Experience

- Contributed to the development of PMI “PMCD Framework – Second Edition”
- Volunteer Evaluator for: PMI Continuing Professional Education Product of the Year Award (2012) and PMI David I Cleland PM Literature Award (2011).

Awards

- Commonwealth of Pennsylvania (CoPA) Outstanding Leadership and Innovation (“Ollie”) award - 2012
- Unisys Global Silver Recognition Award July 2007
- Unisys Global Gold Recognition Award Feb 2005
- Unisys Global Silver Recognition Award Nov 2004
- Unisys Achievement Award for Excellence Dec 2001.

UNISYS

[redacted]
Agency Infrastructure Architect

Key Skills and Knowledge

- Data Center Relocation
- Data Center Architecture
- Data Center management
- Enterprise Storage
- Networking
- SAN
- ITIL
- Budgeting
- Thought Leadership
- Project Management
- People Management.

Hardware Experience

- Intel and RISC-based servers
- IBM z-Series, iSeries, p-Series and x-Series
- EMC, XIV, Avamar and Data Domain storage platforms, Cisco routers/switches
- Checkpoint & Cisco Firewalls, Brocade SAN infrastructure.

Software Experience

- Oracle Financials
- Microsoft OS
- OS2, Novell
- VMware
- Retina
- SCOM,
- BladeLogic
- Various AV tools.

Skills Summary

Over 18 years of experience as a technical manager and technology architect in global sales force effectiveness solutions for State government, local government, and pharmaceutical organizations. Four years of experience with the Commonwealth and provided leadership for large technical organizations including data center and hardware service groups. Support the production of new cost effective technology products and business offerings; managed multiple facility acquisitions, migrations, and plant consolidations; strong record of success building and maintaining strategic vendor partnerships to generate repeat business.; participant in strategic planning sessions, team building, and extensive interaction with both internal and external customers; currently providing solutions and infrastructure design for the Commonwealth of Pennsylvania.

Employment History and Related Experience

UNISYS

Client Architect 2009-present

- Worked as part of Data Center Transformation team for the Commonwealth of Pennsylvania in moving to a Shared Enterprise infrastructure model.
- Design detailed technical data center solutions in support of seventeen the Commonwealth of Pennsylvania agencies for the last four years. Solution technologies include server, mainframe, storage, networking, software, and facilities components; introduced new components to system that improved operational reliability of critical functions.
- Provide guidance and recommendation to the Commonwealth of Pennsylvania agencies on emerging technologies to increase performance, gain functionality, and reduce cost; proven track record of solution implementation success and accuracy.
- Develop and maintain business relationships with key strategic partners, including strategic planning; drive solutions to support the overall portfolio and areas of strength.
- Lead and drive results across cross-functional teams; consults with customers to gather technical and business requirements and facilitate the development of cost saving technology solutions involving multi-vendor products and systems.
- Provide technical support in the solution design; facilitate the design leading edge infrastructure solutions to satisfy requirements by leading cross-functional teams of subject matter experts; improved maintainability of data center systems.
- Manage vendor partners in the design process to obtain solution options with feature detail and costing information.

CEGEDIM DENDRITE 2007 – 2009

Technical Account Manager 2008 – 2009

- Organized and managed customer requirements for multiple accounts and main point of contact for customers.
- Facilitated custom software configuration for each customer for handheld device, web portal, and backoffice database; delivered implementation of new CRM software and upgrades ahead of schedule.

Project Manager IS 2007 – 2008

Responsible for enterprise-wide Oracle projects implementation; overall Project Manager for implementation of software to five business lines and led senior management in Steering Committee meetings. Also responsible for P &L, resources, and project plan delivery.

DENDRITE International 1997 – 2007

Director of Hardware Services 2005-2007

Managed Dendrite's $14 million hardware service operation, supported 16 pharmaceutical and biotech customers (17,000 sales force users), and managed 90 support personnel with six direct reports.

- Developed customer focused metrics to exceed customer service level agreements.
- Facilitated ISO 9001:2000 Certification; engineered facility closure and migration to new facility operations; developed and executed business plan that reduced costs by 20 percent of operating budget.

Technical Project Manager, Data Center Services 1999 – 2004

Provided project management for pricing tasks, new customer implementation tasks, and customer expansion initiatives; built project plans, schedules, and control systems to make sure the work was completed on time and under budget.

- Managed all resources and P & L for all assigned projects; created custom technology solutions for both internal and external customer; tasked by senior leadership with presenting new technology opportunities to reduce cost, increase efficiency, and increase expandability.
- Developed, positioned, and introduced remote backup business offering in partnership with third party software vendor; created cost effective shared server environment offering for small to mid-tier customers and for internal quality assurance and development environments.
- Managed multiple data center consolidation and migration projects to new facility with minimal disruption to business operations; managed day to day operations for both internal and external customers and acted as main liaison between customer and technical teams for ongoing technology projects.

Senior Systems Engineer 1997 – 1999

Oversaw Microsoft Windows and Communication groups; managed customer hosted Windows environments; gathered customer requirements and developed system architecture (Windows Server, Exchange, Novell, Unix, Cisco, SQL Server, Oracle, and NetIQ) for hosted systems; managed communications platforms (USR Total Control, Xcellenet) for customers.

CORNET International 1995 – 1997

Windows and Xcellenet Administrator

Delivered administration of customer Windows and Xcellenet environments; maintained and managed customer Xcellenet server systems and communications; created and maintained Xcellenet communications scripts for customers; managed Microsoft Windows server environments for customers.

Education

- BS – Business, Major in Marketing, Kutztown University

Certifications

- ITIL v3 Foundations

UNISYS

[redacted]

Agency Infrastructure Architect

Key Skills and Knowledge

Management

- Planning, scheduling, costing, and leading projects
- Organizing teams into cohesive groups of experts focused on the project objectives
- Coordinating and collaborating with stakeholders to verify solutions are effective.

Domain Expertise and Solutions

- Access Control
- Active Directory
- ISA/TMG Server
- IIS
- CA Site Minder
- BEA Aqualogic Portal
- Radiant Logic
- PKI.

Network Security

- CSS – Cisco Content Switches
- VPN
- Cryptography.

Databases

- SQL Server.

Project and Program Management

- MS Project.

Operating Systems

- Windows 2008/2003/2000.

Security Clearance

- PSP Background Check.

Languages

- English and Hindi.

Skills Summary

Over 14 years of experience as a Manager of the data center, systems engineering, and networking; more than seven of these last years has been in assessment and implementation of Service Catalogs, applications, servers, and security infrastructure; Microsoft Certified Systems Engineer in windows NT/2000/2003; over three years experience in managing the team and client interaction.

In depth knowledge and hands of experience on TCP/IP networking, DNS and Name Services, Active Directory-Joining Domains COM+ applications, IIS as web server and its configuration, administration and troubleshooting. Wide experience implementing high availability solutions using CSS (Cisco Content Switches), Microsoft Windows Clustering, NLB, and application center with hands on experience in designing and implementing web publishing solutions using MS ISA Server.

Insured that network security corporate policies, security service level agreements, and "best practices" standards were followed during design, installation, and configuration of ISA firewall, NAT server, and Intranet, Extranet, and Internet connections.

Project management experience in gathering the requirements, analyzing and documenting the application requirements, establishing costing for projects, coordinating projects requirements with clients, designing and prototyping the applications in an enterprise environment.

Employment History and Related Experience

UNISYS/ Office of Administration, Commonwealth of Pennsylvania March 2004 –Present

Deployment manager/architect for the data center in Harrisburg, Pennsylvania. Designs and provides solutions for integrating applications securely within the data center; guides team of experts in implementing application on the enterprise infrastructure and providing technical and non-technical assistance when required by the team members; initiates coordination and meetings with clients to discuss the application and infrastructure requirements for deploying applications at the hosting facility; works with clients and provides them with solutions to problems, builds positive client relationships, and delivers effective costing estimates for projects.

- Project – Disaster Recovery (DR)/secondary site for data center (BCDRP): Leader for team of experts and management executives to establish the secondary site for the enterprise data center; provided suggestions related to application designs for secondary site in conjunction with the primary site; delivered the network design document with details on application deployment scenarios and impact of failure of different components.
- Project Single Sign On (SSO) for Commonwealth Portal 2006 (Access Control): Designed and implemented the SSO for the Commonwealth data center portals to leverage CA SiteMinder; designed and supported the costing of the solution to implement SSO among various implementations of SiteMinder at various agency locations; led team of experts for ongoing support including enterprise-wide product upgrades. By leveraging this solution the Commonwealth employees do not have to login multiple times to access various applications and content.
- Project – User provisioning for the Commonwealth of Pennsylvania (Access Control): Technical lead during the requirement, costing, design, and implementation phases for user the provisioning project. IBM Tivoli manager product is leveraged to provide account management and user registration capabilities. This solution provides automatic provisioning of employees per the defined standards and policies.
- Project – PSP CLEAN (Access Control): Supported the project lead during the design phase of security component for CLEAN project. CLEAN is the system that is leveraged by many crime and justice related agencies. Guided a team of experts to provide ongoing support for the CLEAN security components such as SSO and virtual directory services. The support for security components is critical as the CLEAN system is highly secure and processes confidential data.
- Project – PennDOT NDES (Cryptography): Lead engineer, participated in design for certificate enrollment by network and handheld devices using Public Key infrastructure components including network device enrollment services (NDES) and online certificate status protocol (OCSP). PennDOT successfully leveraged the solution for enrolling the certificates for approximately 500 handheld devices initially.

- Project – VPN for mobile users (Telecommunications and Network Security): Supported the design of the VPN solution for Commonwealth mobile users to access internal data center applications. The solution leveraged Netmotion mobility servers and Radius servers for VPN services, PKI, and Active Directory for dual authentication. Commonwealth agencies, like the Game Commission, leverage this solution for mobile users to allow secure access to agency internal applications.
- Other projects – Deployed proxy services to publish internal applications to Internet users by leveraging MS ISA servers and TMG servers. Approximately 150 applications were made available securely to Internet users.
- Other responsibilities – Oversaw team of security experts, coordinated with many other groups involved in all security related projects, cost benefits assessments, and client collaboration events; addressed various security concerns such as data at rest and in transit, user registration, access management, network and infrastructure security.

CitiBank New York, Consultant September 2003 – December 2003

Installed, configured, and managed the Windows 2000 Servers for a data center. Coordinated with application and business groups, Implemented and performance tuning of the applications including IIS based application. Developed and implemented service level agreements to define requirements and required actions related to network performance. Implemented backup servers and created/implemented backup plans for servers. Installed SQL servers and helped DBAs troubleshooting data center system related problems. Create/execute backup of SQL databases using SQL server backup. Troubleshoot Tier-3/Tier-4 Windows 2000/NT server environment and implemented web trends server for logging. Routine troubleshooting and system administration involving application teams, business groups, and network group. Provided ideas and recommendations for better support of the existing environment.

Unisys/Department of Public Welfare, Consultant April 2001 – July 2003

DPW Extranet (Network Security): Responsible for installing, configuring, and maintaining the Department's Extranet by leveraging ISA/Microsoft Proxy Services. Designed and implemented solution to publish secure applications to Internet using MS Internet Security and Acceleration Server/Proxy 2.0 and SSL. Implemented the solution for publishing applications with confidential data using secure socket layer protocol; coordinated with application teams, network infrastructure personnel, and with other offices to fully understand the architecture. Established service agreements with client for system performance. Troubleshooting and managing Tier-3 server problems, LAN, and WAN support management in a complex data center environment including coordination with outside vendors and application vendors like Verizon to meet service agreements.

- Monitored, optimized, administered, supported, and configured security for all enterprise web servers. Support for WINS and DNS servers. Administer Exchange 5.5 environment, troubleshoot email flow problems in an enterprise environment including escalation of problems with other organizations and departments within the same organization. Assist co-workers understand the email flow and hardware/software involved for the entire process. Assisted in design and plan for migration from Exchange 5.5 to Exchange 2000. Helped troubleshoot issues that involved application availability, Network inconsistencies, routine data center issues with user/account management, and policies. Provided support for network infrastructure, publishing applications and their availability, troubleshoot procedures for network, email, web servers, and Internet facing Firewall servers (ISA and proxy servers).
- Project -Active Directory Implementation (Access Control): Designed and implemented Active Directory in an enterprise data center environment, including security policies, service level agreements, delegated administration to user per their role for user and group accounts management. Created the support document and trained the administrators to manage the active directory per their role. Troubleshoot the issues related to active directory policies and authentication problems that involved coordination with various departments.
- Developed and implemented NETIQ performance-monitoring procedures on Windows 2000 enterprise servers. Performance monitoring procedures details the process for monitoring each individual server's health and send alerts in case one of the monitored resources became bottlenecked, modified the scripts per the organization requirement, created reports for resource consumption when required. The servers monitored with NetIQ were Windows 2000 servers supporting the role of web servers, application servers, and database servers.
- Application Center Implementation (Access Control): Designed and executed the phased implementation of application center clusters to load balance the applications running on Windows 2000 enterprise web servers. Created the procedures for application deployment and trained the developers to help them understand the new data center environment. Troubleshoot the problems related to

application deployment, network inconsistencies, and application synchronization. Maintenance of the cluster by taking the node offline alternatively without affecting the end users.

- Implemented unified security solution including deployment and configuration of SiteMinder components on enterprise servers. Integrated Netegrity with active directory for authentication and authorization of resources, configuring policy servers to for multiple active directories for authentication, and for authorization of resources. Troubleshoot the problems with the slow response or unsuccessful authorizations for the application using the Netegrity for single sign on, DNS problems, and network issues in an enterprise environment, escalating the problems with third party software/application vendors whenever required and worked as coordinator.
- Implemented a Windows NT/ 2000-based VPN solution to provide administrator's access to public web servers for upgrades and for monitoring and maintenance. Analyze complex network environment and resolve any security issues. Coordinate with multiple offices and third party hardware/software vendors.

IBM, Arkansas June 2000 – August 2000

NT Administrator

Designed and Implemented the NT Enterprise Network which comprised of NT4.0 Enterprise Version Server, CISCO Routers, 3Com Switches, RAID5 Disk Arrays, and IBM Netfinity Server. Implemented the Backup Policy using DLT4000 tape drives and Backup Exec. NT administration and troubleshooting on Netfinity servers. Troubleshoot disk related problems and tape drive problems. Worked with utilities to flash BIOS settings and change BIOS settings. Configured the RAID hardware. Configured load balancing on network cards. Worked with disaster recovery NT resource kit tools to modify with NT registry.

Northfield Savings Bank, New York(Short Term) February 2000 – May 2000

Network Administrator

Project Firewall Implementation (Network Security) - Studied network design to predict problems before configuring/implementing security policies. Analyzed, designed, implemented, and configured various elements of the network from switches, CISCO Routers to servers, and application Software. Installed and configured NT Servers. Installed and Configured Checkpoint 4.1 (Firewall) on NT 4.0 servers. Configured and integrated of E-Safe content scanning server to work with Checkpoint 4.1. Created policies and rules to define security for the organization.

Interactive Communications Inc. May 1999 – January 2000

NT Administrator/Architect

Designed and reconfigured the network that had multiple subnets for different departments of the company. Installed and configured Checkpoint 4.1 (Firewall) on NT 4.0. Configured and integrated of E-Safe content scanning server to scan for viruses with Checkpoint 4.1.

- Created policies and rules to define security for the organization. Implemented Internet security using MS Proxy Server 2.0. Configured Exchange Server 5.0 including IMS. Implemented VPN using MS PPTP (Point to Point Tunneling Protocol) technology and RAS server technology. Data transfer was secured by enabling the MS CHAP protocol and data encryption at both the server and client levels
- Evaluated the Windows 2000 server (Beta) compatibility with existing devices and tested the product services and new features in the test environment. Created customized packages using custom installation tools and distributed using Windows 2000 group policies. Upgraded from Windows NT server to Windows 2000. Configuring RIS (Remote Installation Server) to remotely install Windows 2000. Configured Terminal Servers in Windows 2000. Configured networking services like DHCP, DNS, etc.

NIIT Limited, India July 1995 – January 1999

Network administration: Comprised of Windows NT Servers, Novell NetWare 3.12, and SCO-UNIX. Administration of users and group accounts, security policies, print servers, implemented, administered, and troubleshoot Exchange environment, configure mail clients, and performance tuning. Implemented migration from Novell to NT Support DNS/Wins/DHCP study and design network. Conducted training on Windows NT 3.51/4.0, Windows 95, UNIX, TCP/IP, SQL Server, MS Exchange Server, and PowerBuilder for corporate clients, Unicenter TNG (Computer Associates).

Education

- Bachelor of Science, University of Delhi, India
- Diploma in Systems Management (NIIT, India)

Professional Certification

- Windows MCSE 2003
- CA SiteMinder
- CISSP
- ITIL Foundation 3.0

Professional Development

- CISSP

UNISYS

[redacted]

Agency Infrastructure Architect

Key Skills and Knowledge

- VMWare vSphere 4/5 and ESX/ESXi
- Windows
- Active Directory
- EMC Avamar
- Symantec NetBackup
- Disaster Recovery Planning
- Powershell Scripting
- Physical Server to Virtual server restore
- Bare Metal restore to dissimilar hardware
- VMware backup/restores
- Avamar backup/restores
- NetBackup Tape backup/restores
- DataDomain Oracle restores
- MS SQL 2000, 2005, and 2008 restores
- Windows 2003, and 2008 Cluster restores to a single and multi-nodes
- SQL 2008 Cluster used for Multiple application management
- DFS deployments
- Incident and Change Management control
- Technical Documentation
- Blade Logic Patch Management
- Systems Builds/Deploys
- Linux administration support (SUSE & Red Hat).

Skills Summary

Five years experience as a data center analyst with Unisys dealing with regular upgrades, security enhancements, virtualization deployments, datacenter consolidations, and migrations, as well as Disaster Recover (DR) design. Routinely lead the architect and design teams as a subject matter expert with multiple projects. Also a regular project leader on about a dozen projects at both the Data PowerHouse (DPH) data center as well as our DR Facility.

Expansive knowledge in the following areas: VMware vSphere ESX/ESXi 3.x, 4.x, & 5.x, Windows 2003, 2008, 2012, Powershell and Visual Basic (VB) script, active directory, security policies, IIS, DHCP, DNS, FTP, IBM Blade center servers, Dell and IBM x86 systems, EMC Data Domain, EMC Avamar, Microsoft Failover Clustering, Network Load Balancing, and Microsoft DFS and DFS-R.

Capable in the following server software: BMC Blade Logic, MS Exchange 2000, 2003, 2007, Microsoft SQL 2005/2008 management, Symantec NetBackup 6.x, and 7.x, Backup Exec system recovery, Symantec AV, McAfee w/EPO, Symantec Ghost, WSUS, IBM Tivoli Endpoint Manager, Microsoft System Center operations manager 2007 and 2012, VMware Capacity Planner, and vCenter operations manager.

Employment History and Related Experience

Unisys Corporation, Harrisburg, Pennsylvania 2008 – Present

Systems Analyst, Project Leader

Responsible for multiple government agencies' central Pennsylvania data centers; principle troubleshooter for systems, virtualization, active directory, and patch management.

- Windows/VMware team lead responsible for maintaining about 800 Servers in the data center. VMware administrator of over 350 VMs (approximately 60 ESX/ESXi hosts in five virtual centers, including Disaster Recovery site).
- Data center active directory and DNS administrator for ESM domain, backup administration including NetBackup, DataDomain, and Avamar; familiar with scripting for server automation using Powershell, VBScript, and PowerCLI (VMware); designed and executed 11 Disaster Recovery tests across four Commonwealth of Pennsylvania agencies.
- Consolidated DPH NetBackup infrastructure. Collaborated with the Commonwealth to establish requirements. Designed and consolidated six isolated backup environments to a single, large, dynamic, highly available backup infrastructure. The data center project design delivered for faster backup and restore times, higher reliability and resiliency, and save costs by using fewer tapes, backup servers, and network equipment. When the data center project was finished in late 2011, the infrastructure moved from about 80 percent utilization to about 50 percent utilization. This reduction was due to the wealth of techniques that were designed into the project such as multiplexing, dynamic tape allocation, and simplifying tape pools. All was done without purchasing any equipment, but rather better utilization of the equipment that was already purchased.
- Upgraded data center Windows 2000 active directory to 2008 R2 active directory with Kerberos Trust to the Commonwealth of Pennsylvania. Supported the development of the cost estimate. Communicated questions to the Commonwealth and interpreted their answers for the Unisys Engineers. The design allowed for faster site-to-site replication speed, enhanced accidental user/object deletion recovery, as well as bringing single sign on (SSO) to all Commonwealth agencies. Using SSO removed the need for multiple usernames for each customer, as well as eliminating overhead associated with multiple user management by DPH staff. Customers may now view performance metrics, systems properties, backup statuses, run reports, etc., all with their existing domain username.
- Migrate the Commonwealth of Pennsylvania data center file share (about 2TB of data) from single node 2003 file server to 2 node 2008 distributed file server with replication (DFS and DFSR). Worked with the Commonwealth to refine the requirements for this project. This project design not only added redundancy with zero downtime in the event of file server failure, power outage, etc., but also simplified the backup solution and allows users to recover their own files when needed, thus reducing management overhead.
- Remote Desktop Manager Consolidation project. Complexities in the Commonwealth data center resulted in a wide range of management consoles, remote desktops, custom applications, and web console that were difficult to updated and manage. Provided support to the cost estimate for this

project. This new design brought a single pane of glass for the operations and DPH server staff. Through the combination of remote desktop manager and a highly available remote desktop services “RemoteApp” farm, served up all operational consoles, and remote desktop connections in a single pane of glass, while enhancing the security behind each connection with two factor authentication. Updates are now handled in house for each application, accomplished in the background with minimal impact to staff and customers.

- Multi-Site HA DNS. This data center project resolved many issues preventing the DPH management systems from growing. Delivered key elements of the estimate for the senior architects. Once completed, using GLOBALNAMES zone as a replacement to WINS and removing hosts files, it aligned the management systems with best practices and prepared us for the rapid growth from about 350 systems to over 1,000 over a four year period without extensive hosts file management.
- VMware host separation. Proposed splitting up each two Node hosts into two single node hosts, as well as doubling the memory in each. This design resulted in over a 200 percent increase in capacity at a fraction of the cost for purchasing new hosts entirely. This design also reduced wasted reserve (failover) capacity from 33 percent to only 12.5 percent.
- DR virtual machine replication of master Net backup servers. This project design simplified the restore process of the database master backup server during a DR. It reduced the overall time to restore readiness from 2.5 hours to .5 hours.
- Integrated enterprise systems data center relocation. Principle Windows SME, designed the cutover process for the WINTEL team, implemented successful move for one of the larger data centers.

Non-Unisys Project Experience

Business Information Group, , York, Pennsylvania 2008 to 2008

Network Engineering Consultant

Administered almost 30 AD domains during the contract (users counts ranging from 10 to over 200). Installed numerous servers including Windows 2003 and 2008, SBS 2003, SQL Server, VMware, and Terminal Server.

- Installed servers from HP, IBM, and Dell
- Multiple small office setups and relocation

Rite Aid Corporation, Harrisburg, Pennsylvania 2004 to 2007

Systems Administrator and Development

Support servers (Both Windows NT4, 2000, 2003 and SCO5 Unix), Cisco routers, Support PCs, setup and repair of HP and Lexmark printers, Network wiring of 29 Rite Aid Pharmacy stores.

Education

- Penn State University Hazleton, Pennsylvania, Associate Degree in Information Sciences and Technology, 2000 - 2002

Certifications

- VMware VCP4
- VMware VCP5
- Microsoft Windows 2008 MCITP: SA
- Microsoft Windows 2008 MCA: Virtualization
- ITILv3.

UNISYS
PCN
Technical Expertise. Tangible Results.

[redacted] Agency Infrastructure Architect

Key Skills and Knowledge

- ITIL Foundations Certified
- Commonwealth agency experience
- Extensive Remedy experience
- VMware - VSphere, VCenter VMotion, ESX, ESXi
- SAN Storage and Recovery
- Enterprise level security infrastructure
- Proxies
- Citrix XenServer
- EAI Enterprise Application Integration
- IBM MQ Series
- Integration Brokers, Mercator, Cyclone.
- Active Directory
- HP configuration Management – Radia
- Automated application and security patch management
- HP Openview Systems and application monitoring
- ITIL Practices
- DePICT Project Management
- Remedy Helpdesk, CMDB
- MS Office
- IBM and HP Blade servers
- IBM AIX OS
- IBM PowerPC Servers
- HPUX VPARs and LPARs
- HP Service Guard
- IBM HACMP
- Microsoft Clustering
- NLB Network Load Balancing
- Oracle 10g RAC Real Application Clusters
- MS SQL Servers
- Clustered SQL Servers
- EMC Symmetrix class Storage
- EMC Clariion Class Storage
- FC, FCoIP, and FcoE
- Brocade SAN Directors and switches
- WAN/LAN Networks

Skills Summary

Infrastructure Data Center Technical Architect for large corporations, introduce new technologies and solutions, set the vision and technical direction for the entire company. Moves in the forefront of emerging Information Technology (IT), provides liaison and collaboration between clients and providers, prototypes new solutions, and fosters the business adoption of data center technologies and solutions.

- Understands the process of gaining business approval through presentations to the business including business justification with detailed cost models
- Project technical lead on major initiatives for data centers, provides leadership for data center sales, operations, and support, delivers project success including installation, testing, quality control, acceptance testing as well as transition training of new technologies to internal support and help desk staff
- Possesses a broad spectrum of products and technologies, consolidated over twenty-five data centers into centralized mega-data centers, built three new data centers, designed six SAN's in six data centers, developed multiple Disaster Recovery (DR) solutions including the use of SunGard as well as in house Disaster Recovery solutions using internal Infrastructure and data centers
- Designed the WAN data center architecture spanning eight countries and over 500 nodes, worked in a global team to design the global WAN encompassing over 120 countries and 3,000 nodes. Designed the WAN architecture in response to the data center strategy
- Introduced automated desktop and server security patch installation to all desktops and servers, reducing the risk of system and data lose
- Designed and implemented many Server High Availability solutions using HP Service Guard, IBM HACMP, Microsoft Clustering, and Oracle RAC
- Consolidated over 350 Intel-servers using VMware ESX and blade centers, used Citrix to centrally host applications for users located worldwide
- Strong ability to work in a team environment, solid negotiator, quickly learn new data center technologies and embrace change; driven and dedicated person with a passion for Information technologies and solutions.

Employment History and Related Experience

Unisys, Solution Architect, Harrisburg, Pennsylvania 2011 – 2012

Contract for a military institution in the greater Harrisburg Area, created the business case for application centralization, generated design interpretation of the business case, and implemented solutions based on those recommendations. Advised clients, nurtured the strategic operational relationship with the military client, designed, tested, and delivered data center support solutions for centralized applications that were distributed throughout the United States. Used VMware Technologies to reduce costs and improve service levels.

- Presented briefing outlining business justification for centralizing distributed applications; advised client on how to exploit current data center capabilities and recommended strategic adjustments to data center architecture that would enhance operations
- Used VMware allowing the customer to better use existing and future hardware and to better leverage existing IT support staff in reducing maintenance costs
- Provided Disaster Recovery solution for applications distribution. Improved application availability service level and reduced risk of lost data
- Collaborated with client to reduce new application provisioning times and costs
- Primary Unisys liaison for data center issues, moved information and ideas between vendor and client
- Supported sales and support, delivered capability briefings, presented service costs and timelines for the initial data center centralized infrastructure build out
- Collaborated with client to define costing strategies, produced cost saving and service improvement estimates capable through a new centralized data center application hosting environment

- Cisco Catalyst 6500 series router
- Cisco 2900 series edge routers
- Cisco IOS firewall
- F5 BigIP, and GTM
- Check Point Firewalls
- IDSs
- IPSs.

- Used existing technical staff to build and develop environment using Blade server hardware, VMware's vSphere running ESX on server hardware was used to host multiple Windows Server and Linux operating systems and was managed via VCenter administration tools. The training of existing staff on the new technologies from VMware reduced the need for outside engineers and enabled the client to support the new infrastructure once it went into production
- Achieved operations capacity planning and management using VMware's DSR with clustered groups. VSphere servers were automatically load balanced within a cluster group. Fault tolerance and DR was achieved using VMotion. Legacy applications that did not have any redundancy in the past gained fault tolerance and DR by being pooled into the new virtualized infrastructure. This reduced labor costs when failures occurred by making normal hardware failures a non-critical repair that is handled during normal business hours. This improved service levels by ensuring non-disruptive application service during normal hardware failures. After initial testing was successfully completed in the development environment, the production environment was built and delivered for operational use

Unisys, Solution Architect, Harrisburg, Pennsylvania 2009 – 2010

Contract for a Pennsylvania government agency to deliver a centralized application to view hundreds of video cameras located across the commonwealth over the Internet using existing and new infrastructure. Supported collaboration between Unisys and the agency, principal liaison and champion for technology change, analyzed the existing network infrastructure and made recommendations to upgrade, replace or modify the infrastructure as necessary to facilitate the new application. Included operational support costs as part of the presented package.

- During the data gathering phase, refined the client strategy to make sure that the Wide Area Network provider was able to provide circuit utilization and performance reports for most of the WAN circuits
- Developed utilization strategies with the client to build visual networks data probes to ascertain availability and reliability performance data; briefed the results of the studies to the agency
- Presented embedded Visio diagrams outlining analysis and recommendations to project stakeholders. Conducted meetings with the project team to address concerns and revisions until a workable set of recommendations were achieved
- Reduced timeline to administer network, introduced several new tools to the infrastructure; Microsoft performance monitor was used for Wintel systems. Tivoli was used for the Unix and Linux systems; operations support staff was trained and prepared to use the applications

Bise LLC, Owner, Harrisburg, Pennsylvania 2008 – Current

Created an automated software product allowing robotic trading trade on financial markets of financial assets. Provided sales briefings; responded to requests for pricing data. Negotiated agreements from conception to signature. Developed and nurtured a customer base using the software product in a controlled (Black Box) environment hosted via VMware at a local facility. After installation, provided operations support and periodic maintenance.

DHL Logistics, Manager IT Architecture 1998 – 2008

Responsible for the technical direction and delivery of new products that reduce costs, improve productivity, and enable new business opportunities to the client. Negotiated the technical portions of subcontract agreements from conception to signature. Managed several employees, guided their engineering careers using human resources tools such as goals, objectives, and performance evaluations.

- Responsible for all new technologies introduced into the company. Prototyping and creating proof of concepts of new solutions, developed design architectures, and ultimately delivered these new technologies into the data center production environments
- Liaised directly with clients to develop IT solutions to enable the client to outsource their logistics to DHL. This resulted in DHL winning new business opportunities
- Delivered documented solutions to the business and support teams and facilitated in the transition of the new data center solutions into the helpdesk and support teams
- Oversaw a Level 3 support team throughout the solutions life cycle
- Instrumental in the introduction of ITIL practices within the IT organization; introduced Remedy for incident management, and instituted configuration management database - CMDB, and certification all of technicians in ITIL foundation
- Managed data center, network, security, server, application, and support teams to deliver new products to the business; used MS Office, created all solution designs and cost estimates; briefed the designs and estimates to DHL upper management for business approval

- Liaison directly with project managers to develop detailed project plans using MS-Project. Responsible for all project budgets and delivery times
- Built three new data centers to facilitate the company's vision of a centralized computing environment
- Generated six Storage Area Networks (SANs) and used them to deliver local and site level DR for data centers. The introduction on SAN technologies such as Business Continuance Volumes (BCVs) - and data snap shots - Snaps enable DHL to improve data backup times and reduce time to recover data. Symmetrix Remote Data Facility (SRDF) - enabled near real time data and application recovery. Improved application availability and enabled DHL to win new business
- Designed and built enterprise level data center security infrastructures using Checkpoint and Cisco firewalls, F5 BigIP and GTM, IDS's, IPS's, proxies and gateways to enable user access to the Internet, application hosting, and Business-to-Business (B2B) capabilities
- Designed and generated an Enterprise Application Integration (EAI) infrastructure using IBM MQ Series, Mercator, Cyclone and proprietary EDI translators to enable B2B with hundreds of our internal and external applications and data center customers
- Designed and built a global active directory Forest with over 5,000 servers and 40,000 users
- Enabled network, server, and application monitoring and management using HP Openview suite of products. This allowed customers to view IT as a service and management to better manage incidents, technicians used the tools as day to day support activities improving time to recover failures
- Designed and created a desktop management system to deliver automated application and security patch installation
- Built server consolidation infrastructures using IBM and HP blades and VMware suite of products to consolidate hundreds of Intel servers, improve server hardware utilization, reduce server provisioning times and costs, reduce administration costs, and deliver DR capabilities
- Used IBM PowerPC/AIX OS and HPUX VPARs and LPAR's to consolidate midrange UNIX systems Improving server hardware utilization and reducing server provisioning times and costs
- Generated dozens of High Availability (HA) applications using HP's Service Guard, IBM's HACMP, Microsoft Clustering, NLB Network load balancing, Oracle RAC - Real Application Clusters. MS-SQL database servers including multi-node Clustered SQL servers

Solution Technologies Incorporated – STI, Systems Consultant 1997 – 1998

Design and build LANs, file and print systems, Email systems, database servers, and desktops for customers. Provide ongoing system support to customers.

YIS Consulting, Systems Consultant 1995 – 1997

Two year project for Exxon Corporation; Designed and implemented WAN/LAN's, file and print systems, Email systems, database servers, and desktops for customers. Provide ongoing system support to customer.

Enviro-Test, Systems Consultant 1994 – 1995

Lead in the development of a 57 node WAN and 57 new LANs for a Commonwealth of Pennsylvania contract for emissions testing. Developed integration between proprietary emissions testing equipment and industry standard computing platforms. Developed integration between PennDOT systems and proprietary in-house systems, provided Level 3 support and maintenance of all statewide computing systems.

Scranton Corporation, Regional Service Manager 1986 – 1994

Responsible for one quarter of the companies services revenue with complete Profit and loss and budgetary responsibility. Work closely with sales teams to increase profitability through new sales and new service products. Developed a service delivery team in 10 branch offices in the Northeastern United States.

Education

- Christopher Newport College, BS Engineering and Computer Science, 1982 – 1986
- Laurel Highland High School, 1982

Certifications

- Microsoft Certified Professional - MCP; Checkpoint Firewall Administrator
- Project Management DePICT (DHLs version of PMP); HP-RADIA Administrator
- ITIL – Foundation

UNISYS

IBM

[redacted]

Agency Infrastructure Architect

Key Skills and Knowledge

- Over 39 years of experience supporting the Commonwealth of Pennsylvania in various capacities
- Designed, implemented, and maintained highly available set of data center systems and sub-systems
- Architected complex solutions to meet the dynamic business requirements of the Commonwealth agencies.

Skills Summary

Over 39 years experience in the Information Technology (IT) field and is located in Harrisburg, Pennsylvania. Proven record in designing and implementing technology infrastructure for complex information systems including large enterprise systems (System z) and mid-range environments (System i).

Employment History and Related Experience

IBM Corporation, IT Architect 1999 Present

Performed as an IT Architect, supporting the Commonwealth of Pennsylvania agencies in an outsourced business relationship for the past 12 years. Accomplishments include designing, implementing, and maintaining a highly available set of data center systems and sub-systems. Consulted with agency stakeholders to gather their requirements and worked with SMEs to size and design solutions that exploit the functions and feature of the hardware and software in the proposed solution.

- Designed and implemented a consolidated and optimized System z solution that migrated workload from multiple mainframe platforms onto one. In addition, functions such as Group Capacity and Sub-Capacity software were exploited to allow the Commonwealth workloads to gain access to available MIPS in excess of their allocated capacity while at the same time not exceeding software pricing limits
- Designed and implemented a Virtual Tape Server and Automated Tape Library (VTS/ATL) in a peer-to peer environment that provided improved batch throughput, improved availability of tape operations, and optimized the libraries which are shared among multiple different operating systems
- Worked with PennDOT stakeholders to design and implement a virtual Linux environment on the System z mainframe (zLinux). The environment includes multiple LPARs (production, test, and monitor). The zLinux environment provides PennDOT with the capability to move distributed (Unix) workloads onto the same system as traditional mainframe applications to improve throughput and business system resiliency
- Implemented a System z Integrated Information Processor (zIIP). This was a new capability introduced to enable PennDOT and the Department of Revenue to decrease general purpose processor MIPS by offloading select DB2 workload.

IBM Corporation, Systems Engineer 1986 – 1999

Served as a Large System Specialist supporting multiple Commonwealth of Pennsylvania agencies with the planning and installation of mainframe processors, peripherals, and software; assisted agency staff with performance and capacity management activities; served as a project manager and team lead, and successfully managed numerous mainframe, storage subsystem (DASD, tape), and front-end communications processor installations and upgrades.

IBM Corporation, Operating System Programmer 1985 – 1986

Upgraded and maintained MVS operating systems, subsystems, and program products running on multiple mainframe processor complexes (Operating Systems Manager). Managed system configurations and performed system generation activities, identified and resolved problems, and managed capacity and tuned system performance.

Pennsylvania Department of Transportation 1973 – 1986

Held various positions within the IT organization of this Commonwealth agency, including computer operations, database administration, MVS systems programming, and operating systems programming supervisor.

Education

- School of Computer Technology, Pittsburgh, Pennsylvania
- Continuous Technical Education

[redacted]

Agency Infrastructure Architect

Key Skills and Knowledge

- Over 17 years IT experience with the Commonwealth of Pennsylvania
- Consultative requirements gathering
- Infrastructure architecture design
- Agency application knowledge
- Team leadership
- Systems management.

Skills Summary

Over 34 years of Information Technology (IT) experience, has been assigned to IBM Commonwealth of Pennsylvania team since 1996, and resides in the Harrisburg, Pennsylvania area. Led the design and implementation of multiple complex IBM infrastructure solutions for the Commonwealth, including the SAP and Unemployment Compensation infrastructure environments.

Employment History and Related Experience

IBM Corporation, IT Architect 1996 – Present

Supported Commonwealth agencies for 17 years, designing and implementing highly available IT systems and sub-systems. Consulted with business stakeholders and IT technical and operations staff to gather requirements and develop highly available infrastructures and systems management solutions. These solutions reduced the number of data centers and servers and significantly increased server virtualization within the Commonwealth.

Unemployment Compensation Management System Project

Performed as the lead infrastructure architect on the more than $100 million contract with Department of Labor and Industry's Unemployment Compensation Management System (UCMS) stakeholders to design and implement a highly available infrastructure in 2006. This infrastructure supported a major rewrite of their wage, tax, and benefits application to replace a 30 year old mainframe system. Supported change, incident/problem, performance, and availability management, provided infrastructure architecture support and supported daily operational management since 2006 with a high level of customer satisfaction.

Enterprise Datacenter Migration

Served as lead infrastructure architect on the more than $100 million contract for the design, build, and installation of the SAP-ERP environment for the Commonwealth's IES project. Provided infrastructure design consulting with agency stakeholders and managed implementation and migration to the new ERP system for the Commonwealth's Enterprise Data Center (EDC). Managed an eight member team responsible for implementing service levels of the ERP application during the early years of the implementation. Implementation consistently met or exceeded service levels with a high level of customer satisfaction.

Department of Labor Datacenter Migration

Lead infrastructure architect for design of systems infrastructure to support complex, statewide network design and implementation at Department of Labor and Industry. Developed high level design and systems management strategy for systems management pilot. Led Department's data center consolidation analysis and oversaw migration to centralized storage management and backup strategy. As part of the project, multiple data centers (SWIF, BWC, and OVR) were successfully migrated to a single central data center at Harrisburg's Boas Street location, eliminating duplication of operational functionality.

Bureau of Workers' Compensation Project

Team leader for distributed systems management architecture of new infrastructure to support mission-critical application set at the Bureau of Workers' Compensation. Team leader for ongoing integration and architectural support for infrastructure expansion including migration and server consolidation to new platforms. The project was completed on time with a high level of customer satisfaction.

Vocational Rehabilitation Project

Lead architect at Office of Vocational Rehabilitation for statewide, distributed system and application architecture. Performed as deputy Project Manager and provided ongoing architectural support. The solution was implemented on time with a high level of customer satisfaction.

IBM Corporation, various positions 1981 – 1996

Held various positions at IBM including System Engineer, Systems Engineering Manager, Brand Manager, and Critical Situation Manager, and Sales Manager.

Education

B.S., Math and Business Administration, Westminster College – New Wilmington, Pennsylvania

Certifications

IBM Senior Certified Architect – Infrastructure

UNISYS

[redacted]
Security Manager

Key Skills and Knowledge

Domain Expertise and Solutions
- Unisys Stealth for Networks
- Unisys Stealth SSVT
- Unisys Law Enforcement Message Switch (LEMS).

Directory Services
- LDAP
- IBM Tivoli Directory Server, Directory Integrator
- Microsoft Active Directory
- Oracle (Sun) Directory Server
- Oracle Virtual Directory
- Radiant Logic Directory, Virtual Directory, Metadirectory (ICS)
- Critical Path Metadirectory
- Banyan StreetTalk.

Identity Management
- CA (Netegrity) IdentityMinder
- IBM Tivoli Identity Manager
- Novell Identity Manager
- Sun Identity Manager (Waveset Lighthouse).

Access Management
- CA (Netegrity) SiteMinder
- IBM Tivoli Access Manager
- RSA Adaptive Authentication
- Sestus Virtual Tokens™ Multi-Factor Authentication
- Sun Access Manager.

Firewalls
- Check Point.

Digital Rights Management
- Liquid Machines.

Management Consulting Services
- Architecture and Design
- Knowledge Transfer
- Business Modeling (ProVision)
- Service Modeling (MindManager).

Project and Program Management
- Project Management
- COTS Implementation.

Communication and Networking
- TCP/IP, Vines IP
- Ethernet, Token Ring
- Sniffer/Wireshark

Skills Summary

Over 38 years of senior technical, management, and business development experience, including six years with the Commonwealth, covering security, design, consulting, project management, technology assessment, automation, and distributed network architecture. Specialized security expertise with identity, including directory, Identification and credentialing, access control, and identity management.

Capable leader with deep experience overseeing large contracts that ensure compliance with all security standards and requirements and provide strong experience in planning, designing, and implementing complex, large scale networking projects; excellent technical leadership, and hands-on skills.

Effective communication and leadership experience with project teams, clients, and pre-sales engagements. Key client technical interface for multiple large security and identity management planning and implementation projects for critical Unisys clients.

Employment History and Related Experience

Selected Unisys Senior Security Architect Project Experience

Unisys Presales Support 8/2006 – Present

Technical security and infrastructure lead on numerous proposals for the Commonwealth, as well as other proposals for both public and private sector organizations in the U.S. and abroad. Provides technical and delivery risk assessment for numerous proposals and provides input to management for approval to submit bids; used our risk management tools to focus Request for Proposals (RFPs) pursuit decisions on contracts that properly fit the Unisys business model.

Prepared HSPD-12 solution demonstrating FIPS-201 compliance and integration with Enterprise Digital Rights Management and integrating Identity Management solution for demonstration to key DoD prospects. Met their demo requirements within a few short weeks thus enabling Unisys to bid for the work. Worked on large government outsourcing proposal, prepared and completed the SOC, Security Portal, and Incident Management, and Response sections, and successfully transitioned the completed sections to the late-addition security subcontractor.

Pennsylvania State Police 3/2009 – Present

Managed security for new Commonwealth Law Enforcement Assistance Network (CLEAN) upgrade (includes Law Enforcement Message Switch and associated applications), encompassing security policy, access control via CA SiteMinder, and integration with PSP's RSA Adaptive Authentication using a RadiantOne Virtual Directory Server (VDS) as the user repository. Collaborated with JNET technical resources to provide access into CLEAN by JNET users through their Novell Access Manager without additional authentication, opening first-hand access to a whole set of users who previously only had second-hand access. This has enabled deployment of the new Megan's Law application (PA SORT) to its full user base much faster than would have been achievable otherwise, enabling PSP to meet its legislatively mandated deadline.

Upon completion of the implementation project: provide security support for the new CLEAN environment for user access issues (SiteMinder, RSA Adaptive Authentication, and RadiantOne VDS), and more often including a full range of technical and security support. Assist PSP with integrating new applications and access modes to the new CLEAN environment. Collaborated with PSP's Megan's Law section to integrate new Pennsylvania SORT into the CLEAN security infrastructure, since their user bases have extensive overlap; provided the team with general networking support (redundancy and load balancing) enabling their on-time deployment to production.

Michigan DHS May 2011 – Present

Managed security for new Child Welfare System project; guided the resolution of security issues by the project team (including the Unisys Team, DHS, and the State's central Information Technology (IT) organization) and the Office of Enterprise Security (now MCS, Michigan Cyber Security). Confirmed the solution met the security laws, regulations, policies, and standards of DHS, the State, and the relevant Federal agencies or could be put on a path to meet those requirements that were outside of DHS' initial planned scope and budget. Identified appropriate integration between the application's access management and the State's Tivoli-based Single Sign On (SSO) infrastructure; worked with the design team and the SSO team to accomplish goals. Documented the resulting system and user access security models, permitting

- Microsoft Windows NT/2000 /2003/2008 Networking
- Banyan VINES
- SNA.

Databases
- dBase-III/Clipper
- Microsoft Access.

Hardware
- Various Intel Servers
- Sun/HP/IBM RISC Servers
- Proprietary Hosts (DEC, Gould/SEL, Honeywell, Burroughs, ACA/32000).

Operating Systems
- VMware ESX/Workstation
- Windows 95/98/2000/XP/7 Clients
- Windows NT/2000/2003/2008 Servers
- Sun Solaris
- HP/UX
- Red Hat Linux
- IBM AIX
- MS/PC DOS
- DEC VMS
- SEL/MPX-32.

Programming Languages and Tools
- HTML/VBScript/JavaScript
- ALGOL/PASCAL
- Fortran
- APL.

Security Clearance

Interim DOJ - MBI (Minimum Background Investigation), Level 5

Security Certifications

CISSP

GSEC (GIAC Security Essentials Certified – SANS Advisory Board)

the MCS team to more easily document its review and audit of the system's security.

U.S. Department of Justice — December 2008 – August 2009

Provided guidance and assistance to a development group that needed to add single authentication technology to their web site, including requirements definition, architecture, product selection, Proof of Concept, and leading to production. Influenced the development team with a suggestion that would save time, effort, and money while gaining functionality and improving maintainability by deploying a customizable COTS SSO product rather than attempting to code their own single authentication into all of their applications.

Minnesota Office of Enterprise Technology — March 2008 – June 2008

Led team that created a secure state-wide Identity and Access Management plan working through the cross-agency steering team. Ran discovery workshops and created the initial high level conceptual architecture to meet the state's needs; managed final technical and ROI deliverables to the state.

Pennsylvania Governor's Office of Administration — March 2006 – December 2007

Created and documented enterprise Identity and Access Management architecture to enable application of HSPD-12 and FIPS-201 to provide identity credentials for the Commonwealth's employees and first responders, and then to other constituencies, working with the IPAM architecture board. Authored and co-authored several Security ITBs to define the policy framework for a shared infrastructure to facilitate that architecture. With the joint OA/OIT-JNET team updated the Commonwealth's digital certificate policies, especially the Certification Practice Statement, for the Commonwealth of Pennsylvania's Public Key Infrastructure; pushed for guidelines to use internally generated Microsoft certificates when possible to minimize spending on commercial certificates from VeriSign and Entrust.

Investment Management Firm — January 2006 – February 2006

Documented SiteMinder policy administration process and trained Security Administrators to maintain policies. Also reviewed security and access control policies and provided general security recommendations on how to better leverage the in-house access control tools.

Massachusetts Information Technology Division — January 2005 – December 2005

Performed discovery (requirements/environment analysis, architecture, scope definition, and product selection), design, and prototype implementation for a planned shared Identity and Access Management infrastructure for all Commonwealth agencies; documented a recommended governance framework.

Software Manufacturer — April 2005 – May 2005

Analyzed Web Access Management marketplace capabilities; helped client identify capability gaps in its product offerings; presented recommendations and approach to correct the gaps.

Delta Dental — December 2004 – July 2005

Analyzed client's web registration and access management solution, determined how to integrate it with the National Association's portal, recommended a solution acceptable to both the client and the Association; designed, implemented, and tested a Proof of Concept to validate the solution.

Building Materials Manufacturer — July 2004 – August 2004

Helped the client determine how to maximize the use of identity and access management software that had already been purchased but didn't correlate with their requirements or environment (platforms and versions). Enabled new ERP system to go into production on time by meeting their requirements to create and manage user identities and passwords.

Retailer — June 2004 – July 2004

With Microsoft Consulting, reviewed client's in-store technology and recommended migration path using Windows Server 2003 and Windows XP. Also analyzed client's network and recommended future Active Directory design for the store network.

National Television Network — April 2004 – June 2004

Architected and designed semi-custom Identity Management solution for this client that: managed their feed from the corporate employee directory to their internal Active Directory and email; updated the corporate directory with current identity information, including processes and workflows for managing, on-boarding and off-boarding of contractors; managed passwords; managed supervisors' assistants (for delegating workflow approval authorization); created users and managed workstation accounts.

Storage Technology Manufacturer — March 2004 – April 2004

Analyzed proposed use of Microsoft's MIIS meta-directory to manage both internal and extranet identities from client's HR system through their full knowledge management portal; oversaw Unisys consultant's designs for portal directory and MIIS to meet my recommendations.

New Jersey Administrative Office of the Courts December 2003 – February 2004

Performed discovery (requirements/environment analysis, architecture, and scope definition) and design for large meta-directory project, enabled client to begin to coordinate and integrate several user data stores. Identified and documented identity management requirements addressed in future projects.

US Treasury Department March 2003 – August 2003

Supported the client and several application teams; integrated customer-facing Internet applications into a Netegrity SiteMinder and Waveset Lighthouse-based security infrastructure. Recommended and designed upgrades to the security infrastructure to meet the integration requirements of those application teams.

Financial Outsourcer July 2001 – September 2001; September 2002 – October 2002

Collaborated with client application teams (marketing, customer service, and development); integrated customer-facing Internet applications into a SiteMinder security infrastructure. Recommended and designed upgrades to the security infrastructure to meet several application integration requirements.

Delivered operational support for client's security infrastructure and application integrations; accomplished initial load testing and analysis to identify possible bottlenecks as the infrastructure scaled, and recommended enhancements to mitigate those bottlenecks.

Employment History

- Banyan Systems/ePresence/Unisys (via name change and acquisition) .....1992 – Present
- Advanced Computer Applications.....1987 – 1992
- Macro Corporation .....1982 – 1987
- Scott Paper Company.....1976 – 1981
- Westinghouse Electric Company .....1974 – 1976

Education

- BS, Engineering and Applied Science, Yale University, 1974
- MSE, Systems Engineering, University of Pennsylvania, 1980

Professional Certifications

- CISSP, ISC2, Issued 10/2008, #317949
- GSEC (SANS/GIAC Security Essentials Certification), 10/2005 and 10/2009, #550097

Professional Development

- Directory Services, including iPanet and OctetString (now Oracle), Microsoft, IBM (Tivoli), and Radiant Logic; building on Banyan's StreetTalk Directory Service to become proficient with other LDAP-based directories and virtual directories for design, installation, and appropriate usage, 1997-2010
- Metadirectory Services from ISOCOR (included in products by Critical Path, iPlanet, and Sun) and Zoomit (purchased by Microsoft and now part of Forefront Identity Manager), design, installation, and appropriate usage of these tools for integrating disparate directory services, 1999-2004
- Web Access Management tools from Netegrity (now CA SiteMinder) and IBM (Tivoli Access Manager), design, installation, and appropriate usage of these tools for providing Single Sign-On while protecting web sites, 1998-2004
- Identity Management tools from Netegrity (now CA IdentityMinder), Sun, IBM Tivoli, Microsoft, and Novell; design, installation, and appropriate usage of these tools for managing user accounts across multiple user repositories with both administrator control and self-service, 2002-2008
- IBM Rational tools and processes, to understand and follow the project lifecycle methodology, 2005-2006
- SANS Security training, in-depth and pre-certification training, 2005-2010
- Sestus Virtual Token Multi-Factor Authentication, design, installation, and integration of this tool with Web Access Management tools, 2009
- RSAM, design, installation, and appropriate usage of this tool for managing Risk and Compliance, 2009
- Ounce Labs (IBM) Static Application Security Testing Suite, now part of IBM AppScan, design, installation, and appropriate usage, 2009
- Unisys Stealth Solution for Networks, design, installation, and appropriate usage of this tool for protecting network traffic by Community of Interest, 2010.

Other Accomplishments

- SANS Advisory Board
- GIAC Test Author
- SecureWorld Philadelphia Steering Council
- IJIS (Integrated Justice Information Systems) Institute Security Advisory Committee
- Presented Master's Thesis ("Real-Time Algorithms for Multiple Missile Evasion: A Game Theoretic Approach) at the 1979 Pittsburgh Conference on Modeling and Simulation and the 1979 International Conference on Information Sciences and Systems in Patras, Greece.

UNISYS

[redacted]
Financial Manager

Key Skills and Knowledge

- Clear understanding if the billing process including accounts receivable and accounts payable
- Diligently supported consolidation of billing reports into a single invoice
- Designed and implemented many process improvements for the oversight of billing
- Recipient of a Unisys Excellence Award.

Skills Summary

Over 25 years of financial management experience using analytical, goal oriented, profit driven skills; supported the Commonwealth for 13 years at Harrisburg. Consistently achieved financial objectives set forth by directors; extensive experience overseeing billing activities; single invoicing processes, and consolidation of the billing process to reduce steps and cost of processing. Diverse range of managerial responsibilities in both field and corporate job functions. Demonstrated managerial proficiency with a proven ability to develop and train staff.

Employment History and Related Experience

Manager, Commonwealth of Pennsylvania, Harrisburg, Pennsylvania 1999– Present

Financial Analysis

Provides financial management support for the outsourcing contract with the Commonwealth of Pennsylvania; delivers financial management and billing oversight for several Unisys internal organizations and subcontractors (including IBM and Bell Atlantic) in accordance with the financial plan; improved the support provided to retained staff at Commonwealth of Pennsylvania for planning, change orders, and pricing of new scope proposal.

Coordinates financial analysis, report consolidation, new business pricing analysis, billing, cash collections, receivables, inventory control, and facilities; Reduced costs involved in inventory control by improving the collection methods and unifying the various sources of data.

Extensive experience delivering consolidated single invoice reports to the Commonwealth, improved the delivery model to remove redundant information bringing increased accuracy for last minute edits; improved packaging tools providing positive confirmation all components were present before transmission to the Commonwealth.

Business Operations Data Center, Cherry Hill, New Jersey 1992 – 1999

Manager

Delivered financial management and invoicing for the Unisys Cherry Hill Outsourcing Service Center including; financial analysis, reporting, new business pricing analysis, billing, cash collections, receivables, inventory control, and facilities; supported migration of clients to [redacted] MN data center as part of Unisys data center consolidation.

Key executive in transition process of migrating clients to and from the data center; expanded outsourcing revenue four-fold during the period 1992 through 1996; and increased client base from one client in 1992 to 10 clients in 1996.

Financial and Asset Control Government Systems, McLean, Virginia 1986 – 1992

Manager

Managed the Department of Defense income statements and balance sheets for the Unisys Government Systems Division; managed billing, invoicing, and processing of financial statements; directed activities of the billing and accounts receivable organizations to improve cash collections and maximize balance sheet impact.

Financial Strategy Customer Services Division, Blue Bell, Pennsylvania 1982 – 1986

Manager

Responsible for the establishment and analysis of software, service, and maintenance profit plans and actual reporting for a $1.1 billion division. Improved system analyst productivity trends, eliminated deficiencies, and identified opportunities to increase revenue.

Employment History

- Manager, Business Operations / Commonwealth of Pennsylvania, Harrisburg, Pennsylvania 1999– Present
- Manager, Business Operations Data Center, Cherry Hill, New Jersey 1992 – 1999
- Manager, Financial & Asset Control Government Systems, McLean, Virginia 1986 – 1992
- Manager, Financial Strategy Customer Services Division, Blue Bell, Pennsylvania 1982 – 1986
- Various Financial Analyst positions, Blue Bell, Pennsylvania 1972 – 1982

Education

- Masters of Business Administration, Temple University, Philadelphia, Pennsylvania, International Business, 1978
- Bachelor of Science, LaSalle University, Philadelphia, Pennsylvania, Accounting, 1971

Certifications

- ITIL V3 September 2012

UNISYS

[redacted]

Financial Analyst

Key Skills and Knowledge

- Wide range of billing experience and accounts receivable experience
- Supported the creation and improvement of consolidated billing processes for clients
- Solid background in single invoice processing for large clients.

Awards

Recipient of the Unisys Excellence Award and Silver Recognition Award for Unwavering Customer Commitment.

Skills Summary

Worked in Finance and Accounting since 1977, supported the Commonwealth for 14 years; committed to accountability, accuracy, communication and timelines. Provided extensive billing support for customers, has contributed immensely to the improvement of billing processes and procedures.

Employment History and Related Experience

Unisys Corporation, Commonwealth of Pennsylvania, Harrisburg, Pennsylvania 1999–Present

Project Controller / Financial Analyst

Provides project control (financial) and all financial reporting related to the $100 million per year outsourcing contract with the Commonwealth of Pennsylvania. Delivers financial reporting and analysis for corporate, local management, internal auditors, and external auditors; accomplishes a wide range of activities including; journal entries, internal billing, external billing, revenue recognition, cash collection, receivables, and asset database entries.

Prepares price impacts for the 21.01A Fee Schedule to support RFS and change order process. Developed internal processes to confirm the change order impacts agree with the timing used in the Commonwealth Invoicing Program. Confirmed the 21.01A Fees Schedule was revised after customer signature of change order.

Took positive steps to accomplish change orders in Unisys system and support ordering of any equipment or software related to signed change order. At time of invoice, established processes to use current fees schedule when producing an integrated 'single invoice' for the Commonwealth. Additionally, these processes maintained alignment of internal Unisys invoices with the invoice sent to the Commonwealth.

AMP, Inc., Harrisburg, Pennsylvania 1997 – 1999

Financial Analyst

Created the consolidated version of the P&L reports and the Fixed Asset reports; maintained an asset pricing and management tool used enterprise-wide. Used Visual Basic to revise the Fixed Asset tool, incorporated corporate investment and profitability targets, improve efficiency of data entry, and extended management utility of the tool for the user community.

AMP, Inc., Valley Forge / Harrisburg, Pennsylvania 1983 – 1997

Pricing Accountant

Coordinated with internal and external users to generate pricing product packages; oversaw the run stream of all price books – both online and in print.

Researched and generated pricing on bulk and packaged items based on costs retrieved from various internal and external sources. Developed processes to organize and identify the customer specific items with unique packaging, labeling, or pricing structures. Reached out and forged professional relationships to accelerate the coordination of everything from pulling pricing from different internal divisions, to working with internal and external print shops, to verification, to large-scale mailings to customer database. Developed and published customer segment price books one to two annually.

Philadelphia Gear Corporation, King of Prussia, Pennsylvania 1977 – 1983

Accountant

Supported all assigned accounting activities including general ledger, cash, and P&L reporting. Maintained data content in various manual general ledgers including cash, investments, assets, liabilities and profit and loss accounts. Confirmed accuracy of cash transactions with banks, resolved numerous errors; submitted all monthly Balance Sheet and Profit and Loss analysis.

Employment History

- Project Controller / Financial Analyst, Unisys Corporation, Commonwealth of Pennsylvania, Harrisburg, Pennsylvania .....1999– Present
- Financial Analyst, AMP, Inc,, Harrisburg, Pennsylvania..... 1997 – 1999
- Pricing Accountant, AMP, Inc., Valley Forge / Harrisburg, Pennsylvania..... 1983 – 1997
- Accountant – Philadelphia Gear Corporation, King of Prussia, Pennsylvania.....1977 – 1983

Education

- Masters of Business Administration, St. Joseph's University, Philadelphia, PA, Finance, 1991
- Bachelor of Science, Pennsylvania State University, University Park, PA, Accounting, 1977

Certifications and Training

- ITIL V3 Foundations Certification September 2012
- Ethics Awareness Training January 2013
- Security Awareness Training December 2012

UNISYS

[redacted]

Service Excellence Officer

Key Skills and Knowledge

Leadership & Management

- Service Delivery Management
- Account Management
- Resource Management
- Transition Resource Management
- SLA & KPI Management
- Profit Optimization Leadership
- Service Delivery Leadership
- Governance Leadership.

Domain Expertise & Solutions

- Six Sigma Lean Black Belt
- ITIL V3 Foundations Certification
- Finance Management
- Transaction Costing
- Enterprise Pricing
- SOX Compliance
- Divestiture Investigation
- Divestiture Separation
- Service Delivery Scheduling.

Management Consulting Services

- Six Sigma Lean
- 3D Blueprinting Business Architecture Tools
- 3D Blueprinting Conducting GOIS Experiential Workshops.

Project and Program Management

- Six Sigma Lean
- Lean Management Systems
- Kaizen Facilitation
- Leader Standard Work
- Project Management
- CSIIP Facilitation
- Client Business Planning
- Change Management
- Knowledge Management: SharePoint
- Risk Management
- Organizational Leadership
- Team Management.

Productivity Tools

- Six Sigma Lean Tools
- ProVision & Minitab
- Microsoft Project
- Microsoft Office Suite

Skills Summary

Operations Management: Driving excellence in service delivery, account management, resource management, transition resource management and profit optimization through best in class Leadership, governance, collaboration, and innovation.

Certified Six Sigma Lean Black Belt: Providing leadership, Six Sigma principles, Lean principles and project management skills in determining process waste, root causes analysis, process improvement opportunities, improvement implementation through standard work processes, and making sure metrics and controls are established and maintained through leader standard work. Program savings are driven and supported through extensive financial experience and skills.

Employment History and Related Experience

Operations Management, Global Managed Services, North America 2011 - Present

Provided Leadership and Management for over $650 million Information Technology (IT) Managed Services organization. Directly responsible for over $20 million annual profit improvement in 2011 and 2012 through extensive workshops and best in class governance. Provided operations management for account management organization with more than 100 clients, while driving 98 percent achievement of over 1,000 SLAs and over 40 KPIs. Customer CSAT is at the highest level in four years. Facilitated client business planning and Continual Service Improvement workshops for key accounts. Provided resource management and leadership for 5,100 employees onshore and offshore, including requisition approval, contractor furlough, extensions, and conversions. Reengineered numerous operational processes, and leveraged offshore resources to streamline operations by more than30 percent. Key leader/contributor in driving overall NA profitability to all-time highs in 2012 in a highly leveraged and matrixed outsourcing organization.

Quality Project Management Experience

Commonwealth of Pennsylvania, Account Process Optimization Workshop 2012

Provided senior leadership and Kaizen facilitation in 2012 Commonwealth of Pennsylvania Process Optimization workshop. Analyzed client business objectives, identified opportunities to meet client expectations, reviewed contractual billing requirements, delivery processes, and implementation schedules. Identified server technology, discovery and mapping tools, security architecture, and VMware opportunities. Reviewed and implemented process efficiencies in ITSM7 implementation, c-RIM ADDM tool implementation, and ITIL data center processes. Specific outputs and deliverables were: improved client satisfaction, enhanced process and tool functionality, and streamlined ITIL delivery processes.

Commonwealth of Pennsylvania, ITSM7 Transition Kaizen Workshop 2009

Managed and facilitated Kaizen workshops to transition Commonwealth of Pennsylvania from Remedy 6.3 to ITSM7. Specifically conducted a gap analysis for c-RIM, incident management, problem management, and change management. Gaps existed in 66 percent of the standard ITIL processes. Created detailed implementation plan to identify Unisys Roles and Responsibilities, Commonwealth responsibilities and dependencies, Partner dependencies, and associated risks. ITIL process improvements were identified in the configuration management database, change management CAB improvements, incident severity definitions, and Incident ticket creation policies. Clearly defined specific impacts, risks, associations, and interrelationships/touch-points for each ITIL process. The results were a detailed implementation plan which allowed for the smooth transition of the Commonwealth from a Remedy 6.3 to the ITSM7 infrastructure. This implementation significantly enhanced the service management capabilities while implementing an ITIL best practice framework for service management.

Billing Improvement Lean Kaizen and Leader Standard Work 2009

Facilitated the NA Billing Kaizen workshop. Process mapped current processes, identified waste, process mapped improvements, implemented improvements and appropriate controls. Driving six sub-teams to address the entire end to end billing improvement processes. Working collaboratively with Field operations and off shore GOIS maintenance administration. Identified $530 thousand, year to date, in additional revenue by assigning $100 thousand quotas to the CSMs. Implementing U-ACT changes to simplify maintenance proposals and verify that maintenance is always proposed and contracted for if there is a maintenance Price. Implemented over 15 standard work processes and over six leader standard work processes to drive cultural change and continuous improvement. Improved the maintenance price increase process and the contract expiration, warranty only expiration, and warranty upgrade expiration reporting.

- Knowledge Management: SharePoint
- Service Delivery Scheduling
- Business Objects Reporting
- Hyperion Reporting.

Piloting three party Purchase Order process improvements to validate Kaizen improvements identified. Improving retroactive cancellations and improving the billing cycle time through collaborative standard work processes and leader standard work. Built significant rapport and working relationship with key stakeholders and driving leader standard work within the GOIS service delivery management structure. Working to coordinate the end to end billing process and the GMA/TPC integration process to confirm that all key metrics and processes are addressed and there is no overlap. Implementing the billing improvement findings within ITO and INTL.

Forecasting Accuracy Kaizen 2008

Forecasting was significantly improved from a ten percent adverse revenue impact in 3Q08 to a positive revenue impact of 4 percent. This was a significant increase in revenue forecasting accuracy. Proactively interfaced with the Kaizen Team to establish the quick win goals, specific actions, timelines, deliverables, and controls. Innovative ideas were immediately implemented. Removed escalations and internal meetings from the CSM's role in order to transform their responsibilities to include client account management. Discipline was evident through extensive communication sessions to confirm all objectives and actions were understood clearly and timelines kept. The results were the beginning steps in transforming the CSMs from a purely service delivery role back into a client facing service manager who is proactively working with their clients in managing the business. Forecasting accuracy has been maintained within three percent throughout each month in 2009.

Infrastructure Support Services Account Profitability Improvement 2008

Worked aggressively with the core WW ISS team to analyze the current state, determine the go forward strategy, provide a governance process to manage the change, Implemented specific action plans for over 20 accounts to generate API profit improvement. Achieved $2.1 million of P&L savings on a $1.8 million target for multi-vendor services accounts. Conducted extensive work on the burden allocation model. Refined the model to be more accurate for Field operations. Worked directly with each theatre and API lead to verify accuracy and effective utilization of the model in resetting full year targets. Developed program governance, program improvements, lessons learned, to provide continuous controls and improvements to the API process.

NYC Transit Appointment Booking and Scheduling Software 2008

Conducted extensive analysis with NYCT management to identify ways to improve client satisfaction, provide greater visibility to SLAs and Call types, Improve management of customer service technicians and identify resource efficiencies to improve client P&Ls. Used Six Sigma Lean principles to reduce backlog, improve SLAs, increase CIR efficiencies, and standardize process and tools. Developed process maps and metrics to measure backlog, call volumes, closed calls per technician, and Average technician time. Analyzed monthly data to determine effectiveness within the campus environments, busses, subways, and normal replacement processes. Analyzed the bid model vs. the current 1Q08 actuals. Implemented click scheduling on the campus environment, a new management structure to manage CIRs, implemented CIR tools: PDAs, service console, paging, electronic CSOs, and Bomgar remote support. Implemented significant control reports to manage processes on a daily basis: Daily CIR IPC reports, weekly reports, trending reports for closed calls per day, backlog, incomplete calls, missed calls, and average technician time per CIR. A significant finding was that staffing needed to be based on the third busiest day versus the overall average to cover the variability in daily call volumes. This level of staffing would allow for peak periods and in maintaining a very low backlog of open calls. Increasing the average calls closed per day to above six would account for the five HC targeted. Finally average technician time was analyzed to determine additional opportunities to improve CIR productivity, establishing best practices and using creative resourcing for high volume days.

Amgen Appointment Booking & Scheduling Software 2007

By applying SSL principles along with strong leadership and communication skills, successfully reducing the Amgen headcount from 34 to 19, thus improving the account profitability by $780 thousand annually and streamlining the service delivery processes. The reduction in headcount and increased service delivery efficiencies has been successfully maintained while continuing to receive high client satisfaction ratings. The success of this project demonstrated to the GOIS service delivery management that the appointment booking processes and click software can be successfully implemented in an Information Technology Outsourcing (ITO) account, with dedicated CIRs vs. a shared resource pool serving multiple accounts. Driving change and creating value was demonstrated through strong leadership and communication. Communicating the facts, showing the inefficiencies and opportunities, through process maps and data analysis allowed the Amgen team to focus on problem resolution. Working collaboratively with the Amgen team to overcome barriers built much needed trust. Effective use of control reports convinced the team of the proven value and effectiveness of the appointment booking process, the click software, and SSL

principles being applied.

Divestiture Project 2007

Drove significant change, created a result that was extremely valuable, and demonstrated extensive creativity and leadership in applying SSL and 3D-blueprinting processes and methodologies. I was able to complete the functional responsibilities of the Finance Director for a divestiture and proactively leverage my SSL knowledge and skills to create a detailed documented Divestiture Process. The finished document provided corporate treasury with the following results: documented divestiture goals and hierarchies, documented divestiture rules and dependencies, defined specific implementation actions, documented accurate process maps - Finance, identified specific issues and risks, Established standards and controls for future divestitures, improved negotiations and forecasting, a framework for increased profits from repeatable and consistent, documented divestiture methodologies. Provided a Communication Plan by creating a SharePoint portal for corporate development/treasury where all of the divestiture documentation resides. Also developed links to specific divestiture SharePoint sites for greater Program specific details. Provided a 100 page divestiture book to corporate treasury/development: Outlined the contents; how to use it for future divestitures; and leverage the knowledge learned to create efficiencies in future divestiture processes.

EMC Mean Time to Repair 2006

By using SSL tools and processes we accomplished the project's goal to reduce the Mean Time To Repair (MTTR) in Asia from 3.2 hours in 2005 to 2.3 in 2006 and in Europe from 2.4 in 2005 to 2.1. This resulted in $500 thousand per year in productivity improvements and savings. More importantly the SSL methodology drove extensive changes and created value within EMC and UIS by: listening to the voice of the customer; looking at process changes based on data driven results vs. assumptions; improving communications and collaboration. EMC and UIS changed multiple processes and methodologies in improving service delivery and client satisfaction: targets were established for MTTR that are measured and tracked; process changes within EMC's Help Desks were implemented; improvements into EMC's tools and diagnostic were launched; UIS service delivery processes were improved; and UIS marketing and sales to EMC are leveraging SSL by demonstrating Unisys' commitment to quality through the use of SSL. These changes and value are a direct result of strong Leadership and excellent communication skills in driving Unisys operating principles and SSL culture within the EMC project.

Director of Finance 2005

Managed enterprise maintenance pricing for $1billion Global Service line. Used Industry data in setting competitive pricing. Developed and implemented a transaction based client profitability tool that provided clear easy to use reporting to understand client profitability, product profitability, average technician time productivity reporting and process controls. Developed Risk Management analysis and confirmed that the Enterprise Service Delivery processes and P&Ls were Sarbanes Oxley Compliant.

Employment History

Unisys 1981 – Present

Education

- Bachelor of Science, Business Administration, University of Delaware
- Masters in Divinity, 2 of 4years, Immaculate Conception Seminary
- Permanent Diaconate Program, 4 of 6 years, Archdiocese of Philadelphia

Professional Certification

- Certified Six Sigma Lean Black Belt
- ITIL V3 Framework Certification.

Professional Training

- Introduction to 3D Blueprinting
- Introduction to Business Architecture at Unisys
- Business Architecture Tools for Practitioners
- 3D Blueprinting Conducting Experiential Workshops for Infrastructure and Outsourcing
- Six Sigma Black Belt Leadership
- Lean Management Systems
- Lean Kaizen Facilitation

- Introduction to Waste
- Innovation
- Managing Others Through Change
- Change Leadership
- Six Sigma Lean Executive Training
- 3D Blueprinting Support for Six Sigma Lean at Unisys
- Organizational Leadership
- GOIS Risk Management
- Communicating and Reinforcing Change
- Overcoming the Challenges of Change
- Managing Others Through Change Simulation
- Fundamentals for Facilitation
- Facilitation at a Glance
- Microsoft Office 2003: Beginning Project Professional
- Creating and Defining a Project
- Specifying and Assigning Resources
- Tracking and Reporting Progress
- Advanced Customization
- Sharing Project Data and Working with Macros
- Organizing and Managing Project Information
- Working Collaboratively
- Enterprise Project Management
- Advanced Analysis of your Project
- SDF Seminar Series - Project and Program Management
- Diversity/Inclusion
- Effective Interviewing
- Blueprint For Success
- Living the Brand
- Speakeasy-Plan Presentations That Work and Developing your Speaking Style.

UNISYS

[redacted]

Service Delivery Executive (Program Manager)

Key Skills and Knowledge

Project and Program Management of Large-scale Programs

Data Center Migration and Consolidation of Large Scale Implementations

Data Center and Help Desk Service Management

Quality Improvement Program Implementation and Management

Organizational Reengineering

Incident Management

Business Continuity and Disaster Recovery

Creation of Training Programs

Management Experience:
Data Center Strategy & Direction
Contract Negotiations
Budgeting and Administration
Customer/Technical Support
Outsourcing
Vendor Relations
Account/Project Management
Software Development
Upgrades
Training and Support Planning
Acquisition/Integration (Voice/Data)
Workload Planning
Methodologies

Technical Expertise:
Operating Systems
VMS, OS2, NT, Unix, and Novell,
RSTS/E with RMS file structure
XENIX, VMS, Pathworks, VMS Cluster,
Windows 3.X, 95, 98, Windows 2000
Windows for Workgroups

Application Software
Lotus Notes
PC-Anywhere
PowerPoint
Scheduler
Excel
Word
Internet Explorer
Visio
Magic
SQL

Skills Summary

Accomplished Service Delivery Executive Director; delivers over 28 years of commercial and state government experience. Possesses broad and unique experience in Information Technology domestically and globally, proven experience effectively managing people, services, and assets with budgets over $60MM.Solid track record of reengineering IT systems to improve performance and efficiencies with a proven ability to lead highly energized teams to accomplish specific goals. Possesses the ability to maximize resources efficiency in fast paced environments, and is experienced working with Outsourcing and managing third party contracts. Has gained extensive experience through IT Operational Management responsibility for the Aon and Textron accounts with direct accountability for 3 major Business units (Bell Helicopter, Textron Financial, Textron Marine and Land Systems), coupled with varied major account management experience including: Nortel Central Region, plus 75 small sites in North America, other Texas sites, Motorola, United Technology Corp, Marconi, Budget Rental Cars, British Aerospace

Demonstrated Results

- Skilled at maintaining executive relationships at the “C” and Director levels
- Developed short and long term IT Strategies with Customer
- Seamlessly transitioned: 200 employees from Nortel & 400 employees from Textron to CSC
- Lead service improvement teams to enhance account performance
- Full operational leadership experience with WAN and LAN technologies
- Established electronic commerce distribution channels worldwide
- Management of large mainframe systems supporting local and remote
- Experienced in off-shoring resources to India, Noida, Hyderabad mainly
- Completed ITIL V3 Foundation Class
- Implemented system management disciplines with full disaster recover
- Management responsibility for Global desktop/laptop refresh program including migration from Windows NT to XP
- Proficient in planning and executing Customer presentations

Reorganized and consolidated internal functions to streamline operations and reduce cost

Professional Experience

CSC, Global Delivery Executive, BHP Corporation, 2010 - 2012

Global IT management account governance. Oversee Business Units, State government units, Mining, Oil, and Gas for BHP Billiton Corp. Spearheaded the rollout of VOIP Worldwide; implemented a Service Delivery Excellence Program with detailed quality audits and Risk Program to address SLA issues. Created and implemented employee recognition program; managed three managers with over 100 employees. Increased and protected availability of customer support with strong continuity of operations plans. SLA reporting from 83% to 99.95%

CSC, Service Executive, Aon Corporation (Client), 2007 - 2010

Global management responsibility for Aon business units (including State governments); reports directly to the account Vice President. Responsible for overall management of all CSC IT-Towers to assure SLA Compliance, customer satisfaction, risk assessments, and financial targets are accomplished. Organized and accomplished program audits to ensure program compliance. Managed networks, midrange workstations, 30K LAN/voice ports, and 2,000 servers; managed over 300 indirect reports and 5 manager, and accountable for $60MM budget.

CSC, Director of Service Delivery, Textron Corporation (Client), 2004 - 2007

Global management responsibility for three Textron business units, reported directly to the account Vice President, Deputy for the Vice President for overall account operations. Directed three Service Delivery managers, provided overall management of all CSC Towers to ensure risk management, SLA Compliance, customer satisfaction, and financial targets met. Maintained 900 Mainframe MIPS, 30,000+ workstations, 40,000 LAN/voice ports, 2,000 servers. Oversaw 400+ indirect reports and 8 managers. Accountable for $40MM budget. Established a Continuity of Operations Program. Worked directly with the Customer CIO and associates on a day to day basis to develop and maintain business relationships that fostered provision of services

Programming Languages
VMS Basic and Visual Basic

Communications Equipment
Infortron, Racal-vadic, Racal-milgo
Multi-tech multiplexers and modems
Emulex terminal servers, Mitel, Meridian
Cisco, Nortel, ATM

Computer Hardware
IBM 3060/2070 series, CPU operations
Digital PDP 11/70
Micro VAX 4000 and 3100
AS400, Sun, HP/Compaq, Dell

CSC, Sr. Manager, Service Delivery, Nortel Corporation (Client), 2001 - 2004

Overall responsibility for over 94 customer sites; provided overall management of 11,400 desktops, 2300 printers, 12 ATM backbones, 9 1Gig backbones, 1400 Unix servers and 1900 NT servers. Successfully completed Company's Service Delivery Excellence and Catalyst (4.0) Delivery Team Workshop programs; delivered overall management of each Tower to ensure SLA compliance and customer satisfaction. Managed 43 direct reports and 300+ indirect reports, provided employee team building, and development, provided Vendor, Asset, Lease management and Warehouse Logistics.

Specific Accomplishments:

- Rolled out 6,200+ desktop/laptops campus wide
- Transitioned 200+ employees to CSC
- Provided service for several state government contracts
- Implemented processes & procedures to create a standard operating model
- Completed a wall-to-wall inventory of over 25,000 devices
- Reduced operating support costs by over 50% ($2.5MM per year) by outsourcing to a managed service. Initiated the project, wrote the RFP and SOW, evaluated bids and negotiated the final contract.

CSC, Sr. Manager, IT, ING Corporation (Client), 1999 - 2001

Managed Information Technology Outsourcing; created solutions resolving system problems. Responsible for managing all aspects of Desktop, LAN and Mainframe environment, directly supervised, scheduled and trained managers, indirectly 43 employees.

Specific Accomplishments:

- Successfully hired new management staff and implemented on-going training programs
- Reduced sub-contractor labor costs by 50%
- Spearheaded completion of NT rollout
- Managed a plan to reduce Back Office servers from 131 to 52 servers
- Implemented a plan to reduce BackOffice operating system from 4 to 1
- Supported other managers to increase SLA performance by 35%
- Implemented CSC Service Delivery Excellent Program
- Established CSC Service Delivery Excellent program

CSC, Sr. Desktop & LAN Manager, CSC/Aon Corporation (Client), 1998 - 1999

Directly supervised and trained managers, indirectly 25 employees; managed all aspects of Desktop, and LAN environment.

Specific Accomplishments:

- Reduced 3rd party contracting firms by 45%
- Developed metric systems for all departments to measure performance
- Implemented daily and weekly meetings Staff meeting by department
- Created and implemented employee recognition programs
- Implemented remote control of desktops for 130 users
- Created and distributed employee job descriptions
- Reorganized Queue management to improve problem and/or project resolution
- Worked in conjunction with the SDEP team to incorporate SDEP compliance
- Instituted standard meetings with CIO and/or their staff

POWERCOM-2000, Inc., Global IT Manager, 1995-2098

Global Management IT and Administrative Services. Employed analytical functions to resolve system problems. Directly supervised, scheduled and trained managers with 60+ employees. Managed setup and relocation of corporate and branch offices in Stanstead, UK, Dublin, Ireland, and Melbourne, Australia.

Specific Accomplishments:

- Negotiated worldwide agreement with Advantis for electronic commerce
- Implemented a strategic plan lowering operating cost by $550,000 annually
- Developed LAN based Telex system saving in excess of $40,000 annually
- Designed and planned Virtual Private Network savings over $45,000
- Off-shored 23% of staff while increasing productivity

Grayson Corporation, Director of Operations, 1983-1995

Managed all aspects of large and complex networks; principle troubleshooter for network problems, provided level III problem resolution; and was the organizational spokesperson on technology issues. Recruited, supervised, trained and motivated support staff.

Specific Accomplishments:

- Designed and implemented an EDI system for Sears' warehouse operation
- Implemented a business plan that decreased corporate operation costs by 14%
- Reduced computer operation expenses by 40%
- Integrated an order entry voice response system with fax capabilities

Education

- Louisiana Tech University

Professional Certification

- ITIL V3
- SDEP- (Service Delivery Excellence Program)
- CSC-Management Program
- CSC-Financial and Budget Program

Honors and Awards

- Appreciation Award for infrastructure Transformation Programs
- Appreciation Award Customer Service

UNISYS

IBM

[redacted]

Delivery Project Executive

Key Skills and Knowledge

- Leadership
- Communication
- Over 10 years Commonwealth experience
- PMI Certified
- ITIL Certified

Skills Summary

Experienced leader with strong professional, interpersonal and communication skills. Adept at leading teams to adapt technology tools to address problems. Known for achieving results in situations involving large, matrix-based organizations to meet client objectives. Over 10 years supporting the Commonwealth of Pennsylvania agencies.

Employment History and Related Experience

IBM Global Technology Services, Harrisburg, Pennsylvania 2002 – Present

Commonwealth Delivery Project Executive

Managed the delivery of service using 60 Full-Time Equivalents from 30 departments in support of the Commonwealth's IBM operating system platforms (z/OS, z/VM, z/VSE, Linux on System z, iSeries, and AIX) included in the IBM scope of the Unisys Data PowerHouse (DPH) contract.

- Managed the team supporting multiple Commonwealth agencies, which included systems management, and operations support to achieve outstanding service level and customer satisfaction results
- Managed contracts of ISVs and monitored progress with monthly reviews to ensure billing accuracy
- Implemented successful continuity planning and testing processes, leveraging success as a model for test scenarios on other contracts.

IBM Global Services, Allentown, Pennsylvania 1999 – 2002

Senior Delivery Manager Agere Systems

Managed high quality delivery of Windows and Unix desktop support, Windows NT and Unix server services and hardware maintenance for 5000 end users and 700 servers located across the United States.

- Directed nine departments and over 200 staff members. Implemented TCO review that identified over $2 million in customer cost savings
- Supported development of new contract proposals, included a new event-based model for EUS service delivery
- Developed strong team of subcontractors to effectively deliver support required by the contract.

IBM Global Services, Reading, Pennsylvania 1997 – 1999

Service Delivery Manager

Managed desktop and Windows NT/Unix server support department at three different customer locations.

- Recognized for nurturing the professional relationships necessary to confirm the successful delivery of technical infrastructure to support the Lucent Microelectronics division global Oracle application suite deployment
- Implemented local metrics and peer reviews for managing desktop installation processes, owned compliance audit responsibilities and maintained consistently low past-due ticket counts.

Additional Employment

- IBM, Quality Engineer, Research Triangle Park, North Carolina, 1994 – 1997
- IBM, Industrial and Quality Engineer, Poughkeepsie, New York 1986 – 1994
- IBM, Resource Planning Manufacturing Engineer, Lexington, Kentucky 1982 – 1986

Education

- M.S. Mechanical Engineering, Penn State University, 1982
- B.S. Mechanical Engineering, Penn State University, 1981

Certifications

- Project Management Professional, Project Management Institute #03217, 1994
- ITIL V3 Foundations Certification, 2012; IBM Certified Delivery Project Executive, 2012

UNISYS

IBM

[redacted]

IBM Project Executive

Key Skills and Knowledge

- Experienced Project Executive
- Contract governance and customer satisfaction
- Transition and tranformation management
- Certified Project Management professional
- Over 15 years experience managing multi-tower IT outsourcing agreements
- Over five years experience supporting the Commonwealth of Pennsylvania.

Skills Summary

A seasoned IBM Project Executive located in the Harrisburg, PA area with over 30 years of experience in leadership positions, contract governance, project management, customer satisfaction, and new business growth in IBM.

For over 15 years, career focus has been in Strategic Outsourcing (SO) delivery and project management supporting multiple tower Information Technology (IT) outsourcing agreements that included:

- Data center operations, mainframe server management and print servers
- Midrange server management, service desk, and end-user support
- Network services and application maintenance services
- State and local government, and healthcare, insurance, and telecommunications industries

Employment History and Related Experience

IBM Corporation, Harrisburg, Pennsylvania 2012 – Present

Project Executive

Manage the IBM scope of the Unisys Data PowerHouse (DPH) contract, which includes service delivery for data center services: mainframe (z/OS, Linux on System z), iSeries, AIX and disaster recovery for multiple agencies within the Commonwealth.

- Successfully improved the quality of deliverables, operations compliance and overall contract performance to meet customer requirements and service levels
- Considered to be the leading developer of new business to meet business goals and changing objectives of the Commonwealth.

IBM Corporation, Multiple Locations 2011 – 2012

Project Executive,

Short-term/interim Project Executive for five Public Sector, healthcare accounts.

- Focused on contract governance, delivery of services, and transformation activities
- Successfully transitioned responsibilities to replacement Project Executives

IBM Corporation, MTA-New York City Transit, New York, New York 2005 – 2011

Project Executive

Managed delivery of data center services including mainframe, midrange, network, help desk, and disaster recovery. Responsibilities successfully performed included contract startup, development of consumption-based billing model, transition of six agencies into the IBM data center, and transformation activities post-data center migration.

- Transitioned into the scope of services a newly formed agency that used Linux virtual machines in support of a PeopleSoft ERP system as a shared service for its customers
- Negotiated an extension to the existing contract in 2010 for an additional three years, which included a new methodology to track and bill midrange services, which provided savings to the customer over the new term.
- Improved overall service level attainment throughout the life of the contract
- Implemented a tape encryption solution to address the State of New York mandate for securing portable media.

IBM Global Technology Services, Harrisburg, Pennsylvania 2000 – 2005

Deputy Project Executive

Provided direction to project office staff and the delivery organization in support of data center services to the Commonwealth of Pennsylvania agencies.

- Effectively performed gathering customer requirements, proposal development, and project planning with responsibilities associated with delivery of services and new business growth
- Managed the transition of services for two of the seven agencies migrating into the Data PowerHouse.

IBM Global Services, Philadelphia, Pennsylvania 1999 – 2000

Delivery Project Executive

Accountable for the overall delivery and fulfillment of the contract deliverables, including the transition of services for support of the help desk, desk-side services, network, and data center operations. Developed the transition and transformation plans to support the ACE-INA move to IBM, and set up the initial program office support structure.

IBM Global Services, Allentown, Pennsylvania 1996 – 1999

Senior Delivery Manager,

As a senior manager, led a team of 300 staff, including 12 managers, to support the Lucent Technologies IT services agreement in Allentown and Reading, Pennsylvania, and Berkley Heights, New Jersey.

- Led the transition of services for the Microelectronics division from Lucent to IBM, which included on-boarding of the Lucent employees hired by IBM as part of the contract
- Managed the Y2K project for Microelectronics.

IBM Software Solutions, Pennsylvania and Colorado 1981 – 1995

Multiple Positions,

Held multiple positions, including management positions, in IBM Software Manufacturing Solutions (a division of IBM to support the manufacturing of software media and publication materials).

Education

- Attended Regis University, Denver, Colorado

Certifications

- IBM Certified Project Executive since 2007
- IBM Certified Project Manager – Executive since 2001
- Project Management Professional (PMP) since 1997

Right to Represent Acknowledgement

By signing below, I acknowledge and agree that Unisys Corporation has the exclusive right to represent me, as an employee of Unisys Corporation, to the Commonwealth of Pennsylvania in all matters of and relating to work assignment and performance relating to the Commonwealth of Pennsylvania, Office of Administration Data Center Computing Services Request for Proposal #RFP6100022698, throughout the procurement process for such RFP and for the term of any prime contract that may result from such procurement, including any extensions, for the type of positions identified below. This Right to Represent Acknowledgement shall be in addition to any other applicable agreements with Unisys Corporation.

[redacted] [redacted]

Candidate Name Candidate Signature

Senior Enterprise Infrastructure Architech

Position Title(s)

03 Jun 2013

Date

Right to Represent Acknowledgement

By signing below, I acknowledge and agree that Unisys Corporation has the exclusive right to represent me, as an employee of Unisys Corporation, to the Commonwealth of Pennsylvania in all matters of and relating to work assignment and performance relating to the Commonwealth of Pennsylvania, Office of Administration Data Center Computing Services Request for Proposal #RFP6100022698, throughout the procurement process for such RFP and for the term of any prime contract that may result from such procurement, including any extensions, for the type of positions identified below. This Right to Represent Acknowledgement shall be in addition to any other applicable agreements with Unisys Corporation.

[redacted] [redacted]

Candidate Name Candidate Signature

Service Delivery Manager
Position Title(s)

05/31/2013
Date

Right to Represent Acknowledgement

By signing below, I acknowledge and agree that Unisys Corporation has the exclusive right to represent me, as a service partner representative of Unisys Corporation, to the Commonwealth of Pennsylvania in all matters of and relating to work assignment and performance relating to the Commonwealth of Pennsylvania, Office of Administration Data Center Services Request for Proposal #RFP6100022698, throughout the procurement process for such RFP and for the term of any prime contract that may result from such procurement, including any extensions, for the type of positions identified below. This Right to Represent Acknowledgement shall be in addition to any other applicable agreements with Unisys Corporation.

[redacted] [redacted]

Candidate Name Candidate Signature

Agency Infrastructure Architect
Position Title(s)

Date 6-17-2013

Right to Represent Acknowledgement

By signing below, I acknowledge and agree that Unisys Corporation has the exclusive right to represent me, as an employee of Unisys Corporation, to the Commonwealth of Pennsylvania in all matters of and relating to work assignment and performance relating to the Commonwealth of Pennsylvania, Office of Administration Data Center Computing Services Request for Proposal #RFP6100022698, throughout the procurement process for such RFP and for the term of any prime contract that may result from such procurement, including any extensions, for the type of positions identified below. This Right to Represent Acknowledgement shall be in addition to any other applicable agreements with Unisys Corporation.

[redacted] [redacted]

Candidate Name Candidate Signature

Incident Management Manager

Position Title(s)

5-28-2013

Date

Right to Represent Acknowledgement

By signing below, I acknowledge and agree that Unisys Corporation has the exclusive right to represent me, as an employee of Unisys Corporation, to the Commonwealth of Pennsylvania in all matters of and relating to work assignment and performance relating to the Commonwealth of Pennsylvania, Office of Administration Data Center Computing Services Request for Proposal #RFP6100022698, throughout the procurement process for such RFP and for the term of any prime contract that may result from such procurement, including any extensions, for the type of positions identified below. This Right to Represent Acknowledgement shall be in addition to any other applicable agreements with Unisys Corporation.

[redacted] [redacted]

Candidate Name Candidate Signature

Service Excellence Officer
Position Title(s)

May 28, 2013
Date

Right to Represent Acknowledgement

By signing below, I acknowledge and agree that Unisys Corporation has the exclusive right to represent me, as an employee of Unisys Corporation, to the Commonwealth of Pennsylvania in all matters of and relating to work assignment and performance relating to the Commonwealth of Pennsylvania, Office of Administration Data Center Computing Services Request for Proposal #RFP6100022698, throughout the procurement process for such RFP and for the term of any prime contract that may result from such procurement, including any extensions, for the type of positions identified below. This Right to Represent Acknowledgement shall be in addition to any other applicable agreements with Unisys Corporation.

[redacted] [redacted]

Candidate Name Candidate Signature

Agency Account Manager

Position Title(s)

May 29, 2013

Date

Right to Represent Acknowledgement

By signing below, I acknowledge and agree that Unisys Corporation has the exclusive right to represent me, as an employee of Unisys Corporation, to the Commonwealth of Pennsylvania in all matters of and relating to work assignment and performance relating to the Commonwealth of Pennsylvania, Office of Administration Data Center Computing Services Request for Proposal #RFP6100022698, throughout the procurement process for such RFP and for the term of any prime contract that may result from such procurement, including any extensions, for the type of positions identified below. This Right to Represent Acknowledgement shall be in addition to any other applicable agreements with Unisys Corporation.

[redacted] [redacted]

Candidate Name Candidate Signature

AGENCY ACCOUNT MANAGER

Position Title(s)

May 28, 2013

Date

Right to Represent Acknowledgement

By signing below, I acknowledge and agree that Unisys Corporation has the exclusive right to represent me, as an employee of Unisys Corporation, to the Commonwealth of Pennsylvania in all matters of and relating to work assignment and performance relating to the Commonwealth of Pennsylvania, Office of Administration Data Center Computing Services Request for Proposal #RFP6100022698, throughout the procurement process for such RFP and for the term of any prime contract that may result from such procurement, including any extensions, for the type of positions identified below. This Right to Represent Acknowledgement shall be in addition to any other applicable agreements with Unisys Corporation.

[redacted] [redacted] _____

Candidate Name Candidate Signature

June 6, 2013
Date

Right to Represent Acknowledgement

By signing below, I acknowledge and agree that Unisys Corporation has the exclusive right to represent me, as an employee of Unisys Corporation, to the Commonwealth of Pennsylvania in all matters of and relating to work assignment and performance relating to the Commonwealth of Pennsylvania, Office of Administration Data Center Computing Services Request for Proposal #RFP6100022698, throughout the procurement process for such RFP and for the term of any prime contract that may result from such procurement, including any extensions, for the type of positions identified below. This Right to Represent Acknowledgement shall be in addition to any other applicable agreements with Unisys Corporation.

[redacted] [redacted]

Candidate Name Candidate Signature

UNISYS CHANGE MANAGER

Position Title(s)

5/29/13

Date

Right to Represent Acknowledgement

By signing below, I acknowledge and agree that Unisys Corporation has the exclusive right to represent me, as an employee of Unisys Corporation, to the Commonwealth of Pennsylvania in all matters of and relating to work assignment and performance relating to the Commonwealth of Pennsylvania, Office of Administration Data Center Computing Services Request for Proposal #RFP6100022698, throughout the procurement process for such RFP and for the term of any prime contract that may result from such procurement, including any extensions, for the type of positions identified below. This Right to Represent Acknowledgement shall be in addition to any other applicable agreements with Unisys Corporation.

[redacted] [redacted]

Candidate Name Candidate Signature

Agency Infrastructure Architect

Position Title(s)

5/29/13

Date

Right to Represent Acknowledgement

By signing below, I acknowledge and agree that Unisys Corporation has the exclusive right to represent me, as an employee of Unisys Corporation, to the Commonwealth of Pennsylvania in all matters of and relating to work assignment and performance relating to the Commonwealth of Pennsylvania, Office of Administration Data Center Computing Services Request for Proposal #RFP6100022698, throughout the procurement process for such RFP and for the term of any prime contract that may result from such procurement, including any extensions, for the type of positions identified below. This Right to Represent Acknowledgement shall be in addition to any other applicable agreements with Unisys Corporation.

[redacted] [redacted]

Candidate Name Candidate Signature

FINANCE MANAGER

Position Title(s)

5-29-13

Date

Right to Represent Acknowledgement

By signing below, I acknowledge and agree that Unisys Corporation has the exclusive right to represent me, as an employee of Unisys Corporation, to the Commonwealth of Pennsylvania in all matters of and relating to work assignment and performance relating to the Commonwealth of Pennsylvania, Office of Administration Data Center Computing Services Request for Proposal #RFP6100022698, throughout the procurement process for such RFP and for the term of any prime contract that may result from such procurement, including any extensions, for the type of positions identified below. This Right to Represent Acknowledgement shall be in addition to any other applicable agreements with Unisys Corporation.

[redacted] [redacted]

Candidate Name Candidate Signature

Sr Project Controller / Financial Analyst

Position Title(s)

5/29/2013

Date

Right to Represent Acknowledgement

By signing below, I acknowledge and agree that Unisys Corporation has the exclusive right to represent me, as an employee of Unisys Corporation, to the Commonwealth of Pennsylvania in all matters of and relating to work assignment and performance relating to the Commonwealth of Pennsylvania, Office of Administration Data Center Computing Services Request for Proposal #RFP6100022698, throughout the procurement process for such RFP and for the term of any prime contract that may result from such procurement, including any extensions, for the type of positions identified below. This Right to Represent Acknowledgement shall be in addition to any other applicable agreements with Unisys Corporation.

[redacted] [redacted]

Candidate Name Candidate Signature

____Client Architect_____

Position Title(s)

__5/30/13_____

Date

Right to Represent Acknowledgement

By signing below, I acknowledge and agree that Unisys Corporation has the exclusive right to represent me, as an employee of Unisys Corporation, to the Commonwealth of Pennsylvania in all matters of and relating to work assignment and performance relating to the Commonwealth of Pennsylvania, Office of Administration Data Center Computing Services Request for Proposal #RFP6100022698, throughout the procurement process for such RFP and for the term of any prime contract that may result from such procurement, including any extensions, for the type of positions identified below. This Right to Represent Acknowledgement shall be in addition to any other applicable agreements with Unisys Corporation.

[redacted]
Candidate Name

[redacted]
Candidate Signature

Vice President
Position Title(s)

6/6/13
Date

Right to Represent Acknowledgement

By signing below, I acknowledge and agree that Unisys Corporation has the exclusive right to represent me, as an employee of Unisys Corporation, to the Commonwealth of Pennsylvania in all matters of and relating to work assignment and performance relating to the Commonwealth of Pennsylvania, Office of Administration Data Center Computing Services Request for Proposal #RFP6100022698, throughout the procurement process for such RFP and for the term of any prime contract that may result from such procurement, including any extensions, for the type of positions identified below. This Right to Represent Acknowledgement shall be in addition to any other applicable agreements with Unisys Corporation.

[redacted] [redacted]

Candidate Name Candidate Signature

Transition Director

Position Title(s)

5/28/2013

Date

Right to Represent Acknowledgement

By signing below, I acknowledge and agree that Unisys Corporation has the exclusive right to represent me, as an employee of Unisys Corporation, to the Commonwealth of Pennsylvania in all matters of and relating to work assignment and performance relating to the Commonwealth of Pennsylvania, Office of Administration Data Center Computing Services Request for Proposal #RFP6100022698, throughout the procurement process for such RFP and for the term of any prime contract that may result from such procurement, including any extensions, for the type of positions identified below. This Right to Represent Acknowledgement shall be in addition to any other applicable agreements with Unisys Corporation.

[redacted]

Candidate Name

[redacted]

Candidate Signature

AGENCY ACCOUNT MANAGER

Position Title(s)

5/29/13

Date

Right to Represent Acknowledgement

By signing below, I acknowledge and agree that Unisys Corporation has the exclusive right to represent me, as an employee of Unisys Corporation, to the Commonwealth of Pennsylvania in all matters of and relating to work assignment and performance relating to the Commonwealth of Pennsylvania, Office of Administration Data Center Computing Services Request for Proposal #RFP6100022698, throughout the procurement process for such RFP and for the term of any prime contract that may result from such procurement, including any extensions, for the type of positions identified below. This Right to Represent Acknowledgement shall be in addition to any other applicable agreements with Unisys Corporation.

[redacted] [redacted]

Candidate Name Candidate Signature

Service Level Management Analyst
Position Title(s)

June 9, 2013
Date

Right to Represent Acknowledgement

By signing below, I acknowledge and agree that Unisys Corporation has the exclusive right to represent me, as an employee of Unisys Corporation, to the Commonwealth of Pennsylvania in all matters of and relating to work assignment and performance relating to the Commonwealth of Pennsylvania, Office of Administration Data Center Computing Services Request for Proposal #RFP6100022698, throughout the procurement process for such RFP and for the term of any prime contract that may result from such procurement, including any extensions, for the type of positions identified below. This Right to Represent Acknowledgement shall be in addition to any other applicable agreements with Unisys Corporation.

[redacted] [redacted]

Candidate Name Candidate Signature

Engagement Executive

Position Title(s)

5/29/13

Date

Right to Represent Acknowledgement

By signing below, I acknowledge and agree that Unisys Corporation has the exclusive right to represent me, as an employee of Unisys Corporation, to the Commonwealth of Pennsylvania in all matters of and relating to work assignment and performance relating to the Commonwealth of Pennsylvania, Office of Administration Data Center Computing Services Request for Proposal #RFP6100022698, throughout the procurement process for such RFP and for the term of any prime contract that may result from such procurement, including any extensions, for the type of positions identified below. This Right to Represent Acknowledgement shall be in addition to any other applicable agreements with Unisys Corporation.

[redacted] [redacted]

Candidate Name Candidate Signature

Deployment Manager

Position Title(s)

6/5/2013

Date

Right to Represent Acknowledgement

By signing below, I acknowledge and agree that Unisys Corporation has the exclusive right to represent me, as an employee of Unisys Corporation, to the Commonwealth of Pennsylvania in all matters of and relating to work assignment and performance relating to the Commonwealth of Pennsylvania, Office of Administration Data Center Computing Services Request for Proposal #RFP6100022698, throughout the procurement process for such RFP and for the term of any prime contract that may result from such procurement, including any extensions, for the type of positions identified below. This Right to Represent Acknowledgement shall be in addition to any other applicable agreements with Unisys Corporation.

[redacted]
Candidate Name

[redacted]
Candidate Signature

CISO
Position Title(s)

May 31, 2013
Date

Right to Represent Acknowledgement

By signing below, I acknowledge and agree that Unisys Corporation has the exclusive right to represent me, as an employee of Unisys Corporation, to the Commonwealth of Pennsylvania in all matters of and relating to work assignment and performance relating to the Commonwealth of Pennsylvania, Office of Administration Data Center Computing Services Request for Proposal #RFP6100022698, throughout the procurement process for such RFP and for the term of any prime contract that may result from such procurement, including any extensions, for the type of positions identified below. This Right to Represent Acknowledgement shall be in addition to any other applicable agreements with Unisys Corporation.

[redacted] [redacted]

Candidate Name Candidate Signature

Change Analyst

Position Title(s)

6/5/13

Date

Right to Represent Acknowledgement

By signing below, I acknowledge and agree that Unisys Corporation has the exclusive right to represent me, as an employee of Unisys Corporation, to the Commonwealth of Pennsylvania in all matters of and relating to work assignment and performance relating to the Commonwealth of Pennsylvania, Office of Administration Data Center Computing Services Request for Proposal #RFP6100022698, throughout the procurement process for such RFP and for the term of any prime contract that may result from such procurement, including any extensions, for the type of positions identified below. This Right to Represent Acknowledgement shall be in addition to any other applicable agreements with Unisys Corporation.

[redacted] [redacted]

Candidate Name Candidate Signature

Service Delivery Executive (Program Manager)

Position Title(s)

06/11/2013

Date

June 19, 2013

Annually, IBM employees are required to certify that they have read, understood and will comply with the IBM Business Conduct Guidelines (BCG). An excerpt of the section concerning conflicts of interest, assisting a competitor and competing against IBM follows:

> Conflicts of Interest
>
> A conflict of interest occurs when you advance a personal interest at the expense of IBM's interests. Some conflicts of interest can be avoided through careful foresight and planning. Others are unavoidable. In some cases, the mere potential for or perception of a conflict can be problematic. It is up to you to avoid situations in which your loyalty may become divided. Some common conflicts are addressed below.
>
> Assisting a Competitor
>
> An obvious conflict of interest is providing assistance to an organization that markets products and services in competition with IBM's current or potential product or service offerings. You may not, without IBM's consent, work for such an organization in any capacity, such as an employee, a consultant or as a member of its board of directors.
>
> Competing against IBM
>
> Also prohibited are individual pursuits that could conflict with IBM's current or future business interests.

A violation of any IBM guideline can result in disciplinary action, including dismissal.

The IBM employees whose resumes have been included in this submission have:

- Been reminded of their obligations under the IBM BCG; and
- Approved of the inclusion of their resumes.

[redacted]

[redacted]

IBM Project Executive

Representative Resumes

This tab contains all of the Representative Resumes that were requested in sections of Schedule F. The table below is organized in alphabetical order by project role. The table lists requested roles first followed by additional positions for Commonwealth consideration. In each project role, the named individual representative resumes are listed in alphabetical order. All resumes under this tab are organized in alphabetical order by last name providing you easy access to the specific resumes you wish to view.

Project Role	Representative Resume
AIX Administrator	Resource 1 Resource 2 Resource 3 Resource 4 Resource 5 Resource 6
Batch Administrator	Resource 7 Resource 8
Database Analyst	Resource 9 Resource 10 Resource 11 Resource 12
Database Architect	Resource 13 Resource 14 Resource 15 Resource 16 Resource 17
Firewall Administrator	Resource 18 Resource 19 Resource 20 Resource 21 Resource 22
Hyper V VMware Certified Admins	Resource 23 Resource 24 Resource 25 Resource 26 Resource 27

Project Role	Representative Resume
Linux Administrator	Resource 28 Resource 29 Resource 30 Resource 31 Resource 32 Resource 33 Resource 34 Resource 35
Mainframe Infrastructure Architect Engineer	Resource 36 Resource 37 Resource 38 Resource 39 Resource 40 Resource 41
Mainframe System Programmer (IBM)	Resource 42 Resource 43 Resource 44 Resource 45 Resource 46 Resource 47 Resource 48 Resource 49 Resource 50 Resource 51
Mainframe System Programmer (Unisys)	Resource 52 Resource 53
Microsoft Product Specialist (e.g. Exchange, SharePoint)	Resource 54 Resource 55 Resource 56 Resource 57 Resource 58 Resource 59 Resource 60 Resource 61 Resource 62 Resource 63 Resource 64 Resource 65

Project Role	Representative Resume
Midrange Infrastructure Architect Engineer	Resource 66 Resource 67 Resource 68 Resource 69 Resource 70 Resource 71 Resource 72
Performance Specialist	Resource 73 Resource 74 Resource 75 Resource 76 Resource 77 Resource 78 Resource 79
Security Administrator	Resource 80 Resource 81 Resource 82 Resource 83
Security Analyst	Resource 84 Resource 85 Resource 22
Security Architect	Resource 80 Resource 86 Resource 87 Resource 88 Resource 89
Security Specialist	Resource 90
Storage Management Administrator	Resource 91 Resource 92 Resource 93 Resource 94 Resource 95 Resource 96 Resource 97
Third Party Software Specialist	Resource 98 Resource 99

Project Role	Representative Resume
UNIX Administrator	Resource 100 Resource 101 Resource 102 Resource 103 Resource 104 Resource 33 Resource 105 Resource 106 Resource 6
Windows Server Administrator	Resource 107 Resource 108 Resource 109 Resource 110 Resource 111 Resource 112 Resource 113 Resource 114 Resource 115 Resource 116 Resource 117 Resource 118
x86 Infrastructure Architect Engineer	Resource 119 Resource 120 Resource 26 Resource 115 Resource 121 Resource 122 Resource 88
Other Positions	
Active Directory	Resource 123 Resource 124 Resource 65
Application Support	Resource 28 Resource 58 Resource 125 Resource 126 Resource 127 Resource 99

Project Role	Representative Resume
	Resource 128
Automation Engineer	Resource 129
Backup Administrator	Resource 130 Resource 131
Network Engineer	Resource 18 Resource 132 Resource 21
Patch Management	Resource 114
Project Manager	Resource 133 Resource 134 Resource 135
Technical Writer	Resource 136 Resource 137

This page intentionally left blank.

AIX Administrator

This page intentionally left blank.

Resource 1

AIX Administrator

Key Skills and Knowledge

Operating Systems

- IBM AIX 4.3.3
- 5L, 5.2, 6.4
- SunOS 5.X
- Solaris, Windows/NT 2000
- 2000 Server
- 2003 Server
- IBM/MVS Mainframe
- Novell 4.11
- Cisco

Hardware

- IBM RS6000 PSeries and ESeries P615,P6C3, P6E3, S80, M80, H80, P610, PC1, P6E1, P620, P630, P690 via HMC console
- ESeries 7017, 7025, 7026, 7028
- servers HP ProLiant servers
- Compaq NT servers
- Sun
- Cisco 8500's switch
- DLT tape jukebox
- Sun UltraSparc
- Sun V120, V240, V490, V890, Sun 6800, T2000

Software

- Windows NT 4sp5
- Novell
- Cisco Catalyst
- Apache Web server
- IBM including Tivoli
- TSM
- running 3rd party SW such as ESM, SSH,
- MS Office
- Backup SW Veritas
- NETBACKUP
- LEXANDRIA
- CA
- MacAfee Anti-Virus
- Oracle v7 - v8
- Hummingbird
- Lotus Notes
- DNS/NIS+

Professional Summary

A seasoned Systems Administrator specializing in UNIX / AIX environments. Has experience with backup/recovery, networking, and a number of server architectures. Has been responsible for the planning and installation of complex multi-vendor environments. A versatile Information Technology (IT) Specialist who has also been responsible for data center operations.

Employment History and Related Experience

Aqua America, Systems TSM Administrator, 2011 – 2012

Responsibilities included TSM administration for disaster recovery planning, vault rotation, AIX administration that includes upgrades, hardware and software updates (third party installs).

- Provided user management and security management.

Bank of America, Systems Administration, Production Control, and Engineering, 2007 – 2010

Responsibilities ranged from Tivoli maestro scheduling to correcting failures in an AIX environment which required root access.

- This position was developed to have a continual problem determination operation.
- Had access to maestro user which ran as root.
- The decision was made not to Sudo the ID.
- Responsible for IBM PSeries servers.
- Responsible for AIX. Additionally, I was responsible for Tivoli Suite running Maestro scheduling with WEBADMIN on AIX servers with clients consisting of, HACMP, LPAR with HMC console control, Standalones, Blades, SAN, EMC assistance, Oracle, DB2, SAS, Abinitio, and Veritas Netback.
- Managed the operating systems Maestro file systems/TSM.
- Developed and planned File space utilization for the software.
- Handled all account ID and group IDs.

Lancaster General, System Administrator, 2006 – 2007

Provided basic AIX system maintenance and performance monitoring utilizing home grown tools at that location.

- Supported Docitweb and Work Load Manager which included on-call rotation every other week

IBM

Resource 1

AIX Administrator

- Abinitio
- SAS
- ORACLE
- DB2

- Responsible for the resolution of performance issues caused by application runaway processes, file system maintenance, disk replacements, and TSM issues
- Supported HW such as M80, H80, P610, PC1, P6E1, P620, 7026 2028, LPAR, and HACMP failovers

IBM, Sr. System Administrator, 2006 – 2006

Supported the installation and administration of a multi-platform environment.

- Responsible for daily upgrades.
- Responsible for file system creation, performance issues, and third-party installations. Hardware included P615, P6C3, P6E3, S80, M80, H80, P610, PC1, P6E1, P620, P630, P690 via HMC console, ESeries 7017, 7025, 7026, and 7028.

JP Morgan, Sr. System Administrator, 1988 – 2006

As a systems administrator, assisted with the ordering the hardware with the project manager in accordance with the client's requirements.

- Responsible for capacity planning and SSA/external SAN conversions
- Installed operating system, configured the network, and set up file systems accordingly along with all applications and Backup solutions (Tivoli Storage Management)
- Maintained and utilized Kornshell scripts
- Supported the development / QA / Production environments. Hardware included P615, P6C3, P6E3, S80, M80, H80, P610, PC1, P6E1, P620, P630, and P690 Eseries 7017, 7025, 7026, and 7028
- Responsible for the installation and maintenance (LPAR via HMC Console)
- Responsible for all 3rd installations including SAP, running with Oracle 9I
- Responsible for backups and disaster recovery architect utilizing Alexandria, NetBackup, and Veritas software
- Worked closely with the DBAs for backup solutions and restores
- Reported Performance Monitoring and Disk / Memory Utilization
- Responsible for capacity and memory vs. CPU utilization. This was significant considering the disk farm utilized was over 400 Terabytes of data shared by many lines of business
- Responsible for reporting the following on a weekly basis:
  - Multi-resource monitoring and tuning including capacity planning
  - CPU-related performance (vmstat, iostat, topas, and sar)
  - Memory-related performance(vmstat, topas, ps,and lsps)
  - Disk I/O-related performance (iostat, lvmstat, lsps, lsattr, and lsdev)
  - Network-related performance (netstat, iostat, topas, enstat, and ifconfig)
  - Performance tracing when required (ps, pstat, and topas)

Resource 1

AIX Administrator

- Workload Manager installation and modifications when applicable (wlm)
- Transmissions across a multi-platform environment

- Responsible for handling transmission issues between UNIX, Mainframe, Windows, and Sun hardware and software
- Monitored production support.
- Responsible for cause and analysis.

Chilton Company, Shift Supervisor/Data Center Manager, 1985 – 1989

Supervised five Computer Operators. Became the Shift Leader and ultimately was promoted to Shift Supervisor.

- Maintained throughput of the mainframe
- Coordinated new and existing systems between operators and programmers
- Solved mechanical problems with prints, tape driver and printers

Pennsylvania Manufactures Association of Pennsylvania, Computer Operator, 1980 – 1985

- Maintained throughput of all systems.

Education

- Southern Methodist University, Dallas, TX
- Pierce Junior College, Philadelphia, PA

This page intentionally left blank.

UNISYS

Resource 2

AIX Administrator

Key Skills and Knowledge

- AIX
- HACMP
- Virtualization
- VIOS
- SEA
- Etherchannel
- HMC
- TCP/IP
- Power7
- LPARs
- Ksh
- Perl
- Nagios
- HTML
- WebSphere
- Wily
- NetView

Professional Summary

20 years of systems administration experience delivering network engineering, administration, and development. Skilful engineer, considered to be a subject matter expert for AIX issues. Develops tests and maintains business recovery plans, plans and implements tape-less Tier-1 recovery systems. Implements automated system configuration documentation, implements SNMP server monitoring, provides clear technical documentation and written procedures for operations. Skills include:

- Troubleshot and perform root cause analysis of server hardware, software, and network issues using tools such as nmon, topas, tcpdump, iptrace, errpt, and system diagnostics
- Plan and implement SAN storage for AIX servers, including sizing of LUNs, HBA redundancy, load balancing, and elimination of SPFs; accomplish capacity planning, performance monitoring, and tuning
- System architecture design of complete TSM solution including servers, networks, ProtecTier/VTL, IBM 3500, and Brocade switches
- Teach public and private CNME, NetView, and Nways courses throughout the USA and abroad, including China, India, Australia, England, Canada, Puerto Rico, Jamaica, Brazil, and Israel
- Certified network management consultants and administrators worldwide.

Employment History and Related Experience

Unisys Corporation, Systems Administrator-1,
Harrisburg, PA 2011 – Present

Responsible for more than 100 P7 servers in a multi-tiered highly available, redundant environment.

- Install, configure, and administer:
  - P7 LPARs, HMC, VIO, SEA, LHEA, and paging spaces
  - AIX PowerHA in a active/standby configuration
  - NFS, DNS, Kerberos, and SNMP
  - Network redundancy using Etherchannel and 802.11q, tagged VLANS
  - MQ monitoring with custom scripts.
- Develop, test, and maintain business recovery plans using NIM and Shadow Copied storage for tapeless recovery of Tier 1 systems.
- Implement automated system configuration documentation with cfg2html for audit and compliance.
- Implement SNMP server monitoring through custom scripting.
- Provide clear technical documentation and written procedures.

UNISYS

Resource 2

AIX Administrator

- Upgrade the firmware of power frames, HMCs, and PCI cards.
- Provide 24/7/365 on-call support.

First Citizens Bank, Systems Engineer Consultant,
Raleigh, NC 2001 – 2011

Senior AIX system administrator and engineer responsible for more than 100 P4 through P7 servers in a multi-tiered highly available, redundant environment.

- Accomplished installation, configuration, and administration of:
  - AIX HA-CMP in a multiserver mutual takeover configuration
  - P5, P6, and P7 LPARs, HMC, VIO, SEA, LHEA, and paging spaces
  - NFS, DNS, SNMP, and Advanced Shell scripting using ksh, and Perl
  - Hitachi and IBM (N and XIV) SAN storage with multipath software
  - High availability networks using Etherchannel and 802.11qand tagged VLANS
  - Tivoli Storage Manager (TSM) 6.2 server
  - MQ, WebSphere, WAS, and Apache Web servers
  - Tivoli Key Lifecycle Manager (TKLM) for IBM tape library encryption.
- Troubleshot and performed root cause analysis of server hardware, software, and network issues using tools such as nmon, topas, tcpdump, iptrace, errpt, and system diagnostics.
- Planned and implemented SAN storage for AIX servers, including sizing of LUNs, HBA redundancy, load balancing and elimination of SPFs; accomplish capacity planning, performance monitoring, and tuning.
- Designed the system architecture of a complete TSM solution, including servers, networks, ProtecTier/VTL, IBM 3500, and Brocade switches.
- Developed, implemented, maintained, and documented backup procedures and business recovery plans for AIX systems; provide clear technical documentation and written procedures.
- Implemented automated system configuration documentation to address audit requirements.
- Implemented automated backups of VIO server configuration using ssh keys, nfs, and crontab.
- Created scripted HMC builds for adding LPARs on new systems, eliminating the need for a GUI.
- Used SNMP for server, Brocade switch, network infrastructure availability and performance monitoring, and documentation. Used this data to check thresholds and alert support personnel.
- Gained experience with racking servers, cabling, hardware support and troubleshooting, firmware upgrades, PCI-X and PCI-e network cards, and expansion drawers.
- Implemented AS/400 (I-series) on Power5 and Power6 LPARs.
- Provided 24/7/365 on-call support.

UNISYS

Resource 2

AIX Administrator

Alliance of Professionals and Consultants, Inc.,
Tivoli Certified Consultant, Raleigh, NC 1995 – 2001

Integrated of Tivoli NetView and IBM Nways into enterprise management solutions. Developed and implemented custom solutions for customer management and automation needs. Worked with IGS to provide after-hours on-call support for NetView for a leading telecommunications company that provides 24x7, outsourced network management.

- Troubleshot software and hardware by telephone and in person.
- Developed courseware and taught the following courses:
  - Tivoli NetView for UNIX and NT
  - IBM Nways Suite (Element Managers) for UNIX and NT
  - IBM Certified Network Management Engineer (CNME certification).
- Taught public and private CNME, NetView, and Nways courses throughout the USA and abroad, including China, India, Australia, England, Canada, Puerto Rico, Jamaica, Brazil, and Israel.
- Certified network management consultants and administrators worldwide.

Additional Employment History

Pennsylvania Blue Shield, Camp Hill, PA	1992 – 1995
AMP Incorporated, Harrisburg, PA	1981 – 1992
Olivetti Corporation of America, Harrisburg, PA	1976 – 1981

Education

- 33 credits in Electronic Engineering Technology, Harrisburg Area Community College

Professional Certifications

- EXIN: ITIL Foundation v3
- IBM: Power HA for AIX II – Problem Determination
- IBM: AIX pSeries Administrator
- AIX HACMP Administration
- IBM/APC: Advisory – Certified Network Management Engineer (A-CNME)
- Tivoli: Certified Network Management Consultant
- Tivoli: Certified NetView Instructor

This page intentionally left blank.

UNISYS

Resource 3

AIX Administrator

Key Skills and Knowledge

- IBM Power VM, Virtual I/O Server, NPIV/vSCSI, Share processor pools, Share storage pools, Thin provisioning, Active memory sharing, Active memory extension, LPM, AIX, PowerHA, WPAR, Solaris, HPUX, BladeLogic

Operating Systems

- IBM AIX 5.3, 6.1 and 7.1, Sun Solaris 9/10,11, HP-UX 10/11i, RHEL 4.x/5.x, SUSE Linux 9/10

Hardware

- IBM Power7, power6 , IBM System x, HMC, IBM DS4K Storage, EMC DMX-4, SUNFIRE 25K/15K,v240 and HP 9000 Servers, Qlogic Infiniband Technologies

Networking

- TCP/IP, NIM, NFS v3 and v4, DHCP

System Software/Tools

- PowerHA 7.1.1/6.1/5.5, HACMP 5.x, Veritas Cluster Server, Veritas Storage Foundation, EMC powerpath Tools, Oracle cluster with ASM, BladeLogic Server Automation

Backup and Recovery Tools

- NBU, TSM, NIM, Sysback, CBMR, Ignite, Jumpstart and Kickstart

Professional Summary

More than 9 years of proven systems project experience including infrastructure administration on IBM AIX 5.x, 6.1, 7.1, RHEL, Solaris (9, 10 and 11), Windows Server, and EMC. Extensive experience with Server Virtualization with IBM PowerVM. Extensive experience in planning, designing, installing, configuring, implementing and supporting IBM AIX 5.3/6.1/7.1, RHEL 4.x/5.x, and Solaris 9/10/11. Experience in EMC SAN configuration with EMC NaviSphere, PowerPath, Access Logix, Replication Manager, Analyzer, EMC Control Center,Snapview, Mirrorview, and Sancopy.

- Experience in system tuning, security, backup, recovery and upgrades of IBM AIX, RHEL Solaris, and HP-UX
- Experience using Advance power Virtualization to virtualize production environment
- Experience using HMC to create VIO Server and Clients (LPAR)
- Configure virtualized network and storage using HMC and VIO server
- Experience Installing operating system onto VIO servers and LPARs
- Backup and restore VIO Server and LPARS using HMC, NIM, DVD, sysback, and CBMR
- Expertise in Planning, Installing, configuring IBM HACMP v 5.x and PowerHA 7.1/6.1
- Configured HACMP version 5.x, PowerHA 7.1/6.1 to monitor, disaster recovery, detect and react to failure events, allow the system to stay available during random and unexpected software problems, and also configured to react to hundreds of system events
- Extensive experience in installing, upgrading, removing, verifying packages using installp/rpm/yum utilities on AIX and RHEL
- Extensive experience in Tivoli Storage Management (TSM) and NetBackup
- Experience in managing LVM and file systems and paging space management in both AIX and RHEL
- Experience in monitoring System/Network Performance and Sendmail administration
- Experience in NFS, Send mail, ftp, remote access, security management, TCP/IP, and system troubleshooting skills
- Experience in Veritas File System, Veritas Volume Manager, and Veritas Cluster Server
- 24X7 on-call production support and troubleshooting problems related to IBM AIX P series servers, Solaris, and HP-UX servers
- Skilled in replacement/repair/upgrade of software, hardware, and firmware
- Excellent skills in Shell Scripts
- Experienced in managing LPAR on SAN (Storage Area Networks)

UNISYS

Resource 3

AIX Administrator

- Good Knowledge of EMC Symmetrix SRDF, Symmetrix DMX 1000/2000/3000 and latest DMX-4 Series, and Timefinder Operations.

Employment History and Related Experience

Unisys Corporation, System Administrator,
Harrisburg, PA 2011 – Present

Works in a large IBM PowerVM environment. Install new power7 frames according to project requirements. Designed a network to support the new virtualized environment. Migrated an AIX 5.3 environment to AIX 7.1. Migrated HACMP from version 5.x to PowerHA 6.1 and 7.1. Install backup and recovery systems such as sysback, NIM, and CBMR.

- Implement and support extensive security and monitoring facilities as mandated by the security agreement with the client. Worked on a new security baseline document for the client.
- Manage SAN storage such as IBM DS4k Series.
- Troubleshoot and fix performance problems.
- Provide on-call support for mission-critical systems.
- Participate in planned disaster recovery exercises for the client.

For the Commonwealth of Pennsylvania:

- Installed IBM Power Systems for the Production environment at DOR.
- Installed VIO servers at DOR.
- Installed AIX on IES and DOR LPARs.
- Designed and installed PowerHA for DOR and IES.
- Supported AIX for IES and DOR.
- Performed backup and recovery testing for IEs and DOR.

Target, AIX Administrator, Harrisburg, PA 2006 – 2007

Worked as an UNIX engineer to support RS/6000, and IBM pSeries systems. Worked on heterogeneous environments that had IBM AIX and Red Hat Enterprise Servers (AS 2.1, RHEL 3, and RHEL 4). Installed and upgraded operating systems for AIX 4.3.3, 5.1, 5.2, and 5.3. Setup and configured network TCP/IP on AIX servers and Linux

- Installed Solaris servers with the jumpstart method.
- Installed and configured HMC, LPAR, and VIO Server on pSeries servers (p590, p550, p520, p670, and p630).
- Managed user accounts and groups.
- Created and restored the backups in AIX 5L and Solaris.
- Planned and configured a SAN environment for TSM and ESS shark storage servers.
- Automated the Virtual I/O Server and HMC backups.

UNISYS

Resource 3

AIX Administrator

- Installed and configured Logical Partitions (LPARS) technology.
- Installed, configured, and troubleshot HACMP 5.3.
- Installed and administered TCP/IP, NIS/NIS+, NFS, DNS, NTP, automounts, Sendmail, and print servers.
- Worked independently and with offshore teams to accomplish the tasks on time according to the client's SLA.
- IBM AIX 5.3, 5.2, 5.1, and 4.3.3); pSeries servers (p590, p550, p520, p670, and p630); Sun Solaris 8 and 10; Red Hat Linux (AS 2 and RHEL 3/4); RS/6000 F50; Blade server JS20 and HS20; Apache Web Server; NIM; nPar; vPar; HP-UX Superdome; Tivoli Performance Viewer; Oracle; UDB DB2; EMC CLARiiON; Tivoli Storage Manager; DS 4300 storage server; tape libraries (STK 9470, STK 9310, TS 3580, TS3200, and TS3310); Veritas Net Backup; HP System Management tools; and Windows 2000 and 2003 Server.

Complete Care Technologies, System Administrator,
Atlanta, GA 2004 – 2006

Supported an internal UNIX/Linux environment. Configured and supported Windows, Linux, and UNIX environments on Intel and System p servers. Managed a virtualized environment that included VIOS and LPARS. Installed IBM DS4300, configured array, created logical volume, and mapped storage to servers.

- Upgraded and migrated AIX to version 5.3 using NIM.
- Performed Logical Volume Management (LVM) for Linux and UNIX.
- Patched AIX to the current ML level using NIM.
- Patched RHEL using the YUM facility.
- Backed up and restored the production environment using TSM, Sysback, and NIM.
- Supported ID administration.
- Provided on-call support for mission-critical systems.

Education

- Bachelor's degree in Electrical Engineering, University of Guyana, 1995

Professional Certifications

- IBM Certified Systems Expert – High availability for AIX technical support, and administration – v2
- IBM Certified System Administrator AIX 7
- BMC Certified Administrator: BMC BladeLogic Server Automation 8.1

UNISYS

Resource 3

AIX Administrator

Training

- HP-UX Fundamentals of the UNIX system, 2001
- HP-UX System and Network Admin I, 2001
- HP-UX System and Network Admin II, 2001
- AIX 5 L Problem Determinations – Tools and Technique, 2006
- Advance Power Virtualization Best Practice, 2006
- EMC Symmetrix Business Continuity – SRDF Solutions, 2008
- EMC Symmetrix Business Continuity – TimeFinder Solution, 2008
- PowerHA SystemMirror 6.1 Migration, Extended Configuration and Problem Determination, 2011
- PowerHA SystemMirror 7 Planning, Implementing, Customizing, Administrating, 2012
- BMC BladeLogic Server Automation 8.1 – Part 2 2012
- BMC BladeLogic Server Automation 8.1 – Part 3 2012

UNISYS

INFO-MATRIX CORPORATION

Resource 4

AIX Administrator

Key Skills and Knowledge

- AIX administration
- SAN administration
- Oracle Database administration
- Linux administration

Professional Summary

10 years of AIX experience, exceptional hands-on technical experience with administering AIX 4.3 and 5L, production support, installations, upgrades, performance and tuning, backup and recovery, disaster recovery planning and execution, system documentation, security administration, and SAN.

- Administer, install, and upgrade AIX operating systems on IBM RS 6000. Use versions 4.3.3 and AIX 5L on IBM pSeries
- Developed backup and recovery procedures in mksysb
- Developed system-level documentation; Implemented Secure Shell (ssh)
- Designed and established AIX security hardening standards and operational standards to comply with Sarbanes-Oxley, and HIPAA regulations
- Because proficient in performance monitoring and tuning using iostat, vmstat, netstat, sar, topas, snap, svmon, and other performance packages
- Manage AIX security hardening at the operating system level by customizing AIXPERT for high-level security to meet DHS ICE standards
- Implemented and maintained an IBM High Availability Cluster Multiprocessing (HACMP) environment on IBM P570s with AIX 5L
- Planned and implemented disaster recovery at the SunGard recovery center
- IBM pSeries Power5 Advanced Virtualization and Virtual I/O Server – LPAR
- Installed, upgraded, and managed on IBM pSeries Hardware Management Console
- Used Shell Scripting and experienced in provided 24X7 support on production AIX systems
- Installed third-party applications on AIX
- Set up batch jobs using cron
- Set up Name Server (DNS)
- Used vi editor
- Installed and configured sudo for security hardening
- Configured Network Time Protocol for synchronizing clocks on AIX servers with atomic clock
- Monitored AIX servers using NetView and Big Brother
- Installed and configured NetView and Big Brother
- Installed, configured, and managed the General Parallel File System (GPFS)
- Installed and configured the NIM master, clients
- Created NIM resources
- Performed upgrades in NIM.

Resource 4

AIX Administrator

Employment History and Related Experience

SAIC – DHS Immigration and Customs Enforcement,
AIX Administrator, Columbia, MD 2007 – Present

Accomplished installs, upgrades, and user administration of AIX 5L on P570s, manage DS4700 storage, install, manage, and upgrade HMC consoles, create LPARS, shuffle resources around LPARS using DLPAR. Set up security auditing on each LPAR, set up AIX security hardening using aixpert as the base line, and manage an HACMP environment. Manage GPFS file systems, manage a NIM master and clients, and install and administer Informatica.

- Install and administer Hyperion.
- Set up NIM mksysb backups.
- Install and configure SUDO.
- Performance monitoring using various tools such as topas, iostat, vmstat, and nmon.
- Tune kernel parameters
- Write Shell scripts to automate the environment.
- Write system-level documentation.
- Perform TSM backups and recovery.
- Set up tsm schedules.
- Manage the Hitachi Tagma storage USP1100.
- Create Oracle databases in Test environments.

Weis Markets, Inc, AIX Administrator, Sunbury, PA 2000 – 2007

AIX administrator for 13 production AIX servers – IBM RS600 H80, B80, P520, P630, and P570. Used AIX versions 4.3.3 and 5L). Managed an enterprise storage server – IBM 2105 F20. Set up AIX security for compliance with the Sarbanes-Oxley Act. Administered HACMP on IBM H80 and AIX 5L.

- Security Administrator for AIX and Oracle environments.
- SAN Administrator 2109 B32, DNS configuration and setup.
- Disaster recovery planning and implementation, participated in 48 hour test at SunGard recovery center.
- TSM Administrator using TSM version 5.1.5 on AIX 5L, IBM RS6000 P5.
- Backed up and recovered 140 servers.
- Managed mid-range application support.
- Mentored Information Technology (IT) associates on AIX, Oracle technical training, and system assurance procedures.
- Planned a strategy and introduced of Oracle database solutions to the Weis Markets enterprise.
- Led Oracle DB administrator for 12 production Oracle databases, Used Oracle 8i, 9i, and 10g on AIX platforms.

- Installed, configured, and set up RMAN scripts for hot and cold backups.
- Set up test environments and cloneD databases.
- Performance and tuning of applications using statspack, sql tracing, tkprof, and quest software where applicable; upgraded Oracle from version 8i to version 9i; performed Oracle patch upgrades from version 9.2.0.0 to version 9.2.0.8; and set up Oracle DB security for compliance with the Sarbanes-Oxley Act.
- Developed many interface programs in pro*c, managed a JSP/Java database development group; and developed programming standards and version control for a database development group.
- Developed a 4690 POS TLOG processing environment for data analysis for the Weis Markets enterprise solutions.
- Developed new applications and reengineered critical business applications infrastructure to maintain and promote expansion of the business plan and long-term corporate strategy.
- Developed and maintained technical procedures to meet regulatory requirements for HIPAA and Sarbanes-Oxley; developed and supported several interface programs in C, pro*c, shell, and Perl scripting; developed and supported SQLplus and PL/SQL programs.
- Installed and configured ETL tools such as VIA SERV to send and retrieve data from the mainframe VSAM to Oracle.
- Critical applications supported: IBM EM/EME electronic customer club programs – OLTP database and Oracle 9i on AIX; VRMS customer relationship marketing – data warehouse and Oracle 9i on AIX; retail expert loss prevention system – data warehouse and Oracle 10g on AIX; scan-based trading development – Data warehouse and Oracle 9i on AIX; human resource self-service development – Oracle 9i; Kronos time and attendance application – OLTP and Oracle 9i on AIX; Triceps warehouse system – C-tree database on AIX; and Pdx – pharmacy system on AIX, and many others.

Environment: Oracle 10gR2, Oracle 9i, Oracle 8i, Toad, SQL, PL/SQL, RMAN scripts, Oracle Enterprise Manager, pro*C, Shell Scripts, IBM RS 6000 (B80, H80, P520, P570, and P630), IBM ESS 2105 F20, SAN 2109 32-port switches, AIX 5L, TSM 5.1.5, HMC console, and Dynamic LPAR micro-partitioning.

Foot Locker, Oracle Database Analyst, Camp Hill, PA 1998 – 2000

Database administrator for a merchandise Planning system – Oracle 8i on AIX 4.3.3; database administrator for a PeopleSoft HRMS system – Oracle 8i on AIX 4.3.3; database administrator for a decision support system – Oracle 8i on AIX 4.3.3; responsible for performance and tuning of Oracle environments; responsible for RMAN backup and recovery.

- Upgraded databases and Applications.

- Developed shell scripts, Sqlplus, and PL/SQL programs.

Environment: Oracle 7.3, 8i, SQL, PL/SQL, RMAN scripts, Oracle Enterprise Manager, Shell Scripts, IBM RS 6000 - AIX 4.3.3, PeopleSoft HRMS.

Rite Aid Corporation, Database Administrator,
Camp Hill, PA 1997 – 1998

Introduced Oracle Database solution to Rite Aid retail store systems; developed a pricing system in Oracle Database and pro*c; and performed backups anD recovery with RMAN.

Environment: Oracle 7.3, SQL, PL/SQL, RMAN scripts, pro*c, Shell Scripts, UNIX operating system, C programming, and c-tree database.

Rite Aid Corporation, Systems Engineer, Camp Hill, PA 1994 - 1997

Developed a Point of Sale application for Rite Aid retail store systems in c and c-tree; maintained a store pricing system; developed several interface programs to send data to the host system; and performed system analysis, design, and implementation of store conversions during acquisitions.

Environment: Shell Scripts, C programming, c-tree database support, and UNIX.

Education

- B.S., Physics, Osmania University, India, 1981
- M.S., Physics, Osmania University. India, 1983
- M.S., Computer and Information Science, New Jersey Institute of Technology, Newark, NJ, 1991

UNISYS

IBM

Resource 5

AIX Administrator

Key Skills and Knowledge

- AIX/pSeries
- Systems administration
- UNIX
- Hardware and software maintenance
- VMware ESX 3, 4, 5; 540 VM
- HA and DRS clusters
- Oracle and Oracle applications on AIX

Professional Summary

Design, implement, and document UNIX and AIX complex solutions and environments, including analysis of current and projected server and storage requirements as well as integration of emerging storage technologies.

- Receive exceptional reviews from the client and IBM account and project teams
- Consultant for AIX and VMware environments, troubleshooting and providing health checks to promote continuous improvement of existing environments.

Employment History and Related Experience

Systems Engineer, Syniverse Technologies, Campbell, CA 2011 – Present

Provides consultative support for AIX/pSeries and virtualized (VMware) server environments in Tampa, Chicago, Dallas, and Sunnyvale.

- Directly interacts with senior management on IBM and AIX related issues.
- Maintained and upgraded hardware and software; resolved problems for hosts running VMware ESX 3, 4, and 5; supported 540 virtual machines across 10 separate hosts in two highly available (HA and DRS) clusters.
- Directly interacts with applications and systems architects to manage increasing demand for resources and bandwidth in a highly competitive and fast-moving business climate.
- Support database administrators and database/applications architects to resolve performance issues with Oracle and Oracle applications on AIX.

University of California, AIX Systems Administrator, San Francisco, CA 2008 – 2009

Supported operating systems for PeopleSoft Financials for the University's academic research community of approximately 500 users campus wide.

- Installed hardware consisted of pSeries managed systems (p520s, p560s, and p570s) using virtualized I/O, SAN, and local storage.
- Planned for future hardware refreshes and upgrades to operating system code (operating system and VIOS) in addition to periodic troubleshooting and problem resolution.

Longs Drugs Inc, Systems Consultant, Walnut Creek, CA 2007 – 2007

On-site contract consultant for the Longs Drugs Accounts Payable Development and Enterprise Server Group.

- Provided a recommendation to development and system engineering staff for the migration of Accounts Payable/PeopleSoft Application Tier servers from the legacy hardware and operating system.

Resource 5

AIX Administrator

- Delivered the recommendation to Longs Drugs corporate staff and upper management.
- Wrote documentation.

Digital Insight Corporation, Systems Engineer,
Westlake Village, CA 2006 – 2006

Supported AIX, Linux, Solaris and various applications in a Financial ASP (Application Service Provider) environment. Supported hardware on Network Appliance and EMC hardware platforms.

Jacobs Engineering Group, UNIX Systems Administrator,
Pasadena, CA 2003 – 2006

Performed general system and storage administration tasks in a global 24/7 environment for IBM pSeries 690/570 and Enterprise Storage Systems.

- Directly managed an operating system migration project for all AIX-based environments and used a partitioned configuration (DLPAR).
- Controlled direct interface support of database administration and application development and functional management teams.
- Managed storage allocation, backup strategy, performance tuning, capacity planning and resolving accessibility issues with databases and applications.

First Horizon Home Loans, Senior Systems Engineer,
Irving, TX 2001 – 2003

Performed general system administration tasks in a 24/7 environment for a 25-node RS6000 p690 (Regatta) plus various standalone RS6000 (MCA/PCI) and Sun Solaris servers in a team-centered IT environment.

- Worked with database administrators to manage storage allocation, back up the solution, and resolve accessibility issues with the databases and application.
- Managed a direct interface with and support of database administration, application development, and accounting groups.

UNISYS

Resource 35

AIX Administrator

Key Skills and Knowledge

- AIX 4, 5, 6, 7
- Power Systems
- VIO
- HMC
- Red Hat Enterprise Linux
- Oracle Enterprise Linux
- SUSE Linux
- Windows
- Scripting
- Networking
- Supervision
- Project Management

Professional Summary

Skillful system administrator with a wide range of experience on Commonwealth projects. 13 years of system analysis experience with 7 years of Commonwealth experience. Skilled in data recovery, migrations, implementations, maintenance, and network management

- Operating systems: AIX 4, 5, 6, and 7; Red Hat Enterprise Linux; Oracle Enterprise Linux; SUSE Linux; Windows NT, 2000, 2003, and 2008; and all Windows desktop operating systems
- Hardware: IBM standalone and IBM p-Series servers; IBM Hardware Management Consoles
- Software: Apache, Samba, VMware, Perl, Vbscript, PowerShell, UNIX/Linux Shell scripting, Oracle RAC clustering, and PowerHA clustering.

Employment History and Related Experience

Unisys Corporation, Senior UNIX Administrator,
Harrisburg, PA 2005 – Present

Responsible for the day to day management of all AIX and Linux systems in the Data PowerHouse (DPH) for various Commonwealth agencies. This includes server deployments through various processes, PowerHA configuration, user requests, and operating system-level migrations and patching.

- Managed a BladeLogic repository for Linux patching across various Linux platforms, including RHEL, SLES, and OEL.
- Developed scripts as needed to maintain a consistent environment across the entire data center
- Participate in all disaster recovery planning and testing. This includes:
  - Gathering customer requirements for recovery of various application and database servers
  - Developing the best recovery method of rootvg and non-rootvg as well as customer data
  - Executing recovery exercises and ensuring consistent support of the client as it proceeds with testing the recovered systems.
- Unemployment Compensation Management System
  - Built the new operating system image on the updated platforms
  - Worked with IBM experts on performance tuning, installed all IBM Power hardware including SAN and network cable (Ethernet and Fibre)
  - Frame mapped physical devices to ensure redundancy, stability, and performance of the systems.
- Collaborated with IBM experts to install VIO servers and PowerHA clusters, verifying the application and files were available with the shortest downtime for a smooth transition.

UNISYS

Resource 35

AIX Administrator

- Supported various business partners: DBAs, application developers, network, SAN/TSM, and Windows administrators for performance testing, and process flow, and so forth.
- Tivoli Monitoring/Network Support – Built a RHEL 5.X image to support application requirements for virtualization, security, and stability from virtual machines and Intel X86 physical servers.
- Red Hat Network Satellite (RHN Satellite) – Developed a RHN Satellite product for patching and maintaining a baseline platform for any RHEL system.
- Configured the central satellite server, set up the database, and registered and connected all clients to their appropriate patching cycle. Worked with the owners of the various RHEL clients.
- Established the most effective patching cycle for systems and ensured all systems were current and met the standards needed as set forth by the Office of Administration.
- Bureau of Workers Compensation – Upgraded field office servers from AIX 5.3 to AIX 6.1 and PowerHA to the most current supported levels in PowerHA 6.1.
- State Workers Insurance Fund – Supported the installation and upgrade maintenance of Dollar Universe application.
- Integrated Enterprise System AIX 5.3 to an AIX 7.1 migration – Developed and executed the migration plan needed to move from AIX 5.3 to AIX 7.1 to ensure the shortest downtime possible for the customer.
- Streamlined mksysb implementation – Generated a new mksysb creation/storage process to confirm redundancy of the backup images and to further enhance the availability of these images for disaster recovery.
- Department of Revenue AIX 5.3 to AIX 7.1 migration – Developed the migration plan needed to move from AIX 5.3 to AIX 7.1 to provide the shortest downtime possible for the customer, scheduled all of the systems in various maintenance windows to verify accurate time for testing and meeting the requirement for a phased implementation.
- Disaster recovery testing – Performed annual disaster recovery testing to ascertain the application's availability in a disaster; built, restored, and configured more than 30 AIX LPARs to fit the current production environment
- Maintenance window management – For an agency with monthly maintenance outage windows
  - Coordinate all events in each maintenance window, including communications between other departments at Unisys as well as Department of Revenue staff.
- Pennsylvania Liquor Control Board Integrated Business Management System (IBMS) Project –Develop a stable 5.X RHEL operating system image and deploy servers to the agency as needed according to the given build requirements using virtual machines with the required level of security, performed day-to-day maintenance of systems, processed change requests

UNISYS

Resource 35

AIX Administrator

related to systems, and responded to incidents.

- Department of Environmental Projection Oracle Enterprise Linux – Performed day-to-day work, including file system expansion, security monitoring and tuning, and storage and performance monitoring.
- Department of Public Welfare Oracle Enterprise Linux – Built and maintained a repository, maintained other OEL servers, and created new OEL servers as the agency sought to expand its environment.

Other Work Experience

EarthLink, UNIX Web Hosting Administrator	2000 – 2004
Global Management Services, Chief Technical Officer	2003 – 2005
Cross Connect Technologies, Network Engineer	2002 – 2003
Keystone Programming, Linux Administrator	1999 – 2000

Education

- Information Technology, Dauphin County Technical School, 2000

Training

- New Horizons: 1999 and 2000
- Microsoft Certified Systems Engineer Training

Professional Certifications

- IBM Certified System Administrator – AIX7
- ITIL v3
- Microsoft Certified Professional

This page intentionally left blank.

Batch Administrator

This page intentionally left blank.

UNISYS

IBM

Resource 7

Batch Administrator

Key Skills and Knowledge

- z/operating system
- Tivoli Workload Scheduler (TWS)
- Linux on System z
- JCL
- Rexx
- RACF

Professional Summary

Product support specialist for Tivoli Workload Scheduler (TWS) for z/operating system support distributed installations, customizations, and problem determination. Additional advanced TWS function expertise includes Dynamic Critical Path (Workload Service Assurance), z-centric agents, restart, and cleanup automation. Other areas of expertise include the use of z/operating system and Linux on System z system commands, RACF, TWS security and Tivoli Dynamic Workload Console (TDWC) interface. Also consult on TWS and related products and applications interfacing directly with commercial clients.

Employment History and Related Experience

IBM, TWS Subsystem Support Programmer, 1994 – Present

Supports TWS for z/operating system: product installation, customization, problem determination, consultation, Rexx programming, and TWS security for various customer accounts.

IBM, CLEAR Library Management Administrator, 1992 – 1994

Provide support for the CLEAR Library Management tool to house the programs for the z/operating system product development lab.

IBM, Application Programmer, 1989 – 1992

Develop Rexx programs for pricing and contract proposal support for two IBM business units.

IBM, Information Center Consultant, 1986 – 1989

Provide consultation on tools for the IBM Sterling Forest, New York location for development and graphics.

IBM, Application Programmer, 1984 – 1986

Develop Rexx programs for the IBM Poughkeepsie, New York location.

IBM, Information Centre Consultant, 1982 – 1984

Provide consultation on tools for the IBM Poughkeepsie, New York location for development and graphics.

Education

Bachelor of Science in Computer Science, Rutgers University

This page intentionally left blank.

UNISYS

Resource 8

Batch Administrator

Key Skills and Knowledge

- OS1100/2200
- ES7000
- Unisys A-Series
- Microsoft Windows
- UNIX-based servers
- Veritas
- NetBackup
- Backup Exec
- Avamar
- OPCONS
- LSAM
- BLSCHED
- BLLIB
- Remedy
- ITSM7
- HP OpenView
- SCOM
- ORION
- DEPCON
- Microsoft Word
- Microsoft Excel
- Microsoft Outlook
- Stargate
- ITIL v3 Foundations Certification

Professional Summary

25 years of Commonwealth experience. Strong ability to operate, trouble shoot, correct, and escalate issues on Unisys mainframe systems, Microsoft Windows, and UNIX-based servers.

- Supervise day-shift operations staff of the Commonwealth of Pennsylvania (Commonwealth of Pennsylvania) Data PowerHouse (DPH)
- Interface as needed with various Commonwealth agencies, technical support personnel, and management personnel
- Maintain operations documentation
- Maintain various operations reports.

Employment History and Related Experience

Unisys Corporation, Commonwealth of Pennsylvania,
Data Center Supervisor, Harrisburg, PA 2011 – Present

Supervise day-to-day operations of first shift operations staff at the Data PowerHouse. Plan, coordinate, and evaluate the work of staff in computer operations and operations support functions. Assign personnel, direct their work, and evaluate operational performance.

- Manage problem and change management of computer operations procedures and control mechanisms.
- Deliver quality assurance and security.
- Advise higher level managers on work problems of own unit and the impact of broader problem.
- Collaborate with other units to coordinate work changes.
- Plan, coordinate, and evaluate the work of staff in computer operations and operations support functions.

Unisys Corporation, Commonwealth of Pennsylvania,
Lead Computer Operator 1, Harrisburg, PA 1999 – 2011

Led the day-to-day operations of first-shift operations staff at the Data PowerHouse. This included monitoring Unisys mainframe systems, Microsoft Windows servers, and UNIX-based servers; monitoring and running backup jobs for multiple agencies; and escalating problems to appropriate management and tech support.

- Interfaced with mainframe and open systems-based customers on job and system problems.
- Represented operations during the PROMISE implementation of several Microsoft Windows, Sun-based servers.
- Worked with the customer and tech support to create operations documentation for this customer.

UNISYS

Resource 8

Batch Administrator

- Updated operations documentation as system enhancements were made.
- Participated in change meetings and other various customer meetings.
- Supervised first-shift operators, assisted with system problems, and coordinated operators' workload and assignments.
- Verified that change requests were started and completed as outlined on the change request.
- Updated daily system status, turnover, and various other reports (MOMS) for management.

Unisys Corporation, Commonwealth of Pennsylvania,
Computer Operator, Harrisburg, PA 1997 – 1999

Operated and monitored operating system 2200 mainframe systems and peripherals. Responsible for the tape library activity. Monitored and ran backups on the mainframes and open systems.

Unisys Corporation, Commonwealth of Pennsylvania,
Logistics Manager, Harrisburg, PA 1994 – 1997

Managed the warehousing, inventory, and ordering of computer parts and replacement peripheral equipment for the Unisys Customer Service Departments in Harrisburg and Pittsburgh. Prepared weekly usage and inventory reports for management.

Unisys Corporation, Commonwealth of Pennsylvania,
Financial Administration, Harrisburg, PA

Prepared weekly, monthly, quarterly, and annual financial projection plans and budgets. Prepared weekly overtime and travel expense reports for more than 90 employees for management. Prepared monthly and annual salary review reports for management. Submitted salary increases to personnel as determined by management.

Unisys Corporation, Commonwealth of Pennsylvania,
Customer Service Engineer, Harrisburg, PA 1980 – 1982

Maintained various hardware including 1,100 systems and peripherals and desktop equipment for multiple clients in the Harrisburg area. Provided reports on hardware problems, ordered replacement parts, and updated of hardware documentation.

Unisys Corporation, Commonwealth of Pennsylvania,
Lead Secretary, Harrisburg, PA 1987 – 1980

Provided administrative support to the Customer Service Branch Manager, six field service managers, and 85 customer service engineers.

UNISYS

Resource 8

Batch Administrator

Education

- Graduated Harrisburg High School 1977 – Business Curriculum
- Basic Electronics Correspondence Course, NRI
- Various CBTs on my positions at Unisys

Professional Certifications

- ITIL v3 Foundations

This page intentionally left blank.

Database Analyst

This page intentionally left blank.

Resource 9

Database Analyst

Key Skills and Knowledge

- z/operating system
- UNIX/AIX
- zLinux
- Oracle DB 9/10/11
- Oracle ASM
- Oracle Grid
- Oracle Enterprise Manager
- DB2
- IBM DB2 utilities
- BMC DB2 utilities
- IMS DB/DC
- Omegamon/IMS
- IBM IMS utilities
- BMC IMS utilities
- SQL
- Shell scripting

Professional Summary

More than 20y years of experience in information technology, specializing in the design, implementation, maintenance, and technical support of database systems. Experience includes programming, database administration and management, and systems programming.

Employment History and Related Experience

IBM, Oracle Database Administrator Harrisburg, PA 2008 – Present

Install, maintain, administer, and support Oracle databases on Linux on System Z, UNIX, and AIX.

- Upgrade and maintain databases.
- Performs logical and physical backup and recovery.
- Performs schema management and security health checking.
- Facilitates problem resolution, patch management, and technical support.
- Provides primary Oracle support for the Commonwealth of Pennsylvania, Department of Transportation.

IBM, Oracle z/Operating System Database Administrator, Harrisburg, PA 2006 – 2008

Delivered technical services, including installation, maintenance, administration, and support of Oracle and related products on the z/operating system platform.

- Upgrades and maintains servers.
- Facilitated logical and physical backup and recovery support.
- Managed database schemas.
- Performed security health checking, problem resolution, patch management, and technical support.

IBM, IMS DB/DC Systems Programmer, Harrisburg, PA 2000 – 2006

Performed systems management Integration, including installation, maintenance, and systems administration.

- Supported IMS DB/DC and related products (including IBM and BMC database tools and Omegamon/IMS).
- Provided primary IMS systems software support for the Commonwealth of Pennsylvania account.
- Supported the Department of Transportation, Department of Revenue, Department Labor and Industry, Department of Health, and the State Workers Insurance Fund.

IBM

Resource 9

Database Analyst

Education

- B.S., Computer Science, Shippensburg University
- MBA, Shippensburg University

UNISYS
IBM

R. Resource 10
IMS Systems Programmer

Key Skills and Knowledge

- IMS
- IMS related products
- z/OS
- JCL
- SMP/E
- TSO/ISPF
- Disaster Recovery
- MS Office
- SAS

Skills Summary

IMS Systems Programmer responsible for the installation and maintenance of IMS and IBM and third-party IMS related products. Have excellent communications skills and acted as the IBM Global Technology Services US IMS Team Lead.

Employment History and Related Experience

IBM, IMS Support, 2001 - 2013

Responsible for the installation and maintenance of IMS and IMS related products from IBM and third parties.

- Responsible for debugging, problem and change management, root cause analysis, and development of installation/upgrade plans.
- Acted as the IBM Global Technology Services US IMS team lead.
- Supported disaster recovery, IMS sysgens and SMP/E.
- Trained junior staff.

AstraZeneca, Technical and Operations Support, 1987 - 2001

Installed third party products, maintained IMS, performance analysis and capacity planning, chargeback accounting, and budgeting.

Computer Task Group, Entry Level Systems Support, 1984 - 1987

Maintained CICS system software, developed help desk procedures, performed COBOL programming.

Education

- Goldey Beacom College, Wilmington, DE
  BS in Business Information Systems, 1980 - 1984
- United States Navy, USS Pargo (SSN-650)
  E-6 Machinist's Mate and qualified Submariner, 1974 - 1980

This page intentionally left blank.

Resource 11

Database Analyst

Key Skills and Knowledge

- SQL Server 2008R2, 2008, 2005, and 2000/7
- Migration from SQL Server 2000 to 2005 and 2000 or 2005 to 2008 by using in-place/side-by-side upgrades
- Documented the upgrade process
- SQL Server Integration Services (SSIS) packages, analysis services (SSAS) cubes, and reporting services (SSRS) reports and models
- Designing, creating, and processing cubes using SSAS and MDX queries
- Data warehouse modeling (designing star schemas and snowflake schemas with identifying facts and dimensions)
- Detect and troubleshoot SQL Server-related CPU, memory bottlenecks, I/O, disk space, and other resource contention
- Backups and restores with SQL Server 2005 tools like SQL Server Management Studio, SQL Server Profiler, SQL Server Agent, and Database Engine Tuning Advisor
- SQL logins, roles and authentication modes as a part of security policies for various categories of users
- Rebuilding indexes with the Idera tool if fragmentation is higher than 30 percent

Professional Summary

6 years of experience in database design, development, and administration for very large and complex databases in SQL Server 2008R2, 2008, 2005, 2000, and 2007. Experience implementing Disaster Recovery and High Availability systems, Native Log shipping, Custom Log shipping, mirroring and replication (snap shot and transactional with updatable subscriptions), clustering (active/passive). Proficient in performance tuning, query optimization, Client/Server connectivity, and database consistency checks using DBCC utilities, DMVs and DMFs.

- Expertise in database administration on production servers with server configuration, performance tuning, and maintenance with outstanding troubleshooting capabilities
- Experience in analyzing the locks, dead locks, and handling the Isolation level and concurrency effects outstanding experience in SQL Enterprises Manager and SSMS – creating and scheduling jobs, alert, and operators with SQL Server Agent, backup/recovery databases
- Implemented the new SQL Server 2005 concepts like data partitioning, snap shot isolation, database snapshot, online indexing, mail setup, jobs and alerts, DTA, SQLCMD, and dedicated administration connection
- Extensively used tools like SQL Profiler, Index Tuning Wizard, and Windows Performance Monitor for tuning and monitoring SQL Server performance
- Good at SQL Server 2008 new features like Policy Based Management, Data Compression, Resource Governor, Performance Data Collector and Transparent Data Encryption (TDE)
- Good at SQL Server 2008R2 new features like Parallel Data Warehouse, Master Data Services, Data-Tier Application, Power Pivot for Excel and SharePoint, and Unicode Compression
- Migration from SQL server 2000 to 2005 and 2000/2005 to 2008 by using In-Place/side-by-side upgrades process, and documented the upgrade process
- Develop and tune SQL Server Integration Services (SSIS) packages, analysis services (SSAS) cubes and reporting services (SSRS) reports and models
- Experience in designing, creating, processing of Cubes using SSAS, and using MDX Queries
- Expert in data warehouse modeling (designing Star Schema, snowflake schemas with identifying Facts and Dimensions)
- Experienced in moving system database and configure tempdb
- Ability to detect and troubleshoot SQL Server related CPU, memory bottlenecks, I/O, disk space, and other resource contention.

Domino Technologies Inc.

Resource 11

Database Analyst

Employment History and Related Experience

Pennsylvania Department of Transportation,
SQL Server DBA, Harrisburg, PA 2012 – Present

The Pennsylvania Department of Transportation (PennDOT) oversees transportation issues in Pennsylvania. PennDOT supports more than 40,500 miles of state roads and highways, about 25,000 bridges, and new roadway construction, except for the Pennsylvania Turnpike Commission, which only follows PennDOT policies and procedures.

- Worked on issues after upgrading a server from SQL 2000, 2005, and 2008.
- Configured database mail in SQL Server 2008.
- Performed daily routine DBA tasks like handling users' permissions and space issues on Production servers and handling maintenance jobs, backups, and restores.
- Implemented SQL logins, roles, and authentication modes as a part of security policies for various categories of users.
- Worked on an active-passive cluster, moving the resources to the passive node and restarting the servers every month.
- Deployed data from the Production server to the Development, System, and Sandbox servers, depending on the SRS, by using backup and restore.
- Solved the SRS, depending on the priority; monitored Production servers.
- Restore the database from the Production server to Development, Sandbox, Test, and System servers.
- Extensively worked on implementation and release to production every month.
- Created SSIS packages for data flows from Oracle to SQL Server by using Oracle.
- Provided and used data conversion data flow tasks, deployed the packages to the server, and scheduled jobs to run.
- Detected and resolved locks and deadlocks using trace flags and native tools like Profiler and the Activity Monitor.
- Worked on 24x7 on call-support.

Buchanan Ingersoll and Rooney P.C, SQL Server DBA,
Pittsburgh, PA 2011 – 2012

Buchanan, Ingersoll & Rooney has the largest state-government lobbying practice in Pennsylvania and is one of the top 20 federal lobbying practices nationwide. The firm also has practices in labor and employment law, immigration law, bankruptcy and creditors' rights, corporate finance, energy, Marcellus shale

rights, tax law, real estate, family law, government contracts, health law, financial institutions, and intellectual property.

- Migrated databases from SQL Server 2000 to SQL Server 2008; documented the process with pre-migration and post-migration steps.
- Applied patches and service packs to update different versions of MS SQL Server in clustered and standalone environments.
- Fixed the failed principals (logins), user permissions and security in Active Directory and SQL Server.
- Scheduled regular backup jobs using the Idera Admin Tool backup tool; tracked database by receiving e-mail on Alerts.
- Extensively used the Idera Admin tool for login copies, database movers, job movers, job editors, serverc , database configuration, partition generator, linked server copy configured database mail in SQL Server 2008.
- Used Idera tools for monitoring blocking, deadlocks, long-running jobs, space issues, and Windows-level performance.
- Extensively used the Lightspeed tool for backups and restores of the database from one server to another for month-end procedures.
- Created logins and mapped users to roles by assigning permissions.
- Used the new features of SQL Server 2008 such as TCE, EKM, Merge Statement, and compressed backups.
- Worked on issues after upgrading the server from SQL 2000, 2005, and 2008 like configuring the database mail in SQL Server 2008.
- Performed daily tasks, including backups and restores, by using SQL Server 2005 tools like SQL Server Management Studio, SQL Server Profiler, SQL Server Agent, and Database Engine Tuning Advisor.
- Implemented SQL logins, roles, and authentication modes as a part of security policies for various categories of users.
- Extensively used the Idera tool for rebuilding the indexes when fragmentation was higher than 30 percent.
- Extensively worked on migrating DTS to SSIS packages.
- Performed daily routine DBA tasks like handling users' permissions and space issues on Production servers and handling maintenance as well as jobs, backups, and restores of databases.
- Extensively worked on month-end outages like shutting down the servers and applying Windows patches; worked on 24/7 on-call support.

Environment: SQL Server 2000 and 2008 with clustering, replication, T-SQL, Windows 2003 64-bit, and Diagnostic Manager.

Bank of New York Mellon, SQL DBA/Developer, PA 2010 – 2011

Established in 2007 from the merger of Mellon Financial Corporation and The Bank of New York Company, Inc., BNY Mellon is a leading asset management

and securities services company uniquely focused to help clients manage and move their financial assets and succeed in the rapidly changing global marketplace.

- Worked in SQL Server 2000 with 2TB of data and SAN infrastructure of a 60 server 2-node cluster of active/active and active/passive on Microsoft Windows Server 2003 R2 Enterprise Edition SP2 in a SAN environment.
- Migrated DTS packages from SQL Server 2000 to SSIS SQL Server 2005.
- Migrated and documented SQL Server 2000 to 2005.
- Created documentation for steps needed to be taken while upgrading SQL Server 2000 to SQL Server 2005.
- Performed BCP, extracting the zip file, and used the xp_cmdc shell for the bulk operation.
- Used Foglight for monitoring deadlocks, blockings, and Windows-level performance.
- Analyzed the consistency of database and fragmentation on the indexes.
- Worked with transactional replication to achieve load balancing.
- Used the DTS Xchange tool for migrating DTS packages to SSIS.
- Troubleshot SSIS packages that failed to execute in the scheduled jobs.
- Created ad hoc reports using SSRS in BIDS.
- Reviewed store procedures and queries; fine-tuned slow running queries.
- Implemented Maintenance Plan tasks like history cleanup and rebuilding indexes in SSIS.
- Detected and resolved locks and deadlocks using trace flags and native tools like Profiler and the Activity Monitor.
- Effectively used Send Mail Task in SSIS.
- Created logins and mapped users to roles by assigning permissions.
- Configured protection levels for the SSIS packages while moving from staging to production.
- Developed reports in SSRS using BIDS studio.
- Pumped the data into the data warehouse using the SSIS packages.
- Retrieved data from partitioning the cube from the data warehouse (OLAP) using BIDS.
- Interacted with the test team to fix the bugs.
- Involved in 24x7 production support.

Environment: TSQL, MS SQL Server 2000, 2005, SSRS, Query Analyser, Visual Studio 2005, VB.Net, C#, Winnows Server 2008, IIS, and SSAS.

Verint Systems Inc, SQL DBA, Atlanta, GA 2010 – 2010

Verint Systems Inc. is a leading provider of actionable intelligence solutions and services for enterprise and security intelligence. These solutions help

organizations make timely, effective decisions for improving enterprise performance and making the world a safer place.

- Created SSIS 2008 release 2 packages from DTS Packages 2000.
- Applied patches and service packs to update different versions of MS SQL Server in clustered and Standalone environments.
- Configured database mail, alerts, and operators in SQL Server 2008.
- Created a new instance in SQL server 2008R2.
- Deployed data from the Development server to the Main, QA, and Production servers every week.
- Implemented SQL logins, roles, and authentication modes as a part of security policies for various categories of users.
- Performed daily tasks, including backups and restores, by using SQL Server 2005 tools like SQL Server Management Studio, SQL Server Profiler, SQL Server Agent, and Database Engine Tuning Advisor.
- Created rebuild indexes; updated and scheduled statistics jobs to run every week.
- Migrated the data from the Production server to the Main, QA, and Development servers.
- Created SSIS packages for data flow from Oracle to SQL Server by using Oracle provider and data conversion data flow task; deployed the packages to server and scheduled jobs to run.
- Performed daily routine DBA tasks like handling users' permissions and space issues on Production servers and handling maintenance jobs, backups, and restores the databases.
- Worked on an active-passive cluster, moving the resources to the passive node and restarting the servers every month.
- Worked on transaction replication, in which data was replicated from the Production to the Main server and the Main server to the QA and Development servers; dropped and recreated the replication during deployment.
- Monitored SQL Server performance using Profiler to measure performance and find deadlocks.
- Solved tickets, depending on the priority.
- Worked on 24/7 on-call support.

Environments: SQL Server 2008 and 2005, T-SQL, Excel, Advanced Windows 2000 Server, Visual Source Safe 6.0 (Version Control Management), and TFS (Team Foundation Server).

Domino Technologies Inc.

Resource 11

Database Analyst

Trustco Bank, SQL Server DBA, New York, NY 2008 – 2010

Trustco Bank is the low-cost provider of high-quality services to customers in the communities it serves and returns to its owners an above-average return on their investment. Through changing times, Trustee's commitment to careful financial management, and high-quality lending standards, and following prudent investment practices has never wavered. The bank's focus has always been to provide its customers with community banking solutions that offer superior convenience, value, and security.

- Worked on client/server tools like SQL Server Management Studio (2005), SQL Server Enterprise Manager (2000), and Query Analyze.
- Migrated SQL Server 2000 databases to SQL Server 2005 databases with an in-place upgrade process; used the Upgrade Advisor tool for upgrades.
- Migrated DTS packages to SSIS packages.
- Handled up to 2TB databases in Clustered and Standalone environments.
- Configured transactional replication on migrated servers.
- Created stored procedures, triggers, views, and functions for the application.
- Extensively worked on Dynamic Management Views (DMVs) and Dynamic Management Functions (DMFs).
- Effectively used the Query Analyzer for Interacting with the databases.
- Developed, deployed, and monitored SSIS packages including upgrading DTS to SSIS.
- Implemented SQL principle, securable, permission, roles, and authentication modes as a part of security policies for various categories of users.
- Maintained a SQL script for creation of database objects in VSS (Visual Source Safe).
- Created a database maintenance planner for the performance of SQL Server that covers database integrity checks.
- Implemented conditional split and merge tasks for data transformation in SSIS.
- Used Configuration files for dynamic connection of SSIS packages.
- Extensively used the Execute utility package to execute packages.
- Used DTS packages to move logins and jobs from one server to another server.
- Acquired good experience in data modeling and metadata services.
- Monitored SQL Server performance using Profiler to measure performance and find deadlocks.
- Worked on a DB2 and Oracle team for handling a linked server.

Environment: TSQL, MS SQL Server 2000 and 2005, SSRS, Query Analyser, and Visual Studio. 2005, VB.NET, C#, Windows Server 2008, IIS, SSAS, DB2, and Oracle 9i.

Domino Technologies Inc.

Resource 11

Database Analyst

SQL DBA/Developer, LIC Insurance, India Insurance Management System 2006 – 2008

LIC Insurance Company provides a wide range of insurance policies such as life insurance, health insurance, overseas travel insurance, student health insurance, fire insurance, motor vehicle insurance, aviation insurance, general insurance, marine insurance, shopkeeper policies, transportation policies, and accident insurance. This project was developed as a process for automation for insurance policy management, which includes policy proposals, claims, accounts, and reports.

- Implemented SQL logins, roles, and authentication modes as a part of security policies for various categories of users.
- Acquired a sound knowledge of stored procedures, indexed views, user-defined functions (UDL), triggers, distributed queries, and common table expressions.
- Wrote stored user-defined data types, procedures, triggers, and functions to rebuild the indexes at regular intervals for better performance.
- Designed and implemented a comprehensive backup plan and disaster recovery strategies.
- Implemented and scheduled replication process for updating our parallel servers.
- Monitored and troubleshot existing DTS packages.
- Troubleshot and fine-tuned databases for performance and concurrency.

Environment: TSQL, MS SQL Server 2000, Enterprise Manager, VB.NET, Windows Server 2003, and IIS.

Education

- Bachelor's degree in Computer Science, JNTU, India

Professional Certifications

- MCTS – SQL Server 2005

This page intentionally left blank.

UNISYS

Resource 12

Database Analyst

Key Skills and Knowledge

Databases

- Microsoft SQL Server 7.0, 2000, 2005, 2008, 2008 R2
- Oracle 10g
- FoxPro, dBaseIII+
- Microsoft Access

Operating Systems

- Windows XP
- Windows Vista
- Windows 2000, 2003, & 2008
- UNIX

Programming Languages & Tools

- Visual Studio .NET
- Visual Basic 6
- FoxPro
- dBaseIII
- Microsoft Access
- Crystal Reports

Office Productivity Tools

- Microsoft Office

Technical Documentation

- Microsoft Office

Professional Summary

Experienced in Information Technology (IT) using MS SQL Server 7.0, 2000, 2005 2008, 2008 R2, dBaseIII+, FoxPro, Microsoft Access, Visual Basic 6.0, Visual Basic .NET, Crystal Reports, Recital, Microsoft Windows, and UNIX. Experienced in Installation and Configuration of MS SQL 2000, SQL 2005, SQL 2008, and SQL 2008 R2.

- Experienced in MS SQL Server High Availability using SQL Server instance clustering, database mirroring, and database replication
- Backup and restore databases using MS SQL Server, SQL Quest LiteSpeed, and Networker
- Experienced in SQL Server Reporting Services, MS SQL Server Integration Services, and Data Transformation Services
- Maintain and support MS SQL Server
- Develop and maintain applications in MS SQL Server, Visual Basic 6.0, Visual Basic .NET, FoxPro, dBaseIII+, and Crystal Reports
- Work in groups and independently with minimal supervision.

Employment History and Related Experience

Unisys Corporation, Database Administrator, 2009 – Present

- Install and configure MS SQL Server.
- Backup and recovery MS SQL Server.
- Maintain and administer MS SQL Server.
- Assist end users with MS SQL Server.
- Participate in reviewing database policies and procedures provide input as requested.
- Monitor the availability of MS SQL Server and Oracle database servers.

Diverse Technologies Corporation, Database Administrator, 2008 – 2009

- Backed up and recovered SQL Server.
- Maintained and administered SQL Server.
- Supported SQL Server database clients.
- Helped develop SQL Integration Services.

Systems and Services Technologies, SQL Server Developer/DBA, 2007 – 2008

- Wrote MS SQL queries and Data Transformation Services using MS SQL Server.
- Worked on a data warehouse using MS SQL Server.
- Tuned and optimized MS SQL queries.

UNISYS

Resource 12

Database Analyst

- Administered and configured development MS SQL Server.
- Monitored MS SQL Server performance.

AMA Computer University, Information Technology Director, 1999 – 2007

- Managed the overall operation of Information Technology–Campus Information.
- Administered MS SQL 2000 and 7.0 databases.
- Installed and configured MS SQL 2000 and 7.0.
- Created database replication using snapshot and transaction replication.
- Installed and configured Windows 2000 and 2003.
- Created databases, indexes, stored procedures, views, and triggers using MS SQL Server 2000.
- Created DTS package in MS SQL Server 2000.
- Designed systems based on user requirements and specifications in Visual Basic and MS SQL Server 2000 and 7.0.
- Performed programming, unit, and module testing.
- Tested, debugged, installed, and maintained programs.
- Outlined requirement specifications, system design specifications, and implementation specification.
- Conducted user and technical training and user acceptance testing.
- Assisted in system documentation.
- Assisted in implementing the system.

Republic Asahi Glass Corporation, Systems Analyst/Programmer, 1997 – 1999

- Designed and developed applications in Recital Database under UNIX, MS SQL, and Crystal Reports.
- Developed and implemented database designs in Recital Database and MS SQL.
- Participated in analysis, design, development, implementation, testing, documentation, and maintenance of client/server applications.
- Supervised database backup and recovery.
- Participated in unit testing of the application.
- Outlined requirement specifications and technical training.
- Performed user acceptance testing.
- Created system documentation.

Country Export Philippines, Incorporated, Network Administrator, 1994 – 1997

- Developed applications in Visual Basic, FoxPro, MS Access, and Crystal Reports.

UNISYS

Resource 12

Database Analyst

- Maintained a local area network.

ExL Worldwide Express, Assistant Systems Analyst, 1993 – 1994

- Assisted in developing applications in FoxPro.

Additional Employment History

Unisys Corporation.....2009 – Present
Diverse Technologies Corporation.....2008 – 2009
Systems and Services Technologies.....2007 – 2008
AMA Computer University.....1999 – 2007
Republic Asahi Glass Corporation.....1997 – 1999
Country Export Philippines, Inc.....1994 – 1997
ExL Worldwide Express.....1993 – 1994

Education

- B.S., Computer Engineering, Central Colleges of the Philippines, 1991

Professional Certification

- Microsoft Certified IT Professional: Database Administrator 2008, Jul 2012
- Microsoft Certified IT Professional: Database Administrator on SQL Server 2005, Dec 2006
- Microsoft Certified Solution Developer for Microsoft .NET, Feb 2006
- Microsoft Certified Database Administrator on Microsoft SQL Server 2000, Jan 2006

This page intentionally left blank.

Database Architect

This page intentionally left blank.

UNISYS

INFO-MATRIX CORPORATION

Resource 13

Database Architect

Key Skills and Knowledge

- More than 10 years of database architect experience
- Mainframe development
- Systems programming
- Capacity planning
- Database design
- System architect administration and BI architect positions.
- BI access to unstructured data with DW access into ESB/SOA and MDM systems
- Design using ERD BPM and BMM models for policy feedback
- Conduct architecture research
- Publish white papers
- Create standards for SSD HDD and distributed OORDBMS key integration

Professional Summary

Principal architect skilled in development efforts that standardize workflows, data warehouse federation, and virtualization.

- Developed department and group dictionaries needed for SOA; generated data scorecards
- Developed data models with enterprise-level conformed dimensions as well as taxonomy and grain specifications
- Formed data management strategy for mixing unstructured data with semi and fully structured data
- Supported the generation of specifications for near-real time ODS, departmental governance, and business rules needed for an ESB
- Published author of a teaser article in *Information Management* magazine on how to devise a data strategy
- Skillful with engineering and design best practices, industry research, and project management
- Experience with database management systems includes Oracle, DB2/UDB, SAS and SQL Server, DDL, and DML
- Data modeling support includes Star for OLAP and ERD tools along with OLTP for dimensional modeling and data mart design with ETL support, All Fusion (7 years), Rational System Architect, Microsoft Visio, and Bachman ERD design tools
- Developed data modeling and standards for enterprise-level ESB/SOA structures
- Established and operated a R&D lab to facilitate on-site benchmarking of various configurations. This included Windows and Sun operating systems with Oracle and DB2 database management systems
- Installed and administered new software and tested the interfaces to the existing system, including firewalls and SAN network storage; integrate COTS packages; and facilitate JAD sessions for gathering business requirements
- Designed data flows, service level agreements, capacity reporting requirements, dashboards, and operational monitoring reports.

Employment History and Related Experience

Major Telecommunications Company, Principal Architect,
New York, NY 2011 – Present

Conduct architecture research, publish white papers, generate standards for SSD HDD, and integrated distributed OORDBMS key

- Produced Data Warehouse (DW) designs, reviews, and roadmaps of harmonization, and virtualization efforts.

- Generated workflows and a Netezza conversion analysis enterprise domain; reviewed data quality.
- Resolved data grain and lexicon issues, conflicting optimization goals, MDM & ESB/SOA configurations, data-driven dimensions, data and architecture measures, and cloud deployment and use.
- Composed industry-standard data models with departmental data stores.
- Install, analyze, test, and test virtual data warehouses.
- Wrote a white paper on integrating hub-and-spoke architecture with point-to-point architecture.
- Evaluate vendor software; review project architecture.
- Created architecture and information roadmap and data ownership plans.
- Planned, supported, and tuned capacity.
- Installed IBM Rational System Architect.

CA, Enterprise Architect DBA, New York, NY 2009 – 2011

For the enterprise architecture group, designed data warehouses, created MDM roadmaps and integrated projects from a data standpoint.

- Consolidated two data warehousing teams into one model change control and data dictionary reporting method.
- Merged models and resolved conflicts across two teams of consultants to produce a single unified model.
- Conformed the data models to the in-scope attribute lists.
- Verified data dictionary entries and other standards were followed.
- Established change control procedures and reports.
- Produced an OLTP and an OLAP star data warehouse design.
- Reverse engineered existing systems for generation of an as-is distributed enterprise ESB/SOA data model.
- Monitored and shaped project development meetings to better integrate data designs across projects.
- Reviewed and analyzed a project portfolio for strategic interfaces to master data management, developed a roadmap for its implementation.
- Mined metadata to uncover de facto standards and tuning objectives.

Environment: Microsoft and Sun servers running Oracle, SAP, SFDC, and Microsoft software.

1-800flowers.com, Architect Modeler, New York, NY 2007 – 2009

For the Business Intelligence group, designed a data warehouse, created a SAS data mart, and worked on bridge migration projects.

- Benchmarked and sized hardware for managing software licenses.
- Created management reports in Microsoft Project, Visio, and PowerPoint.
- Documented a SAS client installation procedure in BPMN.
- Evaluated and assessed the existing ETL and ODS design.

- Designed a logical, fully normalized ODS and mapped to the existing physical system.
- Designed a snowflake dimensional data warehouse for MDM and SOA.
- Interviewed experts in data harmonization and data design generation.
- Created a DFD, BMM, ERD, and business process model of a VB, Access, and Crystal Reports system.
- Migrated that system's business logic to Oracle 10 SQL and data structures.
- Migrated that system's reporting and wrapper functions to SAS on a WAS.

Environment: Microsoft and Sun servers running Oracle, ERwin, SAS, and Microsoft software.

Metropolitan Washington Airports Authority, System Architect, Washington, DC 2006 – 2007

Supported an ERP BPR project as a subcontractor for Booz Allen Hamilton at Washington Ronald [redacted] National Airport.

- Evaluated Rational System Architect software; performed gap analysis.
- Upgraded, customized, and configured the Rational System Architect product.
- Developed BPMN modeling procedures and tutorials for business analysts.
- Generated of process modeling standards and change control conventions.
- Converted diagrams from Visio to SA BPMN for as-is a process model.
- Analyzed installed hardware and software systems.
- Assessed the governance of project scope, generated progress measures.
- Trained process modelers in the use of SA and generation of management reports.

Environment: Microsoft SQL Server, Telelogic System Architect and Doors, and Microsoft Office.

U.S. Department of Health and Human Services – Lockheed Martin Family Parent Locator Service Contract, System Architect, Baltimore, MD 2005 – 2006

Supported Family Parent Locator Service, which runs in the Social Security Administration National Computer Center.

- Authored a GAO capacity report that evaluated system costs.
- Modeled and reported on the administration of the System Architect Zachman framework.
- Discovered requirements and analyzed existing gaps and concerns.
- Reviewed COTS software for non-mission critical tasks.

- Reviewed and enhanced the CMM system.
- Designed and specified ETL PSQL procedures to support changes in the database design; organized and facilitated JAD sessions for data homogenization mappings.
- Assessed and mapped systems using DFD, DD, and ERD in SA.

Environment: DB2 and VSAM on z/operating system; Oracle 9; MS SQL Server; and MySQL on XP, 2000, and Sun platforms with Microsoft Office and Telelogic System Architect.

Social Security Administration – Lockheed Martin,
DB2 Capacity Planner, Baltimore, MD 2004 – 2005

Support for systems that run in the National Computer Center in Baltimore.

- Created hardware maps for the rollout of a ESCON/FICON channel.
- Set and scheduled the implementation of DB2 RLF operational.
- Tuned DB2 buffer pools; planned application locking.
- Mined and warehoused MICS data using customized SAS code.
- Designed a capacity planning performance database based on SMF/RMF.
- Recommended data designs for enhancing system performance.
- Mapped business KVI drivers to a BMM for measurement, forecasting.

Environment: Z99 mainframe, DB2 7 and 8, SQL, SAS, MXG, and MICS Visualizer.

TEK Systems, ICARZ, Systems and Data Architect &
Consultant, Newton, NJ 2003 – 2004

- Performed iterative prototyping for a business process redesign.
- Created ERwin ERD, DD, and Process Modeler DFDs.
- Implemented referential integrity without forcing program changes.
- Mapped all Fusion insert update and delete processes for OLTP security.
- Planned the conversion for 2-tier to 3-tier client server implementation.
- Integrated application with DDL conversion scripts and triggers.
- Tuned DB2 and UDB instances and configurations for locking, paging, and CPU.

Health Management Systems, Senior Database
Administrator & Data Modeler, New York, NY 1998 – 2003

Supported DB2and UDB for Chicago subsidiary H.S.A. In resource management, provides project manager-level support and modeled data.

- Reported on capacity planning using SFM/RMF data and SAS on a Merril system.
- Converted PeopleSoft application systems from mainframe to UDB on NT.

- Created the physical design and implemented applications on DB2 and UDB.
- Produced ERwin logical and physical models for OLTP and OLAP data designs.
- Supported data warehousing tuning as well as tuning and optimization of data mining queries for all application areas and departments.
- Implemented distributed cross platform designs; supported prototype debugging.

Various Companies, Part -Time Positions, New York, NY 1989 – 2003

- Adjunct Instructor for the Pace University Information Systems Department.
- Delivered instruction in systems analysis design, operating systems, and DBMS.

Dean Witter, Database Administration Group,
New York, NY 1997 – 1998

Maintained and updated the Bachman model, Migrated DB2/RACF security and indexes, stored procedures, and column constraints. System managed referential integrity with data mart creation and synchronization.

Federal Reserve Bank of New York, Database
Administration Group, New York, NY 1996 – 1997

Migrated systems from the New York district to the New Jersey national system, Created and standardized utility jobs and new naming conventions. Supported disaster recovery and contingency testing.

Automatic Data Processing, Brokerage Services Division,
Database Administration Group, Jersey City, NJ 1995 – 1996

Applied the full project life cycle (SDLC) to database support requests. Supported the following applications: Proxy Edge Voting, Name and Address, System Service Request, Proxy Investor Track System, and a Brokerage Client Processing Option System. Warehoused data and designed OLTP using the Bachman modeling tool and XDB.

Home Insurance Company, Technical Services,
New York, NY 1989 – 1995

Installed systems and administered various vendor software packages, capacity planning using SAS and MICS, system accounting, and chargeback data warehousing.

INFO-MATRIX CORPORATION

Resource 13

Database Architect

Education

- BBA in Management Information Systems plus graduate credits, Pace University, New York, NY-
- Brokerage Operations and Margin I, NYIF, New York, NY

Professional Certifications

- Certificate in Applications Programming, Pace University, New York, NY
- Various software vendor classes and conferences

UNISYS

INFO-MATRIX CORPORATION

Resource 14, PMP

Database Architect

Key Skills and Knowledge

- PMP (Project Management Professional) – PMI
- Teradata Certified Professional
- Oracle Certified DBA (OCP)
- Certified Data Warehouse Architect – Wipro, India

Technologies

- Teradata, SQL, Dataflux, ERwin, Oracle 10g DB, Informatica, PL/SQL
- Oracle Warehouse Builder (OWB) Discoverer, Designer, Developer, Workflow, Application Serve, Application Foundation, and Toad
- Business Objects, Java, Shell script, HTML, XML, PC SAS, and CA Harvest
- UNIX, ClearQuest
- EDI X12 transactions, HL7, OpenSource DI Talend
- Rational Unified Process (RUP)

Methodologies

- Roadmaps and strategies for Building and Adopting Enterprise Data Warehouse, data modeling, and Architecture
- Data warehousing – Kimball, Inmon methodologies, Data Quality, MDM, and SOA
- Project Management & SDLC

Professional Summary

- Expertise in architecture, design, and implementation of data warehouse and data marts, data quality, and MDM solutions
- Providing technical leadership, architectural direction, and roadmaps for data warehouse initiatives for data modeling, data integration, data access and security, technology acquisition, and application performance
- Data governance – documenting standards and operating procedures; suggesting best practices for confirming data integrity, satisfying regulatory and audit requirements
- Project management, SDLC, and mentoring.

Supported the following data warehouse projects:

- Enterprise Data Warehouse (EDW), healthcare company – Business Intelligence Architect
- Enterprise Data Warehouse (EDW), Highmark Insurance – Data Architect
- Global Hygiene and Match, Dun & Bradstreet – data analysis; design and implementation of customer data integration (CDI) solution
- Metadata Framework (MDF) and Cisco Data Library, Cisco Systems – data architect for Enterprise vocabulary integration and Operational Data Store
- Global Contact Database, Oracle – designed and implemented a customer data integration solution

Employment History and Related Experience

Enterprise Data Warehouse – Healthcare Client, BI Architect — 2010 – Present

The BI Solutions group hosts Enterprise Data Warehouse (EDW) and legacy reporting systems, housing corporate health insurance data that supports analytic reporting, clinical programs, master data, departmental data marts, and third party data feeds.

- Designed systems for EDW foundation to process Medical/Rx/Dental/Vision claims data including provider, product, member, group customer, and care management.
- Developed databases for member data marts, actuarial, individual business, and provider incentives, etc., are built on top of EDW foundation.
- Roadmap and migration strategies from Legacy Systems to EDW.
- Reference architecture, future state definition, architecture governance and quality review.
- Data analysis to identify data anomalies and propose data quality solution.
- Data validation for fitment of use.

- Data governance support.

- Data architecture support for managing Metadata/Master Data/Reference Data.
- Solution architecture/EDW SME support for DW projects.
- Process improvements to enhance data quality, performance, and data access.
- Audit/Balance strategies/Design for EDW with operational systems and data marts.
- ETL process / Mappings design, Implement Change Data Capture (CDC).
- Requirement analysis and Data modeling for EDW and related Data marts using 3NF and Dimensional models.
- Database planning (Oracle), performance tuning, volumetric estimates, environment planning and setup, DB load job setup.

Toolset: Oracle 10g, ERwin, Informatica, Pl/SQL, XML, SAS, Sql*Server, UNIX, EDI X12, Healthcare Solutions: ICD-10; HIPAA 5010; Benchmarks – BHI, Milliman; Ingenix – Health Record, Chronic conditions; Medicare Advantage; Nasco Claims processing; HL7 Lab data.

Enterprise Data Warehouse – Highmark Insurance,
Data Architect/Lead, 2006 – 2010

The Enterprise Data Warehouse (EDW) hosts corporate health insurance data that supports Highmark's operational reporting and analytical needs. It includes data for major medical and dental claims, subject including provider, product, member, client, and enrollment subject areas.

- Requirement analysis and data modeling for main / supporting subject areas for EDW and related data marts using 3NF and dimensional models, data analysis and data profiling.
- Data governance – Plan, Standardize, metadata discovery and publish, data retention policies, Software Operating Process (SOP) setup.
- Roadmap and migration strategies from Legacy Systems to EDW.
- ETL process / Mappings design, implement Change Data Capture (CDC.)
- Security layer design and data access setup.
- Complex SQL/SAS reporting from EDW including EDI X12 reporting.
- Database planning (Teradata and Oracle), performance tuning, volumetric estimates, environment planning and setup, DB load job setup.
- Analysis / design of integrating MDM (Initiate) solution with EDW.
- Project Management activities and technical mentoring.
- Point of contact on Open Source data integration and data quality technologies (Talend).

Toolset: Teradata (BTEQ, TPT (Parallel Transporter), MLOAD, OLELoad, Fast Export), ERwin , Informatica, Oracle 10g, Pl/SQL, XML, SAS , CA

Harvest, Rational RUP, UNIX, EDI X12, Healthcare Solution: HIPAA 5010, and DxcG Risk categories.

Wipro Technologies, Technical Lead 2003 – 2006

Global Hygiene and Match (GHM) – a Dun & Bradstreet project. Customer data integration system channels manage and track customer data from various disparate applications, identify data quality issues, and provide enhanced data. From the cleansed data, GHM generates customer match identifiers based on specific match rules. Data quality and matching modules are exposed as a Web Service to consuming applications.

- Data analysis and profiling; designed and implemented data quality and match rules as a Web Service.
- Dataflux administration.
- Project management.
- Extraction, transformation, and formatting of data; data modeling; database design, and performance tuning.

Toolset: SAS Dataflux, ERwin, Informatica, Oracle 10g, Java, SOA, and WSDL.

GMAC, Discounting and Validation Engine (DAVE),

Data Modeler 2003-2003

DAVE is a credit contract origination and acquisition project for automotive financing, including reengineering of the existing contract acquisitions application to a dynamic configuration engine. The New Acquisition configuration includes processing of e-Contracts originating from the RouteOne® industry-standard application and processing of across-the-counter contracts in a new Discounting Automation Mechanism application.

- Data analysis, design capture, and reengineering.
- Data modeling and database design.

Toolset: ERwin, Oracle Designer, PL/SQL, Oracle 8i DB, Enterprise Manager (OEM), and Toad.

Cisco, Enterprise Architecture Group, Data Architect

Metadata Reporting 2003-2003

MDF End 2 End (E2E) a Reporting is reporting repository (data warehouse) for Metadata Framework (MDF). It is an operational data store (ODS) with consolidation of data from MDF and various content management systems. Data integrated together in the de-normalized ODS structures is further used by downstream reporting applications like Clickstream.

- Requirement analysis, data modeling, and design.
- Designed and developed Extract Transfer Load (ETL) procedures.
- Project management.
- Database administration.
- Performance tuning, design capture, database design, and database audits.
- Evaluated and recommended new database features.

Toolset: Oracle Designer, Pl/Sql, Oracle 8i DB, Enterprise Manager (OEM), and Toad.

Wipro DWH practice, Center of Excellence (CoE) activities

- Proof-of-concept for product features and technologies.
- Approached notes and best practices.
- Data model templates – STAR (automotive retail) and regulatory compliance.
- Created training content on the new feature of Oracle data warehouse and data modeling.
- Mentored staff on data warehouse concepts, data modeling, data warehouse, and business intelligence technologies.

Oracle Corporation, Technical Lead, India 2002 – 2003

Maintained data content for the Global Contact Database (GCD), a data warehouse comprising details on customers and their activity. It was the infrastructure for enterprise marketing applications, helping marketing, and sales to understand customer needs and identify opportunities.

- Data analysis, Data profiling, and Data modeling.
- Implement data quality and match rules.
- Designed and developed Extract Transfer Load (ETL).
- Administered Discoverer; developed business intelligence reports.

Toolset: PL/SQL, Oracle 9i DB, Oracle Warehouse Builder, Discoverer, and Enterprise Manager (OEM).

Knowledge Repository, Technical Lead

The Knowledge Repository is a data-driven application developed with to provide up-to-date information on user support issues affecting e-Marketing application users. It is based on a content management model that goes through various life cycles in document management.

- Designed dashboard reports for e-Marketing applications.
- Administered the database.
- Provided e-Marketing application users with support and guidance.

Toolset: PL/SQL, HTML, Oracle 9i DB, Oracle 9iAS, Oracle Ultra Search, and

Microsoft Project.

Oracle Corporation, Technical Lead - Electronic Services Group, India 1998 – 2002

- Provided technical leadership, especially for resolving complex issues.
- Coordinated on critical issues with the development team.
- Contributed to Oracle knowledgebase by documenting and reporting technical issues.
- Developed tools for enhancing the support process.
- Established and maintained operating policies.
- Sett the support process and SLA guidelines.
- Created analyst utilization plans, allocated work, and maintained adherence to processes.

Toolset: Oracle Designer, Oracle Database, Oracle Developer, and Oracle Application Server (Oracle 9iAS).

Education

Bachelor of Engineering

Professional Certifications

- PMP (Project Management Professional) – PMI
- Teradata Certified Professional
- Oracle Certified DBA (OCP)
- Certified Data Warehouse Architect – Wipro, India
- Professional, Academy for Healthcare Management (PAHM)
- Certified Software Consultant – Wipro ,India
- Certified in Software Process Management – C-DAC, India

This page intentionally left blank.

UNISYS e&e IT Consulting Services, Inc.

Resource 15

Database Architect

Key Skills and Knowledge

- MCITP, MCSE, MCP
- PA Commonwealth experience
- SSIS, SSRS, Access, Oracle

Skills Summary

- Databases - MS SQL 6.0 - 2012, MS Analysis Services, SQL Server Reporting Services, SQL Server Integration Services, Oracle 7.x, 8i,9i,10g, 11, MS Access
- Networking – Windows Active Directory Services, TCP-IP, Intranet/Internet, .NET
- Operating Systems – Windows XP, Windows 2003/2008 Server, Windows 2000 Server/Advanced Server/Datacenter, Windows NT, UNIX, and AIX, Virtual PC, virtual Server, Hyper-V
- Languages – VB 6/VB.NET, ASP/ASP.NET , Java Script, Access VBA 2, 95, 97,2000, MS SQL stored procedures, HTML, VB Script, MS Excel VBA, T-SQL,PL/SQL,XML, CodeSmith – code generator
- Project management – Director of MIS, Project Leader, Data Architect, and Client Server Architect.
- OLAP Technologies – Proclarity (Knowsys), Wired for OLAP, OLAP@Work, MS Analysis Services, MS EXCEL Pivot tables.
- Misc. OOP, Web Services, XML, .Net, N-Tier Client-Server, ER-Win, PVCS, Visual Source Safe, S-Designer, ODBC, SQL*NET, CGI-programming, MS Transaction Server, COM/DCOM, ActiveX, Client Access (AS/400), FX-Cop, Continuous build environment – Cruise Control, Code Smith Code Generation.

Employment History and Related Experience

Unisys – PA State Police (Part time) 6/2012 –Present

Lead Sr. DBA

- Manage numerous MS SQL Server database servers from MS SQL 2000 to MS SQL 2008, including clusters, virtual servers, and dedicated hardware. Tasks include troubleshooting deadlocks, performance tuning T-SQL, indexes, databases, SAN network, managing production systems and lower environments, creating and maintaining DTS and SSIS packages, SSRS reports, database design, application design reviews, code walkthroughs, data archiving, disaster recovery and any database related tasks that may present. Databases managed are in the 2 to 10 terabyte range. Designed and implemented automated sliding window / archiving for large tables (over 3 TB).
- Technical Skills utilized: MS SQL Server 2000 – 2008, MS SQL Server Integration Services, MS SQL Server Reporting Services, MS SQL Server Analysis Services, Windows Clustering, log shipping, SAN, C#.net, Vb.net, ERWin, Windows Server 2003, Windows Performance Monitor, SQL Profiler.

PA Department of Labor and Industry UCMS project. 7/2011 –11/30/2012

Sr. Architect

Support for a large Oracle database environment, including data modeling, performance tuning, technical and business process analysis. Directly support data related activities for the development team including SQL tuning, writing PL/SQL procedures, and model changes. Create and/or review data hot fixes. Provide general overall Oracle expert support, specializing in ETL and development efforts. Monitor database and application performance with in-depth analysis across all tiers of the application. The UCMS application is a $130 million joint project with IBM to rewrite and expand Pennsylvania's Unemployment Compensation System to allow employers to file online, claimants to file claims and inquiry status of account, reports to be generated, as well as personal and public information to be displayed. UCMS utilizes an Oracle database while WebSphere Application Server and WebSphere Process server utilize java code written by over 130 developers. UCMS currently contains over 3.6 million lines of code, operating on 399 severs across five environments, databases in the terabytes and thousands of tables.

- Technical Skills utilized: Oracle, PL/SQL, Clustering, SAN, Websphere, IBM SOA, Java, Crystal Reports, performance tuning, SQL & PL/SQL, ERWin, Rational Clear Quest, Ration ClearQuest, Requisite Pro, Data Stage Rational Architect.

EZData2Go.com - Harrisburg, PA (Part time) 2/2010 – 6/2012

Sr. DBA, Data Modeler, ETL developer.

- Performs all MS SQL Server related activities. Activities include analyzing public domain data sources and loading into MS SQL Server and supporting production. Data models produced in Visio and MS SQL Server tools with extensive use of extended properties. ETL developed in a combination of T-SQL, SQL, and Integration services packages with numerous parts written in .net custom scripts within SQL Server Integration Service to load 100,000+ shape files into to SQL Server tables including geometry and geography data types. Develop and support MS SQL Server Analysis Services cubes. Fully loaded all 2010 US Census Summary Files 1 & 2 data including TIGER/LF shape files for 2010 and 2011 into SQL Server 2008 database representing well over 1 TB of data, nearing 2 TB with applied indexes. Heavy indexes and data file management including both data files and data file groups used to manage databases. Writing and tuning of T-SQL stored procedure, triggers, and user defined functions. Created and maintained 100's of databases in excess of 30 TB.

  Created SSRS reports for both end users and support staff, reports on data modeling rules adherence, table statics beyond the SQL Server values supplied. Managed Windows servers, Windows clusters, SAN, MS Virtual Server Hyper-V, and numerous database and development VMs. Experience in Dell servers, RAID cards, SAN, high performance solid state drive arrays.

- Technical Skills utilized: MS SQL Server 2005, 2008, 2012 including Relational engine, Reporting Service and Integration Services. MS Visio, MS Office, Visual

Studio, VB.net, ASP.net, MS Windows Server, Hyper-V Virtual Machine Server, Windows Clustering, SAN, and Power Shell.

Maximus; Harrisburg, PA 5/2006 – 6/2011

Sr. MS SQL Server DBA – Oversight / IV&V
PA Department of Labor and Industry UCMS / CWDS projects.

- Performed Independent Verification & Validation (IV&V) function of all data related activities for 2 large projects at the PA Dept. of Labor and Industry. Conducts assessments of all deliverables on behalf of the Commonwealth; reporting to senior management including CIO, Steering Committees, and Project management staff. Evaluates project activities to Statements of Work, Proposals, industry best practices, and Commonwealth standards. Provides weekly project status reports, monthly in depth assessment reports documenting findings and recommendations.
- Technical Skills utilized: MS SQL Server 2005, Reporting Services 2005, SQL Server Integration Services, Crystal Reports, performance tuning, T-SQL, ADO.NET, ERWin, VS 2005, Visual Source Safe, Rational Clear Quest, Ration ClearQuest, RequisitPro. Oracle RDMS, and Data Stage.

e.magination; Baltimore, MD 4/2005 – 5/2006
DBA – Developer
Anne E. Casey Foundation

- Performed all DBA and developer activities for small IT department supporting a large non-profit foundation. Created and supported numerous reports, web applications, windows services, and Active Directory integration with most of the applications.
- Technical Skills utilized: MS SQL Server 2005, MS SQL Analysis Services (cubes), Reporting Services 2005, SQL Server log shipping, Windows clusters, Crystal Reports, Share Point Portal Services, SQL Lite Speed, performance tuning, T-SQL, ADO.NET, Visio, VS 2005, Visual Source Safe, Active Directory API, LDAP.

National Drug Intelligence Center – RAID

- Performed all DBA and database developer activities for custom developed data intensive client-server application for a government law enforcement agency. Personally created over 1,000 stored procedures totaling more than 250,000 lines of T-SQL code, 100's of triggers, advanced self configuring indexing. Note: This project failed 2 times previously and was blamed on poor database performance. This project is considered a tremendous success and is now in use all over the world by various law enforcement agencies in numerous languages.
- Technical Skills utilized: MS SQL Server, Reporting Services, Crystal Reports, general admin, performance tuning, T-SQL, ADO.NET, Visio, VS 2003, Visual Source Safe, Cruise Control, Nant, CodeSmith – code generation.
- Conducted internal training for developers on MS SQL Server 2005 new features and best practices.

Technical Sales support

- Provided technical support during sales activities for database related solutions. As a Microsoft Gold Partner specializing in MS SQL Server solutions, met with many organizations to perform assessments of current operations and future business plans to identify technology road maps Designed and implemented many technology proof-of-concepts, including documenting technical proposals, findings and recommendations.

Independent Database Reviews

Developed consulting specialty at e.magination targeting independent review of competitors database models and codebase. Reviews ranged from simple data model reviews to database operations and procedure reviews or assistance in targeted performance tunings.

PA Turnpike Commission 11/2004 – 4/2005
DBA Developer / Web Developer

Electronic Bidding System

- Performed all DBA and Database developer activities for medium sized public web site. General duties include database administration, data modeling (logical and physical), stored procedure / user defined function creation, performance tuning, mentoring developers on SQL Server best practices with ADO.NET, VB.NET, ASP.NET.
- Technical Skills Utilized: MS SQL Server, Disaster recovery, general admin, performance tuning, T-SQL, DTS, ADO.NET, VB.NET, ASP.NET, Visio, VS 2003, Visual Source Safe, CodeSmith – code generation.

Keane, Inc. August 2003 – November 2004
Sr. Consultant - Database Developer / Web Developer

Tyco Electronics – Field Engineer Automation

- Consulted with existing development team on data model changes, and adaptation of best practices with regards to Oracle 9i.
- Technical Skills Utilized: Oracle 9i, PL/SQL, ADO.NET, VB.NET, ASP.NET, Visio 2000

Tyco Electronics – EHS – Environmental Health and Safety application

- As lead developer implemented changes to data sources from a proprietary application to the Tyco Electronics Data Warehouse. Changes made to asp pages, stored procedures, data model and VB 6 COM classes.
- Technical Skills Utilized: MS Windows 2000 Server, VB 6.0, ASP, Visio 2000, Oracle 9i, PL/SQL, Visual Source Safe

Tyco Electronics – Power Channel System

- Lead analyst for large international, multi-currency, multi-language E-commerce web application. Communicated with users around the world developing requirements for enhancements, creating modification specifications then implementing those

changes. System was truly an enterprise solution incorporating no less than 6 databases, numerous feeds in and out and thousands of users worldwide. Emphasis on performance tuning multiple SQL Server databases used for reporting and OLTP.

- Technical Skills Utilized: MS SQL 2000, MS Windows 2000 Server, VB 6.0, VB.NET, ASP, ASP.NET, Office 2000/XP, Visio 2000, MS Project, Oracle 8i., 9i, ETL, UNIX – Korn Shell scripts, MS Terminal Services, DTS, T-SQL, PL/SQL, PC-Anywhere , Visual Source Safe

Tyco Electronics – General Information Management application

- Implemented enhancements to existing application including adding a number of additional fields to reports.
- Technical Skills Utilized: MS Windows 2000 Server, VB 6.0, ASP, Oracle 9i, PL/SQL, Visual Source Safe, COM/DCOM

Tyco Electronics – Quality Non-conformance and Eng. Audit Tracking System

- Implemented enhancements to an existing application including automatic generation of emails for audits that are overdue for various phases and implementation of additional data feeds from SAP and other systems.
- Technical Skills Utilized: MS Windows 2000 Server, VB 6.0, ASP, Oracle 9i, UNIX – Korn Shell scripts, PL/SQL, ETL, Visual Source Safe

Tyco Electronics – SAP Customer Price List

- Performance tuning of an existing web application. Denormalized fields onto driving tables, created indexes and modified VB.NET components to handle data more efficiently.
- Technical Skills Utilized: MS Windows 2000 Server, VB.NET, ASP.NET, Oracle 9i, PL/SQL, , Visual Source Safe

Tyco Electronics – Quality Information and Communication Network application

- Lead developer/analyst for world wide application. Performed numerous enhancements, production support, analysis, proposal writing and functional specifications writing. Also met with end users to determine requirements.
- Technical Skills Utilized: VB.NET, ASP.NET, COM/DCOM, MS Windows 2000 Server, Windows XP, VB 6.0/.net, Office XP, Visio 2000, Oracle 9i, UNIX shell scripts, PL/SQL , Visual Source Safe, ETL

Tyco Electronics – Data Acquisition Framework

- Designed and developed new ETL components in PL/SQL and UNIX supporting enterprise data processing. Production support of existing ETL components.
- Technical Skills Utilized: Visio 2000, Oracle 9i, TOAD,UNIX – Korn Shell scripts, PL/SQL , Visual Source Safe

USTAAD Systems, Inc. September 1999 – June 2003
Data Warehouse DBA Manager / Sr. Technical Architect / Company Onsite Representative

Wells Fargo Structured Analytical Reporting

- Lead technical Architect and DBA manager for very large data warehouse (over 1 terabyte) solution. Architected technical solution based on meta data driven approach. Responsible for logical and physical data models, physical database, ETL, recovery models, data retention/archiving, OLAP modeling, Physical Cubes, cube management, flat file exports, flat reports and multidimensional reports. Company onsite representative supervising up to 10 others and managing client relations.
- Technical Skills Utilized: MS SQL 2000, MS Windows 2000 Advanced Server, MS Data Transformation Services (DTS), MS Analytical Services (OLAP), Proclarity, Erwin, VB 6.0/.net, Office 2000, PVCS, Visio 2000, MS Project, Oracle 8i., 9i, TOAD, UNIX, MS Terminal Services, T-SQL

Data Warehouse Product Manager

- Developed a Multi-dimensional (OLAP) data warehouse for electrical distribution vertical market.
- Technical Skills Utilized: MS SQL 7.0 / 2000 Beta, MS Windows 2000 Advanced Server, MS Data Transformation Services, MS Analytical Services (OLAP), AS/400, DB2/400, Essbase, Wired For OLAP, OLAP@Work, Knoyis Proclarity, Alpha Blocks, Erwin, AppsMart, MS Access, VB 6.0, Office 2000, Visio 2000, MS Project, Oracle 7 / 8i.

School Technology Management, Inc. June 2002 – February 2003
Data Warehouse DBA Manager / DBA

- Developed a full OLAP solution template for school districts. Met with numerous district and school level personal from various districts from NY to MD to develop requirements for a reporting and business intelligence solution. Developed technical architecture, managed development, and delivery.
- Technical Skills Utilized: MS SQL 2000, MS Windows 2000 Advanced Server, MS Data Transformation Services (DTS), MS Analytical Services (OLAP), Proclarity, Erwin, VB 6.0/.net, Office 2000, Visio 2000, MS Project, Oracle 8i., 9i, UNIX, MS Terminal Services, T-SQL

U.S. LifeLine, Inc. February 1999 – September 1999
Director Information Technologies (MS SQL DBA)

- Managed a team of Internet developers in support of custom Internet Information Server 4.0 Active Server Pages. Directed the conversion from a MS Access 2.0 backend to a MS SQL Server 7.0 database backend.
- Transformed internal MS Access 2.0 application to a MS Access 2000 Client Server Application utilizing MS SQL Server 7.0. Transformation included modifications to take advantage of MS SQL Server's new features to enhance existing functionality of the custom MS Access application.
- Technical Skills Utilized: MS SQL Server 7.0, Replication, remote administration, database design, Windows NT 4.0 Server Administration, cable plant administration, project management, personnel management, broad band communications, TCP/IP,

Office 2000, Access 2000 VBA, VB 6.0, Visual Interdev 1 / 6, IIS 4.0, Proxy 2.0, I-Mail, Enterprise Monitor, PC Anywhere, Carbon Copy.

Ajilon May 1995 – February 1999
Senior Consultant - DBA / Client-Server Technologies

Ajilon Offsite:

- Directed a team of network administrators and end user support specialists providing support to over 50 sales and delivery personal.
- Technical Skills Utilized: Windows NT 4.0 Server Administration, cable plant administration, project management, personnel management, T-1 connections, ISDN, RAS, Virtual Private Networks, video conferencing, MS Project, MS Visio.

Harley Davidson Motor Company, Inc.

- Client Server DBA responsible for database management of six MS SQL servers, data modeling, creating MS SQL Server stored procedures and Windows NT network administration. Also assisted in the development of Power Builder applications.
- Technical Skills Utilized: Data modeling using S-Designor, MS SQL server database management, database server tuning, MS SQL server database programming stored procedures. Administered Windows NT network, transfer of decision support tables to IBM AS/400 for further enterprise utilization.

NBC

- Designed and developed a year 2000 repository to track non-IS developed products and/or applications for Century Date Change compliance, verification, and resolution.
- Technical Skills Utilized: MS Windows NT 4.0 Server, MS Windows 95, MS SQL Server, RAS, MS Access, MS Visual Basic 5.0, database replication.

Book-of-the-Month Club, Inc.

- Developed a data warehouse environment, replacing an existing VM APL environment. Conducted business analysis for entire project by interviewing over 200 users from VP's and editors to end-users. Provided technical support to senior management liaisons, helping managers learn the new system and mentoring in relational database navigation and query writing.
- Technical Skills Utilized: Project management, Oracle 7.x, SQL-Net, ODBC, MS Access, Visual Basic, RS600 /AIX, Outbound data transfer utility.

AMP, Inc.

- Responsible for the analysis of business requirements in the reporting of business group performance against a variety of measures. Completed technical specifications for complete project, assisted in formulating proposal and implemented project by leading a team of programmer / analysts. .
- Technical Skills Utilized: Data modeling using ER-Win, MS SQL server database programming stored procedures. Applications developed in MS Access, Harvard Graphics, OLE automation, and ODBC connectivity. Data transfer from mainframe to

Windows NT server using Outbound product.

Tren Tech, Inc. March 1993 – April 1995
System Integrator

- Responsible for installation, maintenance and repairs of bar-code related equipment including thermal transfer printers, laser scanners, bar-code wand readers, magnetic strip card readers, remote data terminals, time and attendance equipment as well as general PC equipment.
- Technical Skills Utilized: Visual Basic Professional 3.0 / Visual Basic Professional 4.0 Beta, Access Jet Database. MS Windows API in a Novel, Windows NT, Windows for Workgroups network environment.

Certifications

MCITP, MCSE,
MCDBA, MCSD,
MCP, MCT,
OCP (Currently updating to 2008 versions of MS certifications.)

Certified Microsoft Instructor for MS SQL Server since MS SQL Server classes began (1996).

UNISYS

Resource 16

Database Architect

Key Skills and Knowledge

Databases

- Oracle 9i, 10g, and 11g
- RAC (Real Application Clusters)
- Oracle 9i; SQL Server 2005, 2008, 2008 R2, and 2012
- SQL Server 2000 and 7.0; OLAP (Analysis Server)
- Microsoft Access Turbo Image XL (HP proprietary database)
- MySQL

Hardware

- Compaq ProLiant servers
- Dell Power Edge servers
- IBM X series and VMware
- Oracle Virtual Server

Operating Systems

- Windows 95, NT 4.0, 2000, 2003, and 2008 R2
- UNIX and Linux
- Oracle Enterprise
- Linux and SuSE Enterprise Linux
- Red Hat Enterprise Linux (RHEL)
- Solaris and Oracle Solaris
- VMware
- Windows Virtual Server

Software/System Architecture

- SQL Enterprise Manager and MSCS Clustering
- ASM (Automated Storage Management)
- DTS, SQL Profiler, Query Analyzer, and SQL Setup
- Security Manager, Service Manager, and ODBC
- BMC PATROL, Control-M, Entegra, and NetIQ
- Quest SQL Litespeed, ERwin, and Veritas I3
- IDERA SQL Diagnostic Manager and Legato Backup Modular

Professional Summary

More than 13 years of experience in Information Technology (IT), database administration, and Oracle high availability technologies like Oracle RAC, Oracle Failsafe Manager, Streams Replication, and Active Data Guard. Experience with Microsoft high availability technologies like Microsoft Cluster servers, database mirroring, and replication. Experience in working with MS SQL Server and upgrades. Extensive database administration experience with Oracle 9i, 10g, and 11g.

- Installed, configured, and implemented 2-node Oracle 10g RAC and 11g RAC (Real Application Clusters) on Windows Server 2003 and 2008 (x64) and Solaris, Oracle Solaris, SLES, and RHEL
- Acquired experience with automated storage management (ASM) on IBM SVC/XIV-type enterprise-class storage systems
- Migrate and upgrade Oracle environments (VLDBs of more than 10 TB in RMAN/Transportable Table space)
- Implement Oracle Enterprise Manager 11g and 12c
- Administer Windows 2008 R2, 2003, 2000, and NT
- Acquired experience with UNIX and Linux environment and administration (Solaris, Oracle Solaris, SLES, and RHEL)
- Acquired experience in MS SQL Server installation, configuration, client/server connectivity, query optimization, backup, recovery, clustering, replication, log shipping, running database consistency checks using DBCC, and troubleshooting large databases.

Employment History and Related Experience

Unisys Corporation, Commonwealth of Pennsylvania,
Sr. DBA, Harrisburg, PA 2006 – Present

Administered databases hosted in Oracle 10g and 11g RAC and Oracle 9i Fail-safe in Windows and Linux environments (Solaris, Oracle Solaris, SLES, and RHEL).

- Database sizes vary from a few MBs to a VLDB.
- Manage the entire software development lifecycle, planning for hardware/software procurement/design, SQL Server responsibilities.
- Administered multiple servers with SQL Server 2000, SQL Server 2005, and SQL Server 2008/SQL Server 2008 R2 Enterprise.
- Support more than 2,000 databases spread all over the environments mentioned above; sizes vary from a few MBs to a VLDB.
- Administer development, testing, production, and disaster recovery environments.

UNISYS

Resource 16

Database Architect

- Veritas NetBackup
- Oracle Fail Safe Manager and RMAN
- Crystal Reports (versions 10 and XIR2)
- Quest TOAD DBA Suite for Oracle

Programming Languages & Tools

- C, C++, C#, UNIX, Linux, and VB.Net

ASAP Software, DBA, IL 2005 – 2006

Administered development, testing, production, and disaster recovery environments.

- Delivered database support of various vendor-based applications and custom applications developed in house.
- Maintained high availability SQL server environment using Microsoft Clustering technologies (4 servers).

QualComm, DBA, CA 2004 – 2005

Administered 30 production and 20 test servers with SQL Server 2000 Enterprise; delivered database support for 60 applications.

- Supported a high availability SQL Server environment using Microsoft Clustering technologies (6 servers).
- Created and maintained a standby environment for business-critical applications and consolidation of servers.
- Extracted, translated, and loaded data using DTS packages. Cleansed and formatted data according to the database requirements before loading. Scheduled packages to run automatically daily or weekly. Set up a test environment to maintain the accuracy of data.

T-Mobile USA, DBA, NJ 2003 – 2003

Lead DBA for the SQL Server group. Managed multiple environments for development, testing, and production.

- Administered 7 production and 4 test servers with SQL Server 2000 Enterprise.
- Maintained database performance; resolved capacity issues.
- Worked closely with NT administrators to develop and maintain a solid backup strategy.

Cooper Health System, DBA, NJ 2001 – 2003

Administered 6 servers with 6.5, 7.0, and SQL Server 2000 Enterprise; systems; implemented and rolled the system out to production.

- Performed project management for the finance, legal, business intelligence, and accounts departments.
- Managed change control and project documentation.
- Controlled the support of Internet and intranet back-end databases.

UNISYS

Resource 16

Database Architect

HSBC, Bank USA, DBA, NY 1999 – 2001

Administered 9 servers: 5 in New York and 4 in California. Used replication mainly for replicating data for reporting departments and for archiving and warehousing.

- Moved the data from staging to testing and from testing to production.
- Worked with client/server tools like SQL Server Enterprise Manager and Query Analyzer to administer SQL Server.
- Planned complete backups of databases; restored databases from disaster recovery.
- Planned and modified permission issues on the server.

Education

- Bachelor of Technology degree, Nagarjuna University, India, 1999

Professional Certification

- Oracle 9i/10g/11g Certified Professional (OCP: DBA 9i, 10g, and 11g)
- Oracle 10g RAC Certified Expert
- Oracle Enterprise Manager 11g/12c Certified Implementation Specialist
- Certified SQL Server DBA 2000 (MCDBA)
- Certified Microsoft Certified Technology Specialist (MCTS: SQL Server 2005)
- Certified Microsoft Certified IT Professional: DBA (MCITP: DBA - SQL Server 2005)
- Certified Microsoft Certified IT Professional: DBA (MCITP: DBA - SQL Server 2008)
- Oracle 9i Forms Developer-Oracle9i PL/SQL Developer OCA (Oracle Certified Associate).
- Certificate course in C, C++, and UNIX

Professional Development

- Oracle Database 11g: Performance Tuning Release 2, 2012

This page intentionally left blank.

UNISYS

Resource 17

Database Architect

Key Skills and Knowledge

- Sybase Products: ASE, Replication Server, Oracle Replication Options, Direct Connect, Open Client, Power Designer
- Oracle Products: SQLPlus, SQL Loader, Job Scheduler, and Data Pump
- Languages: BASIC, FORTRAN, COBOL, C, C++, Java, and UNIX Shell
- Operating systems: UNIX (Solaris, Linux, AIX, and DEC)
- Databases: Sybase ASE, Oracle, MySQL, Unify, Access, and SQL

Clearance

TS/SCI with Polygraph (with lifestyle).

Skills Summary

Mrs. Reinhart has 27 years of experience in the Information Technology (IT) Industry. Skilled in multiple computing languages (including UNIX shell script) and has significant experience in writing Sybase, Oracle, and MySQL Stored Procedures, database design, replication, and implementation. Developed and delivered Sybase courses, briefed Sybase and Oracle users groups, and spoken at Sybase International conferences; authored multiple technical documents.

Employment History and Related Experience

Innovative Engineering Solutions, Inc. (IESI) 2011 – Presen

Principal Database Engineer

Gathered requirements, designed database objects, and programmed stored procedures for multiple Oracle based projects for the National Security Agency (NSA).

Accomplished data transformations and imports using SQL Loader, Oracle Job Scheduler, and Oracle data pump for import/export; provided multiple projects with database related assistance using MySQL and Microsoft SQL Server; accomplished SQL tuning database configuration, backup, and recovery

Provided mentoring and troubleshooting assistance to several co-workers programming in various languages; co-lead for mentoring program. Helped start a mentoring program and conducted workshops to train the mentors; project Manager for the system integration and Cyber/Networks divisions, interacted with the prime contract representatives, and dealing with personnel issues.

SYBASE, Inc., Enterprise Solutions Division, Federal Group 1996 – 2011

Principal Consultant

Sybase Intel practice expert on heterogeneous replication, specializing in Oracle to Oracle replication using Sybase products for National Security Agency.

Wrote technical document on Sybase to Oracle two-way replication; technical expert for the Sybase ASE version 15 database service portion of a project to standardize the installation and configuration of Sybase database software across the enterprise. Partnered with multiple vendors and integrators. IBM prime.; received Sybase Gold Star Award.

Provided programming and documentation support. Reviewed and provided input for requirements documents for agency standardization project. Researched and provided input for the best practices and installation and configuration documents. Wrote the sections on archive databases, row level access, and auditing; presenter at 1997, 2002, and 2004 Sybase International User Group conferences; Extensive experience optimizing stored procedures, receipt of government letter of appreciation for work done in optimizing procedures in the wake of the September 11th attacks.

National Security Agency 1986 – 1996

Program Manager for Database Applications and User Interfaces for the Director and Executive Elements of the Agency.

- Developed a correspondence tracking aystem that became an Agency standard
- Taught Fast Track to Sybase and Introduction to C Programming at the National Cryptologic School
- Chairperson of Agency Gain Users Group.

Education

B.S. Towson University, Towson Maryland, 1974

Certifications

- Certified Sybase Professional
- Database Administrator Versions 10, 11, 12, and 15
- Replication Server Professional Version 12.5, 1.

ERP Administrator

This page intentionally left blank.

No resumes for this category

This page intentionally left blank.

UNISYS

ERP User Account Administrator

This page intentionally left blank.

No resumes for this category

This page intentionally left blank.

Firewall Administrator

This page intentionally left blank.

UNISYS

Resource 18

Firewall Administrator

Key Skills and Knowledge

- Cisco routing
- Cisco switching
- CheckPoint
- Large enterprise Internet connectivity
- Highly redundant networking
- Large enterprise 802.11a, b, g, and n wireless networking
- Resolution of complex problems

Professional Summary

Architect, implement, and support global highly available Cisco-based WAN, LAN, and wireless network solutions for converged voice, video, and data using the following technologies:

- MPLS, DMVPN, BGP, EIGRP, IOS Zone firewall, QoS (queuing, WRED, DSCP, shaping, and policing)
- Cisco 6500 (Supervisor 720-3C), VSS 1440, 4910R+E (Supervisor 7E), 3750, 3750E, 3750X, 3560, 2960, 2960S, 2950, and 2900
- Cisco ISR and ISR2 router series 3900, 2900, and 2800 routers; ASR 1000 routers
- Cisco ASA firewall and VPN appliances
- Cisco 6500 ACE load-balancing modules
- Cisco 5508 wireless LAN controllers, Cisco Aironet 3500 and 1260 series lightweight access points, and autonomous Cisco 1200 series wireless access points
- CiscoWorks LMS 3.2, Cisco ACS 4.2, RADIUS, and TACACS+
- Upgrade CheckPoint Provider-1 firewall.
- Support R65 through R75.40 SecurePlatform, IPSO, and GAIA
- Strong Level 2 and Level 3 switching skills, including MST spanning tree, LACP Etherchannel, VTP, VLAN, DHCP snooping, frame storm control, port security, port-level ACLs, and switching QoS (various models)
- Effective, in-depth troubleshooting and resolution of complex routing and switching problems
- Excellent development and support of QoS LAN, WAN, and Wireless edge-to-edge using the DIFFSERV model
- Particularly adept at engineering issues out of network systems to avoid problem
- Use tools such as Perl, regular expressions (REGEX), script development, EEM, and C programming language to broaden ability to solve problems and provide solutions.

Employment History and Related Experience

Unisys Corporation, Data PowerHouse Project,
Network Design Engineer 1 – Team Lead, Harrisburg, PA 2011 – Present

Engineer network designs; support, optimize, and monitor redundant Data PowerHouse network infrastructure.

- Provide ongoing support for the DPW Managed Security Services contract, including CheckPoint firewalls, high availability Provider-1 firewalls, and Proventia IPS.

UNISYS

Resource 18

Firewall Administrator

- Resolve complex multiagency problems.
- Coordinate resources and set priorities as necessary.

The Hershey Company, Hershey, PA	2001 – 2011
Senior Network Specialist, Network Architect	2007 –2011
Senior Network Analyst	2005 – 2007
Network Contractor	2001 – 2005

Designed, configured, deployed, and maintained a raised floor switching environment with Cisco VSS 1440 at the core and 3750E stacks at the server edge.

- Provided complete redundancy throughout the environment, using LACP Etherchannel to the Solaris and Windows servers and LACP cross-stack Etherchannel trunks from the VSS to the 3750E switch stacks.
- Improved performance and reliability and made deployments simpler, faster, and less error prone by introducing a more methodical switching design.
- Designed, configured, and maintained a redundant gigabit campus internetwork connecting 10 campus buildings spread across several square miles, providing a seamless voice, video, and data network experience for approximately 4,000 users.
- Developed a proven conceptual WAN model, the Hershey WAN Cloud, consisting of a set of rules by which the WAN was scaled and upgraded over time without jeopardizing its reliability or key features such as full mesh, dynamic recovery, and redundant connectivity.
- Migrated a WAN from hub-and-spoke Frame Relay and a dial backup topology to Sprint MPLS with Internet DMVPN-based redundant paths. Changing the topology to full mesh, stabilizing and reducing routes with BGP in place of EIGRP, introducing QoS, and adding DMVPN path redundancy nearly eliminated WAN-related network trouble calls by eliminating known and predicted problems.
- Upgraded a Sprint MPLS to an AT&T MPLS, providing a fully converged and properly scaled voice, video, and data network with QoS LAN and WAN policy that enabled voice and video deployments throughout the enterprise.
- Designed, configured, and managed 802.11b, g, and n wireless networks on Cisco autonomous Aironet 1200 access points and Cisco 5508 controller platforms using 1260/3500 series lightweight access points for 14 plants, 3 warehouses, and various offices and campus environments.
- Introduced VLANs, MST, access port policies, and Layer 3 switching to Hershey network deployments, improving performance, stability, and security throughout the enterprise.
- Installed and maintained CiscoWorks for more than 9 years to manage more than 1,500 Cisco devices, including routers, switches, and wireless access points.

UNISYS

Resource 18

Firewall Administrator

Tyco Electronics MA/COM, Senior Network Engineer,
Harrisburg, PA 2000 – 2001

Troubleshot and configured Cisco routers on 3640s and 3620s. Provided specifications for LAN/WAN performance improvements using Cisco equipment and Compaq servers.

- Developed software to initiate a dialup-networking connection between a wireless radio and a PC in Microsoft Visual C++ for the Windows platform.
- Installed and configured a demonstration wide area radio system consisting of three Sun Ultra 10s running Solaris.
- Developed test plans for factory acceptance testing of wireless radio products in a WAN environment.
- Configured proprietary radio equipment.
- Conducted beta tests and error reporting on radio, base station, and Sun Solaris-based proprietary software.

Harsco Gas & Fluid Control Group, Network Manager, Harrisburg, PA
1998 – 2000

Managed the implementation and maintenance of a Cisco router-based WAN for the entire division. Supported a mixed protocol network using RIP (IPX), OSPF, and NLSP routing protocols on Cisco 2600 and Cisco 2500 routers.

- Worked with SNA tunneling, bridging, and APPN on a Cisco-based WAN with AS/400s.
- Transitioned a Cisco multiprotocol WAN from an IP/IPX network to an all-IP network.
- Provided technical specifications and implementation guidelines for a Cisco PIX, router, and switch-based Internet connection to Harsco corporate headquarters.
- Managed a Cisco-based dial backup for factory sites to provide failover ISDN/PRI dial-on-demand connection when the Frame Relay circuit fails.
- Managed Cisco-based ISDN PPP dialup networking for analog and ISDN callers.
- Used a Cisco IOS firewall in house behind Harsco's primary firewall to refine control over traffic to Harsco's Web sites, AS400s, e-mail, and other systems.
- Completed VoIP pilot project using Cisco 3640 and 2610 routers connected to Lucent phone switches between two locations.
- Hired two highly qualified network technicians.
- Hired a telecommunications coordinator.
- Conducted formal annual reviews of employees.
- Trained employees to be high-quality support personnel.

Morgan Distribution, Systems/Analyst 1993 –1998

Fulfilled a need for and expandable flexible multiprotocol WAN supporting TCP/IP (OSPF), IPX, APPN, SNA, and bridging over Frame Relay, dialup, and point-to-

UNISYS

Resource 18

Firewall Administrator

point networks using Cisco 4700s, Cisco 2521s, and a 2512 16-port Token Ring serial router for dialup. Migrated the enterprise to IP only from IPX, APPN, SNA, and bridging

Education

- 3 years toward B.S., Information Science, Kutztown University

Professional Certifications

- Cisco CCNP, CCNA, and CCDA

UNISYS

e&e IT Consulting Services, Inc.

Resource 19

Firewall Administrator

Key Skills and Knowledge

- Top Secret clearance
- Security +
- CISSP and CCSPA
- Firewall setup and installation
- CCSPA & CISSP certs
- Cisco switch configuration
- UNIX and Windows platforms for workstations and servers
- Configure Cisco switch
- eEye Retina Vulnerability scanner
- Familiarity with Ethernet and FDDI protocols used in LAW/WAN operations
- Knowledgeable of security policies for Air Force, Department of Defense Directives, Public Key Infrastructure/Environment (PKI/PKE), and Common Criteria
- National Security Agency (NSA) Evaluation and Validation program
- Federal Information Processing Standards (FIPS)
- Network vulnerability assessment, including penetration and vulnerability analysis of security technologies
- Implement and maintain computer security plans
- Implement a Security Education Program to ensure facility compliance
- Managed the military base Communications Security (COMSEC) program

Professional Summary

Extremely experienced firewall security administrator with 15 years of experience. Ensures all network users completed the network user's licensing course and received a security clearance or background investigation. Maintain a formal Information System Security Program; ensured compliance with local procedures for clearing, purging, declassifying, and releasing systems, including memory, media, and output. Reviewed and conducts investigations for security incidents.

- Assisted with network vulnerability assessment, including penetration and vulnerability analysis of security technologies
- Ensure compliance with Department of Defense policies, regulations and guidelines
- Configure Cisco switch to run monthly scans on live network using eEye Retina Vulnerability scanner
- Familiarity with Ethernet and FDDI protocols used in LAW/WAN operations
- Reviewed the security on new and existing Information Systems for the Air Force Weather Weapons System Program Office
- Tested and evaluated the security of information systems using various scanning/vulnerability/penetration tools (Nessus, Nmap, Retina, and Wireshark sniffer)
- Performed Certification Testing on new systems using eEye Retina vulnerability scanner and DISA Gold Disk
- Prepared for Annual Federal Information Security Management Act (FISMA) Review Audits by the Air Force Audit Agency.

Employment History and Related Experience

e&e IT Consulting Services Inc., Network Security Engineer, New Cumberland, PA 2011 – Present

Oversee and monitor 36 computer networks worldwide. Lead a third-tier firewall support help desk. Setup and install firewalls, MRVs, IDSs, and WAN optimization appliances.

- Track equipment at all 36 locations.
- Implement, monitor, and update Enterasys Network Access Control (NAC) appliances.
- Retire or replace old equipment.

Quantum Dynamics Inc. Information System Security Officer (ISSO), Otis Air Base, MA 2009 – 2011

Oversaw computer security for a military unit; ensure compliance with Department of Defense policies, regulations, and guidelines.

e&e IT Consulting Services, Inc.

Resource 19

Firewall Administrator

- Configured Cisco switch to run monthly scans on a live network using eEye Retina Vulnerability scanner.
- Became familiar with Ethernet and FDDI protocols used in LAW/WAN operations.
- Evaluated and resolved Information Assurance Vulnerability Alerts (IAVAs).
- Created accounts for new users using LDAP.
- Analyzed audit logs and reported anomalies.
- Reviewed and archived server and workstation audit logs.
- Ensured virus definitions were less than 30 days old and the scan engine was up to date on UNIX/Solaris and Windows platforms (workstations and servers).

Jacobs Technologies Corp, Senior Network Security Engineer,
Hanscom Air Base, MA 2008 – 2009

Reviewed the security for new and existing information systems for the Air Force Weather Weapons System Program Office. Performed certification testing on new systems using eEye Retina vulnerability scanner and DISA Gold Disk.

- Prepared for Annual Federal Information Security Management Act (FISMA) Review Audits by the Air Force Audit Agency.
- Prepared documentation of systems for Army and Air Force approvals: Interim Authorities to Test (IATT), Authorities to Connect (IATC/ATC)/Operate (IATO/ATO), and Certificates of Networthiness (CoN) using the DIACAP format.
- Prepared System Identification Profiles (SIPs) and registered new programs.
- Created new versions and entered information assurance controls (DoD 8500.2) using the Security, Interoperability, Supportability, Sustainability and Usability (SISSU)/IT Lean process in the Enterprise Information Technology Data Repository (EITDR).
- Tracked the progress of a dozen information systems using Gantt charts in Microsoft Project.

Lockheed Martin Corp., Senior Systems Security Analyst,
Hanscom Air Base, MA 2006 – 2008

Worked with development teams on new information systems for the Combat Information Transport System (CITS) Program Management Office.

- Wrote System Security Authorization Agreements/System Security Plans (SSAAs/SSPs) for accreditation in the DITSCAP and DIACAP formats.
- Developed test plans for Certification Test and Evaluation (CT&E).
- Tested and evaluated the security of information systems using various scanning, vulnerability, and penetration tools (Nessus, Nmap, Retina, and Wireshark sniffer).

e&e IT Consulting Services, Inc.

Resource 19

Firewall Administrator

- Ensured system components complied with Air Force Instructions, Department of Defense Directives, Public Key Infrastructure/Environment (PKI/PKE), Common Criteria, the NSA/NIST/NIAP Evaluation and Validation program, and Federal Information Processing Standards (FIPS), in accordance with NSTISSP 11.

Maryland Air National Guard, Information Technology Specialist, Warfield Air Base, MD 1988 – 2006

Team lead for the certification and accreditation of a local area network in the DITSCAP format. Reviewed accreditation to ensure compliance with Air Force and DoD regulations. Reviewed and performed Security Tests and Evaluations (ST&E) of the network. Performed risk assessment and risk analysis; made recommendations

- Ensured all network users completed the network user's licensing course and received a security clearance or background investigation.
- Maintained a formal Information System Security Program.
- Ensured compliance with local procedures for clearing, purging, declassifying, and releasing systems, including memory, media, and output.
- Reviewed and assisted in the investigation of security incidents.
- Assisted with network vulnerability assessment, including penetration and vulnerability analysis of security technologies.
- Implemented and maintained computer security plans.
- Documented and presented a security education program to ensure facility compliance.
- Managed the base Communications Security (COMSEC) program.
- Reviewed server event logs.

Education

- B.S., Management Information Systems, Syracuse University, School of Management

Certifications

- CheckPoint Certified Security Principles Associate (CCSPA), 2011
- Certified Information Systems Security Professional (CISSP), 2010
- Security +, 2009
- Current Top Secret (TS/SCI) clearance

This page intentionally left blank.

UNISYS

e&e IT Consulting Services, Inc.

Resource 20

Firewall Administrator

Key Skills and Knowledge

- Commonwealth experience
- CheckPoint security engineer
- Offshore VPN firewall installtion
- Server farm firewall upgrades
- VMware ESX
- CheckPoint Connectra R62
- Mobile Access
- R75.20 Smart-1 appliances in HA model
- Filtered Internet access via WebSense
- Productivity, reliability, and accessibility improvements
- Diagnose and troubleshoot a broad scope of technical problems
- Disaster recovery
- HP, 3Com, and H3C core technologies
- Cisco ASA and legacy Nortel network equipment
- HP EVA SAN
- Barracuda networks
- BlueCoat Web filtering products

Professional Summary

Highly efficient IT professional qualified by more than 12 years of combined experience in network design, configuration, implementation, and maintenance. Visionary who is skilled at deploying business-class to mid-range networks and provides foundations for advanced network, voice, and security solutions.

- Strong analytical, troubleshooting, and technical acumen enhanced by exceptional organizational and communication skills
- Noted ability to communicate technical concepts to nontechnical users
- Recognized agency-wide as a go-to-guy for resolution of problems
- Particular expertise in network monitoring; HP, 3Com, and H3C core technologies; Cisco ASA; and legacy Nortel network equipment
- Further experience in CheckPoint R75.20 and Connectra R66, VMware ESX Server2, HP EVA SAN, Barracuda networks, and BlueCoat Web filtering products.

Employment History and Related Experience

Bluecross Blueshield, Senior Network Security Engineer, MA 2011 – Present

Member of a design and implementation team. Deploy R75.20 for SecurePlatform on Power-1 appliances using ClutsterXL HA.

- Update Connectra R62 to Mobile Access R75.20.
- Perform day-to-day management of firewall policy and IPS profiles.
- Upgrade management and logging servers to R75.20 on Smart-1 appliances in High Availability mode.
- Install offshore VPN firewalls.
- Upgraded a firewall for a 10 GB server farm.

Dauphin County, LAN/WAN Administrator, PA 2006 – 2011

Network Group analyst and liaison to server and desktop groups in the IT department.

Administered configuration change orders on Cisco ASA firewall access and NAT rules for mail and Web services Maintained ASA backups.

- Deployed and monitored Tippingpoint IPS and firewall profiles as well as VPN support.
- Configured, evaluated, and monitored network performance on HP and 3Com 7500 series core locations as well as all switches and edge devices.
- Built and deployed departmental CheckPoint Connectra portals.
- Continually diagnosed and troubleshot a broad scope of technical problems at site locations.

- Recommended new hardware to meet the County's growing needs.
- Engineered and installed HP and 3Com core data infrastructure for Dauphin County's 911 Center.
- Deployed public safety portals using CheckPoint Connectra R66.

Delaware County, Pennsylvania, Network Administrator, PA 1996 – 2006

Team and project leader challenged to manage, monitor. and support a 46-site Frame Relay-based wide area network with connectivity to all county departments. Processed change orders for the Nokia-based CheckPointNG. Managed and coordinated projects through the entire development cycle together with service providers such as ESRI and Info Systems.

- Standardized local networks on an extensive Microsoft Windows NT and 2000 platform, using Exchange, SMS, SQL7.0-2000, and IIS.
- Implemented network security protocols.
- Evaluated and monitored system and network performance.
- Configured and maintained all servers.
- Tested and recommended new hardware and software to meet the County's growing needs.
- We continually on call to diagnose and troubleshoot a broad scope of technical problems at site locations; played a key role in disaster recovery.
- Supported judicial network project securely connecting all municipalities to the county network architecture and the consolidation of T1s to DS3.
- Participated in launching a countywide Web page (www.co.delaware.pa.us) that allows public and internal access to government departments and schools. The site averaged more than 17,000 hits a day in the fourth quarter of 2003.
- Organized the Real Estate Assessment Web page to consolidate information from three databases into a data warehouse presented with ArcIMS (http://w01.co.delaware.pa.us/pa/publicaccess.asp).
- Developed the CommerceCenter Web page (www.delcopa.org).
- Introduced filtered Internet access to all public libraries with WebSense.
- Captured significant cost savings plus productivity, reliability, and accessibility improvements resulting from service convergence.

Emergency Services Training Center, Computer Support Specialist 1997 – 2006

Designed and implemented a sophisticated network connecting various Delaware County agencies to this $1 million emergency services training facility. Ensured continuity of service to critical fire and police departments with little to no interruption in service. Since 1993, more than 78,000 emergency services personnel were trained at the facility.

e&e
IT Consulting Services, Inc.

Resource 20

Firewall Administrator

- Played a lead role in implementing a secure wireless network connecting the Emergency Services Training Center and Pennsylvania State University, which partnered to create CERT, a citizens emergency response-training program certified by the Board of Fire, Life & Safety.
- Directly after implementation, achieved and continued to maintain up-time support of 99.9 percent.
- Set up and supported wireless mobile labs in various locations.

Neumann College, Computer Lab Assistant/
Teaching Assistant, Aston, PA 1992 – 1996

Capitalized on a wide range of knowledge of AppleTalk, IPX/SPX, and TCP/IP to connect all computers in the Intel and Macintosh labs to a Novell-based network.

- Provided students and staff with technical support and training.
- Conducted nightly ColoradoTrakker system backups.
- Responded to help desk calls.
- Facilitated PC rollouts with minimal downtime.
- Developed and wrote technical resource manuals for the college.

Education

B.A., Liberal Studies, Neumann University, Aston, Pennsylvania 2001

Minor: Computer Information Management

This page intentionally left blank.

UNISYS

Firewall Administrator

Key Skills and Knowledge

- Project and Program Management
- Communication and networking
- Hardware
- Operating systems
- Software/system architecture
- Office productivity tools
- Technical documentation
- Facilities management
- Cisco infrastructure
- 76xx border routers, 65xx series Core Layer 3 switching
- BGP peering to 3 upstream providers
- OSPF as local routing protocol
- Configuration, migration, documentation, and support requirements
- Content switching, high availability switching , routing, and firewall zone management
- Drafted a Quality of Service (QoS) standard to support VoIP, videoconferencing, and ERP
- Produced capital budgets for key business revenue – generating services in 7 separate facilities
- Developed operation figures to maintain and support the capital investments
- Managed multiple successful business acquisitions
- Convert networks

Professional Summary

More than 20 years of building highly resilient secured networks to meet business capacity needs and availability. Ability to lead during changes and maintain sustained performance.

- Detailed problem analysis ability to analyze detailed problems
- Multitasking of time-sensitive projects
- Security structured by the Common Body of Knowledge
- Proficiency with administering with firewall security policy
- Orientation to customer service and results
- Development of integrated organization structure.

Employment History and Related Experience

Unisys Corporation, Commonwealth of Pennsylvania, Network Security Engineer, Harrisburg, PA 2007 – Present

Responsible for Commonwealth of Pennsylvania server farm network & hardware operations, security access & firewall configuration, performance & high availability designs and development.

- Configuration, migration, documentation and support requirements maintaining content switching, high available switching, routing and firewall zone management.
- Detailed technical reviews of all network and security changes proposed to support agency business requirements.
- Detail packet analysis supporting application, network, and security operations.

Harsco Security, Network Engineer, Harrisburg, PA 2006 – 2007

Consultant for a local business as a networking WAN engineer. Reviewed core infrastructure, implemented HSRP, and configured Multi Home BGP access. Diverse MPLS connections interconnected the enterprise campus core hardware.

- Drafted the corporation's Quality of Service (QoS) standardi to support VoIP, videoconferencing, ERP, and other critical business applications.

Susquehanna Communications, Director of Network Engineering 2003 – 2006

Developed, designed, structured, and managed an organizational strategy for voice, video, and high-speed data, providing support and security over a geographically diverse multiple cable service operation.

UNISYS

Firewall Administrator

- Implemented a Cisco infrastructure using 76xx border routers, 65xx series Core Layer 3 switching, BGP peering to three upstream providers, and OSPF as the local routing protocol.
- Directed the overall operations of seven large public network infrastructures providing high bandwidth and availability.
- Managed the conversion of a high-speed data product and infrastructure at a newly acquired cable market supporting more than 14,500 HSD subscribers under complex conditions and a tight timeline.
- Supported interactive video data network operations for this conversion.
- Produced capital budgets for key business revenue-generating services in seven separate facilities along with operation figures to maintain and support capital investments.

BlazeNet (Subsidiary of Susquehanna Media Corporation)
Team Lead Network Engineer 1997 – 2003

Designed networking business product offerings that provided a competitive edge over the competition, driving record sales, using Frame Relay, ATM, point-to-point T1 or fraction T1, DSL, cable modems, wireless, and SONET technology. Designed, implemented, and managed a large Web hosting server farm network using Foundry load balancers and a 802.1Q strategy.

- Maximized business sales opportunity by interacting with commercial customers and finding designs and partnerships that generated their highest ROI, which positioned BlazeNet as the preferred vendor.
- Implemented diverse Internet access points for small business by using EIGRP, which provided dynamic bandwidth failover.
- Managed multiple successful business acquisitions for the network conversion, which secured a stronger local community presence and increased revenue potential on capital investments.
- Influenced early adoption of virtual private networking, leveraging the technology in the commercial product offering and providing businesses with an opportunity to reduce or eliminate dedicated telecommunication lines.
- Led the business in network security for internal application access, commercial resale, and product development, which increased uptime and reduced repairs, providing higher efficiency.

Education

- Associate's degree in Computer and Electronics, Electronic Institute

UNISYS

Firewall Administrator

Professional Certifications

Certifications

- ITIL v3 Foundation Certification, 2012
- Cisco Certified Internetwork Professional (CCIP) Certification – updated, 2012
- CheckPoint Certified Security Expert (CCSE) Certification, 2008
- CheckPoint Certified Security Administrator (CCSA) Certification, 2007
- Cisco Certified Design Professional (CCDP) Certification – updated, 2012
- Cisco CCDA Certification – updated, 2012
- Cisco Certified Networking Professional (CCNP) Certification – updated, 2012
- Cisco CCNA Certification – updated, 2012
- ISC² Certified Information Systems Security Professional (CISSP), 2012
- GIAC Security Leadership Certificate (GSLC), 2005

Professional Development

Certificates of Completion

- Imperva Application Firewall Operation and Administration, 2012
- ITIL 2011 Foundation, 2012
- BMC BladeLogic BBNA Operation and Administration, 2012
- SANS: Google Hacking / Defense, UNIX Security & Auditing, Security Leadership Essentials for Managers, Legal Issues in Information Technologies, Fundamentals of Information Security Policy, 2005
- ARRIS, CMTS C4 Operations, 2003
- Alvarion, 2.4 GHz Wireless, 2002
- Learning Tree, Solaris Administration, 2001
- Global Knowledge, Cisco CCIE Prep Lab, 2000

This page intentionally left blank.

UNISYS

Resource 22

Firewall Administrator

Key Skills and Knowledge

- Routing
- Switching
- Firewalls
- IPS Devices
- SolarWinds Orion
- Cisco Security Manager
- CheckPoint SmartCenter
- Catalyst 6500 VSS
- Cisco Application Control Engine
- IBM Proventia
- McAfee Network Security Platform intrusion prevention systems
- Cisco Pricing tool and Dynamic Configuration tool
- Cisco CSM, ANM, and MARS management tools
- Redesign data centers to reduce footprint and leverage virtualization technologies
- Configure and troubleshot SolarWinds Orion Network Performance Monitor and eEye Retina products
- Recommend products and specify parts to upper management and customers
- Configured Cisco wireless access points for office user connectivity

Professional Summary

Cisco Certified Network/Design Professional with 5 years of experience in designing, configuring, and troubleshooting Cisco and CheckPoint solutions. Able to perform as a key contributor in a team-oriented environment through a diverse technical background. Well-spoken with expertise to effectively communicate ideas and recommendations to facilitate positive change.

Employment History and Related Experience

Unisys Corporation, Network Design Engineer 2007 – Present

Provided network engineering for Commonwealth systems. Implemented Cisco VSS to maximize overall network uptime to 99.999 percent. Used VRFs to leverage common infrastructure for multiple customers with stringent security requirements. Implementing and manage firewall rule bases on CheckPoint and Cisco platforms. Building CheckPoint SPLAT/IPSO boxes from scratch.

- Manage and support Cisco Application Control Engine appliances.
- Enterprise-class devices include Cisco Nexus, 6500 and 4500 series switches and 3800 series routers.
- Use 10 Gbps technologies to reduce port density and overall solution costs.
- Designed and managed a structured cabling project to update a site to data center compliancy standards.
- Manage and configure IBM Proventia and McAfee Network Security Platform intrusion prevention systems.
- Proficient with Cisco CSM, ANM, and MARS management tools.
- Contributed to data center redesign to reduce footprint and leverage virtualization technologies.
- Configure and troubleshot SolarWinds Orion Network Performance Monitor and eEye Retina products.
- Key contributor to recommending product and specifying parts to upper management and customers.
- Use the Cisco Pricing tool and Dynamic Configuration tool.
- Configured Cisco wireless access points for office user connectivity.

Rite Aid Corporation, Merchandise Coordinator 2004 – 2007

Supported business operations by creating store distributions for the seasonal item process so that each store had the appropriate inventory levels to maximize sales at the beginning of each event.

- Reviewed individual store allocations for a seasonal item process to ensure the accuracy of information.
- Created exception reports for management's review; made changes to report items as a result of these reviews.

UNISYS

Resource 22

Firewall Administrator

- Coordinated and monitored the distribution of seasonal item merchandise from the warehouse to the stores to ensure timely receipt of products before the start of each event.
- Prepared preliminary reviews of item allocation for use by department managers.
- Interacted with store personnel on inventory discrepancy issues; corrected errors that occurred.

Circuit City, Network Advisor 2002 – 2004

Designed and installed computer systems, networking components, and related products.

- Went to customers' residences; installed and configured networking components for proper connectivity.
- Sold and installed hardware devices, peripherals, and software.
- Consistently exceeded sales quotas for product and service upgrades.
- Lead staff associate in technical knowledge of hardware devices, networking, peripherals, and software.

NetComm Solutions, Inc., Lead Support Technician 2000 – 2002

Troubleshot, installed, and configured equipment for government contracts; served as a group leader of the statewide thin client rollout for the Administrative Office of Pennsylvania Courts.

- Installed Cisco 1720 routers with U.S. Robotics 56K dial backup modems and Cisco 2900XL switches in each District Justice Court House.
- Extensive work troubleshooting Compaq's complete line of desktop and server products.
- Provided technical support to the Pennsylvania State House of Representatives, Democratic Caucus.
- Installed, configured, and administered Microsoft Terminal Services and Citrix MetaFrame XP.
- Instructed new technicians on configuring and implementing thin clients, desktops, and servers.
- Help desk work involved interacting and supporting users from large accounts such as the Pennsylvania State House of Representatives, Democratic Caucus and the Administrative Office of Pennsylvania Courts.

Education

McAfee Network Security Platform Administration Training – McAfee Education (June 2012)

- Deploy McAfee NSP
- Build Policy
- Manage and administer NSP to defend against attacks

UNISYS

Resource 22

Firewall Administrator

CCSA Training – Fishnet Security (January 2012)

- Secure communications across the Internet
- Defend against network threats
- Configure security policies
- Protect e-mail and messaging content
- Manage user access to corporate LANs

Cisco ACE Bootcamp – Firefly (November 2011)

- Install, configure, and troubleshoot the Cisco Application Control Engine
- Design and configure integration of the ACE into the network topology
- Design and configure multiple ACE contexts to virtualize network services
- Manage allocation of resources to virtual contexts
- Use the Cisco Modular Policy CLI to configure ACE features
- Configure IP application-based security
- Configure Layer 4-7 load balancing
- Configure health monitoring
- Configure Layer 7 protocol processing options
- Configure SSL protocol processing
- Configure the Web application acceleration features on the ACE appliance
- Configure the ACE module or appliance for high availability

Cisco Certified Security Professional – CCBOOTCAMP (September 2010)

- 642-504 Securing Networks with Cisco Routers and Switches (SNRS)
- 642-524 Securing Networks with ASA Foundation (SNAF)
- 642-515 Securing Networks with ASA Advanced (SNAA)
- 642-533 Implementing Cisco Intrusion Prevention System (IPS)

Cisco Certified Network Professional – CCBOOTCAMP (January 2009)

- 652-901 Building Scalable Cisco Internetworks (BSCI)
- 642-812 Building Converged Cisco Multilayer Switched Networks (BCMSN)
- 642-825 Implementing Secure Converged Wide Area Networks (ISCW)
- 642-845 Optimizing Converged Cisco Networks (ONT)

Microsystems Technology – CLN (May 2000)

- Implement and troubleshoot network technologies, Microsoft Windows NT Server, Windows 2000 Server, and cabling in a lab environment
- Work with services such as DNS, WINS, and DHCP
- Configure and use the advanced features of Microsoft Office applications

UNISYS

Resource 22

Firewall Administrator

Professional Certifications

- Cisco Certified Network Professional, January 2009
- Cisco Certified Design Professional, June 2009
- Cisco Certified Security Professional, September 2010
- Cisco Web Security Field Engineer Specialist, February 2011
- Microsoft Certified Professional

Hyper V VMware Certified Admins

This page intentionally left blank.

UNISYS

Resource 23

Hyper V VMware Certified Administrator

Key Skills and Knowledge

- Server Administration
- Infrastructure management and problem resolution
- Data center migration
- VMware ESX/ESXi 3.x thru 5.x
- All Windows Server Operating Systems
- All Windows Desktop Operating Systems
- Symantec Endpoint Protection
- McAfee Security Products
- BMC BladeLogic
- Disaster Recovery Testing
- Server script maintenance
- Remote monitoring and support of Backup Power units
- Inventory and manage system security
- Maintain System Configuration
- Monitor servers and alert the team of hardware failures

Professional Summary

- Operating Systems: All Windows Server Operating Systems, all Windows Desktop Operating Systems
- Hardware: HP, IBM, Dell, and Unisys servers, EMC CLARiiON SAN, APC Power, Racks and Remote Monitoring, Raritan IP KVM Switches
- Software: VMware ESX and ESXi Server 3.5 – 5.0, Microsoft Exchange, Symantec Endpoint Protection 11, McAfee VirusScan Enterprise, Host Intrusion Prevention and ePolicy Orchestrator, HP Insight Manager, SolarWinds IP Monitor, APC Infrastructure Manager

Employment History and Related Experience

Unisys Corporation, Commonwealth of Pennsylvania, Systems Analyst II, Harrisburg, PA — 2010 – Present

- One of the primary resources for VMware Infrastructure management and problem resolution.
- Migrated internal management VM environment from ESX 4.x to 5.x.
- Deployed health check script to check VM stability each night.
- Currently developing and managing VMware View Proof-of-Concept.
- Primary resource supporting McAfee VirusScan environment.
- Migrated entire data center from VSE 8.7i and before to VSE 8.8.
- Moved ePolicy Orchestrator from 4.0 to 4.6.x.
- Conduct Disaster Recovery testing 3 times a year for two different state agencies.
- BMC BladeLogic Patch Management.
- Windows Server 2003 and 2008 Builds.

Commonwealth of Pennsylvania – PSP

- Lead Server Administrator for CLEAN, CCHRI, PATCH, and Megan's Law servers
- Handled all aspects of the CCHRI Tech Refresh in early 2012
- Delivered Megan's Law servers in time for roll-out and testing prior to Go Live in late December
- Currently working on PATCH Server refresh
- Responsible for semi-annual DR Tests for CLEAN and CCHRI environments
- Continual monthly maintenance to keep the servers running at their peak performance and security

UNISYS

Resource 23

Hyper V VMware Certified Administrator

Commonwealth of Pennsylvania – DOR

- Primary Server Administrator for all Wintel DOR servers since they moved to the DPH
- Continued support for agency as they move toward their migration date in the middle of 2013
- Continual monthly maintenance to keep the servers running at their peak performance and security

Commonwealth of Pennsylvania – IES

- Since hired at Unisys in 2010, have been assigned as Secondary Administrator for all Wintel servers in the IES environment
- Assist the agency with frequent builds and decommissions of servers
- Rolled out VMware Capacity IQ to monitor the virtual resource allocation to the VMs
- Upgraded VMware Capacity IQ to the newest version of VMware vCenter Operations Manager
- Configured a health check script in their VM environment that runs each morning to check for problems or errors that could cause issues or outages

Commonwealth of Pennsylvania – DOS

- Secondary Server Administrator for Wintel Environment

Commonwealth of Pennsylvania – PSERS

- Secondary Server Administrator for Wintel Environment

Commonwealth of Pennsylvania – PUC

- Secondary Server Administrator for Wintel Environment

Holy Spirit Hospital, Network Specialist II, Camp Hill, PA 2007 – 2010

- Primary resource on the following:
  - VMware ESX Infrastructure
  - Exchange 2003
  - BlackBerry Enterprise Server
  - Symantec Endpoint Protection (AntiVirus)
- Created database to track inventory and configurations of all servers
- Provide primary support of 275 on-site servers along with other members of Server Team
- Setup, configure, troubleshoot and administer 8 nodes in an HP Blade environment
- Setup HP Insight Manager to monitor the servers and alert the team of any hardware failures

UNISYS

Resource 23

Hyper V VMware Certified Administrator

- Project Lead on migration from McAfee AntiVirus Enterprise to Symantec Endpoint Protection 11
- Migrated Microsoft Exchange 2003 cluster from direct-attached storage to EMC CLARiiON SAN
- Implemented remote surveillance and temperature monitoring system in Server Room
- Developed and carried out project to upgrade existing McAfee VirusScan Enterprise clients from 8.0i to 8.7i
- Perform proactive remote monitoring and support of APC Backup Power units throughout enterprise
- Suggested and implemented Solarwinds IP Monitor to perform up/down and other resource monitoring on Windows Servers
- Planning, designing and migrating from Exchange 2003 to Exchange 2010.

NTN-BCA, Network Support Analyst, Lititz, PA 2006 – 2007

- Disaster recovery for LAN-based systems using HP OpenView
- Administer Windows servers running Lotus Domino, Kronos timekeeping, DHCP, Fax Server, HTTP, and PHP
- Administer Linux servers supporting DNS and NTP
- Support Microsoft Windows (English and Japanese) personal computers running Microsoft Office, AutoCAD, Lotus Notes, Oracle Applications 11i
- Apply technology for improved office and plant efficiency

Exel, Systems Administrator, Palmyra, PA 2001 – 2006

- Responsible for 92 workstations, 6 servers, and the entire building network
- Managed all aspects of complete rollout of 92 brand new Dell desktops and laptops throughout the building as well as migration to new Windows XP operating system
- Maintain over 100 user accounts on a Windows 2003 Domain, and over 80 mailboxes on an Exchange 2003 Server
- Project Manager on Windows NT to Windows 2003 Server Migration as well as Exchange 5.5 to Exchange 2003 migration
- Responsible for inventory accuracy of all the computer equipment in the building
- Manage and maintain all Web-based applications (SharePoint, Intranet, Web-Based Forms, etc.)
- Create documentation for the end-user and system administration processes
- Maintain high availability of file, print, database, and other critical business applications

UNISYS

Resource 23

Hyper V VMware Certified Administrator

Education

- Studied in the College of Information Technology, majoring in IT Management Touro University International, 2004 - 2005

Professional Certifications

- Microsoft Certified Technology Specialist (MCTS), 2010
- VMware Certified Professional (VCP4), 2010
- VMware Certified Professional (VCP5), 201
- VMware Certified Professional – Desktop (VCP5-DT), 2012
- ITIL V3 Certified, 2012

UNISYS

Resource 24

VMware Consultant

Security Clearance

- DOD Secret Clearance

Key Skills and Knowledge

- Hardware
- Operating Systems
- Software/System Architecture
- Programming Languages & Tools
- Call Center and Help Desk
- Office Productivity Tools
- Technical Documentation
- Virtualization

Professional Summary

VMware Certified Professional with over ten years' experience in information technology. Well-versed in designing, implementing, and supporting a virtual infrastructure using VMware products. Working knowledge of Windows server editions. In depth hands on experience with Dell, HP Proliant, IBM P Series, and Solaris hardware. Proven ability to build relationships with all levels of personnel, internally and externally to the organization. Sought out as a project member when new projects are identified. Recognized as a team member that is willing to give 100% and then some.

Professional Experience Include most recent first

Unisys, Commonwealth of Pennsylvania, VMware Consultant, October 25, 2012 to Present

Participate as a member of the Commonwealth's Virtualization team conducting VMware administration. Tasks include building the virtual infrastructure, physical to virtual conversions, business continuity using VMware Site Recovery Manager. Processing Remedy tickets and performing on call duties.

Employment History

Infinite Group, Inc. 2011 – 2012

Viatech, Inc. a DSCI Company 2010 – 2011

Independence Blue Cross 1996 - 2010

Education Include High School or greater

Bachelor of Science, Information Technology, Peirce College, 2003

Associate in Applied Science, Accounting, Burlington County College, 2000

Professional Certification

VMware Certified Professional on vSphere 5, Pearson VUE, February 8, 2012, 30047

VMware Certified Professional on vSphere 4, Pearson VUE, December 16, 2009, 30047

VMware Certified Professional 310, Pearson VUE, September 18, 2008, 30047

UNISYS

Resource 24

VMware Consultant

Professional Development

- VMware Site Recovery Manager Version 1.0.
- Install, configure, and operate VMware Site Recovery Manager
- Execute disaster recovery tests and production failovers. August 2, 2011.

UNISYS

INFO-MATRIX CORPORATION

Resource 25

Hyper-V VMWare Certified Administrator

Key Skills and Knowledge

- VMware Certified Professional – VCP in VI3

Skills Summary

VMWare/Vsphere certified professional. Senior Windows engineer for over 10 years' experience. Responsible for disaster recovery and continuity of business operations.

Employment History and Related Experience

Susquehanna Bancshares, Lititz, Pa, August 2010 – Current

Network Support Specialist II

- Responsible for the overall configuration settings of the VMWare\Vsphere environment which, includes but is not limited to: V-Motion settings, Host Cluster settings, Affinity rule settings, DNS Configuration settings, DRS, and HA.
- Responsible for ensuring that the disaster recovery solution associated with the VMWare\Vsphere environment is documented, regularly tested, and available.

HP Enterprise Services, Camp Hill, Pa, November 2009 – August 2010

Technology Consultant III

- Windows Engineer providing hardware and software support to over 200 Microsoft Windows servers utilizing both physical hardware and VMware virtualization.
- Also utilizing Windows Server Update Server for patch management.

Hudson Advisors, East Hanover, NJ, December 2008 – May 2009

Consultant

- Successfully implemented an entire new infrastructure utilizing both Windows 2008 Server and EMC Clariion technologies, which consisted of two EMC CX-320's containing over 8TB of data.
- Implemented a new Backup, Recovery and DR system utilizing Microsoft's Data Protection Manager 2007, which will provide continuous data protection of the entire infrastructure.

CIT, Livingston, NJ, May 2000 – November 2008

AVP, Network Engineering

Technology Implementation and Delivery

- As a Senior Windows Engineer at CIT, was responsible for maintaining High Availability using Microsoft Cluster Services. Installed and maintained Windows server Clusters using both Windows 2000 and Windows 2003 Operating systems combined with using an EMC SAN Infrastructure on both Symmetrix and Clariion systems.

- Also installed and maintained Windows Clusters with an EMC Clariion backend in our Europe, China, Chicago, and Oklahoma City offices.
- Led a server consolidation and virtual infrastructure project using VMware ESX VI3 virtual server technology to reduce our physical servers by 60%. Participated in the business planning, budget creation and technology platform development. Was also tasked with being the VM administrator, responsible for the build, troubleshooting and backup / recovery of current and proposed virtual servers.
- Took part in the conversion of our entire VMware Infrastructure from ESX Server 2.5x to VMware Infrastructure 3 using Vizioncore's vMigrator, consisting of 10 ESX servers with over 200 VMs.
- Took part of a company-wide server consolidation effort. This on-going project included planning, implementation and testing of an enterprise-scale Storage Area Network solution. During this project, extensive experience was gained utilizing EMC products including Powerpath, Navisphere, Snapview, Solutions Enabler, Timefinder, Replication Manager and both Clariion (CX3 /CX series) and Symmetrix (DMX3 / DMX4) platforms. Details of this project included the establishment of 15 active / active Microsoft Windows SQL Cluster incorporating Veritas Media Servers entwined with EMC Timefinder SQL Integration Module enabling us to mirror production data and back it up.
- Environment included support of 500 physical servers.

Customer Service/Support and Maintenance

- Windows Engineer providing hardware and software support to over 400 Microsoft Windows servers at corporate headquarters. Implemented Microsoft Clustering and Load Balance Designs. Broad knowledge of WINS, DNS, DHCP and TCP/IP protocols.
- Worked closely with the Information Security Group to constantly monitor potential threats and develop mitigation policies and procedures. Member of the incident first response team performing root cause analysis of outages.
- Member of the disaster recovery team, developing and documenting procedures for business continuity and planning for disaster recovery. Participated in many large scale disaster recovery tests at the corporate hot site.
- Assisted all Technology Support Groups throughout CIT in both national and global offices. Took part in projects consisting of deploying new workstations using both Ghost imaging and Altiris deployment software.
- Managed and executed an Antivirus software deployment project which was companywide (6000 nodes) on all desktops and servers using Computer Associated Etrust Integrated Threat Management software

Hamburg-SUD (formerly Columbusline INC), Morristown, NJ, August 1999 – May 2000

Technical Support Representative

Senior level position providing support for all personal computer, server, and hardware/software related problems for all nationwide locations serving over 500 end users. Responsibilities include administration of all Novell and Windows servers, desktop support of all workstations both internal and external locations, provide support for laptops, remote access, and tape backups using Computer Associates Arcserve.

United Parcel Service, Mahwah, NJ, September 1994 - August 1999

Network Administrator / Analyst

Senior level position providing third level support for all personal computer, client-server, and hardware/software related problems for all four corporate locations serving 3000 end users. Responsibilities included administration of Novell and Windows servers, network printers, disaster recovery, and tape backups using Computer Associates Arcserve.

PC Support and Server Administration

Technical resource for a major project that involved migrating users and data from multiple legacy NT domains to a new Global Domain Architecture

Designed and performed an analysis of the department's performance in relation to individual and team goals that dramatically improved technicians' cooperative efforts to attain a significant service level

Education

Nyack College, Nyack, NY

Bachelor of Science in Organizational Management

Plaza School of Technology, Paramus, NJ

Certified Computer Technician

Certifications

VMware Certified Professional – VCP in VI3

This page intentionally left blank.

UNISYS

Resource 26

Hyper V VMware Certified Administrator

Key Skills and Knowledge

- VMware vSphere 4/5 & ESX/ESXi
- Windows
- Active Directory
- EMC Avamar
- Symantec NetBackup
- Disaster Recovery Planning
- PowerShell Scripting

Professional Summary

Knowledge in the following: VMware vSphere ESX/ESXi 3.x, & 4.x, & 5.x, Windows 2003/2008, PowerShell & VB Script, Active Directory, Security Policies, IIS, DHCP, DNS, FTP, IBM Blade Center Servers, Dell Commodity Servers, EMC Data Domain, EMC Avamar, Microsoft Failover Clustering, Network Load Balancing, Microsoft DFS & DFS-R.

Capable in the following Server software: BMC BladeLogic, MS Exchange 2000, 2003, 2007, Microsoft SQL 2005/2008 management, Symantec NetBackup 6.x, & 7.x, Backup Exec System Recovery, Symantec AV, McAfee w/EPO, Symantec Ghost, WSUS, IBM Tivoli Endpoint Manager, Microsoft System Center Ops Manager 2007 & 2012.

Employment History and Related Experience

Unisys Corporation, Systems Analyst, Harrisburg, PA 2008 – Present

Responsible for multiple government agencies at central PA Data Center. Responsible for troubleshooting systems, Active Directory, Patch Management, AntiVirus. Windows/VMware Team Lead responsible for maintaining ~800 Servers in the data center. Roles include:

- VMware Administrator of 350+ VMs (approx 50 ESX/ESXi hosts in 5 virtual centers, including Disaster Recovery site)
- Two site Active Directory & DNS Administrator
- Backup Administration including NetBackup, DataDomain, Avamar
- Scripting for server automation using mostly PowerShell, VBScript, & PowerCLI (VMware).
- Disaster Recovery testing multiple times annually
- Maintain Large 2 Instance SQL 2008 Cluster used for Multiple application management
- Maintain 3 DFS deployments
- Incident & Change Management control
- Technical Documentation using tools like Word & Visio
- BladeLogic Patch Management
- Systems Builds/Deploys
- Basic Linux administration support (SUSE & Redhat)
- Migrate, Update & maintain Windows 2000 Active Directory migration to Active Directory 2008 R2. Migrate COPA file share from single node 2003 file server to 2 node 2008 Distributed File Server with Replication (DFS & DFSR).
- Build Terminal Services & RemoteApp for central application control & updating for DPH Operations Staff.

UNISYS

Resource 26

Hyper V VMware Certified Administrator

- Migrate the DPH management infrastructure from hosts file management to fully integrated DNS including multi-site Active Directory replication & implement GLOBALNAMES zone as a replacement to WINS
- Established a one-way trust with CWOPA domain and internal management domain (ESM) to allow State employees single sign-on to DPH resources managed by Unisys such as performance metrics, or backup reporting, etc.
- Built/assist with managing DPH Shared VMware virtual Infrastructure (8 host cluster & virtual center)
- Built/manage IES Virtual VMware Infrastructure (28 host 2 Blade Center cluster, and 4 hosts in 2 other clusters & Virtual Center)
- Migrate 70+ Physical servers from IES data center to DPH data center as Virtual using Avamar backup & restore
- VM Convert many physical servers to virtual once servers come end of life
- Installed or assisted installs and upgrade EMC Avamar 5.x & 6.x & EMC DataDomain systems
- Built or upgraded multiple Symantec NetBackup systems versions 5.1, 6.0, 6.5, 7.0, 7.1 & 7.5.
- Consolidate & upgrade DPH NetBackup infrastructure from 6 isolated backup environments to a large dynamic redundant Backup infrastructure allowing for faster backup & restore times, higher reliability & resiliency, and save costs by utilizing fewer tapes and backup servers, and network equipment.
- Perform multiple disaster recovery tests for PSP, DPW-CAPS, IES including
  - Physical Server to Virtual server restore
  - Bare Metal restore from NetBackup Tape & Avamar
  - VMware restores
  - Avamar restores
  - NetBackup Tape restores
  - DataDomain Oracle restores
  - MS SQL 2000, 2005, & 2008 restores
  - Windows 2003, & 2008 Cluster restores to a single nodes
- Written many VB & PowerShell scripts for use in Backup & restores, Server subnet IP changes, regular scheduled tasks, VMware tasks with PowerCLI, and software installations/tweaks

Business Information Group, Network Engineer, York, PA 2008 – 2008

Installed numerous servers including Windows 2003 & 2008, SBS 2003, SQL Server, VMware, and Terminal Server. Installed servers from HP, IBM, and Dell.

- Partially or Fully administered almost 30 AD domains during the contract (Users counts ranging from 10-200+)
- Multiple Small Office Setups & relocation.

UNISYS

Resource 26

Hyper V VMware Certified Administrator

Rite Aid Corporation, Field, Systems Administrator & Development, Harrisburg, PA 2004 – 2007

Support Servers (Both Windows NT4, 2000, 2003 & SCO5), Cisco Routers, Support PCs, Setup & Repair of HP and Lexmark Printers, Network wiring of 29 Rite Aid Pharmacy Stores

Education

- Fall 2000 - Spring 2002 Penn State University Hazleton, PA
- Associate Degree in Information Sciences & Technology
- Graduated May 2002 with Associate degree in Computer Networking.

Professional Certifications

- VMware VCP4 & VCP5
- Microsoft Windows 2008 MCITP:SA
- ITILv3

This page intentionally left blank.

UNISYS

INFO-MATRIX CORPORATION

Resource 27

Hyper-V VMWare Certified Administrator

Key Skills and Knowledge

- Commonwealth of PA – experience – multiple agencies
- VMware Certified Professional 4 (VCP4)
- Operations Center experience

Skills Summary

Technical Manager with notable success directing the delivery of a broad range of comprehensive Information Technology Services and Information Management initiatives while collaborating with clients, staff, and IT consultants in planning and implementing IT Services Solutions, with an emphasis on server virtualization and virtual infrastructure services.

Core Competencies: VMware vSphere 3.x/4.x/5.x, VMware Site Recovery Manager 4.x, Network and Systems Administration; Storage Area Network (SAN) implementation, deployment, and management; Regulatory and Policy Adherence; Data Integrity and Recovery; Research and Development; Risk Assessment; Cost and Impact Analysis.

Platforms: VMware vSphere 5.x, vSphere 4.x, and vSphere 3.x; VMware Site Recovery Manager 4.x; Microsoft Windows operating systems (95 to Server 2003 R2); IBM DS3200, IBM FastT600 (DS4300), NTDS (Naval Tactical Data Systems); J.O.T.S (Joint Operations Tactical System)

Services: Microsoft Windows Cluster and Network Load Balance Technologies.

Networking: TCP/IP (DHCP, WINS, DNS), Ethernet.

Tools: VMware vSphere Client, Microsoft Operations Manager, Microsoft SharePoint Portal Server 2003, Microsoft Project Server 2003, Microsoft Systems Management Server 2003, Microsoft Office Professional 2003 (including Infopath), IBM DS4300 Storage Manager 9.10 (FastT600), McAfee ePO (Enterprise Policy Orchestrator), CommVault Galaxy QuiNetix 6.1/Simpana 7, IBM Director 5.1, SurfControl 5.5, Reflex DiskNet Pro 4, Checkpoint NG FP-2/NGX Firewall, McAfee/Norton Virus Protection utilities, ArcServ2000 Advance Edition, Microsoft Biztalk Server 2004 (initial installation and setup), Microsoft SQL Server Reporting Services (initial installation and setup).

Employment History and Related Experience

Commonwealth of Pennsylvania, Harrisburg PA, August 2009 – Present

Office of Administration, Office of Information Technology,

Bureau of Infrastructure and Operations, Server Operations Division

Network Administrator 1

- Primarily responsible for managing and providing technical support for all servers located within the central data centers (Enterprise Data Center, PA State

Police Data Centers, and Disaster Recovery Site).

- Responsible for managing and upgrading VMWare environment, including daily management, troubleshooting, installing, configuring, and deploying hosts and virtual machines.
- Responsible for installing, deploying, and managing IBM Systems Director to monitor server hardware.
- Responsible for performing system and infrastructure maintenance in accordance with Commonwealth ITB-NET-015. Performing maintenance during non-business Commonwealth designated maintenance periods.
- Provide direction to Commonwealth agencies in identifying operational problems related to hardware components; software (both client and server level); network servers, network operating system software and related networking components such as hubs, routers, switches, etc.; and messaging system servers and software; and remedying these problems expeditiously to minimize lost of productivity.
- Performs other related duties as assigned, including those outlined in the Commonwealth's CoG (Continuity of Government) Plan when the plan is activated.

Commonwealth of Pennsylvania, July 2000 – August 2009

Department of State, Bureau of Management Information Systems

Harrisburg, PA.

Network Administrator 1

- Responsible for the implementation, deployment, and configuration the Department's mid-level disk storage system; Storage Area Network (SAN). Responsible for managing a complex distributed network of Microsoft Windows Server 2003 supporting the SAN, web server farm, Network File Shares, and a business process management system. Additional responsibilities include, but not limited to deployment assistance and modification of the Department's internal applications supported within the Storage Area Network (SAN) infrastructures.
- As directed, facilitate the planning, implementation and support of the LAN (Local Area Network) and client systems and other related peripherals. Recover and reconstruct client and server configurations due to system failures. Analyze systems activity trends for preventive maintenance procedures and prepare reports. Coordinate the installation of computer hardware and software for client-end users. Provide technical and administrative support for both bureau and departmental staff.
- Accountable for the planning, implementation, and deployment of the Department's IT security requirements. Principally responsible for managing a multifaceted IT security solution with the implementation SurfControl Webfilter, DisknetPro Desktop, McAfee ePO (Enterprise Policy Orchestrator), and the

Commonwealth's ESA (Enterprise Security Agent) security solution: Preventia SiteProtector. Additional security responsibilities include the essential point of contact for managing the Department's Check Point Firewall solution.

- Other responsibilities include analyzing systems activity trends for preventive maintenance procedures. Provide additional computer hardware and software assistance for client-end user support staff.

Commonwealth of Pennsylvania, November 1998 – July 2000

Department of General Services, Bureau of Management Information Systems

Harrisburg, PA.

Distributed Systems Specialist 1

- Coordinated the installation of computer hardware and software for client-end users. Provided technical and administrative support for network and electronic mail servers. Analyzed systems activity trends for preventive maintenance procedures and prepared reports. Recovered and reconstructed personal computer configurations due to system failures. Managed departmental systems and peripheral equipment inventory. Ensured that equipment warranty and software licensing were in compliance with applicable policies.
- Functioned as liaison between departmental information technology coordinators and the Technical Support Division.

Commonwealth of Pennsylvania, December 1996 – November 1998

Department of General Services, Bureau of Purchases, Harrisburg, PA.

Clerk Typist 3

- Responsible for the assignment and management of commodity codes for state contracts issued by the Department of General Services. Ensured contract information was accurately entered into the purchasing system.
- Functioned as information technology coordinator between the Bureau of Purchases and the Bureau of Management Information Services. Performed tier 1 technical support for the Bureau of Purchases' purchasing systems and processes. Supported the Information Technology Contract tracking system.
- Contributed technical and administrative support to the development of the Summary Documents for the Procurement Reform Initiative presented to Commonwealth Executives as a Procurement Reform Initiative RFI Committee Member.

Pennsylvania High Education Assistance Agency, June 1995 – November 1996

Student Loan Servicing Center, Harrisburg, PA.

Customer Services Representative/Research Specialist

- Responsible for the research of financial discrepancies of assigned client accounts. Completed coding and research for manual payment of client accounts.
- Advised clients of repayment options, research and resolve account discrepancies via direct communications with client borrowers.

Cush Automotive Group, Inc., October 1993 to March 1995

Escondido, CA.

Accounts Specialist

- Responsible for the Collection, verification and deposit of revenue for the Sales, Parts and Service, and Finance Departments. Ensured the appropriated ledgers and accounts are properly and accurately credited and/or debited daily. Prepared monthly accounting reports for corporate comptroller and auditors. Responsible for accuracy of the acquisition of vehicles for the Cush and Mike Smith Honda Motors Division.
- Functioned as assistant to Finance Director and Managers and resolved client disputes as Customer Relation Manager.

U.S. Navy, September 1986 to October 1992

San Diego, CA.

Operations Specialist

(Combat Information Center Supervisor/Watch Officer).

- Supervised a team of one hundred personnel during various warfare conditions. Controlled fighter aircraft utilizing various computer and telecommunications systems as a Junior Air Intercept Controller. In addition to providing warfare tactical analysis assistance and weapons planning, assigned as one of four Search and Rescue Specialists and Communications and Navigation Specialists.
- As Information Systems Manager, managed the Joint Operational Tactical Systems Database. Responsible for the collection, evaluation and dissemination of intelligence data and ensured the proper enforcement of the security of sensitive information.
- As a Data Systems Supervisor, trained and supervised subordinate personnel using the Naval Tactical Data System. Enforced Department of Defense automated communications systems and publications security policies.
- As the Operations Department Administrative Assistant, managed departmental and public correspondence, office information systems and provided technical support to various command centers throughout the U.S. Navy Pacific Surface

INFO-MATRIX CORPORATION

Resource 27

Hyper-V VMWare Certified Administrator

Ships Fleet

Education

- Harrisburg Area Community College and Pennsylvania State University, 1998 – Present
- University of Pittsburgh, 1984 – 1986

Certifications

- VMware Certified Professional 4 (VCP4)

This page intentionally left blank.

Linux Administrator

This page intentionally left blank.

UNISYS

Resource 28

Linux Administrator

Key Skills and Knowledge

Databases

- MS SQL, Oracle, and DB2

Hardware

- IBM server hardware
- Dell server hardware

Operating Systems

- Microsoft Windows: NT 4, 2000, XP, 2003, 7, and 2008
- Linux: SuSE 10 & 11; Red Hat 5 & 6

Programming Languages & Tools

- DOS scripting, PowerShell, VB Script, C, C++, and HMTL

Call Center and Help Desk

- Remedy

Office Productivity Tools

- Microsoft Word, Excel, and Outlook

Facilities Management

- UPS monitoring and design

Professional Summary

Strong experience in systems administration and network management with a facility for learning and implementing unfamiliar technologies to attain customer-required outcomes.

- 12 years of implementing Web applications using Microsoft IIS as the Web and application server
- 12 years of deploying Microsoft Windows on authentication, file, and application servers
- 5 years installating, configuring, and deploying applications using of IBM WebSphere Application Server (WAS)
- 5 years of installing and configuring of Linux users and services, including Samaba, SSH, and BIND
- 4 years of installing and configuring VMware and ESC; as well as hosting of virtual infrastructure for a lab environment
- 2 years of installing and configuring of WebSphere MQ Server to support application communication across multiple platforms and architectures.

Employment History and Related Experience

Elite Systems, Commonwealth of Pennsylvania, Office of Administration, Integration Consultant — 2010 – Present

Supported application deployments for the Commonwealth of Pennsylvania; coordinated and implemented the upgrade of WebSphere MQ from version 5 to version 7 for multiple Commonwealth agencies to access an enterprise SAP environment.

- Review, create, and update documentation used to deploy and support agency applications hosted at the Commonwealth's Enterprise Data Center.
- Evaluate agency requested changes against industry best practices and Commonwealth security standards.
- Coordinate change management processes among multiple Commonwealth enterprise teams to complete application deployments for Commonwealth agencies.
- Manage DNS servers hosting Microsoft Windows DNS and associated DNS records.
- Patch and troubleshoot Linux servers running SuSE and Red Hat distributions.

UNISYS

Resource 28

Linux Administrator

TEKSystems/MindTeck, Pennsylvania Department of Transportation (PennDOT), Network Engineer 2004 – 2009

Provided 24/7 support of numerous applications hosted at the PennDOT server farm for various bureaus in the department; monitored, and maintained APC UPS infrastructure.

- Deployed WebSphere Application Server infrastructure to support migration of PennDOT applications from Lotus Domino-based architecture to Java architecture.
- Deployed IBM DB2 Connect server and DB2 client software upgrades to support access to IBM mainframe-hosted DB2 database instances hosted on z/operating system.

Additional Employment History

Innovative Business Concepts	2004 – 2004
GEF Computers	2002 – 2004
New Horizons	2000 – 2003
Computer Renaissance	1998 – 2000

Education

- High school diploma, Sauquiot Valley High School 1993
- Courses at Clarkson University, 1995

Professional Certifications

- CompTIA A+, May 1999, COMP10157635
- Microsoft Certified Professional, Microsoft, March 2000, MCP ID#1789557
- Microsoft Certified Systems Administrator Microsoft, August 2004, MCP ID#1789557
- Microsoft Certified Systems Engineer, Microsoft, August 2004, MCP ID#1789557

Professional Development

- ITIL v3 Foundation training, Framework that allows for continuous improvement of the documentation, customer service, and change control processes of an IT organization, 2012
- SiteMinder 12.5 training, Access management for Websites using LDAP and Active Directory security, 2012

UNISYS

INFO-MATRIX CORPORATION

Resource 29

Linux Administrator

Key Skills and Knowledge

- Certified systems administrator
- Data Center administrator
- Server Operating Systems: Windows Server NT through 2008, Linux, VAX/VMS, AS/400
- Desktop Operating Systems: Win95 through Win7, Linux, Mac OSX
- Microsoft Exchange 2000 through 2010, Kerio, DeskNow, Lotus Notes, Hosted Exchange Services, BlackBerry Enterprise Server
- Web Servers: IIS 6 & 7, CPanel, ispCP, Apache
- Spam Filtering: Barracuda Spam Filter appliances, GFI Max Mail, Postini
- Networking Appliances: Fortinet firewalls, FortiAnalyzer, FortiManager, SonicWall firewalls, Netgear & Cisco Managed Switches, Ecessa WAN Aggregators, PepLink Load Balancers
- Networking Protocols & Services: TCP/IP, DNS, DHCP, SSH, Telnet, SMTP, POP, HTTP, HTTPS, FTP, SCP, IMAP, SSL Certificates
- Microsoft Products: Office 97 through 2010, SharePoint, SQL 2005 & 2008
- Backup Solutions: Symantec, Acronis, Ahsay, Replay, DoubleTake, iBackup
- Terminal Servers: MS Terminal Server, Citrix MetaFrame, Citrix XenDesktop, Citrix XenApp
- Virtualization Solutions: MS HyperV, VMware
- VoIP: Televantage Server
- Hardware: HP and Dell servers and desktops, HP Printers, Barracuda SSL VPN, Barracuda WebFilter, Barracuda Message Archiver, FortiMail, Barracuda Backup, Synology NAS, Buffalo NAS, Netgear NAS, All Smartphone platforms

Professional Summary

Skilled certified administer with 15 years experience.

- Server Operating Systems: Windows Server NT through 2008, Linux, VAX/VMS, AS/400
- Desktop Operating Systems: Win95 through Win7, Linux, Mac OSX
- E-mail Servers: Microsoft Exchange 2000 through 2010, Kerio, DeskNow, Lotus Notes, Hosted Exchange Services, BlackBerry Enterprise Server
- Web Servers: IIS 6 & 7, CPanel, ispCP, Apache
- Spam Filtering: Barracuda Spam Filter appliances, GFI Max Mail, Postini
- Networking Appliances: Fortinet firewalls, FortiAnalyzer, FortiManager, SonicWall firewalls, Netgear & Cisco Managed Switches, Ecessa WAN Aggregators, PepLink Load Balancers
- Networking Protocols & Services: TCP/IP, DNS, DHCP, SSH, Telnet, SMTP, POP, HTTP, HTTPS, FTP, SCP, IMAP, SSL Certificates
- Microsoft Products: Office 97 through 2010, SharePoint, SQL 2005 & 2008
- Backup Solutions: Symantec, Acronis, Ahsay, Replay, DoubleTake, iBackup
- Terminal Servers: MS Terminal Server, Citrix MetaFrame, Citrix XenDesktop, Citrix XenApp
- Virtualization Solutions: MS HyperV, VMware
- VoIP: Televantage Server
- Hardware: HP and Dell servers and desktops, HP Printers, Barracuda SSL VPN, Barracuda WebFilter, Barracuda Message Archiver, FortiMail, Barracuda Backup, Synology NAS, Buffalo NAS, Netgear NAS, All Smartphone platforms
- Data Center Equipment: Various types of server racks and patch panels, APC UPS, Liebert PDU, Liebert Cooling, NetBotz monitoring appliances

Employment History and Related Experience

Choice Technologies Inc., Data Center Administrator,
Hunt Valley, MD 2006 – Present

Server and network administration providing hosted services as well as maintaining co-located servers. Create and manage client accounts on hosted Exchange services. Create and manage accounts on Egnyte cloud file server. Manage domains and SSL certificates via GoDaddy and GlobalSign.

- Responsible for configuring and maintaining Fortinet firewalls, PowerLink WAN aggregators, Barracuda spam and Web filters, Linux e-mail clusters, Linux DNS, Linux based Ahsay remote backup and replication servers, co-located Linux and MS 2003 and 2008 (32 and 64bit) servers, Exchange 2003 to 2010, BlackBerry Enterprise, Linux Web servers, Synology and

Buffalo NAS devices, Backup Exec server, GFI A/V server, Linux FTP and webDAV servers

- Create and manage accounts on GFI MaxMail spam filtering services.
- Provide support to field technicians and helpdesk in resolving issues at customer locations.
- Provide support to sales in recommending appropriate hardware and software solutions for customers.
- Maintain and create documentation.
- Perform training sessions to helpdesk and field technicians.
- Take great pride and effort in maintaining a high level of support and communication with customers, co-workers, and superiors.

Capital Blue Cross, Support Center Analyst,
Harrisburg, PA 2003 – 2006

Performed both phone and desktop support duties in a Win2000/XP environment, supported both internal and external customers on a broad range of applications, including Citrix based applications.

- Supported and maintained Dell hardware and all HP printers including the administration of a Web JetAdmin server.
- Performed system builds and software installs using Altiris.
- Assisted with projects such as VoIP, laptop and PDA encryption, and data destruction for privacy compliance.
- Responsible for various administrative duties on mainframe, Avaya audix voicemail, and Citrix Metaframe servers.

R.R. Donnelley and Sons, Lancaster, Financial
Application Support Specialist, PA 2001 – 2003

Supported multiple proprietary time-sensitive applications used by employees and clients.

- Performed global LAN/WAN monitoring and administration via HP OpenView. Provided Windows 2000, Novell, and VAX support and administration.
- Interfaced with applications developers and network engineers to solve issues.

D&E Networks Inc. (PennDOT), Windows Administrator,
Harrisburg, PA 2000 – 2001

Administered Windows NT and 2000 domains, performed SMS administration and provided SMS and general IT support to all PennDOT facilities, including district offices.

Resource 29

Linux Administrator

- Created, distributed, and maintained software packages and documentation.
- Performed Exchange 2000 and Active Directory administration and provided Tier 2 MS Office support.
- Performed both physical hardware installations of servers, as well as performing server operating system installs and RAID configurations.

R.R. Donnelley and Sons, Financial Application Support Specialist, Lancaster, PA 2000 – 2000

Supported multiple proprietary applications used by employees and clients.

- Performed VAX/VMS administration and support. Performed LAN/WAN monitoring and administration.
- Interfaced with applications developers and network engineers to solve issues.

Harley-Davidson Motor Co., IT Help Desk Specialist, York, PA 1998 – 2000

Provided desktop support to end-users, performed PC imaging and roll-outs.

- Maintained hardware inventories via a database that I developed.
- Performed AS/400 administration and support.
- Created and maintained documentation and reports.

Education

- York College of Pennyslvania, Dec 1999
- Bachelor of Science in Information Systems

Certifications

- Fortinet and Citrix

This page intentionally left blank.

UNISYS

IBM

Resource 30

Linux Administrator

Key Skills and Knowledge

Platforms

- Linux (CentOS, Red Hat, OpenStack, Debian)
- VMware vSphere ESX/ESXi 4.1/5.0
- Citrix XenServer 5
- Amazon EC2/Rackspace Cloud Technologies
- Microsoft Windows Desktop/Server Families from 95 to 2000/2003/2008 including basic Hyper-V

Networking

- Extensive understanding of Design
- Implementation, and troubleshooting of LAN/WAN/SAN/VoIP/Wi-Fi Technologies such as VPN/SSL, NFS/CIFS, iSCSI/FCoE

Storage

- NetApp/ONTAP
- Dell PowerVault and Equal Logic
- Compellent
- EMC
- OpenFiler

Languages

- UNIX Shell Scripting
- Perl
- PHP
- Python
- Javascript/JQuery
- HTML
- Puppet/Chef/Crowbar
- Hadoop
- Unicenter
- Heat
- Microsoft Exchange 2000/2003
- Exim
- Postfix
- Sendmail
- Cisco IOS

Professional Summary

Over 10 years of Linux server administration, 5 years of Windows Client/Server administration, and 3 years of virtualization experience in enterprise environments such as; healthcare and Military data centers; supported clients through telephone, helpdesk/e-mail including analysis and escalations.

- Strong understanding of Linux Web, Database, DNS, and SMTP services; Many hypervisor and guest operating systems interactions, particularly in P2V situations.
- System and Network Intrusion Prevention and Detection; DdoS Mitigation; Cisco Catalyst, PIX and ASA Firewalls; OpenLDAP/Microsoft Windows Servers (Active Directory, Exchange); Server/Client Based Anti-virus, Spyware, and E-mail Clients
- IP Telephony Systems; Rapid Server/Desktop Deployment, Updates, Restoration, and Imaging.

Employment History and Related Experience

Dell, Enterprise High Complexity Senior-Level Systems Analyst, Oklahoma City, OK — 2010 – 2012

- Provided enterprise level systems analysis for Dell operating systems and applications.
- Promoted to senior-level high complexity analyst by self-studying and quickly obtaining required certifications
- Voluntarily worked many hours of overtime to provide primary PM Support in North America for all alternate operating system and applications issues ranging from drive replacements to mission-critical recovery assistance of virtualized environments
- #8 YTD in Analyst monthly measurements gauging highest-productivity and fastest-resolutions

HostGator.COM, Linux/Windows System Administrator, Houston, TX — 2011 – 2012

Provided Linux administration assistance and customer support via helpd esk and telephone for a very large Web hosting company with 30,000 customers serviced by over 500 Linux and Windows Servers.

- Monitor server and network utilization and performance in real time through various software such as; Nagios/MOM in a team of administrators to ensure quality of service
- Support internal level 1 technicians and representatives while consecutively working in a team to resolve complex, mixed operating system environment application issues for customers

UNISYS

IBM

Resource 30

Linux Administrator

- Call manager and Unity
- Juniper operating system
- Bind 4/9
- Cpanel/WHM
- Plesk
- NginX/Apache 1.3x/2.0
- MySQL 4x/5x
- ProFTPD
- ISS 6/7
- MS SQL 2000/2003
- Cron
- Symantec Enterprise Anti-Virus
- Backup Exec, and Ghost
- Dell OpenManage
- HP OpenView
- SNMP
- Whats Up!
- Nagios
- Cacti
- Snort
- Nmap
- Network Flight Recorder
- IBM Tivoli
- Lotus Notes
- Microsoft Office System

- Installation, configuration, and maintenance of Linux/Windows services such as Apache, MySQL, Exim; and IIS, MS SQL, FTP
- Perform simultaneous server imaging, roll-outs, and back up procedures daily in a high paced, rapidly changing environment.

Advanced Systems Technology, Inc., Network Administrator, Lawton, OK 2006 – 2007

- Recruited to reconstruct and administer Linux/Windows servers, improve bandwidth usage, create performance metrics; analyze complex network and server issues with remote Administrators, troubleshoot simple day-to-day end user problems of over 400 employees in local and remote offices.
- Complete, seamless migration of 400+ users in three locations from separate Linux-based MTA's to a single, redundant Exchange 2003 with Linux Gateway's for Anti-Virus and Spam
- Integrated corporate Web site with load balanced Windows and Linux Web servers after migrating from older technologies
- Remotely administered virtual environment consisting of Red Hat, CentOS Linux and Microsoft Windows 2003 servers through policy-based VPN tunnels in four different locations
- Created company policies and procedures governing corporate security, e-mail and Internet usage, access control, and incident response

McKesson Provider Technologies, Business Development, Lawton, OK 2003 – 2006

Part of a team of five System Administrators and five System Analysts to perform daily tasks required for supporting an enterprise Hospital Network with more than 1,500 users, 150 servers, and 10 remote Clinics.

- Maintained 10 Linux Servers which provided security and services for other Windows machines on the network such as: DNS, NAT, Anti-Virus/Spam, and Firewall via iptables
- Managed backups for Windows, Linux, PACS, and File Servers to EMC Clarion SAN device
- Provisioned, audited, and administered; server logs, backups, and Active Directory objects including remote forests
- Researched and procured BlackBerry Enterprise Server. Assisted with migration from Juniper based core and wireless network to 100% Cisco-based

Education

- Macarthur High School, Lawton Oklahoma, 2003
- Great Plains Technology Center – Network Technology, Lawton, Oklahoma, 2004

UNISYS

IBM

Resource 30

Linux Administrator

Profession Certifications

- Red Hat Certified Engineer 6
- VMware Certified Professional 5.0 Senior-Level Linux Virtualization Professional (LPIC-3+4),
- Novel SuSE Certified Linux Professional
- Dell Certified Server Expert

This page intentionally left blank.

Resource 31

Linux Administrator

Key Skills and Knowledge

- Data Center operations
- Infrastructure Management
- Data security
- Skilled Linux Admin.
- Skilled in numerous technologies
- Windows: NT 4.0, 2000, 2003, 2008
- UNIX: Solaris, IRIX, HPUX, AIX
- Linux: Red Hat, Centos, Debian
- Windows Server platforms: HP, Dell, Compaq
- UNIX Server/Workstations: Solaris, SGI, IBM, HPUX
- NAS/SAN Platforms: Network Appliance, EMC, MTI, Andataco
- Windows Domain Applications: Exchange Server 2003 and 2007, SMS server
- Replication Server, Apache, Active Directory, DHCP, DNS, Wins
- Windows Server Applications: MS SQL, IIS, VM Ware, MS Virtual Server, Citrix
- MS SharePoint, MYSQL, Trend Micro AV server
- Networking: Cisco 5500 and 5600 switches, Cisco 2600 series routers
- Fault tolerant servers, Veritas Storage Foundation, Veritas NetBackup
- EMC NetWorker, NetVault
- Data Domain Disk to disk backup systems, Spectra Logic Tape libraries, Heat, Remedy, Samba, Perl, OnTap
- TCP/IP, NIS, CIFS, NFS, SSH, FTP, SFTP, CUPS, ghost, Acronis, VNC, Cygwin, Putty, Exceed, Nagios
- Brocade fiber switches, Emulex fiber cards
- Raid controllers, Octel Voice Mail systems and Nortel switches.

Professional Summary

IT Professional with 15 years of Infrastructure management, Operations Management, Data security and Data Center operations, Windows system integration, UNIX/Linux servers, storage systems and facility management. Strong leadership skills with data center operations, systems administration infrastructure, and technology project management.

Employment History and Related Experience

Web Entertainment Technologies, Infrastructure Manager, Oakland, NJ — 2009 – Present

Advise the CTO and COO on Data center operations in Oakland, NJ and Smithtown, NY. Focus on company infrastructure, Data center, and Web hosting operations. Maintain and support corporate infrastructure including cabling, hubs, routers, the LAN at each facility, the WAN between the two facilities and providing internal support as needed.

- Deliver data centers operations for storage and backup, server maintenance and configuration, applications and new product offerings and level 3 customer support issues
- Coordinate and negotiate with vendors for hardware, software and communications services
- Maintained an Apache server farm consisting of Red Hat Enterprise 4/5 servers
- Managed file systems and security access in addition to backing up the servers
- Managed the BIND DNS server with upgrades, additions, deletions as needed
- Maintained Linux systems operating system and software with RPM/YUM when available or compile from source code as needed for required software
- Created CRON jobs as required to automate systems tasks
- Managed file system access via NFS shares and permissions and SAMBA SMB shares as required
- Installed and configured Apache Web servers
- Installed and configured MYSQL server

Electronics for Imaging, Site Infrastructure Manager Parsippany, NJ — 1998 – 2008

Administrator responsible for the IT infrastructure in the EFI New Jersey facility consisting of Windows AD and NIS domains with multiple Windows and UNIX/Linux servers and storage systems.

Resource 31

Linux Administrator

- Deliver systems administration of all components of the infrastructure encompassing Windows AD services administration, Systems Engineering, Infrastructure Management, Storage Management, Backup Administration, Windows and UNIX Server Administration.
- Engineered and administered multiple Windows and UNIX/Linux servers in addition to AD administration and management.
- Administered several generations of Microsoft servers from NT 4.0 to 2008 with services such as Active Directory, DNS, DHCP, WINS, File and Print services, Exchange, IIS and MYSQL
- Project lead to standardize and document Remote site facility configurations and best practices for facility management standards within the EFI Remote sites and documenting on a SharePoint server
- Ensured capacity in the New Jersey facility on all network components and developed a hardware refresh plan for the facility systems to ensure systems availability and to keep pace with user needs.
- Administered file systems on several SAN's from various vendors and several Network Appliance (NAS) filers via CIFS, NFS and Veritas Volume Manager.
- Managed the backup architecture on several vendor products starting with Networker running under Solaris and a locally attached Sun tape library
- Migrated through several Enterprise backup solutions and hardware platforms most recently on a Veritas/Symantec NetBackup backup architecture running disk-to-disk to a Data Domain and offline to a Spectra logic tape library.
- Systems administrator on several generations of Solaris, Linux, AIX, IRIX, Red Hat and HPUX servers
- Provided engineering support for product development efforts by engineering teams to include desktop support, server support, Clear Case system and networking
- Supported engineering groups in automating software releases within the intranet by designed and implemented a Microsoft IIS server with an MS SQL system backend to track bug reports and daily build histories and distribute drivers and interpreters to the corporate units via the corporate intranet.
- Upgraded the system to more capable platform running Red Hat, Apache and MySQL
- Performed all SMS administration activities including installing, configuring, upgrading, creating collections and managed software updates for all Applications servers.
- Performed all installation, maintenance and support functions on telephone system, fax and printers within the facility
- Created and maintained systems images on Ghost and Acronis for rapid cloning of developers' workstations.
- Administered several generations of Microsoft Exchange server
- Installed, configured and, maintained all storage hardware consisting of multiple NAS and SAN systems serving Windows and UNIX systems.

- Built and administered multiple Red Hat Linux Enterprise servers used by the developers for their Clear Case version control system.

Air Express International, NT Administrator (Contract),
Darien, CT 1998

Responsible for migration of server platforms from Novell to a Windows NT based architecture. The project consisted of building, configuring and testing servers.

- Designed the domain security model to meet corporate requirements.
- Designed and implemented the backup strategy and procedures documentation for domain servers.
- Managed the migration of users from Novell to Window servers.
- Developed the disaster recovery procedures for the enterprise.

NBC Production Systems, Operations Specialist/Project Manager, New York, NY 1988 – 1997

Primary duties consisted of supporting data center operations, maintenance and upgrading the core components of the News division's data center and managed multiple high profile News Division remote operations nationally and internationally.

- Provided data communication, software and hardware support for the News division global network.
- Managed vendors and contract staff in migrating and upgrading of core systems.
- Manager on-site operations of computer and communication resources for live NBC News events throughout the world.
- Setup the news bureau in Dhahran Saudi Arabia that was the hub for NBC news computer operations for Desert Shield and Desert Storm.
- Supported the interim daily operations on the CNBC Asia systems in Hong Kong and trained a local hire for local support.
- Setup the facilities (network and software systems) for the translation system by Guangzhou TV from Cantonese to Mandarin.
- Trained CNBC Asia system administrators in daily operations, networking hardware and NBC systems and procedures.

Education

Montclair State University
BS, Computer Science, Minor in Mathematics

Bergen Community College
Associate of Applied Science, Data Processing

This page intentionally left blank.

UNISYS

e&e IT Consulting Services, Inc.

Resource 32

Linux Administrator

Key Skills and Knowledge

- Linux Team Lead
- Set up and maintenance of Linux and Windows servers
- Task automation and trouble ticketing with use of Linux apps
- Build and administered servers and tools for task automation
- Ttrouble ticketing and documentation
- Linux, AIX, PHP, MYSQL
- Open source applications
- Maintained Debian Linux servers.
- Plan and manage all IT projects
- Maintenance and upgrades of existing systems
- implementing new technologies
- Research and purchase network components
- Support IT budget process.

Professional Summary

15 years of systems administration experience delivering Linux systems, coordinating data and voice network communications. Outstanding planning and management skills for maintenance and upgrades of existing systems and implementing new technologies

- Created and implemented nationwide internal Network Operations Center processes and procedures.
- Identified inefficient policies and repaired or replaced them to accommodate rapidly expanding demand and new systems.
- Instrumental in the design, build and then supervision of a world class operation that installs casino management systems in all of Pennsylvania's new casinos and collects all financial data in a central control system for revenue and tax purposes.
- Accomplish setup and maintenance of Windows, Linux and HP-UX servers
- Develop scripts and automate procedures for back-up, data mining and other server related tasks
- Install and configure tools for server/network uptime and performance monitoring such as Nagios, MRTG, Munin, Ntop and others
- Resolve communications issues for a twelve office/300 employee MPLS/VoIP network

Employment History and Related Experience

AAA Central Penn, IT Manager 2008 – Present

Coordinate all data and voice network communications. Plan and manage all IT projects including maintenance and upgrades of existing systems and implementing new technologies, Research and purchase everything IT related, assist with the IT budget process.

- Provide training for IT employees and end users
- Handle salary and performance reviews for IT staff. Responsible for day to day IT operations
- Create IT policies and procedures. Communicate with other business lines, assessing needs and recommending solution
- Accomplish setup and maintenance of Windows, Linux and HP-UX servers
- Develop scripts and automate procedures for back-up, data mining and other server related tasks
- Install and configure tools for server/network uptime and performance monitoring such as Nagios, MRTG, Munin, Ntop and others
- Resolve communications issues for a twelve office/300 employee MPLS/VoIP network

e&e IT Consulting Services, Inc.

Resource 32

Linux Administrator

Gtech Corporation, Technology Section Supervisor 2006 – 2008

Instrumental in the design, build and then supervision of a world class operation that installs casino management systems in all of Pennsylvania's new casinos and collects all financial data in a central control system for revenue and tax purposes.

- Selected, interviewed and hired the entire operations staff. Provide staff training, motivation and performance evaluation.
- Build and administered servers and tools for task automation, trouble ticketing and documentation using Linux, AIX, PHP, MYSQL and several open source applications
- Maintained 60+ Debian Linux servers.
- Develop process and procedures for all operations planned and unplanned events, daily operational procedures, postmortem procedures, notification procedures, service level agreements
- Project team leader for annual SAS 70 audits

EDS - Sun Microsystems Project, Team Leader Linux/Solaris Support, 2005 – 2006

Linux Team Leader and Tier 2 Technical Support Engineer for Sun Microsystems supporting Solaris/UNIX and Linux.

- Supported private industry as well as all government contracts including DOD, NASA, & FBI
- Provided guidance and technical expertise to system administrators to diagnose and resolve hardware, operating system, networking and storage problems.

FeatherweightLinux.org, Owner Operator 2003 – 2005

Created, developed, maintained, marketed and sold a custom Linux distribution. Featherweight Linux was a live-CD/installable distribution which was built on Debian Linux using Knoppix technology.

- Supported Editor in Chief of Linux World Magazine and EVP of Marketing for EMU Software
- Created and maintain a boot-able demo CD for EMU Software's NetDirector server management software.

Network Operations Center (NOC) – EarthLink, Senior Project Manager 2001 – 2003

Created and implemented nationwide internal Network Operations Center processes and procedures. Identified inefficient policies and repaired or replaced

them to accommodate rapidly expanding demand and new systems.

- Liaison with other departments and with external partners and vendors on all NOC related company projects to determine and communicate project requirements, resolutions and priorities
- Trained the NOC management staff and tracked performance of all departmental managers and supervisors

Network Operations Center - EarthLink, Site Manager 2000 – 2001

Site Manager, responsible for all facilities related issues and administrative oversight for the department.

Assisted Senior Managers in creating policies and procedures and implemented those policies and procedures

- Accomplished team building, people & resources scheduling and insured that training was useful and timely
- Addressed salary and performance reviews and owned the role of employee advocate for Techs/Engineers, worked with NOC Systems for delivery of tools needed by Tech/Engineers.

MindSpring/EarthLink, Bridge Supervisor and Training Coordinator 1998 – 2000

Supported division of technical support, was instrumental in creating, to perform first level network troubleshooting and alerting, and act as a communications bridge between network operations and technical support.

- Accomplished salary and performance reviews, people & resources scheduling, was responsible for managing team spirit, personnel issues, and overall team function
- Resolved escalations beyond normal means, worked with other departments to ensure tools were working properly and made sure issues were being resolved in a timely manner
- Traveled to our call centers nationwide providing first level network troubleshooting training to our technical support staff. This division ultimately became the nerve center for network monitoring and front line troubleshooting for the Network Operations Center, employing a group of about 15 people.

MindSpring/EarthLink, Team Manager – Tech Support 1998 –1998

Provided support, training and supervision to a team of 12-15 support representatives, assisted representatives with technical and customer issues, maintained overall performance of my team and ensured each member of my team

e&e IT Consulting Services, Inc.

Resource 32

Linux Administrator

Education

- Computer Learning Network
- Diploma, Computer Systems Technology, 1993 - 1994

UNISYS

[redacted]

Linux Administrator

Key Skills and Knowledge

- Hardware Upgrade and Repair
- Linux - RHEL, SLES, OEL
- RHEL 5.X Server Builds from Scratch
- RHEL 6 Support
- RHEL 6 Server Builds from Scratch
- RHN Satellite Implementation
- AIX – 4,5,6,7
- PowerVM – Power5, Power6, Power7
- PowerHA – 5,6,7
- Project and Program Management
- Communication and Networking
- Databases
- Hardware
- Operating Systems
- Software/System Architecture
- Technical Documentation
- Systems Development Life Cycle
- ITIL/ITSM
- Korn/Bash Shell Scripting
- UCMS – Unemployment Compensation Management System
- SWIF – State Workers Insurance Fund
- BWC – Bureau of Workers Compensation
- Avamar
- NetBackup
- BladeLogic

Professional Summary

Manages operations of AIX and Linux systems in the Data PowerHouse data center for the Commonwealth. This included server deployments through various processes, PowerHA configuration, user requests, operating system level migrations and patching. This also includes management of VIO servers, HMCs and VMware Virtual Center as it pertains to VM Linux systems.

- Managed BladeLogic repository for Linux patching across various Linux platforms including RHEL, SLES, and OEL
- Developed scripts as needed to maintain a consistent environment across the entire data center.
- Participate in all Disaster Recovery planning and testing.
- Gathering customer requirements for recovery of various application and database servers
- Developing the best recovery method of rootvg and non-rootvg as well as customer data
- Execute recovery exercises and ensured consistent support to the customer as they proceed with their testing of the recovered systems.

Employment History and Related Experience

Unisys Corporation, Commonwealth of Pennsylvania, Data PowerHouse Project, Harrisburg, PA — 2011 – Present

UNIX Administrator responsible for the management and maintenance of all AIX and Linux servers. Active ITIL v3 certification, Participant in successful disaster recovery testing.

Department of Labor and Industry – DLI Project

- Unemployment Compensation Management System (UCMS) – Integral part of the System Administration refresh team for AIX support. Built the new operating system image on the updated platforms, worked with IBM experts on performance tuning, ground up installation of all IBM Power hardware including SAN and Network cable installation (Ethernet and fiber), frame mapping of physical devices to ensure redundancy, stability, and performance, of the systems. Worked with IBM experts on installing the most advanced VIO servers built for solid redundancy (tested and confirmed) as well as PowerHA clusters that would ensure the application and files were available with the least amount of downtime for a smooth transition. Worked with the various business partners: DBAs, Application Developers, Network, SAN/TSM, Windows Administrators for performance testing, process flow, etc.
- Tivoli Monitoring/Network Support – These two particular groups of business partners wanted to dive into RedHat Enterprise Linux servers as the

UNISYS

[redacted]

Linux Administrator

hosting operating system for their applications. Worked exclusively on building a solid RHEL 5.X image that would meet/exceed the application requirements for virtualization, security, and stability. The systems were primarily Virtual Machines (VM) however there were a few that ran on Intel X86 physical servers.

- RedHat Network Satellite (RHN Satellite) – As part of a growing RHEL environment it was critical to develop and maintain a central management point. An investment was made in the RHN Satellite product for patching and maintaining a base line platform for any RHEL system. As part of the install team, I set up the central satellite server, setup the database and register/connected all clients to their appropriate patching cycle. Working with the owners of the various RHEL clients, we established the most effective patching cycle for their systems and ensured all systems were current and met the standards needed as set forth by OA.
- BWC – Bureau of Workers Compensation – Directly involved in upgrade field office servers from AIX 5.3 to AIX 6.1, PowerHA to the most current supported levels in PowerHA 6.1, and worked with the extended AIX support team to execute the disaster recovery plan when an upgrade did not go as planned. This involved restoring the server image from a sysback image on tape.
- SWIF – State Workers Insurance Fund – Deeply involved in supporting their PowerHA systems were solid and the customer had a level of confidence in the failover of the clusters. Solely supported the installation and upgrade maintenance of Dollar Universe application. Although there was an application team dedicated to the day to day work of Dollar U, the team did not have the AIX experience and administrator access needed to perform much of their work.

Integrated Enterprise System – IES Project

- AIX 5.3 to AIX 7.1 migration – Developed the migration plan needed to move from AIX 5.3 to AIX 7.1 to ensure the least amount of down time possible for the customer. Alt-disk install was the method chosen. I was responsible for scheduling all of the systems in various maintenance windows to ensure accurate time for testing and meeting the requirement for a phased approach of implementation.
- Device Driver upgrade – to ensure accurate connections to Avamar, the backup solution for IES, worked with the application team to upgrade the driver packages.
- Streamlined mksysb implementation – The system mksysb process was antiquated at best. Based on past experience and the need for an extra layer of protection, a new mksysb creation/storage process was created to ensure redundancy of the backup images and to further enhance the availability of these images for Disaster Recovery.

UNISYS

[redacted]

Linux Administrator

- Disaster Recovery Testing – Yearly disaster recovery testing is done to ensure the application's availability should a disaster occur. As part of the DR team, I worked extreme hours to build, restore and configure 30+ AIX LPARs to meet the current production environment as well as worked with the customer to correct minor issues during their database restores and testing process.

Department of Revenue – DOR Project

- AIX 5.3 to AIX 7.1 migration – Developed the migration plan needed to move from AIX 5.3 to AIX 7.1 to ensure the least amount of down time possible for the customer. Alt-disk install was the method chosen. I was responsible for scheduling all of the systems in various maintenance windows to ensure accurate time for testing and meeting the requirement for a phased approach of implementation.
- Device Driver upgrade – to ensure accurate connections to Avamar, the backup solution for IES, worked with the application team to upgrade the driver packages.
- Streamlined mksysb implementation – The system mksysb process was antiquated at best. Based on past experience and the need for an extra layer of protection, a new mksysb creation/storage process was created to ensure redundancy of the backup images and to further enhance the availability of these images for Disaster Recovery.
- Disaster Recovery Testing – Yearly disaster recovery testing is done to ensure the application's availability should a disaster occur. As part of the DR team, I worked extreme hours to build, restore and configure 30+ AIX LPARs to meet the current production environment as well as worked with the customer to correct minor issues during their database restores and testing process.

Pennsylvania Liquor Control Board – PLCB Project

- Integrated Business Management System (IBMS) Project – The agency was refreshing their application and took the opportunity to change operating systems in the process. RedHat Enterprise Linux (RHEL) was chosen as the platform. My role in the project has been to develop a stable 5.X RHEL operating system image and deploy servers to the agency as needed based on the given build requirements. These systems are all Virtual Machines (VM) and maintain the required level of security, with room to grow as the environment changes.
- BladeLogic - The current patching option for the RHEL systems is BladeLogic. I have developed the needed channels to connect the servers to

UNISYS

[redacted]

Linux Administrator

the appropriate patches based on operating system level. Patch cycles are being established based on environment level (UAT, PRD) to ensure testing between cycles and make sure production stability.

Department of Environmental Projection – DEP Project

- Oracle Enterprise Linux – OEL – This environment is comprised of approximately five Oracle Enterprise Linux (OEL) systems with the opportunity for expansion. The environment was a migration from Solaris to Linux and we continue to support this environment on a day to day business as they work through the growing pains of supporting their application(s) on a new operating system. Day to day work includes file system expansion, security monitoring and tuning, and storage and performance monitoring.

Additional Employment History

Commonwealth of Pennsylvania, Department of Labor and Industry	2009 – 2011
Foot Locker, Inc.	2004 – 2009
York Technical Institute	2002 – 2004

Education

Central Pennsylvania College Network Management and Cyber Security
Summerdale, Pennsylvania, July 2005 – Fall 2008
Bachelors of Science, Graduation date: December 2008
Dean's List Each Semester in Attendance Final GPA: 3.88

York Technical Institute Computer Systems Specialist
York, Pennsylvania, July 2002 – May 2004
Associate in Specialized Business Graduation date: May 2004
Student of the Term: Fall Term GPA: 3.75

Professional Certification

- CompTIA Net+ Certification, 2003
- ITIL v3 Foundation, 2012
- IBM AIX Certified System Administrator – AIX 7.1, 2012

UNISYS

IBM

Resource 34

Linux Administrator

Key Skills and Knowledge

Operating System

- Linux
- AIX
- Z/operating system
- Solaris
- Windows
- operating system/2
- Dos

Languages

- Shell Scripting
- Perl
- Java
- PHP
- Assembler
- Cobol
- Rexx
- HTML
- XML

HPC:

- xCAT
- LSF
- Torque/Maui
- SGE

Databases

- Oracle 8i -10g
- DB2/UDB. Mysql

Applications/Middleware

- WebSphere Application Server 1.x-6
- Tomcat
- Apache
- Jboss
- Eclipse
- Samba Bind
- Open office
- Microsoft Office

LDAP

- Openldap
- Tivoli Directory

Professional Summary

Senior-level IT specialist and information technology expert with an established track record in providing mission critical, enterprise level infrastructure and application architectures. A passion for delivering efficient, cost effective solutions to complex business and application requirements, utilizing best of breed commercial and open source software and solutions. Expert at problem determination, performance analysis, and tuning. Extensive experience in designing and implementing solutions requiring integration of multiple platforms, operating systems, network topologies, and applications in both business application and high performance computing environments.

Employment History and Related Experience

IBM, Sr. IT Specialist, Linux Architect, Hartford, CT 2005 – Present

Supported a major credit card company on a series of engagements; initially provided staff augmentation and identification and documentation of acquired systems; provided assistance with data center relocation and implementing previously recommended architectural changes and best practices.

- Designed, installed and supported large SoFS and SoNAS Linux based storage implementations (Samba/CIFS, NFS, GPFS) using either LDAP/NIS or Active Directory for authentication. Designed and implemented Kerberos/NFS solution to satisfy customer requirements.
- Led customer team in testing, collecting and analyzing system performance and customer application benchmark data for high availability Oracle database on Linux. Recommended solutions to resolve identified system bottlenecks to meet critical business capacity and performance requirements.
- Identified and recommended remediation to resolve performance issues in a customer's strategic Java application, allowing for on-time implementation of the application.
- Installed, and provided customer education and support of Linux and Bladecenter hardware for several New England Universities and Colleges. Implemented boot from SAN configurations to provide maximum flexibility and recovery capabilities for the customers.
- Provided onsite subject matter expertise for Linux and Bladecenter hardware, firmware and software support for a major pharmaceutical company. Developed custom single pass firmware upgrade facility to meet customer requirements.
- Developed, implemented and supported HPC environments for several major pharmaceutical companies utilizing both local and cloud based computer resources as well as high density SMP nodes (96-128 cores). Installed and integrated various scheduling systems including Platform LSF, Sun Grid Engine as well as Torque/Maui.

Resource 34

Linux Administrator

SAN/NAS

- IBM ESS
- FastT/DS4000
- EMC Clarrion
- NetApp Filers
- RAID hardware and software
- Tape backup/libraries

Enterprise Architecture Consultant, Enterprise Architect, Hartford, CT 2004–2005

Provided contract consulting services in all aspects of WebSphere architecture, installation, upgrades, clustering and application deployment. Recommended and developed proof of concept implementations for Linux/WebSphere on Intel alternatives to existing Sun/Solaris implementations.

Director, Information Technology, Director Information Technology, Hartford, CT 1984 – 2004

Proposed, developed and implemented corporate wide file/print services, e-mail, antivirus, firewall, proxy and intrusion detection systems based on Linux, open source projects and commercial solutions. Implementing corporate LDAP directory infrastructure for encrypted Single Source authentication, authorization and centralized administration. Significantly reducing administration complexity and support costs.

- Designed and developed Web-based application architecture built around Linux based IBM WebSphere Application Servers, running in a highly available clustered configuration, on IBM Blade servers. Provided architectural, security, problem determination and migration / upgrade support for the production and development infrastructure and applications. Focused on providing access to current technology offerings, while maintaining maximum stability, performance, security and availability of the production and development environments.
- Designed, deployed and supported a nationwide TCPIP Frame-Relay and MPLS network covering over 50 Branch and Home Office locations. Focusing on ensuring the maximum affordable capacity, redundancy and fail over capabilities while providing secure, managed access to corporate and Internet applications and services.
- Provided technical architecture, design and support of all mainframe, RISC and Intel based servers, desktops and networks. Budget development, presentation and management. Vendor negotiation and management.
- Manager, Systems Programming: Responsible for Systems programming staff supporting MVS/SP/XA, CICS, VTAM, NCP, JES2 and other applications on IBM 3090 processors.
- Sr. Systems Programmer: Responsible for the installation maintenance and tuning of MVS and related subsystem. Implemented UCC1 (CA1) Tape management and UCC7 (CA7) Job Scheduling software and procedures.

Professional Certifications

- Red Hat Certified System Administrator
- Red Hat Certified Technician

UNISYS

Resource 35

Linux Administrator

Key Skills and Knowledge

- AIX 4,5,6,7
- Power Systems
- VIO
- HMC
- Red Hat Enterprise Linux
- Oracle Enterprise Linux
- SuSE Linux
- Windows
- Scripting
- Networking
- Supervision
- Project Management

Professional Summary

Skillful system administrator with a wide range of experience with Commonwealth projects. He has a total of 13 years system analysis experience with 7 years of Commonwealth experience. He is skilled in data recovery, migrations, implementations, maintenance, and network management.

- Operating Systems: AIX4, 5, 6, 7. Red Hat Enterprise Linux. Oracle Enterprise Linux. SuSE Linux. Windows NT/2000/2003/2008. All Windows Desktop Operating Systems.
- Hardware: IBM stand-alone and IBM P-series servers. IBM Hardware Management Consoles.
- Software: Apache, Samba, VMware, Perl, VBscript, PowerShell, UNIX/Linux Shell Scripting, Oracle RAC clustering. PowerHA clustering.

Employment History and Related Experience

Unisys Corporation, Senior UNIX Administrator,
Harrisburg, PA 2005 – Current

Responsible for the day to day management of all AIX and Linux systems in the Data PowerHouse data center for various Commonwealth agencies. This included server deployments through various processes, PowerHA configuration, user requests, operating system level migrations and patching.

- Managed BladeLogic repository for Linux patching across various Linux platforms including RHEL, SLES, and OEL.
- Developed scripts as needed to maintain a consistent environment across the entire data center.
- Participate in all Disaster Recovery planning and testing. This included gathering customer requirements for recovery of various application and database servers, developing the best recovery method of rootvg and non-rootvg as well as customer data, execute recovery exercises and ensured consistent support to the customer as they proceed with their testing of the recovered systems.
- Unemployment Compensation Management System – Built the new operating system image on the updated platforms, worked with IBM experts on performance tuning, ground up installation of all IBM Power hardware including SAN and Network cable installation (Ethernet and fiber), frame mapping of physical devices to ensure redundancy, stability, and performance, of the systems
- Collaborated with IBM experts to install VIO servers and PowerHA clusters ensuring the application and files were available with the least amount of downtime for a smooth transition

UNISYS

Resource 35

Linux Administrator

- Supported various business partners: DBAs, Application Developers, Network, SAN/TSM, Windows Administrators for performance testing, process flow, etc
- Tivoli Monitoring/Network Support –Built a RHEL 5.X image to support application requirements for virtualization, security, and stability from Virtual Machines (VM) and Intel X86 physical servers
- RedHat Network Satellite (RHN Satellite) – Developed RHN Satellite product for patching and maintaining a base line platform for any RHEL system.
- Configured the central satellite server, setup the database and register/connected all clients to their appropriate patching cycle. Working with the owners of the various RHEL clients
- Established the most effective patching cycle for their systems and ensured all systems were current and met the standards needed as set forth by OA
- Bureau of Workers Compensation – Upgraded field office servers from AIX 5.3 to AIX 6.1, PowerHA to the most current supported levels in PowerHA 6.1
- State Workers Insurance Fund – Supported the installation and upgrade maintenance of Dollar Universe application
- Integrated Enterprise System AIX 5.3 to AIX 7.1 migration – Developed and executed the migration plan needed to move from AIX 5.3 to AIX 7.1 to ensure the least amount of down time possible for the customer.
- Streamlined mksysb implementation – Generated a new mksysb creation/storage process to ensure redundancy of the backup images and to further enhance the availability of these images for Disaster Recovery.
- Department of Revenue AIX 5.3 to AIX 7.1 migration – Developed the migration plan needed to move from AIX 5.3 to AIX 7.1 to ensure the least amount of down time possible for the customer; scheduled all of the systems in various maintenance windows to ensure accurate time for testing and meeting the requirement for a phased approach of implementation.
- Disaster Recovery Testing – Accomplished annual disaster recovery testing to ensure the application's availability should a disaster occur; built, restored and configured 30+ AIX LPARs to meet the current production environment
- Maintenance Window Management – This agency has monthly maintenance outage windows. I am responsible for coordinating all of the events in the maintenance window, including communications between other departments within Unisys as well as DOR agency staff
- Pennsylvania Liquor Control Board Integrated Business Management System (IBMS) Project –Develop a stable 5.X RHEL operating system image and deploy servers to the agency as needed based on the given build requirements using Virtual Machines (VM) with the required level of security; accomplished day-to-day maintenance of systems, processing of change requests related to systems, and responding to incidents.
- Department of Environmental Projection Oracle Enterprise Linux – Accomplished day to day work includes file system expansion, security monitoring and tuning, and storage and performance monitoring.

UNISYS

Resource 35

Linux Administrator

- Department of Public Welfare Oracle Enterprise Linux – Built and maintained repository, maintenance of other OEL servers and creating new OEL servers as the agency seeks to expand its environment.

Additional Employment History

Earthlink, UNIX Web Hosting Administrator	2000 – 2004
Global Management Services, Chief Technical Officer	2003 – 2005
Cross Connect Technologies, Network Engineer	2002 – 2003
Keystone Programming, Linux Administrator	1999 – 2000

Education

- Dauphin County Technical School, Information Technology, 2000

Training

- New Horizons: 1999, 2000
- Microsoft Certified Systems Engineer Training

Certifications

- IBM Certified System Administrator – AIX7
- ITIL v3
- Microsoft Certified Professional

This page intentionally left blank.

Mainframe Infrastructure Architect_Engineer

This page intentionally left blank.

UNISYS

IBM

Resource 36

Mainframe Infrastructure Architect/Engineer

Key Skills and Knowledge

Performance Tracking Software

- SAS
- MXG
- NeuMICS
- BEST1/ BMC Perceive and Predict
- Macro4 Expetune and Expetune DB
- MainView
- STROBE
- ASTEX
- DB2 Performance Analyzer
- LoadRunner, Candle/Tivoli
- SimNet
- HyPerformix
- HP OpenView
- HP MeasureWare
- SMF/RMF

Operating System and Subsystems

- IBM's z/operating system
- Sysplex
- WLM Goal Mode
- z/VM 5.3
- UNIX (AIX and USS)
- Linux SuSE
- WebSphere Application Server
- WAS v5 HTTP Server
- Apache
- CICS
- IMS
- DB2
- MQ Series (mainframe and AIX)
- XRC (Extended Remote Copy)

Languages, Tools, and Databases

- SAS
- REXX
- z/operating system JCL
- Microsoft Project
- Lotus Notes
- Microsoft VISIO; PERL,
- Visual Basic; J2EE,HTML, XML, ODBC, CGI, API

Professional Summary

Highly experienced and well-grounded infrastructure system architect, capacity planner, performance analyst who believes in fully using what you have before asking for anything more. Strong technical architecture expertise, solid understanding of core business functions, and a broad knowledge of hardware/software products and platforms. Demonstrated capacity planning and performance tuning expertise in complex, high transaction volume environments. Ability to work autonomously or as a team contributor with demonstrated strengths in leadership and consensus building. Keen problem-solving, performance troubleshooting, and risk analysis skills. Easily adaptable to change with an eagerness to learn and expand capabilities.

Holding a Public Trust – High; Security Clearance. (FMS – Dept. of the Treasury)

Employment History and Related Experience

Onpoint Corporation, Lead Technical Architect/Project Leader, Hyattsville, MD 2009 – 2011

Assigned to U.S. Dept. of the Treasury FMS -Financial Management Service – as Lead Technical Architect / Project Manager – for the project to deploy (1) IBM DataStage (-an ETL), (2) zLinux, (3) WebFocus and (4) zVM on System Z. This is the first production Linux application on zSeries architecture for FMS, and the first Linux application placed into production for FMS. The team was a combination of IBM consultants, FMS (Dept of Treasury – Financial Management Services) and FRB (Federal Reserve Bank of San Francisco) employees. Received a letter of commendation from the Dept. Assistant Secretary. As a direct result of the successfully completion of this project, Onpoint received its highest customer satisfaction rating for 2011 from FMS of all the Onpoint federal agencies contracting with Onpoint for services.

- Assisted in administering multiple ETL tools including IBM DataStage; iWAY ETL Manager, within the project scope.
- Provided support for activities such as upgrades and implementations.
- Performed defect analysis; PMR (Problem Management Record) research and problem data collection.
- Reviewed design and architecture documents and provide ETL development teams with input on sound architecture and design principles (such as restart, purging, parallel execution, etc.).
- Performed code migrations according to System Change Management policies.
- Identified risk areas and implemented preventative measures.
- Recognized and implemented performance internal enhancements and optimizations (i.e. Automation, scripting, etc.).

IBM

Resource 36

Mainframe Infrastructure Architect/Engineer

Telecommunications

- TCP/IP
- HiperSockets
- vLAN
- vRouter
- LU6.2
- Cisco
- SNA

Hardware

- IBM z Series – Z10, Z9, 990; 9021 G5 Servers, and 9672 class mainframes
- IBM Power p5/p6 series servers (AIX)
- IBM SHARK
- IBM DS8100
- HDS Lightning and HDS TagmaStore
- EMC Symmetrix and CLARiiON storage arrays

- Conceived and developed process automation/job scheduling using the Autosys scheduler.
- Monitored, measured, and optimized application performance.
- Proactively tracked and addressed capacity management issues.
- Worked with remote Application Support teams to resolve issues that may impact optimal performance of the application.
- Developed and implemented problem management practices that focus on root cause analysis and prevention of future problems.
- Technical environment: (2) z10s (two data centers) , (7200 MIPs in IFLs in each); z/operating system 1.9, DB2 (v8), 18 LPARS, IP based, z/VM 5.3/ 6.2 running Linux SLES10/SLES 11, IBM DS8100, InfoSphere DataStage 8.1, InfoSphere Federated Server 9.1, WebFocus 7.6

PT Global Ltd, Senior Technical Consultant 2009

Collected, extracted and assembled needed data from SMF and RMF, reviewed areas that appeared promising for tuning opportunities, and collected and reviewed setting for IPT, WLM, MQ, CICS and SysPlex. This position required becoming quickly acclimated and oriented to the new site and structure of the customer's IT configuration.

- Determined and tracked time-of-day usage and determined four hour rolling average peak usage, by LPAR, CEC, service (i.e. CICS).
- Utilized monitors and tools (RMF/SMF, Spreadsheet Reporter, SAS/MXG, DB2 Query tool, CICS, DB2 Omegamon) to measure resulting performance.
- Identified the worse performing SQL queries / application programs, within the production workload set of programs. Also determined the most frequently used subroutines and those with highest CPU and I/O usage.
- Reviewed other possible contributors to poor performance, (z/operating system, MVS/JES JCL, CICS parameters, etc.).
- Pinpointed execution delays by type of delay.
- Identified root-cause(s) for suboptimal performance of critical mainframe applications from detailed delay and execution metrics.
- Tracked historical trends and variations for comparative analysis of applications performance to determine effect of volume and code changes.
- Verified if subsystem (CICS, IMS, DBS, VSAM) or and language support (USS, LE) parameter settings are contributing to high CPU.

Lockheed Martin, Systems Infrastructure Architect,
Baltimore, MD 2007 – 2008

Acted as the Senior IT hardware/software mainframe planner for the Centers for Medicare/Medicaid Services (CMS) (Dept. of Health and Human Services) enterprise infrastructure. Advised the CTO and the management team on mainframe technological strategies, development methods, tools, and overall technical direction in support of the customer's requirements. Provided a strong

technical architecture expertise, solid understanding of core business functions, and a broad knowledge of hardware/software products and platforms to deliver and maintain systems solutions to meet CMS business needs.

- Consolidated 2+1 CECs into 1+1 CEC without any service disruption to the customer. This resolved a two year running capacity problem.
- Proposed/implemented hyper sockets to link LPARs for VTAM traffic (and later ETL traffic).
- Consolidated two CEC footprints into one larger, cheaper mainframe.
- Campaigned for Catalog Recovery software when I discovered there was none available. Recommended storage group practice a catalog recovery off hours.
- Joined two mainframe IOCDFs without any major HMC address changes, onto one CEC.
- Revised how CA, BMC, Compuware software was (contracted for) retained – contract review and negotiation lowering yearly charges by using LPAR pricing.
- Proposed zero-based yearly budgeting and justification of ISP software to rationalize the ISP software costs.
- Performed the implementation of two CECs into one CEC without fault or incident, much to the accolades of the CMS senior management.
- Started discussion with Adabas to move toward LPAR based pricing, to be able to eliminate a z890 that was out of support.
- Evangelized the usage of 'jumbo packets' to speed transfer of data external to the z9 CEC. Tried to persuade for a 'private' exclusive SAN network for connection from the z9. Installed DS8100 on a private NAS using jumbo packet.
- Utilized skills in a wide range of functional areas including; mainframe architect, pre/post implementation systems engineer, systems programming, knowledge of data center automation, data center system & application migration/consolidation.
- Utilized expertise in server capacity assessment and consolidation, storage architecture and optimization, network enterprise connectivity, high-performance data management, business continuity, hardware planning, and installation/configuration.
- Consulted on development and delivery of major technology initiatives. Brought external information, ideas and expertise back to the team from various sources and presented information to all levels of the contract and customers organization.
- Advised senior management on mainframe technical architecture strategy.
- Led and influenced cross functional teams.

Resource 36

Mainframe Infrastructure Architect/Engineer

Blue Cross of Florida, Capacity Planner/Performance Analyst 2004 – 2006

Collected and presented data regarding an upgrade requirement for the Z990 that had failed twice before to be accepted by upper management. Prior presentations were poorly received by upper management as prior attempts were too technical and did not have a clear call to action.

- Obtained approval for the upgrade through the use of IBM's RMF SpreadSheet Reporter tool.
- Revised SMF/RMF processing and data retention policy as prior procedures lacked credibility with upper management due to data collection and data retention problems.
- Installed and implemented a new WLM Policy and developed new reporting classes that matched business Key Business Indicators (KBI) to system metrics.
- Reinstalled and upgraded the Merrill MXG installation.
- Re-implemented BMC Best1 MainView mainframe Analyze, Predict, Perceive, enabling the creation of a mainframe usage model to evaluate model changes and upgrades offered by IBM to facilitate the move to a new data center. Verified configuration offered by IBM would sustain the SLAs as the data center workload was moved.
- Modeled TSM (Tivoli Storage Manager) running on z/operating system to resolve performance problems of TSM running on the utility Z900 CEC.
- Installed and implemented data collection for AIX, and Intel servers, using BMC Visualizer ITIL CDB (Capacity Data Base) including modification for SLPAR virtualization in Power p5 servers in support of Blue Cross' initiating a move toward ITIL Service Delivery compliance.
- Re-implemented the BMC Best1 mid-range distributed server to analyze, perceive, and predict to give visibility to mid-range capacity. Initiated a project to wring saving out of AIX servers farm using consolidation, exploitation of AIX Power p5 virtualization, and by achieving greater efficiency in the use of AIX resources.
- Deployed Web-based daily reporting of mainframe, AIX and Intel server metrics and opened this to business owners and system administrators.
- Interfaced with developers to analyze and resolve performance issues.
- Technical environment: z9 and z990 (5000 MIPS), z/operating system 1.5, IMS (v9) and DB2 (v8), and z/VM, 5 LPARS, IP based, 3790 tape robotic library subsystems, three EMC Symmetrix Storage subsystems. 113 Power p5 CECs, running AIX 5.3 (240 LPARs), 26 Hewlett Packard model 380 and 580 servers virtualized running via VM software running 932 Microsoft images.

IBM

Resource 36

Mainframe Infrastructure Architect/Engineer

GlaxoSmithKline, Capacity Planner 2004 – 2004

Served as a Capacity Planner for a z/operating system client server system running SAP R3/DB2 in a z/operating system parallel Sysplex environment.

- Developed the capacity planning and performance reporting functions for this worldwide regulated, ERP SAP 4.6d implementation.
- Evaluated and assessed the capacity and performance issues. Validated IBM and SAP developed capacity forecasts.
- Performed general health check of system operation, and reviewed infrastructure uplift requirements against current usage. Reviewed SMF settings.
- Developed capacity reporting for the ongoing demands of the ERP SAP implementation effort.

Environment: SAP implementation on multiple 9672-Z8Z CECs, across two data centers connected by XRC (eXtended Remote Copy), z/operating system 1.4, four SYSPLEX environments, 14 LPARS, UNIX System Services, IP based, DB2 v.7.1, 3790 tape robotic library subsystems, three ESS Model 800 SHARK TotalStorage DASD/Cache subsystems, (one servicing the middleware P-Series application layer.)

Charles Schwab & Co., Capacity Planner 1997 – 2003

Tasked with establishing a capacity planning methodology that would allow Schwab to grow from 8,000 trades per day via the Internet to over 280,000 trades. Growing the e-trading infrastructure, eight Netscape content servers and ten middleware servers, accessing three legacy mainframes to 100 Netscape content serves, 250+ middleware servers and eight+ Legacy mainframe servers.

COMPASS America, Project Leader 1992-1996

West Coast representative of a European based consulting firm that used benchmarking to provide CoO (Cost of Operation), and 'Gap' analysis of the Information Technology (IT) infrastructures (i.e. -mainframe operation, client/server, and data network) for client companies and communicated best practices in these areas. With detailed metrics gathered from the client about capacity, availability, capacity utilized, cost to provide the capacity, and quality of the delivered service, recommendation were prepared, prioritized by cost savings, and best practices used by other companies were explained.

Nationwide Bank, System Architect/Technology Planning 1987-1992

Installed sufficient capacity just-in-time on the bank's mainframes (Tandem and IBM), data network, and DASD subsystems as the bank replaced all component of its deposit, loan origination, and loan servicing systems and transitioned from a UNISYS/Sperry based onto IBM/Tandem architectures while maintaining and

improve service levels as the bank expanded nationwide thru acquisitions, growing from $11 billion to $47 billion in assets.

Education

- MBA Concentration in IT Management, Colorado State University
- BS Organizational Behavior; Minor: Applied Science & Business, University of San Francisco

UNISYS

IBM

Resource 37

Mainframe Infrastructure Architect/Engineer

Key Skills and Knowledge

- IBM z196, zBX, z10-EC, z10-BC z9-BC, z/890
- 7060-H50
- Capacity on Demand CBU
- zManager(Unified Resource Manager)
- DS8800, DS8700, DS8300, DS8100
- STK
- EMC
- EMC DLm
- 3490, 3590, 3592
- TS3500
- TS7740
- 3745
- Hipersockets
- OSA Express3
- OSX
- OSM
- OSD
- OSC
- OSE
- OSA Express2
- OSA/SF
- FICON
- FlashCopy
- Snapshot
- TimeFinder
- PPRC/XD
- z/operating system 1.12, 1.11, 1.10, 1.9, 1.7
- SystemPac
- ServerPac
- JES2
- HCD
- Parallel Sysplex
- WLM, RMF, SDSF, VTAM, NCP, ISPF, PKZIP
- ZIP390
- Syncsort
- IBM Sort
- UNIX System Services, z/VM V6.1, V5.4, V5.3, V5.1
- VSwitch
- Vdisk
- DDR
- REXX
- zLinux (SLES9 & SLES10)
- YAST2
- CICS

Professional Summary

Technically sophisticated professional with a career that indicates reinforced leadership along with a business savvy and "hands-on" IT and networking skillfulness. Maintain focus on implementing the best advanced technology and business solutions while still succeeding at bottom line results. Excellent record for implementing large scale projects on time and budget. Team player who shows excellent interpersonal, leadership and communication skills.

Employment History and Related Experience

Leading Management Consultancy Firm, Managing Consultant, Marlton, NJ — 2008 – Present

Large Multi-National Retailer, Performed as mainframe architect and trusted adviser for a data center relocation from Massachusetts to Ohio for a major multinational retailer. Since the total data center migration was taking place over an extended period of time, extensive analysis was performed on mainframe and distributed server relationships. An asset discovery process which included developing an asset matrix was created. The asset matrix categorized the applications to be migrated by complexity as well as whether they were tightly coupled or loosely coupled to the mainframe.

- The various 1000 plus applications were assigned to application move events. The distributed servers which were defined as tightly coupled to the mainframe had to be identified and migrated at the same time as the mainframe move event.
- These applications were also assigned to the mainframe move event. Latency tests were performed to identify which servers were truly tightly coupled to the mainframe. SMF 118 records were analyzed to categorize the 5000 plus FTP steps into standard FTP, SSL FTP, and PGP FTP. The SMF 119 records were also analyzed for all of the internal and external IP connections.
- After identifying the external connections, the business partners were notified of the mainframe move event as well as actions needed to communicate with the new data center. Client utilized IBM methodology for the migration process.
- Worked side by side with client project managers so that all migration activities could be managed, tracked and reported for client C level management. This migration also included a client's customer for whom they were providing mainframe IT services.
- It was crucial to have the client's customer involved in the migration planning process. Migration included consolidation of 2 mainframes onto a single z196 at the new data center. Global Copy data replication was performed via TPC-R during the migration process. Physical tape (3592 and 3590), Virtual

- DB2 (V6 & V7)
- Assembler
- RACF
- SMF
- DFSMS
- ATAM
- DFRMM
- CA-1, CA-7, CA-11, CA-Datacom, CA-TLMS, CA-ACF2/CICS, CA-JARS, CA-ENF
- Compuware File-Aid, Xpediter, Abendaid
- DFDSS
- FDR
- SMP/E
- LRS (VPS, LRSNET, VSV, Pagecenter, Anyqueue)
- AFP/PSF
- Netpass
- TPX
- Netview
- DFHSM
- Tivoli Decision Support
- Metron Athene
- Capacity Planning & Performance Tuning
- Disaster Recovery(BCRS & SunGard)
- TMON/MVS/CICS/DB2, Dumpmaster
- Tivoli Storage Manager
- Tivoli DLA
- TADDM
- Advantis
- ICCNET
- TCP/IP
- FTP
- SMTP
- DNS
- DHCP
- IBM HTTP Web server
- Cisco Routers & Switches
- PIX Firewall
- Cisco Call Manager 3.3, 4.1.2, 4.1.3
- VoIP
- Cisco IOS
- Cisco Works LAN/RWAN and ITEM
- Internet, OC12, T1, T3, PRI, VPN, VLANs, WAN acceleration.
- WAN
- Packeteer

tape (CA-VTape on DS8100) were consolidated onto an EMC DLm virtual tape subsystem and then replicated to the new data center.

- The EMC DLm was later replicated to Sungard for disaster recovery purposes. Attended client disaster recovery test as well as made recommendations for their IT methodologies. Created the move day time line and back out project plans as well as tracked and managed their 3 Dry Run testing processes and product mainframe move event.

Large Multi-National Financial Institution, Brazil Stabilization Program, A data center z/operating system Health Check and application SDLC (Software Development Lifecycle) assessment were performed after the data center was relocated from Mexico to Columbus OH. This assessment was prompted by problems when the data center was in Mexico. GRB (Global Resource Banking) batch, which was considered unreliable and often at risk and IT processes were the targets for review.

- Adabas production and development databases were reviewed and evaluated. This analysis included use of best practices, administration, monitoring, backup, recovery, optimization, availability, data protection and compliance.
- Adabas parameters were reviewed as being setup for attaining peak performance. Disk and tape hardware (EMC VMAX using SRDF/A replication and TS7740 grid) and software were reviewed. This included analysis of DCOLLECT data for DFSMS configuration, data set usage, use of disk archival products, and tape management software.
- SMF data was analyzed to identify long batch production jobs and where improvements could be made using different methodologies or tools. UNIX System Services (USS) parameters and USS file structures were examined for use of best practices.
- The master catalogs and user catalogs were reviewed for performance and best practices. The areas of concern were identified and recommendations were prioritized for each area and were included in the assessment report for the client.

Leading Management Consultancy Firm, Network Virtualization for zBX, Created intellectual capital materials so that IBM could make a new product offering (6948-M35 Network Virtualization for zBX) to their z Series clients. It would be offered to clients who wanted to deploy virtual networks in their zBX Ensemble environment.

- Created a Statement of Work, Perform Guide, which would be used by the IBM z Series delivery teams, and 3 training modules. These training modules included materials for configuration of virtual networks, virtual servers, hosts and adding storage to the x Blades, p Blades, and special Optimizer Blades in the zBX. It also included the enablement of the z/operating system and z/VM LPARS for the Ensemble on the zBX.

IBM

Resource 37

Mainframe Infrastructure Architect/Engineer

- Apache
- Tomcat
- HTML
- Applinx
- Java Scripts
- Adabas
- Windows XP/ Windows 2000 Server/Windows 2003
- Front Page
- MS Office Suite (Word, Excel, PowerPoint, Visio, Outlook)

Qualifications

- Provided training to IBM World Wide audience:
- IBM System z - Network Virtualization for zBX

Technical Training

- IBM
- System z Technology University
- zEnterprise and Unified Resource Manager Workshop
- z196 and zBX and zManager
- Engagement Leadership Workshop
- Core Consulting: Deep Blue C
- Core Consulting: Global Blue Consulting
- Server Time Protocol (STP)
- Technical Solution Owner (TSO)
- S/390 Web enabling Workshop Using Java Connectors
- Assembler Language Coding SMP/E
- MVS System Internals MVS Dump Debugging
- Harris Disaster Recovery Associates, Advanced Business Disaster Recovery & Prevention
- Metropolitan Institute of Network Technology, Ethernet TCP/IP Interconnect for the Internet Cisco Router Configuration
- New York University, Management of Technical People
- IEEE Computer Society Member, Learning Java Scripts
- Guide/Share Conference Attendee
- Past Member of DPMA

- Conducted training sessions were given to IBM internal world wide z Series delivery teams that encompassed North America, Latin America, Europe, Asia and Pacific regions. This training would supply these teams with the knowledge to engage the clients who needed this work to be performed.

Large Health Care Insurer, Dual Sysplex Work Stream 2, Performed as the mainframe architect and technical lead of 11 SMEs; Created architectural documents for business and technical requirements, architectural recommendations and solution design documents including data discovery templates, mainframe hardware equipment specifications, data center requirements, network requirements, and workload migration strategies.

- Migrated 2 mainframe workloads (7 z/operating system LPARS and 1 VM LPAR) from an IBM SO managed data center in Staten Island NY to client owned and IBM SO managed data center in St Louis, MO.
- Installed a z196 with zBX for z/operating system and z/10 for workloads. Workloads were replicated to St Louis using Global Copy (PPRC/XD) over OC12 high speed lines. There were over 200 midrange servers which need to be included in the migration from Staten Island, Brooklyn, and Albany NY with the mainframe. The midrange servers also utilized the same OC12 replication network. The mainframe strategy used the same successful 5 replication method which was used in Dual Sysplex Work Stream 1.
- Created architectural documents for business and technical requirements, architectural recommendations and solution design documents including work products for data discovery templates, mainframe hardware equipment specifications, data center requirements, network requirements, and workload migration strategies.
- Migrated 2 mainframe workloads (6 LPARS) from outsourcer location in Dallas to client data center in St Louis. This included new hardware installation in St Louis, install of DS8300 on ACS data center for EMC to TDMF conversion to allow Global Copy replication, OC12 installation for data replication from Dallas to St Louis. Also a TS7720 was installed on outsourcer floor to cover growth in B20 ZORO (zSeries Optical Replacement Option) unit until migration was complete. TS7720 was GRIDed to TS7720 in St Louis. Old tape technology was replaced in St Louis with TS3500/TS7740 ATL/VTS. Global Copy (PPRC/XD) was used for 5 replications (system test, 2 application user tests, dry run, and prod cutover, and customer signoffs). Migration of outsourcer Pittsburgh location (5 LPARS) to St Louis was performed shortly thereafter using same methodology with exception of not needing to perform. TS7720 for ZORO. Both migrations were completed on time to meet contractual agreements had with leaving outsourcer data centers.

Large Outsourcer and supported large greeting card client, Global Mirror, Worked on team that was engaged to convert the greeting card client data center, managed by outsourcer from EMC Symmetrix DASD to IBM DS8300

DASD. After DS8300 was installed and configured, provided ACS with a methodology with samples for converting EMC TimeFinder backup scripts to a replacement using the IBM FlashCopy method.

- Provided a presentation to outsourcer Storage Admin staff in Kansas City, Dallas and Mexico, and client DB2 admins which showed concepts for FlashCopy, FlashCopy Space Efficient, and how DB2 Backup Restore System Utility would use DFHSM Fast Replication through DFSMS.
- Created initial SMS DB2 data base copy pools and log copy pools under SMS for Hallmark DB2 admins and outsourcer storage admins.
- Created documentation for ACS and DB2 admins for the FlashCopy and DB2 Backup Restore System Utility.

Large Health Care Insurer, Mainframe Optimization, Performed as the TSO (Technical Solution Owner) on the Large Health Care Insurer project which is a complex deal involving 7 different SOWs (Statements of Work) across several SPLs with internal IBM SO (Strategic Outsourcing) being the ITS Delivery client. The mainframe component involves consolidating 18 z/operating system and 1 z/VM workload from 2 IT services (outsourcer) locations and 1 IBM SO managed location into an newly SO managed data center in St Louis.

- Current 5 mainframes at the existing SO Richmond managed data center would first be placed into a larger aggregated Parallel Sysplex in the Richmond data center. This included a Production Sysplex and a Sandbox Sysplex.
- Consolidated workloads from 4 St Louis z/operating system mainframes would later be joined into an aggregated Parallel Sysplex.
- Create a Production Sysplex and Sandbox Sysplex environment. The end result allows the client to save on outsourcing charges to the IT services firm as well as on IBM software license charges via the PSLC (Parallel Sysplex License Charge methodology.
- Many iterations of technical solutions (SOWs, WBSs, and RACIs) were created for the client so they would have the flexibility to consolidate the workloads into one or two different data centers and whether to include the currently under contract IT services firm workloads in those consolidations.

Large Regional Supermarket Chain, Dual Data Center Operations, Performed as the Mainframe Architect for the design of a dual data center that provides an environment for high availability servers as well as a disaster recovery location for the primary data center. This included collecting data, documenting the current baseline capabilities, and performing requirements analysis.

- Created Framing documents as well as Detail Solution Design, and Failover and Fallback documents.
- Created a design so that mainframe applications that interacted with other components on distributed platforms could be certified for disaster fail over at the 2nd data center.

- Designed the mainframe at the 2nd data center to use Capacity on Demand CBU feature on z10 CPU to save on software costs. The environment consists of a zSeries with several LPARS and approximately 90 UNIX (AIX, Solaris, and Linux) and 128 Windows servers. Identified the cross-platform inter dependencies for the various applications by using Tivoli application discovery tools DLA on the Mainframe and TADDM on the Open Systems severs.
- Identified the current System Management processes that are in place. Made recommendations for best practices as well as identify potential problem areas. The primary data center is designed to run asynchronous Global Mirror on the DS8000s between the 2 data center which are approximately 170 miles apart and Netapp Snap mirror for the Windows servers. Windows servers are being virtualized as much as possible at the 2nd Data Center via VMware and the PSeries will run as additional LPARS on larger PSeries servers.

Large Outsourcer and IT Services Company, Created and documented a strategy which they could deploy on their newly installed DS8300 disk subsystem for taking a Point-in-Time Copy (FlashCopy) on their client's global 24/7 12 Terabyte DB2 data base. This procedure would include creating an instant Point-in-Time copy of the DB2 data base using DFSMS Copy Pools in conjunction with DFHSM Fast Replication and DB2 Backup System Utility. These instantly created volumes would be dumped with DFDSS and used and tested at the disaster recovery hot site.

State Agency, Upgraded zSeries environment from z/operating system 1.4 to z/operating system 1.9 along with software upgrades to many out of support ISV program products (CA1, CA7, CA11, Ca-Datacom, CA-ACF2, CA-ACF2/CICS, CA-ENF, CA- Common Services, Compuware FileAid, Xpediter, Common Shared Services, and Syncsort across 3 LPARS. This was orchestrated alongside version upgrades to DB2 and CICS/TS.

Large Pharmacy Benefits Managing Company, Insourced 2 existing business units from 2 different outsource vendors onto a z10-EC 2097-710. The environment included 10 LPARs in a Sysplex environment including a zIIP, Crypto and IFL engines for DB2 and z/VM/Linux. This included working with outsourcing vendors and customers.

- Performed HCD and created IODFs dynamically. EMC SRDF replication was used to relocate data from remote outsource data center locations. Once EMC virtual tape (DLm) and disk data was on site, it was replicated via SRDF again to corporate remote site for D/R testing.
- Successfully performed D/R test as a post migration task. Customized SNA and TCP/IP network for new environment.
- Provided RMF workload analysis of new z10-EC combined environment for customer. Provided tuning recommendations for the new combined data center environment.

Resource 37

Mainframe Infrastructure Architect/Engineer

Independent Consultant, IT Consultant, Chalfont, PA 1998 – 2006

Provided software support for z/operating system, Linux for System z, disaster recovery, and network support.

Companies included: Software Developer, Print Publications, Life Insurance, Retail Clothing, Car Insurance and Services and Direct Mail Advertising.

Large National Distributor of Magazines, Assistant IT Director Technical Services, Pennsauken, NJ 1986 – 2008

Managed a group of systems programmers in z z/operating system, z/VM and Linux for System z environment. Supported all aspects of the data center including hardware and software, UPS/Backup Generator, Disaster Recovery. Voice and Data networks, PBX and VoIP phone systems.

Major Financial Publishing Company, Manager Host Systems, Princeton, NJ 1984 – 1986

Managed a group of 6 system programmers in an IBM multi-CPU and multi-operating system environment. Responsible for the ongoing support and maintenance of MVS, VSE and VM, vendor products, system performance and tuning. Instrumental in the planning and implementation of the VSE to MVS conversion.

Major Service Company, Senior Systems Programmer, Philadelphia, PA 1983 – 1984

MVS and VS1 systems programmer. Completed a VS1 to MVS migration that required an upgrade to VS1 so that MVS, VM and VS1 could all coexist on the same Mainframe during the migration. Designed, implemented and tested a VS1 disaster recovery plan (Sungard).

Major Electronics, Media and Govt Services Corp., Senior Systems Programmer, Cherry Hill, NJ 1980 – 1983

MVS Systems Programmer in a multi data center environment.

Major Insurance Company, Systems Programmer, Roseland, NJ 1968 – 1980

MVS Systems Programmer, Operations and Production Support, and Computer Operator

UNISYS

Resource 53

Mainframe Infrastructure Architect/Engineer

Key Skills and Knowledge

- Project Management
- Hardware Installation
- Dorado Mainframe Architecture
- operating system 2200 Software
- MCP Operations
- Software Upgrade
- Problem Solving
- Transaction Processing
- Technical Expertise
- OLTP
- WEBTS
- LSAM
- MAPPER
- System Performance
- SIGHTLINE Software
- Disaster Recovery
- Data Replication - SRDF
- EMC Storage
- Virtual Tape
- Cartridge Tape/SILO
- DEPCON Print Distribution
- NETWORK
- Secure FTP
- ITSM7
- ITIL V3
- Windows
- Excel, Word, PowerPoint
- Visio

Professional Summary

Resource 38has over thirty years of experience in the data processing profession with the Unisys Corporation. He has a proven track record in installing and supporting large mainframe computer systems.

- Strong technical expertise, problem solving abilities, and leadership skills have been displayed in his support of major clients such as United Airlines, IRS, Pennsylvania Department of Public Welfare, Pennsylvania Game Commission and State Police
- Stellar system knowledge, attended numerous internal software, hardware, and management courses providing his background computer knowledge.
- Tracks Emerging Technology attending workshops and seminars dealing with Unisys Clearpath Architecture and Open Systems environments.

Employment History and Related Experience

Unisys Corporation, Global Managed Services, Systems Analyst, Harrisburg, PA — 2000 – Present

Delivers Technical Support for several PA State Agency's which include PADPW, PA State Police, and PA Game Commission.

- Technology studies and analysis for large Mainframe Systems as well as Open System Server environments
- Integration of disaster recovery environments and maintaining Client Satisfaction to avoid SLA penalties.

Unisys Corporation, Computer Systems Group, Project Manager, Harrisburg, PA — 1988 – 2000

Technical Project Manager for the Unisys Computer Systems Group, managed a staff of Computer Systems 2200 Architecture Specialists at a $30 million data processing center servicing the PA Department of Public Welfare.

- Managed migrations for of mainframe, peripheral, and software environments
- Maintained nearly one hundred percent system availability.

Unisys Corporation, Professional Services Systems Analyst/Consultant, Harrisburg, PA — 1982 – 1988

Supported Unisys Contract for Department of Public Welfare as a Systems Analyst. Provided Operating System, telecommunications, and MAPPER support on this multiple mainframe customer site.

UNISYS

Resource 53

Mainframe Infrastructure Architect/Engineer

Unisys Corporation, Professional Services Systems Analyst, Martinsburg, WV 1981 – 1982

Professional Services Analyst assigned to support a major 2200 mainframe installation project at the IRS Service Center in Martinsburg, WV.

Unisys Corp., Professional Services Systems Analyst, Chicago, IL 1979-1981

Provided Operating Systems analysis, supported 2200 mainframe upgrade project at United Airlines in Chicago, IL.

Education

- B.A., Mathematics, Lycoming College, Williamsport, PA, 1978

Training

- 2200 Mainframe Operating System; transaction processing concepts and internals
- Programming languages COBOL, MASM, and 4GL
- Communication concepts and programming
- Management courses for creative problem solving
- Interactive communications, and time management, Clearpath workshops

Professional Certifications

- ITIL V3 Foundations
- Yearly Renewal - Ethics Awareness and Information Security Awareness

UNISYS

IBM

Resource 39

Mainframe Infrastructure Architect/Engineer

Key Skills and Knowledge

- z/VM – z/Linux, z/VSE, MVS, operating system/390, z/operating system Systems Programming
- JES2
- z/operating system UNIX System Services
- WebSphere MQ Series
- Lotus Domino (on z/Series)
- Tivoli Storage Manager (z/operating system and z/Linux)
- Tivoli Monitoring under z/Linux
- TADDM Installation under SLES Linux
- z/Linux Infrastructure Support under z/VM
- RACF/VM
- CSE on z/VM
- Linux High Availability on System z
- Velocity Software - z/VIEW - z/TUNE (z/VM - z/Linux Suite)

Professional Summary

Over 20 years of diverse experience. Expert in installing and maintaining z/Series operating systems and mainframe OEM products. Project lead experience in z/VM-z/Linux, z/VSE and MQ Series on the z/Series systems. Designed a z/VM-Linux system running WebSphere from proof-of-concept through a running production z/Linux system. Worked with TSM on z/operating system for a backup solution for Lotus Domino (TDP) and z/Linux under z/VM. Performed a WebSphere MQ Series health-check and help implement conversion from an older bisynchronous network protocols to running under WebSphere MQ on z/operating system. Implemented z/Linux solution with SOA Components (WebSphere Application Server and WebSphere Message Broker). Main technical lead on a z/VSE to z/operating system Conversion. Implementation of RACF/VM in a z/VM-z/Linux environment. Lead z/Linux SME on a large distributed server to z/Linux Conversion project (+500 servers).

Employment History and Related Experience

IBM, Senior IT Specialist, Jacksonville, FL 2006 – Present

- Assisted with health check for WebSphere MQ Series on z/operating system. Installed new z/VM-z/Linux Production environment and helped install z/operating system Production environments (WebSphere MQ and MQ Series Message Broker).
- Assisted with z/VSE to z/operating system conversion.
- Leading a large distributed server environment project moving to z/LINXUX.

Wachovia Bank, System z Consultant, Jacksonville, FL 2005 – 2006

- Documented and assisted in the implementation of security audit requirements for z/operating system UNIX System Services.

Blue Cross/Blue Shield of Florida, System z Systems Programmer, Jacksonville, FL 2004 – 2005

- Assisted with the conversion of z/operating system 1.4 to z/operating system 1.7 Support and install new releases of z/VM.

Supervalu Inc., Senior Systems Programmer (System z)
Eden Prairie, MN 1993 – 2004

- Supported, installed, and maintained VM/ESA and z/VM for both production and z/Linux environments.
- Supported and maintained operating system/390 and z/operating system for development and production environments.

IBM

Resource 39

Mainframe Infrastructure Architect/Engineer

- Installed and maintained MQ Series for operating system/390 and z/operating system.
- Supported and maintained UNIX System Services and Lotus Domino on System z.
- Helped support Tivoli Storage Manager under UNIX System Services for System z.

Education

- B.S., Computer Science, Moorhead State University

UNISYS

IBM

Resource 40

Mainframe Infrastructure Architect/Engineer

Key Skills and Knowledge

- Hardware configuration management
- Storage Management
- Operating System concepts
- Written communication (Technical & Non-technical)
- Oral communication
- Interpersonal
- Project Management
- Project leadership
- IBM project methodology
- Problem analysis/resolution
- Data replication
- Change Management
- Disaster Recovery
- Business Continuance
- Vendor Management
- Virtualization

Professional Summary

Over thirty-three years experience including enterprise level IT systems management, storage management, Disaster Recovery/Business Continuity and IT project leader experience. Dedicated, hard-working professional with excellent leadership, project management, organizational, analytical, problem solving, communication and people skills. Recognized for quality, integrity, and proven success.

Employment History and Related Experience

IBM, WellPoint Client Data Center Relocation Project, Consultant — 2011 – Present

Developed and successfully executed innovative ISV Product Authorization Management technique to ensure all Client-licensed ISV software availability through transition period and final data and workload (production) cutover as a lead Project Manager. Participated in the integration of DR/BCP team project plans with migration team project plans.Identified overlaps, touch points, hand-offs, dependencies and milestones.

- Gleaned client ISV software product, vendor sales, and vendor support data in a contentious outsourcing company managed environment where minimal accurate information was available or given freely. Consolidated critical material into a comprehensive ISV Product Authorization Management document crucial to many WellPoint data and workload migration activities.
- Identified two major classifications of ISV Product Management: daily management of software product authorization and the complete installation of all product authorizations at major project data synchronization events. Developed procedures to properly install ISV product authorization for each.
- Executed procedures to efficiently and quickly install product authorization and validate product function on multiple data and workload cutover tests, dry run tests, and production cutovers. Provided on-site support at client's Data Center location for major project events.
- Developed Knowledge Transfer training for IBM steady-state team designated to acquire management responsibilities from outsourcing company. This included creation of the "ISV Product License Key Knowledge Transfer" document used as a model for all Transition Team knowledge transfer. Presented multiple large-group sessions to communicate experience and knowledge. Provided all developed documentation and procedures to IBM steady-state team. Provided assistance to IBM steady-state individuals after Production Cutover.
- Performed audit of client's Computer Associates (CA) licensed products and enabled elimination of many unused products. Reviewed WellPoint's CA agreement Addendum, installed product inventory, IBM Steady-state license installation procedures, and products active in production to identify

discrepancies. Documented and presented findings to WellPoint Management, WellPoint Procurement, and IBM Contract Management.

- Developed essential vendor communications and relationships communication to secure temporary product authorization during transition period, permanent authorization when permitted, and special technical support consideration during the Production data and workload cutovers.
- Provided z/operating system technical support to client user community and transition team during transition period testing. This included problem analysis and resolution and, when appropriate, working with vendors.

Allstate Insurance Company, Technical Consultant –
Service Delivery Platform Services, Northbrook, IL 2002 – 2010

Served as Business Continuity Planning Coordinator responsible for design, distribution and awareness, testing, and maintenance of plan. Managed the Disaster Recovery Plan updates made by technical areas into Living Disaster Recovery Planning System (LDRPS). Planned and coordinated HDS involvement in Data Center workload and data migrations and consolidations using TrueCopy, reviewed and modified SOWs to ensure completeness and accuracy.

- Sized, planned, coordinated activities for z/operating system storage platform and I/O connectivity in preparation for numerous Data Center workload and data migrations, data consolidations, Data center builds, and Data Center re-designs.
- Evaluated IBM, EMC, and HDS disk storage arrays in "Best and Final" selection process of primary disk vendor to enhance storage disk hardware reliability, availability, scalability, consolidate data, and simplify storage management; led data migration activities to new platform.
- Reviewed and modified disk storage vendor master agreements, developed contract addendums and numerous SOWs to ensure company goals and data protection.
- Evaluated disk storage vendor performance and rated vendor on key objectives to ensure adherence to contractual obligations; produced management summaries, led evaluation meetings, developed and managed corrective actions.
- Designed z/operating system I/O infrastructure and connectivity for over 80TB z/operating system data and associated tape and virtual tape to ensure proper performance and growth.
- Planned and guided z/operating system storage hardware activities and storage-related projects to ensure data availability, performance, protection, and accommodate growth.
- Developed philosophy to ensure system storage platform stability and minimize all management requirements including I/O configurations changes, HCD updates, data migrations, and firmware upgrades.
- Led Disk Storage Process Refinement team 6-month project to implement

ITIL management techniques, minimize storage FTE requirements, and improve provisioning time; prepared and presented final recommendations to management.

- Served as Change Advisory Board (CAB) member with Change Coordinator duties to review daily storage-related change records for adherence to standards, provide storage team representation at weekly department Change meetings, ensure management knowledge and approval of all changes, communicate and describe major storage-related changes to others, and communicate change-related policy updates, restrictions, and freezes to storage team members.

Allstate Insurance Company, Technical Consultant, Northbrook, IL 1995 – 2002

Chosen by IBM as a member of the z/operating system eBusiness Leaders Council (zBLC, formerly known as S/390 eBusiness Leaders Council – SBLC and Parallel SYSPLEX Leaders Council - PSLC) to guide IBM product development and promote my company's interests. Assumed Hardware Configuration Management team project leadership role. Planned and implemented the configuration change into the Field environment comprised of multiple IBM processors in multiple Data Center locations

- Achieved 100% success rate in significant operating system updates – 450 changes annually.
- Completed 100% of all required I/O configuration changes accurately and on schedule.
- Restored Field Data Center satisfaction and confidence in my unit's ability to manage their hardware environment.
- Facilitated several vendor and Allstate team meetings and conferences during major hardware outages to guide vendor activities and minimize disruption.
- Assumed Storage Management team project leadership role.
- Coordinated Allstate participation in annual IBM International Storage Systems Symposium Events.
- Planned, coordinated, and facilitated the annual Allstate Storage Conference; modified its purpose to include hardware topics; solicited vendor and Allstate participation; negotiated vendor training for Allstate employees at these events.
- Performed critical application and critical system 24-hour "SWAT" performance problem analysis and resolution duties for my unit for an extended length of time.

Allstate Insurance Company, Senior Staff Systems Programmer, Northbrook, IL 1986-1995

Planned and coordinated the consolidation of 12 Regional Office Centers, including the Allstate Motor Club, into 3 new data centers. Prepared and

executed instructions for relocation; guided field data center staff activities. Developed and presented IBM PR/SM hardware and operating system training to data center staff and management on all 3 shifts in each of the new data centers.

- Chosen to lead group of representatives from each technical support area to explore ways to eliminate software migration errors and system outages.
- Planned and coordinated, led discussions, and wrote final document that analyzed an integrated approach to software testing and migration and recommended the solution adopted as the "Preproduction"(Pre-pro) system.
- Chosen to lead "DEC" project: responsible for new Digital Equipment Corporation operating system and subsystem software installation and maintenance to host the Investments critical application data and workload.
- Developed DR plans for the backup and recovery of critical operating system environment, formalized plans in LDRPS, led recovery test efforts and presented test results.
- Prepared and presented a technical overview of the DEC platform and its components to my entire department.
- Prepared and presented monthly DEC project updates to my Director.
- Assumed all IBM VM/ESA system management responsibilities: VM/ESA software installation and support, configuration, VM guest definition and administration, etc.
- Prepared and conducted VM/ESA Test Environment technical presentation to IBM developers on campus for the Allstate/IBM Joint Case Study, later to become the HPTS (Highly Parallel Transactions System) Project.
- Worked with IBM developers to install new HPTS operating system, VTAM, JES2, etc. software and perform testing and verification.
- Led O/S Development Team efforts to implement HPTS in our environment: scheduled and facilitated weekly team meetings, developed team assignments, tracked progress, maintained HPTS-related documentation and published results.
- Participated in the implementation of Parallel SYSPLEX in the Field Data Centers.

Allstate Insurance Company, Senior Software Programmer,
Northbrook, IL 1985 – 1986

Performed NCP gens, network problem analysis.

Allstate Insurance Company, Software, Northbrook, IL 1983 – 1985

Acted as the project leader for IBM 8100 DPCX and DPPX Operating System and subsystem software installation, testing migration.

- Prepared, tested, and migrated software, hardware configuration, and

storage configuration packages and instructions for all local and remote data center installations.

- Prepared and presented Field Staff Specialist training classes.

Allstate Insurance Company, Production Analyst,
Northbrook, IL 1982 – 1983

Wrote several assembler language modules as part of a report distribution monitoring tool. Resolved production batch schedule amends, minor system problems.

Allstate Insurance Company, Computer Scheduler,
Northbrook, IL 1981 – 1982

Scheduled and monitored many critical application schedules.

Allstate Insurance Company, Computer Operator,
Northbrook, IL 1979 – 1981

Trusted with operation of remote, unsupervised, complex equipment and systems: "COM" area to produce micro fiche and "TRAN" area to run and monitor batch production schedule on IBM System.

Allstate Insurance Company, Record Clerk, Northbrook, IL 1978 – 1979

Handled report processing and distribution.

Education

- Computing and Information Science, Roosevelt University, Chicago, Illinois
- Harper College Palatine, Illinois
- Marquette University Milwaukee, Wisconsin, Business Administration

Professional Certifications

Professional Memberships

- IBM zSeries e-Business Leaders Council (zBLC): 2001 – 2002
- IBM S/390 e-Business Leaders Council (SBLC): 2000 – 2001
- IBM Parallel SYSPLEX Leaders Council (PSLC): 2000 – 2000

Awards, Recognition, Certifications

- Allstate Insurance Company Chairman's Award Winner
- Numerous individual and team Company and Department Achievement Awards
- Numerous individual Performance Bonus Awards
- ITIL Foundation Certificate in IT Service Management

This page intentionally left blank.

UNISYS

IBM

Resource 41

Mainframe Infrastructure Architect/Engineer

Key Skills and Knowledge

- MVS, operating system/390, z/operating system
- HMC LPAR definitions
- z/operating system Workload Manager (WLM)
- z/operating system Firewall Technologies
- JES2, RACF security
- z/operating system Performance & Tuning
- z/operating system UNIX System Services (USS)
- WebSphere Application Server V6.x/V7.x
- zVM-zLinux provisioning
- ITCAM for WAS V6.x/V7.x
- TDMF/LDMF
- zVM-zLinux

Professional Summary

Senior Information Technology Specialist in IBM Global Services. Highly skilled IT information system professional specializing in z/operating system Migrations and new z/operating system implementations including extensive skills in z/operating system UNIX System Services (USS), z/operating system WLM, WebSphere Application Server V6.x/V7.x for z/operating system and zVM-zLinux. Over 40 years experience encompassing all phases of IBM System Services, Maintenance and Implementation Services, including large system Hardware Service System Support & Maintenance, and IBM Software Delivery Services on z/operating system, with a focus in new IBM Product implementations for z/operating system, z/operating system Performance & Tuning including WebSphere V6.x/V7.x & ITCAMs, RACF Security definitions and new z/operating system Proof of Concepts. Extensive background performing z/operating system Parallel Sysplex WLM Merges, z/operating system LPAR and Data Center Migrations. Proficient in all areas of Performance and Tuning, Problem Determination (PD/PSI) and Project Management for z/operating system Enterprise customers.

Employment History and Related Experience

IBM Corporation, Senior IT Specialist, Los Angeles, CA 1996 – Present

Healthcare Provider, Senior IT Specialist/Architect, 2011

z/operating system Parallel Sysplex WLM Policy Merge:

- Provided WLM based Performance and Tuning Services to a large health-care enterprise customer, helping with the WLM-merge of six separate sysplex WLM environments.
- Successfully merged 278 combined Service Classes down to less than the architectural limit of WLM; utilized available IBM WLM Tools to successfully process, validate and test the new merged WLM policy onto the final production sysplex.

Automobile Manufacturer, Senior IT Specialist/Architect, 2010

Provide z/operating system Mainframe Architecture support to a global Automobile Manufacturer to help develop a new mainframe Reference Architecture Roadmap for the next 5 years.

- Provided global documentation support using an IBM Document Repository, creating technical support documentation during the term of the contract.
- Provided leadership to the global IBM Team creating reference documents used for technical content input to highly visible customer presentations. At the conclusion of the project, we had a very happy customer, with a resultant high level of future business for IBM Global Services.

IBM

Resource 41

Mainframe Infrastructure Architect/Engineer

Global Financial Enterprise Customer, Senior IT Specialist/Architect, 2009 – 2010

Assigned as Technical z/operating system – z/VM Consultant to a large z/operating system, z/VM – z/Linux enterprise customer to provide assistance with on-demand provisioning for z/VM -- z/Linux images using proven IBM IGS methodologies including high availability and failover processing.

- Provided onsite provisioning assistance with z/VM – z/Linux imaging, PD/PSI and problem resolution & change management on z/VM – z/Linux LPARs.
- Provided assistance with z/VM – z/Linux LPAR & application performance and tuning, based on IBM IGS best practices.
- Provided assistance with a mainframe reference architecture project, defining and identifying existing Service Oriented Architecture (SOA) based enterprise applications.

Global Transportation Enterprise Customer, Senior IT Specialist/Architect, 2009

Assigned as Technical z/operating system Consultant to a large z/operating system Global Transportation enterprise customer to provide a technical assessment of the technical support processes and procedures used in support of mainframe z/operating system hardware, z/operating system software and z/operating system applications.

- Conducted onsite review of technical support staff and reviewed the existing technical support processes and procedures including, PD/PSI and z/operating system problem resolution for z/operating system hardware and software LPAR requirements, solution testing and validation.
- Created a z/operating system hardware & software documentation repository with their existing documented technical support procedures used by the Technical Support staff to support their mainframe production environments; z/operating system hardware, z/operating system software and z/operating system global applications.

Pharmaceutical Enterprise customer, Senior IT Specialist/Architect, 2008

Assigned as Technical z/operating system Consultant to a large z/operating system enterprise customer to provide assistance with a large Data Center Migration and Consolidation Project.

- Provided onsite diagnostic assistance, PD/PSI and problem resolution on z/operating system LPAR bring-up, testing and validation.
- Reviewed z/operating system Performance and Tuning on all migrated LPARs and provided recommendations to customer technical staff, based on IBM best practices.

IBM

Resource 41

Mainframe Infrastructure Architect/Engineer

Midwest Government IT Installation, Senior Consulting IT Specialist/ Architect, 2008

Performed a 'z Server Health Check Assessment' for a Midwest Government IT Installation on a z Server running four separate LPARs and an Integrated Coupling Facility. Two LPARs were running z/operating system V1R8 and another was running z/VM V5.2 - z/Linux (SLESx).

- Provided immediate remediation for an urgent z/operating system Performance issue and then provided a 'z Server Health Check Requirements document' with Observations and Recommendations for consideration.
- Offered our Services to implement our recommendations, based on our findings.

Midwest government installation, Senior Consulting IT Specialist, 2008

Assist a government customer update zLinux, running under zVM (5.3), from SLES9 to SLES10.1 (SP1), updating & migrating TSM (5.4) and IBM Tapes to the new SLES10.1 environment and also with installation of WebSphere Application Server (Dist) V6.1 along with UDB-DB2 (V8.2).

West Coast Government installation, Senior Consulting IT Specialist, 2008

Assist a government customer with z/VM (v5.2) implementation & helped customize and tailor the z/VM LPAR to run z/operating system (V1R7) under z/VM.

- Provide specialized training to the customer staff and assist with changes to Operational procedures for updates to z/VM, to support & maintain z/operating system running under z/VM.

Health Care provider company in Chicago, Senior Consulting IT Specialist, 2007

zOS Consulting - NEW implementation of WAS for zOS V6

- Provided zOS Consulting Services for onsite support on a new WebSphere for zOS V6.1 implementation, including Performance and Tuning, Security and USS Capacity Planning.
- Provided Implementation support services associated with USS daemons & zOS Security definitions.
- Assisted with Application Deployment & coordination of new required HFS File Systems (capacity sizing and HFS size validations).
- Provided Skills Transfer sessions for the technical staff on related zOS & USS facilities.
- Provided analysis, validation and optimization of WAS V6.1 Performance & Tuning using z/operating system WLM.

- During application testing, finalized Performance & Tuning review and tailored to meet the zOS resource needs of deployed applications and validated results with the customer zOS staff.

West Coast Software Development Co, Senior Consulting IT Specialist, 2006 – 2007

Provide z/operating system V1R4 & V1R6 Consulting Services for a West Coast Software Development Company (IBM Business Partner), running separate z/operating system images in their West Coast Laboratory facility and a separate set of z/operating system LAPR images on an IBM CPC under z/VM (Dallas DR/BP Lab systems).

- Provided z/operating system Consultative Services onsite and remotely, to resolve ISV to IBM architecture issues and validate z/operating system compatibility and functionality associated with their ISV Encryption Product. Performance and Tuning Services were provided during the Benchmark Testing and made necessary changes to WLM and validated same.
- Provided long term System Programmer assistance and 24/7 support for the successful beta testing of their ISV Encryption Product.

Large Clothing Manufacturer, Senior Consulting I/T Specialist, 2006

zOS Performance and Tuning:

- Successfully analyzed, validated and optimized Performance & Tuning requirements for a zSeries installation running WAS V6 in production (June 2006) using z/operating system WLM Performance & Tuning methods; applied and validated WLM definitions.
- Reviewed performance results with the Technical Support Staff and provided customized instructions on implementation methods of WLM changes.

Large government installation in the West coast, Senior Consulting IT Specialist, 2004 – 2005

- Coordinated a Hardware & Software migration from a G4 CMOS Processor to a new zSeries z890 Processor for a large government installation in the West coast. Implementation Services included defining a new Integrated Coupling Facility and migration of three existing LPARs, installation of a new z/operating system SystemPac, Project coordination & long term project planning, and Skills Transfer to technical staff on usage of CHPID Mapping Tool and IOCP/HCD tailoring for z/VM & zLinux, including CHPID Definitions for Hipersockets and new FCP & OSD Channel communications.

Successfully analyzed, validated and optimized the new zSeries processor performance using z/operating system WLM Performance & Tuning methods, applied and validated with the customer's Technical Support Staff after the Hardware and Software migration.

IBM

Resource 41

Mainframe Infrastructure Architect/Engineer

Insurance Company in the West coast, Senior Consulting IT Specialist, 2004 – 2005

Successfully implemented new operating system/390 Firewall Technologies for Insurance Company in the West coast in order to use new VPN (Manual & Dynamic) Tunnels for secure FTP transfers.

- Responsibilities included the implementation of the Proof of Concept designed to allow for replacement of expensive Leased Lines to conduct secure FTP data transfers (via new VPN Tunnels) using IPSec.
- Successfully tested from a local MVS LPAR to operating system/400 and to AIX Firewalls
- Through Implementation Services, provided skills transfer to the system programming staff on USS and VPN implementation & maintenance, RACF equivalent definitions for their OEM SAF product (ACF2), project management, project planning, and the development and design of custom IBM Firewall Technology Scripts for user controlled modification processes and customized training for Firewall usage and commands.

Large government installation in the West coast, IT Specialist, 2004

Coordinated a migration from two older CMOS Processors to a new zSeries Processor including merging four LPARs into three, for a large government installation in the West coast.

- Responsible for implementation services which included project leadership and coordination, long term project planning, IOCP/HCD and implementation of new procedures, coordination of change management and migration testing.
- Analyzed and validated the new zSeries performance with customer's operating system Technical Staff after migration.

Education

- Electrical Engineering, Loyola Marymount University

Professional Certification

Professional Education, Credentials, and Affiliations

- SHARE Technical Conference (Anaheim, CA), 2011
- WSC z/operating system W.A.S. Implementation Workshop V7, 2009
- SHARE Technical Conference (San Jose, CA), 2008
- POK zVM-zLinux Implementation Workshop, 2008
- TDMF/LDMF Softek Implementation Workshop, 2007
- FLEX-ES zOS Implementation Training, 2006
- WAS V6.x for z/operating system, zLinux WSC Implementation Workshop (z/VM), 2005

Resource 41

Mainframe Infrastructure Architect/Engineer

- WAS V5.x for z/operating system Implementation Workshop, 2004
- WSC APPN/VTAM Implementation Update for CSV1R3, 2003
- WSC Workshop - Communication Server Update operating system/390 – z/operating system V1R3, 2002
- WebSphere Application Server V4.0 for z/operating system and operating system/390 Installation Workshop operating system/390 V2R8+
- VPN IPSec Tunnels, TCP/IP V2R10 Update Workshop, Linux for S/390 Installation and Configuration Workshop, 2001
- WebSphere Configuration and Java Programming for operating system/390 Web Enablement Gen-2 with WebSphere Application Server V3.x, WSC Workshop Enabling operating system/390 JAVA Applications Using WebSphere, 2000
- WSC Firewall Technologies operating system/390 V2R7, WSC e-business Workshop (WAS12, CTG, Net.Data, IWT) JAVA Programming (IBM E & T), 1999
- WSC Firewall Technologies Workshop operating system/390 V2R4, Net.Commerce V3 for S/390 Customization, Internet Enablement CGI Workshop operating system/390 V2R5, Net.Commerce V3 & CommercePoint (SET) T3 Class, Certified by WSC for PMMVS Performance Studies (MVS, operating system/390), 1998
- Four year curriculum for BS degree in Electrical Engineering at Loyola Marymount University, Los Angeles, CA, 1971

UNISYS

Mainframe System Programmer (IBM)

This page intentionally left blank.

UNISYS

IBM

Resource 42

Mainframe System Programmer (IBM)

Key Skills and Knowledge

- z/VM
- z/VSE
- VSAM
- Assembler
- Cobol
- TCP/IP
- VTAM
- CICS

Professional Summary

Responsible for z/VSE installation and maintenance, debugging, dump reading, problem and change management, programming and root cause analysis. Developed detailed implementation plans for the installation of new products. Additional responsibilities include development and implementation of Disaster Recovery plans and tests.

Employment History and Related Experience

Artech Information Systems, VSE Systems Programmer 2011 – Present

Install and maintain z/VSE system software, using IBM standard procedures, and VSE-related software, including Explore/CICS, Explore/VSE, FAQS/ASO & PCS, Via-Serv LDS, and EPIC.

Contract VSE Systems Programmer 2006 – 2010

Installed and maintained z/VSE & z/VM system software, using client standard procedures, and VSE-related software.

VM/VSE Systems Programmer, Systems Management, Specialist 1994 – 2006

Installed and maintained z/VSE & z/VM system software, using client standard procedures, and VSE-related software at multiple client locations. Document and implement Disaster Recovery plans.

Education

Certificate in Data Processing from West Coast trade school, 1969

This page intentionally left blank.

UNISYS

Resource 43

Mainframe System Programmer (IBM)

Key Skills and Knowledge

- z/VM
- Rexx
- IOCDS
- HCD
- RSCS
- TCPIP
- RACFVM
- DIRMAINT
- Performance Toolkit
- z/VSE
- z/Linux

Professional Summary

Responsible for installation, ongoing support, service and maintenance, problem resolution (debugging and dump reading), support of problem and change management processes, root cause analysis and programming of z/VM systems, subsystems and related products. Develop detailed implementation plans for the installation of new products and other changes. Maintain documentation. Directly interact with client personnel.

Employment History and Related Experience

IBM, z/VM Support Specialist — 2007 – Present

Responsible for maintaining multiple customer environments running z/VM, z/VSE and z/Linux systems as a member of the z/VM team.

- Support customer accounts using standard processes.
- Involved in the day-to-day activities of running the system.
- Troubleshoot problems and issues.

IBM, Resource Configuration Manager — 1997 – 2007

Designed, implemented, and maintained several different environments that used ESCON and FICON technology. Extensive experience in z9, z990 and z900 and other IBM processors.

IBM, z/VM Support Specialist — 1985 – 1997

Responsible for the VM environment at the Poughkeepsie, NY; Kingston, NY; and Lexington, KY IBM locations.

- Installed and maintained the systems at the then currently available levels of the product.
- Supported tools for customer and system support staff use.
- Participated in the VM/ESA Release 2 field test.

IBM, 3081 Final Systems Test Technician — 1982 – 1985

Performed the final system test of 3081 and 3084 processors. Ensured a fully functional and quality product was ready for shipment to the customer.

Education

- Nashville State Technical Institute, Nashville, TN
- Associate of Electronic Engineering Technology, 1982

This page intentionally left blank.

UNISYS

INFO-MATRIX CORPORATION

Resource 44

Mainframe System Programmer (IBM)

Key Skills and Knowledge

- 20 years Commonwealth of Pennsylvania experience
- PSP CHRI experience

Professional Summary

Skilled professional with more than 20 years' experience in mainframe system programming and experience with the Pennsylvania State Police.

Employment History and Related Experience

Commonwealth of Pennsylvania (PSP), Application Developer 2, Harrisburg, PA 2002 – 2011

My responsibilities for this position were to support and maintain various systems within the computerized Criminal History Record Information System. I used COBOL, SQL, and .NET. I also have had training in HTML. I would meet with the users to discuss changes to the existing programs. I would then write specifications detailing the changes. Once the specifications were reviewed and approved by the users I would start making the coding changes. After this process was completed I would then test the programs. After the programs were working correctly the programs would be placed into production. I would then monitor the programs to make sure everything was working properly.

Commonwealth of Pennsylvania (DPW), Application Developer 2, Harrisburg, PA 1993 – 2002

I was responsible for the maintenance and development of automated systems that support the Medical Assistance Management Information System using COBOL. I would meet with the users to discuss modifications to the existing programs. Once the modifications were determined, I would then write the specifications detailing the changes to the programs. These specifications would then be assigned to the programming staff. I would meet with the programmer assigned to make the code changes to go over the specifications for clarification. Once the programmer had the modifications made to the program and the changes were tested by the programmer I would review the testing results. Once I felt the modifications were working correctly I would have the users look over the results. Once the users agreed that the programs were working properly I would then have the programs moved into production. The programs would then be monitored to make sure they were working correctly.

Mansfield University, Computer Trainer Mansfield, PA 1993 – 1993

I taught adults who were attempting to get their GED how to use a computer using software that allowed them to do their studies on a computer.

Education

- B.S., Information Systems, Mansfield University, Mansfield, Pennsylvania, 1991
- High School Diploma, Wellsboro Senior High, Wellsboro, Pennsylvania, 1970

This page intentionally left blank.

UNISYS

IBM

Resource 45

Mainframe System Programmer (IBM)

Key Skills and Knowledge

- CICS
- Assembler
- COBOL
- SMP/E
- TSO / ISPF
- IDCAMS
- JCL

Professional Summary

Responsible for CICS installation and maintenance, debugging, dump reading, problem and change management, programming, root cause analysis, developing detailed implementation plans, backups, training of staff and maintaining documentation. Works well in team and individual environment; interacts in a courteous and professional manner with customers, colleagues and vendors.

Employment History and Related Experience

CDI Inc., CICS Systems Programmer 2008 – Present

Installed and maintained CICS system software, using IBM standard procedures, and CICS-related software, including Xpediter/CICS, Jars/CICS, MIMCICS and Install/1.

Ajilon Consulting, CICS Systems Programmer 1995 –2007

Installed and maintained CICS system software, using client standard procedures, and CICS-related software, including Xpediter/CICS, SmartTest, Jars/CICS and MIMCICS.

- Clients include:
  - IBM Global Technology Services
  - Pennsylvania Department of Revenue
  - Armstrong World Industries
  - RiteAid
  - Pennsylvania National Insurance

AMP Incorporated, CICS Systems Programmer 1979 – 1995

Installed and maintained CICS and CICS related products.

- Developed utilities to aid in problem determination and increase productivity.
- Support ad-hoc SLR reporting for CICS.
- Developed and taught part of the in-house CICS Command Level Class and a CICS Environment class. Proficient in Assembler and COBOL.

McCrory Stores, Application Programmer and Systems Programmer 1975 – 1979

Coded program modifications.

- Coded new programs as a member of a team that implemented a new Order System.
- Installed and maintained CICS and CICS related products supported TOTAL Database Software.

Resource 45

Mainframe System Programmer (IBM)

Education

- B.S., Computer Science, Pennsylvania State University

Certifications

- Certificate of Completion, ComputerTraining.com
- MCP certifications for Windows 2000 Professional and Windows 2000 Server

UNISYS

IBM

Resource 46

Mainframe System Programmer (IBM)

Key Skills and Knowledge

Platforms

- zSeries z/operating system
- operating system/390
- MVS

Subsystems

- JES2
- Parallel Sysplex
- z/operating system UNIX System Services
- Communication Server IP
- TCP/IP

Utility Software

- ServerPac
- CBPDO
- SMP/E
- HCD
- IODF
- IPCS
- TSO/ISPF
- DFSMS/DFDSS
- FDR
- RRS

Performance Software

- Workload Manager
- RMF
- SMF
- MXG
- CA-MICS Resource Management
- CA Sysview
- Omegamon

Program Products

- CICS Transaction Gateway
- WebSphere Application Server
- JAVA
- CA Multi-Image Manager
- CA Mainframe 2.0-Mainframe Software Manager
- CA SMF Director

Professional Summary

IBM zSeries z/operating system systems programmer promoting strategic business objectives by preserving a stable mainframe computing environment, meeting service level requirements, and expediting problem resolution.

Core competencies are:

- Installation and configuration of operating system software
- Performance, tuning, capacity planning and resource analysis
- Problem determination and resolution
- Implementation of new technology initiatives
- Mentoring and training other team members

Enterprise computing experience in the investment banking healthcare, software and data communications industries.

Employment History and Related Experience

CA Technologies (formerly Computer Associates), 1999 – 2010

Infrastructure Engineer, 2008 – 2010

Provided technical leadership to the systems programming and software development staffs. The level of engineering support was not routine. Research, planning, implementation and knowledge sharing was required. Evaluated new operating system and program product features. Defined and documented installation strategies and procedures. Built complex prototype environments. Provided expert technical subject matter support.

- Implemented z/operating system UNIX System Services (USS) Shared File Systems. Built sysplex test beds to verify basic configuration parameters, defined and tested standards, supported software development's QA integration testing and CA-Mainframe Software Manager r3 (CA-MSM) product development. Project was a subtask for CA's "May Mainframe Madness", a major marketing effort occurring during spring 2010.
- Prepared BPXPRMxx file sharing parameters for production implementation. Published new HFS, zFS standards and provided technical briefs for the systems programming and software development staffs.
- Researched, planned and tested SMF MVS Logger recording with existing SMF collection procedures. Published standards and procedures to the systems programming staff. Eliminated intermittent loss of SMF data.
- Wrote SMF logstream queries to identify excessive CPU users during given time slices. Analysis helped with tuning and calibrating WLM parameters. Increased system responsiveness by more evenly distributing resources.
- Prepared internal documentation for our systems programming staff and software developers. Among the titles: Installing WebSphere Application

Resource 46

Mainframe System Programmer (IBM)

Access Methods

- Virtual Storage Access Method (VSAM)
- Hierarchical File System (HFS)
- zFS
- z/operating system UNIX System Services Shared File Systems
- Access Method Services

Languages

- S/390 Assembler
- SAS
- JCL
- CLIST

Hardware

- zSeries (z9, z10)
- HMC
- Coupling Facility
- IFL
- zAAP
- zIIP

Server 5.1, Installing CICS Transaction Gateway 7.0, CA-Mainframe Software Manager Usage. Portions of the latter were adapted by the marketing staff for presentation at CA-World. Assisted staff by teaching a class, BASIC RMF MONITOR PROCEDURES.

Systems Programmer, 1999 – 2008

Served as a senior member of a world-class systems programming team providing global IT mainframe services from two geographically remote data centers. Supported z/operating system operating systems (BCP) and program products across 16 LPARs, 5 sysplexes and 3 IBM zSeries processors.

- Supported z/operating system Releases 1.1 through 1.11, installed z/operating system Release 1.4, 1.11, WebSphere Application Server Releases 5.1 through 7.0, CICS Transaction Gateway Releases 4.0 through 7.2 and IMS Releases 5.1 through 7.1.
- Provided 24/7 pager support, resolving Level 2 and 3 escalation contacts for IPL failures, operating system outages and examining SVC dumps. Opened ETRs on IBMLink, APPLY'ed APARs and PTFs.
- Diagnosed z/operating system performance problems in real time, recommended Workload Manager (WLM) changes.
- Built MIMplexes, assisted Level 2 staff with resolving cross system enqueue conflicts as they were occurring.
- Developed and delivered Resource Accounting Management Summaries to trend processor and memory utilization, extracting data from CA-MICS and MXG SAS databases.
- Installed new CA Technologies product releases and maintenance levels, assisted development with debugging and problem determination. These post-QA efforts were part of our final testing on R&D systems before GA release dates.
- Built z/operating system images, parallel sysplexes and merged the images and sysplexes into CA-MIMplexes across shared DASD farms, defined coupling facility structures, completed necessary system and PR/SM configuration parameter changes.

Office Depot, Systems Programmer II, 1997 – 1999

Provided operating system, parallel sysplex, coupling facility, performance and tuning support.

- Installed operating system/390 operating systems, APPLY'ed CBPDO maintenance levels, provided Hardware Configuration Definition (HCD) support for processor and coupling facility (CF) upgrades, including disruptive microcode CF updates in a DB2 data sharing environment.
- Collaborated with IBM Consulting Services, converting SRM IPS/ICS based performance management to WLM workload management.
- Solely and successfully restored the operating system/390 production operating systems and parallel sysplex during a declared disaster. The data

center was in the potential track area of Georges, a category 4 hurricane. Our Disaster Recovery plan (DR) was executed at SunGuard Availability Services in Philadelphia, Pennsylvania.

Rascal-Datacom (formerly Racal-Milgo), Technical Consultant/ Lead Systems Programmer, 1985 – 1996

Supervised and trained three entry-level systems programmers. Provided installation, configuration, customization, maintenance and administration of operating system software.

- Installed MVS/ESA, MVS/XA operating systems, IBM 3090 and Amdahl 6380 Processors.
- Wrote key 0 supervisor state reentrant S/390 Assembler code for SMF exits IEFACTRT, IEFUSI and RACF's ICHRCX01. Programs included SVC99, ENQ, VSAM OPEN, CLOSE, PUT, MODCB usage.
- Measured and presented system and application performance service levels, tuned SRM IPS/ICS parameters, designed and delivered processor capacity studies to management.

Memorial Sloan-Kettering Cancer Center, Senior Technical Specialist/ Lead Systems Programmer, 1983 – 1985

Managed a three member Operating Systems Services group providing MVS/SP and IBM processor support. Installed an IBM 4381 processor, built additional MVS/SP images to run the increasing production workload.

Salomon Brothers, Systems Programmer, 1980 – 1983

Installed, I/O genned and maintained MVS/SP operating systems and provided software support for IBM 3081 and 4341 processor installations

Education

- Queens College - Arts / Physics-Mathematics
- New York University School of Continuing Education

Certification

- ITIL Certified

This page intentionally left blank.

UNISYS

IBM

Resource 47

Mainframe System Programmer (IBM)

Key Skills and Knowledge

- V6R1 operating system
- BRMS
- CL Programming
- WWTS Applications

Professional Summary

Twenty-eight years of experience with iSeries, AS/400 and System/38 as a Systems Administrator.

Employment History and Related Experience

IBM, iSeries System Administrator/Focal Point,
Harrisburg, PA 1999 – Present

Responsible for system health of iSeries systems for the Commonwealth of Pennsylvania: storage, backup and recovery, device configuration, communication, networking, performance, database administration, journaling and selected elements of security.

- Responded to customer questions and issues.
- Assisted with the successful System i installation in 2009.
- Responsible for monitoring system message queues, and logs and operation and monitoring of the backup processes and alerts.
- Applied PTFs as necessary.
- Maintained technical, operations and customer support documentation.

Rite-Aid, Camp Hill, PA 1997 – 1999

Experienced in Vision Solutions HA software and BRMS. Linked AS/400 to mainframe systems for user access and data transfer.

Quaker City Paper Company, York, PA 1997

Experienced in training users for new software application and supporting hardware migration.

Harrisburg Paper Company, Harrisburg, PA 1969 – 1997

Experience in hardware and software migration and network administration as a COBOL Programmer and S/38 and AS/400 System Administrator.

Education

- Harrisburg Area Community College – COBOL programming (basic and advanced); multiple assorted PC courses; accounting; basic data networking

This page intentionally left blank.

e&e IT Consulting Services, Inc.

Resource 48

Mainframe System Programmer (IBM)

Key Skills and Knowledge

- DB2, CA-Datacom, IDMS, and native VSAM
- CICS TS V2.2 to CICS TS V2.3, TCP/IP stack
- Design and debugging support to the CICS application areas

Professional Summary

Network Administrator and Team leader. Delivers oversight of operation and tailoring of VTAM, installation and maintenance of NetView, NCP, TPX, VPS, NDM, ANET, and TCP/IP. Provided IT support for the 24 hour National Maritime Operations watch on various UNIX and Microsoft based systems; received the Navy/Marine Corps Achievement Medal for superior performance (IT work).

Employment History and Related Experience

Department of Defense; Navy Depot – Mechanicsburg 2005 – Present

Providing daily support of CICS regions and MQ subsystems, performing CICS/MQ and 3rd party software upgrades/maintenance, and performing application debugging and performance tuning

First Data Merchant Services, Senior Systems Lead Technician 2000 – 2005

Install and maintain 125+ CICS region environment across 11 MVS LPAR's.

- Installation and support for CICS, CICSPlex, and MQ Series.
- Conversion from CICS V4.1 to CICS TS V1.3
- Conversion from CICS TS V1.3 to CICS TS V2.3.
- Support for CICS 3rd party products
- Standardization of CICS and its supporting products.
- Using CICSPlex to monitoring CICS, WLM, and provide batch interfaces.
- Migration of our largest single region into an MRO environment to enhance capacity and availability.
- Migration of 11 additional CICS regions on 2 LPAR's and 2 MP3000's to the FDMS environment.

United States Navy, Office of Naval Intelligence, Washington, DC 2002 – 2003

Served on Active Duty in support of operations Noble Eagle and Enduring Freedom, provided IT support for the 24 hour National Maritime Operations watch on various UNIX and Microsoft based systems; received the Navy/Marine Corps Achievement Medal for superior performance (IT work).

United States Naval Reserve, Intelligence Specialist, Washington, DC 1998 – 2002

Intelligence Operations - Stationed at the Office of Naval Intelligence, Washington D.C. -- Classified Mission.

e&e IT Consulting Services, Inc.

Resource 48

Mainframe System Programmer (IBM)

Rite Aid Inc., Network Team Leader, Camphill, PA 1998 – 2000

Team leader, installed and maintained CICS, CICSPlex, and most of the CICS supporting products; 80+ regions that are interconnected using MRO to support almost 4000 stores.

- Migration to CICSPlex V1.3 and CICS TS V1.2.
- Implemented the CICS Web interface and created our first CICS Web application. Our primary database system was DB2 along with some native VSAM.
- Installation and maintenance of SYSM E-mail product.

Pennsylvania Blue Shield, Network/Communications, Camphill, PA

1994 – 1998

Network Administrator, operation and tailoring of VTAM, installation and maintenance of NetView, NCP, TPX, VPS, NDM, ANET, and TCP/IP using the following servers: TN3270, FTP, LPD, NFS, NPF, SMTP, and GUPTA for DB2.

- Maintained NetView 6000, CiscoWorks, Nways Campus Manager, and network monitoring on the AIX platform.
- Beta testing and setting of standards for Windows 95 & Windows NT 4.0 and in the rollout of DHCP.
- Design and rollout of the Tivoli Enterprise Management system for our Client/Server environment that consisted of AIX, NT & Novell.

Additional Employment History

- Pennsylvania Blue Shield - CICS / Medicare Database., 1988 - 1994
- GIANT Food Stores, System programming, Application programming, 1985 – 1988
- York Bank and Trust, Application programming, 1984 – 1985
- Hedstrom Co, Application programming, Operation, 1981 - 1984

Education and Training

2004	CICS Technical Conference, Las Vegas, NV
2003	IBM Education Center, Atlanta, GA – Transaction Server V2.2 migration
2002	IBM Education Center, Baltimore, MD – Transaction Server V2.2 Overview
2001	IBM Education Center, New York, NY – Transaction Server Structure & Debugging II
	CICS Technical Conference, Salt Lake City, UT
1999	IBM Education Center, Arlington, VA –Transaction Server Structure

e&e IT Consulting Services, Inc.

Resource 48

Mainframe System Programmer (IBM)

	& Debugging I
	Techknowledge Corporation, Columbia, MD – Transaction Server Overview & Migration
1998	IBM Education Center, Raleigh, NC – CICSPlex administration
1994-1999	Microsoft Developer Days
1997	IBM Education Center, Atlanta, GA – NetView for AIX administration
	Trinity Group, Raleigh, NC – Tivoli Senior System administration
	Trinity Group, Baltimore, MD – Tivoli Enterprise Console
1996	S.H.A.R.E. Anaheim, CA
	IBM Education Center, Washington, DC – AIX System administration
1995	Sterling Software, Dallas, TX – Connect-Direct (NDM)
	IBM Education Center, Raleigh, NC – SNA Graphics & Automation (NetView)
	IBM Education Center, Chicago, IL – TCP/IP for MVS administration
1994	IBM Education Center, Tampa, FL – VTAM & NCP administration
1993	S.H.A.R.E. San Francisco, CA
1992	Computer Associates, Rockville, MD – CICS/DB2 Interface
1991	S.H.A.R.E. San Francisco, CA
	IBM Education Center, Harrisburg, PA – MVS/ESA Structures
1990	IBM Education Center, Atlanta, GA – CICS Measurement and Tuning
	Online Software International, Toronto Canada – CICS MRO/ISC Communications
	H.A.C.C., Harrisburg, PA – Advanced Assembler Programming
1989	Online Software International, Atlanta, GA – CICS System Logic and Debugging
	Verhoef Information Systems, Lancaster, PA – CICS Internal Logic
1987	G.U.I.D.E. Boston, MA
1986	Harrisburg Area Community College – Assembler Programming
1984	American Institute of Banking, York, PA – Principles of Banking
1980	School of Computer Technology, Pittsburgh, PA – Computer Programming/Operations

This page intentionally left blank.

UNISYS

IBM

Resource 49

Mainframe System Programmer (IBM)

Key Skills and Knowledge

- MVS/XA, MVS/ESA, operating system/390, z/operating system
- MVS ASSEMBLER, SAS, COBOL, REXX, CLIST, FORTRAN and MVS JCL
- TMON/MVS
- RMF
- SMP/E
- RACF
- MVS/DFP Utilities
- DFSORT,SYNCSORT
- FileAid
- TSO/ISPF
- Advanced Function Printing (AFP)
- Print Services Facility (PSF)
- Document Composition Facility (DCF)
- BookMaster
- Overlay Generation Language (OGL)
- Page Printer Formatting Aid/370 (PPFA)
- AFP Workbench for Windows (a Windows based Product)
- Data Facility Data Set Services (DFSMSdss)
- Data Facility Hierarchical Storage Manager (DFSMShsm)
- Storage Technology's Host Component Software (HSC)
- Tape Library Management System (TLMS)
- IBM ATL tape hardware
- Storage Technology's Automated Cartridge System (ACS)
- Library Storage Modules (LSMs)
- EMC Symmetrix Integrated Cached Disk Array
- Hardware Configuration Definition (HCD)
- File Transfer Protocol (FTP), TCP/IP
- z/operating system UNIX Systems Services (USS)
- Abend-Aid

Professional Summary

Senior level MVS Systems Programmer with a BS in mathematics and 19 years of IT experience on the mainframe platform. Proven ability to plan and implement IT solutions.

Employment History and Related Experience

IBM Corporation, Senior I/T Specialist, Greenville, South Carolina, 2006–To Date

- z/operating system (MVS) Systems Programmer
- Systems Availability Leader

Financial Services Company, Network Specialist, 2011–2012

Provided day-to-day support for various mainframe network components such as VTAM, TCP/IP, TELNET, and FTP.

- Supported the client's disaster recovery exercises.

Financial Institution, z/operating system Systems Programmer, 2011–2011

Reviewed all of the major z/operating system subsystems and active address spaces, PROCS, PARMLIB members, PARMLIB concatenations, system page and storage configuration, IEASYSxx and LOADxx parameters, IPL startup, z/operating system SMP/E environment and general performance.

- Provided recommendations and best practices for the major z/operating system subsystems.
- Offered suggestions for z/operating system maintenance strategies and SYSPLEX configuration to prevent system outages.
- Provided options, advantages and hardware/software requirements for the proper planning/implementation of a Multiple LPAR/SYSPLEX environment.
- Recommended best practice scenarios for sharing and isolation of production and development LPARS and data.
- Reviewed current XCF policies, CF structures, GRS constructs and overall SYSPLEX health.
- Reviewed the current TCPIP stack(s), device configuration, IP profiles/parmlib members, associated IP address spaces and general configuration.
- Provided recommendations to optimize and tune the mainframe IP environment as appropriate, as well as outline the changes required to support VIPA, DVIPA and high SYSPLEX availability.
- Reviewed the current USS environment, HFS/ZFS files systems, BPXPRMxx settings and general application usage.
- Provided recommendations and best practices for maintenance, security, end user and application/subsystem support pertaining to UNIX System

Services.

- Provided a detailed overview of USS support and maintenance in a SYSPLEX environment.
- Reviewed ACS routines and ISMF constructs currently in use and provided an analysis of all system and application dataset qualifiers pertaining to SMS and non-SMS management.
- Reviewed current storage configuration by pool, volume naming convention and space management practices.
- Provided suggestions and best practice recommendations to optimize storage management where appropriate, as well as options for utilizing an SMSPLEX in either a SYSPLEX or non-SYSPLEX configuration.

Financial Institution, z/operating system Systems Programmer, 2010–2010

Performed a review of JPMC's z/operating system environment and analyzed its capabilities and architecture.

- Reviewed the utilization of JPMC's z/operating system assets and resources.
- Analyzed the zSeries operating system, the sub-systems, and the ISV software maintenance methodologies and processes for best practices.
- Produced a final report which listed recommendations and suggestions for improving the maintenance & upgrades processes and methodologies.

Telecommunications Company, Sr. I/T Specialist, 2010–2010

Analyzed coupling facility hardware for best practices.

- Recommended software configuration and Parallel Sysplex strategies in-line with IBM best practices.
- Recommended preventive and corrective actions on the Parallel Sysplex technology.
- Identified performance risks and exposures based on IBM observations and recommended avoidance strategies.
- Reviewed Sysplex maintenance strategy.
- Provided report that detailed findings, recommendations, and an improvement roadmap.

Hospital, Sr. I/T Specialist, 2010–2010

Reviewed the WLM constructs for best practices.

- Analyzed batch and on-line workloads.
- Conducted a performance review of the WLM classes to ensure performance objectives were being met.

Insurance Company, Sr. I/T Specialist, 2010–2010

Assessed processor utilization and latent demand, central storage utilization, workload utilization of system resources, response time analysis, and I/O device

utilization.

- Reviewed and analyzed the coupling facilities and FICON switches for best practices.
- Evaluated system performance.
- Conducted a performance review of the Workload Manager (WLM) constructs.
- Reviewed current z/operating system production system configuration for compliance with capacity, availability and performance.
- Conducted a review of the non-IBM Software products and provided software alternatives.
- Reviewed the current toolset / utilities used in the z/operating system environment and made recommendations for alternatives.
- Evaluated current z/operating system staffing and support levels.

Hospital, Sr. I/T Specialist, 2009–2009

Reviewed, analyzed all z/operating system third party (non-IBM) software products.

- Provided upgrade, migration and replacement recommendations for all third party z/operating system software.
- Evaluated the z/operating system software and offered recommendations on utilities that would provide benefits and increase staff productivity.
- Evaluated client's z/operating system tape environment and provided a hardware migration path that would lead to an increase in tape capacity.
- Evaluated the z/operating system and Operations staffs.
- Provided recommendations for staffing and support levels relating to z/operating system and Operations.

Insurance Company, Senior I/T Specialist, 2009 – 2009

Reviewed DFSMShsm Migration and Retention Rules in an effort to reduce data movement between primary and migration volumes.

- Reviewed RMF data to determine the performance impact DFSMShsm was having on the z/operating system system.
- Provided a list of recommendations for reducing the volume of data managed by DFSMShsm and for reducing data movement between primary and DFSMShsm managed migration volumes.
- The recommendations also included comments on best practices for reducing or eliminating thrashing.
- Assisted with the implementation of a number of the recommendations.

Manufacturing, Sr. I/T Specialist, 2008–2008

Defined the SMP/E environment and utilized SMP/E to install a number of third party software products.

- Based upon a set of client requirements, conducted research to determine the best method of cataloging tape data once the tape data set is closed. The solution required the use of the assembler programming language to create the 'File End on Volume' system exit (IFG055FE).

Manufacturing Company, I/T Specialist, 2008–2008

Conducted interviews to determine the duties and responsibilities for all members of the z/operating system staff.

- Determined the z/operating system software components and subsystems in the client's environment.
- Determined the z/operating system related hardware in the client's environment.
- Submitted a report detailing the IT environment. In addition, the report included statistics regarding the z/operating system staff.

Retail Company, Senior I/T Specialist, 2007 – 2007

Documented all system EXITS and USERMODS installed.

- Determined if EXITS and USERMODS can be migrated (either to v1.7 or to v1.9) or eliminated.
- Determined work effort involved to migrate EXITS / USERMODS to z/operating system V1.9.
- Reviewed migration requirements for major subsystems.
- Reviewed Independent Software Vendor (ISV) software migration requirements.
- Performed a high level analysis of the current zOS v1.4 environment for a migration to zOS v1.9.
- Defined roadmap for upgrade from zOS v1.4 to zOS v1.9 which included high level initiatives to accomplish the migration.
- Provided a technical document to client which summarized the z/operating system V1.4 assessment. In addition, the report contained recommendations for a migration roadmap. It also identified areas that required additional investigation.

Clinic / Hospital, Senior I/T Specialist, 2007–2007

Assisted with the upgrade of z/operating system V1.7.

- Installed a significant number of ISV products.
- Utilized FDR software to erase all data on old IBM RAMAC II devices.

Banking Client, Senior I/T Specialist, 2007–2007

Assisted with VSE-to-MVS SAS migration project.

- Reviewed SAS source and JCL.
- Implemented changes as necessary.

- Tested SAS applications in a batch environment.

Power Company, Senior I/T Specialist, 2007–2007

Performed z/operating system V1.4 healthcheck.

- Provided client with a technical report denoting all deviations from 'best practices' regarding z/operating system settings and configurations.

Power Company, Senior I/T Specialist, 2007–2007

Led z/operating system V1.4 to V1.7 migration project.

- Installed all ISV products.

Health Care Company, Systems Availability Leader, 2006–2006

Filled the role of Systems Availability Leader for a large client.

- Advised management of hardware/software availability issues.
- Worked with IBM support to quickly resolve IT related problems.

Clinic / Hospital, Senior I/T Specialist 2006–2006

Assisted with z/operating system V1.4 upgrade.

- Installed all ISV products.
- Assisted with testing of the ISV products and with z/operating system V1.4.

Manufacturing Firm, Senior I/T Specialist, 2006–2006

Generated performance reports using RMF & Omegamon.

- Evaluated performance issues in regard to z/operating system and related hardware.
- Provided client with a technical document denoting all hardware and software performance issues.

National Insurance Company, Senior I/T Specialist, 02/2006-02/2006

Generated performance reports using RMF & Omegamon.

- Evaluated performance issues in regard to z/operating system and related hardware.
- Provided client with technical a document denoting all hardware and software performance issues

Grocery Retailer Located in the South East, Senior MVS Systems Programmer, Greenville, South Carolina, 2005–2006

Installed, maintained and tested various MVS system software components and utilities. This includes IBM and third party products. Maintained the I/O configuration for the MVS system via HCD.

Resource 49

Mainframe System Programmer (IBM)

- Engaged in various MVS storage management related support activities.
- Assisted with the planning and execution of the disaster recover exercises.
- Provided management with periodic risk analysis.
- Worked with operations and with the user community to resolve hardware and software issue.

Grocery Retailer Throughout the South East, Lead Systems Software Specialist, Greenville, South Carolina, 2000–2005

Installed, maintained and tested various MVS system software components and utilities. This includes IBM and third party products.

- Using the assembler language, developed, tested, and installed various system and user exits.
- Assisted with operating system upgrades from operating system/390 V2R8 to z/operating system V1R1 and from z/operating system V1R1 to z/operating system V1R4.
- Maintained various operating systems such as z/operating system and operating system/390.
- Supported components and structures within a Parallel Sysplex environment.
- Supported disaster recovery.

A South Carolina Public University, Lead MVS Systems Programmer, Clemson, South Carolina, 1990–2000

- Responsible for the installation and maintenance of all MVS system software and utilities. This includes both IBM and third party software products.
- Supported various versions/releases of MVS/ESA and operating system/390.
- Provided software support and user assistance for all Advanced Function Printing (AFP) printers.
- Responsible for MVS storage management. This included both tape and DASD.
- Examined hardware/software issues and made recommendations to management.
- Organized and managed all upgrade projects.
- Kept management informed of all ongoing tasks and projects.
- Provided management with risk analysis. Responsible for MVS disaster recovery.
- Assisted as needed with software development and level 2 support of Expert Library Manager (ExLM). Extensive use of Hardware Configuration Definition (HCD) to define and maintain the MVS I/O configurations.

National Insurance Company, Programmer Analyst, Greenville, South Carolina, 1989–1990

Using formal written specifications, developed, tested, and installed new COBOL based medical statistical reporting systems.

Resource 49

Mainframe System Programmer (IBM)

- Maintained existing reporting systems.
- Handled client requests for special custom reports and data files.

Major Metals Manufacturer, Junior / Associate MVS Systems Programmer, Richmond, Virginia, 1988–1989

Installed, tested, and maintained MVS software. Resolved software issues. Assisted the user community as needed.

Education

BS in Mathematics, Clemson University

AA in General, Glendale Community College

This page intentionally left blank.

UNISYS

Resource 50

Mainframe System Programmer (IBM)

Key Skills and Knowledge

- Assembler Language Coding
- COBOL
- zOS Operating Systems Support
- JES2 Support and Exits
- SMP/E
- ACF2
- SDSF
- ISPF
- FDR
- FDRABR
- FDRPAS
- MSWord
- PowerPoint
- Excel
- Outlook

Professional Summary

Performed systems programming support for z/operating system, OS390 and zVM operating systems through research and development of system level software. Supported z/operating system R1.6/7, JES2 Exits, GDPS, XRC, TWS, DFSMS, FDR and CA products and various other vendor software products as an IT Specialist. Has experience as chief of a major government agency systems programming branch.

Employment History and Related Experience

IBM, Senior IT Specialist Jacksonville, Florida, 2008–To Date

Provides systems programmer z/operating system operating system support on various contracts. This support includes z/operating system, JES2, MVS and JES2 Exits, RACF, GDPS, XRC, TWS, SMP/E, HCM, HCD and IOCP, DFSMS, IBM Utilities, Assembler Language Coding, COBOL, FDR, FDRPAS and various other vendor software products.

- Has in depth experience in IBM programming languages.
- Is experienced in IBM processors, both large and medium, with some knowledge of server technology.

IBM, IT Specialist, Bethesda, Maryland, 2005–2008

As a Senior Systems Programmer, provided operating system support on contract to U.S. Department of Defense. This support includes z/operating system R1.6/1.7, JES2, MVS and JES2 Exits, RACF, GDPS, XRC, TWS, SMP/E, HCD and IOCP, DFSMS, IBM Utilities, Assembler Language Coding, COBOL and various other vendor software products.

- Provided customer support with reports, project planning and change coordination through use of many office tools, such as, MSWord, PowerPoint, Excel and Outlook. Has in depth experience in IBM programming languages and superficial knowledge of scripting languages.
- Is experienced in IBM processors, both large and medium, with some knowledge of server technology.

U.S. Department of Defense, IT Specialist, 2005 – 2008

- Provided zOS Operating System Programming to the customer. Includes SMP/E installation of the operating system and other IBM and vendor software products.
- Provided support for customer problems and issues within the scope of the contract.

TekSystems Inc., Senior Systems Programmer, Hanover, Maryland, 2003–2005

As a Senior Systems Programmer, provided sub-contractor services to IBM, Inc. on contract to the U.S. Department of Defense.

Resource 50

Mainframe System Programmer (IBM)

Imperial Systems Group LLC, Senior Systems Programmer/Owner, Silver Spring, MD, US, 1999 –2003

Provided sub-contractor services to Raytheon, Inc. on contract to the U.S. Department of Defense as a Senior Programmer and owner of Imperial Systems Group, LLC.

- Led the planning and installation of the operating system/390 Release 2 Version 10 Operating System.
- Provided technical expertise for the planning and installation of the Agency's mainframe upgrade to an IBM CMOS and a RAMAC Virtual Array Disk Subsystem.
- Experienced in SMP/E, JES2, ACF2, SDSF, ISPF, FDR/ABR, IXFP, SNAPSHOT and other IBM and other vendor software.

QSI, Inc., Senior Systems Analyst, Rockville, MD, US 1998 – 1999

Responsible for Year 2000 assessment of Montgomery County Permit System.

- Analyzed an application system coded in COBOL, IMSADF and SAS.
- Acted as the Systems Programmer for the TIS P390.
- Responsible for installation and maintenance of the operating system/390 System and various IBM and other vendor software products (e.g. CICS, SAS, and FDR).

U.S. Government, Federal Employee, Washington, DC, 1969–1997

Assigned as a Computer Programmer, Systems Programmer, Branch Chief, Systems Analyst, Project Manager, Senior Technical Officer at various U.S. Government Agencies.

Education

MS in Information Resource Management

Syracuse University, Syracuse, NY

Certification

- Certified General Services Administration "1000 by 2000", 1995
- Certified National Defense University, Advanced Management Program, 1995

UNISYS

e&e IT Consulting Services, Inc.

Resource 51

Mainframe System Programmer (IBM)

Key Skills and Knowledge

- Secret Clearance
- CICS, CICSPlex, MQSeries, DB2
- ADABAS DBMS (exits, internals and utilities)
- PLATINUM/BMC tools for DB2,
- RRDF/Log Apply disaster recovery tool
- S/370
- RACF, Top-Secret, Mac-Kinney Batch, assembler
- PL/I, COBOL, TSO/ISPF, CLISTS, SAS

Professional Summary

Skillful Subject Matter Expert for DBMS /BMC/Platinum software upgrades with SMP/E, performed BMC and Platinum installations and evaluations for proposed software, and developed software to automate routine database functions. Knowledgeable of Z/operating system, MVS/XA, operating system/390, RX3, PCs, etc.

Employment History and Related Experience

Navy Depot, CICS/MQ Systems Programmer, Mechanicsburg, 2001 – Present

Provide daily support of CICS regions and MQ subsystem, perform CICS/MQ and 3rd party software upgrades/maintenance, and perform application debugging and performance tuning

First Data Merchant Systems, CICS Senior Systems Engineer, 2001 – 2007

Provided daily support of 134 CICS regions, Performed CICS and CICSPlex software upgrades and maintenance with SMP/E, and Installed/maintained MQ Series subsystems

- Exploited CICSPlex by using its MRO monitoring and batch interface features
- Developed software to automate routine CICS functions
- Performed application debugging and performance tuning
- Interfaced CICS with DB2, CA-Datacom, and IDMS databases
- Migrated to CICS TS 1.3 and TS 2.3
- Installed MRO capabilities using CICSPlex and WLM
- Developed Web presentation of daily CICS shutdown statistics
- Developed a process to report transaction issues

Rite Aid Corporation, Database Administration/Systems Programmer, 1995 to 2001

Performed DBMS /BMC/Platinum software upgrades with SMP/E, performed BMC and Platinum installations and evaluations for proposed software, and developed software to automate routine database functions.

- Performed administration activities in support of database maintenance (PTFs)
- Conducted application performance tuning
- Migrated and maintained DB2 V4.1, V5.1 V6.1 subsystems
- Implemented UDB for NT, JDBC, and Net.Data
- Implemented a production DB2 data sharing environment

e&e IT Consulting Services, Inc.

Resource 51

Mainframe System Programmer (IBM)

CITIBANK, Senior Systems Programmer, South Dakota, 1985 to1995

Upgraded, installed, and evaluated DBMS proposed software, conducted DBMS performance and tuning, and developed in-house tools and automated database functions.

- Administered activities necessary for supporting application projects
- Provided direction and status of key projects to upper management
- Participated in group/department planning
- Assisted coworker with technical solutions for production issues
- Designed and developed multi-site ADABAS and DB2 backup and recovery
- Developed code to dynamically designate ADABAS file(s) to read-only status systems
- Developed code for capturing historical ADABAS command information

Additional Employment

- University of South Dakota, Vermillion, SD, Senior Data Processing Unit Manager, 1981 to 1985
- St. Paul CO., St. Paul MN, Programmer/Analyst, 1980 to 1981

Education

B.A., University of South Dakota, May 1980, Computer Science, minors in Business and Mathematics

UNISYS

Mainframe System Programmer (Unisys)

This page intentionally left blank.

UNISYS

Resource 52

Mainframe System Programmer (Unisys)

Key Skills and Knowledge

- UNIVAC EXEC8
- Sperry Operating System 1100 (OS1100)
- Unisys Operating System 2200 (operating system 2200)
- Sperry TELCON
- Sperry CMS1100
- Sperry Operating System 3 (operating system/3)
- DOS, MS Windows
- COBOL
- MASM
- FORTRAN
- C
- DML
- JCL/ECL
- SSG
- COMUS
- UDS
- DMS
- RDMS
- SENTRY
- SIMAN
- ED
- MCB/TIP
- WINDOWS
- WORD
- EXCEL
- ACCESS
- TELCON
- CMS1100
- DPS
- IPF
- STAR1100
- FAS
- CSC
- Control-M
- Unisys Dorado 280
- Unisys Dorado 350
- Unisys Dorado 740
- UNIVAC 1108
- Sperry 1100 Series
- Unisys 2200 Series
- Personal Computers (PCs)
- System 80
- ITIL

Professional Summary

Senior computer Analyst and Programmer with 30+ years experience in the design, development, implementation and maintenance of technology solutions for business and government. Areas of expertise include

- Implementation and maintenance of hardware and software
- Strong emphasis on operating system configuration and support routines
- Applying fixes and updates to the operating system programs
- Converting and updating user programs to utilize new environments
- Generating new applications in response to emerging requirements

Employment History and Related Experience

DPH and PSP systems at DPW, System Analyst 2 – Harrisburg, Pennsylvania, 2011-Present

Deliver systems support to the Commonwealth of Pennsylvania and Pennsylvania State Police Facility in Harrisburg, Pennsylvania for the Unisys Dorado 350 systems.

- Performed software generations to apply corrections and updates as needed
- Configured and installed third party software including STAR 2200
- Monitored daily system operations and identify and correct problems
- Installed CP12.1 release of the Unisys operating system 2200 suite of software on all DPW systems

County of Los Angeles, Unisys Operating System Specialist – Los Angeles, California, 2006-2011

Working at the County of Los Angeles Facility in Downey, California, provided support for the Unisys Dorado 280 system, generated MASM and COBOL programs to provide information and statistics about the Operating System usage and performance

- developed and installed fixes and local code for the Operating System
- Configured and installed third party software including STAR 2200, CSC and Control-M
- Provided user file maintenance using FAS to assist users in retrieving files which have been archived or to restore a file to a previous version
- Monitored daily system operations and identify and correct problems.

SITA Corporation, FORTRAN Programmer – Atlanta, Georgia, 2005-2005

Working at the SITA Facility in Atlanta, Georgia, participated in updating SITA's airline reservation system which generates and maintains e-tickets for SITA customer Airlines, modified existing FORTRAN programs to provide the new functionality.

Unisys Corporation, Principal Systems Analyst – Niceville, Florida, 1991-2004

Working at the Unisys Support Facility in Niceville, Florida, participated in numerous system updates and conversions

UNISYS

Resource 52

Mainframe System Programmer (Unisys)

- Accomplished operating system configurations and generations, provided site computer operation support.
- Developed and executed test procedures for new software and wrote numerous subroutines and functions for various software written at the Niceville facility
- Reviewed, generated, installed, tested, and implemented new releases of Unisys system software including OS2200, UCOB, UFTN, UC, DMS1100, CMS1100, MCB1100 and many others
- Helped debug problems in the system software and found and installed fixes to correct these problems

Systems Analyst – Hickam Air Force Base, Hawaii, 1990-1991

Supported the U. S. Weather station on Hickam AFB in Honolulu, migrated Sperry 1108 to the new 1100/70 machine; provided system configurations and generations, provided site computer operation support and training.

- Accomplished communications configurations and generated the communication management system
- Provided backup capabilities for the operating system, aided site Air Force personnel in writing programs to analyze weather data and prepare forecast and weather history reports
- Setup and maintained the technical library and interfaced with the Unisys support facility in Texas to identify and correct deficiencies and discrepancies in the system software and communication network.

Systems Analyst – Montgomery, Alabama, 1984-1990

Provided analysis for Unisys Support Facility in Montgomery, Alabama, participated in the migration and implementation of the Air Force Phase IV program.

- Generated numerous utilities, subroutines and functions to aid the Air Force personnel in the support of the Air Force Base Supply System, financial system and world wide data bases
- Debugging DMS programs, implementing and installing the shared tape library system, converting the Air Force data base files to the new system format when UDS was introduced
- Developed utilities to aid Air Force personnel in the maintenance of disk files and in the reading of tape files received from other bases.

Education

Business – University of Richmond

Richmond, Virginia

Associate in Applied Science – Northern Virginia Community College

Annandale, Virginia

UNISYS

Resource 52

Mainframe System Programmer (Unisys)

USAF Technical School:

♦ Electronics ♦ Programming Specialist

Unisys Corporation Education Center:

1100 Executive Control Language	1100 Series Assembler	Symbolic Stream Generator
FORTRAN Programming	DMS 1100	OS1100 EXEC Internals
Communications Concepts	1100/80 Hardware and Software	Telcon Performance and Sizing
operating system/3 Utilization	PLUS 1100 Programming	1100 META Assembler
1100 Operating System Internals	System Instrumentation and Performance Analysis	1100 Operating System Internals Introduction

Certifications

Loyalist Certification Services

ITIL Certification

Unisys Corporation

Annual Renewal – Ethics Awareness and Information Security Awareness

This page intentionally left blank.

UNISYS

Resource 53

Mainframe System Programmer (Unisys)

Key Skills and Knowledge

- Project Management
- Hardware Installation
- Dorado Mainframe Architecture
- operating system 2200 Software
- MCP Operations
- Software Upgrade
- Problem Solving
- Transaction Processing
- Technical Expertise
- OLTP
- WEBTS
- LSAM
- MAPPER
- System Performance
- SIGHTLINE Software
- Disaster Recovery
- Data Replication - SRDF
- EMC Storage
- Virtual Tape
- Cartridge Tape/SILO
- DEPCON Print Distribution
- NETWORK
- Secure FTP
- ITSM7
- ITIL V3
- Windows
- EXCEL,WORD,PPT
- VISIO

Professional Summary

Resource 38has over thirty years of experience in the data processing profession with the Unisys Corporation. He has a proven track record in installing and supporting large mainframe computer systems.

- Strong technical expertise, problem solving abilities, and leadership skills have been displayed in his support of major clients such as United Airlines, IRS, Pennsylvania Department of Public Welfare, Pennsylvania Game Commission and State Police
- Stellar system knowledge, attended numerous internal software, hardware, and management courses providing his background computer knowledge
- Tracks Emerging Technology attending workshops and seminars dealing with Unisys Clearpath Architecture and Open Systems environments

Employment History and Related Experience

Unisys Corp. ,Global Managed Services, Systems Analyst, Harrisburg, PA 2000-Present

Delivers Technical Support for several PA State Agency's which include PADPW, PA State Police, and PA Game Commission.

- Technology studies and analysis for large Mainframe Systems as well as Open System Server environments
- Integration of disaster recovery environments and maintaining Client Satisfaction to avoid SLA penalties

Unisys Corp., Computer Systems Group Project Manager, Harrisburg, PA 1988-2000

Technical Project Manager for the Unisys Computer Systems Group, managed a staff of Computer Systems 2200 Architecture Specialists at a $30 million data processing center servicing the PA Department of Public Welfare.

- Managed migrations for of mainframe, peripheral, and software environments
- Maintained nearly one hundred percent system availability

Unisys Corp., Professional Services Systems Analyst/Consultant, Harrisburg, PA 1982-1988

Supported Unisys Contract for Department of Public Welfare as a Systems Analyst. Provided Operating System, telecommunications, and MAPPER support on this multiple mainframe customer site.

UNISYS

Resource 53

Mainframe System Programmer (Unisys)

Unisys Corp., Professional Services Systems Analyst, Martinsburg, WV 1981-1982

Professional Services Analyst assigned to support a major 2200 mainframe installation project at the IRS Service Center in Martinsburg, WV.

Unisys Corp., Professional Services Systems Analyst, Chicago, IL 1979-1981

Provided Operating Systems analysis, supported 2200 mainframe upgrade project at United Airlines in Chicago, IL.

Education

- B.A. – Mathematics, Lycoming College, Williamsport, PA 1978

Training

- 2200 Mainframe Operating System; transaction processing concepts and internals
- Programming languages COBOL, MASM, and 4GL
- Communication concepts and programming
- Management courses for creative problem solving
- Interactive communications, and time management, Clearpath workshops

Certifications

- ITIL V3 Foundations
- Yearly Renewal - Ethics Awareness and Information Security Awareness

Microsoft Product Specialist (e.g., Exchange, SharePoint)

This page intentionally left blank.

UNISYS

Resource 54

Microsoft Product Specialist

Key Skills and Knowledge

- Domain Expertise & Solutions
- Exchange E-mail Consulting Services
- Operating Systems
- Software/System Architecture
- Technical Documentation

Professional Summary

Expertise and significant hands-on experience in Server Technologies such as:

- Windows 2003 advanced server.
- Windows Server 2008 R2 Server.
- Active Directory, DNS, DHCP installation, configuration, administration and troubleshooting.
- Exchange 2007 implementation, configuration, administration and troubleshooting.
- BlackBerry Enterprise server implementation, configuration, administration and troubleshooting.
- Experience in monitoring and tuning Windows server performance.
- Basic troubleshooting for hardware problems.

Employment History and Related Experience

Unisys, System Analyst (Messaging Consultant), Harrisburg PA, 2012 - Present

Provides systems analysis support for the Commonwealth Roles including tasks such as:

- Tier 2 support for Enterprise active directory domain, DNS, DHCP, GPO (Windows 2008 R2)
- Tier 2 support for Enterprise Exchange 2007, Enterprise BlackBerry Servers, and Good for Enterprise Servers
- Tier 2 support for Enterprise Exchange 2007, Enterprise BlackBerry Servers, and Good for Enterprise Servers

US Tech Solutions, System Analyst, Harrisburg PA, 2011- 2012

Provides systems analysis support for the Commonwealth Roles including tasks such as:

- Tier 2 support for Enterprise active directory domain, DNS, DHCP, GPO (Windows 2008 R2).
- Tier 2 support for Enterprise Exchange 2007, Enterprise BlackBerry Servers, and Good for Enterprise Servers
- Support for Cisco Ironport E-mail Encryption, Postini Anti-spam, and Commvault backup system

Additional Employment

- Good Shepherd Medical Care 01/2011 - 05/2011
- Summit Technology Solutions 01/2004 - 08/2010
- Orascom Technology Solutions 10/1997 - 01/2004

UNISYS

Resource 54

Microsoft Product Specialist

Education

- Bachelor of Science in Electrical Engineering (BSEE), with a major degree in telecommunication, Cairo University, 1990.

Professional Certification

- ITIL Foundation Ver. 3 (Exin, 2012).
- MCSE 2003 (Microsoft, 2006).
- Microsoft Exchange 2003 (Microsoft, 2006).

Professional Training

- Implementing Microsoft Internet security and acceleration server 2004.
- Introduction to installing and managing Microsoft Exchange 2007.
- Implementing HP ProLiant servers.
- Rapid deployment pack and ProLiant blade servers workshop training.
- Managing System Center Configuration Manager 2007 (SCCM).
- Managing System Center Operations Manager 2007 (SCOM).
- NEC Express 5800 servers and software technologies training.
- NEC backup, blade, fault tolerant and SAN storage training.

UNISYS

Resource 55

Microsoft Product Specialist (Windows & Exchange Administrator)

Key Skills and Knowledge

- Enterprise-level Windows based server environments (Windows Server 2003/2008 Server)
- Microsoft Exchange 2007(hot fixes/policy management/troubleshooting mail flows, disaster recovery)
- troubleshooting BlackBerry Enterprise Server environment (policy management/troubleshooting mail flows)
- McAfee Groupshield / EPO policies/ Postini Anti-spam Applications.
- E-mail Archiving Applications like Symantec Enterprise Evault / Google cloud based Archiving

Project and Program Management

- Excellent troubleshooting, written/oral communication and technical documentation skills
- Strong project management skills, time management

Communication and Networking

- TCP/IP, WINS, DHCP, DNS, FTP, SMTP, POP3, IMAP, NetBIOS, IIS Server

Databases

- Exchange Database

Hardware

- All Dell Servers, IBM Servers, EMC CX700

Operating Systems

- Windows 2008/2003/2000
- Windows 7 & Windows 8

System Architecture

- Windows Domain & Exchange Server

Call Center and Help Desk

Professional Summary

Over 15 years of experience in System Administration & Network Administration, led and managed technical teams. Extensive experience planning & implementing backup and recovery procedures, Solid experience with Exchange 2000 / 2003 / 2007 in a large corporate environment (103,000+ employees), strong transition experience migrating Exchange from 5.5 to 2003, 2000 to 2007.

- Experience in Windows 2008 / 2003 domain administration, SPAM and Virus Control
- Having knowledge of principles of administration of ISA server
- Installing, configuring and maintaining Windows servers operating system like Windows 2008 R2, Windows 2003/ XP.
- Windows Active Directory implementation, Active Directory & Sysvol directory replication issues
- Group Policy implementation
- Disaster recovery of database, troubleshooting A.D replication issues
- Configuring DNS, DHCP & Wins server
- Installation and configuration of McAfee Groupshield for Exchange Servers
- Disaster recovery of Exchange servers / databases
- Testing Hot fixes, rollups & service packs and applying them in production
- Root Cause Analysis of Exchange server issues
- Galaxy Commvault software (SIMPANA 7.0 with SP3) backup Technology
- Have working knowledge of Data Protection Manager 2010
- Analyzing the output of Exchange tools like Exmerge / MpsReports / EXBPA / EXPTA
- Document all incidents related to servers and applications
- Managing Dell server class rack mounted systems, Desktops and laptops

Employment History and Related Experience

Commonwealth, Office of Administration, Exchange Consultant, 2007 - Present

Supports a six member "Exchange Management Team" (EMT) which currently manages Windows 2008 Active Directory domain, Exchange 2007 e-mail servers, BlackBerry Servers for the 45 agencies of the Commonwealth of Pennsylvania including, Governor's Office, State Police, Corrections, Dept. of State etc.

- Active Directory Domain: Commonwealth of Pennsylvania Active Directory consists of a single forest with two domains in it. There are approximately 100K user accounts, 300 domain controllers spread across more than 240 active directory sites throughout the PENN state.
- E-mail servers: Exchange 2007 servers in cluster environment on 64bit Windows 2008 servers. We have around 90K mailboxes spread across ten servers. Each server has around 25 databases and in total & we manage

Resource 55

Microsoft Product Specialist (Windows & Exchange Administrator)

- Managing Call center / Help Desk Project

Technical Documentation

- Technical SOP Documents for Patch Management/Groupshield/ Disaster recovery of Exchange databases.

250 mailbox databases; supports a disaster recovery site and exchange servers handling 4.8M messages a day.

- BlackBerry: Supports the needs of around 4000 BlackBerry users.
- Supports Anti-Virus, Anti-Spam, E-mail Encryption as well as Backups / Restores of Active directory servers & Exchange databases
- Provides Tier 2 technical support to Commonwealth of Pennsylvania Agency IT Admins
- Server builds – Install and configure agency windows 2008/2003 DC's, Global Catalog servers, exchange servers 2007, BlackBerry, Commvault QiNetix backup servers, ListServ, MOM Servers
- Installed and deployed Windows 2008 R2 Servers
- Responsible for issues related to Active Directory, WINS & DNS Servers.
- Monitor and troubleshoot AD database problems with NtdsUtil, NetDiag and DCDiag tools
- Providing technical support to the end users (Agency IT admins) for Exchange 2007, DNS, SMTP, LDAP, BlackBerry, ListServ and user accounts
- Restoring AD databases in the Development and Staging labs
- Responsible for server backups and restores using Commvault Simpana Backup Application.
- Tape backup and library maintenance - Monitoring and reviewing all the successful and failed backup jobs, perform makeup jobs, Automated the cleaning of drives once every month.
- Responsible for Disaster Recovery of Exchange servers like restoring exchange databases from backup tapes & rebuilding new servers
- Identify and troubleshoot exchange information store and directory database problems
- Monitor and troubleshoot replication problems between intrasite and intersite replication issues.
- Monitoring of all our Windows 2008 servers, Exchange 2007 using SCOM.
- Carrying out Mailbox recoveries for IT Admins
- Carrying out upgrades and maintenance for Commvault Server& Media Agents
- Responsible for Service pack & patch upgrades on all servers.
- Administering day to day BlackBerry tasks.
- E-mail Account Management
- Managing, deploying and administering McAfee enterprise virus scan and ePolicy agents through ePolicy Orchestrator 4.6 Console
- Migrated the Users, Groups and the Security Translation of Workstations and Servers using ADMT tool.
- Installed, Configured and managing the different server roles of Exchange server 2007.

Microsoft CERTIFIED Technology Specialist

Resource 55

Microsoft Product Specialist (Windows & Exchange Administrator)

- Installed, Configured and managing the Exchange 2007 forefront servers as part of Exchange AntiVirus
- Installed, Configured and managing the SCR (Standby Continuous Replication) between production and DR site.
- Installed, Configured and managing the McAfee 8.5i on all the enterprise DC (289) and McAfee Group Shield on Exchange 2007 Servers.
- Responsible for testing Cloud based Google E-mail Archiving solution as part of "Proof of concept"
- Responsible for Testing on site full blown Symantec Enterprise Vault Archiving solution as part of "Proof of Concept"

Hewlett-Packard, Sr. Systems Engineer, 2005 to 2007

Delivers high level troubleshooting Exchange server 5.5, E2k & E2k3 which includes Performance related issues, disaster recovery & connectors. Maintains Windows 2000 / 2003 domains and troubleshooting issues related to Active directory maintenances, replication, group policies and DNS

- Assisting in installation and configuration of Exchange servers
- Respond to Break Fix issues by working On Call rotation after office hours
- Testing Hot fixes, rollups & service packs and applying them in production
- Deep Level Trouble Shooting of below issues
- Failure setups, Failure migrations, Disaster recoveries of Database and Servers
- Recipient policies, Rus., Mail flow issues (Internal and External)
- DNS issues, Active Directory & Sysvol directory replication
- Active directory issues related to Exchange server
- Exchange services related issues, Server performance problems.
- Anti-Virus issues and Spam Control, Replacing the exchange hardware
- System policies, Single mailbox recovery, Public folder replication
- Offline address book generation, Outlook Client Connectivity issues
- OWA issues, Root cause analysis, GAL synchronization issues
- Connectivity issues with GC (Ds Access issues)
- Configuring Connectors

Microsoft Technologies, Tech Consultant, 2002 to 2005

Provides troubleshooting Exchange server 5.5, E2k & E2k3 issues along with windows 2000 / 2003 Active directory and DNS

- Failure setups, Failure migrations, Disaster recoveries of Exchange servers and Databases
- Installation, configuration and maintenance of Active Directory domains
- Outlook / OWA connectivity issues, Recipient policies, RUS
- Mail flow issues (Internal Mail flow Only), DNS issues related to mail flow
- Active Directory issues related to Exchange server, Exchange services related issues
- Replacing the exchange hardware
- Applying Hot fixes, rollups & service packs

Microsoft CERTIFIED Technology Specialist

Resource 55

Microsoft Product Specialist (Windows & Exchange Administrator)

- System policies, Single mailbox recovery, Offline address book generation
- Public folder replication
- Performance related issues

General Electric, Team Lead, 2000 to 2002

Delivered Facilities Management Service for GE Capital International Services site consisting of about 4000 users and about 60 servers; provided System Administration of Windows NT Server, NT & 2000 clients; and installed and configured NAV server and clients.

- Installed and configured Network Print servers.
- Implementing Fault tolerance methods like Raid 1 & Raid 5.
- Configuring DNS, WINS and DHCP Services of Windows NT & 2000
- Taking care of escalation calls in providing Level 2 support
- Support and administrate Application Software like Mainframe Applications (EPC, Citrix, Clarify), Terminal server clients, etc., Network file/print services and Client applications.
- Configuring & Maintaining Outlook clients; troubleshooting user problems related to Internet/Intranet
- Performing software installations, upgrades, and patches and evaluates Existing technologies and recommending new technologies.
- Configuring and providing support to LAPTOP users on VPN connectivity.
- Exposure to repairing Dell PCs such as Dell Optiplex GX –1, GX-110, GX – 150, GX-60, Dell Laptops such as Latitude 510 / 610, Latitude L-400 & IMB Lap Tops such as ThinkPad R40 Series and also co-coordinating with Vendor for Hardware Problems if any.
- Exposure to troubleshooting and repairing of Computer Peripherals.
- Manage, coach and mentor the Support engineers in the delivery of appropriate Service Levels to the client community, proper problem solving, crisis/escalation management & manage resources accordingly.
- Perform personnel administration tasks as necessary, including resource management, time tracking, time sheet administration, interviewing, and staffing. Set service level targets for the Production Support team.
- Oversee the review of alert/escalation levels within the products.
- Continually review and improve call escalation process, incident management process, problem management process, proactive monitoring process, Exchange change control process

Adroit Info Systems Ltd., System Administrator, 1999 to 2000

As a system administrator, was responsible for installation, configuration and maintenance of all servers and workstation machines.

- Installation, configuration & maintenance of Exchange server 5.5
- Created mail boxes for 45 user accounts, configured the limits for the mailbox.
- Configured Mail box manager Policy
- Backup and restoration of database
- Single mail box recovery and disaster recovery
- Implemented Directory Replication in WINDOWS NT 4.0.

Resource 55

Microsoft Product Specialist (Windows & Exchange Administrator)

- Responsible for installation & configuration of Network consisting Network of 27 nodes with an NT SERVER 4.0, 2 NT -BDC AND 24 Clients inclusive of NT WORKSTATIONS & Windows 98.
- Configured DHCP, DNS & WINS Servers.
- Installed local & Network Printers. Printer pool and auditing of Printers.
- Applied hot fixes, rollups & service packs as and when needed

Vision Computers (A Training Institute). Technical Administrator, 1997 to 1999
Delivered daily Systems Administration for Win NT 4.0, Win 98, and Win 95. Installed, configured, and maintained Windows NT servers for development purpose locally. Responsible for updating the Operating System & Anti-Virus patches; provided troubleshooting Hardware/Software and network connectivity issues.

Education

- Bachelor in Engineering (B.E)

Certifications & Achievements

- Microsoft Certified Technology Specialist in Configuring Exchange Server 2010 (70-662)
- Microsoft Certified Technology Specialist in Configuring Exchange Server 2007 (70-236)
- ITIL Certified in May 2012
- Certified MCSE in Windows 2003
- Certified MCSE in Windows NT 4.0
- Bagged a prestigious Hewlett Packard Award for resolving a high impact issue at the client end.

This page intentionally left blank.

UNISYS

Domino Technologies Inc.

Resource 56

Microsoft Product Specialist (SharePoint)

Key Skills and Knowledge

Operating Systems and Networks

- Windows NT/2000, 2003, 2008 • Windows XP 98, 95, 3.1 • Linux • FreeBSD • Macintosh

Applications

- Active Directory • MS Operations Manager • MS SQL • IBM WebSphere • Remedy • VMware
- Microsoft Office Suite • Visio • MySQL • Exchange Server • ISA Server • Symantec Ghost •
- Acronis True Image
- Windows 2000/2003/2008 installation and configuration, hard drive installation and array configuration, software setup and configuration, updating inventory, and also documenting the entire process
- Microsoft System Installation/Management
- Microsoft SharePoint Server
- Hardware Troubleshooting
- LAN/WAN Connectivity
- Applications Instruction/Training
- DHCP Configuration
- DNS Maintenance
- Microsoft Network Design and Implementation
- Active Directory
- System Backup
- System Conversions
- WLAN Administration
- Disaster Recovery
- Downtime Reduction

Professional Summary

Microsoft Certified Systems Engineer with over ten years of experience in customer-oriented fields, including client support, system administration, and Internet help desk. Demonstrated outstanding ability to analyze and problem solve. Possesses excellent leadership qualities as well as strong customer service and interpersonal skills that focus on team work, team-building and motivating others.

- Microsoft System Installation/Management
- Microsoft SharePoint Server
- Hardware Troubleshooting
- LAN/WAN Connectivity
- Applications Instruction/Training
- DHCP Configuration
- DNS Maintenance
- Microsoft Network Design and Implementation
- Active Directory
- System Backup
- System Conversions
- WLAN Administration
- Disaster Recovery
- Downtime Reduction

Employment History and Related Experience

Domino Technologies, Commonwealth, Network Engineer, Harrisburg, PA, 2006-Present

Daily maintenance of IBM and Dell server hardware in a 24/7 environment that included disk space management, CheckPoint Firewall backups, security patch deployment, virus updates, and monitoring of hardware status and server uptime

- Server building which consisted of racking servers, cabling, Windows 2000/2003/2008 installation and configuration, hard drive installation and array configuration, software setup and configuration, updating inventory, and also documenting the entire process
- Installed and administered Microsoft SharePoint server used by several applications at PennDOT
- Assistance in various tasks which included the use of tools such as Microsoft SMS, Avocent DSView and RDP to manage servers and workstations in remote locations

- Working on various projects which include Active Directory account management, 2003 Terminal Services, SAP, and Access database updates
- Managing, maintaining and setting up printers and print servers, including IP address management and assignment, driver installation, print queue configuration and troubleshooting daily issues
- Responsible for troubleshooting failed server hardware on IBM System X and Dell Power Edge servers and also the applications running on these servers to resolution

Cilicon Solutions, Engineer, Harrisburg, PA, 2006-Present

Installation, configuration and troubleshooting of Cisco 2800 series routers; installation and configuration of POS systems at client sites; and Site survey and rollout, surveying all equipment on site, such as computers, routers, printers, and possibly remote terminals and then installing replacement equipment of the same type

- Repair of drawers and console such as the McKesson Accudose Rx Machines and other emergency room Rx machines

Sentinel, Network Administrator, Harrisburg, PA, 2006 - 2006

Maintained, upgraded and configured an 802.11g wireless network at multiple sites, including over 200 Cisco Aironet 1200 access points, and over 500 wireless clients secured using Cisco Secure ACS software running on Windows 2000 Server.

- Patched and upgraded servers and clients
- Upgraded Cisco IOS firmware on all Cisco products
- Handled helpdesk calls related to the wireless network
- Client rollout and configuration on a Novell network
- Performed network monitoring and data analysis across the entire network composed of Cisco Catalyst 2900, 3500, 4500 and 6500 series switches

Coffee Time, Systems Administrator, Harrisburg, PA, 2005 - 2005

Manage workstations and servers within the domain, including domain controllers, application servers, an e-mail server running MS Exchange 2003, and a database server running MySQL.

- Complete design and implementation of a secure Windows Server 2003 Active Directory network environment
- Developed a new network infrastructure to interface with Pocket PC computers

Resource 56

Microsoft Product Specialist (SharePoint)

- Network security design and implementation, which included workstation and server security, and CheckPoint firewall setup

JFC Staffing Associates, Consultant, Harrisburg, PA, 2004-2005

Supported clients with hardware and software issues, over the phone and in-house

- Performed workstation configuration, which included, network configuration, hardware installation/configuration and software installation/configuration.
- Hardware included Dell and Compaq workstations, Cisco Catalyst 3500 series switches and 802.11b Avaya access points

Education

- The Pennsylvania State University, Bachelor of Information Science and Technology, In progress
- American Intercontinental University, Associate of Business Administration - Information Systems

Certifications

- Microsoft Certified Systems Engineer – 2003 Server
- Comp TIA A+ Certified

This page intentionally left blank.

UNISYS

Resource 57

Microsoft Product Specialist

Key Skills and Knowledge

- Excellent and Knowledge skills in the following:
- Windows 2008/2003/XP, Exchange 2010/2007/2000, CommVault, Legato 6.x, MOM 2005/2000, Altiris, Novell 4.x, BlackBerry, Good for Enterprise, ListServ, McAfee Enterprise Virus Scan, ePolicy Orchestrator, Symantec EVault, Google E-mail Archiving

Domain Expertise & Solutions

- Commonwealth of Pennsylvania, Implemented the backup and recovery procedures for the enterprise with Commvault

Management Consulting Services

Project and Program Management

Communication and Networking

- TCP/IP, WINS, DHCP, DNS,
- IPX/SPX, FTP, SMTP, POP3, IMAP,
- NetBEUI, NetBIOS, IIS Server, LPD, IPX Print Servers

Databases

- SQL Database, Exchange Databases

Hardware

- All Dell Servers, IBM Servers, EMC CX700

Professional Summary

15 years of experience as a System Engineer and System Administrator. Possesses strong experience with Microsoft network technologies such as MCTS (Windows 2008), MCTS, and MCITP (Exchange 2010/2007); ITIL V3 Certified, MCSE 2003, MCSE 2000, MCSE NT4.0, MCSA 2003 Messaging, MCP Exchange 2000/5.5. Strong experience with the installation, configuration management, performance tuning, and security maintenance of Windows Domain Controllers. Subject Matter Expert for Exchange Servers 2007/2000, Commvault QiNetix Backup Server (9.0 SP7b), Commvault QiNetix Media Agents, BlackBerry, Good for Enterprise, Altiris 6.8, Microsoft DPM (Data Protection Manager), EMC Legato, McAfee Enterprise Virus Scan, EPO management and ListServ in the large and medium size enterprise level.

- Hands on experience in managing users, computers, sites, domains, and organizational units (OU) in the Active Directory.
- Intensely used the Active directory tools for troubleshooting such as NTDSUtil, ReplMon, NetDiag, DcDiag, RepAdmin, SONAR etc.
- Strong experience in implementation and administration of DNS, DHCP, WINS and TCP/IP
- Strong experience in implementing and managing the SAN backups both for Legato and Commvault Backups.
- Strong experience in implementing, administration and recovering of Exchange2007
- Strong experience in recovering Windows operating system, System States, Exchange Database Servers 2007 and Mailbox recoveries
- Experience in managing server resources, Hard disks, Raids, Data SAN Storage EMC CX700 and disaster recovery.
- Strong experience in deploying McAfee enterprise virus scan and ePolicy agents through ePolicy Orchestrator 3.6.0 Console
- Excellent Hardware and Software troubleshooting skills
- Migrated Users, Groups and the security translation of Workstation and Servers using ADMT tool
- Successfully tested and deployed the beta version of DPM (Data Protection Manager) in the lab
- Installed and Configured the different server roles of Exchange server 2007 SP3
- Hands on experience on MSCS. Configured and Managed the Exchange 2007 A/A/P clusters.
- Configured the Exchange 2007 SCR between the staging and DR site and production and DR site.
- Deployed and Configured Google E-mail Archiving Solution
- Responsible for testing Cloud based Google E-mail Archiving solution as part of “Proof of concept”

UNISYS

Resource 57

Microsoft Product Specialist

- Responsible for Testing on site full blown Symantec Enterprise Vault Archiving solution as part of "Proof of Concept"

Employment History and Related Experience

Commonwealth of Pennsylvania (Governor's Office of Administration), Exchange Consultant, 2002 - Current

Supports the migration of different mail systems being used by 45 agencies of the Commonwealth into a Single Enterprise wide Exchange Mail system. Its main goals are to provide consistent, reliable and secure platform for communication for around 100K users and also to have centralized administration from a single site.

- Active Directory Domain: Commonwealth of Pennsylvania Active Directory consists of a single forest with two domains in it. There are approximately 100K user accounts, 300 domain controllers spread across more than 240 active directory sites throughout the PENN state.
- E-mail servers: Exchange 2007 servers in cluster environment on 64bit Windows 2003 servers. We have around 90K mailboxes spread across ten servers
- BlackBerry: Support around 4000 BlackBerry users; provide Anti-Virus, Anti-Spam, E-mail Encryption as well as Backups / Restores of Active directory servers & Exchange databases.
- Providing Tier 2 technical support to Commonwealth of Pennsylvania Agency IT Admins
- Server builds – Install and configure agency windows 2008/2003 DC's, Global Catalog servers, exchange servers 2007, BlackBerry, Commvault QiNetix backup servers, ListServ, MOM Servers
- Installed and deployed Windows 2008 Domain controllers
- Prepared the document and tested the schema upgrade for Windows 2008 in the lab that need to be deployed in the production
- Providing operational support of Active Directory, WINS, DNS, LDAP, SMTP, POP3/IMAP, FTP and AD enabled applications
- Monitor and troubleshoot AD database problems with NtdsUtil, NetDiag and DCDiag tools
- Actively monitor the EMC CX700 SAN Storage. Troubleshoot the problem whenever a drive fails.
- Providing technical support to the end users (Agency IT admins) for Exchange 2007, DNS, SMTP, LDAP, BlackBerry, ListServ and user accounts
- Restoring AD databases in the Development and Staging labs
- Intensely used CommVault QiNetix for server backups and restores
- Tape backup and library maintenance - Monitoring and reviewing all the successful and failed backup jobs, perform makeup jobs, Automated the cleaning of drives once every month.

UNISYS

Resource 57

Microsoft Product Specialist

- Taking care of restoring file systems and exchange databases on the production servers
- Identify and troubleshoot exchange information store and directory database problems
- Monitor and troubleshoot replication problems between intrasite and intersite replication with the help of ReplMon and SONAR tools
- Monitoring of all our Windows 2008 servers, Exchange 2007 using SCOM.
- Carrying out Mailbox recoveries for IT Admins
- Resolving Database issues for Exchange servers
- Carrying out upgrades and maintenance for Commvault QiNetix Server, Media Agents and Client iDataAgents (Backup software)
- Carrying out software upgrades, maintenance and troubleshooting for Windows 2008 and Exchange Servers 2007
- Administering and troubleshooting the BlackBerry issues, adding users etc.
- E-mail Account Management
- Prepared the lab mirror to production data with the Microsoft Virtual Server and installed about 10 virtual machines and tested the upgrades and security patches before applying to the production servers
- Managing, deploying and administering McAfee enterprise virus scan and ePolicy agents through ePolicy Orchestrator 4.6 Console
- Tested and upgraded the Altiris Deployment Server 6.0 to Altiris 6.8 SP1.
- Successfully tested and deployed the beta version of DPM (Data Protection Manager)
- Migrated the Users, Groups and the Security Translation of Workstations and Servers using ADMT tool.
- Deployed Ultrasound tool in an enterprise in order to monitor the file replication in AD and to troubleshoot the issues arising due to Morphed directories
- Installed, Configured and managing the different server roles of Exchange server 2007.
- Installed, Configured and managing the Exchange 2007 forefront servers as part of Exchange AntiVirus
- Installed, Configured and managing the SCR (Standby Continuous Replication) between production and DR site.
- Installed, Configured and managing the McAfee 8.5i on all the enterprise DC (289) and McAfee Group Shield on Exchange 2007 Servers.
- Deployed and configured Google E-mail Archiving solution during this project
- Currently working on deploying Symantec eVault archiving solution at Commonwealth of Pennsylvania

UNISYS

Resource 57

Microsoft Product Specialist

Tek Systems Inc., Consultant, State Government and Exchange project, 2001-2002

- Same project s above, different employer.

COMPAQ IT Solutions Inc., GAP, System Administration, 2000-2001

Supported 900 high-end Compaq servers with more than 200,000 users globally with mixed environment of Sun Solaris, Windows NT 4.0 and Novell (4.x, 5.0). Systems monitoring for production servers within Novell, Lotus Notes and Windows NT 4.0 environments.

- Supporting TRC with level two services for help desk questions and other IT groups.
- Supporting Hardware and Software services (includes operating system patches and Upgrades) for Novell, Lotus Notes and Windows NT.
- Maintenance of Servers (Includes Server Disk Drives, Server Memory and Data Migration) under different environments.
- Implementing and deployment of services for systems configuration (includes building of new systems and modifying existing systems).
- Implemented standard backup and recovery routine using ARCSERVE 6.5 software and supporting the Storage Library Modules (9730, 9710), TL891 Mini Library System
- Administering and supporting different operating systems locally as well as remotely through PCAnywhere and rconsoling the Novell servers.
- Implemented Gigabit Networks and upgraded all the servers with Gigabit Adapters.
- Presently testing the migration of NT servers to Windows 2000 and Lotus notes to Exchange 2000.

Al-Khaleej Computers & Electronic Systems, Systems Engineer, Riyadh, Saudi Arabia, 1997 – 2000

As Rapid Deployment Program (RDP), studied the existing network and upgraded 250 desktops and 30 servers to 2000 platform. The project involved a systematic migration of desktops 9x to windows 2000 professional and Windows NT 4.0 to windows 2000 Advanced Server. Transferring skills on windows 2000 was also part of RDP

- Implementation, Installation, Upgradation & Configuration of Operating Systems (Windows 2000 Advanced server/Professional, Windows NT Server, Workstation, Sco-UNIX, Windows 9x).
- Designed and implemented physical and logical structure of Active Directory (Sites, Domains, OU's, Trees and forests).
- Implemented and delegated controls in Dynamic DNS.
- Implemented fault tolerance and disaster recovery techniques for Active Directory.

UNISYS

Resource 57

Microsoft Product Specialist

- Installed and Configured Active Directory Connector (ADC) for directory synchronization with Exchange Server 5.5 directory.
- Installation, Configuration and Disaster recovery of Exchange servers 5.5 in Exchange organization of 5000 users that includes 3 sites with 10 servers.
- Digital clustering 1.1 for Windows NT using RAID Array 310 Deskside subsystem. Single pedestal (SWXRA-Z1) server 3 1/2 SBB's to differential SCSI bus converter.
- Installation and configuring of Primary and Secondary SMS sites, Hardware Inventory, Software Inventory, Software distribution and remote control using SMS 2.0.
- Troubleshooting SMS through event viewer and System Status Messages.
- Installation, Configuration and troubleshooting of Plexus Imaging Software (Object Server /Storage Manager)
- Installation of Image Basic (DHS), imaging software on client machines.
- Installation of Oracle Developer/2000 and configuring and troubleshooting clients database connectivity issues.
- Configured Windows NT Servers as PDC and BDC in a Multi Master Domain Model.
- Implemented and Monitored trust relationships between Windows NT domains
- Setting up rights, permissions and implementing security for centralized administration.
- Installation of HP Jet Direct (NIC) printers and Network printers.
- Implemented DHCP, WINS and DNS Server for automatic IP addressing and name Resolution.
- Implemented a Small Business Server Network with 25 CAL (which includes modem sharing, fax sharing, internet sharing etc.

Integrated Data Systems, Customer Support Engineer, India, 1995 - 1997

Accomplished Server Installations, Client Installations both in NT and Novell NetWare; implemented messaging using Exchange server 4.0 for various clients. Created users, groups, and assigned rights to them.

- Installed Network, Remote printers and configured remote booting.
- Installation and configuration of various applications
- Installations, upgradations, configuring, performance tuning and support for various operating systems.
- Recovered Data from crashed hard disks by manually writing Boot sector Information and Partition Tables.
- Troubleshooting Modems, printers (Dot Matrix, Laser), Multimedia etc

MidEast Data Systems, Systems Administrator, Abu Dhabi, UAE, 1994 - 1995

Installed and administered Windows NT 4.0 in a Domain environment. Also installed Novell NetWare 4.1 and 3.12 servers and configured NT as Gateway for NT clients to access NetWare resources. Designed, Implemented and

administered NDS, Managed Partitions and replicas, solved NetWare volume related problems; migrated users, accounts, and data from Novell NetWare to Windows NT system.

- Installed Network Printers and implemented Remote Booting on both Windows NT and NetWare.
- Carried out Mirroring and Duplexing of partitions on NetWare servers.
- Provided Internet access to every desktop using Proxy server.
- Carried out tuning, and optimization of NT and NetWare Servers.
- Responsible for monitoring and regulating network traffic on NetWare and Windows NT networks

Frank Computer Services, Customer Support Engineer, 1993-1994
Installation, Administration, Fine-tuning and Maintenance of NT 3.51 Networks configured as PDC, BDC and member servers in a Domain environment.

- Carried out and supervised the layout of coaxial and UTP cabling for Ethernet Network.
- Installation & Maintenance of hardware, procuring and testing of new hardware and software

Education

B. S (Electronics), Hyderabad, A.P., INDIA

Certifications

- ITIL V3 Foundation Certified – 05/07/2012
- Microsoft Certified Technology Specialist (MCTS) in Windows 2008 and Exchange 2007
- Microsoft Certified IT Professional (MCITP) in Exchange 2007
- Microsoft Certified Systems Engineer Windows 2003
- Microsoft Certified Systems Administrator in Windows 2003 and Messaging in Exchange 2003 Server
- Microsoft Certified Systems Engineer + Internet (MCSE+I), both in NT 4.0 and Windows 2000
- Installing, Configuring, and Administering Exchange 2000 Server
- Implementing and Supporting Microsoft Exchange Server 5.5
- Certificate in Novell's Installation & Configuration module of CNE 4.x.
- Legato Certified Networker 6.x Administrator for Windows

Professional Training

- Attended the training for CommVault Qinetix 4.2, CommVault Systems, Oceanport, NJ
- Attended the training for Exchange Server 2003, New Horizons, Mechanicsburg, PA
- Attended the training in Implementing and Supporting Microsoft Systems Management Server 2.0

UNISYS

Resource 57

Microsoft Product Specialist

- HP Open View Software Distributor from HP, sponsored by Al-Khaleej Computers & Electronic Systems, Riyadh, Saudi Arabia.
- Attended training in Plexus Imaging Software, BancTec, sponsored by Al-Khaleej Computers & Electronic Systems, Riyadh, Saudi Arabia.
- HP STAR Desktop and Mobile PCs Sales Professional

This page intentionally left blank.

UNISYS

Resource 58

Microsoft Product Specialist

Key Skills and Knowledge

- Domain expertise & solutions
- Management consulting services
- Project and program management
- Communication and networking
- Databases
- Hardware
- Operating systems
- Software/system architecture
- Programming languages and tools
- Call Centers and Help Desks
- Office productivity tools
- Technical documentation
- Facilities management

Professional Summary

Senior IT Consultant with 14 years of experience in delivering Windows client/server platforms and solutions; extensive experience with IIS, SharePoint, BizTalk, and Threat Management Gateway/ISA applications; and skilled project manager and systems analysis leader.

- SharePoint Portal server administrator; create and administer Web apps and site collections along with Commonwealth Technology Center server's presence; rolled out new applications; ensure that the server and application user/administrator interface and experience are at optimal levels.
- Business coordinator during the entire development process; determined user and business functional requirements and translated them to specifications used for enhancements to a system or for new development.
- Worked closely with teams of developers from various business units to facilitate the upgrade and implementation of enterprise-wide applications. Assisted in securing, streamlining, and integrating the underlying business logic, message processing, and middle tier/backend communications of the deployed applications.

Employment History and Related Experience

Unisys Corporation, Commonwealth of Pennsylvania, Senior Consultant, Harrisburg, PA — 2010 – Present

As an applications management deployment lead, fully responsible for the Internet presence of all departments and agencies housing their sites and applications at the Pennsylvania Enterprise Data Center.

- Support a three-tier environment of more than 4,000 servers and 600 Web sites and applications.
- Work extensively with BizTalk 2010, WSS 3.0, Windows 2008 Server, IIS 7.5, and other Web-integrated technologies on presence, format, and presentation.
- Configure and administer IIS 6.0 and 7.5 to facilitate maximum uptime and performance.
- Create and administer Web apps and site collections along with Commonwealth Technology Center server's presence. Roll out new applications; ensure that server and application user/administrator interface and experience are at optimal levels.
- As a BizTalk 2010 administrator, deploy and configure applications; ensure server and application uptime. Research and troubleshoot problems; implement the latest patches and updates to currently deployed applications.

UNISYS

Resource 58

Microsoft Product Specialist

Explore Information Services, Business Systems Analyst,
Marshall, MN 2005 – 2009

Lead analyst on various projects for an insurance information provider with 80 employees and $65 million in revenue.

- Liaised with the business during the entire development process. Determined user and business functional requirements; and translated them to specifications used for enhancements to a system or for new development.
- Created documents and diagrams for test cases, use cases, and data process flows.
- Gathered project estimates of development hours, software, and hardware costs.
- Built logical models; provided high-quality of documentation for system design and development.
- Main focus was a successful product deployment while meeting standards, budget requirements, and deadlines.

Unisys Corporation, The Schwan Food Company, Senior Systems Engineer,
Marshall, MN 2003 – 2005

Administered, upgraded, deployed, and maintained corporate BizTalk 2002 and 2004 and MEI and CRM environments.

- Worked closely with teams of developers from various business units to facilitate the upgrade and implementation of enterprise-wide applications. Assisted in securing, streamlining, and integrating the underlying business logic, message processing, and middle tier/backend communications for the deployed applications.
- Acquired knowledge of application interdependencies, including MSMQ 1.0 and 3.0, IIS 5 and 6, SQL Server 2000, and COM+.

Unisys Corporation, Commonwealth of Pennsylvania,
Senior Consultant, Harrisburg, PA 2002 – 2003

Member of an applications management team fully responsible for the Internet presence of all departments and agencies housing their sites and applications on the Pennsylvania Enterprise Server Farm.

- Supported a three-tier environment of more than 250 servers and 150 Web sites.
- Worked extensively with Microsoft Application Center Server, Microsoft SQL Server 2000, Microsoft SharePoint Portal Server 2001, Microsoft Operations Manager, and PPT Dynamic Site Framework (DSF) for Web sites along with other Web-integrated technologies for presence, format, and presentation.
- Configured and administered IIS 5.0 and SQL 2000 servers to facilitate maximum uptime and performance.

UNISYS

Resource 58

Microsoft Product Specialist

- Functioned as a SharePoint Portal server administrator. Created and administered workspaces and the Commonwealth Technology Center servers' presence. Rolled out new workspaces; ensured that the server and workspace user/administrator interface and experience were at optimal levels.

Corporate Network Solutions, Network Engineer II,
Phoenix, AZ 2001 – 2002

Managed, maintained, upgraded, and administered client networks ranging from small business to mid-sized corporations.

- Functioned as project manager on various assignments, including the setup, testing, and integration of EDI at Fortune 500 and nationwide air freight companies. Lead engineer on a corporate infrastructure upgrade to Windows 2000 Active Directory platform including Exchange and SQL 2000.

Cunningham Technology Group, Systems Engineer,
Phoenix, AZ 2001 – 2001

- Designed and implemented the infrastructure and system components necessary to support local and enterprise-wide business needs and solutions for clients.
- Assessed network needs. Wrote proposals for suggested improvements in architectural design, system implementation and deployment, application configuration, and performance enhancements.

ProNet Solutions, Senior Consulting Engineer, Phoenix, AZ 2000 – 2001

Ensured the highest level of technical expertise and customer service was provided and maintained while functioning in a Tier 2 support position.

- Improved the efficiency and effectiveness of clients by proactively administering and supporting their PC and networking needs.
- Functioned as team lead on assigned projects; acted as escalation point for technical and customer service issues.

Integrated Information Systems, Senior Consultant,
Phoenix, AZ 2000 – 2000

System and security architect for a multiple international domain network.

- Administered rules and security policies on local and remote CheckPoint firewall modules to supply safe and secure internetwork and intranetwork communication and data integrity.

Raymond James Consulting, Sr. Network Administrator,
Denver, CO 1998 – 2000

Lead administrator for a Microsoft NT multiple-domain network. Supported 20 servers and 250 client computers, including desktop and laptop computers.

UNISYS

Resource 58

Microsoft Product Specialist

- Configured, supported, and upgraded, as needed, the following network services: File/Print, WINS, DHCP, RAS, Exchange 5.5 Server, IIS 4.0, Microsoft SQL 6.5 Server running intranet applications, and SQL Server running custom production applications.

Education

B.A., General Studies, University of Iowa, 1990

Professional Certification

- Windows 2003 MCSE, 2010
- Windows 2000 MCSE, 2002
- Windows MCSE + Internet, 1999

e&e IT Consulting Services, Inc.

Resource 59

Microsoft Product Specialist (SharePoint)

Key Skills and Knowledge

- PA Commonwealth experience
- SharePoint Server 2010
- SharePoint Server 2007 (MOSS 2007)
- SharePoint Designer 2007 and 2010
- CRM Consultant
- C# and .NET development skills

Professional Summary

More than five years of IT experience in analysis, design, development, management and implementation of various stand-alone, intranets, client-server and Web-based software applications using Microsoft technologies including SharePoint 2010, MOSS 2007, SPS 2003, WSS 2.0/3.0, .NET Framework 3.5/3.0/2.0/1.1,WWF and C#,AJAX,SQL Server 2008/2005, and XML.

Employment History and Related Experience

PLCB, Share point Developer and System Administrator PA, 2012 to Present

Supported application development for 600 plus retail outlets. Application support involves administration and development work in SharePoint, workflows, customization with Plugins, and JavaScript.

- Actively involved in activities among all four teams including requirement gathering with business users, training and mentoring of employees
- Selected Audience includes Store users, Approvers, IT Team
- Developed the CRUD methods in C# and .NET for all the plugins used in the application
- Created multiple external content types and external lists using SharePoint Designer 2010
- Created users/groups in active directory along with assigning permissions to them while accessing CRM
- Extensively used Workflows
- Created User Profiles for each department individually to each member
- Environment: MS Dynamics CRM 2011, SharePoint 2010, C#, ASP.NET 3.0 , ADO.NET, MS SQL Server 2005/2008, Visual Studio 2010 ultimate, .NET, XML, CSS, BIDS, J Query, JavaScript, Active Directory Service

Home Depot, Share point Developer/Administrator, GA, 2011 to 2012

Worked several projects addressing Task and Workflow Management(TWM) for SharePoint site and to migrate all the contents of the site from MOSS 2007 to SharePoint 2010.

- Actively involved in activities among all four teams including deployment, creation of sites, giving access permissions for selected Audience and development.
- Selected Audience includes Admin users, Super users, Corporate users, Executive Sponsors, Field users and Store users.
- Actively involved in the development of Admin service from writing the code to unit testing and deployment.
- Developed the CRUD methods in C# and .NET for all the Admin links used on the TWM site.

- Created multiple external content types and external lists using SharePoint Designer 2010.
- Created users/groups in active directory along with assigning permissions to them while accessing SharePoint Site
- Customization of Web parts, Tool Parts, Event handlers, Features, List definition, Site definition, Site Templates, Content types and Deploying Solution packages, Document libraries, Lists, Integrating InfoPath Forms and Workflows using CAML and Microsoft Visual Studio Windows Work Flow Foundation(WWF)
- Extensively used Workflows in MOSS 2007 and SharePoint 2010.
- Wrote custom JQuery scripts to allow users to collapse and expand sections of the TWM UI
- Created User Profiles/My Sites for each department individually to each member
- Developed Solution Deployment Packages(WSP) and deployed in to the Share Point as a Feature
- Developed a Feature in the SharePoint to copy the documents from all Document Library's to one central Document Library
- Utilized Microsoft Team Foundation Server to manage the team's software development lifecycle.
- Branded the SharePoint portal and Team sites using the CSS and SharePoint designer 2010 to have a consistent and uniform look throughout the portal.
- Developed Admin Web Services to retrieve data from the SQL Server Backend and to display the data in the current site Custom List
- Worked with the team to solve the share point open issues and actively involved in fixing the issues related to the UI, Data retrieval, and adding new functionality as per the business.
- Designed Site Column which retrieves the data from the SQL Server backend server.
- Environment: SharePoint 2010, WSS 3.0, C#, ASP.NET 3.0 , ADO.NET, MS SQL Server 2005/2008, Internet Information Services (IIS) 6.0,7.5, Visual Studio 2010 ultimate, .NET, XML, CSS, SharePoint Designer 2010, J Query, JavaScript, Active Directory Service.

Credit Union, Share point Developer/Administrator, GA, 2009 – 2011

Maintain and give support to the existing sites, migration of their site content from SharePoint Portal Server 2003 to Microsoft Office SharePoint Server 2007 and customization of personal sites by using features of MOSS 2007.

- Administrated activities including creation of sites, giving access permissions for selected Audience, backup/restore of Site Collection using STSADM Tool
- Upgraded existing Site Collections and transition of Document Content management from SPS 2003 to MOSS 2007/2010.

e&e IT Consulting Services, Inc.

Resource 59

Microsoft Product Specialist (SharePoint)

- Migrated from SharePoint Portal Server 2003 to Microsoft Office SharePoint Server 2007 by using migration tool AVEPOINT
- Created multiple external internet and internal intranet sites, Web Application, Site Collection, Site configuration, Site Template, Team Site, Wiki Site, Blog, Document Workspace and Meeting Workspace for managing Web portal information
- Created users/groups in active directory along with assigning permissions to them while accessing SharePoint Site
- Created a basic SharePoint survey page for the Customer Satisfaction in all the departments
- Managed sites and added the existing sites to the trusted locations to import Excel Services
- Developed Custom Site definitions for the HR Department team that is based on the existing Team Site definition
- Wrote custom JQuery scripts to allow users to collapse and expand sections of SharePoint Quick Launch menu
- Handled AAM, solution management, incoming e-mail, antivirus settings for deploying solutions packages and for accessing outlook mails to the list.
- Developed Solution Deployment Packages(WSP) and deployed in to the Share Point as a Feature
- Customized a sequential work flow engine and publishing forms in Form Library using MS InfoPath 2010 for archiving, reviewing the content using Microsoft Workflow Foundation(WWF).
- Created a Wiki Page library to capture all open issues from all the users and make a separate page for each issue with all steps and solutions
- Managed the Index & Search Engine to Extend the Default Search Functionality of SharePoint
- Created the CIO Status Report forms using InfoPath 2007 in SharePoint Sub sites for collecting user information and customized using InfoPath forms and stored the data in SharePoint list
- Branded the SharePoint portal and Team sites using the CSS and SharePoint designer 2007 to have a consistent and uniform look throughout the portal.
- Developed and Integrated SSRS 2005 BI reports with Share Point 2007
- Created a Wiki Page library to capture all open issues from all the users and make a separate page for each issue with all steps and solutions
- Managed the Index & Search Engine to Extend the Default Search Functionality of SharePoint
- Designed Master Pages and applied different Master Pages to the Sites and Sub sites
- Worked with Microsoft team to solve the share point open issues.
- Environment: Microsoft Windows 2003 Server, MOSS 2007, SharePoint 2010, WSS 3.0, C#, ASP.NET 3.0 , ADO.NET, MS SQL Server 2005/2008, Internet Information Services (IIS) 6.0 SSRS 2005, Visual Studio .NET

2008, XML, CSS, SharePoint Designer 2007, InfoPath 2007, Active Directory Service.

Humana, Share point Developer/Administrator, KY, 2009 – 2009
Support the customer purchase order process, migration of their site content from SharePoint Portal Server 2003 to Microsoft Office SharePoint Server 2007.

- Migrated from SharePoint Portal Server 2003 to Microsoft Office SharePoint Server 2007 by using migration tool AVEPOINT
- Upgraded existing Site Collections and transition of Document Content management from SPS 2003 to MOSS 2007
- Created multiple external internet and internal intranet sites, Web Application, Site Collection, Site configuration, Site Template, Team Site, Wiki Site, Blog, Document Workspace and Meeting Workspace for managing Web portal information
- Created users/groups in active directory along with assigning permissions to them while accessing SharePoint Site
- Expanded a server farm applying service packs and patches using STSADM utility
- Created a basic SharePoint survey page for the Customer Satisfaction in all the departments.
- Administrated activities including creation of sites, giving access permissions for selected Audience, backup/restore of Site Collection using STSADM Tool
- Managed sites and added the existing sites to the trusted locations to import Excel Services
- Developed Custom Site definitions for the HR Department team that is based on the existing Team Site definition
- Developed Solution Deployment Packages(WSP) and deployed in to the Share Point as a Feature
- Customized a sequential work flow engine and publishing forms in Form Library using MS InfoPath 2007 for archiving, reviewing the content using Microsoft Workflow Foundation(WWF).
- Created a Wiki Page library to capture all open issues from all the users and make a separate page for each issue with all steps and solutions
- Utilized Microsoft Team Foundation Server to manage the team's software development lifecycle.
- Developed Custom Event Handlers to create a report list based on the due dates and closing dates
- Configured search, index/query servers, Content Sources, handled and Managed crawled properties and search schedules
- Branded the SharePoint portal and Team sites using the CSS and SharePoint designer 2007 to have a consistent and uniform look throughout the portal.

- Developed Custom Web parts and deployed in the Web part gallery to display the Metadata fields of the document library which was created dynamically
- Configured Outlook 2007 with MOSS 2007 to synchronize Share Point Document Library and lists
- Developed Shared Cases Custom Lists which creates a Document library and display on Quick Launch on item added to the Custom list
- Designed Site Column which retrieves the data from the Oracle backend server
- Environment: Microsoft Windows 2003 Server, MOSS 2007, WSS 3.0, C#, ASP.NET 3.0 , ADO.NET, MS SQL Server 2005, Internet Information Services (IIS) 6.0 ,SSRS 2005, Visual Studio .NET 2008, XML, CSS, SharePoint Designer 2007, InfoPath 2007, Active Directory Service.

Potomac Bank Fairfax, Share point Developer/Administrator, VA,
2007 – 2009

Implement SharePoint and provide a single application platform to all the users of the organizations so work can be collaborated which would give good results to the organizations.

- Migrated from SharePoint Portal Server 2003 to Microsoft Office SharePoint Server 2007 by using 3rd party migration tool
- Created multiple external internet and internal intranet sites, Web Application, Site Collection, Site configuration, Site Template, Team Site, Wiki Site, Blog, Document Workspace and Meeting Workspace for managing Web portal information
- Experience with Live link EMC, with an emphasis on document and records management features that allow organizations to control document
- Conducted Training sessions for Site Administrators and business users
- Created User Profiles and allotted permission levels for secure SharePoint portal
- Created and maintained Document Libraries and Picture Libraries in team and sub sites
- Administrated activities including creation of sites, giving access permissions for selected Audience, backup/restore of Site Collection using STSADM Tool, and error logging and reporting Backed up and restored indexes created by Microsoft Office SharePoint Server 2007 using Data Protection Manager 2007
- Created a basic SharePoint survey page for the Customer Satisfaction in all the departments
- Managed sites and added the existing sites to the trusted locations to import Excel Services
- Worked on Active Directory for creating users and groups set the permissions and site collection administrator and modified permissions of an existing user or group.

e&e IT Consulting Services, Inc.

Resource 59

Microsoft Product Specialist (SharePoint)

- Configured search, index/query servers, Content Sources, handled and Managed crawled properties and search schedules
- Created basic Vendor Request form, Desktop Integration Software Package Documentation

  Submission Form using InfoPath Forms 2007
- Developed Custom Event Handlers to create a Document library based on a template when new item is added to the list
- Provided training for SharePoint functionalities to ensure positive initial experience
- Developed Reports and Dash boards in Report Center using SSRS 2005
- Automatically updated Excel table and saved changes on Share Point site using Excel Services
- Customized Content Query Web Parts by using custom properties in office SharePoint Server 2007
- Environment: Microsoft Windows 2003 Server, MOSS 2007, WSS 3.0, C#, ASP.NET 3.0 , ADO.NET, MS SQL Server 2005, Internet Information Services (IIS) 6.0 ,SSRS 2005,Crystal Reports, Visual Studio .NET 2008, XML, CSS, SharePoint Designer 2007, InfoPath 2007, Microsoft Exchange Server 2005 Server systems, Active Directory Service.

Education

Bachelor of Technology Nagarjuna University, India.

e&e IT Consulting Services, Inc.

Resource 60

Microsoft Product Specialist

Key Skills and Knowledge

- Top Secret Clearance
- Security +
- MCP
- SCCM migrations
- Microsoft Windows Active Directory Domain, Microsoft System Center Configuration Manager (SCCM) 2007, Microsoft Exchange 2010, Windows 2008 Servers, Windows 7 workstations, TCP/IP network.

Professional Summary

Systems Engineer with 12+ years of experience in the Information Technology industry. Extensive experience in server administration and management; provides stellar technical support for computer hardware and software issues.

- Experience with VBscript programming and custom software packaging. Installation and configuration of Microsoft operating systems and software, including Windows server and desktop products
- Provided team lead support on numerous state and federal agency wide project based pc roll-outs
- Developed and implemented SharePoint infrastructure for the United States Army War College, including a full farm migration from SharePoint 2003 to MOSS 2007
- Implemented and performed an SCCM 2007 migration from an existing SMS 2003 environment and implemented a full Windows 7 desktop deployment through SCCM 2007 OSD tools to meet agency requirements and standards.

Employment History and Related Experience

E&E IT Consulting, SCCM Administrator, Mechanicsburg, PA, 2011 – Present

System Administrator responsible for daily maintenance and administration of the SCCM environment for DLA Information Operations located in New Cumberland Pennsylvania. SCCM environment comprised of a single Central Server and 26+ Primary/Secondary Site Servers supporting 12500+ desktops.

- Ensuring uninterrupted services of the SCCM environment and related desktop clients.
- creating custom software packages unique to DLA Information Operations. Test and distribute custom and standard software packages.
- Research, understand, and implement custom reports using SCCM and Microsoft SQL Reporting Services to meet agency requirements.
- Troubleshoot hardware and software problems related to PCs, print servers, and printers in relation to SCCM and DLA Information Operation desktop standards.
- Environment: Microsoft Windows Active Directory Domain, Microsoft System Center Configuration Manager (SCCM) 2007, Microsoft Exchange 2010, Windows 2008 Servers, Windows 7 workstations, TCP/IP network.

e&e IT Consulting Services, Inc.

Resource 60

Microsoft Product Specialist

CIBER Federal IM/IT, Systems Engineer, Carlisle, PA, 2005 – 2011
System Engineer responsible for daily server maintenance tasks and support for US Army War Collage located in Carlisle Pennsylvania. Site housed a 100 Node server farm supporting 1500+ users.

- Ensuring uninterrupted service for all server related applications including e-mail, management of Active Directory user and computer accounts, and maintaining the SCCM environment.
- maintaining and developing a medium SharePoint server farm and provide administrative support to ensure all end-user and departmental needs are met, including the development of custom workflow processes with SharePoint Designer and InfoPath.
- Created, maintained, and distributed custom and pre-built software packages to agency desktop computers through SCCM.
- Performed a site wide deployment of SCCM 2007; upgrading from SMS 2003 in compliance with Army and DISA requirements. Implemented a Windows 7 deployment through SCCM 2007 OSD tools.
- Environment: Microsoft Windows Active Directory Domain, Microsoft System Center Configuration Manager (SCCM) 2007, Microsoft Exchange 2003, SharePoint 2007, Windows 2003 Servers, Windows XP workstations, TCP/IP network.

Intellimark, Inc., Administrator/Technician, Mechanicsburg, PA, 2001 – 2005
Administrative Technician responsible for overseeing the Level 2 support for users of the DLA Information Operations located in New Cumberland, PA. Site consisted of main location with an 80+ Node server farm supporting 2500+ local users and 20+ remote sites with local administrative teams.

- Team lead for 6 technicians who provided Level 2 support for local users, administrated user accounts and policy for local site within Active Directory Domain.
- Installed and maintained workstations and PC equipment while meeting agency policies and needs unique to DLA Information Operations.
- Developed and maintained the Symantec Ghost enterprise solution, which supported the agency wide desktop imaging.
- Provided some site level administrative support to end users for a small SharePoint environment.
- Environment: Microsoft Windows Active Directory Domain, Microsoft Exchange 5.5/2003, SharePoint 2003, Windows 2003 Servers, Windows XP workstations, TCP/IP Network.

e&e IT Consulting Services, Inc.

Resource 60

Microsoft Product Specialist

JFC Pro Temps, PC Technician, Camp Hill, PA, 1999 – 2001
Technician responsible for the installation and upgrading of PC equipment for Department of Labor and Industry of Pennsylvania. Site consisted of main location with a 100+ Node server farm supporting 2000+ users and more then 50 remote sites supporting a total of 5000+ additional users.

- Installing new PC equipment or upgrading existing equipment, while migrating existing users from a mixed Windows NT/2000 environment to a fully integrated Windows Active Directory Domain.
- Converted existing network architecture to a complete TCP/IP solution replacing equipment as needed to meet requirements.
- Environment: Microsoft Windows NT/Active Directory Domain, Microsoft Exchange 5.5/2000, Windows 2000 Servers, Windows NT/2000 workstations, TCP/IP and Token Ring Network

Education/Training

- Computer Network/Internet Technician, Schuylkill Institute of Business and Technology, Pottsville, PA – 1999
- Windows Installer Repackaging Engineer (ENG-30) – March 2012
- SharePoint Workflows & InfoPath (Custom Course) – July 2010
- Planning, Deploying and Managing Microsoft Systems Center Configuration Manager 2007 (Course 6451) – March 2009
- Extreme Makeover SharePoint 2007 Edition – Branding & Customization (Level 200) – April 2008
- SharePoint 2007 Jump-Start (Level 100) – October 2007
- Implementing a Microsoft Exchange Server 2003 (Course 2400) – June 2006
- Microsoft Visual Basic Scripting Edition and Microsoft windows Script Host Essentials (Course 2433) – March 2006
- Managing Microsoft Systems Management Server 2003 (Course 2596) – January 2006IASO Level II (System Administrator/Network Manager Course – October 2005

Certifications

- Top Secret Security Clearance
- CompTIA Security+ Certified – October 2009
- IASO Level II Certified – October 2005
- Microsoft Certified Professional (MCP) Windows 2000 – December 2001

This page intentionally left blank.

UNISYS

IBM

Resource 61

Microsoft Product Specialist (Exchange & SharePoint)

Key Skills and Knowledge

- Key Microsoft technologies
- MS Exchange
- SQL
- SharePoint
- SCOM
- Active Directory

Professional Summary

Have had primary responsibility for architecture, design, and implementation of Active Directory migrations, Exchange server upgrades, SAN moves, data migration, and Citrix Server Farms. Performed as a SharePoint Administrator responsible for migrations and upgrades. Supported MS Exchange server environment operation with significant volume of mailboxes. Experienced in most product sets related to the key Microsoft technologies.

Employment History and Related Experience

Rollins, Senior Network LAN Architect (Messaging, Active Directory, SharePoint & Microsoft Dynamics), Atlanta, Georgia, 2010–2012

Windows Server 2008/2003 Active Directory Management and maintenance; Architecture, design, and implementation of Active Directory Migrations, Exchange Server upgrades, SAN moves, Data migration, Citrix Server Farms; Responsible for SharePoint 2007/2010 administration.

- Migrated SharePoint from 2007 to 2010.
- Microsoft SCOM 2012.
- Microsoft ILM 2007.
- Advanced Management and Configuration of Microsoft Dynamics.
- Management of Company intranet using SharePoint 2010.
- Microsoft Exchange Server 2007/2003 Administration.
- Supported Exchange Server 2007/2003 Management 5,000+ user mailboxes.
- Installed Exchange Server 2007.
- Upgraded Exchange 2003 to Exchange 2007.
- Configured Exchange 2007 for Proactive Management.
- Managed Exchange Server 2007 Security.
- Responsible for the implementation of Front-End and Back-End Servers.
- Microsoft Exchange Server Clustering
- Responsible for the management of Exchange 2007 Address Lists.
- Disaster Recovery Management of Exchange 2007/2003
- Backing Up Exchange 2007/2003
- Active Directory Setup and management
- DNS Setup and management
- Created Technical Design Documentation.
- Expertise in Active Directory Maintenance and Replication.

AT&T, WINTEL/Linux Network LAN Architect (Messaging & Active Directory) Alpharetta, Georgia, 2008–2010

Responsible for Windows Server 2003 Active Directory Management and maintenance. Responsible for the architecture, design, implementation of large

scale Exchange Server Migration from Lotus Notes to 10,000+ user mailboxes running in Exchange Server 2003.

- Served as Team Lead/Senior Engineer for Windows Infrastructure.
- Setup and manage the Active Directory.
- Responsible for administration of Microsoft Exchange Server 2003.
- Responsible for Exchange Server 2003 Management 5,000+ user mailboxes.
- Installed Exchange Server 2003.
- Configured Exchange 2003 for Proactive Management
- Managed Exchange Server 2003 Security
- Responsible for Disaster Recovery Management of Exchange 2003
- Responsible for Data center management and Production/Application Support

Colonial Bank, Network Planning Engineer/Architect, Montgomery, Alabama, 2006–2008

Windows Server 2003 Active Directory Management and maintenance; ITCS104 Security Methodologies for operating system Hardening; Management of major enterprise IT projects.

- Earned PMP Certification(member of PMI)-Member of PMI and Montgomery Chapter
- Responsible for project planning and phase management.
- Responsible for project scheduling and Implementation.
- Led enterprise project roll-outs.
- Responsible for Project Team scheduling.
- Created the Technical Design Documentation.
- Microsoft Exchange Server 2003 Administration
- Responsible for the Exchange Server 2010 Management 10,000+ user mailboxes.
- Responsible for the Windows Server 2003 Distributed File System.

Manheim-COX Enterprises, Network Architect/Engineer, Atlanta, Georgia, 2005–2006

Responsible for Windows Server 2003 Active Directory Management and maintenance. Responsible for the management and troubleshooting of network printers, Supported Microsoft Exchange Server 2003; and ITCS104 Security Methodologies for operating system Hardening. Responsible for Cisco Advanced Router and Switch Configuration.

- Expertise in the Active Directory maintenance and replication
- Macromedia Flex
- Citrix Metaframe Presentation Server 4.0
- Nortel Contivity Series VPN Concentrators
- Nortel Baystack Switches and Routers

IBM

Resource 61

Microsoft Product Specialist (Exchange & SharePoint)

- Managed the CheckPoint R60 Platform running in Provider-1 Interface
- Managed the CheckPoint IPSO running on Nokia IP380 Appliances
- Microsoft Operations Manager 2005 SP1 and 2000 for mainly monitoring and reporting
- Microsoft Exchange Server 2003 and 2000 and Active Server Directories in a vast enterprise environment
- Windows Server 2003 Distributed File System.
- BlackBerry Enterprise Server 3.6 for Microsoft Exchange Server-handling and accounts PIN generation and BlackBerry synchronizations issues resolution.
- Provided remote end user assistance via REAL VNC, DameWare, and Microsoft Remote Desktop and management of Server 2003 Terminal Servers.
- Microsoft Exchange Server 2003, SharePoint Portal Server 2003 config and management, File and Print Server management.

Verizon Enterprise Solutions, Senior Network Architect, Alpharetta, GA, 2001–2005

Served on Engineering team in troubleshooting internet circuit problems for wide range of customers with Frame Relay, T1, SMDS, ATM, HiBACK, ATM LANE circuits.

- Responsible for circuit provisioning/test-and-turn-up
- Supported the Microsoft Exchange Server 2003
- Supported the BlackBerry Enterprise Server for Exchange Server 2000
- Responsible for the imaging and testing of PCs prior to full-scale deployment
- Deployed PCs using SMS, GHOST Enterprise, and Altiris
- Responsible for the Windows Server 2003 Distributed File System
- Responsible for Microsoft Exchange 2003 Administration and Management (Well versed in Novell GroupWise)

QoS Networks, Inc, Senior Network Architect/Team Lead, Atlanta, GA, 2000–2001

Assistant Manager and Senior Network Architect over “Research and Development” dept. This department was responsible for deciding what networking equipment the company would implement in their strategic POP (Points of Presence) locations.

- Performed significant amount of lab testing of various LAN/WAN equipment in a large “Greenfield” environment
- Responsible for the maintenance and configuration of Cisco VPN Concentrators for secure remote access

Resource 61

Microsoft Product Specialist (Exchange & SharePoint)

Brasfield & Gorrie, LLC, IT Manager (LAN/WAN), Kennesaw, GA, 2000–2000

Replacement manager for company's IT Data Network Department. Managed company's entire dept (local and remote). IT Department consisted of 35+ employees, and a large data Center environment with Exchange, Citrix, and SharePoint server farm.

- Provided remote administration of servers in the farm
- Cisco Router 1005/2500/2505/2610/3600/4700/7000 Series setup, configuration, monitoring; RIP/IGRP/EIGRP/BGP-4/eBGP/iBGP/EGP; Network Addressing, IP Subnetting expert; TCP/IPTCP, UDP, DNS, IP, ARP, FTP, SMTP, POP3, ICMP, RIP,OSPF, HTTP, SPX; Network Security- IP ACCESS LISTS- Standard, Extended, SAP; FRAME RELAY monitoring-IP, DECnet, AppleTalk, XNS, Novell IPX, CLNS, ISO, Banyan Vines, Transparent Bridging; FECN/BECN ; X.25, LAPB, NRM, ARM, ABM; MPLS, IS-IS
- Microsoft Operations Manager 2000 for monitoring Exchange Server 200 events
- ISDN BRI/PRI Troubleshooting and monitoring; RAS implementation; Dial-On-Demand RoutingMicrosoft SNA Administrator, Citrix Metaframe XPe and Nfuse Configuration and Setup, IBM Tivoli for software deployment and hardware/software tracking across an enterprise
- Windows 2000 deployment and implementation, Microsoft Terminal Server, ProLog, Norton Anti-Virus Corporate Edition/2000/5.0, GHOST 5.1, AT&T Global Dialer, MS Office 2000/97, Microsoft
- SMS 2.0, Microsoft SQL Server 7.0 Enterprise Edition, CheckPoint VPN Configuration
- Red Hat Linux Network, FileSystem, and user Administration; Kernel Compiling, X Window System, Apache, Linux Routing, IPCHAINS, DHCP, SAMBA, NIS Client/Server, Squid Proxy Server, PAM and INETD Configuration; Versions 5.2, 6.0, 6.1

Computer Science Corp, Mobile, Windows NT Server 4.0 Network Administrator/Desktop Support Manager, First Major CSC Project- Brown & Root, Inc. /Fairmont merge project beg (Exterior Border Gateway Protocol), AL, 1997–2000

The purpose of this particular project was to create and roll-out an autonomous system for more efficient and centralized communication. Assisted the head Cisco Routing Engineer along with a Team of six other Cisco and Network Engineers in the rollout of two Cisco 7513Core Routers using the "eBGP" routing protocol to connect Brown & Root's autonomous system to Fairmont's autonomous system.

iBGP (Interior Border Gateway Protocol), J.B.E. & K, Inc. - Interdomain consolidation project, 1997

Served on same team of six Cisco and Network Engineers in rollout of one Cisco 7500 router using iBGP protocol to better manage company's existing interdomain and also give them faster access to the "cloud".

OSPF (Open Shortest Path First), Kimberly Clark, Inc-Simple WAN upgrade, AL, 1997

Rapid growth of main office in Mobile, Alabama called for a WAN connectivity upgrade from a regular Cisco 2610 access level router to a more robust Cisco 4700 router using OSPF routing protocol.

- Designed and setup OSPF internetwork for Mobile and neighboring offices in a hierarchy of areas.
- Designated the Mobile office LAN as area 0.0.0.0(The Backbone).
- Responsible for administering 300+ user Windows NT Single Master Domain Network.
- Installed and managed SAP R/3.
- Supported SAP R/3 Administration on Windows Server 2000 Platform for FICO, HR, MM, and SD.
- Responsible for the troubleshooting and configuration in RAID 5 fault tolerance, domain trust, DNS/WINS, NetWare to NT Migration, system registry repair, DHCP, browser services, ARC naming convention, RAS, computer/host name resolution, directory replication, Gateway Services for NetWare, profiles and policies, BDC to PDC upgrade, file-level security in NTFS, TCP/IP, NetBEUI, NWLink, IPX/SPX, NDIS, SMB, UNIX Print Server, Novell NetWare Administration, WAN monitoring, ATM, 3Com hubs, Switches, Cisco Routers, FDDI, FTP, Firewall.
- Responsible for Citrix Metaframe 1.8 Administration
- Responsible for the setup and administration of Microsoft Exchange 5.5, IIS v4.0, Proxy Server, SAP R3.
- Configured and maintained Microsoft SQL Server, Prism, and Oracle DBA, Microsoft SMS (Systems Management Server).
- Supported REMEDY Ticketing System for Trouble Requests.
- Responsible for Microstation and Silicon Graphics CAD Applications.
- Supported DOS, Windows 3.X, Windows95/98, Windows NT 3.X, 4.0, Windows 2000 Professional/Server Beta 3, Microsoft Backoffice.

Tek Systems, Inc, Desktop PC Technician/Junior Network Administrator , Birmingham, AL, 1995–1997

Duties were to maintain, troubleshoot, and repair all IBM-compatible and specialized Silicon Graphics UNIX PC, CAD NT Workstations, and Honeywell IGSE non-standard PCs.

Resource 61

Microsoft Product Specialist (Exchange & SharePoint)

- Assigned as a Junior Novell NetWare Systems Administrator
- Novell GroupWise Administration

Inchcape Shipping, PC Hardware Technician/Asst. Novell NetWare Administrator, Mobile, AL, 1994–1995

Assisted Chief Novell NetWare Engineer in the maintenance, upkeep, and configuration of 200+ user network. Responsible for GroupWise configuration and Administration. Performed technical writing

- Responsible for VPN/Remote Access setup and administration.

UNISYS

Resource 62

Microsoft Product Specialist

Key Skills and Knowledge

- Planning, designing, deploying and managing Exchange Messaging infrastructure
- Planning, designing, deploying and managing AD infrastructures
- Planning, designing, deploying and managing BlackBerry Enterprise Servers
- Planning, designing, deploying and managing Microsoft Operations Manager
- Designing EMC storage for Exchange infrastructure.

Project and Program Management

- Windows 2003 AD upgrade
- EMC SAN upgrade
- Exchange 2000 Consolidation
- Exchange 2007 Upgrade
- BlackBerry Deployment

Communication and Networking

- WINS, DHCP, DNS, FTP,
- SMTP, POP3, IMAP,

Databases

- SQL Database,
- Exchange Databases

Hardware

- Dell Servers,
- IBM Servers,
- EMC CX700, CX500
- SAN Brocade Switches
- IBM Ds4800, DS8300

Operating Systems

- Windows 2008/2003/2000
- Windows NT4.0
- Windows 8/7/XP

Software/System Architecture

Programming Languages & Tools

Call Center and Help Desk

- Remedy Help Desk

Professional Summary

Accomplished professional with more than 18 years of experience in IT. A highly motivated and ambitious individual with excellent management skills; strong leader of small teams for more than 10years. Proven ability to lead by example, consistently hit targets, improves best practices and organizes time efficiently.

- Windows 2008/2003 Active Directory, Exchange 2010/2007/2003/2000, Office 365,
- Tivoli Identity Manager (TIM), Ironport E-mail Encryption, Forefront Security, McAfee Groupshield, SQL Server, SCOM, DNS, WINS, BlackBerry, Good Technology, Legato
- Galaxy Commvault, NETIQ AppManager, Altiris, Postini, EMC Clariions, Brocade Directors and EMC management software
- Planning, designing, deploying and managing Active Directory and Exchange for large enterprise-wide networks
- Designing and implementing Messaging and Active Directory infrastructures
- Strong problem-solving and analytical skills

Employment History and Related Experience

Unisys Inc., Exchange Team Lead, 1999 – Present

Supporting the Commonwealth of Pennsylvania Exchange Project –A Pennsylvania Govt. maintenance project is about managing and supporting Exchange 2007 and Windows 2003 Active Directory for over 90,000 users. This project started in 1999 and was carried out by MICROSOFT in partnership with UNISYS, was about migration of different mail systems being used by 47 agencies of the Commonwealth into a Single Enterprise wide Exchange Mail system using Microsoft Exchange.

- Achieve a high customer satisfaction rating and ensure overall success of the Exchange and AD project.
- Act as the primary point of contact for the technical expertise, Exchange team management issues and, support problems for the Commonwealth and Unisys.
- Provide appropriate communications to COPA and Unisys management, including rapid notification of issues that impact Exchange services
- Oversee and manage the day-to-day operations of the Exchange team, ensuring that all resources understand and complete their assignments on time and in a professional manner.
- Oversee individual projects to ensure that the team is meeting and exceeding key objectives and metrics.
- Assist client with performing a risk assessment and gap analysis of current infrastructure and provide a solution to mitigate and remediate risks.

UNISYS

Resource 62

Microsoft Product Specialist

Office Productivity Tools

- MS Project, MS Visio, Ms Word, Excel, PowerPoint

Technical Documentation

- Created and responsible for multiple documents here at Commonwealth

- Assist with business continuity planning, which includes capacity planning, availability and disaster recovery.
- Review e-mail messaging systems hygiene process and assist with addressing complex security challenges related to spam, worms and viruses.
- Provide incident resolution focusing on root cause analysis, prevention, and knowledge transfer.
- Supervise various projects as well as delegate roles and responsibilities to the fellow team members.
- Planned, designed, deployed and migrated Exchange 2000 organization to Exchange 2007
- Successfully completed the transitioning Exchange 2000 to Exchange 2007 for 89,000 mailboxes
- Successfully completed the migration of User accounts from PennDot to Centralized Accounts forest
- Designed EMC SAN disk sub system for CLARiiON CX700 for migrating Exchange 2000 to SAN backend
- Implemented one of the best-consolidated Exchange architectures here at Commonwealth; he implementation was reviewed by Microsoft RAP team and was complemented as one of the best Exchange implementations
- Member of the Exchange 2000 design team in migrating from Exchange 5.5 to Exchange 2000
- Member of the Active Directory design team in implementing Windows 2000 and Windows 2003 Active Directory
- Designed, deployed and administering BlackBerry Enterprise Server for wireless e-mail for over 1500 users.
- Designed, deployed and administered NETIQ Appmanager to monitor mission critical applications at CWOPA
- Designed, deployed and administering NETIQ Appanalyzer for reporting and analysis.
- Designed, deployed and Managing Microsoft Operations Manager for monitoring Active Directory and Exchange infrastructure at the Commonwealth of Pennsylvania
- Member of the Windows 2003 Public Key Infrastructure design team to implement Certificate Authority for wireless and VPN access
- Managing SQL Server 2000 production servers
- Implemented Sybari's Antigen and Anti-Spam solution for Exchange
- Designed, deployed and administered Enterprise wide backup solution using Legato Networker and Smartmedia.
- Identify Pilot groups and deployment phases for deploying the changes to the Exchange environment.
- Member of Enterprise server farm Change management board

UNISYS

Resource 62

Microsoft Product Specialist

- Work with Team members on knowledge transfer and stabilizing all the products that Exchange team manages.
- Update management and the Team about the ongoing software or Hardware Releases.
- Manage escalations with Microsoft TAM and other vendors TAMs for a speedy and timely resolution of operational and design issues.
- Review and work with Team Members on day to day tasks to ensure 100% uptime.
- Ensure timely resolution of critical issues by delegating tasks to appropriate individuals in the team.
- Execute formal post-mortem process on closure of critical issues.

IBM Global Services Inc. Second Tier Exchange Admin, Princeton, NJ, 1998 - 1998

Maintained NT networks on Multiple Master Domain model, with over 500 Domain controllers and an Exchange network based on hub and spoke topology and which includes around 270 servers running on Exchange 5.5, SMS 1.2, SQL 6.5 and Seagate Backup Exec 7.2.

- Monitoring and troubleshooting Trust relationships between NT Master Domains.
- Monitoring and troubleshooting of Windows NT and Exchange servers using SMS.
- Carrying out Exchange backouts as well as site to site migration
- Troubleshooting Information store and Directory database related problems.
- Monitoring and troubleshooting Exchange MTA and IMC queues.
- Carrying out Remote tape backups for Exchange and SMS servers
- Restoring single mailboxes as well as complete servers as and when required.
- Troubleshooting WINS related problems.
- Working on user trouble tickets

ACS Technologies Ltd., Network Engineer, 1994-1997

- Supported several projects for ACS including Windows NT Administrator and Novel Administrator contract
- System Research Group India Ltd., Windows NT Administrator
- Installation, Optimization, Security & Maintenance of NT 4.0 network
- Carried out Windows NT Server installations with diverse Clients like Windows NT Workstation, Windows 95, Windows 3.11 and Network Client for MS-DOS
- Interconnected Windows NT Network with UNIX Networks and vice versa and

UNISYS

Resource 62

Microsoft Product Specialist

- Installed PC-NFS software on Windows NT to allow NT clients to access resources on UNIX and also installed Disk Share software on NT to allow UNIX clients to access resources on NT.
- Implemented and administered Messaging through MS Exchange Server for a single site.
- Installed and administered IIS as Web server and FTP server.
- Installed and administered System Management Server for remote troubleshooting of workstations.
- Carried out tuning and optimization of NT servers.
- Implemented RAID level 1, i.e. Mirroring for fault tolerance purpose. Also recovered the Data from the crashed hard disks by manually writing Partition Table and Boot sector information

Nagarjuna Finance Ltd, Novell Administrator

- Installation, configuring, optimizing and Maintenance of Windows NT and NetWare Networks
- Installed and administered Windows NT 4.0 in a Domain environment. Also installed Novell NetWare 4.1 and 3.12 servers and configured NT as Gateway for NT clients to access NetWare resources. Allowed NetWare clients to access NT resources by installing FPNW on Windows NT4.0
- Designed, Implemented and administered NDS, Managed Partitions and replicas, solved NetWare volume related problems. Migrated users, group accounts and data from Novell NetWare to Windows NT
- Installed Network Printers and implemented Remote Booting on both Windows NT and NetWare.
- Carried out Mirroring and Duplexing of partitions on NetWare servers
- Provided Internet access to every desktop using Proxy server
- Carried out tuning, and optimization of NT and NetWare Servers
- Responsible for monitoring and regulating network traffic on NetWare and Windows NT networks

Frank Computer Ltd., Network Engineer, 1992 to 1994

- Installation, Administration, Fine-tuning and Maintenance of NT 3.51 Network
- Carried out installation of Windows NT3.51 servers, configured as PDC, BDC and member servers in a Domain environment
- Supervised the layout of coaxial and UTP cabling for Ethernet Network.
- Installation & Maintenance of hardware, procuring and testing of new hardware and software
- Installation, Up-gradation & optimization of a NetWare 3.11 and 2.2 ARCnet Network
- Designed and Implemented Novell NetWare 3.11 ARCnet network for over 90 nodes

UNISYS

Resource 62

Microsoft Product Specialist

- Upgraded NetWare 2.2 servers to 3.11 servers
- Responsible for ARCnet cabling, installation of Passive hubs and Active hubs
- Troubleshooting volume, disk space and Memory related problems.
- Training users on the usage and maintenance of network resources
- Provided round the clock support and ensured zero downtime.
- Weekly monitoring of Server and volume logs and taking preventive measures

Education

- B.S. (Electronics and Communications Engg.) from Institute of Electronics and Telecommunications Engineers (IETE), New Delhi, India

Professional Certification

- Microsoft Certified IT Professional in Exchange 2007 Messagin
- Microsoft Certified Specialist in Exchange 2007 Messagin
- Microsoft Certified Systems Engineer (MCSE) – Windows 2003 trac
- Microsoft Certified Systems Engineer (MCSE) – Messaging
- Cisco Certified Network Associate (CCNA)
- Certified NetWare Administrator (CNA)
- Dell Certified Technician
- ITIL Certified.
- Legato Certified Networker Administrator

This page intentionally left blank.

UNISYS

INFO-MATRIX CORPORATION

Resource 63

Microsoft Product Specialist

Key Skills and Knowledge

- SharePoint Developer/ Designer/ Architect
- Development: C#.NET, VB.NET, C++, VB 6, Java/J2EE, Pearl, COBOL
- Internet Technologies: ASP, JSP, CSS, JavaScript, ASP.Net 3.0/2.0, ADO.Net, HTML, XML, XSL, SOAP, Web Services, AJAX, WSDL
- Tools: Visual Studio 2008, Visual Studio 2005, Visual Studio .NET, BDC Metaman, Rational Rose, Jtest
- Database: SQL Server 2005, SQL Server 2000, MySQL
- Reporting: IBM Cognos, Crystal Reports 8.0,11
- Operating System: Linux, Windows NT, Windows 2000, Windows 2003
- Methodologies: Microsoft Solutions Framework, Unified Modeling Language (UML), Use Case design methodology, Object Oriented Design principals.

Professional Summary

Proven skills in Architecture, Design, Development, Implementation and Administration of SharePoint Technology based projects. He has 7 Years of IT experience working in different phases of SDLC wiht in depth hands-on experience in SharePoint Server, C#, ASP.NET, SQL/MYSQL, Visual Studio, XML, SOAP, Web Services. He is a highly motivated professional with proven ability to work with large teams; and extensive Object Oriented Design and Development experience.

- SharePoint: SharePoint 2010, MOSS 2007, SharePoint Designer 2007, Web Parts, Web Controls, SharePoint Portal Server 2003
- Microsoft InfoPath 2007/2005, Microsoft FrontPage 2003, Windows Workflow Foundation, Business Data Catalog, Form Services, CAML, KPI, Event Handlers, Records Management
- Development: C#.NET, VB.NET, C++, VB 6, Java/J2EE, Pearl, COBOL
- Internet Technologies: ASP, JSP, CSS, JavaScript, ASP.Net 3.0/2.0, ADO.Net, HTML, XML, XSL, SOAP, Web Services, AJAX, WSDL
- Tools: Visual Studio 2008, Visual Studio 2005, Visual Studio .NET, BDC Metaman, Rational Rose, Jtest
- Database: SQL Server 2005, SQL Server 2000, MySQL
- Reporting: IBM Cognos, Crystal Reports 8.0,11
- Operating System: Linux, Windows NT, Windows 2000, Windows 2003
- Methodologies: Microsoft Solutions Framework, Unified Modeling Language (UML), Use Case design methodology, Object Oriented Design principals

Employment History and Related Experience

PIMCO, SharePoint Architect, Newport Beach, CA, 2010 - Present
Designed, documented and implemented the SharePoint 2010 upgrade process on the internal MOSS 2007 portal; designing the new Enterprise taxonomy for the new implementation utilizing new SharePoint 2010 content management and information architecture features; and utilized SharePoint designer 2010 to implement custom workflows with custom user forms.

- Modifying custom Web parts built for MOSS 2007 and other solutions with references to 12 hive to work on the new 2010 implementation
- Utilizing BCS to build external lists surfacing tasks initiated from an external project management solution into SharePoint user oriented pages
- Connecting to an Oracle DB using BCS to utilize data in external lists, as well as within custom application pages
- Utilizing Google Maps GIS API to develop mapping information for employees within SharePoint

- Building custom dash boards with a collection of controls reflecting reports from different applications and site collections
- Implementing collaboration features including personal sites, discussion boards and wikis with custom site definitions
- Implementing Enterprise search with custom content sources, scopes and roles built on managed properties
- Creating a custom solution to manage and initiate custom alerts with flexible CAML queries on different list templates
- Maintaining daily backups, monitoring logs, installing hot fixes, configuring e-mail enabled lists and libraries, deploying custom InfoPath templates and utilizing scripting to automate deployments

Mattel, SharePoint Designer / Developer, El Segundo, CA, 2008 – 2010

Involved in the Architectural Design of MOSS 2007 implementation leading the various phases of the Project Lifecycle; Gathered business requirements from business representatives and analyzed and designed the Project Management System; Used MVC software design pattern to design the user interface and logic for the solution based on client requirements.

- Used template design pattern to build the skeleton of some parts of the solution according to requirements
- Created a complex security plan to incorporate custom User Roles and Permission Levels
- Followed the Agile SCRUM methodology to deliver the Project Management System
- Developed Web Services using SOAP integrating the SharePoint system with J2EE based applications for effective data usage
- Designed and developed the metrics tracking and automated testing by creating custom Document Libraries with custom metadata relevant for Project management Tasks
- Created forms utilizing InfoPath 2007, capturing points, tasks, estimated time, developer, tester, tasks and test cases
- Created C# based Web Parts for metrics, facilitating customers and managers to decide between features and release time
- Automated nightly product testing by deploying XML based custom jobs
- Created custom Web Parts to illustrate the status of various project tasks/phases by XML parsing and using ActiveX and JavaScript
- Designed and implemented the migration of the deliverables across the Staging and production environments
- Conducted training sessions for business users and involved in the administration of the system

VeraSun Energy, SharePoint Migration Specialist,Sioux Falls, SD, 2007 – 2008

With the goal to efficiently unify and streamline the company's Web-based assets, involved in the migration of legacy HTTP/HTTPS accessible sites,

portals and Web content into SharePoint; charted the migration path and documented the approach to handle various components mapping legacy artifacts to SharePoint elements and automating page link management.

- Conducted the Pre-Migration Scan to detect and if need be map any legacy elements for successful migration to SharePoint
- Created custom SharePoint items like files, calendar items, contacts, customers and images with custom metadata
- Designed and developed custom Web Service based application to migrate content files to SharePoint, filtering by file types, crating Folder Structure and managing Metadata
- Created custom Master Pages and Page Layouts embedded with custom navigation, user controls and Web Parts
- Implemented Single Sign On (SSO) using Oracle Access Manager
- Extensively utilized CSS, AJAX to implement the look and feel as required by the client
- Designed and developed Web Parts for Reports that were automatically created from the custom Search module for specific executive users
- Created custom Content Types for Document Libraries and Lists to maintain data for Sales and Contract files creating appropriate custom columns
- For efficient user Permission management developed a custom User Clustering Web Part using C# ASP. and NET

Walton EMC, SharePoint Developer, Snellville, GA, 2006 - 2007

Installed and Configured Microsoft Office SharePoint Server in a large server Farm environment including the Web Front End Servers, application servers, Database Server and indexing Server; designed the Web application implementation with foresight to future growth, maintenance and independence; documented the Functional Requirements and Technical Solutions Design by writing the respective documents.

- Created personalized SharePoint sites like blogs, wikis, meeting workspaces and document workspaces
- Implemented Business Data Catalog and created Application Definition Files utilizing BDC Metaman to extract Vendor details from the Documented based CMS
- Created custom document libraries that held resume items which were automatically routed through custom workflows to required personnel for further actions
- Programmed .NET connected Web Parts and used them for interactive exchange of data.
- Created custom Web Controls and utilizing in the customized Windows SharePoint Services site-level Search that returned the Portal Server search results
- Developed State Machine Workflows that utilized InfoPath Forms and were kicked off, upon creation of specific List Items

- Customized the Tool Pane enabling the users to view and modify custom properties
- Using Excel Web Services designed and developed the application to calculate, set and extract values from workbooks, automating the process
- Developed Web Parts and displayed process level of various workflow tasks using Key Performance Indicators (KPI)

Nash-Finch, SharePoint Developer / Administrator, Minneapolis, MN, 2005 - 2006

Installed and configured the SharePoint Server 2003 in a Clustered environment; analyzed the system requirements and created State chart, Activity and Component Diagrams using Rational Rose; Created custom menu action items where in the features were enabled depending on the current user logged in.

- Customized the My Calendar Web Part, the My Inbox Web Part, and the My Tasks Web Part for the Personal sites using VB.NET
- Created complex workflows that included custom reminders for task completion and notifications on completion of certain tasks
- Developed various custom functionalities for the Intranet Portal used by the Marketing team and deployed as Features
- Created custom Site Definitions and custom List definitions and deployed by creating solution Packages
- Using SharePoint Designer implemented branding and custom look and feel across the SharePoint sites
- Designed an auto metadata populating solution on creation of custom List Items and documents with a custom workflow kickoff
- Carried out various Administrative tasks using the 'STSADM' utility and created and maintained various Timer Jobs

HealthSouth, SharePoint Developer, Birmingham, AL, 2005 – 2005

Involved in the design, development and administration of the corporate intranet portal site; Integrated IBM Cognos with SharePoint by creating custom Web Parts for reporting; Utilizing C#.NET, created a breadcrumb site navigation Web part that displayed the hierarchical location on a site on a WSS 2003 site collection.

- Modified the Page viewer Web Part in Visual studio.NET to include the most frequently used custom lists, libraries and folders
- Designed custom workflows for the HR department where in Employee records were archived following the company records management policies
- Created C#.NET based Web Parts that extracted sales data from SQL Server 2000 and displayed in user selected custom views
- Extensively used CSS/HTML to customize the Content Editor Web part for the departmental Portal sites

- Performed various application management tasks using Central Administration and managed Ative Directory users
- Created custom ASP.NET controls to render in the custom Web Parts used to connect to SQL database and edit/delete data as per user permission level
- Involved in End user training and Troubleshoot user issues with the application

Hubbell, .Net Developer, Orange, CT, 2004 – 2004

Participated in the analysis, design and development of the Logistics application based on J2EE specification; Developed custom components using the Model-View-Controller architecture; Used Object Oriented Analysis and Design (OOAD) methodology in implementation of the application.

- Used Servlets as Front Controller gateway into the system and EJBs to talk to the database. The client view was implemented utilizing JSP, HTML and XML
- Developed an HTML Parser and built DOM tree that generated XML documents and extensively used XSL for presentation
- Installed and configured Web Logic application server and wrote various shell scripts for administration purpose
- Automated mail generation and sent based on due dates of certain activities
- Designed and developed Web interface using JSP, Servlets, JDBC and JavaScript for administering and managing end users
- Created complex SQL queries and Stored Procedures and used JDBC connectivity to access the database
- Conducted usability testing of the application using JUnit Test and also automated load testing

Education

- BS in Electrical Engineering, University of Puerto Rico – Mayaguez Campus

This page intentionally left blank.

UNISYS

Resource 64

Microsoft Product Specialist (AD/Exchange Administrator)

Key Skills and Knowledge

Domain Expertise & Solutions

- Windows 2003 and 2008 Active Directory

Communication and Networking

- Active Directory Integrated DNS TCP/IP
- Telnet

Databases

- SQL

Operating Systems

- Windows 95/98/XP/7
- Windows Server NT/2000/2003/2008

Software/System Architecture

- Exchange 000/2003/2007/2010

Programming Languages & Tools

- PowerShell
- Command Line (DOS)

Call Center and Help Desk

- Remedy

Office Productivity Tools

- Outlook
- Excel
- PowerPoint
- Word
- Project
- Access

Professional Summary

16+ years professional experience including 6 years in Marine Corps and 14+ total years in IT; accomplished multiple projects / maintenance working with Exchange, Active Directory, PowerShell, ITIM; Master's Degree in Computer Information Systems and Bachelor's in Electrical Engineering.

- MCTS (Exchange 2007 and others) and MCSE
- Microsoft Certified Trainer - Exchange 2007, AD, SCCM 2007, Windows 2008 Server
- IBM Tivoli Identity Manger (ITIM) Systems Administration (Level III)
- PowerShell Automation to administer approx. 100,000 AD accounts and mailboxes

Employment History and Related Experience

Pinnacle/Unisys/Commonwealth, Exchange Administrator, Harrisburg PA, 2011-Present

Maintained Exchange 2007 / Active Directory environment with over 100K accounts; level III troubleshooting and support for all Exchange, Outlook, AD, and DNS issues; and provided Exchange / AD support for migration of approx. 100K accounts from end of life in-house user provisioning utility to IBM Tivoli Identity Manager (ITIM)

- Responsible for developing data scrubbing / integrity testing procedures to avoid significant "glitches" during migration of users to ITIM
- Responsible for PowerShell scripts to perform data culling, automation and scripting required by migration of users to ITIM
- Responsible for monthly Windows update / security patching of Exchange servers and Domain Controllers using SCCM and scripting
- Identified and referred network / firewall issues to network team for resolution

Exiis, Smart Source, Robert Half, and NetMedia Solutions, Independent Consultant, 2006-2011

Managed a variety of projects, including the designs for a migration of e-mail and communications to Exchange 2007; routine Maintenance /Troubleshooting / Disaster recovery of e-mail servers, domain controllers, Exchange and Active Directory issues; and assisted with migrations / installs for WaWa stations and for Wal-Mart

- Provided network troubleshooting support for connectivity, e-mail and printing issues
- Instructor of Microsoft Official Curriculum, inc. Security Design, Exchange 2007, Exchange 2003, Vista, Active Directory, 2003 Server, and XP average instructor rating of 93%
- Instructor of Comptia Official Curriculum, including Security+, A+ and Network+

UNISYS

Resource 64

Microsoft Product Specialist (AD/Exchange Administrator)

- Troubleshooting hardware / software issues of any possible nature before, during, and after class
- Set up Windows 2003/2000 servers with AD domains and up to 20 PC installs a week with Ghost and automatic scripting

Best Buy for Business, Business Technical Specialist, Tucker, GA, 2005 - 2006
Performed onsite consultation and evaluation of small business IT needs

- Participated in the preparation of business proposals for the owner / decision maker, incl. Windows Server and Cisco products

Solarcom, Hardware Engineer / Network Administrator, Norcross, GA, 2002 - 2005

Designed / implemented / maintained Windows 2003/2000 server / Cisco test environment; made server and networking equipment purchasing recommendations; and responsible for imaging /configuration / maintenance for 100s of servers and1000s of PCs

- Maintained DHCP, DNS, WINS, PXE, and user accounts
- Supervised configuration and use of Ghost in a PXE network boot environment for imaging

Brookhaven Christian School, Consultant, Greenville, NC, 2001 2002

Managed the design and implementation of Windows 2000 and Linux domains including the O.S. loading and configuration of the initial server, creation of backup policy and procedures, creation of 1st user accounts, creation of secure folders on server for individual users, and creation of shares and permissions

- Managed the design and implementation of TCP / IP network, security procedures and policies
- Managed installation, maintenance, upgrades, and troubleshooting of PC software and hardware

Cisco Systems, Level III Customer Support Engineer, Chelmsford, MA, 2000 - 2001

Installed, configured, and maintained software and hardware (XP /2000 / IOS / VCO /etc); Installed and configured various routers / gateways / terminal servers; and Reviewed and critiqued technical documents for publication on the Internet

- Performed troubleshooting of the most difficult problems, providing Level III support
- Configured switch for teleconferencing, voice prompts, touch tone, interface with TCP / IP
- Wrote batch programs to automate connection to various switches and routers

UNISYS

Resource 64

Microsoft Product Specialist (AD/Exchange Administrator)

U.S. Marine Corps, Network / Database Administrator, Jacksonville, NC, 1998 - 2000

Administered UNIX and NT domain (also 95 / 98) in fast-paced, Marine Corps unit with competing demands and critical decision requirements at headquarters level

- Officially recognized and decorated for design of personnel control database for deployment of combined arms detachment
- Managed Exchange / Outlook Servers and Clients for 1000 computer NT domain
- Wrote scripts for various tasks including batch files for boot processing and merging of multiple databases - Supervised, trained, counseled, inspected, and evaluated employees on a daily basis
- Responsible for IT department passing audit of maintenance procedures and inventory control for 1st time ever

US Marine Corps, Database / PC Maintenance, Jacksonville, NC, 1997 - 1998

Performed basic computer workstation and network troubleshooting and repair

- Supervised, taught, and performed database administration of barracks room inventory
- Made modifications of database to perform queries and produce reports as required

US Marine Corps, Crew Chief, Jacksonville, NC, 1994 - 1997

Supervised, taught, and performed in-flight troubleshooting and repair of major communications, radio, avionics, and electronics systems for Marine Corps helicopters

- Configured, maintained, and operated computerized testing systems for helicopters
- Performed final quality control checks on maintenance of helicopter to certify safety

Education

- 2001: M.S. (Masters) Computer Information Systems , Boston University, Boston, MA
- 1993: B.S. (Bachelors) Electrical Engineering, Embry Riddle Aeronautical University, Prescott, AZ

Professional Certifications

- 2008: MCTS – Exchange 2007
- 2006: MCT- Microsoft Certified Trainer

UNISYS

Resource 64

Microsoft Product Specialist (AD/Exchange Administrator)

- 2006: MCSE - Microsoft Certified Systems Engineer (Windows 2003 Server)
- 2006: A+ and Network+ - Comptia
- 2006: MCSA – Windows 2003 Server
- 2005: MCP - Microsoft Certified Professional (Windows XP)
- 2004: CCNA renewal - Cisco Wireless (no longer current
- 2001: CCNA - Cisco Certified Network Associate
- 1999: MCP - Microsoft Certified Professional (Windows NT Server)

UNISYS

Resource 65

Microsoft Product Specialist (Windows Server Systems Administrator)

Key Skills and Knowledge

Domain Expertise & Solutions

- Active Directory
- Microsoft Exchange
- Microsoft DNS
- BlackBerry Enterprise Server

Operating Systems

- Windows Server 2003
- Windows Server 2008
- Windows Server 2008R2

Software/System Architecture

- PowerShell

Call Center and Help Desk

- Remedy

Office Productivity Tools

- Microsoft Office Suite

Professional Summary

Highly proficient systems administrator with 25 years of experience in many phases of the information technology field, effective supervisor and trainer of technicians, managed more than 300 domain controllers in several different environments

- Project Lead for active directory forest level upgrade from Windows Server 2003 to Windows Server 2008 R2
  - Migrated many from physical to virtual servers
  - Administered over 100,000 mailboxes for 70,000 users on Microsoft Exchange 2007
- Managed BlackBerry Enterprise Servers (5.0) used by 4,000 users
- Consistently identified processes for automation – developed and implemented several scripts to save hundreds of man-hours vs. previously used processes.

Employment History and Related Experience

Unisys, Commonwealth of Pennsylvania, System Administrator Consultant, 2009 - Present

Responsible for security patch management for 400 domain controllers and exchange servers

- Migrated 15 Microsoft Exchange Servers to 2003 version; over 4,000 mailboxes migrated with 100% success rate
- Managed 4000 user accounts and 2500 Windows XP-based workstations on 15 isolated networks
- Oversaw the migration of five separate NT domains to Active Directory – project completed on time with zero user impact
- Led project to upgrade 8 domain controllers from windows 2000 server to Windows Server 2003 (64-bit)
- Upgraded remote installation services server to Windows Deployment Server in production and test environments– providing faster imaging of workstations and support for emerging technologies

Elite Systems, Microsoft Exchange Consultant, Harrisburg PA, 2008 - 2009

Responsible for hardware and software troubleshooting of 82 Windows-based servers; provided day-to-day support for wide range of standard applications including: MS Office suite, Form Filler, PureEdge ICS Viewer; and managed networking issues dealing with TCP/IP, DNS, SMTP, and DHCP.

Air Force Flight Test Center, Network Systems Administrator, Detachment 3, 2004 – 2008

UNISYS

Resource 65

Microsoft Product Specialist (Windows Server Systems Administrator)

Consistently provided users with support for peripheral devices, such as, printers, scanners, plotters and all-in-one devices; managed $500,000 budget for work section

- Managed BlackBerry Enterprise server for 2,500 users
- Translated specific needs into Computer systems requirements
- Directed various teams of technicians on many different projects

Network Control Center, Helpdesk Manager, Andersen AFB, GU, 2003 – 2004

Supervised up to 40 individuals, dealing with personal issues, scheduling work hours, assigning daily duties, and evaluating performance

- Authored several procedures pertaining to server and workstation setup, which were adopted as the standard for use by all Air Force personnel world-wide.
- Prepared performance reports and recommended decorations for subordinate individuals

Other Employment History

- Network Control Center, Workgroup Manager Trainer, 36th Communications Squadron, Andersen AFB, GU, 2002 – 2003
- Network Systems Administrator, Detachment 3, Air Force Flight Test Center, 1999 – 2002
- Data Systems Operator, Detachment 3, Air Force Flight Test Center, 1997 – 1999
- Information Systems Security Officer, 48th Intelligence Squadron, Beale AFB, CA, 1993 – 1997
- VAX System Administrator, Foreign Aerospace Science and Technology Division, Wright-Patterson AFB, OH, 1991 – 1993
- Teletype Operator, 609th Tactical Control Squadron, Hessisch-Oldendorf AS, GE, 1989-1991
- Information Systems Operator, 3026th Communications Squadron, Sheppard AFB, TX, 1987 – 1989

Education

- High School, Northern York High School, 1986

Professional Certification

- ITIL Foundation Examination, Loyalist Certification Services, 2012

Midrange Infrastructure Architect_Engineer

This page intentionally left blank.

UNISYS

IBM

Resource 66

Midrange Infrastructure Architect/Engineer

Key Skills and Knowledge

- Cloud Computing
- Service-Oriented Architecture (SOA)
- IT Infrastructure Architecture
- Storage Area Networks (SAN)
- Disaster Recovery
- Data Center Facilities
- Open Systems – Microsoft Windows, AIX, Linux
- System X (xSeries) and System P (pSeries) hardware
- WebSphere Application Server
- Cisco routers and switches

Professional Summary

Certified Infrastructure Architect for IBM Global Technology Services in the IT Strategy and Architecture Service Product Line, specializing in Cloud Computing and Services Oriented Architecture (SOA) Infrastructure. More than twenty years experience in Information Technology, specializing in Local-, Wide-, and Storage-Area Networking, WebSphere, Microsoft Windows, UNIX and server and storage hardware. Commands exceptional communication skills, refined through years of experience in customer service, project management and consulting. Received numerous professional awards from the IBM Corporation, including recognition for leadership, planning, and technical ability. Recognized as a 2-year consecutive member of the IBM Hundred Percent Club for outstanding achievement in customer satisfaction and value to the business.

Employment History and Related Experience

IBM, Certified I/T Architect & Cloud Focal Point, Gaithersburg, MD, 2001-To Date

Delivery architect, serving many of IBM's largest clients in public and private sectors; cloud computing focal point, providing thought leadership to clients and peers in the emerging field of cloud computing; member of the IBM SOA Acceleration Team.

- Presenter to the IBM Academy of Technology regarding SOA infrastructure and Cloud Computing.
- Author of several IBM Redbooks in the fields of storage and content management.

Nationwide Healthcare Provider, Engagement Manager / Lead Architect, 2011-To Date

Led a team of ten people to perform a readiness assessment for a new nationwide health care system.

- As a result of the assessment, we created a wholesale transformation program to fundamentally change the way IT operates, including creating high availability architecture, new processes and procedures, and a completely new organization.
- Works directly with C-level executives, application and infrastructure teams to develop the operating model and architecture for the new health care system.

Global Financial Services Company, Engagement Manager / Cloud Architect, 2010-2011

Led multiple teams of people to perform cloud readiness assessments for multiple lines of business.

- Assessed relationship between IT and the organization to determine optimal cloud delivery and consumption profiles.
- Analyzed computing workloads for applicability to a cloud delivery model.
- Conducted gap analysis of current and future state IT capabilities.
- Delivered analysis and recommendations to C-level executive and direct reports through presentation materials and briefing, including roadmaps.

Large Educational Medical Center, Engagement Manager / Cloud Architect, 2010-2010

Led a team of 3 people to perform a cloud readiness assessment for an educational medical center.

- Leveraged IBM tools to determine optimal cloud delivery and consumption profiles; analyze computing workloads for applicability to a cloud delivery model; and conduct a gap analysis of current and future state IT capabilities.
- Delivered analysis and recommendations to C-level executive and direct reports through presentation materials and briefing, including roadmaps.

Pharmaceutical Manufacturer, Engagement Manager / Cloud Architect, 2010-2010

Led a team of 3 people to perform a cloud readiness assessment for a global IT organization.

- Analyzed various aspects of applications and infrastructure.
- Provided industry data to compare current state with best practices.
- Provided metrics and methodology to demonstrate the business value of cloud computing.
- Assessed organizational alignment with business objectives.
- Delivered analysis and recommendations to executive management through presentation materials and briefing, including roadmaps.

US Federal Government Agency, Cloud Consultant, 2010-2010

Facilitated client workshops and provided thought leadership to develop a cloud computing strategy.

- Led a review of IT and agency goals, current state capabilities, and future state targets and conducted a gap analysis.
- Made recommendations regarding adoption of cloud delivery models and cloud workload affinities and defined roadmaps to close gaps.
- Provided analysis and recommendations to C-level executives and staff in the forms of presentation and white paper.

IBM

Resource 66

Midrange Infrastructure Architect/Engineer

Regional Transportation Services Provider, Cloud Consultant, 2010-2010

- Participated in client workshops and provided thought leadership to develop a cloud computing strategy. Assisted in a review of IT and business goals, current state capabilities, and future state targets and conducted a gap analysis.
- Recommended adopting cloud delivery models and defined cloud workload affinities and defined roadmaps to close gaps.
- Presented analysis and recommendations to C-level executives and staff.

Global Higher Education Provider, Infrastructure Architect / Lead Architect, 2009-2010

Developed desktop services, storage, and server architecture for a globally integrated enterprise.

- Led a review of application performance on a global scale and made recommendations for application deployment and remediation.
- Worked within a cross-LOB team to provide thought leadership and drive high quality deliverables.
- Provided analysis and recommendations to C-level executives and staff.

US Professional Sports League, Infrastructure Architect, 2009-2009

Performed an SOA infrastructure workshop for an IT organization transforming to a shared services model.

- Analyzed computing, storage, and facilities services and provided strategic and tactical recommendations to improve services maturity and resiliency.
- Helped create a data center strategy aligned with the enterprise shared services model.
- Provided analysis and recommendations to executive management in the form of presentation materials and briefing, including roadmaps with cost, resource, and timeline estimates. As a result, IBM was awarded significant follow-on work and public recognition.

Staffing Provider, Infrastructure Architect, 2009-2009

Performed an SOA infrastructure readiness assessment for a rapidly-maturing staffing provider.

- Provided strategic and tactical recommendations to help align IT with business drivers.
- Facilitated a High Availability (HA) solution workshop to select an appropriate HA solution based on business and technical requirements.

Resource 66

Midrange Infrastructure Architect/Engineer

- Demonstrated the business value of IT.
- Provided analysis and recommendations to management in the form of presentation materials and briefing, including roadmaps with cost, resource, and timeline estimates.

Telecommunications Provider, Lead Architect, 2008-2009

Responsible for assessing multiple data centers and associated infrastructure and creating recommendations for infrastructure optimization.

- Analyzed servers, storage, and network components as well as data center facilities.
- Worked with financial analyst to create cost models for future state scenarios.
- Provided analysis and recommendations to C-level executive in the form of presentation material and briefing.

State Government, Lead SOA Infrastructure Architect, 2006-2008

- Lead Infrastructure Architect for a Service-Oriented Architecture (SOA) application development project.
- Led a team of 12 people to architect, design, and implement a virtualized, multi-site infrastructure.
- Deployed a dual-purpose remote data center to support infrastructure and application testing, and disaster recovery.
- Responsible for over $15 Million in revenue. Received numerous awards for delivery excellence and outstanding customer satisfaction.

US Military, Infrastructure Architect, 2004-2004

Responsible for designing, implementing, and documenting an Enterprise Architecture for the newly expanded US Armed Forces interoperability testing center, including analysis of current and projected storage requirements and integration of emerging storage technologies. Received exceptional reviews from the client and IBM account and project teams.

Education

Computer Science, University of Maryland

Certifications

Key Courses and Training

- US Department of Defense Secret Clearance, 2004
- Certified Novell Engineer, 1992
- IBM Professional Server Expert, 1997

Resource 66

Midrange Infrastructure Architect/Engineer

Publications

- IBM Total Storage Productivity Center: The Next Generation, in: IBM Redbook, IBM ITSO, 2006, ISBN/ISSN: 0738495948
- IBM Enterprise Content Management and DR550 for e-Mail Archiving and Records Management, in: IBM Redbook, IBM ITSO, 2007
- IBM Information Lifecycle Management Services for enterprise content management, in: IBM Redbook, IBM Press, 2008

Membership in Professional Organizations

- The Open Group
- Master Certified IT Architect

This page intentionally left blank.

UNISYS

IBM

Resource 67

Midrange Infrastructure Architect/Engineer

Key Skills and Knowledge

Methodologies:

- Project Management (PMI)
- Software Development Life Cycle (SDLC)
- Object Orient (OO) Rapid Application Development (RAD) and Rational Unified Process (RUP)
- Agile PLM Solution

Technology

- Peregrine
- SM7
- Rational ReqPro
- ClearCase
- ClearQuest
- Clarity
- Mercury (Test Director, Win runner, Load runner)
- Compuware (QA Run, QA Director, Track Record)
- Documentum
- MS PowerPoint
- Microsoft Office 95, 97, 98, 2000,2003,
- MSWord
- MS Excel
- MS Project 98, 2000, 2003
- MS Outlook
- Exchange Visio2000
- Windows 3.1, 95, 98, NT, XP, 2000, 2003
- UNIX
- IBM PC
- IBM Compatible PCs
- Client/Server
- RS6000
- DS48XX, DS53XX, DS8XXX
- IBM Mainframe
- IBM SAN
- IBM Storage
- Novell Network
- Internet/ Intranet and 3COM Network
- Lotus Notes, Lotus Notes Architecture, Lotus

Professional Summary

Technology Executive with the proven ability to analyze, develop, implement and lead application deployment initiatives cross platform with global teams following best practices, quality assurance policies, processes and methodologies. Operational and data center support as well as high availability management support. Remarkable career with a proven ability to build and lead multiple cross-functional teams.

Employment History and Related Experience

CTG/IBM – JCP, Systems Availability Manager, 2011–To Date

Manage through to the successful resolution of hardware and software availability issues (San Storage, VMX, San Switch, Mainframe, Mainframe hardware refresh activity, Mainframe upgrade and consolidations, UNIX operating system Patching, Server Consolidation from (P6 technology to P7).

- Act as a customer advocate and situation manager in support of client's IT environment as it relates to Availability Management working with IBM product and support organizations.
- Host IBM status overview meetings to review outstanding or overdue tasks/events, review Problem Management Records and their current status as well as discuss new initiatives and acquisitions to be incorporated into current activities.
- Assist with identifying trends and creating action plans through analysis and review of Problem Management Records (PMRs). Review and understand the service requests (PMRs) opened with the relevant IBM Support Center(s) over the previous quarter and offer technical advice and guidance with regard to those PMRs.
- Periodically review with client the PMRs they've placed with IBM to recognize and analyze trends and emerging issues.
- Provide advice and guidance on how to resolve hardware and software availability issues to prevent reoccurrence.
- Assist client with review and planning for IBM product deployment and maintenance to reduce the risk of potential exposure to client based on knowledge of client's IT technology strategy, current IT environment, knowledge of IBM's products, and industry best practices for systems and availability management.
- Assist in periodic review of client's systems deployment, change control and systems management processes.
- Assess client's current and ongoing readiness to achieve its IT availability objectives.

IBM

Resource 67

Midrange Infrastructure Architect/Engineer

Administration I, II Lotus Development I, SM7

- Review and recommend improvements on the current baseline for the availability of IBM Systems, establishing targets and dates for improving where necessary and appropriate.
- Ensure that all work being performed by IBM is planned, documented and reviewed with client prior to execution of work.
- Facilitate communication between client and IBM Product Specialists in the relevant and appropriate IBM development or support organizations.
- As informed and engaged by the client Project Manager, assist with communication to the appropriate IBM support teams all planned changes to IBM hardware and software products. Advise client of potential impact to planned changes.
- Work with key client leadership and technical decision makers to attain high levels of system availability and stability in the client's IT environment.
- Work globally with all team members.

Rose Int. – PepsiCo, Senior Project Manager – Infrastructure, 2007–2011

Managed multi types of projects (San Storage, VMX, San Switch, Refresh hardware, UNIX operating system Patching, Server Consolidation (SCON, SCONI, SCONII from P6 technology to P7) and upgrades, Oracle financials refresh, SAP Storage, DATA ITO Refresh, Corporate UNIX Refresh projects, Security remediation software implementation, Offshore coordinator and other projects as assigned.

- Led PMM Meeting to review outstanding or overdue tasks/events
- Coordinated the EPMO and the business units to adhere to PepsiCo milestone checkpoints and document quality assurance processes.
- Developed process flows for all current and future application development.
- Insured that all UNIX servers were SOX compliant.
- Maintained centralized oversight of project management documents including Project Schedule, Risks, Issues, and Change Management, Signoff documents and others as required. Work with the EPMO program management team, the functional and technical development leads to ensure that the issues, risk, and change management processes are executed efficiently, effectively, and to the appropriate standards.
- Managed the interface between the UNIX team and the offshore team.
- Managed iCare, offshore communications for daily turnover and all communications.
- Worked globally with all team members.

Red River Systems – 7-Eleven, Senior Project Manager – Wholesale Transition, 2007–2007

Managed multiple types of projects. Led PMM meeting to review outstanding or overdue tasks/events. Coordinated the EPMO and the business units to adhere to 7-Eleven milestone checkpoints and document quality assurance processes.

IBM

Resource 67

Midrange Infrastructure Architect/Engineer

Worked with the outside development team to keep project schedule properly updated and in sync.

- Developed process flows for all current and future application development.
- Coordinated the EPMO and SQA teams to ensure that the Wholesaler transition program adheres to 7-Eleven milestone checkpoints and document quality assurance processes.
- Maintained centralized oversight of project management documents including Project Schedule, Risks, Issues, and Change Management, Signoff documents and others as required. Work with the EPMO program management team, the functional and technical development leads to ensure that the issues, risk, and change management processes are executed efficiently, effectively, and to the appropriate standards.
- Worked globally with all team members.

Rose Int. – PepsiCo, Senior Project Manager – Infrastructure, 2006–2007

Managed multi refresh projects replacing or decupling servers or expanding capabilities. Worked with all DBA (Oracle, PeopleSoft, SAP, Informatica) verify and validate all database activities are complete and that the UNIX team has build the proper directories and give the correct access required to run each application. Coordinated with the all associated teams to verify status and resolve issues.

- Worked with the outside development team to keep project schedule properly updated and in sync.
- Maintained SOx Compliances
- Maintained centralized oversight of project management documents including Project Schedule, Risks, Issues, and Change Management, Signoff documents and others as required.
- Work with the EPMO program management team, the functional and technical development leads to ensure that the issues, risk, and change management processes are executed efficiently, effectively, and to the appropriate standards. Hold meeting as needed.
- Contributed to program status reports and program planning meetings.
- Worked globally with all team members.
- Worked with Vendors to acquire refresh hardware.

Computer Science Corporation – General Dynamics, Manager Global Transformation Solutions (Program Process Manager), 2005–2006

Created Process flow for all current and future application development for GDAISource. Maintained project schedule. Created SOx compliance process checkpoints to match SQA CheckPoints to eliminate double work. Validated SOx compliance.

- Maintained centralized oversight of project management documents including Risks, Issues, and Change Requests, Hanko documents and others as required.

IBM

Resource 67

Midrange Infrastructure Architect/Engineer

- Worked with the GD management team as well as the functional and technical lead to ensure that the issues, risk and change management processes are executed efficiently, effectively, and to the appropriate standards.
- Worked with the GD team to validate UAT testing scripts for GDAISource.
- Contributed to program status reports and program planning meetings.

Capstone – 7-Eleven, Program Process Manager/Schedule Project Manager, 2005 – 2006

Managed multi project schedule linked together. Hosted PMM Meeting to review outstanding or overdue tasks/events. Coordinated with the EPMO and SQA teams to ensure that the STEER program adhered to 7-Eleven milestone checkpoints and document quality assurance processes. Worked with the outside development team to keep project schedule properly updated and in sync.

- Developed process flows for all current and future application development.
- Coordinated with the EPMO and SQA teams to ensure that the GDS program adhered to 7-Eleven milestone checkpoints and document quality assurance processes.
- Administered SOx compliance process assessments to match SQA Checkpoints to eliminate double work.
- Validated SOx compliance for two major retail solutions, Programs Global Data Synchronization and Retail Initiated Invoice.
- Maintained centralized oversight of project management documents including Project Schedule, Risks, Issues, and Change Management, Signoff documents and others as required. Worked with the EPMO program management team, the functional and technical development leads to ensure that the issues, risk, and change management processes are executed efficiently, effectively, and to the appropriate standards.
- Administrator of the documentation development and signoff process.
- Contributed to program status reports and program planning meetings.
- Worked globally with all team members.

Legacy Solutions, Senior Project Manager, 2004 –2005

Responded to all RFP's. Technical Interviewer for all potential new hires. Created Project Plan for all projects.

TekSystems – Sprint, Senior Project Manager, 2004 – 2004

Developed and maintained relationships with key stakeholders (Internal and external). Presented key deliverables and milestones to stakeholders. Established scope of project objectives to address core business requirements. Facilitated project review meetings with stakeholder to validate scope.

IBM

Resource 67

Midrange Infrastructure Architect/Engineer

- Build and lead execution of project plans between multiple departments.
- Managed issues, change management, project risks and escalation with the executive management team.
- Resolved major issues between the stakeholders and outsource team.
- Administered and tracked all project schedules, issues, and document management through DOORS and Sprint Online.
- Established 2 teams for project development.
- Successfully managed over 51 people through several projects.
- Worked with global team members.
- Reviewed possibility of using the Agile PLM Solution, Sprint Management did not make decision before project was completed.

Compuware (PM Leadership at Multiple Clients), Project Director – T-Mobile, 2001–2004

Established and managed team for mission critical testing. Presented key deliverables and milestone to key stakeholders. Facilitated project issues with third party vendor. Developed and implemented release process and automation team. Created Process Improvement plan for releases and test case development.

- Gathered errors and status from team for reporting purposes.
- Managed multiple teams who were responsible for Load and stress automated tools (QA Load).
- Led Web security testing and created user review standards.
- Created each readiness assessment and worked with the architect to prepare viability assessment.
- Created and presented weekly reports for CIO and his direct reports to identify development and QA outstanding issues.
- Worked with team members from several countries.

UICI, Project Director, 2003-2004

Organized recruiting and hiring process for initial QA Team. Instituted testing process and reviewing plans. Evaluated, implemented, and managed test automation tools. Led team that utilized QA Run, QA Director, Track Record and created reports from QA Director that allowed the Executives of UICI to view status of the testing progress and issues.

- Trained and mentored team to gain information for a quality IT assessment and QA perspective.
- Created IT Client Server Assessment Deliverable and presented this assessment to the Executive team.
- Hands-on technical management of QA organization expanded.
- Authored IT Mainframe Assessment Deliverable and presented this assessment to the Executive team.
- Established team for Smart Screen Testing and the test plan to accomplish these tasks.

Resource 67

Midrange Infrastructure Architect/Engineer

- Successfully utilized Compuware Quality Point Methodology.
- Adhered to HIPPA Requirements.

Alliance Data Systems (ADS), Senior Project Manager, 2002-2003

Interviewed members of the IT department to understand work flow and their environment. Created documents that would allow IT department to properly resolve issues without leaving steps out that would cause additional problems or errors. Created Environmental Design Deliverable that allowed IT team to better understand the network, server, and data flow.

- Evaluated CA product against home grown in-house tracking system.
- Created project plan and project schedule as well as a working model that would allow the ADS team to quickly implement a tracking system that would be utilized across ADS.
- Presented deliverables to key stakeholders.

TXU/Oncor, Senior Project Manager, 2001-2002

Resolved issues of application coming on line on time to keep TXU from fines for not meeting Senate Bill Seven require start date for TEEM program. Proposed new rewrite for the TEEM application for better response and user friendly screens as well as utilizing more current technology.

- Established 2nd team to deliver proposed rewrite. Followed SDLC methodology and CMMI process documentation and requirement for TEEM project.
- First project TXU utilized CMMI process to move from CMMI level 2 to Level 3.
- Coordinated requirements between PUC and Senate Bill Seven requirements and changes.
- Created weekly reports to client as well as prototype demo.
- Reviewed QA output for completeness and functional coverage.
- Created test requirements for both functional and integration testing.
- Created requirements for the stress and memory lab testing.
- Utilized Mercury tools for automated testing.
- Created test scripts to validate client required results.
- Managed and monitored quality testing throughout the project life cycle.
- Created end user documentation.
- Delivered product one month early and $40,000 under budget ($400,000 total budget).

DMR, Director – eBusiness, 2000–2001

Created the eBusiness consulting and delivery organization within the Dallas marketplace. Grew the practice to a staff of 27 from conception and generated revenue of $1.3M in 7 months.

Resource 67

Midrange Infrastructure Architect/Engineer

- Developed several recommendations to help IBM implement a standard authentication, authorization and entitlement process across the multitude IBM intranet Web sites.
- Created quality assurance consulting and delivery team to assist Fortune 500 organization in developing proper QA testing methodologies and tracking processes.

The Harbor Group (THG), Vice President – Internet Technology Solutions, 1999–2000

Led implementation of sales force automation at Verizon, resulting in $12M annual savings. Created the Dallas practice for eBusiness consulting and delivery organization. Grew group to a staff of 42 from conception and generated revenue of $1.7M in 12 months. Managed vendor relationships with Sun Microsystems, Forte, IPlanet, E-Security Lotus, IBM and BMC. Initiated the sale, in conjunction with project management of an on-line candidate Web review site. Estimated savings to client of $500K annually.

EDS/MCI Systemhouse, Director - System Integration, 1993–1999

Created the Internet management consulting and delivery organization for the US marketplace. Grew the organization to a staff of 142 from conception and generated revenue of $57M in a 3-year timeframe.

- Year 1 generated $6M, with no revenue target in place. Year 2 generated $18M, exceeded revenue target by 120%. Year 3 generated $33M, exceeded revenue target by 132%.
- Managed vendor relationships with Sun Microsystems, Lotus, IBM, Tivoli, BMC, Mercury, Vision Jade, CommerceOne, Net.Commerce, FileNet and MSFDC.
- Managed international teams from several global locations.
- Successfully led the project management of the outsourcing of Oracle, network and messaging infrastructure resulting in a $1.2M annual savings.
- Managed the healthcare job posting Web implementation project that resulted in a $1M annual savings.
- Managed MCI Systemhouse's exhibition at the LotuSphere trade show and generated revenues of $2.1M.
- Utilized Lotus, Microsoft ASP, JAVA, HTML, Cold Fusion, Oracle, People soft, SQL, Access in most projects.
- Created QA Organization and or enhanced groups to meet the challenge of releasing Error free software.
- Utilized QA testing tools such as Mercury.
- Utilized methodologies such as SDLC, modified Six Sigma, EDS Methodology

GTE, Senior Systems Engineer - Lead (last position held), 1978–1993

Responsible for the design and implementation of a worldwide backbone network mainframe support organization. Established new and maintained the

existing network for five temporary locations.

- Assigned as the lead member of acquisition team to oversee the merger of GTE and Contel's backbone mainframe systems.
- Developed outside facility engineering plans (FAST) for GTE Southwest.
- As a Top Analyst, responsible for generating all outside plant reports (ASIST and RAMIS retrieval).

Education

Computer Science, Angelo State University, San Angelo, Texas

Certifications

- Computer Security Institute (CSI) – Computer and Network Security
- Intrusion Detection and Counter measures – 2001
- PMI – Certification Training

Memberships

- PMI – 559318
- CSI – CI850303

UNISYS

IBM

Resource 68

Midrange Infrastructure Architect/Engineer

Key Skills and Knowledge

- AIX
- LPAR
- DLPAR
- Micropartitioning
- Virtualization
- Hypervisor
- virtual IO
- VIO
- APV
- PowerVM
- Shared Ethernet Adapters
- HACMP/PowerHA 6.1 and 7.1 (High Availability System Design)
- Shared SCSI
- NPIV
- Tivoli Storage Manager 5.3 and 6.1 (TSM)
- UNIX Security
- AIX filesystem e expertise
- p5, p6, power6,power 7
- RS/6000
- Legato (AIX)
- IBM Blade Center
- DS 4000 Series Storage
- WebSphere 5.1 and 6.0 (Application Server and Network Deployment)
- IBM XIV
- GPFS and EMC: CLARiiON & Symmetrix (PowerPath).

Professional Summary

Certified Senior-level Managing Consultant at IBM with over 13 years of diverse experience. Proven ability to lead, manage, design, plan, and implement IT solutions with the pSeries (AIX) servers with supported new applications, processes, and complete lines of business. In addition, using specific TSM skills have proven record of accomplishment, with Tivoli Storage Manager on large-scale implementations.

Gave advice and made contributions on a Redbook named SAP Applications on IBM PowerVM. This was published in January of 2009 (SG24-7564-00 ISBN 0738485004).

Employment History and Related Experience

IBM, Managing Consultant, pSeries (AIX), 2006-To Date

Level 2 IT Specialist Certification Expert Level in Technical Services and Infrastructure & Systems Management specializations. Implemented IBM Blade Center with XIV Storage for both x (RedHat) and p (AIX) Blades. Implementation of WebSphere on AIX and NT environments for a Global Cluster (Load Balanced) configuration using Network Deployment

- Implemented IBM AIX Virtual Server with shared Ethernet and storage (NPIV) for over 35 clients.
- Implemented and Designed HACMP clusters on HACMP Versions 5.4 and 6.1.
- Implemented IBM SAN Switches and DS/4000 product line with Flash Copy.
- Support clients with large and small scale SAP environments using Oracle.
- Built 4 p595 servers with VIO Server and over 25 VIO clients on each frame using NIM.
- Installed Tivoli Storage Manager 5.3/6.1 and over 6 years experience supporting large-scale TSM environments for major retailers.

Insurance Company, Senior AIX Admin. AIX p5 Series, 2005-2006

Implemented EMC Legato on AIX 5.3 with SRDF using Symmetric. Attached Storage using EMC PowerPath to AIX systems on both the Symmetric and Clarion. I also performed allocation of storage using the ECC Console to perform such tasks. Setup Fiber Zones with ECC console and directly with the MDS 9000 family switches.

- Setup IBM AIX Virtual Server with shared Ethernet and storage on 10 p570 Systems and 1 P595.
- Worked with SymCLI (Symmetrix Command Line Interface) on AIX Systems.

Retail Company, Senior AIX Admin. AIX RS/6000, 2001- 2005

During my career at Ahold, administered 300 RS/6000 F50 servers in a complete distributive environment. Responsible for IBM S70 running production software for a million square foot warehouse. In charge of Day-to-Day operations with fixing

operating system problems installations of new equipment including operating system build out, writing perform scripts and administrative tasks for all 300 servers in remote locations.

Retail Company , AIX Administrator and Project Manger, 1998-2001

Implemented AIX to be intergraded with the IBM 4690 operating system, for Electronic Fund Transactions with IBM 4693 and 4694's. Developed a storewide user manual, training program, and help desk support/procedures. Using Tivoli Management Enterprise was able to manage all aspects of the installation and maintenance over 300 stores. Created and altered computer programs to streamline departmental operations and improve efficiency.

Major Pharmaceutical, Power7 VIO Implementation and Design for 6 p795's running SAP Lead Technical Advisor , 2011-To Date

Implemented 6 p795's with four VIO Servers, NPIV, Live Partition Mobility, and design load balanced shared Ethernet adapters between VIO clients. Assist customer with transition from HP to IBM AIX and make sure customer uses best practices with the new IBM hardware and AIX 7.1 operating system. This project will also include starting next year designing and implementing PowerHA with SAP.

Medical Center in Newark New Jersey, Project/Engagement Manager and Technical Advisor PowerHA implementation, 2011

Provided a total solution from proposal to delivering a site to site PowerHA solution. Provided guidance and technical advice to the assigned resources to the project and oversaw the entire delivery.

Major Payroll Company, Technical Project Advisor to assist customer with migrations Engagement Manager and Technical Project Advisor, 2011-To Date

Worked as a liaison between the customers Project Manager and the System Administrators that were performing the logical partition migrations, to improve the migration times and reduce any risk in the process.

Major BC/BS insurance provider for the state of New Jersey, PowerHA GLVM Implementation, Engagement Manager and Lead Architect, 2011

This work was part of a larger project being lead by IBM Software group, which initially was using a clustering product that was lacking the required features to support the customer's requirements. Halfway into the project, it was determined that PowerHa should be used instead. The customer requested IBM to design and implement PowerHA to have an application fail over from one site to another in case of disaster with a fail over up time less than 5 minutes. My role was to architect and lead the implementation of a Cross-site IBM PowerHA (High Availability) with GLVM (Global Logical Volume Mirroring) for Disaster Recovery solution.

Resource 68

Midrange Infrastructure Architect/Engineer

University Hospital, BCRS TSM Specialist, 2010-2011

Customer had no DR stagey or plan to recover AIX systems via TSM. They were not performing a daily offsite tape pool copy. Wrote all of the recovery procedures for TSM and AIX system bare metal restores.

- Provided TSM Expert support at IBM BCRS during their first DR event which was very successful by following my procedures and changes I made to setup their TSM server to perform DR events such as sending tapes offsite.

Drug Company, Power7 P595 VIO Implementation and Design, VIO Design/HACMP Specialist, 2008-2010

Implemented 8 p595's with Dual VIO Servers, designed load balanced shared Ethernet adapters between VIO clients. Created over 50 VIO Client LPAR's for AIX and Linux Red Hat. Implemented IBM Blade Center and XIV Storage for AIX and x/p Blades.

- Helped migrate servers from older hardware to the newer power6 p595 servers.
- Implemented and designed a High Availability System for 14 HACMP clusters running AIX 6.1 with HACMP 5.4.1.

Manufacturing Company, Tru64 To AIX/pSeries SAP Migration- AIX v5.3 LPAR, 2007-2008

Install servers and help assist customer with Migration from Tru64 to AIX 5.3. Re-wrote all Tru64 Korn Shell scripts to AIX 5.3 system commands. Provide ongoing support and assistance as customer requests during key project milestones.

State Government, AIX 5.3 VIO Implementation, VIO Implementation Specialist, 2007

Implementation of VIO Server and assisted customer with Design.

Water Company, DR Assistance, DR Specialist, 2007

Assisted customer with full DR restore of AIX systems with TSM Server.

Energy Utilities Company, HACMP Scope and assistance with Implementation, 2007

HACMP Scope and assistance with Implementation.

Manufacturing Company, VIO Server Implementation, 2007

- Implemented DUAL VIO Servers to p570 server.
- Provided higher serviceability with multiple Virtual I/O Servers. Virtual SCSI redundancy and Shared Ethernet redundancy.

Resource 68

Midrange Infrastructure Architect/Engineer

City Government, HACMP Implementation 5.4, HACMP Specialist, 2007

HACMP Implementation 5.4 with DB2 failover. Wrote stop/start scripts and monitoring process for DB2 failover.

Candy Manufacturing Company, AIX Upgrade Assistance, AIX Server Specialist, 2007

Assisted customer with upgrade from 5.2 T/L 4 to 5.2 T/L 9.

Drug Company, P595 VIO Implementation and Design, VIO Design/HACMP Specialist, 2007

Implemented 2 p595's with Dual VIO Servers, designed load balanced shared Ethernet adapters between VIO clients.

- Created over 40 VIO Client LPAR's and helped migrate servers from older hardware to the newer p595 servers.
- Implemented 14 HACMP clusters running AIX 6.1 with HACMP 5.4.1.

Insurance Company, 2006
HACMP Upgrade from 5.1 to 5.4 and convert customer from serial heartbeats to disk heartbeats.

Water Company, TSM migration and pSeries Services, Tivoli Storage Manager Specialist, 2006-2007

Implemented AIX 5.3 Server and migration from older TSM Server. Wrote TSM scripts for automation of DR pool and daily processes.

City Government, Dual VIO Server Implementation. 2006

Provided higher serviceability with multiple Virtual I/O Servers. Virtual SCSI redundancy and Shared Ethernet redundancy.

Retail Company, Dual VIO Server Implementation, 2006

Provided higher serviceability with multiple Virtual I/O Servers. Customer needed to have VIO clients boot from SAN. Virtual SCSI redundancy and Shared Ethernet redundancy.

Water Company, AIX Performance Analysis, 2006

Performed health check on 2 p690 servers.

- Provided detailed documentation on areas of weakness.
- Recommended better practices.

Retail Company, Project Manager, 2006

Assisted customer with AIX 4.2 systems

Resource 68

Midrange Infrastructure Architect/Engineer

Manufacturing Company, Tru64 To AIX/pSeries SAP Migration - AIX v5.3 LPAR, 2006

Install Servers and help assist customer with Migration from Tru64 to AIX 5.3.

- Re-wrote all Tru64 Korn Shell scripts to AIX 5.3 system commands.
- Customized monitoring solution for the AIX pSeries servers, and develop solution for CUPS printing on AIX.
- Provided ongoing support and assistance as customer requests during key project milestones.

Retail Company, Full Time TSM Administrator, TSM Administrator/Project Manager, 2006

Implemented TSM 5.3 and perform project manager responsibilities for TSM migration from data center in Chicago to Troy Michigan.

Manufacturing Company, Tru64 To AIX/pSeries SAP Migration- AIX v5.3 LPAR, 2006

Installed Servers and assisted customer with Migration from Tru64 to AIX 5.3. Re-wrote all Tru64 Korn Shell scripts to AIX 5.3 system commands.

Warehouse/Distribution Company, Implementation of p570 and DS/4300, 2006

Implemented p570 and DS/4300.

- Assisted customer with hardware migration from older RS/6000 hardware.
- Wrote scripts for flash copy services.

Telecommunications Company, Implementation of pSeries LPAR, 2006

Implemented 2 p550q servers into 2 LPARs with connections to SAN and tape drives.

Local Government, Problem Determination/Problem Source Identification Technical Support Representative, 2006

Customer had p570 that was not booting up correctly. Was able to fix p570 with no data loss within 3 hours.

Local Government, AIX install of Software and hardware, Server Specialist, 2006

Installed pSeries p550 with D20 Expansion Draw. Also installed AIX 5.3 for client.

Insurance Company, AIX Advance Power Virtual (APV) assist, Technical Support Representative, 2006

Assisted customer with VIO Server best practices and fixed their NIM server to perform client installs.

Resource 68

Midrange Infrastructure Architect/Engineer

Energy Company, TSM Implementation Services, Tivoli Storage Manager Specialist, 2006 – 2006

Implemented TSM Server 5.3 in a SAP Environment using ERP.

Education

- Education in Information Technology
  Pennsylvania College of Technology, United States of America, 1997

Certification

- Level 2 IT Specialist Certification Expert Level in Technical Services and Infrastructure & Systems Management specializations Master Certified IT Specialist with the Open Group Certified Specialist -- pSeries AIX System Support AIX System Administration

UNISYS

IBM

Resource 69

Midrange Infrastructure Architect/Engineer

Key Skills and Knowledge

Technical:

- Infrastructure Architect design
- Implementation of I T infrastructures and supporting processes
- Extensive experience on IBM's AIX operating system and Power Servers Linux and Solaris operating systems
- Korne shell programming
- Hardware and software problem determination
- PowerVM Virtualization, including Virtualization I/O (VIO Servers), partition mobility (LPM) and Active Memory Sharing (AMS), on IBM Power Servers
- Network communications for WAN/LAN using SNA and TCP/IP
- SAN network design and implementation on various platforms
- Storage implementation on various products, including IBM's DS8000, DS4000 and NetApp
- IBM Tivoli Storage Management
- IBM PowerHA (aka System Mirror)
- AIX Global Logical Volume Manager, GLVM
- IBM GPFS (General Parallel File System)
- Linux High Availability using Heartbeat
- Apache/Tomcat installation and administration

Professional:

- Technical Project Management Team Leadership
- Negotiations
- Conflict Resolution

Professional Summary

Consulting information technology (IT) expert with over 32 years of diverse experience in all aspects of selling and supporting numerous and diverse IT infrastructure solutions and supporting services to various industry sectors. Uses an extensive background in IT systems infrastructure architecture, from hardware and operating environment through the various applications supporting software, to work effectively in complex, technical environments using strong interpersonal communication and leadership skills. Proven ability to work individually or leading a team through the planning, design and implementation of resilient IT infrastructure solutions that support the applications and processes for various lines of business. Received numerous awards in recognition for leadership, planning, and technical ability.

Consistently recognized for outstanding management and service delivery performance, as well as the ability to resolve complex technical and customer satisfaction issues.

Employment History and Related Experience

IBM, Consulting IT Specialist, Syracuse, New York, United States of America, 1979-To Date

IBM Global Technology Services, Certified Consulting IT Specialist, 1996-To Date

Selling, implementing, managing and supporting over, approximately, $2 Million in I T infrastructure services solutions. Lead in developing the technical and professional skills of the I T Specialists in IBM's Information Technology Services, (I TS) across the United States. Continually recognized, internally and through customers, for creative resolution to complex I T problems and for consultation on support methodologies that increases IT system's availability and performance.

Assignment History

Various Clients, United States of America, 1997-To Date

Lead in the infrastructure architecture and services solution design for several large customers' server consolidations. Developed the infrastructure architectural design and services implementation project plan. Worked to staff the project with technical professionals through interviews and technical questioning. Developed the detailed implementation process plans and led the technical team through the implementation process. Made effect use of various communications and training methods to increase the skill level of the technical staff throughout the project. Worked through various scheduling problems, resource constraints and technical issues during the implementation process. Delivered significant cost savings through the consolidation of over 100 servers into a physically smaller, but more robust, resilient architecture using

virtualization technologies.

- Developed and instructed an AIX-Linux pSeries training class delivered around the country to ISV's (Independent Software Vendors). This class has been a key in helping ISV's technical personnel in transitioning their skills to IBM's pSeries platform.
- Assigned as an IT Architect on an Infrastructure Resiliency Assessment for a large utility company in upstate New York. The customer executive team was very impressed with the detail of information that was collected and presented in the relatively short period of time allocated for the assessment, (4 weeks). The result was implementation of the recommendations resulting in cost savings and improvement in system availability.
- Assigned as a technical and project manager on IBM Tivoli Storage Management contract that involved, AIX-HACMP servers, W2K-MS Clusters, ESS and L TO SAN configuration at a national defense contractor company. The end results and the education they received helped them more easily transition from a Sun environment to an AIX/Linux environment as well as establishing documented procedures for ensuring system currency.
- Provided configuration, installation and upgrade support from for a county-wide 911 server on AIX, running IBM TXSeries, SNA, Encina and DCE used to interface with IBM Mainframe CHAIRS program, as well as links to the 911 center and State DMV database. The support provided and recommendations implemented helped to ensure system availability on a critical link in the county's 911 system.
- Investigated the potential cause of an AIX server outage and made recommendations for future prevention at a worldwide consumer electronics company. The customer management team was extremely satisfied with the study and the deliverable material presented. A result of this study allowed the customer to implement the recommendations to improve system availability.
- Designed, installed, upgraded and consulted on IBM's GPFS (General Parallel File System) at several customers using 2 node and 4 node remote site clusters with a tiebreaker node at a 3rd site in the cluster.
- Improved the procedures and support processes for Disaster Recovery for a major insurance company client and supported them during their Disaster Recovery exercise. The result of these efforts is that the customer has experienced a dramatic reduction in Disaster Recovery test times from 3-4 days to 1-2 days.
- Designed and installed the infrastructure architecture for a high-available Linux 3- Tier Web service. Created the supporting documentation and training of the support staff for daily administration and ongoing support of the service.

IBM

Resource 69

Midrange Infrastructure Architect/Engineer

Certification

Membership in professional organizations

- The Open Group, Master Certified I T Specialist
- IBM I T Specialist Certifications, Board Member
- AIX Certified Advanced Technical Expert

Other job-related activities

- Responsible for the review of I T specialist's certification packages and interviewing candidates being recommended for certification, as well as determining the eligibility of becoming a member of the certification board.
- Responsible for guiding individuals through the certification process as a mentor.
- Responsible for review and presentation of education materials for IT specialists.

This page intentionally left blank.

UNISYS

IBM

Resource 70

Midrange Infrastructure Architect/Engineer

Key Skills and Knowledge

Hardware

- ENTERPRISE SYSTEMS
  - DLPAR
  - LPAR
  - pSeries Servers (p7 770 750, p6, p5+, p5 595 590 570 550, p4 690 630)
  - HMC
  - PowerHA
  - PowerVM
- STORAGE & DUSK SUBSYSTEMS
  - BM DS series
  - IBM ESS 800 RAID-5
  - EMC DMX Series 1000/2000/3000
  - fastT200, fastT800
  - EMC Symmetrix Disk subsystem RAID 0+1
  - Hitachi Disk Array RAID-5
  - NetApp NFS

Storage Services

- FlashCopy
- PPRC
- Metro Mirror
- Global Mirror
- ESS 800 analysis and performance tuning

Software & Tools

- PROGRAMMING ENVIRONMENT
  - Awk
  - UNIX Shell Progg
  - Expect/TCL/TK
  - Oracle SQL
- UNIX and Windows integration with SAM BA
- MKS Toolkit
- Sudo
- COPS Security
- AIX installp software packaging and NIM based end-to-end integration

Professional Summary

Senior Technical Team Leader, Senior Managing Consultant providing consulting, best practice architectural design and implementation services to IBM customers on leading edge IBM technologies in the US.

- Successful as a Technical advisor, Subject Matter Expert & Architect. Highly skilled in leading teams and in technology mentoring on Enterprise class UNIX servers, Enterprise class Storage solutions and in High Availability.
- In-depth experience in enterprise server virtualization, best practice architecture & design, implementation, consolidation, migration & operations. Proven leadership track record across a variety of industries, including telecommunications, defence, finance, government, entertainment and health care sectors.
- Possesses more than twenty years of high quality "operating system software experience" that encompasses systems management, best practice architecture, system design, installation, configuration, system integration, migration, system programming, performance tuning and troubleshooting experiences on a variety of Enterprise class and Highly Available UNIX based machines running databases and ERP software solutions.
- Consistent and proven track record in completing complex mission critical engagements while ensuring a high degree of client satisfaction.
- Pursues new challenges to stretch abilities, to expand knowledge. Recognized for service delivery performance as well as for unique and creative perspectives on problem resolution.

Employment History and Related Experience

IBM, Consulting IT Specialist, Irvine, California, United States of America, 2000 - To date

Technical team lead, Managing Consultant providing consulting and implementation services to customers on leading edge IBM technologies. Specialized in High Availability, Power7/Power6/Power5 Virtualization & Micropartitioning and Storage.

- IBM Power7, Power6, Power5+, Power5 and Power4 hardware architecture and in applying technologies.
- Power7, Power6, Power5+/5 Virtualization, LPAR, DLPAR
- AIX, NIM, SAN storage, UNIX, Korn shell scripting and automation, High availability
- SAN storage products and services - Flashcopy, SAN Volume Controller, TSM

UNISYS

IBM

Resource 70

Midrange Infrastructure Architect/Engineer

Operating Systems

- UNIX - AIX 7.1
- AIX 6.1
- AIX 5.3 TL10 and below
- 4.3.3 and below
- SLES Linux 9.2
- Red Hat Linux 6.2
- Dynix/ptx, Sun

Operating Systems

- PowerHA 6.1 and below
- HACMP Rolling upgrades
- NIM on AIX
- Alternate Disk Installs on AIX
- AIX operating system Upgrades
- UNIX Sendmail
- AIX Packaging
- AIX Sendmail
- NFS
- TCP/IP
- DNS
- DHCP
- Samba

Database & ERP Applications

- Oracle database layout and administration techniques
- Automation via Korn shell scripting
- PowerHA and PowerVM configuration around SAP
- WebSphere 6.0.2 and fixpack installation
- WebSphere Portal Server installation
- D B2 and fixpak installations
- BaaN and Oracle Financials ERP Systems Management and configuration techniques
- MQ Series installation

Achievements:

- Received award for providing pre-sales solution design on various IBM projects - 2011
- Consistently "a top performer" 2000-2011
- Received 3 "Thanks Award" for exceptional customer satisfaction on projects - 2009
- Delivery "Wall of Excellence", Customer Appreciation for technical services - 2007
- Received 3 "Thanks Award" for exceptional customer satisfaction on projects – 2007
- IBM Certified - IT Specialist Profession - Performance Management - 2003, Recertified in 2006
- Merit promotion in 2001
- Received an award for technical contributions in 2000

Sequent Computer Systems, Professional Services Consultant, Irvine, California, USA, 1996 - 2000

Technical team leader and implementation specialist for mission critical enterprise class UNIX projects at various Sequent customer locations in the United States.

- Installation, Configuration, Administration, Migration and Tuning of Enterprise class mission critical UNIX systems
- Technical support, Troubleshooting, Systems Management and operating system upgrades of complex UNIX installations
- Storage implementation and administration - SCSI and Fibre
- Technical Design of a UNIX system
- Documentation preparation & delivery — Technical and Configuration information
- Skills transfer to customer staff

Achievements:

- Received Western Region Q3 Consultant of the Quarter award in 1998
- One of twenty-five nominated from the American Operations for Employee Excellence Program in 1997

Business Systems Group, Lead Software Architect, Bombay, India, 1996 - 1996

Lead architect for designing and developing software solutions for the Computer Education and for the Telecommunications industry. Innovated new tools and solutions that were used and highly appreciated in the market.

- Designed and developed "On-line Grading Module" a suite of tools for conducting online tests in a multi-user UNIX environment. The software solution utilized UNIX ksh and "C Language".

- Innovated custom tools and procedures for the Telecommunications industry using "Data Structures in C Language"

Microwave Communications Limited, Senior Systems Executive, Bombay , India, 1994 - 1996

Technical team leader, Senior Systems Analyst for all technical requirements for the software infrastructure. Achieved systematic implementation of Paging software in Mumbai and assisted other Microwave locations in India with software setup and with best practices in Paging, Billing Software and UNIX system administration.

- Innovated custom tools and procedures utilizing "Data Structures in C Language".
- Designed and developed high performance custom utilities to achieve automation and to extract reporting information from the multi-vendor Paging and Billing software database. Implemented custom tool at various locations in India.

Kale Consultants, Programmer Analyst, Bombay, India. 1994-1994

Technical analyst for software implementation project.

Aptech Computer Education, Software Consultant, Bombay, India, 1993 - 1993

As an industry expert, provided advanced software training to the APTECH faculty and staff on UNIX and C Language.

TATA Engineering & Locomotive Company, Systems Trainee, Bombay , India, 1990 - 1994

Responsible for providing Systems Operations services, Systems Management, System Software and tools development in a multiuser UNIX environment. Provided unique perspectives on problem resolution and automation of tasks on a variety of enterprise class UNIX platforms. Performed and achieved over and above the stipulated job requirements.

- System administration of Enterprise class UNIX systems.
- Design and develop System administration and automation tools - UNIX ksh.
- Job scheduling and automation via UNIX tools - ksh.
- Backup and Recovery of user data.

National Institute of Information Technology, Business Development Executive, Jamshedpur, India, 1989 - 1990

Business development, including business plan & sales strategy development. Generated new business leads for NI IT software courses. Created and implemented an effective advertising strategy. Offered the job by Centre Management and selected for this position while doing Systems

Management course at NI IT - Jamshedpur.

Large financial institution, Level2 team skills assessment and support, Consulting IT Specialist, 2012 - To date

As a lead architect, worked with the customer L2 team handling daily operations and support, analyzed the support activities and provided recommendations for service improvement. The service focused recommendations encompassed virtualization best practices, AIX best practices, AIX upgrades, Firmware upgrades and PowerHA components in a Power7 environment. These service focused recommendations were presented to the customer management for implementation across the server enterprise. Created a LA B environment for IBM Systems Director and assisted with the planning and implementation activities for IBM Systems Director 6.3. The LAB environment for IBM Systems Director showcased the use cases that were of interest to the customer.

Retailer of home improvement and construction products and Services, pSeries Healthcheck and AIX Performance tuning, Lead design architect and implementation specialist, 2012 - 2012

Played a lead role for an AIX performance tuning requirement. As a pSeries and a storage specialist, conducted a comprehensive Health check of the p7 environment, AIX/pSeries and EMC storage disks at a leading home improvement retailer based out of Austin.

- Assisted the operations team with AIX performance tuning and with data gathering and analysis during the assessment phase.
- Assisted the technical team in adopting more efficient business processes on AIX and in creating a run-book for the operations team.
- The final best practices recommendations helped the customer tune the p7 LPAR & AIX environments.

Large financial institution, p770 and NetApp storage implementation, Lead design architect and implementation specialist, 2011 - 2012

Lead architect for a p770 implementation requirement around NetApp storage. As a sole perform resource from IBM, assisted the customer on Virtual IO Server network and storage design, on p770 implementation and on the best practices. Assisted the customer staff in hands on implementation steps. Highly successful implementation from the customer and from the IBM standpoint.

National leader in providing health care services & medical research, PowerHA implementation and testing around EPIC application, Consulting IT Specialist, 2011 - 2011

Lead architect for a PowerHA implementation and testing requirement on IBM p7 hardware. As a sole perform resource from IBM, assisted the customer in

Resource 70

Midrange Infrastructure Architect/Engineer

PowerHA implementation and in conducting PowerHA testing. Highly successful implementation from the customer and from the IBM standpoint.

World's largest publisher and distributor of children's books, HealthCheck and AIX Performance tuning, 2011 - 2011

Played a lead role for an AIX performance tuning requirement. As a pSeries and a storage specialist, conducted a comprehensive Health check of the p7/p5 environment, AIX and NetApp storage disks at a leading distributer of children's book based out of New York. Satisfied with the services provided in 2010, the customer requested for my services by name. The final best practices recommendations helped the customer tune the p7/p5 LPAR & AIX environments and meet the load requirements during the peak business season.

Leading provider of carrier-neutral data centers and internet exchange, IBM p750 implementation and migration, Lead design architect and implementation specialist, 2011 - 2011

Lead architect for a Virtual IO Server network and storage design on 5 p750 frames for an Oracle migration requirement. The design included all virtualized components and utilized PowerHA, PowerVM and LPM technologies. The design architecture followed industry level best practices and created a solid foundation for the LPAR build out and subsequent migration/implementation. As a sole perform resource from IBM, assisted the customer during the design phase, implementation phase and during the migration phase. Highly successful implementation from the customer and from the IBM standpoint.

Leading wholesale provider of technology products & supply chain svcs, Power7 p770 Migration – SAP, Lead design architect and implementation specialist, 2010 - 2011

Architected Virtual I0 Server network and storage designs on 3 p770 frames for a SAP migration requirement. The design included all virtualized components and utilized PowerHA, PowerVM and LPM technologies. The design architecture followed industry level best practices and created a solid foundation for the LPAR build out and subsequent migration/ implementation.

World's largest publisher and distributor of children's books, AIX Performance Tuning, 2010 - 2010

Played a lead role for an AIX performance tuning requirement. As a pSeries and a storage specialist, conducted a comprehensive Health check of the p5 environment, AIX and EMC storage disks at a leading distributer of children's book based out of New York. The final best practices recommendations helped the customer tune the p5 LPAR & AIX environments and meet the load requirements during the peak season.

Resource 70

Midrange Infrastructure Architect/Engineer

Multiple Bidding & Proposal assignments, Multiple assignments, 2010 - 2010

pSeries expert, provided assistance during the DC migration activity at a leading insurance company and at a leading department store. As an experienced practitioner I have been working with the sales team in providing the work breakdown structure for resources required for supporting the pSeries environment at a leading global financial services firm with investment, research, banking, finance, insurance, and other businesses.

- As a Technical Solutions Owner, I have been assisting the IBM sales team in creating RFP proposal and in scoping project timelines for a Power7 implementation requirement at a leading wholesale provider of technology products and supply chain services.

World leader in convenient snacks, foods and beverages, Virtual I0 Server Architecture Analysis, 2010 - 2010

As an expert in virtualization and PowerVM, conducted an architecture analysis of the Virtual I0 server configuration at a leading convenient snacks, foods and beverages company.

Fortune 500 electric and natural gas utility serving company, Migration and Best practice architecture on PowerHA, PowerVM and AIX, Consulting IT Specialist, 2010 - 2010

As a lead implementation Specialist provided best practice architecture on a p6 hardware for a PowerHA, PowerVM environment. My recommendations for migrating to a Power6 based environment assisted the customer in planning out the migration steps. Towards the end of the engagement, I provided the customer with various test cases for the system and for the server environment testing.

Leading defence company and an advanced technology company, Power6 PowerVM, PowerHA & BladeCenter implementation, Consulting IT Specialist, 2009 - 2010

As a sole member of the implementation team and as an implementation architect, provided BladeCenter based PowerVM, PowerHA and AIX implementation services centered around the NetApp filer storage. Successfully implemented the PowerHA clusters in a complex and mission critical customer environment.

Leading security software firm, PowerVM Best Practices on Power6, 2009 - 2009

Pprovided PowerVM best practices to a leading security software company based in the Bay area. Provided industry level best practices for virtualization, methodology documentation as well as knowledge transfer training to the customer staff.

Resource 70

Midrange Infrastructure Architect/Engineer

IBM internal B&P requirements, Multiple Bidding & Proposal assignments, 2009 - 2009

As a Technical Solutions Owner, assisting the IBM sales team in creating customer proposals for a Power6 and Bladecenter based implementation requirement at a leading defense company and for a Power6 based migration requirement at a leading aerospace company.

- As an experienced practitioner I have been working with the sales team on a critical performance tuning engagement on Power5 p595 hardware at a leading cellphone service providing company.

Utilities Company, Augmentation Staff, Lead Consulting IT Specialist - p5, AIX 5.3, HMC, Virtualization, HACMP & Storage, 2007 - 2009

As a Lead Technical resource provided best practice solutions on AIX, p5/p5+ implementation, AIX Performance Tuning, AIX HealthChecks, Server consolidation, LPAR migration, Virtualization, HACMP and on Enterprise Storage.

Semiconductor manufacturer, p5 Virtualization Implementation, Lead implementation specialist - p5 Virtualization, 2007 - 2007

As a p5 Virtualization expert, implemented a dual VIO server environment and provided Virtualization services to a leading semiconductor company based in the Bay area. Provided industry level best practices for virtualization, methodology documentation as well as knowledge transfer training to the customer staff.

Music Company, AIX LPAR, P5 and Storage Performance Tuning, Lead Consulting IT Specialist & SME - AIX LPAR, p5 and Storage, 2007 - 2007

As a pSeries and storage specialist, conducted a comprehensive Health check for the p5 environment, AIX and ESS 800 storage unit at a music company based out of Indiana. The final best practices recommendations report helped the customer tune the ESS 800 storage unit as well as the p5 LPAR & AIX environments.

Health Care Organization, Lead p5 Implementation, p5 Implementation Specialist, 2005 - 2006

As a pSeries implementation specialist, installed around 80 p5 frames, setup LPARS, led configuration of p5 hardware, installed and configured HACMP, installed and configured NIM server, installed WebSphere application server, WebSphere Portal Server, led multiple AIX upgrades, implemented Virtualization and above all provided innovative solutions during various phases of the project.

Resource 70

Midrange Infrastructure Architect/Engineer

Leading cosmetic company, p5 LPAR Implementation, Lead p5 Implementation Specialist, 2005 - 2005

As a pSeries expert, installed p590 frames, led the setup of LPARs and assisted with the EMC Storage connectivity at a leading cosmetic company based out of New Jersey.

Leading Retail Outlet, pSeries LPAR Implementation, Lead pSeries Implementation Specialist, 2004 - 2004

As a pSeries expert, installed LPARs, configured ESS storage and installed WebSphere at a leading retail outlet based out of New Jersey implementing Demand forecasting i2 tool.

Leading Credit Card Company, Korn shell scripting, Korn shell scripting expert, 2004 - 2004

As a storage and Korn shell scripting expert, analyzed customer requirements, designed and developed Korn Shell scripts for carving out Terabytes of DS4000 SAN storage at a leading credit card company based in the Bay area. The project required building Korn shell scripts to facilitate the AIX LVM buildout of a large D B2 database running on multiple AIX logical partitions. The final product increased the client productivity by over 200%.

Health Care Association, Nashville, Tennessee, United States of America, AIX sendmail configuration and tuning, Lead Sendmail Configuration and Tuning Specialist, 2004 - 2004

As a lead sendmail expert, provided best practices on sendmail, provided effective solution that successfully handled error recovery while working with HCA's Lawson ERP application and the Exchange server. The final solution addressed the customer needs completely and the customer was very satisfied.

Entertainment Organization, Korn shell scripting and pSeries Implementations, Senior Consulting IT Specialist - pSeries and Korn shell programming, 2003 - 2004

As a pSeries implementation and scripting expert assisted the customer with Korn shell scripting based automation and with pSeries implementation.

Education, Sendmail Consulting, Lead Technical Resource - AIX and UNIX Sendmail, 2001 - 2004

As a sendmail and systems management expert, provided technical leadership to the IBM technical team on an AIX operating system upgrade and AIX sendmail 8.9 configuration/performance tuning engagements on a highly utilized AIX/RS6000 server. Led the technical team towards successful completion of operating system upgrades on two Production servers and also on a sendmail ruleset configuration assignment on the e-mail server. While on the engagement I also provided performance analysis and best practice

recommendations to the customer IT staff and management. During the latter portion of the project I worked on the project as a sole perform resource.

Disk Drive Manufacturer, NUMA-Q Migration, Lead Consulting IT Specialist - NUMA-Q and AIX, 2001 - 2001

As Systems Management expert, provided RS/6000 (H80 and S85 with ESS Shark) and NU MA-Q 2000 systems management and administration services to a leading disk drive manufacturing company migrating Oracle Financials from an IBM NUMA-Q 2000 to a RS/6000 platform. I was instrumental in the proof-of-concept stage when the customer was proofing the environment in a 2-tier Citrix, NUMA-Q and 3-tier Citrix, NUMA-Q, RS/6000 architectures. I provided quality insights to the IBM Project Manager and to the customer on various migration planning and configuration issues.

Large Manufacturing Company, BaaN Implementation and DC Relocation, Lead Consulting IT Specialist - Dynix/ptx, Storage & Korn shell automation, 2000 - 2002

Subject Matter Expert for all technical tasks on the IBM NUMA-Q server. As a technical lead, I provided System installation, capacity planning, performance tuning and systems management support services during various phases of the BaaN V ERP implementation project.

This engagement was in a demanding fast paced environment and I won the customer's confidence with my skills. I automated routine jobs using UNIX shell scripts, expect, tcl/tk scripting tools, MKS Toolkit on NT which improved the team productivity by at least 50%. Owing to the extensive level of automation, the customer has been successful in handling UNIX system administration with minimum resources. In Oct 2001 I successfully assisted this customer in planning and moving their Data Center from CA to UT. While on the project I recommended and set up disaster recovery procedures and policies and also provided quality documentation for the work that was performed. In this role I enhanced my Oracle database technical knowledge and people skills.

Major online retailer, Disaster recovery & operating system Upgrade, Lead Professional Services Consultant - NUMA-Q Implementation & support, 1999 - 1999

Provided technical leadership on multiple Production class operating system upgrade requirements. As a Dynix/ptx expert I collaborated with other members of the team on DR assessment assignment. In 2000 & 2001 I was called again by the customer to perform operating system upgrades on the Production and Development systems.

IBM

Resource 70

Midrange Infrastructure Architect/Engineer

Direct Selling Promotional Company, Oracle Financials ERP Implementation, Lead Professional Services Consultant - NUMA-Q Implementation & support, 1999 - 1999

Technical Lead and the Subject Matter Expert for all technical tasks on the IBM NUMA-Q server. As a UNIX and NUMA-Q SME I provided System installation, performance tuning and systems management support of the IBM NUMA-Q systems during various phases of the ERP implementation project.

Refiner and marketer of petroleum products, Marketing Data center move and Insourcing, Project Lead Professional Services Consultant - NUMA-Q, Storage, Backup, 1998 - 1998

Technical Lead and the Subject Matter Expert for all technical tasks on the IBM NUMA-Q and on the Sequent Symmetry 5000 servers. While on the engagement I provided System installation, server consolidation and migration, capacity planning, performance tuning and systems management support services on the IBM NUMA-Q/Dynix systems during various phases of the Oracle Financials 11 implementation project.

Data storage pioneer and a longtime leader in the hard drive Industry, Oracle Financials ERP implementation, Professional Services Consultant - ptx/CLUSTER, NUMA-Q, Storage, Backup, 1996 - 1998

Provided systems management services on a Dynix/ptx based Sequent platform. Guided the customer during various phases of the project while providing quality technical solution and support.

Education

Post Graduate Diploma in Software Technology (PGDST) in Software Technology

NCST - Bombay, India

Bachelor of Science in Mathematics

Nagpur University, India

Diploma in Systems Management in Software Programming

National Institute of Information Technology - NIIT, India

Certification

Over 900 Hours of professional and technical education with the following recent trainings:

- IBM SDMC
- Live Partition Mobility (LPM)
- AIX 6 Workload Partitions (WPAR)
- AIX 5L Performance Mgmt II: Analysis & Tuning Complex Performance Issues

Resource 70

Midrange Infrastructure Architect/Engineer

- Exploring HMC Version 7 for POWER5 and POWER6 Servers
- Virtual I/O Server Performance Management
- DS8000/DS6000 Implementation workshop for Open Systems
- Partition Load Manager (PLM) Implementation
- IBM SAN Volume Controller 3.1 - Planning and Implementation Workshop
- IBM Tivoli Storage Manager 5.3 Implementation for AIX
- DS6000/DS8000 Copy Function Implementation Services - FlashCopy, PPRC, Metro & Global Mirror
    - p5 Micro partitioning and Virtualization

This page intentionally left blank.

UNISYS

IBM

Resource 71

Midrange Infrastructure Architect/Engineer

Key Skills and Knowledge

- 22 years AIX experience
- 7 years Advanced POWER Virtualization, including VIO, Live Partition Mobility, and NPIV SAN virtualization
- 12 years high availability experience (HA/CMP & PowerHA)
- 17 years backup & recovery experience, including disaster recovery

Professional Summary

Career with IBM has principally been in systems engineering and architecture for mid-range solutions in State Government. Strengths include analyzing operations to develop solutions to fit unique business needs, developing and customizing implementation plans to meet client needs, coordinating system implementation for complex AIX installations, and providing continuing support for clients of IBM. Recognized leader in Tivoli Storage Management (TSM) and in Disaster Recovery testing. Extensive experience with High Availability solutions combined with AIX. Proven track record in successful AIX installations and is sought after by both her peers and her clients for her outstanding knowledge of the AIX environment.

Employment History and Related Experience

Commonwealth of Pennsylvania - Liquor Control Board, Team Lead for Architecture, Infrastructure, Implementation, and Support (PowerVM/AIX), 2009 – To Date

Responsible for the architecture, implementation, management, and documentation of the POWER (AIX) ERP servers.

- Led design and implementation of Advanced POWER Virtualization, including NPIV SAN virtualization, Live Partition Mobility, and advanced hardware virtualization.
- Led the standardized build processes for AIX LPAR's.
- Technical lead in creating AIX gold images for all AIX LPAR's.
- Led the successful completion of an AIX standardization and best practices project, resulting in increased efficiencies, security, and availability.

Corporation Fortune 400 International Engineering Corporation, Consulting Assignment for PowerVM/AIX & PowerHA in SAP Environment, 2012–Present

Brought in to help stabilize a troubled account. Implemented AIX and PowerHA standardization and best practices, resulting in increased efficiencies, security, and availability. There have been no subsequent system outages.

- Led the design and implemented a project to increase user security.
- Consulted account team on architecture and design for a hardware refresh for POWER (AIX) servers. Design enhanced performance, efficiencies, security, and availability using advanced virtualization.

Pennsylvania Department of Labor and Industry – UCMS Project, 2010–2011

- Developed technical requirements and was responsible for the

architecture, design, and sizing for a hardware refresh for the POWER (AIX) servers, including PowerHA.

- Managed the implementation, including developing detailed AIX and PowerHA build requirements. All project deadlines were completed on time and within budget.

Commonwealth of Pennsylvania - Integrated Enterprise System ERP Project, Team Lead for Architecture, Infrastructure, Implementation, and Support (PowerVM/AIX, HACMP, and TSM), 2001–2010

Responsible for the architecture, implementation, management, and documentation of the Power (AIX) SAP server landscapes and Tivoli Storage Manager (TSM) backup environment for both the initial implementation and subsequent hardware refresh.

- Led the standardized build processes for AIX servers while also providing support for AIX, PowerHA clusters, and Tivoli Storage Manager (TSM).
- Technical lead in creating AIX gold images for all AIX LPAR's.
- Developed customized processes, standards, and procedures for AIX server monitoring, change management, and problem management based on best practices.
- Responsible for the architecture and implementation of the TSM backup server supporting all AIX and Tivoli environments. Worked with IBM development and the SAP/Basis team to architect, develop, and implement customized backup solutions and worked with these groups to test recovery of SAP/Oracle databases.
- Responsible for creating, testing, and documenting disaster recovery procedures for the TSM backup server and all AIX servers. Worked with Windows administrators to implement backup/recovery solutions and perform testing for Intel servers. This resulted in 8 successful disaster recovery tests. Successfully recovered the TSM backup server and 40 AIX and Intel servers, restored over 10TB of data and met all primary and secondary recovery objectives.

Pennsylvania Department of Labor and Industry - Bureau of Workers' Compensation, Team Lead for Architecture, Infrastructure, Implementation, and Support (AIX and TSM),1996 2004
Initial build of the infrastructure and rollout.

- Led the initial architecture, design, implementation, and management of a complex client/server environment, involving over 50 AIX Servers, NT servers, and over 600 PC desktops, involving 24 remote locations.
- Created a sandbox lab and tested all components of this distributed application in a lab environment, including the development of a gold image process which allowed for rollout of servers to Field Offices to be executed remotely. This process saved the project money as remote travel could be avoided.

- Implemented the Tivoli Storage Manager (TSM) backup server, supporting over 50 clients with 1.5TB of data.

Migration of 50 AIX servers at Headquarters and 24 Field Offices.

- Led the efforts to develop migration and implementation plans for 50 servers.
- Successfully spearheaded the migration of these 50 installed servers upgrading AIX, CIMS application, Lotus Notes, Sybase, Visual Image, TSM, Netview, and Software Distribution software products. During the migration effort, was also responsible for documenting, implementing and successfully testing TSM disaster recovery.

Relocation and implementation of the BWC equipment to DLI Server Farm.

- Led and participated in a follow on project to plan for and relocate AIX servers to the DLI Server Farm. This project included migration and consolidation to new enterprise platforms within Labor and Industry, which helped Labor and Industry reduce overall operating costs.

Pennsylvania Department of Labor and Industry - Office of Information Technology, Team Lead for Architecture, Infrastructure, Implementation, and Support for Initial Build (AIX, HACMP, and TSM), 2003–2004

- Provided AIX infrastructure and technical consulting for the OIT Server Farm infrastructure to support mission-critical distributed applications including the Department of Labor & Industry's Bureau of Workers' Compensation imaging system. This allowed the department to provide uninterrupted service to the state wide locations across Pennsylvania while adding applications to improve service to unemployed workers.
- Provided OIT assistance in the creation of AIX gold images for all BWC AIX RS/6000 servers and the development of a standardized build process for other AIX environments.

PHEAA, Team Lead for Architecture, Infrastructure, Implementation, and Support (AIX, HACMP, and TSM), 1998-2001

- Architected, implemented, and managed a 20 AIX SP Node system involving a Loan Guarantee system supporting four states, Lotus Notes for 5,000 users and ERP for human resources.
- Was instrumental in the installation of the Tivoli Storage Manager (TSM) server at PHEAA.
- Created and implemented a disaster recovery test plan for PHEAA. Led the successful design, planning, documentation, and testing of PHEAA's first complete open systems disaster recovery test which was a complete success.

IBM

Resource 71

Midrange Infrastructure Architect/Engineer

Pennsylvania Department of Labor and Industry - Office of Vocational Rehabilitation (OVR), Team Lead for Architecture, Infrastructure, Implementation, and Support (AIX and ADSM), 1997-2000

- Architected, designed, and implemented a client/server solution, involving over 20 AIX Servers in 15 remote locations. Rollout to all locations was accomplished via remote access allowing flexibility and saving money on travel and expenses.
- Responsible for the overall backup strategy and testing of disaster recovery utilizing Tivoli Storage Manager.

Education

- Bachelor of Arts in Economics
  Ohio Wesleyan University 1977
- Saint Claire's Hall
  Oxford, England 1977
- University de Grenoble
- France 1973

UNISYS

IBM

Resource 72

Midrange Infrastruture Architect/Engineerg

Key Skills and Knowledge

- Systems management solution design
- Tivoli Monitoring Implementation
- Systems Automation and Design
- Network Management Implementation

Professional Summary

Designed and implemented servers, enterprise, and network management systems for over 33 years. Experience includes the design, project management, implementation and troubleshooting of systems and networking management software solutions from IBM, Tivoli, and Netcool. Strong technical knowledge in Tivoli distributed systems management software using it to monitor operating systems, databases, networks and applications. Experience with AIX, zLinux, and Windows operating systems, and UNIX shell and Perl scripting.

Supported customer environments with the design, project management, implementation and troubleshooting of systems, and networking management software solutions. Supported the software sales organization with technical assistance during sales and installation activities. Provided systems programming support to IBM in the areas of VM Systems programming and IMS Database Administration on VM and MVS mainframe systems.

Employment History and Related Experience

IBM Corporation, Commonwealth of Pennsylvania, Power House Project, 2007-To Date

Designed a Tivoli systems management solution to the support the customer environment which included Custom applications, Oracle databases, MQSeries integration, WebSphere Application Server, IBM Apache Web servers, zLinux servers on a TCP/IP network.

- Established linkage and monitoring support for z/operating system Omegamon agents supporting MQSeries, DB2, IMS, Storage and z/operating system.
- Implemented the Tivoli software to support the environment and configured based upon customer requirements. The Netcool Omnibus/Impact is the focal point of events as it is used by the Operations staff to manage the servers and network. This effort provided for early detection of problems, proactive management of the servers and network, and increased systems availability. Currently providing ongoing consultative and production support.

IBM Corporation, Commonwealth of Pennsylvania, Integrated Enterprise System ERP Project, 2001-2010

Designed a Tivoli systems management solution to the support the customer environment which included SAP applications, Oracle databases, MQSeries integration, AIX and Windows servers on a TCP/IP net-work.

- Implemented the Tivoli software to support the environment and configured based upon customer requirements. The Tivoli Enterprise Console was the focal point of events as it was used by the Operations staff to manage the servers and network. This effort provided for early detection of problems, proactive management of the servers and network, and increased systems

availability.

- Currently providing ongoing consultative and production support.

IBM Corporation, State of Delaware, Network Management Implementation, 2002-2002

Developed an overall integrated network management strategy.

- The SNMP-based network management system integrated with event correlation and reporting tools provided the client with a solution that performs root-cause analysis of the network failure, performs automated actions to resolve the problem and compiles management reports. The client was able to anticipate and prevent network outages as a result of the implementation, and to react more quickly to problems. This increased network availability and end user satisfaction.

IBM Corporation, Commonwealth of Pennsylvania, ESM Design and Implementation, 2001-2002

Successfully lead the Tivoli implementation based upon Event Management Design Workshops.

- The Tivoli solution gathered events from 30+ event sources including network devices, storage management, SAN devices, and AIX and Windows operating systems and forwarded them to the Tivoli Enterprise Console where selected events were then sent to the Remedy Problem Management system. Installed and customized Tivoli Enterprise Console to Remedy Integration module.

IBM Corporation, Pitney Bowes, Inc., System Management Implementation, 2000-2001

Implemented, customized, and delivered skills transfer on several Tivoli Event Management solutions.

- Customized the NetView network management system to monitor the network and send events to the Tivoli Enterprise Console for customer support notification.
- Implemented Tivoli Remote Control application then developed and delivered classes to Help Desk personnel.
- Installed and customized the ARS Plus module for Tivoli which enables Tivoli to Remedy problem ticket generation. Tivoli Enterprise Console was the focal point of events as it was used by the Operations staff to manage the servers and network. This effort provided for early detection of problems, proactive management of the servers and network, and increased systems availability.

Education

Bachelor of Science in Computer Science, Pennsylvania State University

UNISYS

Performance Specialist

This page intentionally left blank.

UNISYS

IBM

Resource 73

Performance Specialist

Key Skills and Knowledge

- Performance test management
- Performance test planning & design
- Performance test process

Professional Summary

Thirty-four years experience in information technology including both corporate IT and professional services consulting. A Certified Managing Consultant in the IBM Performance Management & Testing Practice; having served the practice as both a Principal and Practitioner. Significant experience and expertise in leading and performing Performance, Load, & Stress Testing, as well as Full Lifecycle Test Consulting engagements. As one of the original members of the testing practice in the Northeast Region, played a major role in the development of much of the intellectual capital currently integrated into IBM's Performance Test Consulting Methodology.

Employment History and Related Experience

IBM Corporation, Certified Managing Consultant, Tampa, Florida, 1998-To Date

Served as Engagement Manager and Test Consultant on numerous performance, load & stress testing engagements.

- Exposed customers to a fundamental understanding of performance testing and the process employed by IBM.
- Led customers through the requirements gathering process in the areas of goals & objectives, environment, tools, workload, and reporting.
- Developed detailed test plans, facilitated the creation of test environments, architected simulated workloads, and led the execution of the test followed by the analysis and reporting of results.

Computer Horizons Corp., Engagement Manager, Mountain Lakes, New Jersey, 1994-1998

Served as a Client Engagement Manager and IT Management Consultant developing and delivering technology solutions, and providing IT Management expertise across a wide range of industries and technology platforms.

- Worked extensively developing new technology environments for businesses whose focus was shifting from "back-office" processing to front-line customer service.
- Specialized in the areas of document and content management, imaging, workflow, business process reengineering, and electronic data interchange.
- Led a consulting practice specializing in Y2K compliance for enterprise applications.

John Hancock Financial Services, Director, Boston, Massachusetts, 1978-1994

Fifteen years in corporate information technology. Progressed through

Resource 73

Performance Specialist

increasing levels of responsibility to Director of Information Technology; spanning all aspects of IT from traditional mainframe development, through the evolution to distribute computing, and the introduction of electronic commerce.

Certification

Certified IBM Information & Technology Management Consultant.

UNISYS

IBM

Resource 74

Performance Specialst

Key Skills and Knowledge

- Network infrastructure
- Midrange systems
- operating system/400, Windows NT/2000, AIX, Linux, UNIX
- Ethernet, Token Ring, ATM
- SecureWays Firewall, CheckPoint Firewall, PIX Firewall
- Tivoli Management, Tivoli Netview
- Voice over ATM,VoIP
- OPNET IT/Guru, ACE
- NetIQ AppManager
- RadCom PrisimLite, Acterna Domino, Fluke Optiview, Sniffer Pro, Solarwinds
- Microsoft Excel, Microsoft Access, Microsoft SQL Server, IBM DB2, Crystal Reports, Visio

Professional Summary

Senior-level IT Specialist and Consultant with 30 years diverse experience in systems management, network management, and problem management. Proven expertise with systems and network problem isolation and resolution as well as performance analysis, design, and implementation. Specializing in application performance engineering, providing critical information required for data center relocations, server consolidations and virtualization. Consulting skills in troubleshooting techniques and tools, systems and network management processes, and team leadership. Expert in developing and implementing action and resolution plans that address and resolve problems in systems and network availability, reliability, and performance.

Employment History and Related Experience

IBM, Senior IT Consultant, Memphis, Tennessee, 1978-To Date

Application performance engineering in support of data center relocations/consolidations and application performance management. Capture, review, and analysis of network application performance. Network management consulting.

Assignment History

Larger Consulting Firm, Sr. IT Consultant, 2009-2010

Conducted workshops on major applications/services involved in data center relocation.

- Determined application/server dependencies.
- Worked with Data Center Relocation team in developing move groups.
- Performed latency impact analysis.
- Provided recommendations to insure a successful move.

Large Manufacturing Company, Sr. IT Consultant, 2009-2009

Responsible for Problem Determination and Problem Source Identification on applications running slow as result of data center move to Service Provider. Collected data including packet captures on application flows, reviewed with client personnel, and developed approach for improving performance.

- Conducted workshops to evaluate future application moves.
- Performed application performance engineering to insure successful transition.

Medical Supply Company, Sr. IT Consultant, 2009 -2009

Responsible for Problem Determination and Problem Source Identification on poor performing applications after relocating.

- Reviewed application flows and requirements with client in workshops

Resource 74

Performance Specialst

- Collected data on application flows.
- Analyzed data.

Leading Service Provider, 2008 -2009

Responsible for the discovery and review of impact on applications involved with data center relocation.

Large Global Security Company, Team lead, Data collection and analysis, 2006 - 2008

Developed a network assessment for support of Enterprise Transformation project to include consolidation of 7 data centers. Responsibilities included application performance impact study, application discovery, server impact analysis, and application testing.

Automotive Company, 2005 -2006

Developed a network management assessment and plan. Provided consulting services to review and develop strategic direction for a network management system for BMW North American Dealership Support Network.

Large Hotel Chain, 2004-2005

Developed model of new application being deployed to Marriott properties to determine network requirements.

Large Public School System, 1997-2003

Responsible to develop, build, and run the Network Operations System for 200+ site ATM network. Includes deployment of Tivoli Netview and DM, Solarwinds Orion and various network management tools.

Various, 1996-1997

Delivered nationwide software support including problem determination and problem resolution for mid-range systems.

Various, 1987-1996

Provided nationwide on-site support to field personnel for midrange systems. Delivered nationwide software problem determination/problem resolution for mid-range systems. Acted as "Top Gun" for mid-range systems hardware support.

Various, 1978-1987

Responsible for maintaining hardware for various mid-range system accounts.

Education

Associates of Engineering in Biomedical Electronics, Tennessee State Technical Institute, US

UNISYS

Resource 75

Performance Specialist

Key Skills and Knowledge

- Domain Expertise & Solutions
- System Monitoring
- Hardware
- Operating Systems
- Software/System Architecture
- Technical Documentation
- DNS, DHCP, and WINS infrastructure maintenance
- DNS scavenging WINS consolation
- DHCP standardization
- Researching, testing, and deploying SCOM updates
- Researched and designed SCOM Disaster Recovery environment
- Day-to-day alert monitoring;
- Implement custom monitoring of performance
- Develop and deploy availability metrics based on customer requirements.

Professional Summary

Over twenty four years of system management experience. Project lead for numerous activities with Six Sigma and Microsoft Project management experience; Subject Matter Expert for Microsoft Active Directory, DNS, DHCP, WINS, and Clustering technologies. Substantial experience installing Microsoft Windows NT, Server 2000, Server 2003, and Server 2008 Management tools. A 'go to' engineer for:

- Network storage systems – NAS & SAN installation and operation
- Experience with VMware and Citrix technologies
- Server Monitoring - Microsoft SCOM, Dell IT Assistant & HP Insight Manager
- HP & Dell and servers including HP C-Class blade environment
- Chief architect of Server Provisioning process
- Server Builds, Maintenance, & Upgrades
- Local and Wide Area Network Design and Implementation

Professional Experience

Unisys, SCOM Consultant, Harrisburg, PA 2012 to Present

Delivers substantial support to the Commonwealth server environment for multiple SCOM 2007 R2 Environments; currently supports 2700+ Windows (and Linux) servers, and 500+ Web sites. Provides:

- Researching, testing, and deploying SCOM updates.
- Researched and designed SCOM Disaster Recovery environment.
- Day-to-day alert monitoring; implement custom monitoring of performance and availability metrics based on customer requirements.
- Performance and Availability Monitoring and Reporting
- Support tickets management and troubleshooting Windows, IIS, SQL and application issues.

DLA Piper US LLP, Senior Systems Engineer, Baltimore, MD, 2007 to 2012

Project lead for SCOM implementation and upgrade to AD 2008 environment. Primary SCOM engineer for daily monitoring of 600+ production servers, alert tuning & overrides, creation of new monitors, and alert subscriptions. AD activities include initial contact for all AD related errors, server additions and removals, site link & subnet updates, and ADRAP review & corrections. Provides:

- SAN environment support for EMC Clarion, HP EVA, & Cisco MDS equipment
- Lights-out facility evaluation and setup of infrastructure including layout, rack setup, power, cabling, support equipment, and migrations of AD services
- Leadership for Symantec Enterprise Vault project; created initial project implementation plan and team creation
- APC StruxureWare Central installation and maintenance for over 200 devices
- DNS, DHCP, and WINS infrastructure maintenance; DNS scavenging WINS

UNISYS

Resource 75

Performance Specialist

consolation, DHCP standardization
- Documentation to standardize procedures for server and storage provisioning, Active Directory, SCOM, APC equipment
- Recent training on SCOM 2007 R2: Monitoring Optimizing and Troubleshooting

Becton Dickinson, Network Specialist/Administrator, Baltimore, MD, 1998 to 2007

Delivered support for Baltimore campus and 5 remote sites; maintained Microsoft Windows servers, IBM AS400 systems, Cisco & Nortel switches, Dell/EMC Network Attached Storage & Storage Area Network. Provided:
- VMware setup for development and disaster recovery.
- Installation of Citrix farm for applications and remote access.
- Monitor and manage APC InfraStruXure Manager. Covers all ups systems for servers and networking equipment including environmental systems.
- User & Group account, maintenance, and deletion as well as
- Share creation and maintenance.
- Configuration and maintenance for all Network Printers.
- Backups for Windows systems utilizing CA Brightstore ARCserve.
- Documentation on new and updated systems.
- Installation and support of Kronos time keeping system.

Other Employment includes:

- Prudential Health Care Plan, Sr. LAN Administrator, Baltimore, MD, 1992 to 1998
- Olin Corporation, System Manager/Programmer/Analyst, Red Lion, PA, 1988 to1992
- CACI Field Services, Systems Programmer, Mechanicsburg, PA, 1988 to 1988

Education

- Loyola College, Baltimore, MD, Masters of Engineering, Computer Science. 1997
- College Misericordia, Dallas, PA, B.S. Computer Science and Mathematics, 1988

Professional Certification

Microsoft Corporation

- Certified Systems Engineer – MCSE - Windows Server 2003, August 2006
- Certified Systems Engineer – MCSE - Windows NT 4.0, February 1998

UNISYS

Resource 75

Performance Specialist

ITIL

- ITIL Foundation v3 – May 2012

Hewlett-Packard

- Accredited System Engineer – ASE – March 1999

This page intentionally left blank.

UNISYS

Resource 76

Performance Specialist

Key Skills and Knowledge

- Domain Expertise & Solutions
- Management Consulting Services
- Project and Program Management
- Communication and Networking
- Databases
- Hardware
- Operating Systems
- Software/System Architecture
- Programming Languages & Tools
- Call Center and Help Desk
- Office Productivity Tools
- Technical Documentation
- Facilities Management
- .Net , TMG 2010, IIS, BizTalk
- Windows server 2003 / 2008, SQL 2005 / 2008
- Microsoft Operations Manager 2005(MOM)
- Microsoft system center configuration Manager (SCCM)
- Citrix Netscalers
- DNS and Active Directory
- Custom built Scripting(WMI/ WSH/Power shell/ Vbscript/ Jscript) for Various Automated System Wide Functions

Professional Summary

Strong Established track record with 17 years of experience in helping organizations to efficiently use their systems, networks and resources; ensuring that the design of a site allows all of the components, including computers, the network, and software, to fit together and work properly. Also monitor and adjust the performance of existing networks and continually survey the current computer site to determine future network needs; as well as troubleshoot problems reported by users and by automated network monitoring systems and make recommendations for enhancements in the implementation of future servers Technologies

- High skill level in Windows user level operating system, including user and application installation.
- Windows System Administration including an extremely wide variety of Enterprise applications that runs on and for them. Ranging from NetIQ, Microsoft Operations Manager (MOM) monitoring, System center Operations Manager 2007 R2, system Center Configuration Manager 2007 R2, System center operation manager 2012 , SQL Reporting services, Microsoft Cluster service, Oracle and SQL DB servers, VBScript, Power shell, ASP, .NET, BIZTALK Server, IBM Director, .
- Expertise in installing and maintaining Microsoft Web Server Clusters.
- Expertise in custom monitoring setup for third party applications.
- Advanced Virtualization Experience with Hardware migrations and Consolidations.
- Expert in Windows server 2000/03/08, MOM, SCOM SCCM, IIS, Microsoft Cluster Servers, Microsoft Active Directory, DNS, VBScript and Power shell.

Professional Experience

Commonwealth of Pennsylvania, Availability Consultant, Harrisburg, 2001 – Current

Provide System and Network Level 3 support for the servers, hardware, and applications. Primarily involved with the Design, implementation of System center Operations Manager 2007 R2, (Migrating monitoring infrastructure from MOM to SCOM, security audit, technical review, migration, implementation, maintenance and administration of agencies into the CTC Managed Hosting Facility .

- Work with application developers to ensure their application is compatible to environment. Application stress testing and deployment, configuring Web application in clustered environment.
- Developing dynamic reports using SQL reporting services
- On call support for Network Connectivity, operating system, and Application level Issues.

UNISYS

Resource 76

Performance Specialist

- Server Performance Analysis and Tuning.
- Developing MOM/SCOM management Pack depends on agency requirement.
- Working with agency to plan and implement projects on schedule.
- Resolving trouble ticket using Remedy Ticketing System.
- Review and updating application testing document
- Review and updating management packs in SCOM.
- Developing custom management packs for agency managed third party applications.
- Supporting applications 365/24/7
- Custom dashboard development using SCOM operational database.
- Troubleshooting VMware Host and Guest performance issue.
- Review and update documents as per agency requirements.
- Using Change Management Process for all Changes.
- Configuring and managing clusters and troubleshooting cluster related issues.

WasteSaver Inc., Senior Developer, New York City, 2000 - 2001

Develop applications to match waste removal requirements received from brokers and customers with the haulers preferences.

- Accomplished system study and design of the project, designing database coding, testing and implementation and maintaining Web server.
- Tools Used: IIS 4.0 with ASP 2.0 SQL Server 7.0, COM+, visual Interdev, visual sourcesafe 6.0, visual basic,6.0, macromedia dream weaver 3.0, Microsoft transaction server 2.0, vbscript, Java script, Maptitude for the Web and cybercash.

Easton Inc., Senior Developer, Downers Grove, IL. 2000 - 2000

Developed and implemented sales forecast reports.

- IIS 4.0 with ASP 2.0 SQL Server 7.0, COM+
- visual Interdev, visual sourcesafe 6.0, visual basic,6.0
- vbscript, Java script

First Horizon Home Loan Corporation, Senior Developer, Irving, TX, 1999 - 2000

Responsible for day-today- tasks on the production and development systems

- Maintained application for 400 Web sites for loan officers.
- Administering IIS servers and SQL Database.

UNISYS

Resource 76

Performance Specialist

Other Employment:

- Mass Mailing Center Pvt Ltd, System Administrator, India 1993 - 1999
- Pascal Computer Center, Network Administrator, India , 1991 - 1992

Education

- Bachelor of Commerce (B.COM), University of Madras, India (1988-1991)
- Advanced Post Graduate Diploma in Computer Application, LANESDA, Chennai, 1990-1992

Professional Certification

- Microsoft Certified Solution Developer
- Microsoft Certified System Administrator
- Microsoft Certified Professional
- Microsoft Certified Professional in Monitoring and Operating a Private Cloud
- Certified in ITIL

Professional Development

- Microsoft System center Operation Manager 2007
- Microsoft Clustering service (MSCS)
- Microsoft IIS7.0

This page intentionally left blank.

UNISYS

IBM

Resource 77

Performance Specialst

Key Skills and Knowledge

- z/operating system
- z/operating system Performance
- Software Tools
- Linux
- SAS70

Professional Summary

z/operating system Analyst responsible for providing performance engineering, programming, analysis, and support for systems on which applications are developed and deployed. The role requires in depth knowledge of multiple aspects of software including operating system software, related subsystem software, and a multitude of various program products. In depth knowledge of multiple types of hardware is also required. Expert use of software tools used to analyze and report on software and hardware effectiveness and efficiency is required. This includes, but is not limited to: creation and modification of computer programs, evaluating planned hardware and software changes, comparing alternative technologies and configurations, recommending system and subsystem performance enhancements, testing changes, and ensuring performance service levels are continually attained,. The role is key in ensuring mainframe computing dependent business goals are achieved. The role has responsibility for independently interpreting complex customer requirements, implementing solutions, and providing leadership and direction within and across competencies, sectors, and customers.

Employment History and Related Experience

OAOT/POMEROY CONTRACTOR, Performance and Measurements Analyst on contract to IBM, Harrisburg, Pennsylvania, 1999-To Date

As a Performance and Measurements Analyst, was responsible to:

- Collect of daily measurement and performance data and maintaining required retentions for existing LPARS.
- Provide Service Level reporting.
- Ensure Performance tool selection and usage provides optimum functionality with minimum resource consumption. Analyze product specifications, relevant standards, dependencies and business impact.
- Perform thorough research and analysis to identify trends for the purpose of predicting and avoiding negative performance impact.
- Perform analytical studies identifying deficiencies and developing solutions which enhance effectiveness.
- Provide input for hardware / software changes.
- Develop baselines for new SLA components.
- Perform production workload and resource analysis for the purpose of forecasting.
- Analyze and implement configuration parameters to optimize system usage.
- Create and support ad-hoc reporting.
- Provide z/operating system Workload Manager support.
- Provide SAS70 Audit support.

Resource 77

Performance Specialst

- Analyze Linux Performance Statistics
- Install and support of Omegamon z/operating system.
- Install and support Sub-capacity reporting (SCRT) and submission thru LMDS.

VENATOR GROUP INC., Data Center Manager, Camp Hill, Pennsylvania, 1987-1998

Responsible for maintaining enterprise wide Computer Operations, Job Scheduling, Report Distribution, Telecommunications, and Contingency Planning.

VENATOR GROUP INC., Resource Management Technician, Camp Hill, Pennsylvania, 1978-1987

Establish and provide a comprehensive management reporting system. Capacity planning and forecasting, performance and workload analysis Impact analysis of new applications on system resources. Support Chargeback. Perform modeling and simulations for hardware / software acquisitions.

Education

Huntington Area High School, Huntington, Pennsylvania

Electronics Institute – Basic Electronics

UNISYS

IBM

Resource 78

Performance Specialst

Key Skills and Knowledge

- Application delivery optimization and tuning; i.e. understanding how the application interacts with and impacts the network, and how the network interacts and impacts the application, especially how it relates to data center optimization projects such as data center and / or server consolidation or application migration.
- Strong leadership skills, solution design based on overall customer requirements, and building customer relationships.

Professional Summary

An experienced Senior Consultant with concentration in network application performance, simulation, modeling, and capacity planning. Thirty-one years in the network communications industry, twenty-six with the IBM Corporation with roles ranging from network Sales Engineer post and pre-sales technical support, network consulting, application performance optimization consulting to service offering development. Consulted in network design and implementation with an emphasis on end-to-end application performance, optimization, and scalability, systems and network management. This includes client/server, multi-tier, Web (Internet/Intranet) and Web Services.

Solves customer's complex network application performance, testing, and scalability issues using proven methodologies, effective leadership and analysis skills, modeling and profiling tools. Focus is on application delivery optimization using issue based consulting as a foundation and mathematical and discrete simulation tools to identify network and application impacts, network bottlenecks and other network application performance inhibitors. Acquired in-depth knowledge of key customer initiatives, such as Data Center / Server consolidation and application migration by working closely with IBM customers, and through the development and support of various IBM services offerings.

Employment History and Related Experience

IBM, Global Services ITS / Certified IT Specialist, Raleigh, North Carolina, 1994-To Date

As a Senior Consultant, I work in the currently named Application Performance Optimization Consulting (APOC) ICS practice.

- Provide team leadership through engagement management.
- Responsible for solution development, design and delivery.

IBM, Marketing Branch Office Communications Specialist, San Diego, California, 1989-1994

Provided pre and post-sales support of all IBM hardware and software networking products such as the 3174 and 3745 controllers, VTAM and NCP, with emphasis on emerging SNA and IP based LAN and WAN technologies.

IBM, Data Communications Systems Engineer, Rolm Company, New York, New York, 1986-1989

As a Marketing Branch Office Data Communications Systems Engineer, provided both pre and post-sales support for all Rolm Company voice and data communications products.

Resource 78

Performance Specialst

Education

Certificate of Diploma equivalent to a BS in Computer Science, Coleman College, San Diego, California

Certification

Member of IBM IT Certification board since 1995; IBM 2010 Corporate Innovation Award winner; multiple patent disclosures submitted for review and patent filing.

UNISYS

IBM

Resource 79

Performance Specialist

Key Skills and Knowledge

Hardware

- IBM e-Servers (Z - z900 and z990, X and P series)
- Sun E4500
- IBM F20 and M800 ESS
- IBM 3174 and 2074 CUs
- 3490E and 3590 tape systems
- Hitachi 9900 lightning series
- EMC 5830 DASD and Cisco routers
- Switches and load balancers.

Enterprise Banking and Brokerage Applications and Delivery Channels

- Hogan and CAMS II
- Teller, ATM, VRU, Call Center, Internet Banking and other on-line and batch banking applications
- GSTP (Global Straight Through Processing - Equities Clearing/Settlement)
- CLS (Currency Clearing/Settlement)

Systems Software (Mainframe)

- VM
- z/operating system
- TPF
- MQ
- WAS
- CICS
- DB2
- Parallel Sysplex
- Data sharing, and

Professional Summary

Experienced IT specialist with concentration in performance and scalability testing of complex mainframe and distributed systems. Over twenty years of professional experience with roles ranging from project lead for benchmarking of mainframe and distributed systems to integration lead of large scale distributed systems integration projects. Experienced in benchmarking and performance testing solutions of z/operating system based mainframe and e-business applications and infrastructure. Strong technical and leadership experience in a wide range of technologies and platforms. Extensive consulting experience with IBM enterprise customers in the finance industry and expertise in systems integration and testing of mainframe and Web-based applications. Worked with IBM development and field organizations as well as business partners and sub-contractors and has a good understanding of IBM's business management systems and practices.

Employment History and Related Experience

IBM, Certified IT Specialist, Gaithersburg, Maryland, 1996-To Date

Led several mainframe and e-business performance benchmarking engagements as a performance test lead and architect.

Lockheed Martin, Advisory Programmer, Rockville, Maryland, 1994-1996

Worked as an advisory programmer in Lockheed Martin's Federal Systems Division.

IBM, Senior Associate Programmer, Endicott, New York, 1984-1994

Worked as a senior associate programmer in IBM's National Service Division and a staff programmer in IBM's Federal Systems Division.

Assignment History

Capital One Financial, Project Lead, Richmond, 2009-2010

Assigned as the project lead in conducting a scalability benchmark of CSC's credit card processing application CAMS II and assisting Capital One Financial in evaluating the scalability of the on-line and batch components of CAMS II. The benchmark was part of Capital One's initiative to replace some or all portions of the existing card-holder systems - Billing, Authorizations, Account Management, Customer Information, Account Information and Terms Management.

- Assisted Capital One with gathering customization requirements for Hardware: Processors, channels, storage, I/O subsystem, coupling facilities; LPAR configuration: Number, processor definitions, weighting; CICS configuration: Number of regions, system initialization parameters; DB2 data sharing: Buffer pool tuning, thread management; Workload management and priorities and Multi-streamed batch.

IBM

Resource 79

Performance Specialist

VSAM/RLS

Systems and Applications Software (Distributed Systems)

- AIX, NT, Web and Apps.

Servers and PeopleSoft Financials

- General Ledger
- Accounts Payable
- Purchasing, e-Procurement
- Project Costing
- Asset Management
- Inventory
- Delivery System and SCM.

Performance Testing Tools

- IBM's Workload Simulator (TPNS)
- Load Runner and Silk Performer.

Protocols and Languages

- LU0
- U2
- LU6.2
- SNA
- TCP/IP
- IBM S/390 Assembler
- Rexx

Air Traffic Control Systems

- National Airspace System (NAS)
- Flight Data Management
- Control and Monitoring
- ATC SIM
- System Analysis and Recording (SAR).

- Involved with the planning and configuring of a test infrastructure and providing technical consulting and systems support for workload development, test execution and performance analysis and reporting for assessing the scalability of the base CAMS II application for supporting Capital One's projected growth of the card business.

Continuous Link Settlement, Project Lead, London, United Kingdom, 2002-

Assisted with the planning and configuring of a distributed systems infrastructure and conducted performance and fail-over testing for IBM UK's CLS integration contract for modernizing the currency settlement and clearing system that was funded by a group of major regional and reserve banks from the US, UK, Japan, Germany, France, etc.

- Led a planning session with IBM UK architects and developers to gather requirements related to building of the infrastructure and workloads, SLAs, load drivers, etc. for conducting the performance and fail-over testing.
- Assisted with the planning and building of primary and secondary sites to mirror the IBM UK CLS production system. Provided technical leadership and assistance with supporting the infrastructure, including setting up the load drivers, stubbing out-of scope interfaces and executing the performance and fail-over tests.

Global Straight Through Processing, Project Lead, Zurich, Switzerland, 2001-2002

Involved in conducting performance, scalability and fail-over validation testing of the equities settlement and clearing system for GSTP AG, which was a consortium of full service brokerages such as, Merrill Lynch, Solomon Smith Barney, CSFB, Prudential, etc.

- Assisted GSTP with identifying performance and capacity requirements and fail-over support required for redundancy and continuous operation of a mission critical system. He provided insight into the performance characteristics and architectural constraints of the system, which enabled GSTP AG to make critical decisions related to system acceptance.
- Led a planning workshop for gathering requirements, defining objectives, scope, physical/logical configurations, workload analysis, driver development, and testing strategy. He also developed and reviewed with GSTP a detailed test strategy plan and obtained customer concurrence on key issues.
- Assisted with the performance testing of mainframe and distributed systems consisting of an IBM S/390 Parallel Sysplex (GDPS) running MQ Series, CICS, DB2 and front-end Sun E4500 processors running Solaris and MQ Series. He provided support for the development, execution and performance monitoring and reporting of the workloads.

IBM

Resource 79

Performance Specialist

Goldman Sachs, Project Lead, New York, New York, 1999-2000

Assisted Goldman Sachs with the planning and execution of a performance test of their Order Book Java application using Orbix proprietary protocol for supporting connectivity and end-user interface between the Java Virtual Machines (JVMs) and the Order Book application running on a Sun E4500.

- Assisted with the execution of Order Book workloads to determine the number of users and transaction rates that can be supported with acceptable response times, number of concurrent sessions and orders that can be processed and the resource consumption from scaling the workloads and evaluated the performance and capacity of the supporting infrastructure.
- Involved in collecting system and application performance metrics to determine performance in terms of CPU busy, I/O rates, run queues, memory utilization, transaction processing time and end-to-end response times.

National City Bank, Project Lead, 1999

Involved in planning and executing a performance test of the Teller, ATM, CIMS, VRU, Call Center, DDA and SVN on-line and batch workloads to verify if the UFAM VSAM/RLS architecture would work with expanded sizes and larger volume of data for a $166 billion bank and if the hardware/software infrastructure would handle peak production transaction volumes.

- Assisted with the development of 3270 LU0 and LU2 based ATM and CI MS workloads. Extracted the message traffic from FEPI logs and captured formatted 3270 data streams for the ATM and CIMS workloads.
- Assisted with the execution of on-line workloads in a VSAM RLS parallel sysplex data sharing environment at the projected peak transaction rates along with critical path batch schedules to identify problems related to I/O bottlenecks and elongated run times.

VISA, VISA Integrated Payment Performance Benchmark Project Lead, San Mateo, California, 1998 – 1998

Assisted VISA with planning the benchmark, building a complex VM, MVS and TPF large systems environment and executing performance tests of the VIP system to evaluate new processor and storage technologies from IBM, EMC and STK and to ensure their projected growth in transaction volumes could be handled by the available resources.

- Planned switchable physical configurations of front and back end processors consisting of IBM XZ7, ZZ7 and z900 processors along with EMC DASD and STK tape systems to mirror VISA's production systems and provide variations of front and back end systems for a variety of performance/capacity configurations.

Resource 79

Performance Specialist

- Involved in implementing a solution for capturing and replaying production transactional messages and developed/maintained Acquirer and Responder scripts to simulate the Acquirer and Issuer by sending requests to the VIP system and generating matching responses.
- Assisted VISA with collecting performance measurements and testing tuning changes for improving performance. In this benchmark, there was a simulation of a high volume of SNA and TCP/IP transaction workloads running on the XZ7 and ZZ7 processors using a TPNS/MVS driver running on a z900 processor and connected to the target systems with CTCs and gigabit OSA adapters. .

United Kingdom Civil Aviation Authority, Technical Lead, Portsmouth, United Kingdom, 1993-1996

Responsible for the planning and integration testing of a complex large scale air traffic control system involving hardware and software from IBM and other vendors as an advisory programmer and systems integration technical lead of the Control and Monitoring (CMS) and Flight Data Processing (FDP) subsystems on assignment at IBM, UK.

- Assigned to a team that delivered, to the UK CAA's specifications, an integrated mainframe and distributed client/server system to provide ATC functionality for flight and radar processing and controller display support for Euro Control.
- Integrated the FDP subsystem containing enhancements to the existing National Airspace System (NAS) mainframe application and a new distributed FDP client/server implementation in which flight data was stored and processed to allow correlation with radar data and posting of electronic flight strips at controller workstations.
- Integrated the CMS subsystem to control and monitor all local and remote hardware and software components within the ATC system using hierarchical rules for propagating system status to the operator. Worked with the development and integration teams to track and manage configuration and change (code and new releases) management requests using CMVC.
- Planned and managed the production and inspection of the system acceptance test (SAT) scripts. Conducted the final system acceptance (SAT) tests to demonstrate to the customer that program specifications and requirements were met. He also supported the planning and development of operational training courses for CAA personnel.

Federal Aviation Administration, Staff Programmer/System Integration Technical Lead, Rockville, Maryland, 1988-1993

Assigned as a Staff programmer and system integration technical lead for the Federal Aviation Administration's multi-billion air traffic control (ATC) contract to design, develop, integrate and implement the next generation of air traffic control

system for the United States.

- Performed as a key member of the software integration and test (SWIT) group and technical lead of the ATC integration team. Made significant contributions towards integrating ATC functionality - flight, radar and controller display support across multiple platforms and application components and identifying and resolving system problems in the mainframe and AIX environments.
- Hands-on experience with the NAS mainframe application and supporting utilities running in native and guest modes. Gained experience with UNIX externals, commands, shell programming, file system, tools and compilers, such as ADA and 'C'. RS6000 applications included CXSS - Common Support Services providing LAN services and distributed processing support for mission critical ATC flight and radar applications.
- Documented testable system functions and interfaces. Developed tools, ATC scenarios and simulation techniques and identified areas of the system that were operationally unacceptable and made recommendations to improve functionality and performance. Provided technical guidance to team members on requirements and assisted with problem determination and resolution.

Level 2/Change Team, Senior Associate Programmer, Endicott, New York, 1984-1988

Worked on IBM VM/370 systems and provided world-wide L2/L3 software support for the VM/SP and VM/SP HPO control program and the VM/SP CMS operating system on the IBM 3090, 3081, 3083, 4381 and 9370 series of processors as a senior associate programmer on the L2 and Change team member for VM large systems support, NSD central programming services.

- Extensive knowledge and familiarity with the large systems architecture, assembler and the internal structure and function of the VM control program and CMS operating system. Worked closely with the internals of VM operating system - Installation and Migration, Directory Maintenance, Guest Operating Systems, Real and Virtual IPL, Paging, Spooling, I/O Subsystem, Interrupt Handling and Uni/Multi processor configurations.
- Developed code and documentation alterations through APARS for correcting reported failures without changing program specifications. Built and maintained second level test systems and developed test cases for recreation and testing of the original problems and verified that the alterations had preserved the program interfaces with no regression. Participated in code reviews and APAR certification processes involving new/modified development code and PTFs.

UNISYS

IBM

Resource 79

Performance Specialist

Education

Master of Science in Computer Science

Fairleigh Dickinson University, United States of America, 1983

UNISYS

Security Administrator

This page intentionally left blank.

UNISYS

Resource 80

Security Administrator

Key Skills and Knowledge

- Certified Information Systems Manager (CISM)
- Certified Information Systems Auditor (CISA)
- Certified Business Continuity Professional (CBCP)
- ITIL v3 Foundations Certified
- Experience with COBIT, ITIL, FISMA, FBI, CJIS, NIST, IRS, SSAE16, PCI, HIPAA, ISO 27000 & 20000 Audit Standards

Hardware Experience

- Intel and RISC-based servers, IBM z-Series, i-Series, p-Series and x-Series; EMC, XIV, Avamar and Data Domain storage platforms, Cisco routers/switches; CheckPoint & Cisco Firewalls

Software Experience

- LDRPS and BIA Professional planning software, Microsoft operating system, VMware, Retina, Qualys, RSA enVision and AA, SCOM, Cisco MARS & IDSM, BladeLogic and various PC forensic tools

Professional Summary

15 years of engineering and technology leadership for global enterprises, regional consulting firms, and state governments. Strong advocate of ISO 27001 & 20000 certification processes. Always ensures IT security and business continuity contractual obligations are met, leads all internal and external audits related to various state, federal & industry standards (SSAE16/SAS70, CJIS, IRS & FISMA), and consulting with cross-functional Unisys and Commonwealth of Pennsylvania agencies on how to properly apply risk mitigation techniques in support of protecting IT assets.

- Managed up to twelve direct reports at one time as well as directed cross-functional teams on multiple, simultaneous security and continuity projects
- Trusted advisor to CIO, VP and other upper management roles in support of high priority initiatives affecting organizational reputation as well as the confidentiality, integrity and availability of valued IT assets

Employment History and Related Experience

Unisys, Project Security & Continuity Manager– Commonwealth of Pennsylvania DPH, Harrisburg, PA, 2009 to Present

Delivers proper audit and compliance methods are applied to the infrastructure managed by Unisys for the Commonwealth of Pennsylvania (Commonwealth of Pennsylvania) Data PowerHouse contract.

- Leading the ISO 27001 & 20000 certification processes, ensuring IT security and business continuity contractual obligations are met
- Leads all internal and oversees external audits related to various state, federal & industry standards including SSAE16/SAS70, CJIS, IRS & FISMA
- Consults with cross-functional Unisys and Commonwealth of Pennsylvania agencies on how to properly apply risk mitigation techniques in support of protecting IT assets.
- Managed end to end disaster recovery tests for Bureau of Integrated Enterprise Systems (IES) and Department of Revenue (DOR) AIX/SAP platforms as well as other Wintel/VMware platforms for various agencies (DOH, PSP, DPW) in the Commonwealth of Pennsylvania Data PowerHouse.

AOPC, IT Systems Security Officer, Mechanicsburg, PA, 2008 to 2009

Responsible for the design, development, oversight and coordination of information security and business continuity related activities for the Administrative Office of the Pennsylvania Courts.

- Creation of information security policies, development of risk assessments for executive review

UNISYS

Resource 80

Security Administrator

- Generation of application security reviews, firewall and network change management reviews
- Assurance of proper risk mitigation methods in support of the protection of data stored in the Unified Judicial System for the Commonwealth of Pennsylvania

Penn National Gaming, Inc. Corporate, IT Risk Manager., Wyomissing, PA, 2006 to 2008

Delivered design, development, oversight and coordination of information security and business continuity related activities for a 17-property, $3B casino gaming firm.

- Created of security policies, standards, architecture and risk assessments ensuring the security and integrity of the company's networks and databases
- Business continuity and IT recovery strategy amongst all properties and applications
- Coordination of IT compliance associated with PCI, Sarbanes-Oxley and HIPPA (self-insured employer) standards and regulations in conjunction with senior management and internal audit staff.

Other Employment History

- Principal Consultant/Owner for Ethix Consulting, LLC, Harrisburg, PA, 2005 to 2006
- Practice Director for Anexinet Corporation, Philadelphia, PA, 2000 to 2004
- Senior Consultant for Actium (now Idea Integration), Conshohocken, PA, 1996 to 2000
- Systems Administrator for Lehigh Press, Cherry Hill, NJ, 1995 to 1996
- Technology Specialist for Good Samaritan Hospital, Lebanon, PA, 994 to1995
- IT Manager for GemChem, Inc., Lancaster, PA, 1993 to 1994
- Systems Analyst (Intern) for Medical College of Pennsylvania, Philadelphia, PA, 1992 to 1993

Education

- BS, Management Information Systems: Saint Joseph's University, Philadelphia, PA, 1993

Certifications

- CISM, CISA, CBCP, ITIL, currently pursuing CISS

UNISYS

INFO-MATRIX CORPORATION

Resource 81

Security Administrator

Key Skills and Knowledge

- Network & System Security
- Risk Management
- Vulnerability Assessments
- Authentication & Access Control
- System Monitoring
- Regulatory Compliance
- System Integration Planning
- System Administration
- Certified Information Systems Security Professional (CISSP) (May 2012)
- Citrix Certified Enterprise Administrator (CCEA)
- CompTIA A+ Certification
- CompTIA Network + Certification
- Microsoft Certified Professional (NT 4 & 2000)

Platforms: Windows 9x/NT, 2000/2003, 2008, XP/7, VM Ware, Mac operating system

Networking:
- TCP/IP, TLS, VPN, SSH, PKI
- CheckPoint Firewall,
- Proventia IPS/IDS

Tools and Software:
- CheckPoint,
- ISS RealSecure
- Trend Micro OfficeScan and Intrusion Defense Firewall, IWSVA,
- Anti-spam software,
- EMC EmailXtender
- Tumbleweed, Lotus Notes, Encase
- VPN Software, Nessus
- Network Solutions
- Active Identity
- Proxy Servers
- IBM Content Collector
- VB scripting.

Professional Summary

Security Analyst with 10 years' of experience delivering information security, CISSP certification, detailed knowledge of security tools, technologies and best practices.

- Experienced in the creation and deployment of solutions protecting networks, systems and information assets
- Utilize Internet Security Systems (ISS) RealSecure Server Sensor, RealSecure Desktop Sensor and Proventia Desktop sensor to support customers
- Update CheckPoint firewall rules as needed
- Perform computer forensics using Encase when security incidents warrant.
- Develop and test disaster recovery procedures.
- Evaluate new security technology as needed and present findings to management.

Employment History and Related Experience

PHEAA, Information Security Analyst, Harrisburg, Pa., 2002 - Present

Utilize Internet Security Systems (ISS) RealSecure Server Sensor, RealSecure Desktop Sensor and Proventia Desktop sensor to monitor IDS alerts. Create Proventia polices to protect workstations as needed.

- Deployed and maintain Trend Micro' Anti-Virus software on over 3000 workstations and 200 servers.
- Responds to security related incidents and taking appropriate action.
- Implemented and administer an appliance based Anti-Spam/Anti-Virus solution for all inbound e-mail.
- Administer EMC EmailExtender e-mail archiving solution and EMC CLARiiON.
- Resolve security related trouble tickets.
- Responsible for patching security servers, also ensure all other agency servers are patched.
- Administer enterprise patching software WSUS, to ensure all 3000 workstations are patched.
- Maintained Verizon Business (Cybertrust) certification.
- Update CheckPoint firewall rules, Perform computer forensics using Encase
- Develop and test disaster recovery procedures.
- Evaluate new security technology as needed and present findings to management.
- Configured and manage software that monitors user Internet activity.
- Deploy and administer two-factor smartcard authentication system.

Resource 81

Security Administrator

Perfect Order, Senior Consultant, Mechanicsburg, Pa., 2000 - 2002

Provided support to over 200 nodes in multiple remote locations, end-user telephone support in a 50+ client, multi-platform corporate environment, and provided onsite Desktop support for new installs and established clients.

- Provided onsite support for new Proprietary application rollouts
- Diagnose and resolve advanced software and operating system issues

Square D Company, Systems Analyst, Mechanicsburg, Pa., 1992 - 2000

Analyzed data to determine if products were missing from a shipment, provided data that customer shipments were received, and worked closely with management to find ways of improving processes.

- Utilized SAS to analyze data and run reports and a daily basis.
- Maintained database records and developed reports used to convey project metrics and analysis.
- Created an Access database to record and track returned parts lost during shipping.

Contel/GTE, Computer Operator Hershey, Pa., 1991 - 1992

Maintained computer systems, performed nightly backups, ran pay roll processing.

- Assisted users in troubleshooting PC and communication problems.
- Installed/Maintained hardware and software.
- Preformed full and incremental backups on a VAX system nightly.
- On-call during weekends to handle any system outages.

Education

Computer Learning Network Camp Hill, Pa.

Computer Systems Technology 400 Certificate January 1991

Harrisburg Area Community College Harrisburg, Pa.

Completed all courses for MCSE NT 4.0 April 2000

Certifications

- Certified Information Systems Security Professional (CISSP) (May 2012)
- Citrix Certified Enterprise Administrator (CCEA)
- CompTIA A+ Certification
- CompTIA Network + Certification
- Microsoft Certified Professional (NT 4 & 2000)

UNISYS

e&e IT Consulting Services, Inc.

Resource 82

Security Administrator

Key Skills and Knowledge

- Top Secret Clearance
- CISSP
- Security +
- ITIL foundation V3
- ASA/PIX Cisco firewalls
- CheckPoint: SPLAT, R62 R65 R70
- VMware maintenance and troubleshooting
- Firewall maintenance for DOD, DISA, DLA, DDC…
- Troubleshooting network connection issues
- Implementing firewall rules
- Windows Server admin
- CheckPoint firewall admin
- Nokia/Check Point
- IP Series Firewalls
- Smartview Tracker
- Smartview Monitor, SmartDashboard
- Smart Update
- Remedy
- InfiniStream Sniffer
- Firewall Optimization.
- Microsoft Windows: 95, 98, 2000
- Blue Coat Proxy: SG800, SG810, BC Proxy Reporter
- Cisco Switches: 2900, 3500, 4500, and 6500 Series
- Cisco Routers:7200, 2800 Series
- Cisco Wireless:1131 & 1242 2700 Location Appliance, WCS Server
- Cisco Firewalls: ASA, PIX
- Juniper Routers: M-Series
- Stingray Load Balancer
- CiscoWorks, InfiniStream Sniffer

Professional Summary

Strong technical leader with 12 years of experience supporting DLA J6N networks in support of the DIACAP and vulnerability assessment as required. Participate in the development, testing, and implementation of an effective Incident Response plan. Respond to incidents as directed in the IR plans and provide investigative and forensic assistance as required. Participate in the development and implementation of INFOCON plans and guidance

- Maintain all current applicable firewall policies to include DOD, DISA, DLA, DDC, etc.
- Respond appropriately to reported or discovered incidents in accordance with the DLA J6N Incident response plan
- Prepare quotes and documents required to renew licenses and equipment maintenance for firewall
- Notify appropriate DLA J6N personnel of possible threats or systems vulnerabilities
- Develop and deliver briefings to the upper level management as required on a variety of subjects relating to Enclave Boundary Defense
- Ensure users are aware of and adhere to systems security policies and procedures
- Conduct systems security assessments, audits and reviews

Employment History and Related Experience

e&e IT Consulting / DoD, Network Security Engineer, New Cumberland, PA, 2012 – Present

Plan and deploy Enclave Boundary Defense systems and programs including FW, IDS, VPN devices and applications to all DLA Distribution activities. Provide daily maintenance and support for all DLA J6N Enclave Boundary Defense systems including monitoring system and log files.

- Review and resolve firewall log issues as to threats or possible compromises. Plan and deploy DMZs for each DLA J6N Firewall as required
- Provide assistance to DLA J6N personnel in maintaining the FW rule sets and provide advice on impact of requested changes to the FW rules on the network and compliance with applicable DOD, DLA and DDC policy
- Participate in the development, testing, and implementation of an effective Incident Response plan. Respond to incidents as directed in the IR plans and provide investigative and forensic assistance as required. Participate in the development and implementation of INFOCON plans and guidance

e&e IT Consulting Services, Inc.

Resource 82

Security Administrator

- Participate in the development and deployment of a comprehensive INFOCON test plan. Participate in the development and implementation of a secure and effective means of remote access for DLA/DDC employees who are working offsite
- Maintain all current applicable firewall policies to include DOD, DISA, DLA, DDC, etc. Respond appropriately to reported or discovered incidents in accordance with the DLA J6N Incident response plan. Prepare quotes and documents required to renew licenses and equipment maintenance for firewall
- Notify appropriate DLA J6N personnel of possible threats or systems vulnerabilities
- Develop and deliver briefings to the upper level management as required on a variety of subjects relating to Enclave Boundary Defense
- Ensure users are aware of and adhere to systems security policies and procedures. Conduct systems security assessments, audits and reviews
- Provide SIPRNet firewall and network support; perform information technology project management duties Advise the Branch Chief on new network developments and technology
- Recommend long range designs to the Branch Chief for planning and implementing network resources.

General Dynamics Information Technology, Network Engineer, Hagerstown, MD, 2010 - 2012

Plan and perform new installations and upgrades to applications and networks within DISA ESD as a new business team member. Engineer networking solutions and provide analysis of communications networks for Department of Defense customers. Work with the customer to translate requirements into a technical solution.

- Gathering technical information from clients and researching solutions, creating preplanning guides for customer review, presenting solutions to customers, creating communication documentation, creating appropriate networking additions and changes, troubleshooting issues and ensuring customer satisfaction
- Ensure standards compliance and network security while providing configuration changes for Cisco and Juniper routers, multi-vendor content switches, Blue Coat proxies and Cisco firewalls
- Worked closely with the Information Assurance group to make sure all changes were approved through DoD IA
- Create configuration paste files and submitted them to the government networking group. Plan network layouts, configure systems to user environments, and provide technical support and troubleshooting
- Regularly create COOP documentation and assist in COOP exercises. Create network drawings, reserve IP space and coordinate all efforts with

CCC network support. Act as a team lead and provide advice to meet customer requirements

- Configure and STIG equipment. Perform information technology project management duties and assist with DISA cost estimates
- Ensure that technical components are well integrated and proposals meet the needs of the customer
- Attend meetings and conferences to exchange information and advice on engineering, implementation, and sustainment of customer IT systems; prepare and present briefings.

Summit Health, Network Specialist, Chambersburg, PA, 2004 - 2010

Provide LAN and WLAN technical support for two hospitals and approximately 40 remote facilities. Check Point firewall administrator performing upgrades to R65 and R70, troubleshooting network connectivity issues and adding firewall rules. Blue Coat Proxy administrator in charge of proxy rule updates, device installations and upgrades.

- Performed proxy upgrade from a SG800 to a SG810 appliance
- Tracked company-wide Internet usage as a Blue Coat Proxy Reporter administrator
- Managed a five server Citrix Server Farm running Citrix Metaframe XP
- Configured, installed and supported Cisco wireless access points and controllers in both autonomous and LWAPP configurations
- Performed wireless site surveys for new installations and additional coverage. Support thin clients, laptops, tablets, VoIP phones, and handheld scanners
- Provided support for switches, routers, hubs, and other network hardware. Install and support the Neoteris remote access SSL VPN
- Performed server administration for over 100 servers on Windows Server operating systems
- Supported DHCP, Active Directory and GroupWise e-mail, VMware maintenance
- Administered file servers, the latest Microsoft Windows operating systems and electronic mail software. Assisting in preparation for the incorporation of the several architectures into an open system distributed network

Summit Health , PC/Desktop Support Technician, Chambersburg, PA, 1998 –2004

Troubleshoot end user connectivity issues. Configure, install, maintain, modify and troubleshoot personal computers, laptops, printers, wireless devices, various peripherals and software applications. Troubleshoot and resolve technical problems identified in trouble tickets.

e&e IT Consulting Services, Inc.

Resource 82

Security Administrator

- Provide initial setup of personal computers, high level Helpdesk phone support to end users, physicians and vendors
- Lead projects for the Windows desktop deployment for 1500 client computers
- Became a Certified HP Printer Technician and provided hands-on training to other technicians
- Developed and coordinated life cycle replacement and preventive maintenance plans for personal computers and printers
- Provided excellent support and communication to end users.

Education

- Hagerstown Community College, Hagerstown, MD, Cisco Network Academy, 2010
- York Technical Institute, York, PA, Associate, Computer Systems, 1998

Certifications

- ITIL Foundation v3, A+, Security+,
- CCENT, CCSPA, CISSP
- DoD Top Secret Clearance

UNISYS

e&e IT Consulting Services, Inc.

Resource 83

Security Administrator

Key Skills and Knowledge

- Top Secret / SCI security clearance
- CISSP
- RHCSA
- CEH
- Security +
- CheckPoint firewalls
- PfSense firewalls
- IBM WebSphere
- Apachchessl, Mysql, and Mod_Perl.
- contributed tools to the Nagios Exchange community (user knobbysideup) Senior Associate

Professional Summary

12 years of systems experience, primary analyst responsible for our high availability checkpoint clusters world-wide. Developed VPN appliance based on Linux, Iptables, and Freeswan to form tunnels and segregate internal untrusted networks. Developed cost saving solutions for hardware, licensing, and support. Generated deployable and manageable systems for entry level administrators freeing higher level security analysts to focus on other tasks.

- Create and maintain several virtual machine environments for development and production using VMware ESX server and VirtualBox
- Systems Monitoriing. used Nagios, contributed tools to the Nagios Exchange community (user knobbysideup) Senior Associate
- Develop and maintain Internet-accessible event and membership database; Created this using Apachchessl, Mysql, and Mod_Perl

Employment History and Related Experience

SAGE Dining Services, Linux System Administrator, 2010 – Present

Lead systems administrator in charge of all development and production servers, high availability clusters, networking infrastructure, and firewalls in 3 data centers located throughout the country.

- Developed systems management and development tool sets and processes, migrating from a complicated mess of systems and configurations to one that can be easily managed by a single administrator.
- Developed and deployed anti-spam relaying solution around Sendmail, MimeDefang, and SpamAssassin.
- Create and maintain several virtual machine environments for development and production using VMware ESX server and VirtualBox.
- Systems Monitoriing. used Nagios, contributed tools to the Nagios Exchange community (user knobbysideup) Senior Associate.

ICF Jacob & Sundstrom, Network Administrator, Sep 2007 - Dec 2010

Administer Linux systems used for analysis in a custom Network Intrusion Detection system. Travel for on-site NIDS Sensor deployments

- Cyber Defense research with the Army Research Laboratory's Center for Intrusion Monitoring and Protection (ARL CIMP).
- .Technical and Project Management lead in effort to automate packaging, deployment, configuration, hardening, and updates to remote IDS sensors, as well as automation of IDS sensor builds using kickstart, autoyast, rpmbuild, and yum.

- Developed SOPs for IDS Sensor development and maintenance.
- Research and Development of Systems Engineering and maintenance around Intrusion Detection Systems.
- Maintain infrastructure for vulnerability assessment team's scanning.

Yellow Breeches Racing, Developer / Systems Administrator Consultant, 2000 – 2007

Develop and maintain Internet-accessible event and membership database; Created this using Apachchessl, Mysql, and Mod_Perl. It uses Apache::DBI for persistent database connections, and uses Apache::Session for authentication and user preferences.

- Maintain Linux servers and network.
- Maintain team mailing lists. normal spam-fighting techniques are included, support list security and appending of a disclosure through some custom Mimedefang routines. Support mailing lists for some other groups.

Armstrong World Industries, Inc, Infrastructure Security Analyst, . 2002 – 2007

Delivers global infrastructure security, security systems management, reporting, incident response, risk management, and policy creation and enforcement to include HIPAA and SOX compliance. Delivers networking and security consulting with business units and technical staff to create solutions to meet the business's needs.

- Team lead and project management around security-focused projects. For example, the design and deployment of a system to detect wireless (802.11) policy violations.
- SSL certificate and reverse-proxy management
- Mail server and anti-spam management. created a mail quarantine system which is used by Armstrong to thwart '0-day' attacks, while also providing a method to detach large incoming attachments and multimedia files and provide a download area for the same. In addition, managed Armstrong's corporate SMTP gateways using a combination of sendmail, spamassassin, a custom mimedefang filter, NAI virus scanning, clamd virus scanning, and milter greylist
- Global Firewall and IPSec VPN management. Created standards to be used for forming network to network IPSec VPNs with business partner networks and branch offices.
- Developed a VPN appliance based on Linux, Iptables, and Freeswan to form tunnels with smaller branch offices, and also to segregate internal untrusted networks (like wireless barcode scanners at plant locations). This solution saved significant costs in hardware, licensing, and support. It was also deployable and manageable by network operations groups, freeing higher level security analysts to focus on other tasks.

e&e IT Consulting Services, Inc.

Resource 83

Security Administrator

- Client VPN management with strong authentication via RSA securid.
- Created online chat system for periodic interactive Q&A sessions with the CEO. This was based on a purchased Java applet, an ircd backend, and a Perl script for question moderation.
- Led transition of security operations and reporting tasks to outsourcing company.

ICSA Labs /TruSecure Corporation, Network Security Analyst, 1998 - 2001

Delivered Process, procedure, certification criteria, and report format development for both remote vulnerability assessment scanning and commercial firewall/VPN certification. Support remote network vulnerability scanning, analysis, assessment, and reporting.

- Database, vulnerability probing, and filtering software development to help automate the previous bullet.
- Commercial firewall and VPN testing and certification using a variety of tools to analyze all aspects of the products, often byte-by-byte using TCP/IP packet sniffers or product verbose logging facilities.
- Tool and filter development to aid in the previous bullet.
- Design, implementation, and administration of a Web-based database to track firewall and vpn product testing status. This database is still in use by ICSA Labs, and makes use of linux, apache, embedded perl, mod_perl, apache_session, and mysql.

Education

- BS Aerospace Engineering, Pennsylvania State University, 1993

Training

- Perl classes at Usenix LISA conference, 1998.
- CheckPoint firewall basic and advanced courses, 2002.
- Toorcon security conference 2002.
- Keane Project Management Methodology, 2003.
- Black Hat / Defcon security training: 2006, 2008, 2009.

Certifications

- Brainbench certifications: Internet Security Specialist, Perl Programmer, 2000.
- Red Hat Certified Technician (RHCT): 2008
- CompTIA Security+: 2008
- CISSP: 2009
- Certified Ethical Hacker (CEH): 2010
- Certified Penetration Tester (CPT): 2010

This page intentionally left blank.

UNISYS

Security Analyst

This page intentionally left blank.

UNISYS

e&e IT Consulting Services, Inc.

Resource 84

Security Analyst

Key Skills and Knowledge

- Top Secret Clearance
- CISSP, MCSE+1
- CheckPoint firewall design, configuration and implementations
- Enterprise level architecture
- Change and Risk management
- Multitier network configuration and deployment
- Network system security and monitoring
- Vulnerability and security support
- Security integrity and application of DoD security policies and procedures
- Automated security assessment tools and benchmarks (using OVAL code)
- Test and evaluate security configuration requirements
- United States General Services Administration (GSA) and Homeland Security Presidential Directive 12 (HSPD-12).
- Level 1 and 2 Security Assertion Markup Language (SAML) assertions.
- Computer Emergency Response Team (CERT)

Professional Summary

Technically astute IT professional; proficient at the strategic planning and deployment of innovative, comprehensive and scalable infrastructure solutions aligned with organizational core goals and strategies. Qualifications include MCSE+I, CISSP, and 21+ years of experience on numerous operating systems, network protocols and administration tools.

- Network and Infrastructure – Involved in Project Planning Management (PPM) and Life Cycle process to enable the effective integration of projects and their outputs.
- Vulnerability Assessments – Identify, quantify and prioritize vulnerabilities; Develop written discussion as to why vulnerabilities exists
- Systems Security – Cultivate security guidance for multiple operating system platforms and applications; Develop Information Assurance (IA) system architecture, policies and implementation guidance in accordance with Federal and DoD AIS security regulations and effectiveness of existing IA best practices and policies
- Technical Liaison – Develop and present PowerPoint presentations dealing with classified vulnerability briefings to DoD high level commanders of different branches of the armed forces including the National Security Agency (NSA)

Employment History and Related Experience

Hewlett Packard (acquired EDS), Letterkenny Army Depot, Senior Systems Engineer, Chambersburg, PA, 2009 – Present

Technical lead supporting the Defense Information Systems Agency (DISA) Field Security Operations (FSO) division in providing Information Assurance/Information Security Services to the Department of Defense (DoD). Provide expert security vulnerability analysis, guidance, recommendations and deficiency resolution support to customer locations.

- Security Technical Implementation Guides (STIGS) – Gather requirements, develop and publish assessments and configuration checklists for Multiple Operating Systems, Networking Components, Application Servers and Administration Policies
- Utilize the 8500 for existing STIG updates and the 800-53 for new STIG development.
- Participate in pre DIACAP assessments; Work closely with security team in coordination of project timelines.
- Research/devise methodology for examination of the system for vulnerability; Collaborate with customer for concurrence before development and deployment of corrective action

- Provide vulnerability and security support to global DoD sites.
- Ensure security integrity and application of DoD security policies and procedures throughout the project life cycle of proposed system changes; Develop automated security assessment tools and benchmarks (using OVAL code)
- Build, test and evaluate security configuration requirements ensuring compliance with existing guidance or documented test requirements
- Create evaluation scripts with Security Content Automation Protocol; Develop; Cultivate security guidance for multiple operating system platforms and applications
- Incident Response – Deliver Incident response and 2nd level STIG support.

EDS/HP, County of San Diego, Project Lead, 2007 – 2009
Project Lead for the County of San Diego Active Directory (AD) redesign and migration to multiple remote facilities for 45,000 users across 8 remote sites at Tulsa, OK and Plano, TX

- Analyzed business processes by interviewing department leads.
- Re-designed the Network Architecture to improve response times.
- Technical Liaison between the Chief Information Officer of San Diego and the host remote sites of Tulsa, OK and Plano, TX.
- Technical Lead for the AD migration to all remote sites.

EDS/HP, FedTraveler.com E-Gov Travel Service (ETS), Technical Lead, 2005 – 2007
Technical Lead for the integration of a single "sign-on" solution for the Federal Travel portal.
Technical support provided through 2009.

- Engineered Identity Management (IdM) Integration for E-Authentication.
- Incorporate IdM for front end user authentication using RSA Federated Identity and Access Management software.
- Evaluate and verify compatibility with 6 other IdM vendors for United States General Services Administration (GSA) and Homeland Security Presidential Directive 12 (HSPD-12).
- Performed Level 1 and 2 Security Assertion Markup Language (SAML) assertions.

EDS/HP, Commonwealth of Pennsylvania, Security Consultant, 1999 – 2005
Assigned by the Deputy Director to work with the following state agencies: Attorney General's Office, Department of Health, Department of Labor and Industry, Department of Education, Department of the Interior and the Commonwealth Technology Center.

- Install Cisco switches and routers and configure initial routes and Access Control Lists (ACL's) for several agencies

e&e IT Consulting Services, Inc.

Resource 84

Security Analyst

- Worked with Intrusion Detection System (IDS) vendor on compatibility issues between Host Based Intrusion Detection Systems (HIDS) and Microsoft Data center Edition software
- Design and implement Clustered Firewalls solutions
- Participate in the design, installation and maintenance of the Enterprise Intrusion Detection System (IDS) and Intrusion prevention system (IPS); configuration of central log monitoring which included firewall, server and IDS logs and the automation of the Host Based Intrusion Detector Sensors (HIDS).
- Develop system security policies and procedures in compliance with the Commonwealth of Pennsylvania security regulations
- Participate in security network architecture for the enterprise
- Perform Web scans and penetration testing on the enterprise server farm and provide agency specific reports on vulnerabilities and how to mitigate
- Implement a Certificate Authority/Public Key Infrastructure (CA/PKI) solution
- Member of Computer Emergency Response Team (CERT), Provided the Department of Education with pre-notification of a Hacker intrusion (when and how) by profiling said Hacker
- Responded to a CERT call for the Sequel Server "slammer" worm that had infected Commonwealth mission critical systems
- Demonstrated ability to trace and identify the overseas hacker, and provided documented to the Pennsylvania State Police for prosecution

EDS/HP Internal Support Services, System Analyst, 1997 - 1999
Executed Domain administration including Windows NT 4.0 through Windows 2008R2 AD migration. Provided desktop support. Provided administration and migration of Exchange 5.5 thru Exchange 2010.

- CheckPoint Firewall support and network DMZ configurations
- Performed network design and security analysis
- Configure multiple DMZ's using Nokia Network appliances and CheckPoint firewall software for EDS internal use.

Department of Defense Financial and Accounting Services (DFAS), Technical Lead, 1995 – 1997
Perform network analysis and monitoring, system sizing, and performance tuning of the client/server configurations.

- Design and implement new imaging technologies
- Automate client application installation procedures and supporting documentation using multiple package configurations (VB install, Rapid Install, SMS, and scripts)
- Develop and maintain Daily Operation Guides (DOG) and Continuity of Operations Plan (COOP).

e&e IT Consulting Services, Inc.

Resource 84

Security Analyst

- Defense Distribution – Susquehanna, PA (DDSP) Initial and configure initial Server farm consisting of 12 servers.

ACCO Chain and Lifting Products, UNIX System/Network Administrator, 1994 – 1995
Design and implement a class B TCP/IP network using LAN Manager 2.2 and Microsoft Windows 3.x/95 accessing HP 9000 servers.

- Oversee the acquisition and installation of the hardware; perform system administration backup, and recovery procedures
- Manage 17 remote locations accessed via T-1 throughout the US and Canada
- Design and test duplicate network infrastructures, installation of new communications equipment, and software at each of the new sites
- Evaluate the network and system performance requirements

Administrative Office of Pennsylvania Courts, Technical Services Network Manager, 989 – 1994
Supported the Common Pleas Courts Automation Project. Design client/server network prototype utilizing Ethernet topology over T1 communication links. responsible for the day to day operations and networking performance.

- Managed an operations and networking staff of 10 employees at the Central Site location
- Employed high speed routers for 67 counties on 180 servers and 2200 clients
- Implement statewide networking of 34 AS/400's supporting 534 District Justice Offices

Education

Harrisburg Area Community College - Computer Science
Certified Ethical Hacker & Countermeasure Department of Defense training
Hewlett Packard - HP-UX System & Network Administration
CheckPoint Firewall configuration and implementation
FBI Cyber Forensic Investigation course
IBM - Network Tuning/Problem Determination
Sun java system: Identity Manager 5.0, Access Manager 5.0, Directory Services 5.x

Certifications

Top Secret
Certified Information Systems Security Professional (CISSP)
Microsoft Certified Systems Engineer (MCSE+I)

UNISYS

Resource 85

Security Analyst

Key Skills and Knowledge

- CCNP
- CCNP Security
- ITIL v3 Foundation
- HP OpenView, Remedy Administration
- Veritas NetBackup, EMML for Fujitsu 9600 Phone Systems
- Orion, Retina, CheckPoint, Cisco Mars, Cisco Security Manager,
- DS/IPS, ASA, Omnipeek, WireShark
- FWSM, ACE
- Cisco 2600 routers, Cisco 2900, 3500, 3700, 6500 switches
- Cisco Nexus 7000/5000/2000

Professional Summary

12 years of experience delivering network engineering, desktop support, systems analysis, and data recovery. Skillful with HP OpenView, Remedy Administration and development, Veritas NetBackup, EMML for Fujitsu 9600 Phone Systems, Orion, Retina, CheckPoint, Cisco Mars, Cisco Security Manager, IDS/IPS, ASA, Omnipeek, WireShark, FWSM, ACE, Cisco 2600 routers, Cisco 2900/3500/3700/6500 switches, Cisco Nexus 7000/5000/2000

Employment History and Related Experience

Unisys Corporation, Network Design Engineer Harrisburg, PA, 2009 –Present

Integral team member providing 24x7 end-user and infrastructure (network and routing) support to state customer base on LAN

- Proactive monitoring and management of routers, switches, and infrastructure connectivity
- Cable, rack and configure Cisco devices using technologies such as HSRP, VSS, VRF, and VPC
- Responsible for incident management and problem resolution of client related issues
- Implement IOS upgrades
- Independently responsible for managing retina vulnerability scanning and reporting
- Make administrative changes to the phone system including: re-route numbers, change names, add features, connect/disconnect, etc.

Unisys Corporation, Desktop Support, Harrisburg PA, 2007-2009

Provided Computer Desktop Support for equipment assigned to employees located at local Unisys Sites

- Responsible for purchasing all technology related equipment to support the project.
- Migrated network and telephone systems for an office move

Unisys Corporation, Systems Analyst, Harrisburg PA, 2006 – 2007

Served as first point of contact for all server and mainframe issues, resolving issues on first call

- Managed nightly backups for all agencies
- Implemented patch updates and minor system upgrades locally and via BigFix
- Created performance reports and reviewed vulnerability scans

UNISYS

Resource 85

Security Analyst

Plexus Scientific, Network Engineer, Columbia, MD, 2005 - 2006

Installing equipment needed for research and development

R and R Networks, Inc., Tier 1 Technical Support, Dillsburg, PA, 2005 - 2005

On location repair of computers, servers, and network equipment

- Assist coworkers with server and network installations and Migrations
- Remote support via Netmeeting, Remote Desktop, and Terminal Services
- Recommend software and hardware to suit the customer's needs

Unisys Corporation, Computer Operator 2, Harrisburg, PA, 2001 – 2005

Supported 24/7/365 environment as essential personnel for the Pennsylvania Data PowerHouse Project monitoring mission-critical mainframes and servers

- Operate and monitor Unisys 2200, Unisys A Series, Unisys CS7800, HP OpenView, and Dell Servers for CPU Utilization, hung services, and failed jobs
- Remedy Ticket entry, status updates, procedure implementation, testing of Disaster recovery procedures, repair, troubleshoot, or assist with repair of desktop computers

American Personnel, Data Recovery Engineer, Camp Hill, PA, 2000 – 2001

Supported 24/7/365 environment as essential personnel for the Pennsylvania Data PowerHouse.

- Pulling, mounting, and filing of data cartridges.
- Logging, tracking, recording, and researching data coming and going.
- Working with Unisys 2200 and Unisys A series hardware and media
- Authored written procedures for several departmental functions and unique processes.

Education

Cumberland Valley High School, Mechanicsburg, Pennsylvania, 1996

Certifications

- 2012: ITIL v3 Foundations, 2012
- 2010: CCNP – Security, 2010
- 2009: CCNP, 2009
- 2007: AR System 6.X: Administering Parts I, II, III, 2007
- 2006: Microsoft Certified Professional, 2006

UNISYS

Resource 85

Security Analyst

- 2005: CompTIA Network+ Certification, 2005
- 2004: CompTIA A+ Certification, 2004

Dell Inspiron Foundation 2003, 2004
Dell Latitude Foundation 2003, 2004
Dell Inspiron 1100/5100, 2004
Dell Inspiron 4200/Latitude D600, 2004
CompTIA Server+ Certification, 2004

This page intentionally left blank.

UNISYS

Resource 22

Security Analyst

Key Skills and Knowledge

- Routing
- Switching
- Firewalls
- IPS Devices
- SolarWinds Orion
- Cisco Security Manager
- CheckPoint SmartCenter
- Catalyst 6500 VSS
- Cisco Application Control Engine
- IBM Proventia
- McAfee Network Security Platform Intrusion Prevention systems
- Cisco's Pricing Tool and Dynamic Configuration Tool
- Cisco's CSM, ANM and MARS management tools
- Data center redesign to reduce footprint and leverage virtualization technologies
- Configure and troubleshooting SolarWinds Orion Network Performance Monitor and eEye Retina products
- Deliver product recommendation and parts specification to upper management and customers
- Configured Cisco wireless access points for office user connectivity

Professional Summary

Cisco Certified Network/Design Professional with five years of experience designing, configuring, and troubleshooting both Cisco and CheckPoint solutions. Able to perform as a key contributor in a team oriented environment through diverse technical background. Well-spoken with expertise to effectively communicate ideas and recommendations to facilitate positive change.

Employment History and Related Experience

Unisys, Network Design Engineer, 2007 – Present

Provided network engineering for Commonwealth systems. Implemented Cisco VSS to maximize overall network uptime to 99.999% Utilized VRFs to leverage common infrastructure for multiple customers with stringent security requirements. Experience implementing and managing firewall rule bases on CheckPoint and Cisco platforms as well as building checkpoint SPLAT/IPSO boxes from scratch

- Able to manage and support Cisco Application Control Engine appliances
- Enterprise class devices include Cisco's Nexus, 6500, 4500 series switches and 3800 series routers
- Utilize 10Gbps technologies to reduce port density and overall solution costs
- Designed and managed structured cabling project to update site to data center compliancy standards
- Experience managing and configuring IBM Proventia as well as McAfee Network Security Platform Intrusion Prevention systems
- Proficient with Cisco's CSM, ANM and MARS management tools
- Contributed towards data center redesign to reduce footprint and leverage virtualization technologies
- Experience configuring and troubleshooting SolarWinds Orion Network Performance Monitor and eEye Retina products
- Key contributor to providing product recommendation and parts specification to upper management and customers
- Experienced using Cisco's Pricing Tool and Dynamic Configuration Tool
- Configured Cisco wireless access points for office user connectivity

Rite Aid Corporation, Merchandise Coordinator, 2004-2007

Support business operations creating store distributions for seasonal item process so that each store has the appropriate inventory levels to maximize sales at the beginning of each event

- Review individual store allocations for seasonal item process to ensure the accuracy of information

UNISYS

Resource 22

Security Analyst

- Create exception reports for management's review; make changes to report items as a result of management's review
- Coordinate and monitor the distribution of seasonal item merchandise from the warehouse to the stores to ensure timely receipt of product prior to the start of each event
- Prepare preliminary reviews of item allocation for use by department Managers
- Interact with store personnel regarding inventory discrepancy issues; correct errors that occur

Circuit City, Network Advisor, 2002 – 2004

Responsible for designing and installing computer systems, networking components and related products

- Went to customers residences and installed/configured networking components for proper connectivity
- Sold and installed hardware devices, peripherals and Software
- Consistently exceeded sales quotas for product and service upgrades
- Lead staff associate in technical knowledge of hardware devices, networking, peripherals, and software

NetComm Solutions, Inc., Lead Support Technician, 2000 – 2002

Delivered troubleshooting, installing, and configuring equipment for government contracts; performed as a group leader for the state-wide thin client rollout for the Administration of PA Courts

- Installed Cisco 1720 Routers with U.S. Robotics 56K dial backup modems and Cisco 2900XL switches in each District Justice Court House
- Extensive work troubleshooting Compaq's complete line of desktop and server products
- Responsible for providing technical support to the PA State House of Representatives, Democratic Caucus
- Experience installing, configuring, and administering Microsoft Terminal Services and Citrix MetaFrame XP
- Responsible for instructing new technicians on configuring and implementing thin clients, desktops and servers
- Help desk work involved with interacting and supporting users from large accounts such as the PA State House of Representatives, Democratic Caucus and the Administration of PA Courts

UNISYS

Resource 22

Security Analyst

Education

McAfee Network Security Platform Administration Training – McAfee Education (June 2012)

- Deploy McAfee NSP
- Building Policy
- Manage and Administer NSP to defend against attacks

CCSA Training – Fishnet Security (January 2012)

- Secure communications across the internet
- Defend against network threats
- Configure security policies
- Protect e-mail and messaging content
- Manage user access to corporate LANs

Cisco ACE Bootcamp – Firefly (November 2011)

- Installing, Configuring and Troubleshooting Cisco Application Control Engine
- Design and configure integration of the ACE into the network topology
- Design and configure multiple ACE contexts to virtualize network services
- Manage allocation of resources to virtual contexts
- Use the Cisco Modular Policy CLI to configure ACE features
- Configure IP application-based security
- Configure Layer 4-7 load balancing
- Configure health monitoring
- Configure Layer 7 protocol processing options
- Configure SSL protocol processing
- Configure the Web application acceleration features on the ACE appliance
- Configure the ACE module or appliance for high availability

Cisco Certified Security Professional – CCBOOTCAMP (September 2010)

- 642-504 Securing Networks with Cisco Routers and Switches (SNRS)
- 642-524 Securing Networks with ASA Foundation (SNAF)
- 642-515 Securing Networks with ASA Advanced (SNAA)
- 642-533 Implementing Cisco Intrusion Prevention System (IPS)

Cisco Certified Network Professional – CCBOOTCAMP (January 2009)

- 652-901 Building Scalable Cisco Internetworks (BSCI)
- 642-812 Building Converged Cisco Multilayer Switched Networks (BCMSN)
- 642-825 Implementing Secure Converged Wide Area Networks (ISCW)

UNISYS

Resource 22

Security Analyst

- 642-845 Optimizing Converged Cisco Networks (ONT)

Microsystems Technology – CLN (May 2000)

- Implementing and troubleshooting network technologies, Microsoft Windows NT Server, Windows 2000 Server, and cabling in a lab environment
- Working with services such as DNS, WINS, and DHCP
- Configuring and using the advanced features of Microsoft's suite of Office applications

Certifications

- Cisco Certified Network Professional (January 2009)
- Cisco Certified Design Professional (June 2009)
- Cisco Certified Security Professional (September 2010)
- Cisco Web Security Field Engineer Specialist (February 2011)
- Microsoft Certified Professional

UNISYS

Security Architect

This page intentionally left blank.

UNISYS

Resource 80

Security Architect

Key Skills and Knowledge

- Certified Information Systems Manager (CISM)
- Certified Information Systems Auditor (CISA)
- Certified Business Continuity Professional (CBCP)
- ITIL v3 Foundations Certified
- Experience with COBIT, ITIL, FISMA, FBI, CJIS, NIST, IRS, SSAE16, PCI, HIPAA, ISO 27000 & 20000 Audit Standards

Hardware Experience

- Intel and RISC-based servers, IBM z-Series, i-Series, p-Series and x-Series; EMC, XIV, Avamar and Data Domain storage platforms, Cisco routers/switches; CheckPoint & Cisco Firewalls

Software Experience

- LDRPS and BIA Professional planning software, Microsoft operating system, VMware, Retina, Qualys, RSA enVision and AA, SCOM, Cisco MARS & IDSM, BladeLogic and

Professional Summary

15 years of engineering and technology leadership for global enterprises, regional consulting firms, and state governments. Strong advocate of ISO 27001 & 20000 certification processes. Alwasy ensures IT security and business continuity contractual obligations are met, leads all internal and external audits related to various state, federal & industry standards (SSAE16/SAS70, CJIS, IRS & FISMA), and consulting with cross-functional Unisys and Commonwealth of Pennsylvania agencies on how to properly apply risk mitigation techniques in support of protecting IT assets.

- Managed up to twelve direct reports at one time as well as directed cross-functional teams on multiple, simultaneous security and continuity projects
- Trusted advisor to CIO, VP and other upper management roles in support of high priority initiatives affecting organizational reputation as well as the confidentiality, integrity and availability of valued IT assets

Employment History and Related Experience

Unisys, Project Security & Continuity Manager– Commonwealth of Pennsylvania DPH, Harrisburg, PA, 2009 to Present

Delivers proper audit and compliance methods are applied to the infrastructure managed by Unisys for the Commonwealth of Pennsylvania (Commonwealth of Pennsylvania) Data PowerHouse contract.

- Leading the ISO 27001 & 20000 certification processes, ensuring IT security and business continuity contractual obligations are met
- Leads all internal and oversees external audits related to various state, federal & industry standards including SSAE16/SAS70, CJIS, IRS & FISMA
- Consults with cross-functional Unisys and Commonwealth of Pennsylvania agencies on how to properly apply risk mitigation techniques in support of protecting IT assets.
- Managed end to end disaster recovery tests for Bureau of Integrated Enterprise Systems (IES) and Department of Revenue (DOR) AIX/SAP platforms as well as other Wintel/VMware platforms for various agencies (DOH, PSP, DPW) in the Commonwealth of Pennsylvania Data PowerHouse.

AOPC, IT Systems Security Officer, Mechanicsburg, PA, 2008 to 2009

Responsible for the design, development, oversight and coordination of information security and business continuity related activities for the Administrative Office of the Pennsylvania Courts.

- Creation of information security policies, development of risk assessments for executive review

UNISYS

Resource 80

Security Architect

various PC forensic tools

- Generation of application security reviews, firewall and network change management reviews
- Assurance of proper risk mitigation methods in support of the protection of data stored in the Unified Judicial System for the Commonwealth of Pennsylvania

Penn National Gaming, Inc Corporate, IT Risk Manager., Wyomissing, PA, 2006 to 2008

Delivered design, development, oversight and coordination of information security and business continuity related activities for a 17-property, $3B casino gaming firm.

- Created of security policies, standards, architecture and risk assessments ensuring the security and integrity of the company's networks and databases
- Business continuity and IT recovery strategy amongst all properties and applications
- Coordination of IT compliance associated with PCI, Sarbanes-Oxley and HIPPA (self-insured employer) standards and regulations in conjunction with senior management and internal audit staff.

Other Employment History

- Principal Consultant/Owner for Ethix Consulting, LLC, Harrisburg, PA, 2005 to 2006
- Practice Director for Anexinet Corporation, Philadelphia, PA, 2000 to 2004
- Senior Consultant for Actium (now Idea Integration), Conshohocken, PA, 1996 to 2000
- Systems Administrator for Lehigh Press, Cherry Hill, NJ, 1995 to 1996
- Technology Specialist for Good Samaritan Hospital, Lebanon, PA, 994 to1995
- IT Manager for GemChem, Inc., Lancaster, PA, 1993 to 1994
- Systems Analyst (Intern) for Medical College of Pennsylvania, Philadelphia, PA, 1992 to 1993

Education

- BS, Management Information Systems: Saint Joseph's University, Philadelphia, PA, 1993

Certifications

- CISM, CISA, CBCP, ITIL, currently pursuing CISS

UNISYS

Resource 86

Security Architect

Key Skills and Knowledge

- Security Consultant
- Security Architect
- Project Management
- Cisco Networking
- Data Loss Protection
- Network Access Control
- Virtual Private Networking

Professional Summary

Currently serves as an IBM Certified Consultant in the Centralized Security Practice of IBM Global Services. Has 26 years of experience at IBM US and IBM France, working in various positions as Network Consultant, Security Consultant, System Test Lead, Project Manager, Software and Hardware Developer. Has a proven track record in IT Security that can be attributed to his very broad technical skills in networking and security, his project management experience, and also to his ability to handle architecture, design, implementation as well as troubleshooting work.

Has recently focused on two critical domains in the security spectrum: Network Access Control, and Data Loss Prevention. They are fundamental security components to properly address the current and future threats.

Holds a Cisco CCNP and a CISSP certification. He also holds a Nortel Network Optical Design certification, and a Cisco VPN certification.

Employment History and Related Experience

IBM Security Practice - ISS, Consultant, Raleigh, North Carolina, 2004–To Date

Managing Security Consultant

IBM Global Services, Certified Network Consultant, Raleigh, North Carolina, 2000–2004

Senior Network Consultant

Technical Lead for Nortel Practice (Data)

IBM Software Group, System Test Supervisor, Raleigh, North Carolina, 1996–2000

In charge of a team of up to 20 test Engineers for the validation of IBM software products (IBM Firewall, Tivoli Policy director, TCP/IP utilities for Windows and operating system/2)

IBM France, Software Developer, La Gaude, France, 1985–1996

Team lead software developer

Hardware developer

UNISYS

IBM

Resource 86

Security Architect

Assignment History

Credit Report Company, ISS Consultant, 2011–To Date

The engagement consisted in assessing the maturity level of data security, identifying gaps and recommending tactical and strategic security initiatives.

- The engagement included a detailed evaluation of sensitive data in motion and at rest using data loss protection solutions.
- The final presentation to the executive committee proposed short term and far reaching strategic decisions that were very positively received by the executives and VPs.

Beverage company, ISS Consultant, 2011–To Date

Data Security Assessment of the worldwide server infrastructure (Over 600 servers) of the company. The results of the assessment lead to recommend the implementing a Data Loss Protection program to address tactically and strategically to the excessive exposure of sensitive data.

Major Hospital Group, Trusted Advisor - Security Architect and Lead deployment Engineer, 2009–To Date

With HIPAA getting more teeth in 2010, this large hospital decided to deploy and enforce encryption on all mobile workstations. Was the lead architect for a Data Loss Protection initiative at Duke.

Products used include PGP Universal Server, Lumension End Point Media control, Fidelis extrusion protection solution.

State Government, ISS Consultant, 2009

This State Government outsourced its entire IT infrastructure to IBM in 2008. One of the numerous challenges was the understanding of the traffic flows from 12 different agencies over 1000 firewalls.

- Researched, recommended and used the best technology available to perform the security mapping of the infrastructure.
- Ensured the project, completed on schedule and within budget provided additional side benefits specifically the detection of vulnerabilities and misconfigurations.

Large Northeastern University, ISS Consultant, 2009

Interviewed over 40 people at the University to assess security in the administrative and academic units in the following areas:

- Security policy
- Organization of information security

- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development and maintenance
- Information security incident management
- Business continuity management
- Compliance with PCI, FERPA, and HIPAA

A detailed report describing the issues found, recommendations and a multi-year roadmap was delivered to the CIO. The university started implementing the suggested remediation described in the report to raise their level of security.

Mid-Size Insurance Company, Trusted Advisor, 2007–2008

Tasked to assess the Internet security and to provide recommendations for a NAC solution at a mid-size insurance company. After presenting the assessment results, the Senior Executive for IT and operations extended Mr. Henrion for 10 months and asked him to define the security and infrastructure priorities, to recommend resources and to lead the execution of over twenty initiatives. Some initiatives lead to:

- cost saving (Telco cost trimming, deferred or cancellation of questionable investments)
- increased productivity, (defining and enforcing IT policies such as Internet access)
- security improvement through a company-wide deployment of a NAC (Network Access Control) solution.
- drastic reduction for potential exposure of Personally Identifiable Information.
- improved quality (Implementation of additional formal processes).

These projects accomplished the goal of closing very significant security gaps. (At the beginning of the engagement, only 2 out of 12 PCI criteria were met, a performance lower than the retail company who suffered the largest break-in in history).

Office Management Company, Security Subject Matter Expert, 2007

Architected and implemented the US security policy for the voip/data converged network. It involved hundreds of IOS routers, Cisco ASA or Check Point firewalls, as well as centralized access control.

UNISYS

IBM

Resource 86

Security Architect

Fortune 10 company in Health Care, Security Subject Matter Expert , 2006–2006

The focus of the engagement was on Network Access Control and on defining a worldwide strategy for the 220 sites and 5 main divisions. Participated in the development of security requirements, product pre-selection, and lab evaluation of several NAC approaches at this large pharmaceutical company. Some of challenges pertained to the unique requirements of bio-medical devices, or nontraditional Microsoft workstations such as mobile devices, voice over IP phones or security systems.

An in-depth analysis of the Vernier Network, Symantec and McAfee solutions in the customer network was performed.

County Government, Security Expert, 2005

Digital Video Surveillance originating from devices mounted on vehicles is transferred to a central location. Responsible for securing the whole infrastructure.

Contracting for Center of Medicaid and Medicare, PM, Security Expert, 2004–To Date

Architected, deployed and maintained a distributed firewall solution for one of the largest federal government agency spanning over the 50 American states and serving over 200,000 users. Had also project management responsibilities, handled contractors including a group that provided 24 x 7 network monitoring. This has been a very successful engagement from a customer satisfaction and financial performance perspective.

Mid Size Financial Institution, Consultant, 2002–2003

In another project for a mid-size financial institution, recommended network security and remote access and has allowed this company to decrease its telecommunication costs and retain its largest own customer after they had expressed concerns about the potential vulnerability of their network.

Major Contract Manufacturing Company, Technical Lead, 2001–2002

Architected, designed and implemented VPN and network solutions for various customers in the manufacturing, insurance, automotive and life science segments. For this large project, was the technical lead of a complex remote access project spanning over 4 continents for 60,000 end users.

State Insurance Company, Technical Lead, 2001–2002

A large insurance company accepted IBM's recommendations to move their remote access to the Internet and asked IBM to lead the project. It ended up saving the company over $5 million yearly in telecommunication costs for a ROI of about 3 months. Assumed the role of the technical leader in this project which was delivered on schedule.

UNISYS

IBM

Resource 86

Security Architect

Biomedical Equipment Manufacturer, Team Lead, 2000

This manufacturer of biomedical equipment was concerned about the remote access costs and security to its network.

- Proposed a couple of options to address these issues. The client chose to go with the more secure certificate based VPN solution and still ended up saving tens of thousands of dollars every year.

Education

Qualifications

- Master degree in Electrical and Computer Engineering
  University of Michigan, US
- Master in Electrical Engineering
  Polytechnic Institute of Grenoble, France

Languages

- English – (Fluent)
- French – (Fluent)
- German – (Good)

Certifications

- PGP encryption Boot Camp
- Verdasys Digital Guardian Boot Camp
- Forescout Technology CounterAct Boot Camp
- CISSP training
- 20 critical security controls
- Symantec Data Loss Protection

Membership in professional Organizations

- ISC2 (Member)

This page intentionally left blank.

UNISYS

IBM

Resource 87

Senior Security Consultant

Key Skills and Knowledge

- Penetration Testing (physical, network, application, wireless)
- Application Assessments
- Ethical Hacking
- Social Engineering
- Vulnerability Assessments
- Security Remediation
- Network Architecture Reviews
- Payment Card Industry Payment Application Assessments
- Payment Card Industry Assessments

Professional Summary

Currently a Senior Security Consultant for IBM Security Services (East Region). Perform penetration testing and vulnerability assessments for internal and external customers, including wireless, host and vendor applications, Web, and custom application testing. Provide security consulting services including network architecture reviews, security policies/controls reviews, and social engineering. Perform PCI audits, including final audits, gap analyses, and payment application assessments as a PCI Qualified Security Assessor (PCI-QSA) and PCI Payment Application Qualified Security Assessor (PA-QSA). Has 12 years experience in Information Technology at IBM, including 9 years as an Ethical Hacker and Security Consultant. Expertise is in penetration testing (wireless, network, and Web application), vulnerability assessments and recommendations, and intrusion detection and analysis. Discovered several "zero-day" vulnerabilities during the course of various assessments.

Employment History and Related Experience

IBM Security Services, Senior Security Consultant, Florence, Alabama, 2004–To Date

Conducted physical security assessments for both physical and logical security locations/devices and developed remediation plans based on findings. Performed numerous internal, external, and wireless penetration tests and prepared detailed reports of results, including recommendations based on findings. Discovered several "zero-day" vulnerabilities across multiple penetration tests and application assessments.

- Provided security consulting and recommendations on internal and external intrusion attempts.
- Conducted detailed network and security architecture reviews with recommendations based on industry accepted best practices.
- Performed numerous Web application tests for internal and external facing Web applications.
- Prepared detailed reports of vulnerability assessments and Web application test results.
- Discovered and provided recommendations for several serious vulnerabilities in customer Web applications.
- Performed incident response/analysis for approximately 60 worldwide Windows domain controller servers.
- Provided customers with PCI audit consulting to help customers better understand the requirements of the Payment Card Industry Data Security Standards.
- Conducted numerous PCI audits, to include final audits and gap analyses.

Resource 87

Senior Security Consultant

- Provided security advice and expertise on any new technologies that are being considered for customer environments.
- Worked with all levels of the management team to ensure everyone is kept abreast of the latest security information.

IBM Global Services, Distributed Operations Team Lead, Boulder, Colorado, 2002–2004

Provided leadership and direction to a 30 person team, which provides a varied set of services in support of multi-vendor, multi-protocol complex, network/systems environments including NT, Windows, UNIX, MVS, and MVS production control.

- Interfaced with customer, vendor, and/or internal senior management and possess discernment and judgment necessary to make mission critical decisions relative to network/systems support, problem resolution, and escalation.
- Participated in defining best practices, recommend process improvements, and set direction based on customer requirements.
- Assessed and analyzed complex customer or service requirements including planning, designing, and implementing support solutions with high visibility and direct impact to customer satisfaction.

IBM Global Services, Global Situation Manager, Boulder, Colorado, 2001–2002

Managed problem determination/troubleshooting procedures, problem/outage coordination, and escalation procedures for approximately 5,000 devices located worldwide, including Windows 2000, NT, UNIX, and Microsoft Exchange servers and various Cisco LAN/WAN equipment to include switches, routers, and hubs.

- Monitored and evaluated service call volumes/requirements, set priorities, and made decisions regarding the deployment of available resources and the initiation of emergency callouts of service personnel to meet service delivery requirements.
- Managed alerts, critical situations, and escalations and took action as required to ensure application of appropriate IBM resources, resolution/escalation of parts procurement issues, communication with customer management, and notification of management.
- Provided management support, assistance, and work direction to Systems Services Representatives and Customer Engineers as necessary to coordinate service delivery for entitled customer service requests.

UNISYS

IBM

Resource 87

Senior Security Consultant

IBM Global Services, Systems Management Professional, Boulder, Colorado, 2000–2001

Provided services to install, operate, and maintain complex centralized and/or distributed computer systems in a multi-vendor operating environment, including designing, implementing, and coordinating solutions to ensure acceptable performance levels with proven and advanced systems technologies.

- Performed problem determination and monitoring for IBM Global Services systems on various platforms including AIX, UNIX, and NT.
- Provided Level 1 and Level 2 problem determination and support for internal server systems and applications.
- Maintained a high level of accountability for quick determination of outages.
- Interacted daily with various levels of management, project managers, and support personnel.

Education

BS in Computer Science, University of North Alabama

BS in Mathematics, University of North Alabama

BS in Computer Information Systems, University of North Alabama

Certifications

- Certified Ethical Hacker (CEH)
- Payment Card Industry Council - Payment Applications Qualified Security Assessor (PCI PA-QSA)
- Payment Card Industry Council - Qualified Security Assessor (PCI-QSA)
- GIAC Certified Intrusion Analyst (GCIA)
- GIAC Cutting Edge Hacking Techniques (GHTQ)
- AirDefense Certified Engineer (ACE)
- Snort Sourcefire 3D System Training

Membership in Professional Organizations

- University of North Alabama Computer Science and Information Systems Industrial Advisory Committee – (Member)

This page intentionally left blank.

UNISYS

Resource 88

Security Architect

Security Clearance

- PSP Background Check

Languages

- English and Hindi

Key Skills and Knowledge

Domain Expertise & Solutions

- Access Control
- Active Directory
- ISA/TMG Server
- IIS
- CA SiteMinder
- BEA Aqualogic Portal
- Radiant Logic
- PKI

Network Security

- CSS – Cisco Content Switches
- VPN
- Cryptography

Databases

- SQL Server

Project and Program Management

- MS Project

Operating Systems

- Windows 2008/2003/2000

Professional Summary

Summary of Experience and Qualifications

Shobha is Manager for over 14 years of Systems Engineering and Networking experience with the last 7+ years in assessment and implementation of Applications, Servers and Security infrastructure. Microsoft Certified Systems Engineer in windows NT/2000/2003. Over 3 years experience in managing the team and client interaction In depth knowledge and hands of Experience on TCP/IP Networking, DNS and Name Services, Active Directory-Joining Domains COM+ Applications, IIS as Web server and its configuration, administration and troubleshooting. Wide Experience in Implementing high availability solutions using CSS (Cisco Content Switches), Microsoft Windows Clustering, NLB, and Application Center. Hands on experience in designing and implementing Web publishing solutions using MS ISA Server. Ensured network security corporate policies and "best practices" standards were followed during design, installation, and configuration of ISA firewall, NAT server, and Intranet, Extranet, and Internet connections. Project Management experience in gathering the requirements, analyzing and document the application requirements, design and prototyping the applications in an enterprise environment.

Professional Experience Include most recent first

Unisys/Office of Administration, State-PA 2004-Present

- Working as deployment manager/architect for the data center. Routine job responsibilities include- Design and provide solutions for integrating applications securely within the data center. Leading team of experts who are responsible for implementing application on the enterprise infrastructure. embers as per their expertise and provide technical as well as non technical assistance as and when required by the team members. Coordination and meeting with clients to discuss the application/infrastructure requirements for deploying applications at the hosting facility. Work with Clients and provides them solution to a problem and built positive client relationship
- Project - Disaster Recovery/Secondary Site for Data Center (BCDRP) – Shobha is working with team of experts and Management executives for establishing the secondary site for the enterprise data center. Her role is to provide suggestions relates to application designs for secondary site in conjunction with primary site.
- Project Single Sign On for Commonwealth Portal 2006 (Access Control) – Designed and implemented the SSO for commonwealth Portal be leveraging CA SiteMinder. Designed the solution to implement SSO among various implementations of SiteMinder at various agency locations. Leading team of experts for ongoing support like upgrade of the products throughout the enterprise.

UNISYS

Resource 88

Security Architect

- Project – User Provisioning for commonwealth of Pennsylvania (Access Control)– Shobha was the technical lead during the requirement, design and implementation phases for user provisioning project. IBM Tivoli manager product is leveraged to provide account management and user registration capabilities.
- Project – PSP CLEAN (Access Control) – Shobha assisted the project lead during the design phase of security component for CLEAN project. CLEAN is the system that is leveraged by many crime and justice related agencies. Leading the team of experts to provide ongoing support for the CLEAN security components like single sign on and virtual directory services
- Project – Penndot NDES (Cryptography) – Shobha was the lead and helped in designing the solution for certificate enrollment by network and handheld devices. The solution was designed using Public Key infrastructure components like network device enrollment services(NDES) and OCSP (online certificate status protocol)
- Project – VPN for Mobile users (Telecommunications and Network Security) – Shobha along with other experts helped in designing the VPN solution for Commonwealth mobile users to access internal applications. The solution leveraged Netmotion mobility servers and Radius servers for VPN services, PKI and Active directory for dual authentication.
- Other responsibilities – Shobha leads team of experts and work with many other groups and is involved in all security related projects and addresses various security concerns like data at rest and in transit, user registration, access management, network and infrastructure security.

CitiBank New York, Consultant 2003-2003

Responsible for installing, configuring and managing the windows 2000 Servers. Co-ordinate with application and business groups, implementation and performance tuning of the applications Including IIS based application. Implement backup servers and create/implement backup plans for servers .Install SQL servers and help DBAs troubleshooting System related problems. Create/Execute backup of SQL databases using SQL server backup. Troubleshooting tier-3/tier-4 windows 2000/nt server environment Implement Web Trends server for logging. Routine troubleshooting and system administration involving application teams, business groups and network group

Unisys/Department of Public Welfare Consultant 2001-2003

- Project – DPW Extranet (Network Security) - Responsible for installing, configuring and maintaining the Department's Extranet by leveraging ISA/Microsoft Proxy Services. Designed and implemented solution to publish secure applications to Internet using MS Internet Security and Acceleration Server/Proxy 2.0 and SSL. Implemented the solution for

UNISYS

Resource 88

Security Architect

publishing applications with confidential data using secure socket layer protocol involving co-ordination with application teams, network infrastructure people and with other offices to fully understand the architecture. Troubleshooting and managing tier-3 servers problems, LAN, WAN support management in a complex environment including co-ordination with outside vendors and application vendors like Verizon

- Other Responsibilities: Monitoring, optimization, administration and support and configuring security for all enterprise Web servers. Support for WINS and DNS servers. Administer Exchange 5.5 environment, troubleshooting e-mail flow problems in an enterprise environment including escalation of problems with other organizations and departments within the same organization. Help and assist co-workers understand the e-mail flow and hardware/software involved in the whole process. Assisted in design and plan for migration from exchange 5.5 to exchange 2000. Helped in troubleshooting issues involving application availability, Network inconsistencies, routine issues with user/account management and policies. Provided support for network infrastructure, publishing applications and their availability, troubleshooting procedures for network, e-mail, Web servers and Internet facing Firewall servers (ISA and proxy servers)
- Project -Active Directory Implementation (Access Control)- Designed and implemented Active Directory in an enterprise environment, including security policies, delegate administration to user as per their role User and group accounts management. Created the support document and trained the administrators to manage the active directory as per their role. Troubleshooting the issues related to active directory policies and authentication problems involving co-ordination with different departments.
- Developed and implemented NETIQ performance-monitoring procedures on windows 2000 enterprise servers. Performance monitoring procedures details the process of monitoring each individual server's health and send alerts in case one of the monitored resources become a bottleneck, modified the scripts as per the organization requirement, created reports for resource consumption as and when required. The servers monitored with NetIQ were windows 2000 servers serving the role of Web servers, application servers and database servers
- Application Center Implementation (Access Control) - Designed and executed the phased implementation of application center clusters to load balance the applications running on windows 2000 enterprise Web servers. Created the procedures for application deployment and trained the developers to help them understand the new environment. Troubleshooting the problems related to application deployment, network inconsistencies and application synchronization. Maintenance of the cluster by taking the node offline alternatively without affecting the end users

UNISYS

Resource 88

Security Architect

- Implemented unified security solution includes deployment and configuration of SiteMinder components on enterprise servers. Integrating Netegrity with Active directory for authentication and authorization of resources, configuring policy servers to for multiple active directories for authentication and for authorization of resources. Troubleshooting the problems with the slow response or unsuccessful authorizations for the application using the Netegrity for single sign on, DNS problems and network issues in an enterprise environment, escalating the problems with third party software/application vendors whenever required and worked as coordinator.
- Implementing a Windows NT/ 2000-based VPN solution to provide administrator's access to public Web servers for upgrades, monitoring and maintenance. Analyze complex network environment and resolve any security issues. Co-ordination with multiple offices and third party hardware/software vendors

NT Administrator / IBM, Arkansas 20000-2000

Designed and Implemented the NT Enterprise Network which comprised of NT4.0 Enterprise Version, Server, Cisco Routers, 3Com Switches, RAID5 Disk Arrays, and IBM Netfinity Server. Implemented the Backup Policy using DLT4000 Tape Drives and Backup Exec. NT administration and troubleshooting on Netfinity servers. Troubleshooting disk related problems and tape drive problems. Working with utilities to flash BIOS settings and change BIOS settings. Configuring the hardware RAID. Configuring Load Balancing on Network cards. Worked with Disaster recovery NT resource kit tools to modify with NT registry

Network Administrator, Northfield Savings Bank, NY
(Short Term) 2000-2000

Project Firewall Implementation (Network Security) - Studied Network Design to foresee the problems before configuring/implementing security policies. Analyzed, designed, implemented and configured various elements of the network right from switches, Cisco Routers to servers and application Software. Installed and configured NT Servers. Installed and Configured CheckPoint 4.1 (Firewall) on NT 4.0 servers. Configuration and integration of E-Safe content scanning server to work with CheckPoint 4.1. Created policies and rules to define security for the organization.

NT Administrator/Architect, Interactive
Communications Inc., 1999-2000

- Designed and reconfigured the network having multiple subnets for different departments of the company. Installed and Configured CheckPoint 4.1 (Firewall) on NT 4.0. Configuration and integration of E-

UNISYS

Resource 88

Security Architect

Safe content scanning server to scan for viruses with CheckPoint 4.1

- Creating policies and rules to define security for the organization. Implemented Internet Security using MS Proxy Server 2.0. Configured Exchange Server 5.0 including IMS. Implemented VPN using MS PPTP (Point to Point Tunneling Protocol) technology and RAS server technology. The data transfer is secured by enabling the MS CHAP Protocol and Data encryption at the server level and client level.
- Evaluated the Windows 2000 server (Beta) compatibility with existing devices and testing the product services and new features in testing environment. Created customized packages using custom installation tools and distributing those using Windows 2000 group policies. Upgrading from Windows NT server to Windows 2000. Configuring RIS (Remote Installation Server) to remotely install Windows 2000. Configured Terminal Servers in Windows 2000. Configured networking services like DHCP, DNS, etc.

NIIT Limited, India 1995-1999

Network administration for network. Comprises of Windows NT Servers, Novell NetWare 3.12 and SCO-UNIX. Administration of users & group accounts, security policies, print servers, Implement, administer and troubleshoot Exchange environment, configure mail clients, Performance tuning. Implemented migration from Novell to NT Support DNS/Wins/DHCP Study and design network Conducted training on Windows NT 3.51/4.0, Windows 95, UNIX, TCP/IP, SQL Server, MS Exchange Server, PowerBuilder for corporate clients, Unicenter TNG (Computer Associates).

Education Include High School or greater

Bachelor of Science, University of Delhi, India

Diploma in Systems Management (NIIT, India)

Professional Certification

- Windows MCSE 2003
- CA SiteMinder
- CISSP
- ITIL Foundation 3.0

Professional Development

- CISSP

This page intentionally left blank.

UNISYS

IBM

Resource 89

Security Architect

Key Skills and Knowledge

- Network Security
- Firewall
- Network and Host Assessment
- Vulnerability Scanning
- Penetration Testing
- Firewall Consulting and Implementation
- Firewall Migration Consulting and Implementation
- Network Segmentation Consulting and Implementation
- "UTM" Unified Threat Management Consulting and Implementation
- Intrusion Detection and Prevention Consulting and Implementation
- Network Access Control "NAC" Consulting and Implementation
- Secure Remote Access Consulting and Implementation
- IPSec VPN Consulting and Implementation
- SSL VPN Consulting and Implementation
- AAA Consulting and Implementation
- Network Security Operations & Management
- Security Information and Event Management Consulting and Implementation
- NA
- PN-MARS
- Juniper Netscreen
- Cisco PIX
- Cisco ASA
- Check Point Firewall NGX
- Cisco VPN Concentrator
- Cisco IDS
- Cisco IPS
- Cisco Clean Access
- Medical Grade Network
- PCI
- Cisco Wireless Network
- Cisco Routers
- Cisco Switches
- BlueCoat
- AlgoSec

Professional Summary

An Infrastructure Architect in IBM Security Services. Responsible for delivering a full security product and service portfolio as well as supporting sales, business development and internal projects. Joined IBM Global Services in 1998, working in Strategic Outsourcing. Led transition teams, global Network Security teams, projects and consulting engagements.

Employment History and Related Experience

IBM Security Services, Advisory IT Architect, US, 2006–To Date

Delivered engagements, developed best practices for delivery and supported sales and internal work.

IBM Global Services, IT Specialist, US, 2001–2006

Was in the technical delivery on the Firewall Team of the Network Security Services organization of IBM Global Services, Strategic Outsourcing. Initially took part in the Universal Server Farm team supporting Web Hosting customers, but eventually began supporting Strategic Outsourcing and Managed Security Services customer. This position proved to be valuable in learning the strategic value of technical leadership, delivery and operational excellence and innovation to improve overall performance and growth in existing accounts.

IBM Global Services, IT Specialist, US, 1998–2001

Joined IBM Global Services, working in Strategic Outsourcing, providing Help Desk and End User Support for large clients. Responsibilities eventually included leading teams to transition and consolidate Help Desks using IBM best practices and tools. This position proved to be valuable in learning the strategic value of metrics, intellectual capital and technology investments to improve customer service and deliver IBM's unique value to customers making IT investments.

Washington University School of Medicine, Research Assistant, US, 1994–1998

Technical experience providing statistical data collection using PC and Client-Server platforms. Technologies included Windows 95, Windows NT, Windows 2000, SAS and DOS.

Assignment History

Large School District, Network and Security Architect, 2011–2011

The customer needed to reduce IT security risks in their existing network environment. This required an assessment of their Security Environment, LAN, WAN and Wireless

- RedSeal

network environments. The customer also required high level conceptual design of their network.

As the Network and Security Architect, I identified issues in the existing environments and provided high level Network and Security designs.

Global Bank, Advisory IT Architect, 2010–2011

The customer required a cross discipline review and assessment of the physical and logical elements of the technology and process infrastructures supporting their online Banking environment.

- Identified issues in the environment that had the potential to impact the delivery of services through the infrastructure.
- Provided recommendations to correct identified issues and enhance the performance and availability of the large systems delivery infrastructure.

Global Bank, Advisory IT Architect, 2010

The customer required the IBM project team to review and assess their Secure Data Management (SDM) architecture that relates to the personally identifiable or sensitive information within their non-production environment. The assessment covered personally identifiable or sensitive information used within non-production environments where applications are developed. The environment included over 1000 applications in multiple data centers, covering 6 business lines, with approximately 350,000 customer profiles, using multiple platforms including UNIX, Wintel, and Mainframe.

- Documented personally identifiable or sensitive information in the non-production environment, existing data management practices including an analysis of data flows into and out of the non-production environment.
- Provided recommendations for appropriate methodologies to perform data obfuscation, mitigating security controls, and suggestions on the “Best Practices” use of the recommended tools.

Regional Insurance Company, Advisory IT Architect, 2010

The customer required an Information Security Assessment to evaluate their security posture. The assessment included an analysis of the architecture and risks in the existing environment and networks, analysis of the network and security device configurations and an analysis of the technical security controls.

- Provided an analysis of in place threat mitigation technologies and made recommendations to strengthen the current state.
- Recommended changes to the existing technologies and platforms to realize immediate value.

UNISYS

IBM

Resource 89

Security Architect

State Healthcare Agency, Advisory IT Architect, 2010

The large government agency customer required a data center migration of their existing processing environment.

- Assisted the customer by reviewing the customer's network design to verify that it was complete in terms of scope, requirements, and technical details.
- Provided initial gap analysis of the current environment and subsequently provided the network security conceptual, specified and detailed designs.
- Provided an implementation plan and led the deployment of the network security solution. The solution was based on Cisco and Juniper Security appliances and Cisco switches.

Global Automobile Manufacturer, Advisory IT Architect, 2009–2011

The customer required an automated and centralized compliance management service to audit their global firewall infrastructure.

- Architected the process and technical solution for pilot and deployment. The service analyzes, reports, and tracks firewall configurations and policies for compliance to customer firewall standards. This service integrates into the customer's existing Security Operations Center service provided by IBM.

Global Defense Contractor, Advisory IT Architect, 2009

The customer required a global IDS solution for worldwide infrastructure.

- Assisted the customer by configuring and deploying ISS Proventia devices.

Regional Power Company, IT Specialist, 2009

The customer required a complete network refresh, upgrade and support of an office move. The customer's environment and topology included a Primary Data Center, Disaster Recovery site and a new office building.

- Assisted the customer by reviewing the customer's network design to verify that it was complete in terms of scope, requirements, and technical details.
- Provided gap analysis and recommendations for the conceptual, specified and detailed design.
- Provided an implementation plan and assisted with deploying the network solution. The Cisco solution at the core included 6500 platform with FWSM, WAAS Acceleration, GSS, 3500 switches and ASA firewalls. The solution at the access and distribution included 6500 and 3500 switches.

IBM

Resource 89

Security Architect

International Travel and Tourism Customer, IT Specialist, 2009

The customer required a secure hosting environment. IBM provided a hosting solution based at an IBM data center.

- Deployed network security equipment including Cisco ASA Firewalls and Proventia IPS devices.

Large University, IT Specialist, 2009

A large university required a network refresh with a Medical Grade component for an affiliated research hospital.

- Provided Network Security reference architecture consulting and design for a large University and affiliated research hospital. The technologies included Cisco Clean Access Manager, Cisco Clean Access Server, Cisco ACS, Cisco Security Monitoring Analysis and Response System, Cisco Security Manager, Network Admission Control Framework, and Cisco IDS/IPS Architecture.

Large Retailer, IT Specialist, 2008

- Led an assessment of the organization's firewall architecture. This assessment of the current firewall architecture provided best practices-based recommendations for improving the current design, configuration(s) and performance of their firewall architecture.
- Delivered findings ranked by risk and operational, tactical and strategic recommendations in order to help the organization understand the security risks involved.

Large Healthcare Management Company, IT Specialist, 2008

- Supported BCRS application assessment of a large health care insurer.
- Provided data mining of the applications and systems in order to help the team understand the synchronization points of the environment.

National Bank, IT Specialist, 2008

Providing testing environment security assessment for a large bank, focusing on Security Management and network segmentation in a regulatory environment.

- Developed findings and recommendations for Security Management and network segmentation.

Large Regional Bank, IT Specialist, 2008–2009

Provided Network Security design review for large bank. Technologies include Cisco ASA Firewalls, Cisco CS-MARS and Cisco NAC.

Resource 89

Security Architect

- Developed Network Security strategy and recommendation for NAC Appliance deployment.
- Performed Design Review for Cisco NAC Deployment and provided workshop to discuss findings.

Large Federal Government Department, IT Specialist, 2008

Provided hardware and software upgrade and Security Consulting for Federal Agency. Technologies included Check Point and Check Point Secure Platform.

- Upgraded from Nortel Switch based firewall to HP hardware.
- Upgraded from Check Point version R55 to NGX R62.

Large City Agency, IT Specialist, 2008

Provided Security and encryption consulting for large city Public Safety Agency. Technologies include Microsoft Windows CE, Global Bay handhelds Check Point and Check Point Secure Platform.

- Provided encryption strategy and recommendation for handheld device secure login, encryption of data at rest and encryption of data in transit.
- Provided approach and strategy to meet business and functional requirements and to achieve compliance with electronic signature requirement.

National Retailer, IT Specialist, 2008

Provided Security Consulting and secure network segmentation reference architecture for a large retailer. Technologies included Check Point, Cisco Switches, Active Directory, Check Point Firewall and Cisco PIX Firewall.

- Responsible for Security Lead and Network design. Deliverables included secure Network Design to support strategic growth of company and supporting Security Process Guide based on ISO/IEC 27002:2005.

National Retailer, IT Specialist, 2007

Provided PCI remediation and Network Security consulting for a large retailer. Technologies included Active Directory, Check Point Firewall, Cisco PIX

- Provided consulting and support for Network Security team for PCI remediation. Activities included Cisco VPN Client Deployment for use with Two Factor (RSA) authentication, Check Point Management Server rebuilds and Deployment, Remote Site Firewall Infrastructure Deployment, Remote Site Firewall Infrastructure Deployment, and Mainframe and Teradata Segmentation.
- Developed a remote site deployment strategy.

- Developed a Network Security Devices Password Management Strategy and developed a Network Security Devices Inventory Management Strategy.

National Retailer, IT Specialist, 2007

Provided PCI remediation and Security consulting for a large retailer. Technologies included Active Directory, Check Point Firewall, Cisco PIX, and Cisco FWSM.

- Updated the company's security policy to comply with Payment Card Industry (PCI) Data Security Standard (DSS) requirements.
- Created Quarterly Rule Review Process of firewall and router rule sets is required to validate compliance with Payment Card Industry (PCI) Data Security Standard (DSS) requirements.
- Performed PCI rule identification and cleanup for customer firewalls. Created Firewall Standards document.

Global Hospitality Company, IT Specialist, 2007–2009

- Provided Network Security reference architecture consulting and design for a global hospitality company. Technologies included Active Directory, Cisco Clean Access Manager, Cisco Clean Access Server, Cisco ACS, ISS IDS/IPS Architecture, ISS Log Aggregator, Nomadix Access Gateway and Cisco ASA.

Global Advertising Agency, IT Specialist, 2006–2007

- Provided Network Security consulting, design, assessment and deployment for an advertising company. Technologies included Cisco Network Assessment Module, Cisco Clean Access Manager, Cisco Clean Access Server, Cisco ACS, Cisco Security Monitoring Analysis and Response System, Cisco Security Manager, Network Admission Control Framework, and Cisco IDS/IPS Architecture.

Global Shipping Company, IT Specialist, 2006

A global shipping company was required to separate and secured the wireless inventory device network from the production wireless and wired networks.

- Developed the reference architecture, project plans, deployment strategy and led the deployment.
- Managed both the project management and technical delivery for the North America rollout of 26 sites. Technologies included Cisco firewalls, Cisco switches, multiple wireless devices and Symbol handheld wireless devices.

IBM

Resource 89

Security Architect

Other job-related activities

- Provided support for RFP responses, B&P, business development, scoping and/or QA for the following opportunities:

  ACE Hardware, Atlanta Public Schools, Citigroup, Coca Cola, Diageo, Flint Group, GAP, Keybank, Manpower, Nationwide Insurance, Regence, Schneider, Telmex and US Cellular.

Education

Qualifications

- Masters in Information Resource Management
  Washington University School of Engineering and Applied Science, US
- Master of Arts in Human Resources Management
  Washington University, US
- Bachelor of Science in Hotel and Restaurant Management
  University of Missouri-Columbia, US

Languages

- English – Fluent
- French – Basic

Certifications

- Check Point Firewall
- Cisco ASA
- Juniper Netscreen Firewall
- Juniper Security Manager
- Solution Development

This page intentionally left blank.

UNISYS

Security Specialist

This page intentionally left blank.

UNISYS

INFO-MATRIX CORPORATION

Resource 90

Security Specialist

Key Skills and Knowledge

- Extensive knowledge of information security, including physical security and identity and access management concepts
- Assisted in implementation and administration of the Living Disaster Recovery Planning System (LDRPS) and the enterprisewide policy software tool called VPC.
- Assist in administering a security awareness program using e-mail alerts, training sessions, and the Enterprise Security Web page.
- Facilitated risk assessments by interviewing key business and technical staff, documenting the process, and following up with audit recommendations.
- Created and implemented an annual access review process using Microsoft Access to pull in multiple applications and generate a management report to validate access.
- Project manager for an implementation of SecurID implementation.

Professional Summary

15 years of security management primarily in a RACF environment. Skilled professional with extensive knowledge of information security, including physical security and identity and access management concepts. Manage the execution and use of security controls to protect data and for supervising the conduct of personnel in the protection of data. Build working relationships with internal staff and external clients to achieve results through others. Develop and implement information systems security policy, standards, and procedures for information processing systems. Evaluate security and analyze information systems to identify requirements, information workflows, and sound structures based on regulations and business needs.

- Develop and implement information security awareness programs
- Monitor security systems and analyze logs for violations, patterns, or incidents that require further investigation; provide the root cause and a plan of action documentation
- Provide technical advice to staff and management on information security issues
- Oversee the enterprisewide business continuity plan for the Pennsylvania Higher Education Assistance Agency; facilitated the annual exercise for 3 years
- Evaluate software, tools, and equipment for automating compliance and security administration
- Facilitated and administered a risk analysis program for Allfirst Bank
- Acquired extensive experience with PC applications such as Microsoft Word, Excel, Access, PowerPoint, Visio, and Adobe Acrobat Professional.

Employment History and Related Experience

Pennsylvania Higher Education Assistance Agency (PHEAA),
Identity & Access Manager, Harrisburg, PA 2004 – Present

Manage security for multiple systems, including RACF, Linux on zSeries, PeopleSoft, SalesLogix, SQL Server, and other application security systems. Develop and implement security policies based on NIST 800-53 Standards. Evaluate information security systems to assess effectiveness, monitor security performance and adequacy, and resolve security problems. Define and test new security monitoring processes, including audit requirements, exception reporting, and automatic incident notification.

- Administered and coordinated PHEAA's business continuity plan, risk assessments, and management of vendors and equipment at the hot site.
- Coordinated the annual exercise for PHEAA, which involved 75 business units and 10 IT departments, testing at 5 different sites, and working with 4 business recovery vendors.

- Assisted in implementation and administration of the Living Disaster Recovery Planning System (LDRPS) and the enterprisewide policy software tool called VPC.
- Assist in administering a security awareness program using e-mail alerts, training sessions, and the Enterprise Security Web page.
- Work with associates and external clients to assess their security needs, provide solutions, and resolve their problem, while striving for excellent customer service.

M&T Bank, Senior Security Analyst, Vice President,
Buffalo, NY 2003 – 2004

Defined and developed new security monitoring processes for the LAN and the mainframe, including audit requirements, exception reporting, and automatic incident notification. Researched the technical environment and worked with vendors to identify tools that can be used for monitoring. Worked with security administrators in defining and implementing security requirements.

- Administered the quarterly access and remote user activity review process, including the report creation, distribution, and tracking.
- Prepared metrics for management to track based trends (access request volumes).
- Configured the System Access Request system, which included automatic management, system administrator approvals, tracking requests, and management reports.

Allfist Bank, Senior Data Security Analyst, Vice President,
Baltimore, MD 1998 – 2003

- Created a Security Awareness Program for more than 5,000 employees, including quarterly newsletters, designing a Web-based training program, Web publishing, semiannual security administrator meetings, and an annual computer security week to evaluate the program's effectiveness.
- Managed security administration for the IBM mainframe (RACF), Tandem (SafeGuard), and remote access (SecurID) systems. Acquired experience with NT and UNIX/AIX security administration.
- Evaluated the security of application systems based on the data owner's business requirements and regulatory controls and implemented the proper controls.
- Designed and implemented an online access request form to address multiple platforms and systems, automating the manager/security administrator approval process and a tracking method.
- Managed all access control requests, including problem resolution, monitoring outstanding requests, table changes, documentation, end user training, and communications.

Security Specialist

- Facilitated risk assessments by interviewing key business and technical staff, documenting the process, and following up with audit recommendations.
- Created and implemented an annual access review process in Microsoft Access to pull in multiple applications and generate a management report to validate access.
- Project manager for an implementation of SecurID.
- Assisted in implementing policies and procedures, ensuring compliance with federal banking regulations such as the Gramm-Leach-Bliley Act.

Dauphin Deposit Bank (DDB), Data Security Manager,
Vice President, Harrisburg, PA 1988 – 1998

Oversaw the administration of data security for all platforms (RACF, NT, AIX, and operating system/2) and applications (CICS, SHAW, OFCS, and Genesys). Developed and implemented an access request system that included data ownership approvals. Implemented RACF security administrative and reporting tools, increasing productivity by 50 percent.

- Implemented and administered a SDLC tool (Librarian/CCF).
- Developed and presented information security training and awareness seminars.
- Assisted in installing, monitoring, and user training of McAfee antivirus software.
- Implemented, administered, and tested the contingency plan for the bank.

Farmers Bank & Trust Co., Data Processing Manager,
Hummelstown, PA 1883 – 1988

Managed all data processing functions to ensure production jobs were completed accurately and promptly. Managed various departments; Document Processing, Data Entry, Data Security, Computer Operations, and Technical Services.

Education and Training

- Computer Operations Certificate, Computer Learning Center, Camp Hill, PA (1983)
- B1000 Computer Operations Cert, Burroughs Education Center, King of Prussia, PA (1984)
- Intro to COBOL Programming, Penn State Capital Campus, Middletown, PA (1987)
- Effective RACF Administration Certificate, The Henderson Group, NJ (1989)
- MVS/ESA Security Topics, IBM Education Center, Chicago, IL (1992)
- NetWare System Administration, ADT (Knowledge Soft), Mechanicsburg, PA (1996)

Resource 90

Security Specialist

- Mastering Windows NT Security, The Henderson Group, Harrisburg, PA (1997)
- NOTES Domino Designer Fundamentals, Application Security and Workflow, Attronica, Gaithersburg, MD (2001)
- Advanced z/operating system Security, Raleigh, NC (2011)
- Other Software/Management Courses: Microsoft Office products, Managing/Leading for Success, Counsel and Develop Employees, Diversity Training, and LDRPS Administration training

UNISYS

Storage Management Administrator

This page intentionally left blank.

UNISYS

Resource 91

Storage Management Administrator

Key Skills and Knowledge

- SAP
- Oracle for DMX
- Symmetrix
- CLARiiON and HDS storage arrays
- Design, administration, and management of enterprise systems
- Storage systems and network infrastructure
- Documentation of management systems

Professional Summary

Specialize in EMC SAN, Hitachi SAN, HP SAN, IBM SAN, TSM, NetBackup, and CommVault technologies. Certified in EMC Technology Foundations (EMCPA). Deliver professional services and EMC integrated solutions for enterprise applications such as SAP and databases such as Oracle for DMX, Symmetrix, CLARiiON, and HDS storage arrays. 10 years of experience in the design, administration, and management of enterprise systems. Extensive experience with supporting storage systems, network infrastructure, and detailed documentation of management systems.

- Expertise in administration of information technology with a very specific emphasis on storage management and virtualization, network and system operations, system administration, and project management
- A results-oriented professional experienced in the analysis, design, implementation, and management of multifaceted projects, integrating varied technologies for maximum effect
- Worked with an EMC consulting team as an implementation specialist
- Worked with a Hitachi consulting team as an implementation specialist; acquired extensive knowledge of Hitachi SAN
- Worked with a IBM consulting team as an implementation specialist; acquired extensive knowledge of IBM SAN
- Strong management and leadership skills with the ability to motivate and maximize productivity
- Excellent communicator with an emphasis on building strong client relationships
- Experienced in information technology, operations management, account management, client services, organizational development, rollouts of new products, networking, process improvement, training, mentoring, international technology liaison, sales, marketing, and e-commerce initiatives
- An accomplished consultant with a deep understanding of technical implementations and business functions in Fortune 1000 companies across North America, Europe, the Middle East, Africa, and Asia Pacific regions.

Employment History and Related Experience

Unisys Corporation, SAN Administrator, Harrisburg, PA 2011 – Present

SAN administrator on the American Red Cross project as a member of the NAEC storage SAN team.

- As a backup SAN Administrator for the Commonwealth of Pennsylvania, assisted in upgrading Brocade switch code.
- Completed ITSM 7.6 change requests for storage allocation on EMC and IBM arrays.

EMC Residency Consultant, Dana, Maumee, OH 2011 – 2011

Supported change requests for storage allocation and reclaim requests for EMC

UNISYS

Resource 91

Storage Management Administrator

arrays. Participated on projects for migration from DMX-3 to VNX5300 arrays.

- Involved in VMAX for open systems and mainframes.
- Performed regular status check of SAN (EMC arrays and Cisco switches) and backups (Avamar, Datadomain,and Networker) environments in primary and disaster recovery sites
- Created and updated EMC documentation for primary and disaster recovery.

Other Employment and Consulting Experience

• Henry Ford Health System, Sr. SAN Engineer	2011 – 2011
• AdvizeX Technologies, LLC/EMC Services Practice	2011 – 2011
• Providence Health, PennDOT, SAN Administrator	2007 – 2011
• AdvizeX Technologies, LLC/EMC Services Practice	2006 – 2006
• EMC Services Practice, Advizex Technologies	2006 – 2007
• PASSHE, Systems Engineer	2005 – 2006
• Panasonic, Consultant	2005 – 2005
• Merck & Co, System Engineer	2004 – 2005
• Daimler Chrysler, Inc., Consultant	2003 – 2003
• Northwestern Mutual Inc., Consultant	2002 – 2003
• 3COM, Inc., Senior Engineer	2000 – 2002
• Motorola INC, Consultant	1999 – 1999
• Baxter Healthcare Corporation, Consultant	1996 – 1999

Education

- M.S., Computer Information Systems, Roosevelt University, Chicago, IL
- B.S., Electronics and Communication Engineering, Osmania University, Hyderabad, Andhra Pradesh, India,

.

Certifications

- Certificate of EMC Technology Foundations (EMCPA)
- Preparing for the ITIL v.3 certification exam

UNISYS

IBM

Resource 92

Storage Management Administrator

Key Skills and Knowledge

Software:

- DFDSS,
- DFSMS,
- DFHSM,
- DFP,
- IDCAMS,
- VSAM,
- TDMF,
- REXX,
- TSM
- Hardware:
- DS8000,
- TS7740 VTS,
- TS3584 ATL
- Additional experience
- Disaster Recovery,
- VM
- VSE

Professional Summary

Vast experience in Information Technology with skills ranging from a Systems Programmer to a Storage Management Specialist. Currently supporting the Commonwealth of Pennsylvania contract as a Systems Administrator: Mainframe Storage Manager. Significant experience in a zOS environment.

Employment History and Related Experience

IBM Corporation, Technical Services Professional, Harrisburg, Pennsylvania, 2001-To Date

As part of the IBM supporting the Commonwealth of Pennsylvania, I provide day to day support by performing maintenance and administrative duties for the SMS control data sets, allocation rules, and constructs. I provide evaluations, make recommendations, and control implementation of enhanced SMS features including, but not limited to hardware compression, stripping and extended addressability.

- Support hardware migrations and implementations DS8300, ATL/VTS.
- Provide evaluations, make recommendations, and control implementation of enhanced DFSMS features including, but not limited to hardware compression, stripping and extended addressability. Managed 16 Tbyte DASD environment, supporting hardware installation, replacement and removal.
- Provide required DASD capacity based on business forecasts and historical growth. Also established and maintained standards for appropriate allocation of DASD and tape storage media.
- Monitor and maintain volume pool utilization, and volume/data performance in accordance with Business Service Level agreements.
- Create and update user catalogs/aliases.
- Provide backup and support for offsite business resumption.
- Provide recommendations for VSAM tuning and optimizing.
- Review and approve application changes to ensure conformity to standards and availability of required resources.
- Coordinate and/or perform verification and testing of software upgrades and maintenance of the following products: DFSMS, DF HSM, DFRMM, DSF, and TSM/ADSM.

IBM Corporation, Storage Management Specialist, Martinsburg, West Virginia , 1999-2000

As part of an IRS Data Center Consolidation, evaluated and configured the Database Management System (DBMS) products to match user requirements with system capabilities. Determined the file organization, indexing methods, and security procedures for system databases.

Resource 92

Storage Management Administrator

- Participated in the Service Center (SC) site survey.
- Assisted the Lead Analyst with storage assessment of the IAP/ACS/PRINT (IAP) system, and with the SC data captures and restoration process.
- Provided support for the systems environments and works with the storage lead and assists System Software Development (SSD) through systems monitoring, tuning, analysis, and problem resolution as required.

Citigroup, Senior Resource Manager, Wilmington, Delaware, 1993-1999

Performed maintenance and administrative duties for the SMS control data sets, allocation rules, and constructs. Provided evaluations, recommendations, and control implementation of enhanced SMS features including, but not limited to hardware compression, stripping and extended addressability.

- Managed the 3.25 Tbyte DASD environment, supporting hardware installation, replacement and removal.
- Provided required DASD capacity based on business forecasts and historical growth. Also established and maintained standards for appropriate allocation of DASD and tape storage media.
- Monitored and maintained volume pool utilization, and volume/data performance in accordance with Business Service Level agreements.
- Created and updated user catalogs/aliases.
- Provided backup and support for offsite business resumption.
- Provided recommendations for VSAM tuning and optimizing.
- Reviewed and approved application changes to ensure conformity to standards and availability of required resources.
- Coordinated and/or performed verification and testing of software upgrades and maintenance of the following products: Catalog Solutions, DSF, and DFSMS.

User's Incorporated, Systems Programmer, Malvern, Pennsylvania, 1989-1993

Planned and implemented VM operating system upgrade to VM/ESA 1.1 from VM/SP Release 5, and the migration of product applications to the new operation system.

- Upgraded VM execs to conform to the new release, and trained operations, programmers and the user staff in the operation of the new system.
- Planned and implemented VSE operating system upgrade to VSE/SP 3.2.1 under VM/SP Release 5.
- Migrated online network to VTAM, NCP, performed network maintenance and upgrade, and provided technical support to the user community.

UNISYS

IBM

Resource 92

Storage Management Administrator

- Planned, installed and implemented systems and application software as required and managed DASD resources.

Education

Bachelor of Science in Biology, St Bernard College

Fluent in Spanish

This page intentionally left blank.

UNISYS

IBM

Resource 93

Storage Management Administrator

Key Skills and Knowledge

- SMS
- z/operating system
- HSM
- ABAR
- RMM
- DSS
- CLIST
- SAS
- REXX
- TSO/ISPF
- JCL
- COBOL
- ISMF
- MAINVIEW
- FDR/DSF
- Mainstar Suite
- TDMF
- LDMF
- CA1
- RACF
- ACF2
- GDPS
- PPRC
- Flash Copy
- FICON
- Cisco Switch
- PAV (Hyper PAV)
- MS Office Suite
- Word Perfect Suite
- Open Office
- Swish Max
- Adobe Suite
- CSS
- HTML/XHTML
- Coffee Cup Suite
- Kool Moves

Qualifications

- >170 SMS Conversions
- IBM Business Partner
- Educator to over 5,000 students in z/operating system & MVS topics
- Extensive knowledge of several OEM vendors software
- Handled several projects with savings > $1million

Professional Summary

Have over 36 years within the IT mainframe environment experiencing on different installations, processes and procedures while employed as an employee or consultant. Started as entry level computer operator and advanced into more challenging positions within operations and then into technical support with experience in database, DASD and tape support. installed and supported IBM and OEM vendor software. Have successfully handled many projects, some with millions of dollars in savings.

Employment History and Related Experience

IBM/RBS Citizens Application Resiliency Project, Storage Specialist / Architect, Global Technology Solutions Group, Evansville, Indiana, 2011–To Date

Provided application and infrastructure services in support of an end--to-end resiliency assessment performed on critical customer facing banking systems. Additionally, contributed to and worked on the overall team deliverable with the IBM EM.

IBM/WellPoint Data Center Consolidation Project, Storage Specialist / Architect, Global Technology Solutions Group, Evansville, Indiana, 2011–Current

Provided Mainframe Storage Technical direction and Architect services for the Wellpoint project, relocating the Staten Island data center to St. Louis for integration in a Sysplex. Responsible for assisting in the architect design & layout of the DSS8700 in St. Louis. A DSS8300 & DS87700 in Staten Island was to be merged into it. Responsible for the configuration of the DS87000 in St. Louis, and setting up PPRC-XD from the DS88300 & DS87000 in Staten Island to the DDS8700 in St. Louis.

- Performed several data replications and data syncs throughout the project (excess of 400TTB and 5, 0000 volumes) and also provided Storage Management functions to the testing (Bubble) environments in St. Louis du ring 3 testing cycles, a dry run cycle and the fin al cutover. These functions included VTS/Tape support, DFHSSM, DFSMS support, FTP of any required/missing data to the Test environments. Cleaned up the environments after each testing cycle and prepped them for the next replication process.
- Assisted with overall system customization and support utilizing my wide range knowledge.

UNISYS

IBM

Resource 93

Storage Management Administrator

Certifications

- MSCE, 1998
- TCE, (GTE) 1993
- NaSPA
- NCA
- CIC, (TechKnowledge) 1996

Knowledge Areas

- DBMS: IMS, CICS, & DB2
- Scheduling Systems
- Tape Mgmt Systems; CA, IBM, others
- DASD Mgmt Systems; IBM, CA, others
- Monitoring Systems: Candle, IBM, BMC, others
- Disaster Recovery: ABARS, Innovation, Mainstar , Mirroring Solutions (IBM, EMC, & HDS)
- Automation; IBM, BMC, CA
- Hardware: DASD (IBM, HDS, EMC) TAPE (IBM, HDS, EMC, Sun)
- Mainframes: IBM, Amdahl

References

- Provided on Request

Ford Motor Company, Storage COE Technical Advisor & Architect, Dearborn, Michigan, 2002–2008

Provided Technical direction and Technology strategies for the mainframe computing platforms at Ford Motor Company (domestic and international) locations. Helped develop and implement the Center of Excellence strategy for Enterprise Storage Management. Determined, evaluated and decided Hardware and Software solutions for the Mainframe offered by vendors.

- Served as Technical Advisor & Design Architect for a staff of 15 Storage Administrators who managed just shy of 1PPB of disk storage in addition to 5PB of tape storage.
- Provided Day to Day support in DFFHSM, DFSMMS, Tape, and Disaster Recovery Services. Process re-engineered all phases of storage manage and implement automation too reduce headcounts, on-calls, and optimize the storage environment.
- Created a Technical Services Taskforce to set direction for Ford data centers worldwide to implement bleeding edge technologies and to standardize processes & procedures enterprise -wide. Headed consolidation of several Ford subsidiaries data centers into the Dearborn mega centers.
- Chaired several key projects within IT that saved Ford in excess of $30+ million during my tenure, while providing excellent customer service.

Developed and implemented processes to change Disaster Recovery/Business Continuity from a batch ABARS process to a PPPRC Metro Mirroring process between the Dearborn mega centers. Headed multiple Storage refreshes that included replacing a vendor or upgrading technology. Storage vendor s during my tenure with Ford included (HDS, EMCC, and IBM). We were an IBM DS87700 & DS83000 environment when I departed Ford. Also headed Tape technology refreshes from (EMMC to IBM VTTS), and a IBMM VTS upgrade to the IBMM TS7700/TSAA3500 VTS solution looking to implement a Quad configuration, this DR standard was implemented at all worldwide data centers. Our mirroring was accomplished using PPRCC Metro Mirror, controlled by an IBM developed package at Ford, called PPRC Migration Manager.

- Developed and was Implemented the Global Standard Storage Management Environment at Ford across all data centers that would allow for any job to run on an y system, this meant implementing Parallel Sysplex and eventually going GGDPS, rewriting thousands of lines of code for standards for DDFSMS, DFHSSM, DFRMM, and RACF security.
- Migrated hundreds of PetaBytes of DASSD using TDMMF for Technology refreshes and migrations of data centers to the US. Also implemented an internal data transferring mechanism using TDMF to move vast amounts of data nightly among Ford's data centers.

Resource 93

Storage Management Administrator

- Was instrumental in getting the LDMF product developed and under IBM control. Handled Project Orange and Project Blue which was the separation of Visteon a Ford subsidiary that was sold and Project Blue was the integration of additional companies Ford purchased and wanted integrated.
- Handled the migration of data of Jaguar to its new owners, and the migration of the Mazda corporate data center from Irvine CCA, to Dearborn MI, utilizing PPRC Global Mirroring and TDMF Extended Distance over IP.

Enterprise Systems Consulting, Inc., President, CEO, Senior IT Consultant, Kendallville, Indiana, 1996–2002

Serving primarily as a Senior IT Consultant, provided Storage Management, Resource Management, Disaster Recovery, Security, and Automation in the Mainframe (MVS) arena. Provided solutions to many different client situations and also assisted with staff augmentation requirements. Partnered with several OEM Hardware/Software vendors (BMC Software, Mainstar Software, Innovation Data Processing, Softek, and IBM) and used their products in our solutions.

- Worked on a large project which was a DAASD Technology change, Disaster Recovery, and SMS implementation ((including HSSM, DSS, and RMM) for Bank Central Asia, (largest Bank in Asia headquartered in Jakarta, Indonesia). The BCA project lasted 2 years.
- Handled hundreds of smaller projects for Fortune 500 companies, including DFSSMS implementation, DDFHSM implementations & Health checks, DASD technology refreshes that encompassed configuration of the hardware and migration off data to it utilizing TDMF and data center consolidations and Disaster Recovery & Testing.
- Developed a 2-week Storage Management Boot camp class taught to over 2,800 students at TechKnowledge Corporation and is still being taught today.
- Developed/taught several courses and hands-on labs that covered topics in the MVS & z/OOS platform including, JESS, Catalogs, DASD, Performance & Tuning, Hardware, & Computer Operations for IBM Education Services, HDS Education, and TechKnowledge Corporation and other leading education suppliers.

Verizon Data Services, Senior Advisor y Systems Engineer, Temple Terrace, Florida, 1978–1996

Provided technical direction for Storage Management/Security at GGTE. Served as project lead for a Resource Management team with 28 direct reports.

- Managed a DASD environment in excess of 800TTB, 38 MVS images, 15 million tapes, within 4 mega data centers. Provided services for Mainframe and Open systems including Disaster Recovery.
- Served as consolidation manager, developed the data movement plans,

and performed the tasks to dump the data, fly via jet then restore the data.

- Responsible for consolidating 24 data centers into 4 mega centers, additionally successfully integrated CONNTEL and CITIZENS telephone company acquisitions. Developed a plan to integrate CONTEL and CITIZENS data into GTTE applications.
- Completed first successful SMS implementation in South America working at CANTV in Venezuela (a GTE subsidiary) and was featured in Computer World Magazine.

Retegeano Associates, Senior Technical Programmer, Erie, Pennsylvania, 1977-1978

Analyzed, designed, and coded COBOL and RPG programs to handle varied requirements for business applications as requested by clients. Worked on applications such as Order Entry, Accounts Payable, Accounts Receivable, Inventory, Credit Processing, Payroll and Taxes.

Greenleaf Corporation, Lead Programmer, Saegertown, Pennsylvania, 1977–1978

Analyzed, designed, and coded COBOL, RPPG, and Fort ran program s to handle office systems and manufacturing applications. Wrote Work In Progress, Taxes and Depreciation, Expediting, and Engineering applications. Served as Lead Computer Opera tor and trainer for Computer Operations' personal and was primary contact for any problems with computer systems.

Education

Computer Science, Associates of Science, ICM School of Business (Institute of Computer Management), Pittsburgh, Pennsylvania

Data Processing, Technical Certificate, Venango County Vocational-Technical Campus, Oil City, Pennsylvania

Computer Based Training, Certificate of Completion,1978 –2008

Certifications

- Presented several times at SHAARE, GUIDE(UUS and South America), and CMG
- Member, IBM East Coast Storage Consortium
- Member, National Computer Association Board Member – SHARE (2005 – 2008)
- Member, NaSPA
- Board Member – Indiana 4-H Foundation (11992 – 2004)
- Received (4) GTE Presidents Awards, (1) Personal Best Group Award,, (28) Quest for Quality Awards, (1) Power of One Award, (16) Once of Quality Awards, (11) International President Leadership Award Received (10) For d IT One Awards, (6) Ford IT Team Awards

INFO-MATRIX CORPORATION

Resource 94

Storage Management Administrator

Key Skills and Knowledge

- Storage Area Network engineer
- 25 years of experience in the state government and public safety market sectors

Certifications

- Microsoft NT Workstation
- Microsoft NT 4.0 Server
- Microsoft Networking
- Microsoft Windows 2000 Active Directory
- CommVault Administration
- VMware (VCP)
- VMware Capacity Planner
- EMCSE – EMC SE Accreditation: Strategies & Solutions
- EMCPA – EMC Proven Professional in Information Storage and Management
- EMCPP – SE Operational Practices
- EMCTA – EMC Technology Architect Specialty Credentials

Skills used:

- EMC DMX2000, DMX3, & DMX4
- CLARiiON CX300, 400, 500, 600, & 700
- Brocade Director switches and Cisco switches,
- EMC Control Center 6.1
- PowerPath, Emulex, and Qlogic HBAs
- Windows 2008, 2003, and 2000 Server
- CommVault
- VMware, Equalogic, Isilon, and NEXSAN

Professional Summary

Quality-driven, service-oriented Storage Area Network engineer with more than 25 years of experience in the state government and public safety market sectors. A skilled Microsoft system administrator and EMC proven professional who maintains a customer-centric focus while providing precise problem solving, decision-making, and administrative expertise.

Employment History and Related Experience

SANpulse, Storage Manager — 2012 – Present

Planned migrations of multiple EMC storage arrays across several data centers to a EMC VMAX storage array and Hitachi storage arrays to Hitachi AMS 2500; migrated more than 500 hosts.

- Create scripts for migrating data from DMX to VMAX for host-based migrations and the array base.
- Create volumes and map them to fiber adapter ports with EMC Solutions Enabler.
- Create zones for hosts to see storage ports at the command line.
- Set up SRDF Adaptive Copy between DMX arrays to the VMAX.
- Set up Cascade SRDF for migrating production hosts to disaster recovery hosts.
- Create SRDF scripts to migrate data between the DMX arrays to the VMAX.
- Migrated DMX thick devices to VMAX thin devices.
- Create masking view, storage, port, and initiator groups for hosts connecting to the VMAX.
- Gather data to design migration methods from various storage vendors to a single storage vendor, depending on the storage tier required.

KForce Contractor, Build Engineer — 2010 – 2011

Set up and configured 64 Cisco Director SAN switches; migrated Brocade DCX SAN switches to Cisco Director SAN switches. Migrated more than 10,000 SAN ports – one of the largest SAN migrations done, according to Cisco. Created scripts for migrating Brocade switches to Cisco.

- Prepared migration workbooks for the different data centers for migrating fabric.
- Planned the migration of 13 EMC storage arrays to one EMC VMAX storage array and our Hitachi storage arrays to one Hitachi AMS 2500. More than 500 hosts were migrated.
- Created scripts for migrating data from DMX to VMAX for host-based

migrations and the array base.

- Created volumes and mapped them to fiber adapter ports with EMC Solutions Enabler.
- Created zones for hosts to see storage ports on the command line.
- Set up SRDF Adaptive Copy between DMX arrays to VMAX.
- Created SRDF scripts to migrate data between the DMX arrays to the VMAX.
- Migrated DMX thick devices to VMAX thin devices.
- Created masking view, storage, port, and initiator groups for hosts connecting to the VMAX.
- Migrated CLARiiON arrays to IBM XIV using IBM XIV migration tools.
- Gathered data to design migration methods from various storage vendors to a single storage vendor, depending on the storage tier required.

IP Datasystems, Inc., Senior Technical Consultant 2008 – 2010

Installed EMC Control Center, Resource View, Symm Optimizer, Timefinder, SRDF, CommVault, EMC PowerPath, and EMC SMC software. Performed a host-based migration from DMX3 to DMX4 for a client in Newark, Delaware; worked closely with business managers and project managers; and assisted sales representatives on sales calls.

- Worked with clients on root cause analysis of issues with backups, storage, and Windows 2003 issues.
- Attended planning meeting with customers to discuss best practices on implementing software and hardware.
- Set up iSCSI on various storage arrays including Isilon, Dell Equalogic, EMC CLARiiON, EMC NX Series, Celerra installation and configuration
- Installed and configured Cisco 9513 and 9134 and Brocade 12000 SAN switches
- Zoned of new hosts to SAN environment and LUN masking to give volume access to new/existing hosts
- Installed and configured host bus adapters.
- Created basic Timefinder and SRDF scripts for use with BCV and SRDF devices.
- Set up and configured EMC CLARiiON hardware and software.
- Set up and configured NX hardware and software.
- Installed and configured Windows 2003, including WINS, DNS, DHCP, and TCP/IP.

MTM Technologies, Senior Storage Consultant 2008 – 2008

Set up and configured EMC CLARiiON hardware and software, including EMC Control Center, Resource View, Symm Optimizer, Timefinder, SRDF, and

CommVault.

- Worked closely with business managers, project managers, and technical architects.
- Assisted sales representatives on sales calls.
- Attended planning meeting with customers to discuss best practices on implementing EMC software and hardware.
- Zoned new hosts to the SAN environment and granted volume access to new hosts.

Unisys Corporation, SAN Manager, Harrisburg, PA 2004 – 2008

Managed 8 SANs consisting of Brocade fabric; designed and implemented Core/Edge using Brocade 12000 switches; and managed and oversaw configuration of EMC Clariions, Symmetrix, and DMX. Architected new SAN and storage solutions; installed EMC software upgrades; and installed EMC agents on servers to monitor errors on servers, SAN switches, and storage arrays.

- Zoned new hosts to the SAN environment; granted volume access to new hosts.
- Worked closely with business managers and project managers.
- Attended meetings with customers to discuss best practices, new projects, and current issues.
- Managed a $4.3 million project that included data migration from DMX2000 to DMX-3.
- Migrated data from DMX2000 to DMX-3 consisting of 57 Windows servers.
- Migrated data from Symmetrix 8830 to DMX-3 consisting of 14 Windows servers.
- Developed project plans; managed data migrations to the DMX-3.
- Architected a solution for migrating data from the Symmetrix 8830 to the DMX-3.
- Worked with EMC on configuring SRDF from the DMX-3 to the remote location in Philadelphia to a DMX2000.
- Installed and configured of Windows 2003, including WINS, DNS, DHCP, and TCP/IP for more than 400 servers.

Other Employment

EMC, Senior Implementation Specialist, Camp Hill, PA 1999 – 2004

Sphere Solutions, Inc., Systems Engineer, Sykesville, MD 1997 – 1999

Gateway Technical Services, Operations Manager, Owings Mills, MD 1996 – 1997

SAIC, LAN Administrator/Lead System Engineer, Abingdon, MD 1994 – 1996

General Physics Corporation, LAN Administration,

UNISYS

INFO-MATRIX CORPORATION

Resource 94

Storage Management Administrator

Columbia, MD 1992 – 1994

Education

Concepts of CICS: Mainframe	Time Management
NetWare Service/Support	Introduction to Data Communications
NetWare 3.11	NetWare v.2.2 AdvANCED System Manager
NetWare Advanced Topics	Training for Trainers
Better Writing for Results	Consulting Skills Workshop
NetWare 3.x – 4.1 Update	NetWare 5.1 Training
EMC RSSS String	EMC Volume Logix
EMC ESN Manager	EMC Switch Zoning
EMC ECC/Open Edition	VMware Training
CUA Web Base Training	Centerra Foundation Training
Isilon Storage	EMC SE
EMC PA	EMC PP
VMware Capacity Planning	EMC CLARiiON
EMC NAS Training	CommVault Administration

UNISYS

IBM

Resource 95

Storage Management Administrator

Key Skills and Knowledge

Hardware

- EMC Symmetrix VMAX w/FAST
- DMX-4/3
- DMX-2000
- 8830/8730
- CLARiiON CX3-80
- CX-700
- CX-600
- EMC Celerra
- EMC Connectrix
- EMC Centera
- IBM DS8300
- IBM SVC
- IBM XIV
- Hitachi Tagmastore
- VSP
- USP/USP-V
- 3PAR
- HP-9500
- NetApp
- Cisco 9509/9513
- Brocade
- Sun Starfire E10000
- E6000
- E4500
- E450
- ADIC Libraries
- StorageTeK
- IBM

Network

- Fibre Channel
- FCIP
- iSCSI
- FCoE
- Internet/Intranet
- Ethernet
- Cisco 9513/9509 McData
- Brocade
- TCP/IP
- OSI
- DHCP
- WINS

Professional Summary

Expert Capacity Planner, accomplished performance assessment across storage tiers (one-time analysis, quarterly or monthly analysis & trending); accomplished Application Performance Profiling for Tiering recommendations (RAID Level); and delivers skillful Bandwidth Analysis for EMC SRDF/A, MirrorView, SANCopy etc. Subject Matter Expert for:

- SAN Consolidation Analysis for EMC, IBM and Hitachi Storage Arrays
- Technical SAN and Storage Assessments
- Disaster Recovery Planning
- Performance based Data Center Migration Planning with source to target device level plan
- Performance Analysis for Storage Platforms supported: EMC Symmetrix/VMAX, CLARiiON, IBM
- DS8300, IBM SVC, Hitachi Tagmastore, USP, USP-V/VM
- Performance Analysis for Operating Systems. Support for: Solaris, Linux, AIX & Windows

Employment History and Related Experience

STATE OF TEXAS, SAN Assessment & Application Profiling, Austin, Texas, 2011

Worked proactively with state of Texas to provide a detailed SAN Assessment based on IBM recommended best practices. SAN comprises of Cisco 9513 switches, IBM Storage Volume Controller (SVC) and IBM DS8300.

- Provided detailed performance profiles using the internally developed Perfonics™ tool that can analyze data from various SAN components and performance data from Tivoli Productivity Center (TPC).
- Analyzed critical Food Stamps application used state wide from performance and best practices perspective. Conducted end to end performance analysis for AIX and Windows hosts with DR replication profiles.

EMC PROFESSIONAL SERVICES (Partner), Independent Consultant (Founder) – Interscape Technologies Inc., Performance Engineer, Storage Architect and Disaster Recovery, New York, New York, 2002-2011

Credit Suisse: Instrumental with Tech Refresh project, providing services for performance and capacity based migration planning using Open Replicator. Over 100 arrays and 500 hosts.

- Performed Capacity Planning and Storage Architecture for new data center in Princeton & Clifton, NJ. (EMC VMAX, CLARiiONs, Netapp, 3PAR).

IBM

Resource 95

Storage Management Administrator

Operating Systems

- VMware 3.5
- Solaris 10/8/7/2.6/2.5.1
- AIX
- Linux Fedora/Red-Hat
- HP-UX
- Windows Server 2007
- AT&T/NCR MP-RAS UNIX 4.x
- Windows 2008
- NT 4.0

Software/Languages

- CA-TNG Unicenter
- Oracle Financials 10.7
- Siebel
- MS Office
- Motif
- EMC ECC 6.x/5.x
- C
- C++
- Visual Basic
- Pascal
- Perl
- Shell script
- Assembly
- EMC Control Center
- Performance Manager/WLA
- EMC TimeFinder
- EMC SRDF
- SRDF/A
- SANCopy
- Recover Point
- MirrorView
- SANScreen
- Tivoli Productivity Center
- Legato Networker
- Veritas Volume Mgr
- NetBackup
- Sybase 9.x
- Oracle 8.0/7.3.x
- Mysql
- MS SQL Server
- Progress 9.1b/8.3
- UDB

- ITIL implementation for storage infrastructure. Custom SRM Tool implementation with integration with external infrastructure related systems (SANscreen, Tideway, and Data Warehouse).
- Consolidation and Migration Planning for three data centers for 50 storage arrays (CLARiiON, DMX).

Goldman Sachs: Very Large Infrastructure base of VMAX, DMX-4/3, DMX-2000, and DMX-3000.

Over 150 CLARiiONs (CX3-80, CX-700, CX-600), using RAID 1+0 RAID 1 and RAID 5 on Cisco SANs (9513, 9509, McData ED-140M).

- Responsible for Storage and SAN Capacity Planning for over 10 PetaByte storage and 10000 Ports across 5 Data Centers. Instrumental in planning for every SAN attached host. Created Performance and Capacity Planning team and processes for North America operations.
- Lead the CLARiiON Consolidation Modeling project for target Mixed Tier VMAX arrays using FASTVP and Thin Provisioning. Over 120 arrays and 2000 hosts.
- Helped design storage architecture for 4 Data Centers with synchronous replication and multiple tiers of storage.
- Planned storage consolidation for complete storage environment from EMC DMX-2000, DMX-3000 to DMX-3 and DMX-4. Consolidated 36 SRDF replicated storage arrays into fewer DMX arrays using performance centric planning.
- Served as Performance Engineer, Analyzing System Performance for Solaris, Linux, AIX and Windows using iostat, sar and perfmon data.
- Conducted Storage Performance Analysis using Symstat, WLA, SymmMerge, and Perfonics. All storage arrays replicated over Wide Area Network, using SRDF and SANCopy.
- Developed Technical Migration Plans and Design for storage migration of over 5000 Solaris, Windows and Linux servers and over 1.2 PetaByte using SRDF and SANCopy Replication. Migrations to DMX-4 and CX4-80 arrays.
- Assisted architect EMC Storage Area Networks for migration of 140 Symmetrix Units to 30 8830 Symmetrix and Connectrix ED-64 & ED-140M switches.
- Provided documents with detailed Visio diagrams, and Implementation and Migration Plans. Using ECC 6.x, EMC Control Center.

Verizon Business & Verizon Telecom: Performed SAN Assessment for Verizon Business clients, such as JetBlue Airlines which included multiple DMX-2500. Celerra Performance Assessment. Analyzed CPU utilizations, Memory, Network Bandwidth, CIFS Fileshares, Cache hits, and Fileserver operations.

- TimeFinder implementation with scripting on Windows server using clones and TimeFinder Integration.
- Module (TEIM) and SRDF.

- MS Access

- VMAX resident expert, helped with VMAX solutions design with FAST and Thin Provisioning features.

Bank of New York: Executed multiple projects during 2006-2008. Post Migration Performance Analysis for DMX Arrays attached to Open Systems and IBM Mainframes. Identify bottlenecks and establish baseline IO Profiles

- Engaged to provide the following scope for the BNY and Mellon Bank Merger:
  - Baseline Performance analysis for 17 DMX arrays
  - RAID-5 application recommendations based on array level IO performance profiling for over 650 Servers
  - Application Tiering recommendations
  - RDF/A bandwidth analysis across data centers for Disaster Recovery
- Conducted Performance analysis on over 10 DMX Arrays for Migration planning at Array level, Device level and Disk level to select best RAID Level strategies for SRDF replicated arrays.
- Performed Host and Array level performance planning for MVS Mainframes using Work Load Analyzer and RMF Data. Two Mainframes Complex with two DMX Arrays on each site.

CitiGroup: Performance Analysis and troubleshooting for the RBNAW application running on IBM AIX LPAR servers on multiple DMX Arrays. Conducted performance assessment of 30 Mainframe Symmetrix setup in STAR configuration as part of ITIL project.

- Assisted in providing application assessment and documentation for the current environment.
- Coordinated presentation of final analysis and recommendations.

ADP: Engaged for performing Bandwidth Analysis study for the Magellan application for MirrorView implementation. Worked on a project to do performance analysis and recommendations for scaling the recommendations for file system layout for SQL DB Planning.

NYSE: Performance Analysis for Symmetrix 8830 and DMX arrays and present recommendations. Symmetrix connected to UNIX, Windows and MVS Hosts.

Medco Healthcare Solutions: Provided Performance Analysis for DMX arrays and present recommendations.

CREDIT SUISSE FIRST BOSTON, Independent Consultant – Storage Architecture/Disaster Recovery, New York, New York, 2001-2002

Designed Total Architecture for Storage Area Network and Disaster Recovery using EMC SRDF. Implemented over 200 TB of EMC Symmetrix Storage with a 400 port SAN using EMC/McData Connectrix switches.

IBM

Resource 95

Storage Management Administrator

- Over 100 mid to large Sun Solaris and HP Servers. Exchange Microsoft Clusters on SAN with SRDF based DR implementation. Used ESN Manager, Volume Logix, SDDR and other EMC tools.
- Celerra NAS implementation with Active/Passive redundant design using 12 Data Movers on each side and over 6TB of EMC BCV/TimeFinder storage.
- Disaster Recovery over Dark Fibre using DWDMs with a completely redundant multiple Fabric design, using EMC SRDF.
- Wrote extensive shell scripts to automate various trouble-shooting procedures and DR failover. recovery.
- Provided critical documentation to manage the total project with detailed Visio diagrams, Implementation Plans and checklists.

Education

- M.S. Computer Science, New Jersey Institute of Technology, Newark, NJ
- B.S. Computer Science (Program Distinction), Stockton State College, Pomona, NJ
- B.S. Physics (Honors), University of Calcutta, Calcutta, India

Certifications

Trainings and Certifications:

EMC Proven Professional - Master Operator+ Certified | Legato Certified Engineer | Sun System Administrator Certified | VMware 3.5 Infrastructure Trained | Netapp SANscreen Training | Principle Centered Leadership | Project Management | Effective Technical Presentations | Managing People and Performance | Extensive internal technical training | Product Management Concepts | Diversity Workshops

UNISYS

IBM

Resource 96

Storage Management Administrator

Key Skills and Knowledge

Hardware

- IBM
- EMC
- Sun/STK
- HP
- Dell
- Brocade

Mainframe Operating System

- z/operating system
- operating system/390
- MVS/XA
- MVS/XP

Application/Utilities

- TSO
- ISPF
- Remedy
- CICS
- SYNCSORT
- DFSORT
- File Aid
- JCLPREP
- MS

Programming Languages

- JCL
- COBOL
- SAS
- CLIST
- REXX
- ACS

Softek Replicator (TDMF)

Computer Associates

- CA-1
- CA-Vantage
- CA-7
- JobTrac

Professional Summary

Over 20 years experience in Storage Management, Disaster Recovery, and Computer Operations. Establish and maintain Storage Management: standards, policies, retention, backup/restore, scheduling, conversion, fall back, disaster recovery, and performance. Develop Information Management Policies - performance, space and availability requirements

- Manage data; moving, copying and manipulating files using DFDS and other utilities.
- Track and report Storage growth, usage, free space, etc.
- Perform backup and recovery: Full volume, incremental, disaster recovery, mirroring, slit/establish, etc.
- Migrate to new equipment (i.e. EMC, 3390s, VTS, etc.), software, etc.
- Provide SMS education to developers, analysts, operators, production control, systems programmers, managers, etc.
- Identify requirements such as data, user, hardware, and software.
- Perform storage, system and application troubleshooting.
- Identify and document Recovery Time Objective (RTO) and Recovery Point Objective
- (RPO).
- Conduct Business Impact Analysis (BIA).
- Monitor DFSMShsm activities including migrations, recalls, backups and data set recovery.
- Monitor DFSMShsm and DFSMS logs and control data sets like the MCDS, BCDS, OCDS, and Journals.
- Monitor DASD volumes and storage pools; ensuring sufficient free space, minimal fragmentation, etc.
- Monitor DFSMShsm primary and secondary automatic space management activities
- Monitor DFSMShsm Recycle of ML2 and Backup tapes.
- Monitor DFSMShsm Control Data Set and Log backup
- Monitor SRDF links and replication processes
- Monitor files exceeding 16 extents, VSAM files exceeding 240 extents and/or 4gb in size

Storage Administration

Participated in the outsourcing of Mainframe Storage Operations. Documented the processes and procedures used by the Storage Administration team. Assisted in the Identification, collection and documentation of the storage equipment, maintenance agreements and I/O configurations. Identified storage related software and license keys and agreements. Obtained necessary system, software and security access for off-shore team. Oversaw education, training and "shadowing" of the offshore team. Participated and Coordinated disaster recovery tests.

Resource 96

Storage Management Administrator

- CA-Disk (SAMS)

IBM

- DFSMS
- DFSMShsm
- DFSMSpdf
- DFSMSdss
- ISMF
- IDCAMS
- ICKDSF
- IEBCOPY
- IEBGENER

Innovation Data Processing

- FDR
- ABR
- EXHPDM

EMC

- SRDF
- TimeFinder
- ECC

Softek Replicator (TDMF)

- Monitored DFSMShsm activities including migrations, recalls, backups and data set recovery.
- Monitored DFSMShsm and DFSMS logs and control data sets like the MCDS, BCDS, OCDS, Journals.
- Monitored DASD volumes and storage pools; ensuring sufficient free space, minimal fragmentation, etc.
- Monitored DFSMShsm primary and secondary automatic space management activities.
- Monitored DFSMShsm Recycle of ML2 and Backup tapes.
- Monitored of DFSMShsm Control Data Set and Log backup. Monitored SRDF links and replication processes. Storage Administrator.
- Established and maintained Storage Management: standards, policies, retention, backup/restore, scheduling, conversion, fall back, disaster recovery, and performance.
- Developed Information Management Policies - performance, space and availability requirements. Managing Data; moving, copying and manipulating files using DFDSS and other utilities.
- Tracked and reported Storage growth, usage, free space, etc. Backup and recovery: Full volume, incremental, disaster recovery, mirroring, split/establish, etc.
- Migrated to new equipment (i.e. EMC, 3390s, VTS, etc.), software, etc.
- Provided SMS education to developers, analysts, operators, production control, systems programmers, managers, etc.
- Assigned as the lead storage administrator for disaster recovery tests.
- Worked with user groups to identify recovery requirements, including Recovery Time Objective (RTO) and Recovery Point Objective (RPO).
- Assisted in conducting Business Impact Analysis (BIA).
- Analyzed, implemented and maintained Disaster Recovery processes.

Data Center

Consolidated two (2) Data Centers. Activities included:

- Worked with application groups to identify and document files to be moved.
- Developed procedures and processes for the movement/transportation of data. Tested and verified these process and procedures.
- Worked with Applications, Scheduling and Operations to schedule and monitor data movement. Verified the data moved as expected.
- Researched problems as required.

Employment History and Related Experience

- WellPoint Storage Data Center Consolidation (2010-2011)
- Wells Fargo Bank Storage Administrator (1998-2007)
- Wells Fargo Bank Shift Manager/Production Analyst/Storage
- Assistant (1988)
- Wells Fargo Bank Development Support Analyst (1985-1989)

IBM

Resource 96

Storage Management Administrator

- Wells Fargo Bank Senior COBOL Programmer/Analyst (1983-1985)
- Trust Fund, Inc. COBOL Programmer (1980-1983)

Education

Chabot College — Business and Computer Science

Served 4 years in United States Military

This page intentionally left blank.

UNISYS

Resource 97

Storage Management Administrator

Key Skills and Knowledge

- SAN and Storage expertise and solutions
- Hardware: IBMDS8300, Cisco directors9513, IBM SVC, IBM XIV
- Brocade Fibre Channel switches
- IBM pSeries and xSeries servers
- Operating systems: Microsoft Windows 2000, 2003, and 2008; RHEL; and IBM AIX
- Software/system architecture
- IBM Storage Manager
- IBM TPC
- Cisco Fabric Manager
- On-command Core
- Data Fabric Manager
- MSCS clustering
- SVC
- DS8300 – 2107 - 922 and DS8100 2107 - 921
- IBM SVC 2145 4F2, 8F2, CF8, and D4800
- Cisco MDS 9509 and 9513
- SAN Director and switches
- Windows 2000, 2003, and 2008 Server Cluster environment
- Linux RHEL
- ESX hosts 4.1 and 5.0

Professional Summary

16 years of total IT experience of systems implementation, configuration, and troubleshooting with expertise on IBM storage DS 8100/DS 8300, ESS800/DS4000 series Storage in IBM AIX, Sun Solaris, Linux, Windows environment. Practical expertise in SAN design, deployment, and management Cisco MDS 9509/9513 Directors SAN switches. End-to-end Storage provisioning expertise with DS8100. DS8300 and DS4000 Series, IBM SAN Volume controller SVC, IBM XIV 2810/2812.

- Worked as Storage Architect in to design/configure and implement the IBM DS8300 storage to provide the best performance. Completed storage upgrade from DS8100 model 921 to DS8300 model 922; used IBM SVC for Data migration storage side, Used LVM and VMware cold migration to migrate data
- Implemented Metro mirror/Global mirror DR solutions using IBM SVC and IBM XIV.
- Expertise on DSCLI command line to do the storage configuration/provisioning and Storage administration
- Worked with Large VMware ESX 3.5/4.1/4.2 hosts cluster environment for configuring SAN on ESX hosts and creating Data stores; worked with high-end AIX/UNIX servers and Storage as a senior level UNIX System Administrator, Systems Support Engineer or back line Support Engineer. Programming: UNIX shell programming, PERL scripting
- A fast, resourceful troubleshooter with a strong attention to detail, who likes to get the job done, Ability to work in a team environment, good communication skills
- Experienced with working with and management of teams, clients, and vendors.

Professional Experience

Unisys Corporation, Commonwealth of Pennsylvania,
SAN Administrator,
Harrisburg, PA 2007 – Present

Maintain and support IBM DS8100 and 8300 and IBM XIV, DS4500, and DS4800 with about 750 TB of finished space with Cisco SAN MDS-9509 and 9513. Upgraded storage DS8100-921 to DS8300-922, which involved data migration from the old model to a temporary/swing DS8100 box and back to the upgraded DS8300-922 model.

- Configure and Implement DS8300 with two 92E expansion frames.
- Design and configure the complete logical configuration of DS8300 to promote the best performance.
- Install and configure IBM XIV 2810/2812 storage; create and assign LUNs to the ESX clusters.

UNISYS

Resource 97

Storage Management Administrator

- Implement storage metro mirroring storage replication to the disaster recovery site.
- Install and upgrade SDD/SDDDSM and RDAC drivers in Windows and Linux RHEL 3.0 servers.
- Implement and configure Flash copy to backup the database servers' LUN.
- Collect storage requirements from customers and provide them with a best solution.
- Attach and configure the DS4500 storage controller behind the IBM SVC.
- Create the image mode.
- Manage disk to migrate the LUNs from the DS4500 to the DS8100/D8300.
- Upgrade SVC code and MDS 9509 and MDS9513 code.
- Upgrade DS4000 controller firmware disk firmware and ESM firmware.
- Install, configure, and manage Netapp and NSeries FAS 6240 storage.
- Install and configure storage performance monitoring software IBM TPC and on-command core.
- Collect performance data and create performance line graphs.
- Create design zones for the new host attachment requirements or for a new storage controller.
- Plan, forecast, and review capacity with customers.
- Tune the performance of storage of LUNs RAID types and controllable settings in a storage controller.

IBM Global Service, AIX Administration and Storage Specialist, Boulder, CO 2004 – 2007

Maintained DS4500, DS8100, 8300, and DS4000 series in a Cisco Fabric environment; installed, configured, and administered SANs for large external and international IBM customers; designed SAN consisting of core/edge technology with dual Cisco fabrics for redundancy and to allow "no downtime" maintenance windows; each SAN consisted of a primary and a failover site.

- Created LUNs and mapped them to AIX servers.
- Created file systems.
- Worked extensively with Cisco, McData, and IBM Enterprise class storage devices.
- Helped design and implement various backup solutions like Backup & Restoration/Recovery from snapshot to disk, tape to disk, and disk to disk on the production and test application, reporting, database servers.
- Migrated storage from Shark F20 to DS8000.

Environment: Cisco, McData, IBM DS8300, ESS 800, DS4500 and DS4800 SAN volume controllers, Power4 and Power5 AIX servers, and TSM (Tivoli Storage Manager).

UNISYS

Resource 97

Storage Management Administrator

IBM Global service, Storage Technician, India 2003 – 2004

Designed a SAN and implemented IBM FastT Storage 500/700 and Shark F20; configured storage in the SAN and assigned them to hosts running AIX, Linux, and Windows operating systems.

- Designed the LUNs of RAID 0, RAID 0+1, and RAID 5 RAID groups and storage groups according to an application's size and performance requirements.
- Implemented and configured a storage manager client and ESS specialist Flash copy.
- Configured EMC SnapView snapshots and snap clones (BCVs) together with Mirror view and SAN copy for advanced data protection, created replicas locally and remotely.
- Installed and configured HBA driver firmware. Updated HBA firmware and multipath drivers on IBM AIX, Solaris, Linux, and Windows servers. Performed end-to-end storage provisioning for Sun, AIX, HP, Novell, Linux, and Windows hosts using ESS specialist and Fabric Manager on SAN switches.

Environment: FatsT500 and 700; Shark F20; SP frames; p630, p650, and S58 servers running AIX 5.x; Solaris 8 and 9, Linux 7.x, 3, and 4; TSM; and Sun SPARC Enterprise Server workstations.

DCM Data Systems, Sr. Systems Administrator, ltd.
India 2001 – 2003

Planned, installed, and configured servers and HMC. Created and customized LPAR profiles. Installed AIX 5.1 on each LPAR server profile. Created mirror at oslevel for rootvg. Configured FastT700 arrays and logical drives; assigned them to the AIX host. Installed, configured, and split a 2104 du3 storage disk array for access by the AIX host simultaneously. Configured RAID5 on all AIX servers using du3 storage.

- Created and managed file system sizes.
- Set up the complete environment for installation of SAP r/3 on AIX 5.1.
- Installed a configuring performance meter to take and exact view of system performance.
- Planned and configured storage using LVM.
- Set up and deployed security standards, openssh, SSL, TCB, and so forth.

Environment: FastT200, 300, and 900 ESS shark SP tall frame; 7026 B50 servers; and SCSI disk array

UNISYS

Resource 97

Storage Management Administrator

Other Employment

DCM Data Systems Ltd. India, UNIX System Administrator	2001 – 2003
Hindustan Petroleum Ltd. India, Systems Engineer	2000 - 2001
CMC LTD – India, Systems Engineer	1996 – 2000

Education

- Bachelor of Engineering, Electronics & Telecom, Amravati University, India

Training

- IBM High End Storage for Open System Implementation DS8300, IBM USA, 2008
- MSCSE Windows NT, India, 1998
- IBM AIX 5L system administration, IBM India, 2003
- IBM Tivoli Access Manager, IBM Malaysia, 2003

Professional Certification

- IBM Certified Specialist – High End Disk Storage for open systems, 2008
- MCP Windows NT Server, 1998
- IBM Certified Specialist – AIX 5L, 2004

UNISYS

Third Party Software Specialist

This page intentionally left blank.

UNISYS

Resource 28

Third Party Software Specialist

Key Skills and Knowledge

Databases

- MS SQL, Oracle, and DB2

Hardware

- IBM server hardware
- Dell server hardware

Operating Systems

- Microsoft Windows: NT 4, 2000, XP, 2003, 7, and 2008
- Linux: SuSE 10 & 11; Red Hat 5 & 6

Programming Languages & Tools

- DOS scripting, PowerShell, VB Script, C, C++, and HMTL

Call Center and Help Desk

- Remedy

Office Productivity Tools

- Microsoft Word, Excel, and Outlook

Facilities Management

- UPS monitoring and design

Professional Summary

Strong experience in systems administration and network management with a facility for learning and implementing unfamiliar technologies to attain customer-required outcomes.

- 12 years of implementing Web applications using Microsoft IIS as the Web and application server
- 12 years of deploying Microsoft Windows on authentication, file, and application servers
- 5 years installating, configuring, and deploying applications using of IBM WebSphere Application Server (WAS)
- 5 years of installing and configuring of Linux users and services, including Samaba, SSH, and BIND
- 4 years of installing and configuring VMware and ESC; as well as hosting of virtual infrastructure for a lab environment
- 2 years of installing and configuring of WebSphere MQ Server to support application communication across multiple platforms and architectures.

Professional Experience

Elite Systems, Commonwealth of Pennsylvania
Office of Administration, Integration Consultant, 2010 – Present

Supported application deployments for the Commonwealth of Pennsylvania; coordinated and implemented the upgrade of WebSphere MQ from version 5 to version 7 for multiple Commonwealth agencies to access an enterprise SAP environment.

- Review, create, and update documentation used to deploy and support agency applications hosted at the Commonwealth's Enterprise Data Center.
- Evaluate agency requested changes against industry best practices and Commonwealth security standards.
- Coordinate change management processes among multiple Commonwealth enterprise teams to complete application deployments for Commonwealth agencies.
- Manage DNS servers hosting Microsoft Windows DNS and associated DNS records.
- Patch and troubleshoot Linux servers running SuSE and Red Hat distributions.

UNISYS

Resource 28

Third Party Software Specialist

TEKSystems/MindTeck, Pennsylvania Department of Transportation (PennDOT), Network Engineer, 2004 – 2009

Provided 24/7 support of numerous applications hosted at the PennDOT server farm for various bureaus in the department; monitored, and maintained APC UPS infrastructure.

- Deployed WebSphere Application Server infrastructure to support migration of PennDOT applications from Lotus Domino-based architecture to Java architecture.
- Deployed IBM DB2 Connect server and DB2 client software upgrades to support access to IBM mainframe-hosted DB2 database instances hosted on z/operating system.

Other Employment History

Innovative Business Concepts	2004 – 2004
GEF Computers	2002 – 2004
New Horizons	2000 – 2003
Computer Renaissance	1998 – 2000

Education

High school diploma, Sauquiot Valley High School 1993

Courses at Clarkson University, 1995

Professional Certifications

- CompTIA A+, May 1999, COMP10157635
- Microsoft Certified Professional, Microsoft, March 2000, MCP ID#1789557
- Microsoft Certified Systems Administrator Microsoft, August 2004, MCP ID#1789557
- Microsoft Certified Systems Engineer, Microsoft, August 2004, MCP ID#1789557

Professional Development

- ITIL v3 Foundation training, Framework that allows for continuous improvement of the documentation, customer service, and change control processes of an IT organization, 2012
- SiteMinder 12.5 training, Access management for Websites using LDAP and Active Directory security, 2012

UNISYS

Resource 98

Third Party Software Specialist

Key Skills and Knowledge

- ITIL Foundations v3
- Software licensing
- Contract management & administration
- Technical writing
- SharePoint administration
- Self-Service Purchasing (SSP5)
- P-Relay

Professional Summary

Self-Service Purchasing (SSP5) Application, P-Relay, strong written and oral communication skills, attention to detail, technical writing, and SharePoint administration.

Project Experience

Unisys Corporation, Commonwealth of Pennsylvania
Project, Business Analyst 2008 – Present

Assist project managers with procurement, third-party software administration, contract management, technical writing, and SharePoint administration.

Unisys Corporation, Site Services Administrator 2003 – 2008

Assisted project managers with performance management, recruiting, physical security, and procurement.

Education

B.S., Business Administration, eneral Management,
Shippensburg University, 1991

Awards

Silver Recognition Award, June 2005

Silver Recognition Award, January 2005

Silver Recognition Award, February 2004

Certifications

- ITIL Foundations v3

This page intentionally left blank.

UNISYS

Resource 99

Third Party Software Specialist

Key Skills and Knowledge

Domain Expertise & Solutions

- Public Sector
- Fortune 100 Private Sector
- Data Center Operations

Databases

- Microsoft Access
- MS SQL Server
- Oracle 10g

Operating Systems

- Windows 7, 8, and 9x
- Windows Vista
- Windows XP
- Windows NT
- Windows 2008
- UNIX
- Linux
- DOS

Programming Languages & Tools

- C#
- C++
- Visual Basic, Batch, PowerShell
- Crystal Management Console
- Crystal Reports
- HTML
- Java
- Microsoft FrontPage
- Microsoft Project
- Microsoft Office
- Microsoft Visio
- Microsoft Visual Basic .NET
- Remedy Action Request System
- SQL
- DameWare
- Remotely Anywhere, Compaq/HP
- ILO
- IBM RSA, IBM Director
- Cygwin, OpenSSH
- Aelita Domain Migration Tool, Altiris 5.5

Professional Summary

Progressive experience in implementing and administering new technologies to the existing networks in Windows 2008, 2003, 2000, Vista, XP, NT-based client/server environment, which also includes managing projects.

- Enterprise-level experience working with fortune 100 companies and Government Agency like Hewlett-Packard, IBM, Merrill Lynch, Unilever North America and Commonwealth of Pennsylvania
- Expertise in deployment, migration, and administration of Windows Server 2008, 2003, and 2000
- Expertise in administration and deployment of CA SiteMinder
- Installing and configuring VMware Server, VMware Player, and VMware Converter
- Expertise in administration and deployment of Radiant Logic VDS
- Installing and configuring Microsoft TMG 2010 Enterprise Servers
- Expertise in network administration; database administration; TCP/IP network implementation; system integration, management, and troubleshooting
- Expertise in installing and maintaining Microsoft Web Server clusters
- Configuring and administering ESRI GIS (Geographic Information Systems)
- Installing, configuring, and troubleshooting IBM Tivoli Monitoring and IBM Director
- Testing and integrating-various third party applications on Windows 2003 and 2000
- Extensive experience in testing, evaluation, and implementation of Windows 2003 and 2008
- Used PowerShell and VB Script for modifying and administering object properties in Active Directory
- Disaster recovery planning
- Experience with installation, configuration, and administration NetScaler Access Gateway and Citrix XenServer
- Configuration and administration of UNIX and Linux
- Excellent creation and editing of technical documentation; fast learner
- Excellent leadership and communication skills and strong analytical skills.

Employment History and Related Experience

Commonwealth Technology Center, Senior Integration Consultant, Harrisburg, PA — 2007 – Present

Configure and maintain SiteMinder Cluster Server for authentication, authorization and Single Sign-On on the Commonwealth network. Install, configure, and maintain Radiant Logic Virtual Directory Server for the Commonwealth Technology Center. Provide Level 3 support (regular and on-call) for the servers at the hardware, operating system, IIS, Microsoft .NET application, and multiapplication

UNISYS

Resource 99

Third Party Software Specialist

- Microsoft TMG 2010
- Radiant Logic (Virtual Directory
- Services)
- Microsoft SCOM Console
- CA SiteMinder R12.5

Web Technologies

- Microsoft IIS 6.0 and 7.5
- JBoSS

levels.

- Support is 365/24/7 in an environment with application availability of 99.99 percent.
- Ongoing deployment of Windows 2003, 2008, IIS, and Database Server for the Commonwealth of Pennsylvania and its agencies.
- Troubleshoot and configure VMware hosts.
- Administer Windows 2003 and 2008 Active Directory and support more than 10,000 users.
- Configure, support, and troubleshoot Microsoft Clustered Server.
- Troubleshoot DNS and network issues.
- Support the entire environment (development to production) comprising more than 250 IBM xSeries servers.
- Resolve trouble tickets Using Remedy Ticketing System.
- Use the Change Management process for all changes; review change management requests.
- Install, configure, and administer NetScaler Access Gateway and Citrix XenServer.
- Install, configure, and manage Microsoft TMG 2010 Enterprise Proxy Server.
- Review and update documents according to agency requirements.
- Work with agencies to plan and implement projects on schedule.

Deloitte, Active Directory Engineer, Harrisburg, PA 2007 – 2007

Level 3 support (regular and on-call) for the servers at the hardware, operating system, and IIS levels. The project involved deployment of Window 2003 IIS and Database Server for the Commonwealth of Pennsylvania. Project was to develop a solution for the Commonwealth's Department of Labor.

- Configured and administered Windows 2000 and 2003 Active Directory and supported more than 10,000 users.
- Configured, supported, and troubleshot Microsoft Clustered Server.
- Configured and troubleshot DNS and network issues.
- Installed and troubleshot IBM Tivoli Storage Manager Client.
- Installed and troubleshot IBM Tivoli Monitoring.
- Installed and configured VMware for testing regular patches and other software before installing them in production servers.
- Supported the entire environment (development to production) comprising 110 IBM xSeries Servers.

IBM, Wintel Systems Administrator, Poughkeepsie, NY 2005 – 2007

This project involved deployment and maintenance of Windows 2000 and 2003 Server Standalone in an Active Directory domain. Supported IBM internal and external clients, which included more that 500 IBM servers. Led the knowledge transfer and transition of work to teams in India, Brazil, and China (training and

cutover).

- Level 3 support for IBM servers at the hardware, operating system, and application levels.
- Configured and administered Windows 2000 and 2003 Active Directory.
- Configuring and troubleshot DNS and network issues.
- Installed and troubleshot IBM Tivoli Storage Manager Client.
- Installed and troubleshot IBM Tivoli Monitoring.
- Installed and configuring VMware for testing regular patches and other software before Installed them on production servers.
- Supported IIS on the production servers. Troubleshot and supported internal clients on requirements for Web hosting.
- Installed and supported two-node cluster with Microsoft SQL and shared resources on Shark.
- Installed and maintained IBM servers in the Poughkeepsie and Fishkill Data Centers.
- Provided 24/7 on-call Level 3 support for servers.
- Decided on technical and hardware details for clients.
- Performed extensive work on OpenSSH and Cygwin for communication between Windows and AIX servers.
- Performed change and problem management with IBM Manage-now (ITIL process).
- Configured and maintained Symantec System Center Console.
- Implemented and supported new business clients on the servers and the transition.
- Maintained up-to-date documentation on the process and procedure.

Hewlett-Packard/Unilever, Project Lead 2003 – 2005

Created Active Directory sites. configured and scheduled site replication for these sites. Created and managed user accounts and groups. Migrated users from the NT4 domain to Windows 2003 domain using Aelita.

- Configured network services, including DC, GC, DFS, FRS, DHCP, and DNS.
- Migrated DHCP scope.
- Installed and configured Tivoli, Enterprise Security Manager, and Legato.
- Generated ESM reports on the new servers after deployment to make sure they all met security requirements.
- Restricted space allocated to each user using Disk Quota Management.
- Configured RAID on HP ProLiant DL380 servers.
- Turned over servers to production after the total quality check.
- Assessed the site and ordered required components to make the site ready for server deployment. Coordinated with the network team on network issues and to get the server up and running in time to meet the SLA.

UNISYS

Resource 99

Third Party Software Specialist

- Defined and refined a process for building and configuring Windows 2003 servers.
- Troubleshot problems that arose during server deployment and configuration.
- Installed and managed Exchange Server in the enterprise.
- Migrated the servers from Exchange 5.5 to Exchange 2000.

Hewlett-Packard/Unilever, Project Lead 2003 – 2003

Led an eight-member team and led the deployment and migration to Unilever. Migrated users from the NT domain to Active Directory. Synchronized home shares using Aelita. The project involved building the new laptops according to Unilever standards.

- Created and assigned entrust certificates.
- Migrated user profiles for desktops and favorites using Altiris.
- Met deadlines and supported users for 7 days after the migration.
- Configured and created printers on Windows 2000 and 2003 servers.
- Performed group migration using Aelita.

Hewlett-Packard/Merrill Lynch, Senior Systems Engineer 2003 – 2003

Implemented Active Directory Services. Configured and scheduled site replication over these sites. Created and managed user accounts and groups. Configured network services, including DHCP and DNS.

- Automated client PC installation using Remote Installation Services (RIS).
- Implemented security using Domain Security Policy, Group Policy, and file permissions of NTFS5.
- Restricted the space allocated to each user using Disk Quota Management.
- Migrated mail for users from the Windows NT4 environment to Windows 2000 Exchange Servers.
- Configured and tested the mail migration process using Aelita mail migration tool in a test lab before going to live migration.
- After successful mail migration of the users, provided users with daily support.
- Maintained problem and solution documentation from day to day.
- Coordinated team members for 24/7 operation to meet deadlines.

Hewlett-Packard/Unilever, Senior Systems Engineer 2001 – 2003

Built and configured NT servers for different locations across North America. Once the servers were in production, configured, and tested the backup device for the server. Migrated and consolidated users' data from Novell and NT servers to the centralized server. Configured and created printers on the new servers.

UNISYS

Resource 99

Third Party Software Specialist

- Created group shares for common groups and granting appropriate permissions.
- Configured and tested the IBM backup device for the server using Legato.
- Built and deployed desktops and laptops for users on the Unilever build standard (Aztec)
- Created new NT IDs, Sprint IDs, and entrust certificates for users.
- Performed quality checks before delivering desktops and laptops to users.
- Performed user support on the client and server sides.

Additional Employment History

Ramco Systems Limited, Network Engineer	1999 – 2000
CIDER, Systems Executive	1995 – 1999
Horizon Computers, Software Executive	1994 – 1995

Education

- B.S., Physics, University of Madras, Chennai, India, 1993
- Master's degree in Software Engineering, APTECH Computer Education, Mumbai, India, 1996

Professional Development Training

- PowerShell v2 Essentials – Basic PowerShell commands for administrators - April 2011
- CA SiteMinder r12 Core 200 – February 2010

Certifications

- Microsoft Certified Solutions Associate – Windows Server 2008
- MCITP: Server & Enterprise Administrator Windows Server 2008
- Microsoft Certified Systems Engineer MCSE (NT 4.0, 2000, and 2003)
- Microsoft Certified Database Administrator (MCDBA)
- Microsoft Certified Systems Administrator (MCSA): Messaging
- Certified CA SiteMinder r12 Administrator
- Certified CA SiteMinder r12 Professional
- Certified in ITIL V3 Foundation
- Nortel Networks Certified Account Specialist, Enterprise Solutions – Data

This page intentionally left blank.

UNIX Administrator

This page intentionally left blank.

UNISYS

INFO-MATRIX CORPORATION

Resource 100

UNIX Administrator

Key Skills and Knowledge

- General Systems and Network Administration
- Detailed Technical Writing and Documentation
- CheckPoint FireWall-1, FloodGate-1, WebSense
- Development of Training Classes and Seminars
- Sun/Veritas Volume Managers and ZFS
- Solaris Zones, LDAP, Veritas NetBackup
- Sun Certified Systems Engineer
- WebSense Certified Engineer
- RSA Certified Engineer
- Veritas NetBackup Certified Engineer
- Languages: Perl, C, Shell Scripting: Bourne, Csh, Tcsh, Zsh, Bash, Korn, Ash, and Rsh
- Operating Systems: Sun Solaris, Linux, BSDI, HP/UX, Irix/operating system, VMS, Windows, VMware
- Databases: Oracle, MySQL, PostgreSQL
- Emulation: Xterm, SSH Client, tn3270, PuTTY, RUMBA, ZOC, PASSPORT
- Troubleshooting Specialist: Hardware/Software diagnostics Special-Case solutions provider Network Throughput Issues
- Applications: DHCP, DNS, NIS/NIS+, NFS, SSH, HTTP, FTP, Check Point Firewall-1, WebSense, Cisco Network Registrar, Cisco, Lantronix, Apache/Sun Web Servers, Tomcat, JBoss, Java
- Tools: Jumpstart, Veritas NetBackup, LOM, ALOM, ILOM, SecurID ACE/Server, Veritas and Sun Volume Managers, Sendmail, Imap, PGP, Check Point FireWall-1 and FloodGate-1, WebSense Enterprise
- Professional Affiliations:
- Sun Microsystems, Inc. and its affiliates

Professional Summary

Numerous years of professional experience with advanced expertise in the areas of systems administration and integration, and security consultation with skills that include extensive technical writing and documentation. Experienced professional with excellent communication skills, capable of independent work as well as team-based and cooperative ventures; delivers required technical writing of customized user guides and briefs for in-house and third-party applications, documentation to record research and results of systemic issues that included root cause, warning signs, and proactive measures.

- General Systems and Network Administration
- Detailed Technical Writing and Documentation
- CheckPoint FireWall-1, FloodGate-1, WebSense
- Development of Training Classes and Seminars
- Sun/Veritas Volume Managers and ZFS
- Solaris Zones, LDAP, Veritas NetBackup

Employment History and Related Experience

The Vanguard Group, Tech Ops: WAS and UNIX Administrator Services, 2008 - Present

UNIX Technical Services (UTS) Tier-3 support. Duties included daily systems administrative projects and mid- to large-scale enterprise-wide projects. Provided additional support to Tier-2 personnel. Documented new projects such as the seven-month enterprise-wide upgrade of NetBackup. Prepared and maintained system-run books.

Specific work included:

- Solaris Zones, ZFS, Veritas and Sun Volume Managers, Flash Archives, installation of new software, software upgrades, patch installations, general maintenance, JumpStart, LDAP, NetBackup Administration, and general troubleshooting.

Perfect Order, Inc., Comcast Interactive Media Group, Senior Consultant, 2006 – 2007

Systems administration including LDAP/Samba support, Solaris Zones, ZFS, major projects included: Ziddio, Game Invasion, Xanadu, and Milhouse that depended on Apache, Tomcat, JBoss, and Java. Installation and maintenance of software packages, installation of hardware components, troubleshooting and monitoring of services, research of new technologies. Documented all projects, prepared and maintained system run books.

UNIX Administrator

- USENIX, SAGE, SANS, CERT, AUCERT

Comcast Interactive Media Group, System Admin, University of Rochester, 2005 – 2006

Installation and configuration of a dual-server Cisco CNR configuration, planning and deployment, and prepared technical documentation to support the administrators, staff, and students. Prepared run books for each system. Ongoing support of the CNR system for the calendar year.

Comcast Interactive Media Group, System Admin, 2006 to 2006

Systems administration and assistance with LDAP server user population, and research of methodologies supporting NAS authentication mechanism, deployment of systems at Inflow. Documented research results.

Comcast Interactive Media Group, Urban Outfitters, Network Administrator, 2006 to 2006

Configured new IP addresses, netmasks, and default gateways on four V440 systems. Installed a dual HBA on the database server and connected a StorEdge C2 Autoloader. Installed, configured, and tested NetBackup 6.0 on the database server, configured initial full and incremental backup schedules. Prepared a Technical Brief for System Administrators.

Comcast Interactive Media Group, Certanteed, Philadelphia, 2006 to 2006

Worked with personnel in planning a Disaster Recovery test for Certainteed scheduled at Sun Guard, documented all procedures and prepared a project summary to the project leads. Provided support for disk space problems on production database servers.

Comcast Interactive Media Group, Philhaven, 2006 to 2006

Installed, configured, and tested NetBackup 6.0 and the Oracle Agent on the production database server. Prepared initial run book and wrote technical briefs to assist administrators in daily operations.

Comcast Interactive Media Group, Case New Holland, 2006 to 2006

Configured and deployed secure host-based SSH file transfers between UNIX systems and developed and documented a plan for extending the same technology to PC-based systems.

Comcast Interactive Media Group, 2006 to 2006

Performed systems administration duties and documented the development infrastructure.

CNR/BACC Training Development, September 2005 –- March 2006

Collaborated with CNR Team to develop a three-day course for Cisco Systems. Built a test laboratory to support The University of Rochester's CNR server pair. ocumented progress of project.

Resource 100

UNIX Administrator

School District of Philadelphia, June 1999 – August 2005

Systems administration, installation, configuration, management, and maintenance of over seventy Solaris systems on a variety of platforms

- Sunfire 6800/Hitachi 9960, V880, V240, V120, Netra, E450, E250, E420, E220, assisted SDP staff with projects, supplied user support for SDP Community.
- ISC BIND DNS Services, ISC and NetID DHCP Services, Check Point Firewall-1, WebSense Enterprise Server, IP Telephony Services deployment at SDP Headquarters
- Enterprise-wide NetBackup, Sun Java Enterprise Systems LDAP Services, Sendmail, Annex ERPCD Authentication Services for Dial-Up Modem Pool, Jumpstart.
- Wrote customized Perl and Shell scripts required to accomplish repeated tasks.

Temple University, Senior IT Technical Staff, 1998 to 1999

November 1989 – May 1998

Performed daily System Administrative tasks that included software installations and maintenance, operating system installation, patching and maintenance, system and network troubleshooting, security services that included intrusion detection, auditing, technical documentation, and the development of proactive methods to mitigate illicit intrusions targeting the University's systems and networks.

Education

- BA in Computer Information Sciences, Minor in Mathematics, Temple University, 1989

Certifications

- Sun Certified Systems Engineer
- WebSense Certified Engineer
- RSA Certified Engineer
- Veritas NetBackup Certified Engineer

This page intentionally left blank.

UNISYS

INFO-MATRIX CORPORATION

Resource 101

UNIX Administrator

Key Skills and Knowledge

- Data center planning and administration. Space, power, cooling.
- Data center infrastructure management (DCIM) tools and administration. Facilities management and monitoring tools.
- Disaster recovery planning and administration.
- UNIX / Linux administration and scripting
- UNIX / Linux monitoring – Nagios
- UNIX / Linux security – User ID management, sudo, Access Control
- Apache and IIS administration
- Windows administration
- Website analytics deployment and analysis – includes WebTrends, Google Analytics, Omniture, Urchin. Incudes both raw log file analysis and javascript based code tracking
- Website monitoring
- NetBackup / Veritas monitoring and administration

Professional Summary

A leader with 7+ years of experience in the modernization of business processes and reporting through the use of technology. A self-motivated individual with a strong talent for understanding complex information relationships and with an ability to communicate to business partners in both technical and business terms. An extensive record of successfully leading cross-functional projects by drawing upon emotional intelligence, problem-solving and interpersonal skills.

Employment History and Related Experience

John Wiley & Sons, Inc., Lead Systems Hosting Resource Analyst, 2003 to Present

Lead technical resource for data center operations, expansions, maintenance, and planning. Project Lead on integrating Foreseer power management monitoring to pro-actively manages company-wide mission-critical infrastructure equipment, including power, environmental, and life/safety devices.

- Implementation of modern data center power and management systems; reduced hosting costs by phasing out legacy equipment and connections
- Responsible for Data Center work flow migration and management. This includes coordination of all maintenance work: dealing with UPS, PDU, AC units (CRAC, RTU, etc.), and integrating the services of electricians and other outside contractors.
- Implementation and management of DCIM tools for strategic data center consolidation and off site hosting
- Hosting Resource duties include day-to-day operations of the Data Center, power management for all devices, cooling needs, and the layout and planning of the room.
- Key Member of the UNIX Security Team controlling access to all Wiley UNIX and Linux systems; This includes monitoring UNIX hardware; Standardized setup across all UNIX systems.
- Apache webserver configuration in the UNIX and Linux environments.
- Responsible for ServerVantage reporting and analysis on all Wiley UNIX and Linux hardware; Project Lead for migrations and upgrades.
- Veritas Backup Reporter for determining that our backups were timely, accurate and complete Driver in the IBM audit on all UNIX servers
- Team Lead analyzing and presenting Wiley traffic statistics and patterns for all Wiley Web sites worldwide; incorporated Webtrends, SmartSource, Keynote Systems and Akamai software, processes and

protocols to create a complete picture of Wiley's Web presence, bandwidth usage, and next generation Web site tracking. Introduced smart tagging of Web sites, e.g., Google Analytics

- Responsibilities for Sarbanes-Oxley compliance

Johnson & Johnson, Network Technician, Raritan, NJ, 2001 – 2002

PRD Raritan campus PC technical support team responsible for software troubleshooting and upgrades; included both standard software such as Microsoft Office and Windows along with industry specific pharmaceutical programs.

- Internal portal Web site development and handoff to permanent staff
- Technical writing for SOP documentation for business departments
- Coordination and implementation of software to gain compliance with FDA regulations; included proof of concept testing, final deployment, and user training

Education

Rutgers University, New Brunswick, NJ – Bachelor of Science
(Simultaneous Majors)

- 1st Major: Computer Science
- 2nd Major: Economics

UNISYS

INFO-MATRIX CORPORATION

Resource 102

UNIX Administrator

Key Skills and Knowledge

- Certified system administrator
- DoD TS Security Clearance with SSBI
- CompTIA Linux +
- CompTIA Security +
- DODD 8570 Certified
- LPIC-1 from the Linux Professional Institute
- Novell Certified Linux Administrator
- Oracle Solaris 10
- Fedora Linux
- Oracle Virtual Box
- Red Hat Linux (RHCT), RH033 and RH133
- VPN
- UNIX/Linux Administration
- AIX Administration
- AS/400, NIS, LDAP
- Microsoft Server 2003
- Cisco Routers
- System upgrades
- Back-ups and recovery
- Microsoft Office Suite (2007/2010)
- Remedy
- Windows operating system

Professional Summary

Certified system administrator with over 10 years of IT administration experience. Experienced with DoD Security standards as well as a certified Linux Administrator.

Employment History and Related Experience

Fleet Numerical Meteorology and Oceanography Center, *System Administrator,* Monterey, CA, 2012 -2012

Systems Administrator supporting Red Hat, SUSE, Solaris 10, CFengine Nova.

Tecport Solutions, *UNIX Administrator (Contractor)* Harrisburg, PA, 2011 – 2012

Perform routine tasks including file editing using UNIX commands/utilities. Assisted in the Development of a Forensic Data Recovery Lab. Training on Department of Defense Standards

- Process security functions including user creation and password setting
- Fedora (15, 16), SUSE 12, Solaris 11 open source training
- Environment: UNIX, Fedora, Solaris, SUSE

Department of Defense*, Solaris / RHEL Administrator (Contractor),* Mechanicsburg, PA, 2011 – 2011

Shadowed the "BladeLogic" system to administer Naval Servers. Enforced DOD security standards, i.e.: secure user account creation and password management. Extensive use of VPN connections to classified data. Provided SPARC systems support.

- Provided Solaris system administration, operational support and problem resolution
- Environment: Linux/UNIX, Solaris, LDAP, NIS, Backups/Recovery, VPN

UPS Supply Chain Solutions, *Computer Operator/System Administrator,* Lititz, PA, 2000 – 2010

Managed computer room on second shift. Offered cloud computing and administration to our pharmaceutical client base in a Linux and Windows environment. Operated and maintained AIX, Microsoft Server 2003 and AS/400, 620 operating systems

- Responsible for: Brocades, Telnet, SSH, VMware, Cisco routers, VPN concentrators, Fiber, Ethernet, and cable connections; Maintained each server's availability and backup

Resource 102

UNIX Administrator

- Monitored logistics management system, including order management and warehouse management
- Updated log books of operating records for equipment and recorded all malfunctions and errors
- Analyzed console instructions, queries, error messages, machine malfunctions, stops, schedules, programs, and control language information to determine proper operating procedures
- Installed software, patches, upgrades, applications, and hardware
- Environment: Linux/UNIX, AIX, Windows, VMware, VPN, Servers, Cisco Routers

Livingston Health Care, IT Operator, Lititz, PA, 1999 – 2000

Managed 2nd shift of a 24/7 technical support operations for health care clients

United States Army, *Mechanized Infantry,* 1997 - 1999

Driver of M2A2 Bradley Fighting Vehicle. Maintained a safe and operationally functioning vehicle to support mechanical infantry mission One-year deployment in Kuwait.

Education

Harrisburg Area Community College, Lancaster, PA, Criminal Justice, 27 credits

Certifications

- DoD TS Security Clearance with SSBI
- CompTIA Linux +, CompTIA Security + . DODD 8570 Certified
- LPIC-1 from the Linux Professional Institute
- Novell Certified Linux Administrator

UNISYS

e&e IT Consulting Services, Inc.

Resource 103

UNIX Administrator

Key Skills and Knowledge

- Developed a multi-threaded Java application to move data from Oracle to DB2 utilizing JDBC, JMX, LOG4J, JDOM and Java Mail technologies
- Performed z/operating system UNIX System Services administration
- Provided support for security related aspects of z/operating system UNIX Systems Services and TCP/IP
- Maintained DB2, Java and WebSphere z/operating system products with SMP/E
- Developed software using VS COBOL II, MVS/Assembler, COOL:Enterprize, Borland C/C++, Smalltalk/V, Micro Focus COBOL and SQL
- Developed tools that interact with COOL:Enterprize and COOL:Gen Development products

Professional Summary

14 years of experience delivering database management, systems administration, and network engineering. Installed and configured DB2 on Linux, UNIX, Windows and z/operating system, configured and deployed SQLJ Java Stored Procedures, conducted DB2 Performance tuning at system and application levels. Developed, implemented and successfully executed DB2 disaster recovery plan.

- Supported development team with hardware/software technology
- Generated utilities, training and standards to aid development staff
- Provided recommendations for application design and problem resolution.
- Reviewed applications for technical feasibility, performance and standards adherence
- Analyzed and documented business applications

Employment History and Related Experience

First Data Merchant Services, Systems DBA, Web Administrator, Hagerstown, MD, 1999 – Present

Installed and configured DB2 on Linux, UNIX, Windows and z/operating system, configured and deployed SQLJ Java Stored Procedures, conducted DB2 Performance tuning. Maintained Unicode Service for z/operating system to support DB2 V8 functionality, developed, implemented and successfully executed DB2 disaster recovery plan.

- Installed IBM WebSphere on Linux, UNIX, Windows and z/operating system
- Supported HTML, XML, JSP and Java development
- Installed and maintained Java for Linux, UNIX, Windows and z/operating system
- Conducted performance tuning and problem analysis of stand-alone Java applications, WebSphere and JRun utilizing Wily Introscope and IBM JVM dumps/traces
- Developed Java application for UNIX, Windows and z/operating system platforms
- Developed a multi-threaded Java application to move data from Oracle to DB2 utilizing JDBC, JMX, LOG4J, JDOM and Java Mail technologies, performed z/operating system UNIX System Services administration
- Provided support for security related aspects of z/operating system UNIX Systems Services and TCP/IP
- Maintained DB2, Java and WebSphere z/operating system products with SMP/E
- Developed a working knowledge of security implementation on Linux, UNIX, Windows and z/operating system

e&e IT Consulting Services, Inc.

Resource 103

UNIX Administrator

ObjectWare, Inc, Systems Developer, San Francisco, CA 1997 to 1999

Configured and maintained Windows, operating system/2 and Linux and operating system/390 Web, FTP and Networking configurations. Configured and administered database for DB2 V5, DB2 UDB, Oracle 8 and SQLServer Configured communications using ORACLE SQLNet, DDF using SNA/VTAM, ODBC and TCP/IP

- Programmed systems for IBM P/390 system running operating system/390
- Developed tools that interact with COOL:Enterprize and COOL:Gen Development products
- Acted as project leader and developer for Reverse Engineering products
- Developed applications in Smalltalk and C/C++ that utilize data from DB2, Oracle

PHEAA, System Analyst, Harrisburg, PA, 1989 to 1997

Assisted development team with hardware/software technology, developed utilities, training and standards to aid development staff, and provided recommendations for application design and problem resolution.

- Reviewed applications for technical feasibility, performance and standards adherence
- Analyzed and documented business applications
- Developed software using VS COBOL II, MVS/Assembler, COOL:Enterprize, Borland C/C++, Smalltalk/V, Micro Focus COBOL and SQL

Accounting Services, Consultant, York, PA, 1994 – Present

Self Employed, Installed hardware and software installation & Configured networks, provide client support.

Education and Training

- IBM Certified Solutions Expert – DB2 UDB V7.1 Database Administration, 2004
- IBM Learning Services Administration of WebSphere 5.0 for AIX Training, 2004
- IBM Professional Services - DB2 Net.Data and WebSphere Application Server, 2000
- IBM Professional Services Education - DB2 Fundamentals and SQL workshop, 1991
- School of Computer Technology, Certificate of Computer Information Systems, 1988

UNISYS

IBM

Resource 104

UNIX Administrator

Key Skills and Knowledge

- AIX/UNIX/VIO System Administration & Security Management
- Enterprise Storage and SAN Administration
- Scripting… task automation, data gathering, status monitoring, process efficiencies

Professional Summary

An IT Specialist with IBM Global Technology Services and integral member of the IT Infrastructure Management team serving the Commonwealth of Pennsylvania's Liquor Control Board (PLCB) environment. Over sixteen years of UNIX system administration experience in realms ranging from task automation to filesystem management to operating system support to implementing and optimizing virtualization. A proven track record of successful project deliveries, savvy problem-solving, creative script solutions, leadership in storage planning/utilization/management. Expertise in maintaining, deploying, and monitoring the enterprise storage system and it's fault-tolerant, highly-customizable SAN connectivity to UNIX servers.

Employment History and Related Experience

Commonwealth of Pennsylvania – MSP/LCB, IT Specialist, Harrisburg, Pennsylvania, 2003-To Date

Designed and automated a DS8300 FlashCopy® monitoring scheme with various scripts and command files that report daily backup copying status. In addition to validating logged results, a summary note is sent to storage admins and Site Operators every night. I duplicated the process for XIV snapshots after the customer moved some production LPARs to XIV storage.

- Supported the EBS Environment Oracle Upgrade, migrated all the Oracle Application directories to a mounted file system. Wrote scripts that collected the sub-directory names and sizes across the servers, ported that info into a spreadsheet and calculated required LUNs (quantities & sizes) to accommodate space requirements.
- Performing the role of AIX security focal, led our team through numerous IBM audits and assessments - passing all; and most with times with 0 defects.
- Developed a script solution to accurately and quickly capture/rebuild AIX file system "containers". One script captures all the current values, settings, & options related to the AIX file systems; the other script uses that info to generate the AIX commands to recreate the same file system with all the same characteristics vastly improving the efficiency of the procedure.

Education

- Watson School of Engineering, Applied Science, and Technology
  - In conjunction with State University of New York - Binghamton, New York
  - IBM Homestead Programmer Retraining Certificate (completed 9 undergraduate courses)
- University of Vermont, Continuing Education (Non-Degree)
- Electronics Institute of Harrisburg - Harrisburg, Pennsylvania
- Associates Degree in Electronics & Computer Technology

This page intentionally left blank.

UNISYS

UNIX Administrator

Key Skills and Knowledge

- Hardware Upgrade and Repair
- Linux - RHEL, SLES, OEL
- RHEL 5.X Server Builds from Scratch
- RHEL 6 Support
- RHEL 6 Server Builds from Scratch
- RHN Satellite Implementation
- AIX – 4,5,6,7
- PowerVM – Power5, Power6, Power7
- PowerHA – 5,6,7
- Project and Program Management
- Communication and Networking
- Databases
- Hardware
- Operating Systems
- Software/System Architecture
- Technical Documentation
- Systems Development Life Cycle
- ITIL/ITSM
- Korn/Bash Shell Scripting
- UCMS – Unemployment Compensation Management System
- SWIF – State Workers Insurance Fund
- BWC – Bureau of Workers Compensation
- Avamar
- NetBackup
- BladeLogic

Professional Summary

Manages operations of AIX and Linux systems in the Data PowerHouse data center for the Commonwealth. This included server deployments through various processes, PowerHA configuration, user requests, operating system level migrations and patching. This also includes management of VIO servers, HMCs and VMware Virtual Center as it pertains to VM Linux systems.

- Managed BladeLogic repository for Linux patching across various Linux platforms including RHEL, SLES, and OEL
- Developed scripts as needed to maintain a consistent environment across the entire data center.
- Participate in all Disaster Recovery planning and testing.
- Gathering customer requirements for recovery of various application and database servers
- Developing the best recovery method of rootvg and non-rootvg as well as customer data
- Execute recovery exercises and ensured consistent support to the customer as they proceed with their testing of the recovered systems.

Employment History and Related Experience

UNISYS, Commonwealth of Pennsylvania Data PowerHouse Project, 2011 – current

- UNIX Administrator responsible for the management and maintenance of all AIX and Linux servers. Active ITIL v3 certification, Participant in successful disaster recovery testing.

Department of Labor and Industry – DLI project

- UCMS – Unemployment Compensation Management System – Integral part of the System Administration refresh team for AIX support. Built the new operating system image on the updated platforms, worked with IBM experts on performance tuning, ground up installation of all IBM Power hardware including SAN and Network cable installation (Ethernet and fiber), frame mapping of physical devices to ensure redundancy, stability, and performance, of the systems. Worked with IBM experts on installing the most advanced VIO servers built for solid redundancy (tested and confirmed) as well as PowerHA clusters that would ensure the application and files were available with the least amount of downtime for a smooth transition. Worked with the various business partners: DBAs, Application Developers, Network, SAN/TSM, Windows Administrators for performance testing, process flow, etc.
- Tivoli Monitoring/Network Support – These two particular groups of business partners wanted to dive into RedHat Enterprise Linux servers

UNISYS

UNIX Administrator

as the hosting operating system for their applications. Worked exclusively on building a solid RHEL 5.X image that would meet/exceed the application requirements for virtualization, security, and stability. The systems were primarily Virtual Machines (VM) however there were a few that ran on Intel X86 physical servers.

- RedHat Network Satellite (RHN Satellite) – As part of a growing RHEL environment it was critical to develop and maintain a central management point. An investment was made in the RHN Satellite product for patching and maintaining a base line platform for any RHEL system. As part of the install team, I set up the central satellite server, setup the database and register/connected all clients to their appropriate patching cycle. Working with the owners of the various RHEL clients, we established the most effective patching cycle for their systems and ensured all systems were current and met the standards needed as set forth by OA.
- BWC – Bureau of Workers Compensation – Directly involved in upgrade field office servers from AIX 5.3 to AIX 6.1, PowerHA to the most current supported levels in PowerHA 6.1, and worked with the extended AIX support team to execute the disaster recovery plan when an upgrade did not go as planned. This involved restoring the server image from a sysback image on tape.
- SWIF – State Workers Insurance Fund – Deeply involved in supporting their PowerHA systems were solid and the customer had a level of confidence in the failover of the clusters. Solely supported the installation and upgrade maintenance of Dollar Universe application. Although there was an application team dedicated to the day to day work of Dollar U, the team did not have the AIX experience and administrator access needed to perform much of their work.

Integrated Enterprise System – IES Project

- AIX 5.3 to AIX 7.1 migration – Developed the migration plan needed to move from AIX 5.3 to AIX 7.1 to ensure the least amount of down time possible for the customer. Alt-disk install was the method chosen. I was responsible for scheduling all of the systems in various maintenance windows to ensure accurate time for testing and meeting the requirement for a phased approach of implementation.
- Device Driver upgrade – to ensure accurate connections to Avamar, the backup solution for IES, worked with the application team to upgrade the driver packages.
- Streamlined mksysb implementation – The system mksysb process was antiquated at best. Based on past experience and the need for an extra layer of protection, a new mksysb creation/storage process was created to ensure redundancy of the backup images and to further enhance the availability of these images for Disaster Recovery.

UNISYS

UNIX Administrator

- Disaster Recovery Testing – Yearly disaster recovery testing is done to ensure the application's availability should a disaster occur. As part of the DR team, I worked extreme hours to build, restore and configure 30+ AIX LPARs to meet the current production environment as well as worked with the customer to correct minor issues during their database restores and testing process.

Department of Revenue – DOR Project

- AIX 5.3 to AIX 7.1 migration – Developed the migration plan needed to move from AIX 5.3 to AIX 7.1 to ensure the least amount of down time possible for the customer. Alt-disk install was the method chosen. I was responsible for scheduling all of the systems in various maintenance windows to ensure accurate time for testing and meeting the requirement for a phased approach of implementation.
- Device Driver upgrade – to ensure accurate connections to Avamar, the backup solution for IES, worked with the application team to upgrade the driver packages.
- Streamlined mksysb implementation – The system mksysb process was antiquated at best. Based on past experience and the need for an extra layer of protection, a new mksysb creation/storage process was created to ensure redundancy of the backup images and to further enhance the availability of these images for Disaster Recovery.
- Disaster Recovery Testing – Yearly disaster recovery testing is done to ensure the application's availability should a disaster occur. As part of the DR team, I worked extreme hours to build, restore and configure 30+ AIX LPARs to meet the current production environment as well as worked with the customer to correct minor issues during their database restores and testing process.

Pennsylvania Liquor Control Board – PLCB Project

- Integrated Business Management System (IBMS) Project – The agency was refreshing their application and took the opportunity to change operating systems in the process. RedHat Enterprise Linux (RHEL) was chosen as the platform. My role in the project has been to develop a stable 5.X RHEL operating system image and deploy servers to the agency as needed based on the given build requirements. These systems are all Virtual Machines (VM) and maintain the required level of security, with room to grow as the environment changes.
- BladeLogic - The current patching option for the RHEL systems is BladeLogic. I have developed the needed channels to connect the servers to the appropriate patches based on operating system level. Patch cycles are being established based on environment level (UAT, PRD) to ensure testing between cycles and make sure production stability.

UNISYS

UNIX Administrator

Department of Environmental Projection – DEP Project

- Oracle Enterprise Linux – OEL – This environment is comprised of approximately five Oracle Enterprise Linux (OEL) systems with the opportunity for expansion. The environment was a migration from Solaris to Linux and we continue to support this environment on a day to day business as they work through the growing pains of supporting their application(s) on a new operating system. Day to day work includes file system expansion, security monitoring and tuning, and storage and performance monitoring.

Employment History and Related Experience

Unisys, 2011 - Current

Commonwealth of Pennsylvania, Department of Labor and Industry, 2009 - 2011

Foot Locker, Inc., 2004 - 2009

York Technical Institute, 2002 - 2004

Education

Central Pennsylvania College Network Management and Cyber Security

Summerdale, Pennsylvania July 2005 – Fall 2008

Bachelors of Science Graduation date: December 2008

Deans List Each Semester in Attendance Final GPA: 3.88

York Technical Institute Computer Systems Specialist

York, Pennsylvania July 2002 – May 2004

Associate in Specialized Business Graduation date: May 2004

Student of the Term: Fall Term GPA: 3.75

Professional Certification

- CompTIA Net+ Certification – 2003
- ITIL v3 Foundation – 2012
- IBM AIX Certified System Administrator – AIX 7.1 2012

UNISYS

INFO-MATRIX CORPORATION

Resource 105

UNIX Administrator

Key Skills and Knowledge

- Extensive experience in UNIX System Administration
- Oracle Solaris UNIX 8, Oracle Solaris UNIX 10, Red Hat Enterprise Linux Advanced Server 3, Red Hat Enterprise Linux Advanced Server 4, Red Hat Linux 2.2.14, Red Hat Linux 3.2
- HP ProLiant (DL 385 G1, DL 585 G1),
- SunFire T2000, T5220, V440, V490, V890, 280R, 480R, 4800, 6800, E2900, E4900
- Sun Enterprise 3000, 4000, 4500, 6500,
- Sun Ultra (1,2,5),
- Cyclades TS2000 Console Server, Proofpoint P-800 Mail Filter
- F5 Big-IP
- Perl, SQL, Shell Scripting
- JCL, HTML, J2EE, XML
- CA (eTrust Access Control, Wily Introscope, SiteMinder Web Access Manager)
- Vertias (Volume Manager 6.1, NetBackup)

Professional Summary

Mr. Reesman possess eight + years of IT experience with special emphasis on UNIX systems administration over the past 6 years.

- Created usage metrics and breakdown reports for management of the SFG application
- Created new file transfers for various government entities utilizing Perl and the Bash Shell scripting languages
- Managed user security, public/private keys, and security of the SFG and Control-M applications
- Received 'Passion Award' on August 20, 2012 from Craig Technologies for implementation of SSH capabilities on a server which allowed for secure transmission of file transfers for a high profile client
- Utilized Veritas Volume Manager and Sun Volume Manager for administration of server storage
- Point of contact for Veritas NetBackup application troubleshooting and file system restores
- Conducted disaster recovery tests twice a year with various application teams for testing of various internal and external served client applications
- Utilized UNIX shell scripting along with PERL to gather server and application information
- Performed Server maintenance including software upgrades, patch maintenance, hardware replacements
- Supported IBM WebSphere Application Server and Sun One Web Server on a 24x7 basis

Employment History and Related Experience

Craig Technologies, Defense Information Services Agency, Application Support/UNIX Systems Administrator, 2011 – Present

Responsible for the administration and development for the Secure File Gateway custom application which handles close to 25,000 file transfers daily between various Federal Government Agencies and other business entities. Responsible for the administration of the BMC Control-M job control and scheduling application

- Created usage metrics and breakdown reports for management of the SFG application
- Created new file transfers for various government entities utilizing Perl and the Bash Shell scripting languages
- Managed user security, public/private keys, and security of the SFG and Control-M applications

- Sun Solaris (Cluster 3.1, Volume Manager),
- IBM (WebSphere 5, WebSphere 6.0, WebSphere 6.1, WebSphere Portal 6.1
- Tivoli Enterprise Console, MQ Series Messaging
- Tivoli Enterprise Console)
- Peregrine ServiceCenter,
- Sun One WebServer 6, BMC (Control-M batch scheduling, Performance Manager)
- Kerberos, Samba, Postini Mail Filter,
- TeamQuest IT Service Analyzer, HP SiteScope, HP OpenView ITO, Sendmail Mail Transfer Agent, Oracle (9, 10), Sybase, DB2, IBM Tivoli Workload Scheduler,
- TCP/IP, MQ/Series, DNS, DHCP, FTP, SFTP, SSH

- Received 'Passion Award' on August 20, 2012 from Craig Technologies for implementation of SSH capabilities on a server which allowed for secure transmission of file transfers for a high profile client

TE Connectivity, Application Deployment/UNIX Systems Administrator, Harrisburg, PA, 2008 – 2011

Responsible for the deployment of 36 applications and their updates to the Solaris 10 Operating System in the development, quality assurance, and production environments. Created project plans for weekend deployment and maintenance activities. Monitored various systems management consoles to recognize problem events, and reacting appropriately

- Created automated schedules for shutting down and starting up applications and components
- Created shell scripts to start up tomcat application and apache Web servers
- Managed all of the general infrastructure information relating to 10 enterprise level applications
- Managed user security, security of various Solaris servers, and implementing audit security policies

The Vanguard Group, UNIX/Linux Systems Administrator Valley Forge, PA 2006 – 2008

Single point of contact for all Sun Solaris UNIX, Red Hat Linux, Sybase, Oracle, and net-centric related problems. Monitored various systems management consoles to recognize problem events, and reacting appropriately. Performed various Oracle and Sybase database administration including troubleshooting and adding storage

- Utilized Veritas Volume Manager and Sun Volume Manager for administration of server storage
- Point of contact for Veritas NetBackup application troubleshooting and filesystem restores
- Conduct disaster recovery tests twice a year with various application teams for testing of various internal and external served client applications
- Utilized UNIX shell scripting along with PERL to gather server and application information
- Performed Server maintenance including software upgrades, patch maintenance, hardware replacements
- Supported IBM WebSphere Application Server and Sun One Web Server on a 24x7 basis

The Vanguard Group, Voice Telecommunications Analyst, Valley Forge, PA, 2006 – 2006

Performed backups and restores of call recordings using the NICE call

recording system; managed truck groups using the Avaya site administrator software; added call groups for recording using the NICE call recording software

The Vanguard Group, Electronic Data Interchange Analyst, Valley Forge, PA, 2005- 2006

Responsible for the development, implementation, maintenance, and 24x7 production support of data transmissions between vanguard and external clients. Managed file transmissions through FTP or RemoteWare dial-up.

- Analyzed problems with incoming files and corrected errors to ensure proper transmission
- Managed project of transitioning over 10000 processes to a new software system to handle transmissions more efficiently

Pennsylvania Army National Guard, Database and Network Administrator Annville, PA, 2000-2006

Performed various database administration duties served in Operation Enduring Freedom, received 'Soldier of the cycle award' on August 10, 2001 for 'demonstrated leadership among your peers during advanced individual training

Select Medical Corporation, Intranet and Web Design, Mechanicsburg, PA, 2004- 2004

Designed an Intranet for the outpatient IT department, developed a way for standard documents to be served to various outpatient offices, and created a database for patients in Lotus Notes that let patients schedule appointments with their doctor in a seamless manner

Education

- Drexel University, Philadelphia, PA, M.S. Information Systems, in progress, graduation 2016
- The Pennsylvania State University, B.S. Information Sciences and Technology, 2005
- Cisco Networking Academy Semester, Lebanon Career Technology Center, 2000

This page intentionally left blank.

UNISYS

IBM

Resource 106

UNIX Administrator

Key Skills and Knowledge

- Linux on z/Series system administrator
- z/VM systems programming
- z/VSE systems programming

Professional Summary

Experienced system administrator for Linux on System z. Provided z/VM and z/VSE systems programming support.

Employment History and Related Experience

IBM Global Technology Services, Commonwealth of Pennsylvania DPH, Technical Services Professional, 2007-To Date

Provide Linux on z/Series system administrator support on over 80 Linux guests running under z/VM for PA Department of Transportation. Significant accomplishments during this time include SLES 9 to SLES 10 upgrade and a subsequent SLES 10 to SLES 11 Upgrade, a processor upgrade, and a DASD migration.

IBM Global Technology Services, Commonwealth of Pennsylvania DPH, Technical Services Professional, 2000-2007

Provided z/VM and z/VSE systems programming support to the PA Department of Corrections and PA Liquor Control Board. Major accomplishments included several z/VM and z/VSE operating system upgrades and various processor and DASD migrations.

IBM Global Services, Commonwealth of Pennsylvania, Information Technology Specialist, 1992-2000

Provided z/VM and z/VSE systems programming support to various commonwealth agencies including the PA Department of Corrections, PA Liquor Control Board, PA Department of Health, PA Turnpike Commission, and PA Treasury, as well as several legislative caucuses. Major accomplishments included z/VM and z/VSE operating system upgrades and various processor and DASD migrations as well as business as usual system programmer activities.

IBM Professional Services, Commonwealth of Pennsylvania, 1989-1992

Provided VSE/VTAM telecommunications support during the PLCB Point of Sale application roll-out to the state liquor stores.

This page intentionally left blank.

UNISYS

Resource 35

UNIX Administrator

Key Skills and Knowledge

- AIX 4,5,6,7
- Power Systems
- VIO
- HMC
- Red Hat Enterprise Linux
- Oracle Enterprise Linux
- SuSE Linux
- Windows
- Scripting
- Networking
- Supervision
- Project Management

Professional Summary

Skillful system administrator with a wide range of experience with Commonwealth projects. He has a total of 13 years system analysis experience with 7 years of Commonwealth experience. He is skilled in data recovery, migrations, implementations, maintenance, and network management.

- Operating Systems: AIX4, 5, 6, 7. Red Hat Enterprise Linux. Oracle Enterprise Linux. SuSE Linux. Windows NT/2000/2003/2008. All Windows Desktop Operating Systems.
- Hardware: IBM stand-alone and IBM P-series servers. IBM Hardware Management Consoles.
- Software: Apache, Samba, VMware, Perl, VBscript, PowerShell, UNIX/Linux Shell Scripting, Oracle RAC clustering. PowerHA clustering.

Employment History and Related Experience

Unisys, Senior UNIX Administrator, Harrisburg, PA, 2005 – Current

Responsible for the day to day management of all AIX and Linux systems in the Data PowerHouse data center for various Commonwealth agencies. This included server deployments through various processes, PowerHA configuration, user requests, operating system level migrations and patching.

- Managed BladeLogic repository for Linux patching across various Linux platforms including RHEL, SLES, and OEL.
- Developed scripts as needed to maintain a consistent environment across the entire data center.
- Participate in all Disaster Recovery planning and testing. This included gathering customer requirements for recovery of various application and database servers, developing the best recovery method of rootvg and non-rootvg as well as customer data, execute recovery exercises and ensured consistent support to the customer as they proceed with their testing of the recovered systems.
- Unemployment Compensation Management System – Built the new operating system image on the updated platforms, worked with IBM experts on performance tuning, ground up installation of all IBM Power hardware including SAN and Network cable installation (Ethernet and fiber), frame mapping of physical devices to ensure redundancy, stability, and performance, of the systems
- Collaborated with IBM experts to install VIO servers and PowerHA clusters ensuring the application and files were available with the least amount of downtime for a smooth transition
- Supported various business partners: DBAs, Application Developers, Network, SAN/TSM, Windows Administrators for performance testing, process flow, etc.

UNISYS

Resource 35

UNIX Administrator

- Tivoli Monitoring/Network Support –Built a RHEL 5.X image to support application requirements for virtualization, security, and stability from Virtual Machines (VM) and Intel X86 physical servers
- RedHat Network Satellite (RHN Satellite) – Developed RHN Satellite product for patching and maintaining a base line platform for any RHEL system.
- Configured the central satellite server, setup the database and register/connected all clients to their appropriate patching cycle. Working with the owners of the various RHEL clients
- Established the most effective patching cycle for their systems and ensured all systems were current and met the standards needed as set forth by OA
- Bureau of Workers Compensation – Upgraded field office servers from AIX 5.3 to AIX 6.1, PowerHA to the most current supported levels in PowerHA 6.1
- State Workers Insurance Fund – Supported the installation and upgrade maintenance of Dollar Universe application
- Integrated Enterprise System AIX 5.3 to AIX 7.1 migration – Developed and executed the migration plan needed to move from AIX 5.3 to AIX 7.1 to ensure the least amount of down time possible for the customer.
- Streamlined mksysb implementation – Generated a new mksysb creation/storage process to ensure redundancy of the backup images and to further enhance the availability of these images for Disaster Recovery.
- Department of Revenue AIX 5.3 to AIX 7.1 migration – Developed the migration plan needed to move from AIX 5.3 to AIX 7.1 to ensure the least amount of down time possible for the customer; scheduled all of the systems in various maintenance windows to ensure accurate time for testing and meeting the requirement for a phased approach of implementation.
- Disaster Recovery Testing – Accomplished annual disaster recovery testing to ensure the application's availability should a disaster occur; built, restored and configured 30+ AIX LPARs to meet the current production environment
- Maintenance Window Management – This agency has monthly maintenance outage windows. I am responsible for coordinating all of the events in the maintenance window, including communications between other departments within Unisys as well as DOR agency staff
- Pennsylvania Liquor Control Board Integrated Business Management System (IBMS) Project –Develop a stable 5.X RHEL operating system image and deploy servers to the agency as needed based on the given build requirements using Virtual Machines (VM) with the required level of security; accomplished day-to-day maintenance of systems, processing of change requests related to systems, and responding to incidents.
- Department of Environmental Projection Oracle Enterprise Linux – Accomplished day to day work includes file system expansion, security

UNISYS

Resource 35

UNIX Administrator

monitoring and tuning, and storage and performance monitoring.

- Department of Public Welfare Oracle Enterprise Linux – Built and maintained repository, maintenance of other OEL servers and creating new OEL servers as the agency seeks to expand its environment.

Other Work Experience

- Earthlink, UNIX Web Hosting Administrator, 2000 – 2004
- Global Management Services, Chief Technical Officer: 2003 – 2005
- Cross Connect Technologies, Network Engineer, 2002 – 2003
- Keystone Programming, Linux Administrator, 1999 – 2000

Education

- Dauphin County Technical School, Information Technology, 2000

Training

- New Horizons: 1999, 2000
- Microsoft Certified Systems Engineer Training

Certifications

IBM Certified System Administrator – AIX7

ITIL v3

Microsoft Certified Professional

This page intentionally left blank.

UNISYS

Windows Server Administrator

This page intentionally left blank.

UNISYS

Resource 107

Windows Server Administrator

Key Skills and Knowledge

- Domain expertise & solutions
- Communication and networking
- Hardware
- Operating systems
- Software/system architecture
- Call center and help desk
- Office productivity tools
- Technical documentation
- Facilities management
- Quality assurance testing
- Telephone systems
- Cabling

Professional Summary

18 years of IT experience; 16 years of systems administration experience; have been a been Microsoft Certified Professional since 2000.

- CompTIA Security+ Certification
- Knowledge of a wide range of hardware and software
- Experience with all major desktop, server, and mobile operating systems.

Employment History and Related Experience

Unisys Corporation, Commonwealth of Pennsylvania,
Enterprise Systems Support Analyst 2012 – Present

Member of Technical Operation Team – Server. Troubleshoot, builds, and decommission servers.

North American Communications, IT Technician 2011 – 2012

Performed IT-related activities, including hardware, software, and networking.

Digital Solutions, Inc., Field Technician 2009 – 2010

Installed and troubleshot custom telephone systems throughout the USA.

Additional Employment

JJ Powell, Inc.	2008 – 2009
PMG Pennsylvania Corp.	2006 – 2007
Accuweather, Inc.	2004 – 2006
Pharmacia Corp	2003 – 2004
Verizon Wireless	1999 – 2003

Education

Delaware Valley Regional High School, 1994

Professional Certification

- Microsoft Certified IT Professional – Server Administrator, 2012
- CompTIA Security+, 2012
- Microsoft Certified Professional, 2000

UNISYS

Resource 107

Windows Server Administrator

Professional Development

- Microsoft Certified Professional – Windows NT 4.0
- Microsoft Certified IT Professional – Server Administrator
- CompTIA Security+
- Microsoft Certified Solutions Expert – Private Cloud

UNISYS

e&e IT Consulting Services, Inc.

Resoruce 108

Windows Server Administrator

Key Skills and Knowledge

- Secret Clearance
- CCNA
- MCSE
- Security +
- Server and workstation migrations
- SCCM installs

Professional Summary

Provided LAN/WAN support in a broad spectrum of technologies from main frame to PC, and satellites to building Ethernet wiring closets. Fanatical attitude for customer service and technical knowledge. As a technical service engineer for Sun Solaris, kept work backload down and provided prompt responsive solutions for system administrators at numerous government agencies and large businesses.

- Resolved connectivity issues for a 3,500-node national corporation network, making sure to provide network availability of 99.999 percent for continued business operations
- Reduced the downtime of remote and virtual sites by 50 percent, transforming legacy dumb terminal operations to modern Ethernet/PC locations overnight
- Subject matter expert in Microsoft technologies extends from enterprise servers to end users and Microsoft Office applications.

Employment History and Related Experience

U.S. Army Corps of Engineers/Lockheed Martin,
System Administrator 2009 – Present

Verify installations and performance of SCCM clients. Maintain Active Directory user and computer accounts. Monitor log records for intrusion detection and system services functionality. Install, repair, configure, image drives, and perform preventive maintenance of personal computers and network equipment. Answer internal inquiries and troubleshoot software and hardware failures on site or remotely.

- Oversee configurations of switches and routers as well as installation of cable.
- Support IAVA and STIG maintenance Microsoft security updates.
- Maintain server health, security, updates, and service packs; Symantec Backup Exec, data backups, and file restoration.
- Acquired experience with RAS, Support Soft, Bomgar, Microsoft Office, Outlook, Cisco VPN, Remedy, and Oracle.
- Management projects.
- Migrate Secure Copy files.

Milton S. Hershey Medical Center, Field Service
Engineer 2008 – 2008

Completed a project ahead of schedule and budget because of effective implementation. Updated hardware on medical equipment using proprietary software. Performed electrical, safety, and functional tests on medical equipment. Interacted with medical staff and other field service technical support personnel.

e&e IT Consulting Services, Inc.

Resoruce 108

Windows Server Administrator

NOVA Corporation (short-term contract), Solaris Systems Administrator 2008 – 2008

Initiated effective reduction of the system footprint by using Solaris 10 Zones — virtual servers. Installed software and hardware fixes, updates, and enhancements.

- Installed and configured applications, software, and hardware.
- Developed and implemented system diagnostic and maintenance tools to ensure the availability and functionality of systems, including Veritas NetBackup.
- Distributed software across network and Solaris zones.

EDS (Electronic Data Systems), Technical Support Engineer 2008 – 2008

Troubleshot and analyzed Sun Solaris operating system, storage, (Veritas, VX, and Solaris Volume Manager, and Disk Suite) and networking issues. Assisted UNIX and Sun system administrators with diagnosis and troubleshooting of systems and servers. Acquired command line experience.

Craig Technologies, Lead Senior Administrator 2007 – 2008

Microsoft 2003 engineering, network support, and development of deployable video conferencing system. Troubleshot LANs (wired and wireless) and WANs (satellite). Created server images for disaster recovery preparations. Nurtured backup and restore functions with Symantec Ghost. Developed, tested, and hardened HP server configurations for DIACAP requirements through application of Army Gold Master, security IAVM, and STIG requirements as directed by CERDEC for information assurance.

- Supported Cisco routers, switches, VoIP telephones, and satellite.
- Tested software applications testing (Symantec Backup Exec and RadVision Click to Meet).
- Documented system configurations, especially exceptions to policy.
- Tracked the project and reported weekly on development issues.
- Performed and documented Retina scans.
- Created procedural documentation and SOPs for the military and government.
- Served as liaison for the contractor to coordinate government and on-site personnel.

e&e IT Consulting Services, Inc.

Resoruce 108

Windows Server Administrator

EDS (Electronic Data Systems), Technical Ambassador 2005 – 2007

Assisted customers with the installation and configuration of software and hardware products. Assisted customers with implementing system diagnostic and maintenance tools. Analyze and troubleshot operating system, hardware, storage, and networking issues.

- Recommended remediation processes through system diagnostics and patch updates.
- Provided outstanding customer service to keep the caseload low with quick resolutions.
- Identified system-related issues and trends; recommended remedial action.
- Managed software and hardware fixes, updates, and enhancements.
- Supported installation and configuration of applications, and software, and hardware.
- Supported the development and implementation of system diagnostic and maintenance tools.

Manheim Auction, Condition Report Analyst 2004 – 2005

Oversaw inventory condition reports of vehicles using handheld computers and a wireless LAN. Assisted technicians with applying RFID research in the work environment.

Datatec Systems Inc., Network Deployment Consultant 2003 – 2003

Installed more than 50 Microsoft Windows 2000 servers. Migrated workstation and server data from Windows NT to XP and Windows 20000 Server. Configured organizational units, Active Directory, user accounts, permissions, and groups.

- Troubleshoot fiber and Ethernet (CAT 5) network connections.
- Deployed Cisco and Nortel routers, concentrators, and switch hardware.
- Installed and built wiring closets (IDF).
- Tested, troubleshot, and repaired wireless devices, and router T1 circuit backups; received a commendation for high-quality service from a customer district representative.

Rite Aid Corporation, Network Operations Technician 2000 – 2003

Monitored and maintained the 3,500-node communications network, including VSAT. Managed a Frame Relay Network and a leased line network. Acquired experience with Space Net and Hughes VSAT systems.

- Assisted remote field technicians in diagnosing and repairing connectivity issues usually caused by environment or normal wear and tear.

e&e IT Consulting Services, Inc.

Resoruce 108

Windows Server Administrator

- Used network monitoring tools such as MAINVIEW, VSAT Network Management Systems, HP OpenView, and ADTRAN NMS to identify and troubleshoot issues in the network.
- Migrated the WAN to a new satellite vendor; migrated and troubleshot the.
- Troubleshot DS-1, ISDN, and Frame Relay circuits with telco, LECs, circuit vendors, field technicians, and satellite (VSAT) providers to ensure high network availability and functionality of system connectivity 24/7/365.
- Worked with UNIX, TCP/IP, FTP, VPN, remote logon, and EMC storage. Monitored, troubleshot, and resolved issues with distribution center connectivity.
- Tracked network congestion issues with software and a protocol analyzer.
- Created and updated network documentation SOPs, Visio maps, and procedural documents.
- Acquired experience with NetView, Novell NetWare (Zen), Rumba, and What's up Gold.

Education

Associate's Degree in Computer Networking, Harrisburg Area Community College

Bachelor's Degree in Computer Science, University of Phoenix

SCO UNIX, Rite Aid University

Certifications

- Microsoft Certified System Engineer (MCSE certification)
- CCNA Cisco Certified Network Associate, 2012
- CompTIA Security+, 2010
- DoD Secret Clearance
- SSBI Interim Clearance

UNISYS

Resource 109

Windows Server Administrator

Key Skills and Knowledge

- Microsoft Windows Server operating systems
- Microsoft Windows Active Directory
- Microsoft Windows Group Policy
- Server and operating systems troubleshooting
- DataDomain
- VMware vSphere 5
- PowerShell scripting
- BladeLogic administration

Commonwealth of Pennsylvania Project Skills

- DataDomain administration
- NetBackup administration
- Avamar administration
- VMware infrastructure administration and implementation
- ESM BladeLogic infrastructure design and administration
- DPW server support
- PSP server support
- ESM server support
- DPH server deployment architecture design and deployment

Professional Summary

17 years of experience with network administration, implementation, maintenance, and system upgrades. Strong team player and skillful technician with experience in migration, transition, design, and testing.

- Hardware troubleshooting and repair experience: Windows servers, Windows desktops, Windows laptops, Apple servers, Apple desktops, Apple laptops, Android smart phones, Apple smart phones, printers, Cisco routers and switches, Viewsonic projectors, APC Enterprise UPS, and Netgear Enterprise NAS
- Operating systems experience: Windows Server 2008, Windows Server 2003, Windows 7, Windows Vista, Windows XP, Windows versions earlier than XP, VMware ESXi 4, various versions of Linux, Apple operating system X Server 10.4-10.7, Apple operating system X 10.4 through 10.7, Apple iOS, Cisco iOS, and the Android operating system
- Server experience: Active Directory, Group Policy, LDAP, SSL Certification Authority, Server 2008 Cluster, Windows Print Server, iSCSI, RAID, DNS, DHCP, operating system X Open Directory, operating system X Workgroup Manager, NTFS Permissions, IIS, Windows Backup, WMI, PowerShell scripting, and Server 2008 WDS
- Network experience: TCP/IP, Cisco network equipment configuration, firewall configuration, SNMP, CIFS, SMB, AFP, NFS, network cabling
- Enterprise Application Experience: Equitrac Express, Symantec Endpoint Protection, Sophos Endpoint Protection, Ipswitch What's Up Gold, HP Web Jetadmin, Kayako Help Desk, Moodle, Google Apps, Exchange 2010, VMware Server, Spiceworks, and Extron GlobalViewer Enterprise
- Commonwealth of Pennsylvania DPW, PSP, and ESM experience: Building and configuring servers, supporting servers, applying server security patches, and administering VMware infrastructure.

Employment History and Related Experience

Unisys Corporation, Enterprise Support Systems
Analyst I 2012 – Present

Troubleshoot and repair server and operating system issues. Install and configure server operating systems. Administer VMware hosts and clusters.

- Patch server operating systems with monthly security updates.
- Developed and deployed a centralized server imaging and provisioning system.
- Configure and administer server backups using Symantec NetBackup and Data Domain.

UNISYS

Resource 109

Windows Server Administrator

Central Dauphin School District, IT Technician 2004 – 2012

Administered Windows Server 2008 and 2003 Active Directory and Group Policy. Backed up critical student record archives. Administered system monitoring applications, including Equitrac Express, Ipswitch What's Up Gold, and Spiceworks.

- Troubleshot and repaired all district IT hardware, including desktops, PCs, servers, printers, routers, laptops, UPS, and projectors.
- Administered district clustered print servers.
- Oversaw IT monitoring system and on-call alerts.
- Configured and supported applications.
- Worked directly with hardware vendors for ordering and replacement.
- Provided top-level support for district IT technicians.
- Facilitated training and documentation for technicians and end users.
- Deployed and configured of district smart phones and tablets.
- Controlled classroom projection systems and Extron server.
- Administered district IT Help Desk ticketing application.
- Managed network equipment including routers, switches.
- Controlled IT parts ordering and inventory.

Halifax Corporation, Field Service Technician 2001 – 2004

Field service support, field technician at a help desk, webmaster, and depot repair technician.

Scantron Service Group, Field Service Representative 1995 – 2001

Troubleshot and repaired networks and various hardware.

Education

Associate's degree, Specialized Technology For Electronics, York Technical Institute, 1995

Certificate of Completion in Microcomputer Repair, Cumberland-Perry Vocational School, 1993

Certifications

- ITIL v3 Foundations Certification

UNISYS

Domino Technologies Inc.

Resource 110

Windows Server Administrator

Key Skills and Knowledge

- Perform daily PennDOT server farm CheckPoint backups by batch script
- Create and update the PennDOT build procedure documentation for loading Microsoft Server 2003 and 2008
- Assist with PM Network Engineer Remedy tickets; complete the tickets, including printer issues and server hardware issues
- Follow PennDOT build procedure for loading Microsoft Server 2003 and 2008 Standard and Enterprise editions on servers, including BIOS updates, and RAID setups

Professional Summary

Network and system administrator support for 9 years. Experience encompasses the support of a wide range of applications and operating systems. Certified Microsoft Professional. Have served PennDOT since 2006.

- Delete PennDOT server farm terminal server profiles on the Exchange 2003 terminal servers
- Prepare weekly Cat-Tools switch reports for the PennDOT weekly server farm; import text data files to Excel and save them on the server in Excel format
- Perform weekly McAfee.DAT file checks on all PennDOT DMZ servers; fix issues, making sure they have the latest .DAT file updates from McAfee: reinstalling McAfee, fix batch scripts, or run the update manual
- Check trouble lights on the IBM servers on PennDOT's server farm; diagnose, troubleshoot, and resolve issues such as bad hard drives, server error logs, processors, memory, RAID cards, network cards, power supplies. Create support tickets with Pomeroy or IBM as needed
- Troubleshoot servers that become unresponsive and fix the issue: make service calls to vendors for service or parts if needed, reboot servers, fix software and server hardware issues, and notify the on-call supervisor if an appropriate team must be notified for support
- Maintain documents on the PM Engineer SharePoint Web site: update templates for upcoming weekly report logs and archive old reports.

Employment History and Related Experience

Domino Technologies, PennDOT – Consultant Engineer 2007 – Present

Perform daily PennDOT server farm checkpoint backups by batch script. Prepare weekly SMS reports on PennDOT enterprise server disk. Fix issues, including paging file disk space and moving it to another partition, moving files, compressing files or e-mailing the appropriate team or person if unable to find space. Prepare weekly uptime reports for PennDOT servers and fix issues, including setting up scheduled reboots and troubleshooting script errors.

- Perform PennDOT server farm daily terminal sever profile deletions on the 2003 terminal servers.
- Prepare weekly Cat-Tools switch reports on the PennDOT weekly server farm, including importing text data files to Excel and saving them on the server in Excel format.
- Perform weekly McAfee .DAT file checks on all PennDOT DMZ servers, and make sure they all have the latest .DAT file updates from McAfee, reinstalling McAfee, fix batch scripts, and run the update manual.

Domino Technologies Inc.

Resource 110

Windows Server Administrator

- Check trouble lights on the IBM servers on PennDOT's server farm, diagnose, troubleshoot, and resolve issues. Replace bad hard drives, clear server error logs and hardware issues, including processors, memory, RAID cards, network cards, and power supplies. Create support tickets with Pomeroy or IBM as needed.
- Assist Preventive Maintenance Network Engineers with Remedy tickets and complete tickets including printer issues, and server hardware issues.
- Use PennDOT's SRS request system to complete assigned tasks, including building new servers, racking servers, and setting up new printers.
- Create and update PennDOT's build procedure for loading Microsoft Server 2003 and 2008 Server.
- Follow PennDOT's build procedure for loading Microsoft Server 2003 and 2008 Standard and Enterprise Editions on servers, including BIOS updates; RAID setups; hard drive partitions; installing operating systems, security patches, updates, approved applications; defragging hard drives; and creating patch requests for network connectivity.
- Set up IBM RSA carda setup over a laptop connection to the RSA LAN port, setting up the IP address, subnet mask, gateway DNS servers, user name, and password.
- Use Microsoft SCCM for remote control of desktops to help solve off-hour customer issues, to application support, desktop errors, and hardware errors. If unable to resolve and issue, forward it to the appropriate team.
- Use Microsoft SMS queries when needed to gather data for assigned reports from supervisors.
- Use Avocent DSView for remote control of all servers and VMware Virtual Infrastructure Client on VMware servers.
- Use an IBM RSA card or Remote Desktop for remote control of off-site servers.
- Troubleshoot servers that become unresponsive; fix the issue, including working service calls to vendors for service or parts if needed. Troubleshooting includes rebooting servers, fixing issues with software and server hardware, and notifing the on-call supervisor if an appropriate team needs to be notified for support.
- Maintain documents on the preventive maintenance engineer SharePoint Web site. This would include updating templates for upcoming weekly report logs, and archive old reports.
- Degauss defunct hard drives on the degauss machine and placing drive to appropriate location for destruction.
- Replace APC batteries as needed in the server farm APC units. This includes un-boxing and taking out the old battery and replacing with new battery replacing it back in the box. Accepting the alerts on the APC control unit.
- Perform monthly Critical System Recovery Plan backups. This includes taking all the data from the different teams and creating zip files and then burning them to DVDs.

Domino Technologies Inc.

Resource 110

Windows Server Administrator

- Perform inventory procedure on anything that would come into stock to by tagging and scanning into the RFID tag system using Symbol hand held scanner.
- Help in the Microsoft security patch deployment on the PennDOT DMZ servers. This includes getting the patches from the SMS team or downloading from Microsoft Web site, logging on to the server, applying the patches, and rebooting the servers.
- Follow PennDOT's emergency call procedure for power outages occur, including calling the on-call supervisor, notifying the PennDOT staff, monitoring server temperatures and battery power reserve for the generator, and powering servers down as directed by PennDOT staff.

Domino Technologies, PennDOT, Workstation Specialist 2006 – 2007

Provided customer support on PennDOT workstations and laptops statewide. Troubleshot workstation and laptop errors, including system problems, customer inquiries, profile issues, printer setup and problems, network, and software errors. Provided support to PennDOT for loading Windows XP Profesional on statewide workstations and laptops, including imaging and maintaining those images.

- Developed Vista Enterprise workstation and laptop images.
- Documented all trouble tickets in Remedy.
- Installed IBM, Microsoft, Adobe, and other software as needed.

3T Security, Network/Telecommunication Technician 2006 – 2006

Monitored, maintained, set up, and troubleshot Microsoft Server 2003. Maintained, set up, and troubleshot Windows 2000 Professional and Windows XP Professional workstations and laptops. Installed, troubleshot, repaired, terminated, and ran cables for network and telecom including CAT3, CAT5E, CAT6, and fiber optics.

- Installed, troubleshot, and repaired network patch panels and telecom punchdown blocks.
- Set up, maintained, and troubleshot digital DVRs.

Realty Select, Network Administrator 2006 – 2006

Monitored, maintained, set up, and troubleshot Windows 2000 and 2003 Servers, ISA 2004, Cisco 515E pix, and Cisco 1700-3550 switches. Maintained, set up, and troubleshot Windows 2000 Professional and Windows XP Professional workstations and laptops, including Dell and HP. Maintained, set up, and

troubleshot printers and copiers.

- Documented how to instructions for staff.
- Maintained and troubleshot Exchange 2003 e-mail environment.
- Installed applications and software patches.
- Monitored, maintained, set up, and troubleshot a Cisco ICS telephone system and Cisco VoIP 7940 telephones.
- Maintained the current network cabling closet.
- Maintained, troubleshot, set up, and administered all Active Directory users and computers.
- Maintained, troubleshot, and restored company backup tapes using a DLT tape drive with Symantec Veritas 10.

TEK Systems, Systems Engineer 2005 – 2006

Installed and set up a HP ProLiant ML310 server on a contract with D&E Communications. Installed and configured hardware, which included SCSI hard drives, memory, s DAT72 tape drive, and a RAID controller card. Installed Small Business Server 2000; applied all Microsoft patches and Norton AntiVirus Corporation Edition 10, including the System Center console, and Veritas Backup Exec 8.6 on the server.

- Troubleshot, set up, configured, and maintained workstations and laptops running Windows NT 4, 2000, and XP made by HP, Compaq, and Dell.
- Troubleshot, set up, configured, and maintained servers running Windows NT 4, 2000, and 2003 made by HP, Compaq, and Dell.
- Offered support for clients, including Internet services, network, desktop, server, system design, software installations, and user setup.
- Installed and set up network equipment, to including HP and Cisco switches and routers.
- Configured Small Business Server 2000, including Active Directory, DNS, DHCP, data shares, login scripts for mapping drive shares, and folder security. Joined five workstations to the domain. Installed and set up sharing for printers. Configured user and computer accounts.
- Configured Norton AntiVirus Corporate Edition 10 on the server, applying updates, pushing the client software out to the domain's Windows XP clients, and pushing the updates out to those clients daily.
- Configured Veritas Backup Exec 8.6 to back up Small Business Server 2000 along with the system state and the server's data partitions of to a HP DAT72 tape drive, which included building the media set for a five-tape rotation.

Domino Technologies Inc.

Resource 110

Windows Server Administrator

Lancaster General Hospital, System Administrator 2005 – 2005

Supported the radiology department's efforts with Power Scribe for dictation of studies. Provided our initial point of contact for various problems, including microphone defects, computer configuration, and system problems. Installed, troubleshot, and supported 25 USB Dictaphone microphones and computers throughout the department.

- Designed and developed Power Scribe reports using Crystal Reports against a Microsoft SQL database.
- Reset user passwords when needed.
- Installed various software, including Microsoft Word Viewer, Siemens Novius Radiology, and Dictaphone Power Scribe Radiology.
- Diagnosed, troubleshot, repaired, and maintained Dell workstations with Windows XP Professional.

The Milton S. Hershey Medical Center, MMIS Analyst 2001 – 2004

Supported materials management efforts in the Lawson system for inventory control, requisition, and warehouse operations. Served as the initial point of contact for various problems, including coordination of products, stock locations, troubleshooting of error messages, and coordination of Lawson support. Troubleshot and supported five Symbol handheld units, the E-Fax agent, and error messages before escalation.

- Installed, troubleshot, and repaired desktops and laptops, including Dell and Gateway products.
- Designed and developed Lawson system reports using Crystal Reports against an Oracle database.
- Maintained Web-based applications using Crystal Enterprise for the Department of Materials Management.
- Maintained internal and external Web site presence using FrontPage for the Department of Materials Management.
- Trained various users on medical center applications training to various users including Lawson and GroupWise in a Windows 2000 environment.
- Provided preliminary help desk support for departmental workstations.
- Converted supply and distribution from a paper catalog to a Web catalog, saving $3,000 a year on printing costs.
- Converted the printed monthly billing statements for supply & distribution.
- Installed, configured, and maintained Crystal Enterprise for the Department of Materials Management, providing a self-service report system.
- Named Employee of the Month for October 2001.

Resource 110

Windows Server Administrator

Education

ComputerTraining.com

- Microsoft Certified Systems Engineer
- Microsoft Certified Systems Administrator
- Microsoft Certified Professional

Certifications

- Microsoft Certified Systems Engineer
- Microsoft Certified Systems Administrator
- Microsoft Certified Professional

UNISYS

e&e IT Consulting Services, Inc.

Resource 111

Windows Server Administrator

Key Skills and Knowledge

- Secret Clearance
- CISSP
- Network +
- Security +
- Wireshark, Nessus, Nmap, Retina, and DISA GoldDisk
- vSphere, vCenter Server, WSUS, SCCM, WDS, and HBSS
- Windows 7; XP; Server 2003 & 2008 R2
- VMware vSphere 4.1 (ESXi)
- EquaLogic PS6000, Dell MD3000/I, ReadyNAS, HP LeftHand P4000, and Virtual SAN
- Exchange 2003

Professional Summary

16 years of experience as systems engineer and administrator, Web developer, and IT consultant for organizations in the education, manufacturing, real estate, medical, legal, and defense industries.

- Reported C&A issues to Designated Approving Authority (DAA) and C&A staff. Recommended additional protection mechanisms to the project manager
- Excellent oral and written skills; comfortable with briefing senior leadership and command staff
- Information Security Analyst; identified vulnerabilities in network and system architecture
- Acquired experience as SRR reviewer and remediator of STIGs for DoD systems
- Enthusiastic about implementing industry best practices as well as prudent security policies and procedures as required for mission success to ensure the confidentiality, integrity and availability of systems
- Fast learner: motivated to master technologies, languages, and system platforms
- Served as storage manager of a variety of storage area networks (SANs) used for Windows and UNIX environments using leading industry protocols
- Managed a network and servers containing more than $7 million in data running in a Windows Server environment
- Engineered site-to-site VPN WAN solutions for multiple medical practices
- Developed a database Web management tool that allowed nontechnical staff to update real estate listings
- Earned the Ke'Aki Mission Impact Award for exemplary performancein December 2010 and November 2011.

Employment History and Related Experience

E&E IT Consulting, Defense Logistics Agency,
System Administrator, New Cumberland, PA 2012 – Present

Maintain configurations, analyze performance, and provide technical support for more than 30 sites worldwide. Technologies include VMware vSphere virtualization, Windows Server 2003 and Windows Server 2008 R2, Microsoft System Center Configuration Manager (SCCM), Exchange 2003, Office Communicator, and Remedy.

- Deploy and configure virtual machines to remote enterprise sites to support project specifications.
- Provide server and client-side support of issues with Exchange, Outlook, and Office Communicator account.
- Configure user accounts in Active Directory and Group Policy.

e&e IT Consulting Services, Inc.

Resource 111

Windows Server Administrator

- Publish PKI certificates for identification and authentication.
- Obtain proper IA authorization for use of IA tools and technical resources.
- Configure and analyze performance of VMware ESXi 4.1 hypervisors and virtual machines; assess the potential performance for optimizing.

Ke'aki Technologies, System Administrator,
US Army, Ft. Detrick, MD 2010 – 2012

Identified, isolated, and reported security violations and incidents to the security officer and senior USAMRMC leadership. Reported C&A issues to DAA and C&A staff. Recommended additional protection mechanisms to the project manager. Followed the Army/MEDCOM-approved procedures for destruction of failed mass storage devices. Reviewed and updated a IA C&A support documentation package to ensure accuracy, completeness, and compliance with minimal risk acceptance standards.

- Maintained a repository for systems C&A documentation and modifications with version control.
- Identified information systems within the scope of my responsibility that were not properly certified and accredited in accordance with DIACAP policies.
- Researched the requirements for submitting Certificate of Networthiness documentation.
- Began to implement required IA guidance, policies, procedures, and regulations as directed and as resources permitted.
- Assisted, supported, and reported to USAMRMC CIO/DCSIM (Deputy Chief of Staff of Information Management) as required for AR 15-6 investigation.
- Helped enforce IA policy and guidance in accordance with regulations and identified best business practices.
- Conducted security inspections, assessments, tests, and reviews.
- Reviewed and audited log files; researched log correlation tools for acquisition of log management.
- Reviewed and evaluated the effects on security of system changes, including interfaces to public-facing Web sites and compliance with DMZ configuration.
- Served as storage manager of four storage arrays for Windows and UNIX environments using NFS, SMB, SAS, and iSCSI. Took array and system-level snapshots.
- Wrote backup and recovery policy documentation.
- Remediated Windows environment STIGs; helped spearhead the DIACAP process.
- Reviewed a SRR checklist of the SQL Server 2008 database, identified misconfigurations.
- Implemented an Active Directory child domain and Exchange 2003 Server.
- Maintained the Windows 2003 Active Directory NTDS database and schema.
- Installed and configured Windows 2003 and 2008 servers.

e&e IT Consulting Services, Inc.

Resource 111

Windows Server Administrator

- Installed and configured ESXi 4.1 hypervisors, vCenter and storage.
- Installed and maintained Windows Server Update Services (WSUS).
- Installed and maintained Windows Deployment Server (WDS/PXE).
- Implemented Acronis 10 Management server and clients as well as backup policies.
- Implemented management policies and procedures for maintenance of the CM library.
- Served as team Lead for the relocation of the AHLTA test environment from Ft. Gordon to Ft. Detrick.
- Identified, isolated, and reported security vulnerabilities in the computing environment.

Walkersville Christian Family Schools, Systems Administrator & Web Developer 1995 – 2010

Managed workstations as well as Windows 2000 and 2003 servers. Trained and mentored student interns in Web development with PHP. Implemented Windows 2000 domain controller and migrated it later to Windows 2003. Planned disaster recovery with successful disaster recovery of servers from backup tapes. Implemented policy for strong passwords, backup and tape rotation, file share access, firewall and routing, and remote access.

- Implemented SSL for school Web services.
- Audited network traffic with Wireshark.
- Monitored Web access logs in IIS, ISA, SurfWatch, and the Exchange e-mail system.
- Developed a student record system Web front end using PHP, FileMaker Server, and SSL.
- Implemented input validation, preventing XSS and injection attacks.
- Spearheaded the development and integration of the school's Web site in 1996, with subsequent redevelopments in 2001, 2005, and 2008. Migrated the Web site from static HTML to DotNetNuke 4 and PHP Web applications.
- Upgraded and maintained database systems in FileMaker Pro and Server.
- Implemented MS SQL Server 2005 and MySQL for enterprise and Web applications.

Environment: Active Directory, Exchange, Outlook Web Access, DNS, DHCP, IIS, ISA, FileMaker Server, MySQL, and WireShark.

Keysville Enterprises, LLC, IT Consultant, Web Developer, Systems Architect 2002 – 2010

Developed a FileMaker and PHP Web application for the Congressional Award Foundation. Implemented site-to-site VPN WANs for multiple medical practices

in the greater Washington area, saving each client nearly $5,000 a month.

- Provided remote and on-site IT support services to more than 50 real estate clients in the Baltimore/Washington region.
- Designated by Llewellyn Realtors as its approved on-site IT support technician for LLE real estate agents.
- Developed a database-based Web management tool that allowed nontechnical staff to update real estate listings and PDFs on agent's Web site, saving the client $2,500 a year.

Wright Manufacturing, Inc, IT Manager & Systems Administrator 2000 – 2005

Managed network servers with more than $7 million in data, running Exchange, IIS, ISA, and Outlook Web Access in a small business server environment. Planned disaster recovery with successful disaster recovery of servers from backup tape.

- Migrated a domain from Windows NT 4 to Windows 2000.
- Relocated company information systems to the Frederick facility.
- Implemented policy for strong passwords, backup and tape rotation, file share access, firewall and routing, and remote access.
- Implemented encryption technologies (SSL and IPSec) for company Web and e-mail services.
- Negotiated telephone service contract in 2001 and Internet service in 2005, saving the company about 25 percent annually.

Education

- MCSE Certification Course, ISMart, Elkridge, MD, 1999
- Security+ IA Training Course, U.S. Army, Ft. Gordon schoolhouse, 2010
- CISSP Training Course, U.S. Army, Ft. Gordon schoolhouse, 2011
- Training Camp VMware vSphere 4.1 VCP Certification Course, 2011
- Information Assurance Fundamentals, U.S. Army, 2011
- High School Diploma, Walkersville Christian Family Schools, 1996

Certifications

- FAA Private Pilot, 1997
- Microsoft MCSE NT 4, 1999
- Active Secret Clearance, 2010
- Network + and Security+, 2010
- CISSP, 2011

UNISYS

INFO-MATRIX CORPORATION

Resource 112

Windows Server Administrator

Key Skills and Knowledge

- Microsoft Windows XP, 7, 2003, 2008; Visio; and Office & Active Directory administration
- Exposure to Linux and Fix, DameWare, WhatsUp, and various other monitoring tools

Professional Summary

Deep experience with hardware, wiring, network security and wireless networks, 24x7x365 on-call support and maintenance; well-rounded utility player with experience delivering user training, technical writing, and asset procurement. Adds additional value through process analysis, re-engineering workflows, and implementing industry best practices.

- Self-motivated as a team lead, individual contributor, or both – does what it takes to get the job done in a professional way and motivate or mentor others as needed
- Exposure to full-life cycle project management.

Employment History and Related Experience

Born Capital LLC, Level Two Support Engineer, Chicago, IL 2010 – 2012

Managed 250 servers in the firm Chicago, NY/NJ, London, Toronto, and FFT data centers. Acquired experience in remote support and platform virtualization (RDP, DameWare, VMware, and ESX). Installed and supported server and network hardware and software (100M, 1G, and 10G)

- Performed server imaging and rapid deployment (Altiris, Insight, and Ghost).
- Administered Microsoft Active Directory (new users, permissions, and minor group policies).
- Participated on a global infrastructure team and in its initiatives; traveled as needed.
- Built, installed, and configured client sites.
- Managed a data center (installation, space, power, cooling, cabling, planning, and disaster recovery).
- Performed general desktop troubleshooting, networking, device management, and support.
- Installed and supported TT, PATS, and Eurex MISS systems from the front to back ends.
- Provided application support as a secondary focus for trading applications.

Actant Inc, Support Services Specialist, Chicago, IL 2008 – 2010

Installed and configured hardware and software. Trained users on the software. Resolved problem tickets. Configured, set up connectivity, and modified. Installed, configured, and monitored the status of Citrix connectivity. Analyzed and mapped Fix logs for market or trading system investigations.

- Performed daily monitoring, system analysis, and troubleshooting of mission-critical systems.

Resource 112

Windows Server Administrator

Fimat USA, E-Trading Support Specialist, Chicago, IL 2007 – 2008

Set up new accounts (Pats, TT, Web-ICE,and CQG). Set up, configured, and trained users.

- Provided VPN and Level 1 technical support.
- Set up trade routing and configuration.

KidTalk, Inc, Technical Consultant, New Lenox, IL 2005 – 2007

Installed and maintained a hybrid LAN/wireless network (static and dynamic IPs, DNS, and DHCP). Installed software and hardware; trained users.

- Daily and weekly secure file backup.
- Administered e-mail and the Web site (set up TCP/IP for Telnet and remote access tools).

Cargill Investor Services, Chicago, Foreign Exchange
Senior Desk Broker & Head of Electronic Trading 1997 – 2005

Brokered cash, swaps, options, and EFPs on foreign exchanges. Provided Level 1 and 2 support as well as project management for a 100-user international trading system. Managed sales relationships. Served as an assistant desk manager.

- Set up computer workstations (hardware, software, and user administration).
- Acquired hands-on experience in trading (tools used: Project A, Globex, Reuters 2000, TT, and Bloomberg).
- Managed disaster recovery (file backups, cloning and imaging of drives, and testing).

Education

- B.S., Network and Communications Management, DeVry University, in progress
- GPA of 3.91 – 109 of 122 credits (88 percent complete)

UNISYS

INFO-MATRIX CORPORATION

Resource 113

Windows Server Administrator

Key Skills and Knowledge

- 11 years of experience as an IT administrator
- Microsoft Certified Systems Engineer
- Microsoft Certified Professional
- Performed data backups
- Developed a full disaster recovery plan
- Standardized all desktop installations
- Planned, coordinated, and implemented network security measures
- Developed new computer clients
- Recommended hardware purchases
- Monitored and maintained Exchange 2010 Server
- Analyzed software and hardware performance
- Developed a strategy for encryption and implementation of laptops

Professional Summary

Results-oriented, enthusiastic, and dedicated IT and sales professional seeking a challenging new position. More than 11 years of experience as an IT administrator; 15 years of sales experience. Detail-oriented employee adept at multitasking in high-pressure environments to accomplish stated company objectives and meet deadlines.

- Proven ability to increase efficiencies and streamline operations
- Skilled at adapting quickly to changing needs and priorities.

Employment History and Related Experience

Walz, Deihm, Geisenberger, Bucklen & Tennis, PC, IT Administrator, Lancaster, PA 2001 – 2012

Oversaw all IT functions for a large CPA firm. Maintained and administered the firm's computer network and related computing environments, including computer hardware, systems software, applications software, and all configurations. Diagnosed, troubleshot, and resolved hardware, software, and other network and system issues. Replaced defective components as needed.

- Performed data backups and developed a full disaster recovery plan and additional policies to create a more secure and stable network environment.
- Standardized all desktop installations to increase efficiency.
- Planned, coordinated, and implemented network security measures to protect data, software, and hardware.
- Developed new computer clients; recommended and purchased their hardware.
- Monitored and maintained Exchange 2010 Server, Vipre spam filter, and Symantec antivirus protection software.
- Analyzed software and hardware performance as well as researched and recommended improvements to systems and the network.
- Administered all third-party applications and configurations used by employees.
- Developed a strategy for encryption and implementation of laptops.
- Gathered client-specific data to identify, predict, interpret, and evaluate system and network requirements.
- Served as a liaison between the firm and vendors to resolve issues and facilitate purchases.
- Migrated an existing Watch Guard firewall to a new Watch Guard firewall and reconfigured it.
- Maintained logs of network functions as well as maintenance and repair records.
- Developed tutorials to train employees on computer system use.
- Conferred with network users to solve problems and increase employee

efficiency.

- Performed routine network startup and shutdown procedures and maintained control records.

Ralph A. Davis Inc./Davis Insurance Agency,
Consultant, Lampeter, PA 2001 –2001

Maintained all computer hardware and software applications. Built the client database. Created and designed marketing materials. Assisted with the overall marketing strategy.

Waypoint Bank, Investment Representative,
Harrisburg, PA 1999 – 2001

Introduced bank customers to alternate investment products using Web-based sites and software for seven Waypoint branches in Lancaster and Lebanon Counties. Trained bank employees on lead in techniques for generating leads.

The Copeland Companies, Financial Advisor,
Mechanicsburg, PA 1997 – 1999

Oversaw on-site administration of York Hospital's 403(b) retirement program.

- Provided employees with consulting services for available financial products using Windows-based sales software.
- Developed new accounts and services for 1,400 existing accounts.
- Named top overall producer for the Harrisburg office in 1998.

Busy Barn Inc., Owner, Lancaster, PA 1993 – 1997

Owned and operated a supervised indoor playground business.

- Developed and updated a strategic business plan.
- Performed all aspects of running the business, including marketing and public relations, human resources, and accounts payable and receivable.

Prudential Insurance Company, Sales Manager,
Lancaster, PA 1985 – 1993

Oversaw policyholder service and public relations for a staff of eight.

- Recruited and trained new sales representatives.
- Supervised and continued training for veteran representatives using Prudential software.
- Developed personalized financial portfolios for new accounts using Prudential software for financial products and services.

Resource 113

Windows Server Administrator

Education

- B.A., Marketing, Millersville University, Millersville, Pennsylvania

Certifications

- Microsoft Certified Systems Engineer, 2001
- Microsoft Certified Professional, 2000

This page intentionally left blank.

UNISYS

Resource 114

Windows Server Administrator

Key Skills and Knowledge

Databases

- Microsoft SQL 2000, 2005, $ 2008
- Oracle 8i & 9i

Hardware

- Cisco routers and Catalyst switches, HP ProLiant GL360 & 380, Dell Power Edge servers, Compaq ProLiant servers, Dell workstations, IBM Thinkpads. IBM 3650s & 3850s, Quantum DLT Libraries, Big-IP (F5), Dell Dimension & Optiplex workstations, Dell & Gateway laptops, BlackBerry 8700 & 8800 series, Palm Tungsten & Treos, video teleconferencing equipment (VSX7000)

Operating Systems

- Windows NT, 9x, XP, 2000, 2003, & 2008 R2, Sun Solaris 7, 8, & 9, Red Hat Linux, Fedora, Novell NetWare 5.x & 6.x.

Software/System Architecture

- HP Insight Manager, HP OpenView, Veritas Backup Exec & NetBackup, J2EE 1.3, Microsoft Office, Microsoft Visual Studio .NET, SharePoint Portal Services, BMC Patrol 7.0, Connect Direct, Axway, SCCM 2007, & SCOM 2007

Programming Languages & Tools

- Treesizepro, BeyondCompare, Httpwatchpro, Idera, Litespeed, C, C++, & Java

Office Productivity Tools

- Microsoft Word, Excel, Access, FrontPage, & Notepad+

Professional Summary

More than 15 years of experience implementing and supporting Windows NT, 2000, 2003, and 2008 R2; Novell; and UNIX networking environments. Excellent understanding and troubleshooting skills in a large-scale enterprise network infrastructure.

- Experienced in the design and implementation od LANS and WANs, including leased lines, Frame Relay, ISDN and switched Ethernet (fast and gigabit), and FibreChannel switches
- Experienced in network, routing, and switching protocols, including TCP/IP (4.0 and 6.0), IPX/SPX, RIP, EIGRP, OSPF, IGRP, BGP, ISDN, and Frame Relay, and integrating IP networks with VoIP-based voice networks
- Solid knowledge of Microsoft Cluster Services, information security, risk management principles, Citrix MetaFrame Presentation Server, Microsoft SharePoint Portal Services, HP OpenView, and other similar tools
- Designed and implemented SAN solutions for clients using SAN hardware (FibreChannel switches and HP storage servers) and software components (Windows 2003 Storage Server and iSCSI).
- Experienced in technical presentations using Microsoft Visio and PowerPoint
- Experienced in DNS; DHCP; WINS; SNMP; NIS; LDAP; SMTP; POP3; IMAP; NTP; NAT; VPN; BIND; Terminal Services; Exchange Server 5.5, 2000, and 2003; Citrix Presentation Server, Xen desktop, SiteMinder; Microsoft Cluster Services, and RAID 10 and 5
- Implemented Linux Networks successfully — Linux as E-mail server, Web server, and Samba server for Windows network connectivity
- Handle large Enterprise networks for more than 50,000 users.

Professional Experience

Patch Management Consultant, Commonwealth of Pennsylvania, Sr. Infrastructure Engineer, Harrisburg, PA 2012 – Present

Testing, Supporting, and Deploying Microsoft and third-Party Security patches, including Service Packs in different enterprise environments like Development, Stage, and Production using System Center Configuration Manager (SCCM 2007 R2). Process service tickets (in Remedy) in a 5,000-server environment; perform change management, problem management, and configuration management. Provide 24x7x365 application user support. Assign on-call rotation schedules to team members. Monitor the perfomance of servers (application clusters, database, BizTalk, and Web), and event logs. Track various issues and problems using Microsoft Terminal Services and the Windows PerfMon tool.

UNISYS

Resource 114

Windows Server Administrator

- Create and manage system center deployments using SCCM 2007; consolidate and clean up collections periodically.
- Design, plan, and architect large-enterprise Windows environments with experience in managing and implementing large-scale servers in a production data center environment.
- Use experience with Infrastructure design, Active Directory implementation, system builds, performance monitoring and tuning, application and server high availability, and strong knowledge of disaster recovery.
- Underwent training programs in BMC BladeLogic Server Automation and ADDM (Asset Discovery and Deployment Manager). Created patch deployment packages in BladeLogic for deployment in the lab environment.
- Develop and manage patch release strategies and production delivery schedules for software applications.
- Troubleshoot performance-related issue in the IIS application.
- Verify security logs on different region servers for tracking user logins and logouts to the system, including unsuccessful login attempts. Load balanced and performance tune Web Server farms using SiteMinder 6.

Bank of New York Mellon, Sr. Infrastructure Consultant, King of Prussia, PA 2010 – 2011

Tested and supported banking applications (ASP.NET) in different enterprise environments like development, QA, mirror, stage, and production, including trade floor support. Processed service tickets (in Seapine Test Track) in a 5,000-server environment. Implemented change management, problem management, and configuration management. Provided 24x7x365 application user support. Assigned on-call rotation schedules to team members. Maintained the perfomance of servers (application clusters, database, BizTalk, and Web) and event logs. Tracked various issues and problems with Microsoft Terminal Services and the Windows PerfMon tool. Applied service packs, hot fixes, and patches monthly through SMS 2007 to application and Web servers in all the testing and production environments.

- Designed, planned, and architected large enterprise Windows environments, managed and implemented large-scale servers in a production data center environment.
- Acquired experience with Infrastructure design, Active Directory implementation, system builds, performance monitoring and tuning, and application and server high availability. Acquired strong knowledge of disaster recovery.
- Created, ran, and maintained thousands of batch job schedules using ADVSYSCON Active Batch software on Web and SQL servers in all regions. Escalated issues and problems to various Global Operational

UNISYS

Resource 114

Windows Server Administrator

Services teams in King of Prussia or Pittsburgh.

- Actively participated in data center migration and relocation, including application and business process discovery, scheduling, physical move execution and vendor certification. Also participated in migrating applications from Windows 2003 and 2008 as well as IIS 6 and 7 platforms.
- Scheduled, configured, and maintained transmission jobs on Axway/Sterling Connect Direct software for clients like SunTrust, Genworth, ETrade, and FiServ. Set up NDM/FTP and subscriptions to leased lines from Verizon and AT&T.
- Created packages in BladeLogic for deployments and upgrades of various .NET applications.
- Troubleshot performance-related issues in the IIS application.
- Rolled SiteMinder out on the IIS server; troubleshot connectivity issues with these master server.
- Performed weekly and monthly application migrations (code moves as well as database fixes and updates) in production environments. Maintained Web sites quarterly. Monitored Web site traffic periodically with Truesight Coradiant.
- Backed up servers using NetBackup software, including monitoring backup logs and troubleshooting backup and restore errors. Created and executed disaster recovery preventive maintenance procedures at the Philadelphia site.
- Verified security logs on different region servers for tracking user logins and logouts to the system, including unsuccessful login attempts. Load balanced and performance tuned Web server farms using SiteMinder v 6. Installing and configuring policy servers.
- Performed complete Active Directory administration, network conversions, remote access and system security using HP OpenView and IPsec.
- Installed and configured certificates on Windows production and test boxes for SSL connectivity to the portal sites (http://www.advisorport.com).
- Installed, configured, and administered SQL Server 2000 and 2005 and processes, including process monitoring using the Idera SQL tool and database core administration. Worked extensively with SQL Enterprise Manager; created databases, tables, views, and stored procedures. Backing up and restoring databases using Litespeed for SQL software was an integral part of the job.
- Created and administered virtual machines using VMware ESX Server 3.5. Worked extensively with VMware Infrastructure Client and administered Virtual Center 2.5.

Credit Suisse, Application Support Specialist,
New York, NY 2009 – 2010

UNISYS

Resource 114

Windows Server Administrator

Tested, deployed, and supported security management products in different enterprise environments such as QA, staging, and production using the Repliweb tool. Processed service tickets (ith Remedy 6.0 and 7.0) in a 5,000-server environment; implemented change management, problem and configuration management. Provided 24x7x365 application user support in the Americas, Europe, and Asia. Gathered functional requirements for the security product (Lumension). Prepared technical documentation for release to the various support teams, including branch support. Identified users for user acceptance testing of the product.

- Installed, configured, and maintained application servers using Windows 2008 Virtual Workstations application servers on HP DL 580s as well as SharePoint team Web sites. Load balanced the IIS 6.0 and 7.0 Web farm.
- Deployed content, both IIS Metabase and .NET assemblies, using Repliweb 4.1.1. Configured distribution and replication jobs.
- Assisted with and developed a process flow for automating content deployments across various environments such as QA, staging, and production.
- Created and modified vbscripts and batch scripts for automating the Windows environment.
- Deployed Lumension successfully in Altiris pushes to 25,000 clients, including laptops, workstations, and virtual desktops in the Americas region.
- Installed and configured SQL Server 2000 and 2005 clusters and processes, including process monitoring and database administration.
- Extensively used the Active Directory CSFB tool for issuing group memberships to aid users in application access. Remotely accessed user machines with Carbon Copy and fixed problems.
- Thoroughly tested Lumension on various USB devices such as memory sticks, BlackBerry SD cards, smart phones, and hard drives. Sought users' acceptance for the product from the support teams.
- Identified and whitelisted about 50 BlackBerry device models including 8800s, 9000s, 9500s, and 9700s. Used Lumension Security Management Console to generate reports executing queries from SQL 2000 and 2005 databases. Administered and troubleshot Lumension application server problems.

Ernst & Young LLC, Systems Administrator,
Secaucus, NJ 2007 – 2009

Tested and supported gT&E (global time and expense) and eRooms SharePoint sites and applications in different enterprise environments like development, QA, and production. Processed service tickets (with Remedy 6.0 and 7.0) in a 5,000-server environment; implemented change management, problem management, and configuration management. Performed 24x7x365 application user support in the Americas (Region 1),

UNISYS

Resource 114

Windows Server Administrator

Europe (Region 2), and Asia (Region 3). Assigned 2-week on-call rotation schedules to team members.

- Monitored performance of servers (application, database, BizTalk and Web), and event logs. Tracked various issues and problems using Microsoft Terminal Services and the Windows PerfMon tool. Applied service packs, hot fixes, and patches monthly through SMS 2007 to the gT&E and eRooms servers in all the testing and production environments.
- Tested and monitored simple Web transaction response time and availability with BMC Patrol 7.1. Monitored applications, storage, and system devices.
- Created, ran, and maintained thousands of batch job schedules with Control-M agent 6.2 software on Web and SQL servers in all regions (1, 2, and 3). Escalated issues and problems to various Global Operational Services teams in Secaucus or worldwide.
- Changed application, SQL, and cluster services' passwords quarterly for all IIS 6.0, application, and database cluster servers enterprise-wide information security policy.
- Connected to Oracle database servers using Oracle Enterprise Manager or SQLPlus on Oracle client software for performing application server tasks.
- Performed weekly gT&E migrations (code moves as well as database fixes and updates) in production environments. Performed monthly eRooms code moves (deployed extensions) in production environments in all three regions.
- Backed up servers using NetBackup software, including monitoring backup logs and troubleshooting backup and restore errors. Created and executed disaster recovery preventive maintenance procedures in gT&E regions 1, 2, and 3.
- Verified security logs on different region servers for tracking user logins (SSO) and logouts to the system, including unsuccessful login attempts. Load balanced and performance tuned Web servers with SiteMinder 6.
- Performed complete Active Directory administration, network conversions, remote access, and system security with HP OpenView and IPsec.
- Installed and configured certificates on Windows and UNIX boxes for SSL connectivity to the portal sites.
- Implemented and maintained DNS services on Linux servers.
- Created and modified cleanup DOS scripts to VB scripts for automating the Windows environment.
- Created and maintained documentation for various operating environments in Microsoft Visio 2003, Microsoft Project 2003, and Wintel.
- Installed, configured, and administered SQL Server 2000 and 2005 and processes, including process monitoring and database core administration. Worked extensively with SQL Enterprise Manager.

UNISYS

Resource 114

Windows Server Administrator

Created databases, tables, views, and stored procedures. Backingup and restoring databases was an integral part of the job.

- Configured SAN HBA cards on servers, including resolving any connectivity issues. Allocated SAN drive space of up to 500 gigs depending on requirements.
- Created and administered virtual machines using VMware ESX Server 3.5. Worked extensively with VMware Infrastructure Client; administered Virtual Center 2.5.

Maine Center for Disease Control, Server Administrator, Augusta, ME 2007 – 2007

Supported IPHIS (Integrated Patient Health Information Systems) in different testing environments like development, staging, standby, and production. Processed service tickets (using Footprints) in a 200-server environment. Implemented change management, problem management, and configuration management. Provided desktop support with LANdesk and in person for all local and remote end users.

- Monitored servers (application, database, integration, and IIS 6.0) and event logs, tracked various problems. Applied service packs and hot fixes to IPHIS in all the testing environments. Started and stopped the WebLogic Server instances on the server.
- Ran scheduled tasks daily like Msgin, Msgout, MasterETL, and Drop_create_tables. Traced the log files. Escalated issues and problems to Office of Information Technology, State of Maine.
- Changed database schema owner passwords, Web servers, Sun One Directory Server Manager passwords, and batch process login accounts.
- Connected to Oracle database servers using Oracle Enterprise Manager or SQLPlus on Oracle client software for performing application server tasks.
- Installed and configured Terminal Services (Application Server mode) and SSL VPNs on Windows 2003 servers.
- Installed and configured BIND 7 DNS server for providing a naming service on the IPv6 network and the Internet.
- Installed and configured Rhapsody licenses on the integration server.
- Configured and monitored WSUS on Windows 2003 Server for patch management.
- Monitored and fixed synchronizing issues between the application server and the integration server.
- Backed up servers with Veritas Enterprise BackExec client software, including monitoring backup logs and troubleshooting backup and restore errors.
- Verified security logs on different servers for tracking user logins and logouts to the system, including unsuccessful login attempts.
- Extensively used RSA Database Administration for issuing security tokens to facility users for application access.

UNISYS

Resource 114

Windows Server Administrator

- Installed and configured certificates on Windows and UNIX boxes for SSL connectivity to the Maine's iphis portal.
- Created and modifying vbscripts, wscripts for automating Windows environment.

New York State/Office of Mental Health, Network Administrator, Manhattan, NY 2006 – 2007

Processed service tickets in a 500-server environment; implemented change management, problem management, and configuration management. Provided desktop support with LANdesk and in person for all local and remote end users. Assisted a group of four to five members in Windows 2000 Professional, 98, and Me rollouts to Windows XP Professional. Configured and administered Windows 2000 and 2003 and Solaris 8 and 9 Servers.

- Configured Novell NetWare Cluster Services on a two-node Dell PowerEdge 2600 server for file and print services.
- Worked with Windows Active Directory and Novell e-Directory services to maintain facility users and resources. Also worked with iManager to install and configure Novell NetWare printers.
- Monitored and fixed synchronization issues between Active Directory and e-Directory using IDM.
- Monitored the perfomance of servers (application, database, and Web) and event logs. Tracked various issues and problems via MS Terminal Services and BMC Patrol 7.0.
- Worked extensively with Novell GroupWise 7.0.1 for messaging services in the facility.
- Configured and maintained Microsoft Exchange 2000 and 2003 in the facility. Worked extensively with Microsoft Exchange Service Manager (ESM). Worked with storage groups, mailbox, and public folder store administration.
- Performed complete Active Directory administration, network conversions, remote access, and system security with HP OpenView and IPsec.
- Implemented VLANs and Spanning Tree protocol on the LAN using VLSMs. Maintained network cabling for Ethernet connectivity to workstations using CAT3 and 5e cables.
- Maintained GroupWise, including post office rebuilds, DST remediations, and day-to-day administration.
- Supported OMH applications like CAIRS, CONCERTS, Meds Manager, and RAS.
- Installed, configured, and administered SQL Server 2000 and 2005 and processes, including process monitoring and database core administration. Worked extensively with SQL Service Manager and Enterprise Manager.

UNISYS

Resource 114

Windows Server Administrator

- Extensively used RSA database administration for issuing security tokens to facility users for application access.
- Configured and maintained BlackBerrys and Palm Treo desktops for users in the facility.
- Wrote vbscripts and wscripts for automating the Windows environment.
- Configured and maintained SharePoint team Web sites and load balanced the IIS 6.0 and 7.0 Web farm.
- Monitored and implemented video teleconferencing service for the facility, including troubleshooting over ISDN lines.
- Configured Toshiba telephones for users, including backups of AMANDA voicemail.
- Installed and configured WSUS on Windows 2003 Server for patch management.
- Managed patches, Microsoft and Microsoft Office updates, Novell service updates, and hot fixes on servers including Firmware updates.
- Configured desktops for remote connectivity of applications using secure gateway.
- Administered the Novell servers through AdRemote console software.
- Backed up Novell servers using Veritas Enterprise BackExec client software, including monitoring backup logs and troubleshooting backup and restore errors.

Hanover Insurance Group, Server Administrator,
Worcester, MA 2006 – 2006

Processed service tickets in a 500-server environment, change management, problem management, and configuration management. Provided desktop support over the phone and in person for all local and remote end users. Configured and administered Solaris 9 as well as SunFire V480R and V440R servers.

- Configured Microsoft Windows 2003 Cluster Services on a two-node HP DL360 server for file services. Designed Microsoft Print Cluster Services on HP DL360 servers.
- Installed and configured Microsoft SharePoint services with MSDE on the primary domain controller. Organized corporate documentation, including contacts and meetings, using SharePoint Services.
- Added groups and resources under Veritas Cluster Server 4.0.
- Installed and configured BIND 7 DNS Server for providing a naming service on the IPv4 network and the Internet.
- Created and administered virtual servers using VMware ESX Server and load balancing. Moved GSX servers to the ESX farm.
- Developed Shell scripts, Perl scripts for automating, reported, and scheduled jobs using CRON and AT.

UNISYS

Resource 114

Windows Server Administrator

- Installed and configured WebSphere AS 5.1 on Windows 2000 Advanced Server SP3, including Web and SOAP Services.
- Deployed Web components (servlets and JSP files) on the application server.
- Managed patches, Microsoft and Microsoft Office updates, and hot fixes on servers; updated Firmware.
- Configured and administered Terminal Services (Application Server mode) and Citrix Metaframe presentation services on Microsoft XP Professional desktops for remote connectivity of applications using Secure Gateway.
- Installed, configured, and administered SQL Server 2000 and processes, including process monitoring.
- Installed and configured SAMBA services on Linux servers for connecting to Windows machines.
- Backed up servers using Tivoli Storage Manager Client software on IBM 800 and 8300 storage systems.
- Maintained DHCP, DNS, and WINS servers.
- Configured DFS for sharing folders and files over the enterprise network.
- Gathered and prepared technical documentation in Microsoft Visio software.

Varsitybooks Inc, Network/System Administrator,
Washington, DC 2005 – 2006

Configured and administered Windows 2000 and 2003, Wintel servers on HP DL blade servers, and Windows XP Professional workstations, including Dell and IBM ThinkPads. Installed and configured Microsoft SharePoint services on the Primary domain controller. Installing and configuring Solaris 9 on SunFire servers, including patching.

- Administered and configured the volumes using Veritas volume managers according to the customer's requirements.
- Performed complete Active Directory administration, network conversions, remote access, and system security using HP Insight Manager and IPsec.
- Worked with a system monitor to tune performance, thereby identifying potential bottlenecks.
- Configured and administered Terminal Services (Application Server mode) and VPN on Windows 2003 servers.
- Load balanced and performance tuned Web servers using a Big-IP F5 load balancer.
- Configured and administered .NET Framework Application Server on IIS 6.0 Server. Worked in XML to validate the configuration files.
- Administered and monitored the Big-IP load balancers for dynamic load balancing of the varsitybooks Web site.

UNISYS

Resource 114

Windows Server Administrator

- Installed, configured, and administered SQL Server 2000 and processes, including process monitoring.
- Backed up servers using BrightStor ARCserve backup software.
- Installed and configured DNS, NIS, and NFS servers.
- Installed and configured WebSphere AS 5.1 on Windows 2000 Advanced Server 5.1.
- Installed and configured Web and SOAP Services on application servers.
- Assisted in deploying applications on application servers.
- Gathered and prepared technical documentation for a simple disk-to-disk, disk-to-tape HP SAN solution for the production environment.
- Provided desktop support over the phone and in person for all local and remote end users.

American Florists Inc, Network/System Administrator, Boston, MA 2005 – 2005

Upgraded a Windows NT network to Windows 2003. Migrated data server using the Aelita migration suite, including building trusts. Worked with 1,000 to1,500 users. Configured and administered Windows 2003 servers and Windows XP, 2000 Professional, NT, XP, 98, and 95 workstations.

- Worked with a system monitor in .NET application performance tuning.
- Wrote vbscripts and wscripts for automating the Windows environment.
- Performed complete Active Directory administration, network conversions, remote access, and system security using HP OpenView and IPsec.
- Installed and configured Terminal Services (Application Server mode), VPN, Web Server, and a Watchguard firewall on Windows 2003 servers.
- Backed up, restored, load balanced, performance tuned Web and app servers.
- Migrated Micrsoft Exchange Server 5.5 to version 2000 and eventually to Exchange Server 2003.
- Installed and configured RPC over HTTP for Exchange 2003 Server Services.
- Worked with Windows 2003 Cluster Server Administrator to administer clusters. Created nodes and resources as part of cluster server management.
- Configured and administered Ecommerce 2002 and BizTalk servers for Web and SOAP Services.
- Configured RAID volumes with Veritas Volume Manager.
- Maintained DHCP, DNS, and WINS servers.
- Developed Shell scripts and Perl scripts for automating, reporting, and scheduling jobs using CRON and AT.

UNISYS

Resource 114

Windows Server Administrator

Adelphi Academy, Network/System Administrator,
New York, NY 2001 – 2005

Upgraded a Windows NT network to Windows 2003. Migrated data from Windows NT to Windows 2003 Server using the NetIQ migration suite, including building trusts. Configured and administered Windows 2000 cluster servers and Windows XP, 2000 Professional, NT, XP, 98, and 95 workstations. Worked with more than 2,000 users and workstations.

- Executed vbscripts and wscripts using WMI.
- Configured send mail, fetch mail, and a virtual user and aliases table for enabling e-mail for users from multiple domains with SMTP, IMAP, and POP3 protocol support.
- Implemented and maintained IGRP between the head office and branches on Cisco 1700 through 2500 series routers using leased lines for WAN connectivity and Catalyst switches for LAN connectivity.
- Installed and configured a Sun StorEdge 3310 and 3510 storage area network.
- Installed and configured Terminal Services (Application Server mode), VPN, Web server, and a firewall on Windows 2003 servers.
- Installed, configured, and administered WebSphere Application Server, HTTP Web Server, and Secure Way Directory (LDAP) for e-product development.
- Resolved Windows and UNIX connectivity issues using SAMBA.
- Monitored jobs on SQL server 2000 databases.
- Performed backups, restores, load balancing, and performance tuning of Web and app servers.

Education

- Master's in Computer Engineering, Fairleigh Dickinson University, NJ
- Master's degree in Physics, Andhra Pradesh, India
- Bachelor's degree in Physics, Andhra Pradesh, India

Professional Certification

- Microsoft Certified Professional Systems Engineer (MCSE)
- Microsoft Certified Professional (MCP + I)

This page intentionally left blank.

UNISYS

Resource 115

Windows Server Administrator

Key Skills and Knowledge

- Windows Server 2008 R2, 2008, 2003 R2, 2003, 2000, & NT Server
- IIS, DNS, and WINS
- .NET & COM+
- VMware 5.x, 4.x, and 3.5
- IRU 1100
- UDSC 1100
- DMS 1100
- RDMS 1100
- UREP 1100
- TIP 1100
- SOLAR & COMUS
- MASM 1100
- SSG 1100
- ECL
- ACOB/UCOB
- ITILv3
- BladeLogic server automation
- Symantec Backup Exec system recovery

Professional Summary

Providing Windows operating system technical support for the Pennsylvania Department of Public Welfare (DPW). Install and configure operating system and apply security patches using BladeLogic. Continually support a large 24x7 server farm running Windows Server 2008 R2, Windows Server 2008, and Windows 2003 Server. Many Unisys ES7000 (/one, /G1, /G2 and /G3) servers running Windows and VMware comprise this environment. Experience with installing, configuring, and supporting the Unisys OpenTi product. Supporting and troubleshoot several OpenTi/OLTP projects.

- IIS, .NET, COM+, DNS, WINS, and performance monitoring.
- Install, configure, and troubleshoot third-party software.
- Review and install Microsoft security patches and hot fixes.
- Provided technical support for the Data Base Division of the DPW. Maintained database integrity, consistency, recovery, and support. Provided system generation, installation, and support of the network and relational database management system software (IRU, UDSC, RDMS, DMS, and UREP). Installed and supported client/server database software. Experience in database design, reorganization, maintenance, and COBOL batch/transaction programming.
- Assist DPW programmers with resolving their problems with batch and transaction programming of databases in COBOL.
- Coordinated a major DPW project to implement the first installation in the USA of the Unisys Extended Transaction Capacity (XTC) system that allowed multiple mainframes concurrent access to the DPW database. Conducted two training sessions for six new DPW employees.

Employment History and Related Experience

Unisys Corporation, Global Managed Services,
System Analyst 1, Harrisburg, PA 2006 – Present

Provide technical support for Windows operating system at DPW. Installed and configured operating system . Applied security patches using BladeLogic. Provided ongoing support for a large 24x7 server farm running Windows Server 2008 R2, Windows Server 2008 and Windows 2003 Server. Many Unisys ES7000 (/one, /G1, /G2, and /G3) servers running Windows and VMware comprise this environment.

- Install, configure, and support the Unisys OpenTi product.
- Support and troubleshoot several OpenTi/OLTP projects.
- Acquired experience with IIS, COM+, DNS, WINS, and performance monitoring.
- Install, configure, and troubleshoot third-party software.

UNISYS

Resource 115

Windows Server Administrator

Unisys Corporation, Systems & Technology,
Consultant 1, Harrisburg, PA 2005 – 2005

Provided technical support for the Network Operating Systems group at DPW. Installed and configured operating systems; provided ongoing support for a large server farm running Windows NT 4 Server and Windows 2000 Server as well as four Unisys ES7000 servers (18 partitions) running Windows 2000 Data center.

- Installed, configured, and supported the Unisys OpenTi product.
- Supported and troubleshot several OpenTi/OLTP projects.
- Acquired experience with IIS, COM+, DNS, WINS, and performance monitoring.
- Installed and configured, and troubleshot third-party software.
- Reviewed and installed Microsoft security patches and hot fixes.
- Exposed to and trained in a Dell SAN environment, with limited exposure to working with EMC Symmetrix storage.
- Successfully worked on a 9-month project coordinating activities among Microsoft, Oracle, and the Unisys Joint Support Queue to resolve major application problems with one of DPW's key Internet-facing applications. Played a key role in providing ES7000 support during the project—supported requests from all three companies.

Unisys Corporation, Systems & Technology,
Architectural Specialist, Harrisburg, PA 1993 – 2000

Provided daily on-site software technical support for the Data Base Division of DPW. Maintained database integrity, consistency, recovery, and support. Responsible for system generation, installation, and support of network and relational database management system software. Installed and supported client/server database software.

- Acquired experience in database design, reorganization, maintenance, and COBOL batch and transaction programming.
- Assisted DPW programmers in resolving their database and COBOL batch and transaction programming problems.
- Coordinated a major DPW project to implement the first installation in the USA of the Unisys XTC system that allowed multiple mainframes concurrent access to the DPW database.
- Conducted two training sessions for six new DPW employees.

Pennsylvania Power and Light Co, Developer,
Allentown, PA 1992 –1992

Learned and used the SAS language in writing performance analysis programs to analyze the use of IBM mainframes.

UNISYS

Resource 115

Windows Server Administrator

Education

B.S., Computer and Information Science, Bloomsburg University, Bloomsburg, Pennsylvania 1983

Major: Computer and Information Science

Minor: Business Administration

Training

Unisys Professional Education includes classes on:

- Relational/Network Database Design
- Relational/Network Database Programming
- Database System Installation and Support
- Transaction. Assembler, and COBOL Programming

Certifications

- ITIL V3 Foundation
- Microsoft Certified System Engineer (Windows NT 4)
- Microsoft Certified Professional + Internet
- Microsoft Certified Professional

This page intentionally left blank.

UNISYS

Domino Technologies Inc.

Resource 116

Windows Server Administrator

Key Skills and Knowledge

- On-site consulting services for Microsoft and various network
- Create architectural documentation for delivery of network and server requirements
- Support and resolve Microsoft Active Directory, IIS, SQL, Server 2008 R2, and Web applications
- MCSE, MCP+I, CCNA (recertifying), and MSS certifications

Professional Summary

Qualifications include 12 years of nationwide government and healthcare IT consulting and many years of mid-level management experience. Thorough understanding of all Microsoft server, network, and SQL database technologies. Hold MCSE, MCP+I, and MSS certifications. Recertifying for CCNA.

- Have an extensive background in LAN and WAN environments
- Served as a CDMS director of professional services and senior systems engineer on the Commonwealth of Pennsylvania Comptroller's Office consulting project, including seven Commonwealth agencies
- Provided network services for many large and medium-sized companies throughout the United States
- Certified in Kodak and several other ECM technologies.

Employment History and Related Experience

Unisys Corporation, Deployment Consultant, Commonwealth of Pennsylvania Enterprise Data Center — 2011 – 2012

Provide on-site consulting services for Microsoft and various network technologies to Commonwealth agencies as part of a multiyear project to move all off-site server and application operations to one central data center leveraging VM technologies.

- Create architectural documentation for delivery of network and server requirements to a Data Center engineering team facilitating relocation deployments of field network operations.
- Support and resolve Microsoft Active Directory, IIS, SQL, Server 2008 R2, and Web applications.

Computer Document Management Systems, Senior Systems Engineer — 1999 – 2011

Provided management-level support for large services engagements. Served as systems engineer and project manager for Microsoft network and Cisco WAN consulting activities. Configured and supported all Microsoft ,Cisco, SQL, and VM server technologies (SQL and Exchange certified).

- Provided strong network troubleshooting skills (always sought by others for resolutions when all others failed).
- Installed and supported document management, ECM, OCR, workflow, and storage technologies.
- Provided enterprise-level hardware planning and installation services.

Resource 116

Windows Server Administrator

- Solved server and network performance issues through performance monitoring and baselining.

NetVision, Technical Consultant 1999 – 1999

Designed, laid out, and implemented computer networks.

Fleming Foods, Regional Manager 1990 – 1998

Managed about 120 locations (400 associates) covering three states.

Education

Harrisburg Area Community College, DCTS (degree in Electronic Technology)
JFC IT Training Center, Camp Hill, PA (MCSE, MCP+I, and Advanced DOS)
SCG Senior Management Training Program, Training Center, Woodbridge, NJ
Human Relations course, Dale Carnegie
Effective Writing, Cornell University

Certifications

- Microsoft Certified Systems Engineer

UNISYS

e&e IT Consulting Services, Inc.

Resource 117

Windows Server Administrator

Key Skills and Knowledge

- Top secret clearance
- Security +
- Network +
- SCCM

Professional Summary

9 years of solid technical experience with supporting Windows networks and server farms. Performed remote customer support from SCCM, imaged PCs, administered user accounts in Microsoft Active Directory, wiped hard drives to comply with DoD security, recommended and implemented solutions for hardware and software problems, and used Remedy for tracking incident tickets.

Developed network boot CDs, slipstreamed Windows XP Server Pack 2, and customized a Bart PE disk for a department. Completed physical network drop installations and all relevant IP addressing information for efficient administration of network.

Employment History and Related Experience

e&e IT Consulting Services, DLA, RFID Administration Technical Support, New Cumberland, PA 2012 – Present

Maintain radiofrequency (RF) Windows 2003 and 2008 servers and RFID portal health metrics. Report downed equipment; configure handheld RF scanners; tracking assets.

e&e IT Consulting Services, End User Support Technician, DLA, New Cumberland, PA 2011 – 2012

Performed remote customer support from SCCM, imaged PCs, administered user accounts in Active Directory, wiped hard drives to company with DoD security, recommended and implemented solutions for hardware and software problems, and used Remedy for tracking incident tickets.

Qinetiq-NA, System Administator, NASA Goddard Space Flight Center, Greenbelt, MD 2007 – 2011

Redesigned and upgraded an isolated Active Directory, implemented a backup database, and designed a VMware workstation and server for software development. Designed and installed an upgrade to network infrastructure, upgraded server hardware, and maintained custom images for specialized systems.

- Responded to virus alerts.
- Customized PE disk for security compliance.
- Built and maintained custom images for specialized systems.
- Developed a digital signage system.

e&e IT Consulting Services, Inc.

Resource 117

Windows Server Administrator

- Configured partial counters for a clean room.
- Attended training for managing and maintaining Microsoft Windows Server 2003.

Harrisburg Area Community College, Instructional Support Technician, Harrisburg, PA 2005 – 2007

Distributed and set up instructional equipment. Troubleshot PCs, LCD projectors, and audiovisual equipment. Provided temporary network access in classrooms. Assisted users in accessing data over the campus network.

- Performed transportation assembly and permanent installation of computer and audiovisual equipment.
- Installed, troubleshot, and supported SmartTechnology.
- Set up and troubleshot audio-conferencing equipment.
- Processed user requests for instructional equipment.

Harrisburg Area Community College, End User Support Technician, Harrisburg, PA 2003 – 2005

Developed network boot CDs, slipstreamed Windows XP Server Pack 2, and customized a Bart PE disk for a department. Completed physical network drop installations and all relevant IP addressing information for efficient administration of the network.

- Made CAT 5e patch cables, installed plenum cabling for network and telephone drops around campus, and transported computers to all branch campuses.
- Troubleshot PCs, repaired laser printers, troubleshot hardware on existing computers, and was instrumental in the rollout of more than 2,000 PCs.
- Inspected unboxed hardware and entered serial numbers into a database.
- Conducted a campus-wide inventory of all hardware components, including identification of leased PC components for return to vendors.

Education

A.S., Electronic Engineering Technology, Harrisburg Area Community College, 2003

A.S., Nanofabrication Manufacturing Technology, Harrisburg Area Community College, 2002

Certifications

- CompTIA Security+ Certificate, 2011
- CompTIA Network+ Certificate, 2005
- CompTIA A+ Certificate, 2004

UNISYS

e&e IT Consulting Services, Inc.

Resource 118

Windows Server Administrator

Key Skills and Knowledge

- DOD Top Secret Security Clearance
- MCSE
- DCSE
- Design, construction, testing, and implementation of server farm infrastructure in a Windows environment
- Project management
- Asset management
- Backup and restore
- Parts replacement
- Incident management
- Server farm monitoring
- Case management
- Server farm management and administration

Professional Summary

Apply specialized knowledge of systems and server farm infrastructures that include conceptualizing, designing, constructing, testing, implementing, and optimizing systems. Enable and support business, manufacturing, and engineering functions. Interact with customers, clients, and team members daily to gain an understanding of the business environment, technical context, and the organization's strategic direction.

- Operating Systems – Experience with supporting, installing, and configuring Microsoft Windows platforms, including Windows Server 2003, 2000, NT, XP Professional, Vista, and Microsoft Exchange
- Software – Experience with supporting, installing, and configuring Active Directory, Microsoft Office, Norton AntiVirus Corporate Edition, Symantec Ghost, Tivoli, Remedy Action Request System, BlackBerry Desktop, Netscreen Remote, and PC Firewalls
- Hardware – Dell servers; HP servers; Dell desktops and laptops (Optiplex and Latitude series); HP notebooks; Panasonic notebooks; Micron desktops and notebooks; IBM ThinkPad notebooks; BlackBerry 957, 6510, 7280, 7780, and 7790 wireless devices; and Palm Pilots
- Experience with upgrading and repairing IBM and PC computers.

Employment History and Related Experience

HP Enterprise Services, Navy Marine Corps Intranet Server Farm Operations, Consultant, Mechanicsburg, PA 2005 – Present

Provide on-site server farm operation support and troubleshooting of various Windows 2000 Server and Windows Server 2003 and data storage systems in coordination with a regional network operations center.

- Conceptualize, construct, test, and implement, integrated network, hardware, and software solutions; distributed computing solutions; and physical and logical communication networks for the client. Manage quality and records for the team.
- Create Remedy change, task, and help desk requests for server farm projects and maintenance scheduling. Administer the tickets from approval through completion. Perform the following duties according to documented procedures: project management, asset management. backups and restores, parts replacement, incident management, server farm monitoring, case management, and server farm management and administration. Repair systems and coordinate recoveries around the clock.
- Install operating system base builds in accordance with approved configuration documentation as required. Coordinate all testing and

maintenance of server farm power and environmental systems.

- Provide Tier 3 access to the NMCI Active Directory when ACTRs require assistance with resetting passwords, and verifying that user accounts are enabled or disabled and allowing access to shared databases.
- Provide technical advice and on-site assistance with issues dealing with data access and the required rights for a customer to access his or her data.

TSR, Inc., Navy Marine Corps Intranet Operations,
Consultant, Mechanicsburg, PA 2003 – 2005

Resolved issues with user accounts, roaming profiles, and passwords using Active Directory. Researched user and computer associations with applicable software. Provided on-site end user assistance as well as support for and orientation to new computer systems.

- Maintained and updated computer software and hardware. Provided on-call/off-hours support for a server farm. Provided support for Black Berry Wireless devices and for client remote access using Netscreen client. Used Remedy ARS to open, work, and resolve trouble tickets. Used Tivoli Remote Management Agent to remotely resolve software issues.
- Provided support for the classified side of the NMCI network. Planned, installed, implemented, modified, and operated all end user computing equipment, including all PCs and peripheral configurations, hardware, and software.
- Assisted end users with complex access and usage problems. Troubleshot problem calls. Assisted with the preparation and installation of new equipment. Developed operating procedures.
- Served as the principal technical expert on BlackBerrys, software, and hardware. Because comfortable working routinely with little or no supervision.

TSR, Inc., Naval Supply Systems Command Help
Desk/Computer Specialist, Mechanicsburg, PA 1999 – 2003

Provided notebook and desktop support for more than 500 clients on a Novell/NT network with Windows 2000, Windows NT Workstation, and Windows 95 and 98 machines using Lotus Notes R5 for e-mail.

- Developed and updated images for new notebooks using Symantec Ghost Imaging software.
- Provided support and training for users of BlackBerry wireless and Palm Pilot handheld devices.
- Provided support and training for Lotus Notes remote clients. Configured notebooks for remote use. Answered telephone calls for support.
- Covered the help desk as needed to answer incoming support calls; determined the priority of each call and assigned it to appropriate support staff.

e&e IT Consulting Services, Inc.

Resource 118

Windows Server Administrator

- Created documentation and procedures for use by clients and the information center.

Laurel Bank, Electronic Banking Product Specialist,
Johnstown, PA 1996 – 1999

Provided support to customers using the bank's electronic banking products: PC Banking, Business PC Banking, and the IVR telephone system. Upgraded software and hardware for the electronic banking systems. Created and produced monthly statistical reports tracking the usage of the three electronic banking products. Wrote daily work procedures to be used by customers, branch offices, and the electronic banking department.

Education

Data Processing, Greater Johnstown Area Vocational-Technical School, Johnstown, PA, 1990

Microsoft Certified Systems Engineer (MCSE) classroom training, 1999

MCSE Certification, 2000

Certifications

- Microsoft Certified Systems Engineer (MCSE Windows NT)
- Dell Certified Systems Expert (DCSE Latitude Series Notebooks)

This page intentionally left blank.

UNISYS

X86 Infrastructure Architect Engineer

This page intentionally left blank.

UNISYS

Domino Technologies Inc.

Resource 119

X86 Infrastructure Architect/Engineer

Key Skills and Knowledge

- VMware - Vsphere, VCenter VMotion, ESX, ESXi
- Enterprise level security infrastructure
- Proxies
- Citrix XenServer
- EAI Enterprise Application Integration
- IBM MQ Series
- Integration Brokers, Mercator, Cyclone.
- Active Directory
- HP configuration Management - Radia
- Automated application and security patch management
- HP OpenView Systems and application monitoring.
- ITIL Practices
- DePICT Project Management
- Remedy Helpdesk, CMDB
- MS Office
- IPS's
- IBM and HP Blade servers
- IBM AIX operating system
- IBM PowerPC Servers
- HPUX VPARs and LPAR's
- HP Service Guard
- IBM HACMP
- Microsoft Clustering
- NLB Network Load Balancing
- Oracle 10g RAC Real Application Clusters
- MS SQL Servers
- Clustered SQL Servers
- EMC Symmetrix class Storage
- EMC CLARiiON Class Storage
- FC, FCoIP. FcoE
- SAN Storage and Recovery

Professional Summary

Contract for a Pennsylvania government agency to deliver a centralized application to view hundreds of video cameras located across the commonwealth over the internet utilizing existing and new infrastructure. Utilized visual networks data probes to ascertain utilization and performance data. Analyzed the existing network infrastructure and make recommendations to upgrade, replace or modify the infrastructure as necessary to facilitate the new application

- Certifications: Microsoft Certified Professional- MCP, CheckPoint Firewall, SANS Windows Server Security, Project Management, RADIA, ITIL
- Provide Disaster Recovery solution that was not practical at the time of applications distribution.
- Reduce new application provisioning times and costs.
- Designed, tested and delivered a solution to centralized applications that were distributed throughout the United States. By utilizing VMware Technologies I was able to reduce costs and improve service levels.
- Provide senior-level technical leadership to application development and implementation teams.
- Provide designs for complex solutions in conjunction with vendor specialists
- Preparing and delivering design and solution presentations to the business.
- Worked with delivery teams to ensure that all solutions could be delivered within the customer time line, budget as well as support after deployment.

Employment History and Related Experience

Solution Architect, 2011 – 2012

Contract for a military institution in the greater Harrisburg Area, creating the technical design and business case for application centralization design and implemented solutions based on those recommendations.

- Designed, tested and delivered a solution to centralized applications that were distributed throughout the United States. By utilizing VMware Technologies was able to reduce costs and improve service levels.
- Presented a power point outlining business justification for centralizing distributed applications
- Utilized VMware allowing the customer to better utilize existing and future hardware
- Provide Disaster Recovery solution that was not practical at the time of applications distribution.
- Reduce new application provisioning times and costs.

Domino Technologies Inc.

Resource 119

X86 Infrastructure Architect/Engineer

- Brocade SAN Directors and switches
- WAN/LAN Networks
- Cisco Catalyst 6500 series router
- Cisco 2900 series edge routers
- Cisco IOS firewall
- F5 BigIP, and GTM
- Check Point Firewalls,
- IDS's

Technical skills

- Microsoft Desktop operating system's, XP, Vista MS-SQL; System infrastructure and Clustering.
- Microsoft Server operating system's 2003 Oracle and Oracle RAC (System infrastructure)
- EMC DMX, CLARiiON, Clarai Centera SRDF Commvault backup/restore SAN – Brocade switches and Directors HP OpenView - Node manager, Operations manager
- Cisco IOS - Switches, Routers and PIX Firewalls EDI.– Mercator, MQSI, Cyclone, IBM -MQ Series TCP/IP and routing protocols EGIRP, OSPF, BGP etc... CheckPoint Firewalls Clustering –MS Clusters, HP-ServiceGuard AIX-HACMP Citrix Application hosting
- F5 –Bip IP and GMT VMware server virtualization;

- Presented costs and timelines for the initial centralized infrastructure build out.
- Produced cost saving and service improvement estimates capable of being delivered by the new centralized application hosting environment.
- Utilizing existing technical staff in building the initial testing and development environment utilizing Blade server hardware
- Capacity planning and management was achieved using VMware's DSR with clustered groups. Vsphere servers were automatically load balanced within a cluster group
- Fault tolerance and disaster Recovery was achieved using Vmotion
- After initial testing was successfully completed in the development environment the production environment was built

Commonwealth, Solution Architect, 2009-2010

Contract for a Pennsylvania government agency to deliver a centralized application to view hundreds of video cameras located across the commonwealth over the internet utilizing existing and new infrastructure.

- During the data gathering phase the Wide Area Network provider was able to provide circuit utilization and performance reports for most of the WAN circuits
- Utilized visual networks data probes to ascertain utilization and performance data
- Analyzed the existing network infrastructure and make recommendations to upgrade, replace or modify the infrastructure as necessary to facilitate the new application
- Microsoft performance monitor was used for Wintel systems. Tivoli was used for the UNIX and Linux systems
- Presented embedded Visio diagrams out lining analysis and recommendations to project stakeholders. Conducted meetings with the project team to address concerns and revisions until a workable set of recommendations were achieved

Bise LLC, Software Development, Systems Hosting, 2008 to Present

Deliver custom software to automatically trade electronic financial markets in a black box configuration, maintain all systems, applications and networks to host customer broker accounts on the systems.

- The hosting application is Meta trader 4.0 running on Windows Server 2003. VMware ESX is used to host each customer on their own operating system.

Domino Technologies Inc.

Resource 119

X86 Infrastructure Architect/Engineer

DHL Logistics IT Infrastructure Architect, 1999 -2008

Provide senior-level technical leadership to application development and implementation teams. Champion new solutions and approaches and guide successful technical adoption through mentoring, instruction, and by actively participating in system implementation projects.

- Provide designs for complex solutions in conjunction with vendor specialists
- Liaise closely with Service Delivery Managers and their technicians to ensure correct scoping and pricing of solutions.
- Preparing and delivering design and solution presentations to the business.
- Work closely with vendors and external customers as well as Services Delivery Managers and the business to design and package together solution offerings.
- Worked with delivery teams to ensure that all solutions could be delivered within the customer time line, budget as well as support after deployment.
- Maintain up-to-date knowledge of present and future technological trends, processes and methodologies and maintain a strong understanding of all IT technologies.

Solution Technologies Incorporated, Systems Consultant, 1997 – 199

Design and build LAN's, File and Print systems, E-mail systems, Database servers and desktops for various customers. Provide ongoing system support to customers.

- Create and maintain system architecture models and designs.
- Conduct technical research and prototyping of technical solutions.
- Create detailed requirements specifications to fulfill product requirements

Exxon, Systems Consultant, 1995 – 1997

Two year project for Exxon Corporation; Designed and implemented WAN/LAN's, File and Print systems, E-mail systems, Database servers and desktops. Provide ongoing system support to customers.

Enviro-Test, Systems Consultant, 1994-1995

Lead in the development of a 57 node WAN and 57 new LAN's for a Pennsylvania State contract for emissions testing; provided Level 3 support and maintenance for statewide computing systems.

Domino Technologies Inc.

Resource 119

X86 Infrastructure Architect/Engineer

Scantron, Regional Service Manager1986- 1994

Responsible for one quarter of the companies services revenue with complete P/L and budgetary responsibility. Work closely with sales teams to increase profitability through new sales and new service products. I developed and managed service delivery teams in 10 branch offices.

Education

- Newport College – Engineering and Computer Science, 1986
- Laurel Highland High School 1982

Certifications

- Microsoft Certified Professional- MCP
- CheckPoint Firewall
- SANS Windows Server Security
- Project Management, RADIA, ITIL

UNISYS

Resource 120

IBM

Midrange Infrastructure Architect / Engineer

Key Skills and Knowledge

- Systems Analysis/Implementation
- System Design/Development
- Virtualization Strategies
- Data Center, Engineering and Infrastructure Planning/Design
- Migrations
- Systems
- Architecture
- Strategic Planning/Testing
- Cloud Services
- Quality Assurance
- ProcessImprovement
- Problem Identification/Resolution
- Lifecycle Management
- Disaster Planning/Recovery
- Systems Reliability/Troubleshooting
- Security/Risk Management
- Web-Based Solutions
- Cost Controls
- Relationship-Building
- Strategic Communications
- Customer Satisfaction

Skills Summary

Highly-accomplished, results-driven senior IT Infrastructure Engineer/Architect with vast background of skills and expertise devising innovative, cost-effective solutions that increase technical capabilities, boost productivity and contribute to business growth. More than 17 years of enterprise-level infrastructure experience with demonstrated achievements impacting superior performance in areas of systems analysis/engineering, technology development/ deployment, process redesign, virtualization and cloud computing. Dedicated problem-solver with outstanding communication, relationship-building and customer satisfaction attributes.

Employment History and Related Experience

HENDALPHER CONSULTING /MOREDIRECT, Consulting Systems Analyst, Buckeye, Arizona, 2011-To Date

Satisfied business requirements through strategic systems analysis and planning success for client, Catholic Healthcare West (CHW), adeptly identifying/resolving critical IT issues that affect business performance.

- Valued as knowledgeable technical advisor building trust and keeping systems running and problem free by assessing needs and conceptualizing cost-effective solutions, processes and procedures for best results.
- Expanded technical capabilities as Systems Engineer/Liaison for CHW overseeing server refresh, consolidation and migration of applications and resources from older unsupported hardware to new virtual or actual systems.
- Reduced impact of migration and transition to new systems through implementation of strict change controls in collaboration with CHW engineering teams, Dell outsourcing partners, resource teams and application owners.
- Improved application and systems reliability by expertly performing complex change and OS platform build outs according to customer specifications. Conducted server/application inventory audits on 200+ systems.
- Delivered OS level support and guided application teams before, during and after migration to resolve outlying issues and OS level problems.

CVS / CAREMARK, Systems Analyst (PBM), Scottsdale, Arizona, 2004-2010

Devised effective virtualization strategy to fulfill user needs as VMWare Infrastructure and Systems Lead of vSphere/HP Chassis design and implementation team for private cloud computing.

- Performed expert operational transformation and employed latest technology in redesign of data center as Engineering Team Infrastructure Liaison with architecture, application, vendor and data/storage teams.
- Increased operational efficiency by developing innovative, enterprise-wide virtualization and data center reduction initiatives. Engineered effective network

and storage requirements.

- Optimized achievement of organizational objectives, increased quality and mitigated risk by developing ESX Farm to host mandated application lifecycle, including infrastructure development, QA and disaster recovery.
- Developed Web content and facilitated workplace collaborations through SharePoint 2007 farm-wide administration in instrumental role on SharePoint design and implementation team. Directed farm migrations.
- Elevated operational performance through infrastructure and core application rollout, design and builds for SME. Delivered infrastructure support for 2100 WINTEL/VMWare systems in 53 locations across the US.
- Supported 10+ enterprise-scale application deployments as Project Engineer/Wintel Systems Engineer for core and high profile application rollouts on VMWare and Wintel OS platforms, including 30+ Web-based projects.

NATURAL DATA, INTEL CORP, Consulting Systems Engineer, Phoenix, Arizona, 2004

Enhanced productivity and operational effectiveness in support of Intel SPEC control and document management development teams. Cataloged/documented greater than 10 systems and virtual servers.

- Utilized advanced analytical skills to conduct requirements analysis, capacity planning and feasibility testing to compare MS Virtual Server 2005 with existing VMWare solutions.
- Updated systems and improved performance through hardware reallocation, host deployment, server imaging, load balancing, reporting and documentation of findings for deployment and maintenance.

TEK SYSTEMS, IBM for AMERICAN EXPRESS, Delivery Systems Administrator, Phoenix, AZ, 2003

- Served in key supporting role as Wintel Systems Administrator delivering 2nd and 3rd level support for more than 250 3-tier Web applications on 1000+ American Express data complex servers for IBM Global Services. Drove business/technical success by creating WMI/SQL Server/Web tool for mapping app to server for billing and server management. Performed code changes, security patches, problem resolution, and break/fix analysis.

VOLT TECHNICAL SYSTEMS, Performance Systems Engineer, Redmond, Washington, 2001-2002

Achieved exemplary performance in systems design, implementation and administration of Windows Server 2003 builds as MS Windows Core Development Team Member, performing stress and performance analyses for Windows Server

Resource 120

Midrange Infrastructure Architect / Engineer

2003 release with TPC-c, TPC-h and SAP benchmarking.

STAMPS.COM, Systems Engineer, Bellevue, Washington, 2000-2001

Facilitated major application releases as Systems Engineer for development, test, QA and stress teams. Redesigned/administered Web, SQL and Domain servers. Restored production database.

- Supported corporate and production initiatives by managing rollout of SNMP, SNTP, load-balancing and reporting servers. Served as build engineer for Visual SourceSafe code libraries for development teams.

SALTMINE LLC, Systems Engineer, Seattle, Washington, 1998-2000

Successfully executed project with MSN and MCP design and application Web teams, as well as Nordstrom in-house design group. Provided expert oversight of server/network architecture. Administered 75+ servers.

BOEING COMMERCIAL AIRPLANE GROUP, Systems Analyst 3, Renton, Washington, 1996-1998

Performed systems administration/requirements analysis for 737-757 final assembly and wing responsibility center (WRC) initiatives. Technical Lead for WRC executive and airplane-on-ground engineering teams.

Certifications

Certifications: MCP, MCSE

Training: VMWare, vSphere, SharePoint, XHTML, CSS, Web Development, VB, .NET, MS Windows Server, Active Directory, Data Warehouse with SQL Server, MS Access, Database Design, MS Systems Management Server, Client/Server Networking Design and Architecture, Client/Server Analysis and Design, LAN, TCP/IP, Computing Security, Windows NT, MS Office

This page intentionally left blank.

UNISYS

Resource 26

X86 Infrastructure Architect/Engineer

Key Skills and Knowledge

- VMware vSphere 4/5 & ESX/ESXi
- Windows
- Active Directory
- EMC Avamar
- Symantec NetBackup
- Disaster Recovery Planning
- PowerShell Scripting

Professional Summary

Knowledge in the following: VMware vSphere ESX/ESXi 3.x, & 4.x, & 5.x, Windows 2003/2008, PowerShell & VB Script, Active Directory, Security Policies, IIS, DHCP, DNS, FTP, IBM Blade Center Servers, Dell Commodity Servers, EMC Data Domain, EMC Avamar, Microsoft Failover Clustering, Network Load Balancing, Microsoft DFS & DFS-R.

Capable in the following Server software: BMC BladeLogic, MS Exchange 2000, 2003, 2007, Microsoft SQL 2005/2008 management, Symantec NetBackup 6.x, & 7.x, Backup Exec System Recovery, Symantec AV, McAfee w/EPO, Symantec Ghost, WSUS, IBM Tivoli Endpoint Manager, Microsoft System Center Ops Manager 2007 & 2012.

Employment History and Related Experience

Unisys Corporation, Systems Analyst, Harrisburg, PA, 2008 – Present

Responsible for multiple government agencies at central PA Data Center. Responsible for troubleshooting systems, Active Directory, Patch Management, AntiVirus. Windows/VMware Team Lead responsible for maintaining ~800 Servers in the data center. Roles include:

- VMware Administrator of 350+ VMs (approx 50 ESX/ESXi hosts in 5 virtual centers, including Disaster Recovery site)
- Two site Active Directory & DNS Administrator
- Backup Administration including NetBackup, DataDomain, Avamar
- Scripting for server automation using mostly PowerShell, VBScript, & PowerCLI (VMware).
- Disaster Recovery testing multiple times annually
- Maintain Large 2 Instance SQL 2008 Cluster used for Multiple application management
- Maintain 3 DFS deployments
- Incident & Change Management control
- Technical Documentation using tools like Word & Visio
- BladeLogic Patch Management
- Systems Builds/Deploys
- Basic Linux administration support (SUSE & Redhat)
- Migrate, Update & maintain Windows 2000 Active Directory migration to Active Directory 2008 R2. Migrate COPA file share from single node 2003 file server to 2 node 2008 Distributed File Server with Replication (DFS & DFSR).
- Build Terminal Services & RemoteApp for central application control & updating for DPH Operations Staff.

UNISYS

Resource 26

X86 Infrastructure Architect/Engineer

- Migrate the DPH management infrastructure from hosts file management to fully integrated DNS including multi-site Active Directory replication & implement GLOBALNAMES zone as a replacement to WINS
- Established a one-way trust with CWOPA domain and internal management domain (ESM) to allow State employees single sign-on to DPH resources managed by Unisys such as performance metrics, or backup reporting, etc.
- Built/assist with managing DPH Shared VMware virtual Infrastructure (8 host cluster & virtual center)
- Built/manage IES Virtual VMware Infrastructure (28 host 2 Blade Center cluster, and 4 hosts in 2 other clusters & Virtual Center)
- Migrate 70+ Physical servers from IES data center to DPH data center as Virtual using Avamar backup & restore
- VM Convert many physical servers to virtual once servers come end of life
- Installed or assisted installs and upgrade EMC Avamar 5.x & 6.x & EMC DataDomain systems
- Built or upgraded multiple Symantec NetBackup systems versions 5.1, 6.0, 6.5, 7.0, 7.1 & 7.5.
- Consolidate & upgrade DPH NetBackup infrastructure from 6 isolated backup environments to a large dynamic redundant Backup infrastructure allowing for faster backup & restore times, higher reliability & resiliency, and save costs by utilizing fewer tapes and backup servers, and network equipment.
- Perform multiple disaster recovery tests for PSP, DPW-CAPS, IES including
  - Physical Server to Virtual server restore
  - Bare Metal restore from NetBackup Tape & Avamar
  - VMware restores
  - Avamar restores
  - NetBackup Tape restores
  - DataDomain Oracle restores
  - MS SQL 2000, 2005, & 2008 restores
  - Windows 2003, & 2008 Cluster restores to a single nodes
- Written many VB & PowerShell scripts for use in Backup & restores, Server subnet IP changes, regular scheduled tasks, VMware tasks with PowerCLI, and software installations/tweaks

Business Information Group, Network Engineer, York, PA, 2008 – 2008

Installed numerous servers including Windows 2003 & 2008, SBS 2003, SQL Server, VMware, and Terminal Server. Installed servers from HP, IBM, and Dell.

- Partially or Fully administered almost 30 AD domains during the contract (Users counts ranging from 10-200+)
- Multiple Small Office Setups & relocation.

UNISYS

Resource 26

X86 Infrastructure Architect/Engineer

Rite Aid Corporation, Field, Systems Administrator & Development, Harrisburg, PA, 2004 – 2007

Support Servers (Both Windows NT4, 2000, 2003 & SCO5), Cisco Routers, Support PCs, Setup & Repair of HP and Lexmark Printers, Network wiring of 29 Rite Aid Pharmacy Stores

Education

- Fall 2000 - Spring 2002 Penn State University Hazleton, PA
- Associate Degree in Information Sciences & Technology
- Graduated May 2002 with Associate degree in Computer Networking.

Certifications

- VMware VCP4 & VCP5
- Microsoft Windows 2008 MCITP:SA
- ITILv3

This page intentionally left blank.

UNISYS

Resource 115

X86 Infrastructure Architect/Engineer

Key Skills and Knowledge

- Windows Server 2008 R2, 2008, 2003 R2, 2003, 2000, & NT Server
- IIS, DNS, and WINS
- .NET & COM+
- VMware 5.x, 4.x, and 3.5
- IRU 1100
- UDSC 1100
- DMS 1100
- RDMS 1100
- UREP 1100
- TIP 1100
- SOLAR & COMUS
- MASM 1100
- SSG 1100
- ECL
- ACOB/UCOB
- ITILv3
- BladeLogic server automation
- Symantec Backup Exec system recovery

Professional Summary

Providing Windows operating system technical support for the Pennsylvania Department of Public Welfare (DPW). Install and configure operating system and apply security patches using BladeLogic. Continually support a large 24x7 server farm running Windows Server 2008 R2, Windows Server 2008, and Windows 2003 Server. Many Unisys ES7000 (/one, /G1, /G2 and /G3) servers running Windows and VMware comprise this environment. Experience with installing, configuring, and supporting the Unisys OpenTi product. Supporting and troubleshoot several OpenTi/OLTP projects.

- IIS, .NET, COM+, DNS, WINS, and performance monitoring.
- Install, configure, and troubleshoot third-party software.
- Review and install Microsoft security patches and hot fixes.
- Provided technical support for the Data Base Division of the DPW. Maintained database integrity, consistency, recovery, and support. Provided system generation, installation, and support of the network and relational database management system software (IRU, UDSC, RDMS, DMS, and UREP). Installed and supported client/server database software. Experience in database design, reorganization, maintenance, and COBOL batch/transaction programming.
- Assist DPW programmers with resolving their problems with batch and transaction programming of databases in COBOL.
- Coordinated a major DPW project to implement the first installation in the USA of the Unisys Extended Transaction Capacity (XTC) system that allowed multiple mainframes concurrent access to the DPW database. Conducted two training sessions for six new DPW employees.

Employment History and Related Experience

Unisys Corporation, Global Managed Services, System Analyst 1, Harrisburg, PA, 2006 – Present

Provide technical support for Windows operating system at DPW. Installed and configured operating system . Applied security patches using BladeLogic. Provided ongoing support for a large 24x7 server farm running Windows Server 2008 R2, Windows Server 2008 and Windows 2003 Server. Many Unisys ES7000 (/one, /G1, /G2, and /G3) servers running Windows and VMware comprise this environment.

- Install, configure, and support the Unisys OpenTi product.
- Support and troubleshoot several OpenTi/OLTP projects.
- Acquired experience with IIS, COM+, DNS, WINS, and performance monitoring.

UNISYS

Resource 115

X86 Infrastructure Architect/Engineer

- Install, configure, and troubleshoot third-party software.

Unisys Corporation, Systems & Technology, Consultant 1, Harrisburg, PA, 2005 – 2005

Provided technical support for the Network Operating Systems group at DPW. Installed and configured operating systems; provided ongoing support for a large server farm running Windows NT 4 Server and Windows 2000 Server as well as four Unisys ES7000 servers (18 partitions) running Windows 2000 Data center.

- Installed, configured, and supported the Unisys OpenTi product.
- Supported and troubleshot several OpenTi/OLTP projects.
- Acquired experience with IIS, COM+, DNS, WINS, and performance monitoring.
- Installed and configured, and troubleshot third-party software.
- Reviewed and installed Microsoft security patches and hot fixes.
- Exposed to and trained in a Dell SAN environment, with limited exposure to working with EMC Symmetrix storage.
- Successfully worked on a 9-month project coordinating activities among Microsoft, Oracle, and the Unisys Joint Support Queue to resolve major application problems with one of DPW's key Internet-facing applications. Played a key role in providing ES7000 support during the project—supported requests from all three companies.

Unisys Corporation, Systems & Technology, Architectural Specialist, Harrisburg, PA, 1993 – 2000

Provided daily on-site software technical support for the Data Base Division of DPW. Maintained database integrity, consistency, recovery, and support. Responsible for system generation, installation, and support of network and relational database management system software. Installed and supported client/server database software.

- Acquired experience in database design, reorganization, maintenance, and COBOL batch and transaction programming.
- Assisted DPW programmers in resolving their database and COBOL batch and transaction programming problems.
- Coordinated a major DPW project to implement the first installation in the USA of the Unisys XTC system that allowed multiple mainframes concurrent access to the DPW database.
- Conducted two training sessions for six new DPW employees.

Pennsylvania Power and Light Co, Developer, Allentown, PA, 1992 –1992

Learned and used the SAS language in writing performance analysis programs to analyze the use of IBM mainframes.

UNISYS

Resource 115

X86 Infrastructure Architect/Engineer

Education

B.S., Computer and Information Science, Bloomsburg University, Bloomsburg, Pennsylvania 1983

Major: Computer and Information Science

Minor: Business Administration

Training

Unisys Professional Education includes classes on:

- Relational/Network Database Design
- Relational/Network Database Programming
- Database System Installation and Support
- Transaction. Assembler, and COBOL Programming

Certifications

- ITIL V3 Foundation
- Microsoft Certified System Engineer (Windows NT 4)
- Microsoft Certified Professional + Internet
- Microsoft Certified Professional

This page intentionally left blank.

UNISYS

IBM

Resource 121

X86 Infrastructure Architect/Engineer

Key Skills and Knowledge

Operating Systems

- System x
- Blade Servers
- Storage Systems
- Red Hat
- NetApps
- Microsoft

Professional Summary

IBM Certified System X Blade Center Top Gun specializing in System X, Microsoft, Red Hat, and Netapp Computing. Significant experience in the Cisco arena. Commands exceptional technical and communication skills, refined through years of experience in customer service, project management and consulting.

Employment History and Related Experience

IBM Corporation, IT Specialist System X/Bladecenter/ISD/Sonas, Providence, Rhode Island, 2011-To Date

System X, Bladecenter Top Gun, 1997-2010

Numark Industries, Electronic Engineer, Providence, RI, 1993-1996

Quad Eight Electronics, Design Engineer and Production Supervisor, Valencia, CA, 1989-1993

Large Financial Institution

Installed and provided trouble-shooting and supporting for ALL Windows Operating Systems and Applications.

- Was responsible to trouble-shooting networking and switch, router and gateway issues.
- Led data analyzing, backup & recovery activities.
- Consistently applied strong hardware and software trouble-shooting skills. Leveraged extensive experienced with System x Servers, Blade Servers and Storage Systems.

Large Insurance Firm

Responsible for managing Server/Network/Desktop Installation Projects.

- Leveraged depth of experience with Microsoft Hyper-V, VMware ESX, Linux and Mac OSX.
- Demonstrated an Ability to work well both independently and in a team environment.

Certification

- MCP (Microsoft Certified Professional)
- DCSE (Dell Certified Systems Engineer)
- Netapp Certified
- RHCSA (Red Hat Certified System Admin) (in progress)
- A+ Certified
- Cisco Trained

This page intentionally left blank.

UNISYS

IBM

Resource 122

X86 Infrastructure Architect/Engineer

Key Skills and Knowledge

Operating Systems

- Capacity
- Migration
- Best Practices Capacity
- Migration
- Best Practices

Professional Summary

Infrastructure Architect with extensive experience across a variety of verticals. Wide range of hands on technical skills and enterprise project experience. Excellent communication, presentation and documentation skills. Proven ability to deliver effective, scalable solutions drawing on both existing and emerging technologies.

Employment History and Related Experience

TJX Companies inc., Solutions Architect Wintel Infrastructure Services, 2011–To Present

Document and define the Business and Technical Requirements for the data center migration. Document and present a Full Architecture design document to the advisory board for technology approval. Performed capacity study of existing infrastructure to justify the required footprint within the new data facility.

- Worked closely with Enterprise Architecture to the define wintel computing platform standards.
- Lead the technical discussion on a vSphere 5 and HP blade architecture within the new data facility.
- Managed on-site resources during the phase 1 roll out within the new data facility.
- Define and document the migration of physical workloads from existing data facility to new remote location.
- Provide technical guidance on new technology within the TJX Companies, Inc. infrastructure.
- Lead the Cisco UCS PoC and Hybrid cloud effort+.

Novartis biomedical research, Solutions Architect Virtual Services, 2010 to 2010

Architected and deployed a virtualized Citrix XenApp 5.0 infrastructure for NIBR to accommodate their globalization efforts. Document and Define the Business and Technical Requirements to meet the team's charter. Documented network monitoring best practices for the remote computing environment hardware and middleware based on Citrix Edge Sight.

- Designed a GPO to allow for consistency across machines, applications and users.
- Documented application solution sets for NIBR internal support staff.
- Designed a highly scalable Citrix system by utilizing XenApp provisioning server (operating system Streaming), profile manager, and APP-V to allow for rapid expansion of the system to accommodate increased demand.

IBM

Resource 122

X86 Infrastructure Architect/Engineer

- Provide best practices – Windows operating system, Citrix configuration, security settings.
- Created a framework for design, performance testing, and support of the current and future Citrix environments.
- Worked closely with deskside engineering on a PoC effort for VDI deployment using XenDesktop, Pano Logic, and Unidesk provisioning servers.
- XenDesktop PoC use case was to design a solution for 400 test users from various areas of the Novarits research business unit.
- Lead the technical discussion on the Vsphere 4 implementation and dell blade design.

Biogen Idec, Solutions Architect/Team Lead Virtual Services, 2008-2010

Evaluate the existing VMware and Citrix infrastructure & document recommendations to accommodate biogen idec globalization efforts. Managed day to day operations and provided team leadership. Meet weekly with management in order to provide status reports on the health of the environment.

- Participated in companywide initiatives and provide virtualization and remote computing guidance.
- Documented and Defined the business and technical requirements to meet the team's charter.
- Stabilized the current Citrix environment XPe environment and document the migration path to MetaFrame Presentation Server 4.5.
- Assisted on new application rollouts and provided guidance on best practices on the Citrix systems.
- Lead and managed the global migration of the VMware 3.x infrastructure ESX 3.5 U4Wrote a custom upgrade tool to silently push and perform a hot install of the vm tools to all Windows guest VMs.
- Lead the discussions and technology direction toward the HP blade platform for biogen idec.
- Documented the logical and physical designs for the ESX platform.
- Managed the deployment VM team and documented processes regarding VM deployments and image management.
- Worked closely with all lines of business and provided guidance on implementing products into the virtual environment.
- Utilized VMware lab manager to deploy development systems for the scientific community.
- Designed custom health/environmental reports which provided forecasting and growth metrics for IT management.
- Familiar with FDA regulatory policies and procedures (GxP Compliance).

UNISYS

IBM

Resource 122

X86 Infrastructure Architect/Engineer

Robeco Investment Management, Solutions Architect, 2007-2008

Evaluate the existing Citrix Presentation server 4.0 infrastructures for Robeco and documented recommendations to accommodate their globalization efforts. Evaluated best of breed SSL VPN hardware to determine the best overall fit for Robeco. Document and Define the Business and Technical Requirements to meet the team's charter.

- Incorporate development requirements in order to provide a remote computing environment for the near shore/off shore development teams.
- Assist with the build out of VMware ESX 3.x environment (HA, DRS, VMotion, Backup)
- Leverage VMware for Citrix DEV, TEST, and CERT environments.
- Implement a Citrix DR strategy that leverages VMware in remote sites for server redundancy.
- Assist Robeco Investments with its global strategy as it relates to remote office computing.
- Designed a GPO to allow for consistency across machines, applications and users.
- Documented application solution sets for Robeco Investments internal support staff.
- Provide best practices – Windows operating system, Citrix configuration, security settings.
- Created a framework for design, performance testing, and support of the current and future Citrix environments.

Staples, Inc., Solutions Architect, 2007-2008

Architected a Citrix Presentation server 4.5 infrastructure for Staples Inc. to accommodate their globalization efforts. Implement Citrix Access Gateways to accommodate offshore partners and 3rd party vendor access. Coordinate efforts between Performance, engineering, & application QA, to qualify applications for the Citrix environment.

- Document and Define the Business and Technical Requirements to meet the team's charter.
- Incorporate development requirements in order to provide a remote computing environment for the near shore/off shore development teams and work from home initiative.
- Assisted with firewall configuration to accommodate the Citrix Access gateway infrastructure in addition to access from Citrix to the Staples restricted systems.
- Documented network monitoring best practices for the remote computing environment hardware and middleware based on the HP Open View platform.

Resource 122

X86 Infrastructure Architect/Engineer

- Assist Staples Inc. with its global strategy as it relates to off shoring, remote office computing.
- Hardened Windows operating system to meet security requirement for offshore associates.
- Designed a GPO to allow for consistency across machines, applications and users.
- Documented application solution sets for Staples Inc. internal support staff.
- Provide best practices – Windows operating system, Citrix configuration, security settings.
- Created a framework for design, performance testing, and support of the current and future Citrix environments.

Wellington Management, Solutions Architect, 2005-2007

Architected a Citrix Presentation server 4.0 infrastructure for Wellington Management LLP to accommodate their globalization efforts and Disaster recovery strategy. Coordinate efforts between Performance, engineering, & application QA, to qualify applications for the Citrix environment. Document and Define the Business and Technical Requirements to meet the team's charter.

- Incorporate additional Investments systems development requirements in order to provide a remote computing environment for the near shore/off shore development teams.
- Assist Wellington Management LLP with its global strategy as it relates to off shoring, remote office computing, and all global trading efforts.
- Designed and wrote a custom Web browser and provided guidance on application layer security as it related to Citrix application hosting for the IMS Recon partnership with State Street Bank.
- Stabilize the current Citrix environment XPe environment and document the migration path to MetaFrame Presentation Server 4.0.
- Managed the migration of all Citrix servers from end of life platforms and built new Citrix infrastructure.
- Implemented VMware solution for the following Citrix environments Dev, Test, Cert, Stage/Prod Mirror Designed a GPO to allow for consistency across machines, applications and users.
- Provided performance reports for application sizing to the internal development teams.
- Documented application solution sets for Wellington internal support staff.
- Provide best practices – Windows operating system, Citrix configuration, security settings.
- Created a framework for design, performance testing, and support of the current and future Citrix environment.
- Collaborate with users and development teams to coordinate system

maintenance policies and participated in development of comprehensive system documentation.

Fidelity Investments, Solutions Architect, 2003-2005

Managed the relationship for the Trusted Partner program (Ford, Bank of America, And Fleet Bank) to allow for seamless Citrix integration with the client native environment. Developed and managed the migration to MetaFrame Presentation Server 3.0. Evaluated and consulted with FCAT (R&D) on the 64bit operating system and Citrix Presentation server 4.0.

- Worked closely with Performance Engineering to determine best mix of physical to virtual servers per ESX host.
- Architect a Citrix MetaFrame 3.0 infrastructure utilizing Citrix Web interface, Windows Server 2003 & Active Directory authentication for over 6000 plus remote users.
- Built and currently support a Citrix Secure Gateway environment in order to allow trusted partners to manage their mutual and other employee funds. Estimated value of transacted business in excess of 25 billion.
- Manage the migration from Windows NT 4.0 TSE to Windows 2003 server infrastructure.
- Designed the Citrix GPO to facilitate the migration of local user and machine policies to active directory.
- Consulted with & Directed the Active Directory team on industry best practices for system security and infrastructure stability.
- Customized the Web interface for our internal clients – branded the Web portal to mirror Fidelity Web standards.
- Developed an H/A multi-site failover procedure for the MetaFrame environment.
- Document a standard build process for Citrix MetaFrame FR3 on Windows Sever 2003.
- Utilized Hybrid profiles in order to facilitate a standard remote user environment.
- Primary contact in the design and deployment of a Active Directory domain containing over 10,000 users which provided authentication services to central MetaFrame application servers, data stores and client server applications.
- Managed the migration of 3000 plus Citrix 1.8 users to the MetaFrame XPe & Nfuse environment.

Resource 122

X86 Infrastructure Architect/Engineer

Harvard Vanguard Medical Associates, Senior Security Consultant, 2003-2003

Architect a secure Web infrastructure for Harvard Vanguard Medical Associates. Document the principles used in a minimal trust system for Harvard Vanguard Medical Associates technical staff. Implemented a highly available and load balanced IIS cluster.

- Performed penetration and load testing of Web cluster systems.
- Review findings with HVMA information security officer.
- Built Windows 2000 DHCP servers and migrated Windows NT 4.0 scopes to new environment.

Greenwich Technology Partners, Senior Security Consultant (Fleet Boston Financial), 2003-2003

Documented the encryption policy on the RSA encryption suite for Fleet Boston Financial. Developed internal strategy for high level solution set presentation and documentation.

- Designed and implemented a VMware GSX server proof of concept environment for server consolidation & QA (Windows 2000 Advanced Server, IIS 5/6.x, & Active Directory, RedHat 8.0, Windows Server 2003, NetWare 6.0.).
- Documented the installation and configuration on each virtual environment for Fleet Boston Financial.

Fidelity Investments FISC, Senior Control-SA Security Consultant, 2001-2002

Organize, schedule and facilitate meetings with business units to establish role based profiles that include access for current and future roles.

- Coordinate with other Information Security business units to ensure correct enforcement of policies and procedures.
- Revise and document application specifications during validation in the certification environment.
- Technical architect for the implementation of the BMC Software Control-SA role based system.
- Provided business unit support for STARS program within Fidelity Investments.
- Developed Control-SA disaster recovery architecture for Fidelity Investments.
- Managed the integration of Control-SA with Active Directory for centralized access administration and reporting.
- Assisted internal customers with Control-SA agent installation and problem resolution.

IBM

Resource 122

X86 Infrastructure Architect/Engineer

- Performed the installation and configuration of Control-SA (3.01, 3.10, 3.2) and maintenance releases on Solaris 2.6 & 8.
- Managed production support of Sun servers and windows 2000 infrastructure environment.
- Integrated the following security systems within the Control-SA infrastructure – NT, Active Directory, Novell, UNIX (Solaris, VMS, and AIX), TopSecret, LDAP, IIS, and WebSphere.
- Senior technical resource for Control-SA links, Passport beta site testing.
- Utilized VMware for rapid testing of Control-SA agents in a development environment.
- Worked closely with the development team in Israel on the enhancement of the agent architecture.
- Conducted internal Control SA training for Fidelity Investments development groups.
- Provided daily operations support of Sun Solaris systems.

State Street Global Advisors, Systems Security Project Leader, 2000-2001

Integrated MS office, UNIX X Windows, and other 3rd party applications into the MetaFrame farm for remote traders and client access. Implanted Citrix resource manager in order to better monitor and load balance the Citrix systems.

- Consulted with State Street Bank on NT security policy and procedures for use within SSGA.
- Utilized Axent ESM 5.01 on NT to perform automated server audits and QA policy checks.
- Implemented Clustered Windows NT terminal for Global client access.
- Managed the implementation of a Citrix MetaFrame application server farm for SSGA.
- Managed the roll out of security profiles for all NT server builds.
- Documented all aspects of the installation and configuration process for the NT server support staff.
- Planned and Implemented Axent ESM 5.x for SSGA's NT infrastructure.
- Coordinated with the NT server team to run nightly batch jobs on NT to collect security logs.
- Managed the installation and configuration of new server hardware and Network Operating Systems.

Manulife Financial, Systems Security E-Commerce Project Leader, 2000-2000

Managed the implementation of secure NT Web servers for Manulife's Web applications. Developed Secure NT IIS 5.0 Web server configuration for

IBM

Resource 122

X86 Infrastructure Architect/Engineer

Manulife's Web infrastructure. Leveraged Windows network load balancing & windows cluster server technologies in order to provide a fault tolerant Web site.

- Integrated Web accelerators in order to offload the SSL transaction processing.
- Integrated Citrix Metaframe system for remote access and network management of Manulife systems.
- Responsible for the implementation of a Highly Available Autosys environment.
- Installed and configured Autosys batch jobs for data collection and nightly feeds to SQL databases.
- Documented the data flow within Autosys for the help desk.
- Installed and configured the Web interface to Autosys for monitoring of job status, edit, and submit new jobs.
- Managed the conversion of the NetWare 4.x to 5.x server environment.
- Coordinated with the development team to ensure full application functionality on the Secure NT Web server.
- Automated Software installs using custom INF and NT shell scripts.
- Evaluated host based security products for Web-based systems (Axent, Tripwire, etc.).
- Developed and implemented migration plan to move application data to EMC disk arrays.
- Installed and configured Microsoft IIS Web servers for E-Commerce application testing.
- Documented all aspects of the installation and configuration process for the production support staff.
- Configured nightly batch jobs on NT to collect application and security logs.
- Resolved session loss issues with the existing Microsoft SNA server environment.
- Instructed existing personal on the installation and configuration of secure NT Web servers.
- Performed the installation and configuration of new server hardware and Network Operating Systems.

Fidelity Investments, Systems Security Project Leader LAN Technical Services, 1999-2000

Managed the implementation of Fidelity Power Street NT servers and system upgrades. Consulted with @Stake inc. to develop a secure build evaluation and release process for NT. Developed Secure NT Web server configuration for Fidelity Investments Power Street Web applications.

- Leveraged Windows network load balancing & windows cluster server technologies in order to provide a geographically fault tolerant Web site.

IBM

Resource 122

X86 Infrastructure Architect/Engineer

- Integrated Web accelerators in order to offload the SSL transaction processing.
- Managed the rollout of NetWare 5.x infrastructure servers for the core file and print environment.
- Coordinated with the development team to ensure full application functionality on the Secure NT Web server.
- Consulted with Exodus Communications on other Web application projects (My Lycos, EIS, and On-line Statements).
- Implemented end to end monitoring infrastructure for NT Web servers utilizing TNG 2.1.
- Developed the future release of the secure NT Web server using Windows 2000 advanced server and IIS 5.0.
- Installed and configured NSH on both Solaris and NT platforms, utilized 3DES encryption for secure communication (ssh like peer to peer protocol).
- Leveraged VMware technology for the development of Web server security and application testing.
- Automated Software installs using custom INF and NT shell scripts.
- Implemented Axent ESM 4.x and 5.x on both NT and NetWare.
- Documented all aspects of the installation and configuration process for the integration and support teams.
- Installed and configured Sun servers for use as security log repository.
- Built Solaris servers for use NT log rotation and NTSMF data collection.
- Installed and configured Solaris systems for penetration testing of NT systems.
- Supported 50 plus Citrix systems for internal Fidelity business units.
- Performed system penetration tests using a wide variety of tools (ISS, Cybercop, etc.).
- Developed custom NSH UNIX shell scripts to perform various security log rotation and backup,
- Configured nightly batch jobs on NT and Solaris to collect Web, application and security logs,
- Consulted with Network Planning & Management to resolve network issues for Fidelity E-Business.
- Performed the installation and configuration of new server hardware and Network Operating Systems.

State Street Bank, Project Manager Enterprise Server Consolidation FMG, 1998-1999

Managed the consolidation of 50 NetWare servers into the core FMG Novell 4.11 infrastructure. Responsible for the desktop migration from windows 95 to NT 4.0 for FMG internal customers. Evaluated Windows NT high availability solutions utilizing Veritas FirstWatch and Vinca Co-standby server Using EMC & Storagetek disk arrays.

Resource 122

X86 Infrastructure Architect/Engineer

- Managed and implemented the SEI Investment trust application running on Windows NT server and MSSQL6.5.
- Designed and Evaluated Citrix metaframe environment for thin client workstation deployment within the FMG LAN.
- Evaluated Enterprise backup solution using Veritas NetBackup for Windows NT and NetWare.
- Developed custom NT shell scripts to perform various database backups and data replication.
- Managed several server consolidations of legacy systems within the FMG Technology division.
- Consulted with Network Planning & Management to resolve WAN/LAN issues for FMG.
- Performed the installation and configuration of new server hardware and Network Operating System.

Brown Brothers Harriman & Co., Tivoli Enterprise Software Distribution, 1997-1998

Primary responsibilities included managing Tivoli software distribution server's (operating system/2/, NT 4.0, AIX). Assisted with ESD policy and procedures development for BBH & Co. Recommended solutions for software distribution under IBM Tivoli TME 10.

- Evaluated third party software solutions for the operating system/2 to Windows 95/NT conversion.
- Created automated processes for the installation of client software via Tivoli Scripting, Shell Script.
- Modified Windows 95/NT registry files for custom workstation configuration using Tivoli and custom written INF files.
- Assisted with the Windows NT Enterprise Edition evaluation of server clustering technology.
- Performed various administrative functions within the AIX operating system.

Metropolitan Insurance, FileNet Imaging and Workflow Project Leader, 1997 to 1997

Project Leader for the roll out of FileNet document imaging software. Managed the rollout of the Windows NT application servers for the FileNet application. Managed and Implemented client conversation of 2000 IBM operating system/2 PCs to Windows NT workstation 4.0.

- Researched and recommended software and hardware configurations for the FileNet image platform.
- Designed networked solutions for software distribution using SMS.
- Evaluated Single sign-on environment for MetLife NT, Novell, and FileNet imaging environment.

- Responsible for the Rollout and managing the implementation of Windows NT applications servers.
- Managed the HP UX cache server for FileNet imaging software.

AT&T Solutions, Network Project Manager, 1997 to 1997

Architect on the Global enterprise network solutions team for Textron's Manufacturing and financial divisions (Bell Helicopter/T.E.T/Cessna, Textron Fuel systems, Avco). Managed the rollout/upgrade of WAN/LAN Solutions for various Domestic and International Textron divisions.

- Configured wide area network hardware for Textron manufacturing divisions.
- Managed data center migrations for various Textron divisions.
- Designed & Managed the integration of Citrix Solutions for remote access to subsidiary network systems.
- Managed the migration from O.C.C (other common carriers) to AT&T Interspan Frame Relay network.
- Coordinated weekly with all Textron Divisions to discuss network solutions and upgrades.
- Managed all stages on network implementations and configurations.
- Consulted with Textron's Network Security Team to discuss various security system standards.

Putnam Investments Inc., Network Project Manager PFTC, 1996 to 1996

Managed a Novell 3.11/3.12 NetWare environment. Managed both NT and NetWare server installations utilizing industry standard configurations. Designed/Implemented Norman enterprise Anti-Virus Strategy for Novell Servers.

- Managed the rollout of a site wide Novell backup solution of Cheyenne Arcserve 5.01g.
- Maintained Multiple Lotus cc: Mail Post Offices and operating system/2 mail connectors.
- Managed Lotus cc: Mail/Mobile installation team (Franklin).
- Senior Architect for the implementation of Ca-Unicenter on the Novell 3.1x platform.
- Responsible for the installation/upgrade of Novell SAA gateways from 1.x to 2.0.
- Responsible for server security.
- Managed Intel Video Conferencing rollout (PFTC).
- Developed Standards for Novell Servers and Windows 3.11 Desktops.
- Advised Installation team on standard configurations for new installation of Windows NT workstation 3.51.
- Coordinated with business units to review current operations and advise on future projects...

Resource 122

X86 Infrastructure Architect/Engineer

- Member of Enterprise LAN committee for Putnam Investments (Advisory board for System standards).

First Winthrop Corp. , MIS Consultant LAN Manager, 1995-1996

Managed Novell NetWare servers in a multi-server environment. Implemented Palindrome Network Archivist Novell backup Solution. Designed and Implemented Lotus cc: Mail e-mail system for local and Internet messaging. Responsible for Remote Access to Lotus cc: Mail Server.

- Integrated Citrix WinFrame server for remote access to corporate LAN.
- Migrated from DOS/windows to Windows 95 and Windows NT 3.51 clients.
- Maintained Multiple AS400 WAN links for the reservation system.
- Managed Workstation to Host (AS/400) connectivity Rollout of over 200 clients.
- Maintained remote access to AS/400(5250 emulation via dial in).
- Responsible for Token-Ring to Ethernet infrastructure conversion.
- Coordinate with business units to review current operations and advise on future upgrades.

UNISYS

[redacted]

X86 Infrastructure Architect/Engineer

Key Skills and Knowledge

Domain Expertise & Solutions

- Access Control
- Active Directory
- ISA/TMG Server
- IIS
- CA SiteMinder
- BEA Aqualogic Portal
- Radiant Logic
- PKI

Network Security

- CSS – Cisco Content Switches
- VPN
- Cryptography

Databases

- SQL Server

Project and Program Management

- MS Project

Operating Systems

- Windows 2008/2003/2000

Professional Summary

Summary of Experience and Qualifications

Shobha is Manager for over 14 years of Systems Engineering and Networking experience with the last 7+ years in assessment and implementation of Applications, Servers and Security infrastructure. Microsoft Certified Systems Engineer in windows NT/2000/2003. Over 3 years experience in managing the team and client interaction In depth knowledge and hands of Experience on TCP/IP Networking, DNS and Name Services, Active Directory-Joining Domains COM+ Applications, IIS as Web server and its configuration, administration and troubleshooting. Wide Experience in Implementing high availability solutions using CSS (Cisco Content Switches), Microsoft Windows Clustering, NLB, and Application Center. Hands on experience in designing and implementing Web publishing solutions using MS ISA Server. Ensured network security corporate policies and "best practices" standards were followed during design, installation, and configuration of ISA firewall, NAT server, and Intranet, Extranet, and Internet connections. Project Management experience in gathering the requirements, analyzing and document the application requirements, design and prototyping the applications in an enterprise environment.

Professional Experience Include most recent first

Unisys/ Office of Administration, State-PA, 03/2004-Present

- Working as deployment manager/architect for the data center. Routine job responsibilities include- Design and provide solutions for integrating applications securely within the data center. Leading team of experts who are responsible for implementing application on the enterprise infrastructure. embers as per their expertise and provide technical as well as non technical assistance as and when required by the team members. Coordination and meeting with clients to discuss the application/infrastructure requirements for deploying applications at the hosting facility. Work with Clients and provides them solution to a problem and built positive client relationship
- Project - Disaster Recovery/Secondary Site for Data Center (BCDRP) – Shobha is working with team of experts and Management executives for establishing the secondary site for the enterprise data center. Her role is to provide suggestions relates to application designs for secondary site in conjunction with primary site.
- Project Single Sign On for Commonwealth Portal 2006 (Access Control) – Designed and implemented the SSO for commonwealth Portal be leveraging CA SiteMinder. Designed the solution to implement SSO among various implementations of SiteMinder at various agency locations. Leading team of experts for ongoing support like upgrade of the products throughout the enterprise.

UNISYS

[redacted]

X86 Infrastructure Architect/Engineer

- Project – User Provisioning for commonwealth of Pennsylvania (Access Control)– Shobha was the technical lead during the requirement, design and implementation phases for user provisioning project. IBM Tivoli manager product is leveraged to provide account management and user registration capabilities.
- Project – PSP CLEAN (Access Control) – Shobha assisted the project lead during the design phase of security component for CLEAN project. CLEAN is the system that is leveraged by many crime and justice related agencies. Leading the team of experts to provide ongoing support for the CLEAN security components like single sign on and virtual directory services
- Project – Penndot NDES (Cryptography) – Shobha was the lead and helped in designing the solution for certificate enrollment by network and handheld devices. The solution was designed using Public Key infrastructure components like network device enrollment services(NDES) and OCSP (online certificate status protocol)
- Project – VPN for Mobile users (Telecommunications and Network Security) – Shobha along with other experts helped in designing the VPN solution for Commonwealth mobile users to access internal applications. The solution leveraged Netmotion mobility servers and Radius servers for VPN services, PKI and Active directory for dual authentication.
- Other responsibilities – Shobha leads team of experts and work with many other groups and is involved in all security related projects and addresses various security concerns like data at rest and in transit, user registration, access management, network and infrastructure security.

CitiBank New York, Consultant, 09/2003-12/2003

Responsible for installing, configuring and managing the windows 2000 Servers. Co-ordinate with application and business groups, implementation and performance tuning of the applications Including IIS based application. Implement backup servers and create/implement backup plans for servers .Install SQL servers and help DBAs troubleshooting System related problems. Create/Execute backup of SQL databases using SQL server backup. Troubleshooting tier-3/tier-4 windows 2000/nt server environment Implement Web Trends server for logging. Routine troubleshooting and system administration involving application teams, business groups and network group

Unisys/Department of Public Welfare Consultant, 04/2001-07/2003

- Project – DPW Extranet (Network Security) - Responsible for installing, configuring and maintaining the Department's Extranet by leveraging ISA/Microsoft Proxy Services. Designed and implemented solution to publish secure applications to Internet using MS Internet Security and Acceleration Server/Proxy 2.0 and SSL. Implemented the solution for

UNISYS

[redacted]

X86 Infrastructure Architect/Engineer

publishing applications with confidential data using secure socket layer protocol involving co-ordination with application teams, network infrastructure people and with other offices to fully understand the architecture. Troubleshooting and managing tier-3 servers problems, LAN, WAN support management in a complex environment including co-ordination with outside vendors and application vendors like Verizon

- Other Responsibilities: Monitoring, optimization, administration and support and configuring security for all enterprise Web servers. Support for WINS and DNS servers. Administer Exchange 5.5 environment, troubleshooting e-mail flow problems in an enterprise environment including escalation of problems with other organizations and departments within the same organization. Help and assist co-workers understand the e-mail flow and hardware/software involved in the whole process. Assisted in design and plan for migration from exchange 5.5 to exchange 2000. Helped in troubleshooting issues involving application availability, Network inconsistencies, routine issues with user/account management and policies. Provided support for network infrastructure, publishing applications and their availability, troubleshooting procedures for network, e-mail, Web servers and Internet facing Firewall servers (ISA and proxy servers)
- Project -Active Directory Implementation (Access Control)- Designed and implemented Active Directory in an enterprise environment, including security policies, delegate administration to user as per their role User and group accounts management. Created the support document and trained the administrators to manage the active directory as per their role. Troubleshooting the issues related to active directory policies and authentication problems involving co-ordination with different departments.
- Developed and implemented NETIQ performance-monitoring procedures on windows 2000 enterprise servers. Performance monitoring procedures details the process of monitoring each individual server's health and send alerts in case one of the monitored resources become a bottleneck, modified the scripts as per the organization requirement, created reports for resource consumption as and when required. The servers monitored with NetIQ were windows 2000 servers serving the role of Web servers, application servers and database servers
- Application Center Implementation (Access Control) - Designed and executed the phased implementation of application center clusters to load balance the applications running on windows 2000 enterprise Web servers. Created the procedures for application deployment and trained the developers to help them understand the new environment. Troubleshooting the problems related to application deployment, network inconsistencies and application synchronization. Maintenance of the cluster by taking the node offline alternatively without affecting the end users

UNISYS

[redacted]

X86 Infrastructure Architect/Engineer

- Implemented unified security solution includes deployment and configuration of SiteMinder components on enterprise servers. Integrating Netegrity with Active directory for authentication and authorization of resources, configuring policy servers to for multiple active directories for authentication and for authorization of resources. Troubleshooting the problems with the slow response or unsuccessful authorizations for the application using the Netegrity for single sign on, DNS problems and network issues in an enterprise environment, escalating the problems with third party software/application vendors whenever required and worked as coordinator.
- Implementing a Windows NT/ 2000-based VPN solution to provide administrator's access to public Web servers for upgrades, monitoring and maintenance. Analyze complex network environment and resolve any security issues. Co-ordination with multiple offices and third party hardware/software vendors

NT Administrator / IBM, Arkansas, 06/00-08/00

Designed and Implemented the NT Enterprise Network which comprised of NT4.0 Enterprise Version, Server, Cisco Routers, 3Com Switches, RAID5 Disk Arrays, and IBM Netfinity Server. Implemented the Backup Policy using DLT4000 Tape Drives and Backup Exec. NT administration and troubleshooting on Netfinity servers. Troubleshooting disk related problems and tape drive problems. Working with utilities to flash BIOS settings and change BIOS settings. Configuring the hardware RAID. Configuring Load Balancing on Network cards. Worked with Disaster recovery NT resource kit tools to modify with NT registry

Network Administrator, Northfield Savings Bank, NY(Short Term), 02/00-05/00

Project Firewall Implementation (Network Security) - Studied Network Design to foresee the problems before configuring/implementing security policies. Analyzed, designed, implemented and configured various elements of the network right from switches, Cisco Routers to servers and application Software. Installed and configured NT Servers. Installed and Configured CheckPoint 4.1 (Firewall) on NT 4.0 servers. Configuration and integration of E-Safe content scanning server to work with CheckPoint 4.1. Created policies and rules to define security for the organization.

NT Administrator/Architect, Interactive Communications Inc., 05/1999-01/00

- Designed and reconfigured the network having multiple subnets for different departments of the company. Installed and Configured CheckPoint 4.1 (Firewall) on NT 4.0. Configuration and integration of E-Safe content scanning server to scan for viruses with CheckPoint 4.1
- Creating policies and rules to define security for the organization. Implemented Internet Security using MS Proxy Server 2.0. Configured

UNISYS

[redacted]

X86 Infrastructure Architect/Engineer

Exchange Server 5.0 including IMS. Implemented VPN using MS PPTP (Point to Point Tunneling Protocol) technology and RAS server technology. The data transfer is secured by enabling the MS CHAP Protocol and Data encryption at the server level and client level.

- Evaluated the Windows 2000 server (Beta) compatibility with existing devices and testing the product services and new features in testing environment. Created customized packages using custom installation tools and distributing those using Windows 2000 group policies. Upgrading from Windows NT server to Windows 2000. Configuring RIS (Remote Installation Server) to remotely install Windows 2000. Configured Terminal Servers in Windows 2000. Configured networking services like DHCP, DNS, etc.

NIIT Limited, India, 07/95-01/99

Network administration for network. Comprises of Windows NT Servers, Novell NetWare 3.12 and SCO-UNIX. Administration of users & group accounts, security policies, print servers, Implement, administer and troubleshoot Exchange environment, configure mail clients, Performance tuning. Implemented migration from Novell to NT Support DNS/Wins/DHCP Study and design network Conducted training on Windows NT 3.51/4.0, Windows 95, UNIX, TCP/IP, SQL Server, MS Exchange Server, PowerBuilder for corporate clients, Unicenter TNG (Computer Associates).

Education Include High School or greater

Bachelor of Science, University of Delhi, India

Diploma in Systems Management (NIIT, India)

Professional Certification

- Windows MCSE 2003
- CA SiteMinder
- CISSP
- ITIL Foundation 3.0

Professional Development

- CISSP

This page intentionally left blank.

Active Directory

This page intentionally left blank.

UNISYS

Resource 123

Active Directory

Key Skills and Knowledge

- Domain expertise and solutions
- Management consulting services
- Project and program management
- Communication and networking
- Databases
- Server hardware
- Operating systems
- Internet Information Server (IIS)
- Customer service
- Team player
- Office productivity tools
- Technical documentation

Professional Summary

10 years of experience with managing IT systems in medium to enterprise environments; 7 years of experience with Microsoft Active Directory; and 5 years of experience with supporting Exchange servers. 2 years of experience with supporting Web-based load balanced Internet applications in a large data center environment.

- Extensive experience in supporting Windows 2003 and 2008 servers
- 7 years of working with small to large clients while providing on-site IT services
- 2 years of experience with coordinating a Change Management process in an enterprise environment
- Certified in MCSE, MCT, MCITP, and ITIL 2011.

Professional Experience

Unisys Corporation, Commonwealth of Pennsylvania, Harrisburg, PA

Perform IT operations for the Enterprise Data Center (EDC) hosting more than 1,000 load and non-load balanced Web-based applications.

- Perform operational support for Enterprise Windows Servers 2003 and 2008 in physical and VMware environments.
- Support multi-tier load balanced Web applications residing on Windows Web Servers.
- Manage multi-domain Active Directory projects.
- Support Windows 2003 and 2008 clusters.
- Support application availability using SCOM 2007 and performance tuning for Windows Servers.
- Complete Active Directory, SAN, SCOM 2007 monitoring, and disk space remediation projects.
- Coordinate Change Management process tasks with stakeholders.
- Configure servers for requested changes.

Innotion Enterprises, Inc, Bordentown, NJ

Effectively managed day- to-day IT operations for a U.S. Department of Housing and Urban Development (HUD) contractor. Supported LAN/WAN network infrastructure to securely connect with HUD network applications and maintain corporate data, e-mail, and Voice over IP (VoIP) communication systems.

- Performed technical and operational support on enterprise Windows Server 2003 and 2008 infrastructure systems and application software.
- Installed, configured, and managed Active Directory, Microsoft Exchange Server 2003and 2007, BlackBerry Enterprise Server, DHCP, WSUS, DNS, Cisco firewalls, Cisco routers, and Norton AntiVirus Server in a corporate environment.

UNISYS

Resource 123

Active Directory

- Defined and implemented improved corporate policies for the location, safety, and security of computer equipment.
- Performed routine maintenance and upgrades as required on servers, network devices, and related peripherals—improved reliability and 24/7 availability of mission-critical IT systems.
- Researched and developed network systems and related technologies; recommended products to meet future business and technological challenges.
- Developed and implemented disaster recovery strategies and procedures for network resources to ensure continuity of business and IT operations.
- Conducted internal Information Security Audits (ISAs) and implemented system security measures to improve the security and reliability of IT assets.

A&Y IT Solutions, Ontario, Canada

Consulted with clients for network performance, system administration, and user requirements.

- Analyzed networks to identify bottlenecks; proposed network design solutions to improve network performance and worker productivity.
- Proposed, designed, and built networks for small businesses with up to 50 workstations.
- Successfully installed and configured Windows Server 2003 Active Directory, Exchange Servers, and printers for up to 100 users.

Wintronics Computers Plus, Ontario, Canada

Consulted medium-sized business to analyze its IT infrastructures to improve business operations and propose solutions.

- Installed, configured, and supported Windows Server 2000 and 2003 for small and medium sized clients to improve security, productivity, and performance.
- Provided on-site support for end users and resolved the issues promptly to minimize production downtime.
- Performed routine monitoring of network and infrastructure for optimal performance and information security.
- Built customized Intel-based servers and workstations for businesses.

Education

- MIS, Network Architect and Design, Capella University, Minneapolis, Minnesota, 2008
- Bachelor of Engineering (B.E), Electrical Engineering, NED University of Engineering and Technology, Karachi, Pakistan, 1992

UNISYS

Resource 123

Active Directory

Professional Certification

- MCTIP, Windows Server 2008 & 2012
- MCT, SCOM 2007 & 2012
- ITIL Foundation 2011 & 2012
- MCT, Windows Server 2008 & 2009
- MCSE, Windows Server 2003 & 2007
- Cisco Certified Network Associate (CCNA), 2005
- MCSE, Windows NT4, 1999

This page intentionally left blank.

UNISYS

Resource 124

Active Directory

Key Skills and Knowledge

- Domain expertise and solutions
- Project and program management
- Operating systems
- Software and system architecture
- Office productivity tools
- Technical documentation

Professional Summary

10 years of IT experience. Administer enterprise systems with a special focus on security infrastructure. Support more than 3,000 servers at the Enterprise Data Center for the Commonwealth of Pennsylvania. Broad range of professional experience: Microsoft Active Directory environments, hardware support, backups and restores, VoIP phone systems, network communication, Windows, Linux, and Mac OS.

- Design and support Microsoft Active Directory services, including AD and Certificate Services
- Experience in IT project management and solution deployments in an enterprise environment
- Exceptional retention of knowledge
- Organized, logical troubleshooting skills.

Professional Experience

Unisys Corporation, Commonwealth of Pennsylvania, Operations/Integration Consultant, Harrisburg, PA, 2011 – Present

Designed and deployed Microsoft's Network Device Enrollment Service and Online Responder Service, features of Microsoft Active Directory Certificate Services. This solution is an enterprise service offering for Commonwealth agencies that require certificates for network devices and a location on the Internet for checking internal certificate revocation lists.

- Implemented a scripted solution to monitor use of the Microsoft Active Directory Certificate Services infrastructure. The script exports a report of provisioned certificates for a specific certificate template on a scheduled so Commonwealth clients can monitor user certificate enrollment activity.
- Manage patches for Commonwealth of Pennsylvania Linux servers as required to maintain current patch levels in the Enterprise Data Center.
- Resolved a longstanding delayed login problem for a public-facing Commonwealth of Pennsylvania Web Service. Captured traffic with Wireshark and identified a failure in NetBIOS name resolution due to a discrepancy between a client's query and the NetBIOS record type. Recommended and implemented a successful solution g DNS.
- Identified and resolved a chronic problem in which an authentication function intermittently would not work in a public-facing enterprise application. Captured failed traffic with Wireshark and determined that not all Active Directory servers in the LDAP query string were accessible across the firewalls. Modified firewall rules to resolve the issue.
- Completed Active Directory Health Check remediation steps to maintain a secure and optimized network recommended by Microsoft Premier Support.
- Completed Active Directory Certificate Services remediation steps to maintain an optimized PKI infrastructure recommended by Microsoft.

UNISYS

Resource 124

Active Directory

TCW Computer Systems, Inc., Multiple Consultant Contracts,
Network Engineer, 2007 – 2011

Performed an in-depth migration from Windows Server 2000, Microsoft Exchange 2000, and Citrix Metaframe Server to Windows Server 2008, Exchange 2007, and Microsoft Terminal Services. Other migration processes included moving line-of-business applications, data, printers, user accounts, and security groups.

- Maintained HIPAA and PCI-compliant networks. Implemented compliance scanning, monitored reports, and provided ongoing remediation so networks remained compliant.
- Managed a patch management system and centrally deployed patches for all managed services customer networks.
- Designed and deployed a campuswide wireless network. Performed a wireless site survey to determine infrastructure requirements for the desired coverage. Performed a network site survey to determine necessary network device upgrades. Deployed a wireless controller, managed switches, and implemented the necessary VLAN infrastructure to allow secure private communication and publicly accessible Wi-Fi access.
- Designed and implemented a new VoIP telephony solution to replace a client's aging phone system. The solution included integrated desktop software for call control and voicemail to e-mail functionality among other network integrated services.

Other Employment

Landis Computer 2002 –2007

Professional Certifications

- CompTIA Security+, 2012
- The ITIL Foundation, BCS Institute of IT, 2012
- MCITP: Enterprise Administrator, Microsoft, 2011
- VCX VoIP Telephony Certified, 3com, 2010
- NBX VoIP Telephony Certified, 3com, 2009
- MCSA 2003, Microsoft, 2008
- MCSA 2000, Microsoft, 2003

Professional Development

- Windows Server 2012 Training, 2012
- Microsoft Active Directory Certificate Services Training, 2011
- 3com VCX VoIP Training, 2010
- Windows Server 2008 Training, 2009
- Planning, Deploying, and Managing a Network Solution for the Small and Medium-Sized Business (MS 70-282), 2006

UNISYS

Resource 65

Active Directory

Key Skills and Knowledge

Domain Expertise & Solutions

- Active Directory
- Microsoft Exchange
- Microsoft DNS
- BlackBerry Enterprise Server

Operating Systems

- Windows Server 2003
- Windows Server 2008
- Windows Server 2008R2

Software/System Architecture

- PowerShell

Call Center and Help Desk

- Remedy

Office Productivity Tools

- Microsoft Office Suite

Professional Summary

Highly proficient systems administrator with 25 years of experience in many phases of the information technology and effective supervisor and trainer of technicians, managed more than 300 domain controllers in several different environments.

- Project lead for a forest-level upgrade of Microsoft active directory from Windows Server 2003 to Windows Server 2008 R2
  - Migrated many physical servers to virtual servers
  - Administered more than 100,000 mailboxes for 70,000 users on Microsoft Exchange 2007
- Managed BlackBerry Enterprise 5.0 Servers used by 4,000 users
- Consistently identified processes for automation — developed and implemented several scripts to save hundreds of staff hours versus previously used processes.

Professional Experience

Unisys Corporation, Commonwealth of Pennsylvania, System Administrator Consultant, Harrisburg, PA, 2009 – Present

Managed security patches for 400 domain controllers and Exchange servers.

- Migrated 15 Microsoft Exchange servers to version 2003; more than 4,000 mailboxes migrated with a success rate of 100 percent.
- Managed 4,000 user accounts and 2,500 Windows XP-based workstations on 15 isolated networks.
- Oversaw the migration of five separate NT domains to Active Directory—completed the project on time with zero impact on users.
- Led a project to upgrade ight domain controllers from Windows 2000 server to 64-bitWindows Server 2003.
- Upgraded a remote installation services server to Windows Deployment Server in production and test environments — enabled faster imaging of workstations and support for emerging technologies.

Elite Systems, Microsoft Exchange Consultant, Harrisburg, PA, 2008 – 2009

- Troubleshot hardware and software on 82 Windows-based servers.
- Provided day-to-day support for a wide range of standard applications. including the Microsoft Office suite, Form Filler, and PureEdge ICS Viewer.
- Managed networking issues dealing with TCP/IP, DNS, SMTP, and DHCP.

Air Force Flight Test Center, Network Systems Administrator, Detachment 3, 2004 – 2008

Consistently provided users with support for peripheral devices, such as printers,

UNISYS

Resource 65

Active Directory

scanners, plotters, and all-in-one devices; managed a $500,000 budget for a work section.

- Managed BlackBerry Enterprise Server for 2,500 users.
- Translated specific needs to computer systems requirements.
- Directed various teams of technicians on many different projects.

Network Control Center, Help Desk Manager, Andersen AFB, GU, 2003 – 2004

Supervised up to 40 individuals, dealing with personal issues, scheduling work hours, assigning daily duties, and evaluating performance.

- Authored several procedures for setting up servers and workstations that were adopted as the standard for use by all Air Force personnel worldwide.
- Prepared performance reports and recommended decorations for subordinate individuals.

Other Employment History

Network Control Center, 36th Communications Squadron, Andersen AFB, Guam	2002 – 2003
Air Force Flight Test Center, Detachment 3	1997 – 2002
8th Intelligence Squadron, Beale AFB, California	1993 – 1997
Foreign Aerospace Science and Technology Division, Wright-Patterson AFB, Ohio	1991 – 1993
609th Tactical Control Squadron, Hessisch-Oldendorf AS, Germany	1989 – 1991
3026th Communications Squadron, Sheppard AFB, Texas	1987 – 1989

Education

- Northern York High School, 1986

Professional Certification

- ITIL Foundation Examination, Loyalist Certification Services, 2012

Application Support

This page intentionally left blank.

UNISYS

Resource 28

Application Support

Key Skills and Knowledge

Databases

- MS SQL, Oracle, and DB2

Hardware

- IBM server hardware
- Dell server hardware

Operating Systems

- Microsoft Windows: NT 4, 2000, XP, 2003, 7, and 2008
- Linux: SuSE 10 & 11; Red Hat 5 & 6

Programming Languages & Tools

- DOS scripting, PowerShell, VB Script, C, C++, and HMTL

Call Center and Help Desk

- Remedy

Office Productivity Tools

- Microsoft Word, Excel, and Outlook

Facilities Management

- UPS monitoring and design

Professional Summary

Strong experience in systems administration and network management with a facility for learning and implementing unfamiliar technologies to attain customer-required outcomes.

- 12 years of implementing Web applications using Microsoft IIS as the Web and application server
- 12 years of deploying Microsoft Windows on authentication, file, and application servers
- 5 years installing, configuring, and deploying applications using of IBM WebSphere Application Server (WAS)
- 5 years of installing and configuring of Linux users and services, including Samaba, SSH, and BIND
- 4 years of installing and configuring VMware and ESC; as well as hosting of virtual infrastructure for a lab environment
- 2 years of installing and configuring of WebSphere MQ Server to support application communication across multiple platforms and architectures.

Professional Experience

Elite Systems, Commonwealth of Pennsylvania Office of Administration, Integration Consultant, 2010 – Present

Supported application deployments for the Commonwealth of Pennsylvania; coordinated and implemented the upgrade of WebSphere MQ from version 5 to version 7 for multiple Commonwealth agencies to access an enterprise SAP environment.

- Review, create, and update documentation used to deploy and support agency applications hosted at the Commonwealth's Enterprise Data Center.
- Evaluate agency requested changes against industry best practices and Commonwealth security standards.
- Coordinate change management processes among multiple Commonwealth enterprise teams to complete application deployments for Commonwealth agencies.
- Manage DNS servers hosting Microsoft Windows DNS and associated DNS records.
- Patch and troubleshoot Linux servers running SuSE and Red Hat distributions.

UNISYS

Resource 28

Application Support

TEKSystems/MindTeck, Pennsylvania Department of Transportation (PennDOT), Network Engineer, 2004 – 2009

Provided 24/7 support of numerous applications hosted at the PennDOT server farm for various bureaus in the department; monitored, and maintained APC UPS infrastructure.

- Deployed WebSphere Application Server infrastructure to support migration of PennDOT applications from Lotus Domino-based architecture to Java architecture.
- Deployed IBM DB2 Connect server and DB2 client software upgrades to support access to IBM mainframe-hosted DB2 database instances hosted on z/operating system.

Other Employment History

Innovative Business Concepts	2004 – 2004
GEF Computers	2002 – 2004
New Horizons	2000 – 2003
Computer Renaissance	1998 – 2000

Education

High school diploma, Sauquiot Valley High School 1993

Courses at Clarkson University, 1995

Professional Certifications

- CompTIA A+, May 1999, COMP10157635
- Microsoft Certified Professional, Microsoft, March 2000, MCP ID#1789557
- Microsoft Certified Systems Administrator Microsoft, August 2004, MCP ID#1789557
- Microsoft Certified Systems Engineer, Microsoft, August 2004, MCP ID#1789557

Professional Development

- ITIL v3 Foundation training, Framework that allows for continuous improvement of the documentation, customer service, and change control processes of an IT organization, 2012
- SiteMinder 12.5 training, Access management for Websites using LDAP and Active Directory security, 2012

UNISYS

Resource 58

Application Support

Key Skills and Knowledge

- Domain expertise & solutions
- Management consulting services
- Project and program management
- Communication and networking
- Databases
- Hardware
- Operating systems
- Software/system architecture
- Programming languages and tools
- Call Centers and Help Desks
- Office productivity tools
- Technical documentation
- Facilities management

Professional Summary

Senior IT Consultant with 14 years of experience in delivering Windows client/server platforms and solutions; extensive experience with IIS, SharePoint, BizTalk, and Threat Management Gateway/ISA applications; and skilled project manager and systems analysis leader.

- SharePoint Portal server administrator; create and administer Web apps and site collections along with Commonwealth Technology Center server's presence; rolled out new applications; ensure that the server and application user/administrator interface and experience are at optimal levels.
- Business coordinator during the entire development process; determined user and business functional requirements and translated them to specifications used for enhancements to a system or for new development.
- Worked closely with teams of developers from various business units to facilitate the upgrade and implementation of enterprisewide applications. Assisted in securing, streamlining, and integrating the underlying business logic, message processing, and middle tier/backend communications of the deployed applications.

Employment History and Related Experience

Unisys Corporation, Commonwealth of Pennsylvania, Senior Consultant, Harrisburg, PA, 2010 – Present

As an applications management deployment lead, fully responsible for the Internet presence of all departments and agencies housing their sites and applications at the Pennsylvania Enterprise Data Center.

- Support a three-tier environment of more than 4,000 servers and 600 Web sites and applications.
- Work extensively with BizTalk 2010, WSS 3.0, Windows 2008 Server, IIS 7.5, and other Web-integrated technologies on presence, format, and presentation.
- Configure and administer IIS 6.0 and 7.5 to facilitate maximum uptime and performance.
- Create and administer Web apps and site collections along with Commonwealth Technology Center server's presence. Roll out new applications; ensure that server and application user/administrator interface and experience are at optimal levels.
- As a BizTalk 2010 administrator, deploy and configure applications; ensure server and application uptime. Research and troubleshoot problems; implement the latest patches and updates to currently deployed applications.

UNISYS

Resource 58

Application Support

Explore Information Services, Business Systems Analyst, Marshall, MN, 2005 – 2009

Lead analyst on various projects for an insurance information provider with 80 employees and $65 million in revenue.

- Liaised with the business during the entire development process. Determined user and business functional requirements; and translated them to specifications used for enhancements to a system or for new development.
- Created documents and diagrams for test cases, use cases, and data process flows.
- Gathered project estimates of development hours, software, and hardware costs.
- Built logical models; provided high-quality of documentation for system design and development.
- Main focus was a successful product deployment while meeting standards, budget requirements, and deadlines.

Unisys Corporation, The Schwan Food Company, Senior Systems Engineer, Marshall, MN, 2003 – 2005

Administered, upgraded, deployed, and maintained corporate BizTalk 2002 and 2004 and MEI and CRM environments.

- Worked closely with teams of developers from various business units to facilitate the upgrade and implementation of enterprise-wide applications. Assisted in securing, streamlining, and integrating the underlying business logic, message processing, and middle tier/backend communications for the deployed applications.
- Acquired knowledge of application interdependencies, including MSMQ 1.0 and 3.0, IIS 5 and 6, SQL Server 2000, and COM+.

Unisys Corporation, Commonwealth of Pennsylvania, Senior Consultant, Harrisburg, PA, 2002 – 2003

Member of an applications management team fully responsible for the Internet presence of all departments and agencies housing their sites and applications on the Pennsylvania Enterprise Server Farm.

- Supported a three-tier environment of more than 250 servers and 150 Web sites.
- Worked extensively with Microsoft Application Center Server, Microsoft SQL Server 2000, Microsoft SharePoint Portal Server 2001, Microsoft Operations Manager, and PPT Dynamic Site Framework (DSF) for Web sites along with other Web-integrated technologies for presence, format, and presentation.
- Configured and administered IIS 5.0 and SQL 2000 servers to facilitate maximum uptime and performance.
- Functioned as a SharePoint Portal server administrator. Created and administered workspaces and the Commonwealth Technology Center servers'

presence. Rolled out new workspaces; ensured that the server and workspace user/administrator interface and experience were at optimal levels.

Corporate Network Solutions, Network Engineer II, Phoenix, AZ, 2001 – 2002

Managed, maintained, upgraded, and administered client networks ranging from small business to mid-sized corporations.

- Functioned as project manager on various assignments, including the setup, testing, and integration of EDI at Fortune 500 and nationwide air freight companies. Lead engineer on a corporate infrastructure upgrade to Windows 2000 Active Directory platform including Exchange and SQL 2000.

Cunningham Technology Group, Systems Engineer, Phoenix, AZ, 2001 – 2001

- Designed and implemented the infrastructure and system components necessary to support local and enterprise-wide business needs and solutions for clients.
- Assessed network needs. Wrote proposals for suggested improvements in architectural design, system implementation and deployment, application configuration, and performance enhancements.

ProNet Solutions, Senior Consulting Engineer, Phoenix, AZ, 2000 – 2001

Ensured the highest level of technical expertise and customer service was provided and maintained while functioning in a Tier 2 support position.

- Improved the efficiency and effectiveness of clients by proactively administering and supporting their PC and networking needs.
- Functioned as team lead on assigned projects; acted as escalation point for technical and customer service issues.

Integrated Information Systems, Senior Consultant, Phoenix, AZ, 2000 – 2000

System and security architect for a multiple international domain network.

- Administered rules and security policies on local and remote CheckPoint firewall modules to supply safe and secure internetwork and intranetwork communication and data integrity.

Raymond James Consulting, Sr. Network Administrator, Denver, CO, 1998 – 2000

Lead administrator for a Microsoft NT multiple-domain network. Supported 20 servers and 250 client computers, including desktop and laptop computers.

- Configured, supported, and upgraded, as needed, the following network services: File/Print, WINS, DHCP, RAS, Exchange 5.5 Server, IIS 4.0, Microsoft SQL 6.5 Server running intranet applications, and SQL Server running custom production applications.

UNISYS

Resource 58

Application Support

Education

B.A., General Studies, University of Iowa, 1990

Professional Certification

- Windows 2003 MCSE, 2010
- Windows 2000 MCSE, 2002
- Windows MCSE + Internet, 1999

UNISYS

Resource 125

Application Support

Languages

- English

Key Skills and Knowledge

- Domain Expertise & Solutions
- Consulting Services
- Project Management
- Operating Systems
- Software/System Architecture
- Office Productivity Tools
- Technical Documentation

Professional Summary

Technical Specialist/Project Manager offering 14+ years of experience in the IT field. My job experience includes Enterprise Administration of an 80,000-user Active Directory and Exchange Server farm, hardware/software troubleshooting and network security. I also offer experience in training, technical writing, knowledgebase administration and management experience in supervision and classroom management.

Professional Experience / Employment History

Unisys/Commonwealth of Pennsylvania, Integration Consultant, Harrisburg, PA, 2010 - Present

Project Management – Integrating agency infrastructure into Enterprise Server Farm, Windows 2003/2008 Server, Active Directory, IIS, and Web application troubleshooting, ande Monitoring SCOM alerts

- Active Director Federation Services (AD FS) 2.0
- Remedy ticket resolution
- VMware/vSphere
- SharePoint Server

BlackRose Consulting, Independent Consultant, York, PA,, 2003, 2004, and 2010

Windows Server and workstation setup, configuration, installation and troubleshooting, hardware and software planning and purchasing, and Project Management

Computer Learning Network, Network Security Instructor, Mechanicsburg, PA, 2006 - 2009

Windows 2008/2003 Active Directory network planning, creation and administration for NISA/CTIS department. Setup and management of DNS and DHCP for NISA/CTIS department. NAS setup and administration

- Teaching students the fundamentals of Networking, Windows 2003/2008 Server, Active Directory and Security. Training students for Security+ exam and Server portions of MCSE
- Managing classroom of 10-15 students. Overseeing projects, guiding classroom activities and keeping students on task
- Observation and evaluation of performance. One-on-one counseling when behavior and performance didn't meet expectations
- Lesson planning and project creation. Adaptive teaching techniques to meet the varying needs of students

Ajilon Consulting/Fannie Mae, Infrastructure Administrator, Urbana, MD, 2006 - 2006

Windows 2000 and 2003 server installation, configuration and troubleshooting,

UNISYS

Resource 125

Application Support

Network Security - Installing and configuring Tripwire, User and Group management, Print Server management, and Patch management

Unisys/Commonwealth of Pennsylvania, Enterprise Exchange Admin
Harrisburg, PA, 2005 - 2006
Enterprise Administration team member who helped maintain the Commonwealth of Pennsylvania's 90,000 user Active Directory Forest. Windows 2000 and 2003 server installation, configuration, troubleshooting, and user/group management. Assisted in the Commonwealth's upgrade from Windows 2000 to 2003 Server. Microsoft Exchange 2000 Server management

- CommVault Backup management
- Network security auditing
- Patch management
- Anti-Virus and Anti-Spam administration
- Providing resolutions to Tier 2 Remedy trouble tickets

Dataware, Inc., Network Consultant, York, PA, 2004 - 2005
Network planning, cabling, installation and troubleshooting. Windows 2000 and 2003 Server setup, configuration, and troubleshooting. Active Directory setup, configuration, troubleshooting. Microsoft Exchange Server setup, configuration, maintenance, troubleshooting, and mailbox/user management. Hardware and software planning, purchasing, configuration, installation and troubleshooting

Earthlink Inc. Project Manager, Harrisburg, PA, 2002 - 2003
Responsible for assisting Business Operations Project Manager with optimizing mail (Kana), chat (LivePerson) support systems, policies, and procedures, Created and updated documentation and canned answers for E-Support service and support representatives. User management for e-mail and chat databases

- Assisted in training support representatives on new products and services
- Wrote, updated, and maintained EarthLink Electronic Support Intranet Department Web site

Earthlink Inc., Electronic Support Technician Generalist, Harrisburg, PA, 2002 - 2002
Provided technical support and customer service for Earthlink customers via e-mail and live chat, Troubleshooting broadband and dial-up Internet connection, associated applications, and Troubleshooting Web site issues

- Monitor Network Operations Center for area problems
- Resolved Ethernet and TCP/IP issues on various operating systems
- Aided customers in resolving issues and educate them on technical issues
- Wrote and maintained Electronic Support Team and department Web sites
- Assisted as fill-in supervisor

UNISYS

Resource 125

Application Support

- Provided Web Hosting related training and refresher courses for non-Web Hosting trained support representatives

Earthlink Inc., Web Host Master Tech, Harrisburg, PA, 2000 - 2002
Responsible for providing technical support and customer service for Earthlink Web Hosting customers via phone. Troubleshooting Web site and UNIX Web server issues. Wrote and maintained Web Support Team Web site. Wrote and maintained Web Hosting Harrisburg department Web site

- Wrote department Virtual Applications
- Wrote training documentation
- Provided new hire training to incoming Web Hosting Support representatives
- Provided ongoing training for existing Web Hosting Support representatives
- Assisted as fill-in supervisor

Earthlink Inc., Technical Support Senior Technician, Harrisburg, PA, 1998 - 2000

- Responsible for providing technical support for Earthlink customers via phone. Troubleshooting dial-up and broadband Internet connections as well as associated applications. Wrote and maintained Support Team Web site. Wrote department Virtual Applications
- Wrote and maintained Support Knowledgebase documentation
- Managed Support Knowledge Base
- Wrote technical documents to assist training department
- Assisted with special projects
- Assisted as fill-in supervisor

Education

- Network and Internet Security Administration, Computer Learning Network, Mechanicsburg, PA
- West York Area High School, York, PA

Professional Certification

- MCSE – Messaging and Security, Network+, Security+, ITIL Foundation

This page intentionally left blank.

UNISYS

Resource 126

Application Support

Key Skills and Knowledge

Domain Expertise & Solutions

- Fortune 500
- Enterprise Data Centers
- Banking and Finance
- Non-profits
- Public sector

Software/System Architecture

- Active Directory
- Exchange 2003/2010
- SQL 2005/2008r2
- Oracle 10r2/11r2
- SharePoint 2003/2010
- VMware
- HyperV
- IIS 6 / 7.5
- Apache
- McAfee EPO, AV and IDS
- Symantec Corp, AV and Veritas SCCM
- SCOM
- Citrix
- BladeLogic
- Remedy
- ISA/TMG
- NetIQ Security Manager NetIQ Secure Configuration Mngr
- MS Project/Visio
- MS Licensing Ent Core CAL WSA
- Adobe CS5 suite
- Ticketmaster POS
- BizTalk
- Zenworks

Programming Languages & Tools

- .NET, JavaScript
- C++
- PowerShell , Hyena

Communication and Networking

Professional Summary

Over 20 years experience in designing, administrating and troubleshooting CIT systems infrastructures. Expert in server administration and troubleshooting in a virtual enterprise environment.. Expert in deploying, administering and troubleshooting applications and providing high availability. Expert in monitoring and securing all servers and network communications including being proactive instead of reactive

- Thorough knowledge of Web technologies in a distributed multi-tiered environment including front end load balancing, IIS/.net Web deployment and back end applications, SQL/Oracle databases
- Thorough knowledge of networking including firewalls, routers, switches, IDS/IPS, VPN, CSS, etc
- Well experienced in patching, disaster recovery, and business continuity, maintaining uptime, minimizing downtime and fulfilling auditing requirements for enterprise /financial institutions.
- 'Jack of all IT trades' – For example, able to do anything IT related from scripting to running penetration tests to fixing hardware failures to automating deployment of system upgrades
- Able to be services oriented team player who follows instructions as well as take the initiative when appropriate.
- Able to handle complex assignments and see projects through all phases as well as keep current with new technologies

Employment History

Unisys, State of Pennsylvania, Harrisburg, PA Integration Consultant/ Systems Analyst 2011-2012

Monitor and support over 4000 servers hosting over 1500 Web sites, 1000 applications and 3000 databases. Deploy and manage new application code, server builds, firewall rules, CSS, DNS, SSL certs, etc

- Provide service oriented support by interfacing with agencies on projects, deployments and incident tickets and then coordinate efforts with internal departments including the operations, networking, firewall, security and database teams.

Cape Bank, Court House NJ Systems Administrator 2005-2011

Same as Crest Savings and DCR duties plus:

- Manage two employees, give reviews, hire, oversee and train.
- Document Risk Assessments and Business Impact Analysis and test DR policies
- Monitor and troubleshoot any issues with IIS, Web applications

UNISYS

Resource 126

Application Support

- Cisco routers and switches
- Check Point firewalls
- IBM Proventia IDS/IPS
- NEC VoIP

Hardware

- HP
- Dell
- IBM
-

Operating Systems

- Windows Server 2003/2008 R2
- Windows XP/7/8
- Linux Redhat/Solaris
- UNIX/AIX

- Prepare budget, get budget approved and stay within budget documenting all expenses.

Crest Savings Bank, Wildwood NJ, IT Administrator, 2003-2005

Same as DCR duties plus:

- Provide 24 hour support all servers and enterprise level infrastructure and applications
- Manage all servers, workstations, users and groups through active directory and group policy.
- Manage/configure all network devices including all Cisco routers, switches and check point firewalls
- Manage Exchange/SQL/SharePoint and other critical applications.

DCR Business Products, Inc., Philadelphia PA, MIS (Information Services Manager), 1988-2003

Maintain LAN and WAN hardware, servers, workstations, printers and all associated hardware and software. Update system logs and other required recordkeeping. Initiate preventive maintenance and recommend improvements to processes or procedures.

- Assist in installation of new or upgraded equipment and applications. Test and troubleshoot as needed.
- Support phone systems including completion of moves, additions, changes, and punch downs.
- Answer tech support help line and support end-users. Train employees as needed.
- Respond to user requests in a timely manner. Escalate troubles to management and vendor support in an appropriate manner and time
- Provide training / share knowledge to IT staff and all employees as needed

Education

Bachelors Degree in Music, Jazz Composition/Arranging, Temple University, May 1987

Professional Certifications

- MCITP Enterprise Administrator, Microsoft, 2012
- ITILv3 (2012), ISEB, 2012
- CEH (Certified Ethical Hacker), Ecouncil, 2009
- MCSE 2003, Microsoft, 2007

UNISYS

Resource 126

Application Support

- Security+, • CompTIA, 2006
- CCNA (Cisco Certified Network Associate), Cisco, 2005
- CIW (Certified Internet Webmaster), CIW, 2004
- iNet+, CompTIA , 2004
- MCSE 2000. Microsoft, 2003
- Network+, CompTIA, 2002
- A+, CompTIA, 2001

Professional Development

- Implementing and Managing Microsoft Server Virtualization (10215), NH Online 2010
- Planning and Managing Windows 7 Deployment (6294), New Horizons Online 2010
- Microsoft SharePoint Designer 2010 (50354), New Horizons Online 2010
- Adobe CS4/CS5 suite training, New Horizons 2010 (included several courses)
- Microsoft Project Levels 1 and 2, New Horizons 2010
- SQL Server 2005 Implementation and Management, Springhouse Online - 2007
- Certified Ethical Hacking, New Horizons Online - 2007
- Programming with MS .NET Framework, New Horizons Online - 2006
- Cisco Certified Network Associate, Cape May County Tech Center - 2004-2005
- Microsoft Certified System Engineer, Atlantic Country Community College - 2001

This page intentionally left blank.

UNISYS

Resource 127

Application Support

Key Skills and Knowledge

Domain Expertise & Solutions

- AD, MS Exchange, MS TMG, Hyper V, VMware, Symantec Backup Exec, Symantec Endpoint, Web Proxy, Anti-Spam Filters – Symantec, McAfee, Postini, Sonicwall, HP ProLiant Servers

Communication and Networking

- Cisco CCNA

Databases

- MS SQL

Hardware

- HP ProLiant, Dell PowerEdge

Operating Systems

- Windows 2008/2003 operating system

Programming Languages & Tools

- C++, C, VB

Office Productivity Tools

- MS Office, MS Visio

Professional Summary

7 years combined experience in Infrastructure Administration & technical Support, Experience in IT Consultancy and Audit Services for SMB Business Units, Experience in administration of Win 2008/2003 Active Directory and Domain Controller, IIS, MS Exchange Server 2010/2007/2003, MS TMG/ISA 2006, Hyper V, VMware EsX 4.1.

- Administration of HP ProLiant Dl&ML server, HP MSA and Dell PowerEdge server
- Administration of Symantec Backup Exec and HP Storage Works

Professional Experience

Employment History

- Unisys (Commonwealth of Pennsylvania) 2012 to Present (System Analyst)
- Alpha Data LLC, Dubai, UAE 2008 –2012 (IT Consultant & Server Support Eng)
- Alpha Data LLC , Dubai, UAE, 2005 –2007 (Technical Support Engineer)
- UBS Solutions, Bangalore, India, 2003 –2004 (Software Developer)

Education

- Masters in Computer Applications MCA, Bangalore University ,India, 2004
- Bachelors in Computer Applications, BCA, MG University, India, 2001

Professional Certification

- MCITP- Enterprise Messaging, MCSE, Microsoft, ID #3347491
- CCNA, Cisco, ID #CSCO11370734
- Comptia A+, Comptia, COMP001004677845
- CSSA, Sonicwall
- STS, Symantec
- HP APS - Hp

Professional Development

- ITIL 2011 Foundation – Course Attended (Dubai)

This page intentionally left blank.

UNISYS

Resource 99

Application Support

Key Skills and Knowledge

Domain Expertise & Solutions

- Public Sector
- Fortune 100 Private Sector
- Data Center Operations

Databases

- Microsoft Access
- MS SQL Server
- Oracle 10g

Operating Systems

- Windows 7, 8, and 9x
- Windows Vista
- Windows XP
- Windows NT
- Windows 2008
- UNIX
- Linux
- DOS

Programming Languages & Tools

- C#
- C++
- Visual Basic, Batch, PowerShell
- Crystal Management Console
- Crystal Reports
- HTML
- Java
- Microsoft FrontPage
- Microsoft Project
- Microsoft Office
- Microsoft Visio
- Microsoft Visual Basic .NET
- Remedy Action Request System
- SQL
- DameWare
- Remotely Anywhere, Compaq/HP
- ILO
- IBM RSA, IBM Director
- Cygwin, OpenSSH

Professional Summary

Progressive experience in implementing and administering new technologies to the existing networks in Windows 2008, 2003, 2000, Vista, XP, NT-based client/server environment, which also includes managing projects.

- Enterprise-level experience working with fortune 100 companies and Government Agency like Hewlett-Packard, IBM, Merrill Lynch, Unilever North America and Commonwealth of Pennsylvania
- Expertise in deployment, migration, and administration of Windows Server 2008, 2003, and 2000
- Expertise in administration and deployment of CA SiteMinder
- Installing and configuring VMware Server, VMware Player, and VMware Converter
- Expertise in administration and deployment of Radiant Logic VDS
- Installing and configuring Microsoft TMG 2010 Enterprise Servers
- Expertise in network administration; database administration; TCP/IP network implementation; system integration, management, and troubleshooting
- Expertise in installing and maintaining Microsoft Web Server clusters
- Configuring and administering ESRI GIS (Geographic Information Systems)
- Installing, configuring, and troubleshooting IBM Tivoli Monitoring and IBM Director
- Testing and integrating-various third party applications on Windows 2003 and 2000
- Extensive experience in testing, evaluation, and implementation of Windows 2003 and 2008
- Used PowerShell and VB Script for modifying and administering object properties in Active Directory
- Disaster recovery planning
- Experience with installation, configuration, and administration NetScaler Access Gateway and Citrix XenServer
- Configuration and administration of UNIX and Linux
- Excellent creation and editing of technical documentation; fast learner
- Excellent leadership and communication skills and strong analytical skills.

Employment History and Related Experience

Commonwealth Technology Center, Senior Integration Consultant, Harrisburg, PA, 2007 – Present

Configure and maintain SiteMinder Cluster Server for authentication, authorization and Single Sign-On on the Commonwealth network. Install, configure, and maintain Radiant Logic Virtual Directory Server for the Commonwealth Technology

UNISYS

Resource 99

Application Support

- Aelita Domain Migration Tool, Altiris 5.5
- Microsoft TMG 2010
- Radiant Logic (Virtual Directory
- Services)
- Microsoft SCOM Console
- CA SiteMinder R12.5

Web Technologies

- Microsoft IIS 6.0 and 7.5
- JBoSS

Center. Provide Level 3 support (regular and on-call) for the servers at the hardware, operating system, IIS, Microsoft .NET application, and multi-application levels.

- Support is 365/24/7 in an environment with application availability of 99.99 percent.
- Ongoing deployment of Windows 2003, 2008, IIS, and Database Server for the Commonwealth of Pennsylvania and its agencies.
- Troubleshoot and configure VMware hosts.
- Administer Windows 2003 and 2008 Active Directory and support more than 10,000 users.
- Configure, support, and troubleshoot Microsoft Clustered Server.
- Troubleshoot DNS and network issues.
- Support the entire environment (development to production) comprising more than 250 IBM xSeries servers.
- Resolve trouble tickets Using Remedy Ticketing System.
- Use the Change Management process for all changes; review change management requests.
- Install, configure, and administer NetScaler Access Gateway and Citrix XenServer.
- Install, configure, and manage Microsoft TMG 2010 Enterprise Proxy Server.
- Review and update documents according to agency requirements.
- Work with agencies to plan and implement projects on schedule.

Deloitte, Active Directory Engineer, Harrisburg, PA, 2007 – 2007

Level 3 support (regular and on-call) for the servers at the hardware, operating system, and IIS levels. The project involved deployment of Window 2003 IIS and Database Server for the Commonwealth of Pennsylvania. Project was to develop a solution for the Commonwealth's Department of Labor.

- Configured and administered Windows 2000 and 2003 Active Directory and supported more than 10,000 users.
- Configured, supported, and troubleshot Microsoft Clustered Server.
- Configured and troubleshot DNS and network issues.
- Installed and troubleshot IBM Tivoli Storage Manager Client.
- Installed and troubleshot IBM Tivoli Monitoring.
- Installed and configured VMware for testing regular patches and other software before installing them in production servers.
- Supported the entire environment (development to production) comprising 110 IBM xSeries Servers.

IBM, Wintel Systems Administrator, Poughkeepsie, NY, 2005 – 2007

This project involved deployment and maintenance of Windows 2000 and 2003 Server Standalone in an Active Directory domain. Supported IBM internal and

UNISYS

Resource 99

Application Support

external clients, which included more that 500 IBM servers. Led the knowledge transfer and transition of work to teams in India, Brazil, and China (training and cutover).

- Level 3 support for IBM servers at the hardware, operating system, and application levels.
- Configured and administered Windows 2000 and 2003 Active Directory.
- Configuring and troubleshot DNS and network issues.
- Installed and troubleshot IBM Tivoli Storage Manager Client.
- Installed and troubleshot IBM Tivoli Monitoring.
- Installed and configuring VMware for testing regular patches and other software before Installed them on production servers.
- Supported IIS on the production servers. Troubleshot and supported internal clients on requirements for Web hosting.
- Installed and supported two-node cluster with Microsoft SQL and shared resources on Shark.
- Installed and maintained IBM servers in the Poughkeepsie and Fishkill Data Centers.
- Provided 24/7 on-call Level 3 support for servers.
- Decided on technical and hardware details for clients.
- Performed extensive work on OpenSSH and Cygwin for communication between Windows and AIX servers.
- Performed change and problem management with IBM Manage-now (ITIL process).
- Configured and maintained Symantec System Center Console.
- Implemented and supported new business clients on the servers and the transition.
- Maintained up-to-date documentation on the process and procedure.

Hewlett-Packard/Unilever, Project Lead, 2003 – 2005

Created Active Directory sites. configured and scheduled site replication for these sites. Created and managed user accounts and groups. Migrated users from the NT4 domain to Windows 2003 domain using Aelita.

- Configured network services, including DC, GC, DFS, FRS, DHCP, and DNS.
- Migrated DHCP scope.
- Installed and configured Tivoli, Enterprise Security Manager, and Legato.
- Generated ESM reports on the new servers after deployment to make sure they all met security requirements.
- Restricted space allocated to each user using Disk Quota Management.
- Configured RAID on HP ProLiant DL380 servers.
- Turned over servers to production after the total quality check.
- Assessed the site and ordered required components to make the site ready for server deployment. Coordinated with the network team on network issues and

to get the server up and running in time to meet the SLA.

- Defined and refined a process for building and configuring Windows 2003 servers.
- Troubleshot problems that arose during server deployment and configuration.
- Installed and managed Exchange Server in the enterprise.
- Migrated the servers from Exchange 5.5 to Exchange 2000.

Hewlett-Packard/Unilever, Project Lead, 2003 – 2003

Led an eight-member team and led the deployment and migration to Unilever. Migrated users from the NT domain to Active Directory. Sychronized home shares using Aelita. The project involved building the new laptops according to Unilever standards.

- Created and assigned entrust certificates.
- Migrated user profiles for desktops and favorites using Altiris.
- Met deadlines and supported users for 7 days after the migration.
- Configured and created printers on Windows 2000 and 2003 servers.
- Performed group migration using Aelita.

Hewlett-Packard/Merrill Lynch, Senior Systems Engineer, 2003 – 2003

Implemented Active Directory Services. Configured and scheduled site replication over these sites. Created and managed user accounts and groups. Configured network services, including DHCP and DNS.

- Automated client PC installation using Remote Installation Services (RIS).
- Implemented security using Domain Security Policy, Group Policy, and file permissions of NTFS5.
- Restricted the space allocated to each user using Disk Quota Management.
- Migrated mail for users from the Windows NT4 environment to Windows 2000 Exchange Servers.
- Configured and tested the mail migration process using Aelita mail migration tool in a test lab before going to live migration.
- After successful mail migration of the users, provided users with daily support.
- Maintained problem and solution documentation from day to day.
- Coordinated team members for 24/7 operation to meet deadlines.

Hewlett-Packard/Unilever, Senior Systems Engineer, 2001 – 2003

Built and configured NT servers for different locations across North America. Once the servers were in production, configured, and tested the backup device for the server. Migrated and consolidated users' data from Novell and NT servers to the centralized server. Configured and created printers on the new servers.

- Created group shares for common groups and granting appropriate permissions.

UNISYS

Resource 99

Application Support

- Configured and tested the IBM backup device for the server using Legato.
- Built and deployed desktops and laptops for users on the Unilever build standard (Aztec)
- Created new NT IDs, Sprint IDs, and entrust certificates for users.
- Performed quality checks before delivering desktops and laptops to users.
- Performed user support on the client and server sides.

Additional Employment History

Ramco Systems Limited, Network Engineer	1999 – 2000
CIDER, Systems Executive	1995 – 1999
Horizon Computers, Software Executive	1994 – 1995

Education

- B.S., Physics, University of Madras, Chennai, India, 1993
- Master's degree in Software Engineering, APTECH Computer Education, Mumbai, India, 1996

Professional Development Training

- PowerShell v2 Essentials – Basic PowerShell commands for administrators - April 2011
- CA SiteMinder r12 Core 200 – February 2010

Certifications

- Microsoft Certified Solutions Associate – Windows Server 2008
- MCITP: Server & Enterprise Administrator Windows Server 2008
- Microsoft Certified Systems Engineer MCSE (NT 4.0, 2000, and 2003)
- Microsoft Certified Database Administrator (MCDBA)
- Microsoft Certified Systems Administrator (MCSA): Messaging
- Certified CA SiteMinder r12 Administrator
- Certified CA SiteMinder r12 Professional
- Certified in ITIL V3 Foundation
- Nortel Networks Certified Account Specialist, Enterprise Solutions – Data

This page intentionally left blank.

UNISYS

Domino Technologies Inc.

Resource 128

Application Support

Key Skills and Knowledge

- VMware ESX
- Execute server virtualization initiative resulting in nearly 90% virtualization of PennDOT server resources
- Manage shared enterprise IIS .NET application server platforms
- Manage shared enterprise IBM WebSphere MQ server platforms
- Install and manage IIS .NET based 511PA Web service application servers
- Assist in management and operations of IBM Host on Demand application servers

Professional Summary

System engineer with eight years of technical experience, primarily in server operations management.; Experienced with VMware ESX, Windows server, Intelligent Transportation Systems, Microsoft SQL, and Microsoft IIS.

Employment History and Related Experience

Domino Technologies, Inc., Pennsylvania Department of Transportation, Systems Engineer, Harrisburg PA, 2006 to Present

Design, implement and manage mission-critical VMware ESX environment. Execute server virtualization initiative resulting in nearly 90% virtualization of PennDOT server resources. Install and manage Advanced Traffic Management System servers and software. Install and manage HIS Platinum Highway Advisory Radio servers and software

- Design, implement and manage fully redundant IIS based solution to provide real-time traffic camera images to Web. Manage and troubleshoot file and print servers. Plan, coordinate and execute upgrade and refresh of district office file and print servers
- Perform on-site installation and troubleshooting of servers, routers, switches, KVMs and UPSs
- Assist in management and operations of PennDOT eGovernment WebSphere application servers
- Assist in installation and management of Axis CCTV traffic camera encoders
- Manage shared enterprise IIS .NET application server platforms, Manage shared enterprise Microsoft SQL server platforms, Assist in management and operations of PennDOT Right of Way application servers, Manage shared enterprise IBM WebSphere MQ server platforms
- Install and manage IIS .NET based 511PA Web service application servers
- Assist in management and operations of IBM Host on Demand application servers

Domino Technologies, Inc., Pennsylvania Department of Transportation, Technologist, Harrisburg PA, 2002-2006

Support user base of over 10,000, Troubleshoot hardware and software issues on workstations and servers running Windows NT/2000/XP/2003, Install and manage IBM Host on Demand mainframe terminal emulator, Use and support productivity suites including Microsoft Office 2000/XP/2003 and WordPerfect

- Create, deploy and maintain images for various workstations, laptops and tablet PCs

Resource 128

Application Support

- Install and support network and desktop printers, Install and support handhelds, including BlackBerry, Palm and Pocket PC devices, Manage systems using Microsoft SMS 2.0 and 2003
- Perform maintenance tasks within Microsoft SMS 2.0 and 2003
- Manage McAfee ePolicy Orchestrator and AntiVirus clients
- Test and deploy Microsoft patches using SMS and scripted CD, Support QMatic systems at remote sites. Assign and complete tickets with Remedy ARS

Education

- Central Pennsylvania College
- B. S. Information Technology – Cyber Security
- B. S. Criminal Justice Administration

Certifications

- Cisco Certified Networking Associate
- Microsoft Certified Professional

UNISYS

Automation Engineer

This page intentionally left blank.

UNISYS

Resource 129

Automation Engineer

Key Skills and Knowledge

Domain Expertise & Solutions

- Windows ISP operations
- Government IT operations
- Banking / Brokerage solutions
- Automation/Deployment

Project and Program Management

- Small development team
- Mentoring

Communication and Networking

- Distributed computing over routed / firewalled TCP/IP network

Databases

- MS SQL 2000 – 2008 R2

Hardware

- Dell PowerEdge
- IBM xSeries
- IBM BladeCenter

Operating Systems

- Windows 2008 R2 SP1
- Windows 2000 SP4
- Windows 2003 SP2

Software/System Architecture

- IIS 5.0 – 7.5
- .NET Framework 1.1 – 4.5
- AJAX technologies
- Windows Services in .NET
- BMC ADDM 9.0
- BMC BBSA 8.3 SP3
- BMC BAO
- .NET Enterprise Services (COM+)
- Queued Components in .NET
- MS ADAM (LDAP) in .NET
- MSMQ
- SCOM 2007
  SCCM 2007 R2
- Authorization Manager (AzMan)
- WMI

Professional Summary

Senior Microsoft technology consultant, skilled in both systems architecture design and software development; 20 years of experience, Extensive background in construction of software-based automated frameworks; Specializing in Microsoft technologies

Professional Experience

Unisys Corporation

Enterprise Workflow and Automation Development, 03/02-Present

Supporting Commonwealth of Pennsylvania Enterprise Data Center (ISP). Authored, designed, developed, and implemented the following enterprise solutions:

- ISP Workflow/Inventory System to keep register of servers, network hardware, Web applications, and their complex relationships, featuring security/audit trail, DPAPI encryption, performance superior to traditional ASP.NET, modular presentation layer, on-demand client code delivery, asynchronous processing (AJAX), integration with BMC Software's Remedy,
- Routed ISP Change Management center, ISP Maintenance Notifications module, outage log, work log, custom reporting. VB.NET 4.0, ASP.NET, Crystal Reports.NET, MS SQL 2008 R2
- Comprehensive Basebuild Automation (Base software deployment) for MS Windows-based servers (Dell / IBM / VMware Guest), featuring Web-based monitoring and management of basebuild settings/progress, hardware configuration
- Deployment and customization of Windows 2003/2008 operating system, security settings, various system management applications.
- Simultaneous deployments are supported. Flexible modular design. Integrated with the above-mentioned Inventory; solution is currently in production supporting over 2700 enterprise class servers. Designed for remote unattended execution. .NET Framework 4.0, VBScript, WinPE 3.1
- ISP Ad-hoc Automation Framework - integrated with the above-mentioned solutions to cover various post-basebuild activities, such as data collection, configuration changes, patch management, or application deployment; solution is designed for low connectivity (cross-firewall) requirements and low residual contamination of automation targets.

UNISYS

Resource 129

Automation Engineer

Merrill Lynch, Ajilon Services, Inc., Senior Systems Artchitect, New York, USA, 2000 - 2001

Performed code and data flow analysis, application design and integration, advanced troubleshooting, systems engineering, automation development, and upper-level production support. Provided expert knowledge of Internet application systems in investment banking/trading environment to ensure effective functionality, security, and performance of solution.

- Developed a distributed application management system that provides for monitoring, system configuration, automated application deployment and validation on MS Win2K based servers. The system is highly scalable and contains approx. 4000 lines of code.
- Technologies: MS Win2K Advanced Server, IIS 5.0, ASP, DHTML, Jscript, VBScript, VB 6.0 SP5, MS XML 3.0/XSL, SOAP 2.0 SP2, COM+, MS Site Server(LDAP, CRS), MS SQL 7.0, IBM MQ Series, MS Installer, Bridge MD Systems, Cisco LD/DD.

Other Employment

- Consulting Merrill Lynch & Co., Inc., New York, USA, 1999 - 2000
- Consulting Credit Suisse Asset Management, New York, USA, 1998 to 1999
- Assistant EDP Manager at Societe Generale Bank, Riga, LATVIA, 1995 1998

Education

- B.Sc. Riga Technical University, Latvia

Professional Certification

- ITIL v.3
- MCSE(Win2K/XP/NT), MCDBA(SQL2K), MCNE.

UNISYS

Backup Administrator

This page intentionally left blank.

UNISYS

Resource 130

Backup Administrator

Key Skills and Knowledge

- Domain Expertise & Solutions
- Project and Program Management
- Communication and Networking
- Databases
- Hardware
- Operating Systems
- Office Productivity Tools
- Technical Documentation

Professional Summary

Systems engineer with over 10 years of in depth knowledge and expertise in network infrastructure, protocol and security. Adept at moving into new environments and extrapolate from previous experience to quickly adapt to new technologies. Constant superior record of client assistance, facilitating timely and in depth analysis of technical issues explaining technical situations to clients in real world language

- Systems Administration: Windows 2000 Pro/ Server, Windows XP, Windows Vista, Windows 7, Windows Mobile, Windows 2003 Server, Windows 2003 Small Business Server, Windows 2008 Server, Windows 2008 Small Business Server.
- Network Infrastructure: DNS, WINS, VLAN, VPN, Routing, DHCP, Firewalls
- Operating systems: Linux (Red hat, Suse), and Microsoft
- Programs: Office 2000 – 2007, .NET Framework, IP Monitor, M.O.M (Microsoft Operations Manager), Symantec / Veritas Backup Exec, Symantec Anti- virus and End Point, Exchange, BlackBerry Enterprise, SQL, Viper enterprise antivirus, CA Unicenter, Acronis backup, EMC Networker, EMC AVAMAR, EMC DPA,

Employment History

- CWOPA / UNISYS: Backup Administration / Operations Consultant 2010 - Present
- US Army DOD Contractor/ B&D Consulting: DOIM IT Support Specialist 2009 - 2010 Kasual Computing Inc. : Systems Engineer / IT Consultant 2008 – 2009
- CompuMage Inc.: System Administrator / Network Administrator 2007 – 2008
- University Loft Co.: Intelligence Manager 2005 - 2007

Education

- LTS Computer Certification Training 2003-2004
- Indiana University-Purdue University Indianapolis 1999-2001
- McCutcheon High School Graduate 1995

Professional Certification

- ITILv3 foundation (May 2012)
- MCSA -Microsoft Certified Systems Administrator (Managing a Windows 2000 Network Environment 70-218 Mar 2008) (Windows 2000 Server 70-215 April 2004)
- MCTS -Microsoft Certified Technology Specialist (TS: Configuring Microsoft Windows Vista Client 70-620 Jul 2008)

UNISYS

Resource 130

Backup Administrator

- MCP -Microsoft Certified Professional (Windows 2000 Professional 70-210 July 2003)
- Watch Guard Certified Systems Professional (Firewall Basics with Fire ware v10.0 May 2008)

Professional Development

- EMC Tailored AVAMAR Admin Dec 2010
- EMC Education Services Course for Networker and AVAMAR administration fundamentals with focus on AVAMAR integration to Networker.

UNISYS

Resource 131

Backup Administrator

Key Skills and Knowledge

Domain Expertise & Solutions

- Avamar
- NetWorker
- CommVault
- Data Protection Advisor

Hardware

- IBM Tape Library
- Tape Drives
- Physical servers

Operating Systems

- Windows Server 2003
- Windows Server 2008 R2
- SuSE Linux
- RHEL / CentOS
- VMware ESXi

Office Productivity Tools

- MS Office
- Remedy
- Siemens phone

Technical Documentation

- Visio
- SharePoint

Professional Summary

17 years of experience as a system administrator, Experience with backups of large and small systems in complex environments, and Familiarity with backup products and procedures in use by Commonwealth of Pennsylvania.

Professional Experience

Unisys, LanceSoft, Inc, Commonwealth Backup Administrator, Herndon VA, 2011 - Present

Deliver backups of approximately 3000 physical and virtual servers in the Commonwealth Technology Center. Set up new clients for back up; ensuring backups occur properly, troubleshooting backups when problems occur, documenting backup configuration, and performing backups and restores as needed.

- Install and configure backup software for servers and clients, and create and run reports to verify proper operation of backups.
- On Call as part of a rotation to troubleshoot backup-related problems that occur, as well as performing system- and file-level restorations that are required after hours.

US Air Force, Integral Systems, Inc, Systems Administrator, Lanham MD, 2008 - 2011

Maintain servers and workstations, provided desktop support, performed regular backups, performed scheduled and unscheduled maintenance, performed software upgrades, assisted other members of the Sysadmin team, and other duties as necessary.

- Installed, documented, and performed integration testing on software install packages.
- Performed various troubleshooting to support customers locally and in remote locations. In addition,
- Worked in secured areas as needed, maintaining systems to DISA standards, and assisting cleared personnel with installing and testing software.
- Set up networks, using Cisco switches, routers, and firewalls. I installed servers using Linux, Solaris, and Windows, as well as Linux and Windows workstations.
- Assisted with company's move, secured all the servers and workstations for transport, performed hardware troubleshooting, repairing or replacing parts that failed, or were near failure.

UNISYS

Resource 131

Backup Administrator

- Assisted with the tech refresh process, to obtain and set up new servers and workstations. I set up new physical and virtual servers, and virtualized existing servers to better utilize existing hardware

Applied Security, Inc. Systems Engineering Consultant, Reston, 2007 - 2008

Supported the IT department for Linux administration and networking; maintained physical and virtual servers, added software, and configuring systems.

- Maintained the Asterisk VoIP phone system for internal and external phone calls, kept our servers up to date, configured VPNs (IPSec and OpenVPN) and VLANs as required
- Configured and maintained a variety of switches and routers. I also was responsible for purchasing equipment for our IT infrastructure.

US Post Office, Nortel Govt. Solutions, Systems Technician, Fairfax, VA, 2003 - 2007

Performed setup, installation, testing and evaluation of systems, including workstation and server computers and networks, both in our office and at postal facilities around the country

- Accomplished software analysis and testing, including failure analysis.
- Performed various system administration (including Debian and Fedora Linux administration) and networking tasks as assigned.

Computing Edge, Inc. Systems Technician, Springfield, MO, 2001 - 2003

I performed a wide variety of technical duties in the office and in the field. These included solving networking, software, and hardware problems for our company and for our customers. I also wrote software and analyzed the IT needs of customers using Windows 95, 98, 2000, linux, php, apache, and PostgreSQL

Education

- High School: Hillcrest High School, Springfield MO. High School Diploma. Specialized in Physics, Computer Science, and Media. Graduated 1994
- College: Southwest Missouri State University (now called Missouri State University), Springfield MO. Bachelor's of Science in Computer Science. Minors in Mathematics and Physics. Graduated 2001

UNISYS

Resource 131

Backup Administrator

Professional Certification

- Master Linux Administrator - Brainbench - 2001, 2007

Professional Development

- ITIL v3

This page intentionally left blank.

UNISYS

Network Engineer

This page intentionally left blank.

UNISYS

Resource 18

Network Engineer

Key Skills and Knowledge

- Cisco routing
- Cisco switching
- CheckPoint
- Large enterprise Internet connectivity
- Highly redundant networking
- Large enterprise 802.11a, b, g, and n wireless networking
- Resolution of complex problems

Professional Summary

Architect, implement, and support global highly available Cisco-based WAN, LAN, and wireless network solutions for converged voice, video, and data using the following technologies:

- MPLS, DMVPN, BGP, EIGRP, IOS Zone firewall, QoS (queuing, WRED, DSCP, shaping, and policing)
- Cisco 6500 (Supervisor 720-3C), VSS 1440, 4910R+E (Supervisor 7E), 3750, 3750E, 3750X, 3560, 2960, 2960S, 2950, and 2900
- Cisco ISR and ISR2 router series 3900, 2900, and 2800 routers; ASR 1000 routers
- Cisco ASA firewall and VPN appliances
- Cisco 6500 ACE load-balancing modules
- Cisco 5508 wireless LAN controllers, Cisco Aironet 3500 and 1260 series lightweight access points, and autonomous Cisco 1200 series wireless access points
- CiscoWorks LMS 3.2, Cisco ACS 4.2, RADIUS, and TACACS+
- Upgrade CheckPoint Provider-1 firewall.
- Support R65 through R75.40 SecurePlatform, IPSO, and GAIA
- Strong Level 2 and Level 3 switching skills, including MST spanning tree, LACP Etherchannel, VTP, VLAN, DHCP snooping, frame storm control, port security, port-level ACLs, and switching QoS (various models)
- Effective, in-depth troubleshooting and resolution of complex routing and switching problems
- Excellent development and support of QoS LAN, WAN, and Wireless edge-to-edge using the DIFFSERV model
- Particularly adept at engineering issues out of network systems to avoid problem
- Use tools such as Perl, regular expressions (REGEX), script development, EEM, and C programming language to broaden ability to solve problems and provide solutions.

Employment History and Related Experience

Unisys Corporation, Data PowerHouse Project, Network Design Engineer 1 – Team Lead, 2011 – Present

Engineer network designs; support, optimize, and monitor redundant Data PowerHouse network infrastructure.

- Provide ongoing support for the DPW Managed Security Services contract, including CheckPoint firewalls, high availability Provider-1 firewalls, and Proventia IPS.
- Resolve complex multiagency problems.
- Coordinate resources and set priorities as necessary.

UNISYS

Resource 18

Network Engineer

The Hershey Company, Hershey, PA, 2001 – 2011

Senior Network Specialist, Network Architect, 2007 –2011

Senior Network Analyst, 2005 – 2007

Network Contractor, 2001 – 2005

Designed, configured, deployed, and maintained a raised floor switching environment with Cisco VSS 1440 at the core and 3750E stacks at the server edge.

- Provided complete redundancy throughout the environment, using LACP Etherchannel to the Solaris and Windows servers and LACP cross-stack Etherchannel trunks from the VSS to the 3750E switch stacks.
- Improved performance and reliability and made deployments simpler, faster, and less error prone by introducing a more methodical switching design.
- Designed, configured, and maintained a redundant gigabit campus internetwork connecting 10 campus buildings spread across several square miles, providing a seamless voice, video, and data network experience for approximately 4,000 users.
- Developed a proven conceptual WAN model, the Hershey WAN Cloud, consisting of a set of rules by which the WAN was scaled and upgraded over time without jeopardizing its reliability or key features such as full mesh, dynamic recovery, and redundant connectivity.
- Migrated a WAN from hub-and-spoke Frame Relay and a dial backup topology to Sprint MPLS with Internet DMVPN-based redundant paths. Changing the topology to full mesh, stabilizing and reducing routes with BGP in place of EIGRP, introducing QoS, and adding DMVPN path redundancy nearly eliminated WAN-related network trouble calls by eliminating known and predicted problems.
- Upgraded a Sprint MPLS to an AT&T MPLS, providing a fully converged and properly scaled voice, video, and data network with QoS LAN and WAN policy that enabled voice and video deployments throughout the enterprise.
- Designed, configured, and managed 802.11b, g, and n wireless networks on Cisco autonomous Aironet 1200 access points and Cisco 5508 controller platforms using 1260/3500 series lightweight access points for 14 plants, 3 warehouses, and various offices and campus environments.
- Introduced VLANs, MST, access port policies, and Layer 3 switching to Hershey network deployments, improving performance, stability, and security throughout the enterprise.
- Installed and maintained CiscoWorks for more than 9 years to manage more than 1,500 Cisco devices, including routers, switches, and wireless access points.

Tyco Electronics MA/COM, Senior Network Engineer, Harrisburg, PA, 2000 – 2001

Troubleshot and configured Cisco routers on 3640s and 3620s. Provided specifications for LAN/WAN performance improvements using Cisco equipment

UNISYS

Resource 18

Network Engineer

and Compaq servers.

- Developed software to initiate a dialup-networking connection between a wireless radio and a PC in Microsoft Visual C++ for the Windows platform.
- Installed and configured a demonstration wide area radio system consisting of three Sun Ultra 10s running Solaris.
- Developed test plans for factory acceptance testing of wireless radio products in a WAN environment.
- Configured proprietary radio equipment.
- Conducted beta tests and error reporting on radio, base station, and Sun Solaris-based proprietary software.

Harsco Gas & Fluid Control Group, Network Manager, 1998 – 2000

Managed the implementation and maintenance of a Cisco router-based WAN for the entire division. Supported a mixed protocol network using RIP (IPX), OSPF, and NLSP routing protocols on Cisco 2600 and Cisco 2500 routers.

- Worked with SNA tunneling, bridging, and APPN on a Cisco-based WAN with AS/400s.
- Transitioned a Cisco multiprotocol WAN from an IP/IPX network to an all-IP network.
- Provided technical specifications and implementation guidelines for a Cisco PIX, router, and switch-based Internet connection to Harsco corporate headquarters.
- Managed a Cisco-based dial backup for factory sites to provide failover ISDN/PRI dial-on-demand connection when the Frame Relay circuit fails.
- Managed Cisco-based ISDN PPP dialup networking for analog and ISDN callers.
- Used a Cisco IOS firewall in house behind Harsco's primary firewall to refine control over traffic to Harsco's Web sites, AS400s, e-mail, and other systems.
- Completed VoIP pilot project using Cisco 3640 and 2610 routers connected to Lucent phone switches between two locations.
- Hired two highly qualified network technicians.
- Hired a telecommunications coordinator.
- Conducted formal annual reviews of employees.
- Trained employees to be high-quality support personnel.

Morgan Distribution, Systems/Analyst, 1993 –1998

Fulfilled a need for and expandable flexible multiprotocol WAN supporting TCP/IP (OSPF), IPX, APPN, SNA, and bridging over Frame Relay, dialup, and point-to-point networks using Cisco 4700s, Cisco 2521s, and a 2512 16-port Token Ring serial router for dialup. Migrated the enterprise to IP only from IPX, APPN, SNA, and bridging.

UNISYS

Resource 18

Network Engineer

Education

- 3 years toward B.S., Information Science, Kutztown University

Certifications

- Cisco CCNP, CCNA, and CCDA

UNISYS

Domino Technologies Inc.

Resource 132

Network Engineer

Key Skills and Knowledge

Technical Skills

- Windows Server 2003 – 7 Years
- Windows Server 2008 – 3+ Year
- Windows Desktop – 10+ Years
- Cisco LAN Switch Configuration - 7+ Years
- Cisco PIX Firewall Boot camp - 3 day bootcamp training
- Cisco Internetwork Troubleshooting - 7+ Years
- Linux – 7+ Years
- UNIX (Free BSD) – 7 Years
- operating system X – 10.0 – 10.6 Client/Server
- Data Center operations
- Solutions architecture
- Infrastructure architecture
- Network/Firewall Design
- Information Security
- Project Management
- Knowledge and experience with PennDOT and Commonwealth of Pennsylvania infrastructure
- He has more than 15 years of experience in all aspects of enterprise IT disciplines.

Professional Summary

He has more than 15 years of experience in all aspects of enterprise IT disciplines. Knowledge and experience with PennDOT and Commonwealth of Pennsylvania infrastructure. Information Technology professional with experience in designing and managing entire technology infrastructure

- Experience providing subject matter expertise in the areas of enterprise architecture, software development, system integration, IT infrastructure, IT operation, IT security, and development process modernization.
- Certified as Network Engineer, Experienced in Windows Server setup and administration
- Experienced as Information Technology manager
- Experienced in architecting infrastructure design for large complex applications in various platforms – Windows, UNIX, Linux, operating system X
- Worked as Voice and data communications technical lead for a large company's distribution centers and 6 corporate offices

Employment History and Related Experience

Domino Technologies, Inc, PennDOT, Network Engineer, Harrisburg, PA, 2011 - Current

Core Network Engineer and part of the Core Network Services Team, responsible for support for the PennDOT Keystone Building as well as all Drivers License Centers and Photo License Centers; Primary responsibility for PennDOT Keystone building and handled multi-agency support.

- Worked with carriers on network outages, ticket resolution and improving response time for our internal customers
- Planned and implemented CiscoWorks Prime, LMS solution for automating configured backup(s) and large scale config changes
- Responsible for network infrastructure in all District and County offices. I have provided on call support for all District and County Offices.

Standex ADP, I.T. Manager/Network Manager, Philadelphia, PA, 2010 – 2011

Responsible for architecting infrastructure design for enterprise solutions and applications. Voice and data communications technical lead for the company's distribution centers and 6 corporate offices. Involvement in a number of initiatives related to improve centralized and automated network management systems to meet corporate goals with minimum capital expenditure.

Domino Technologies Inc.

Resource 132

Network Engineer

- Lead for the network re-architecture efforts to facilitate better product delivery to customers. Team of 5
- Member of the final technical escalation team for all data centers network events and post sales customer support.
- Member of the customer incident review team.
- Team lead for the Exchange Server upgrade (moved from 2007 to 2010). Extensive technical experience with Exchange Server, including Internet Mail Service, OWA (Outlook anywhere), SMTP, SendMail, X.400 connectors, RAS connectors and gateways to disparate messaging systems.
- Team lead for a number of formal training exercises for the Engineering, NOC and Customer Care organizations.

PASSHE, Help Desk Manager, Harrisburg, PA., 2009 – 2010

I was a member of the Office of the Chancellor Technical Services Team. Managed a team of up to 15 Help Desk personnel, serving the entire Pennsylvania State System of Higher Education organization.

- Fielded incoming support requests via a central help desk phone line and e-mail box.
- Responsible for troubleshooting and resolving application and hardware issues for the end users.
- Provided one-on-one guidance and knowledge transfer to end users related to the various applications in use in the environment.
- Performed help desk duties in person whenever possible so as to produce the highest levels of customer satisfaction when performing such duties.
- Assisted with the support of the telephony system including on site telephony servers

Structure Interactive, I.T. Project Manager, Grand Rapids, MI. 2000 - 2009

Acted as technical liaison between Structure Interactive and various Dow Chemical division stakeholders, communicating technical issues and challenges in everyday language.

- Provided technical expertise for the seamless transfer of the dow.com property from being internally hosted by Dow Chemical to being managed by the IBM Web Services group.
- Implemented, installed and configured Windows SBS Server 2003.
- Provided critical path scheduling for all programming related tasks for the dow.com redesign.
- Created the 'Socrates' Web portal to provide information to disparate groups with centralized documentation on the various architectures and subsequent integration projects (Exchange/Active Directory related).

Domino Technologies Inc.

Resource 132

Network Engineer

- Implemented Check-Point Security for all VPN and remote user access by employees needing access to the internal network.
- Architected application solutions for several groups within Dow chemicals. Responsible for gathering their business and technical requirements and converting it in to optimal infrastructure solution.

John Deere, NOC Analyst, Moline, IL, 1996 - 2000

Managed a team of up to 15 engineers, 100+ Cisco 6509 layer 3 switches / routers serving over 600 internal customers and 3,000 Web servers. Hands on familiarity with products from Cisco, Nortel / Altheon, Juniper, Netscreen, IBM/AS400, F5, Blue Coat, Foundry and Avaya.

- Team lead for the network equipment rationalization project for the West Coast data centers.
- Networking team lead in the migration and integration of all customers from the Scott's Valley, Avasta, Progress Software and Conxion data centers to Navisite's San Jose data center. This involved moving over 750 servers.
- Lead for the "Architecture Desk" which has responsibility for the research, evaluation, approval and implementation of all equipment additions to our customer topologies with an eye to long-term supportability.

Education

- Northland Bible College, Dunbar, WI. Study, Major: Bible

Additional Training

- Windows Server 2003
- Windows Server 2008
- Windows Desktop
- Cisco Lan Switch Configuration
- Cisco Pix Firewall Boot Camp - 3 Day Bootcamp Training
- Cisco Internetwork Troubleshooting
- Linux
- Unix (Free BSD)
- Operating system X – 10.0 – 10.6 Client/Server

This page intentionally left blank.

UNISYS

Network Engineer

Key Skills and Knowledge

- Project and Program Management
- Communication and networking
- Hardware
- Operating systems
- Software/system architecture
- Office productivity tools
- Technical documentation
- Facilities management
- Cisco infrastructure
- 76xx border routers, 65xx series Core Layer 3 switching
- BGP peering to 3 upstream providers
- OSPF as local routing protocol
- Configuration, migration, documentation, and support requirements
- Content switching, high availability switching , routing, and firewall zone management
- Drafted a Quality of Service (QoS) standard to support VoIP, videoconferencing, and ERP
- Produced capital budgets for key business revenue – generating services in 7 separate facilities
- Developed operation figures to maintain and support the capital investments
- Managed multiple successful business acquisitions
- Convert networks

Professional Summary

More than 20 years of building highly resilient secured networks to meet business capacity needs and availability. Ability to lead during changes and maintain sustained performance.

- Detailed problem analysis ability to analyze detailed problems
- Multitasking of time-sensitive projects
- Security structured by the Common Body of Knowledge
- Proficiency with administering with firewall security policy
- Orientation to customer service and results
- Development of integrated organization structure.

Employment History and Related Experience

Unisys Corporation, Commonwealth of Pennsylvania, Network Security Engineer, Harrisburg, PA, 2007 – Present

Responsible for Commonwealth of Pennsylvania server farm network & hardware operations, security access & firewall configuration, performance & high availability designs and development

- Configuration, migration, documentation and support requirements maintaining content switching, high available switching, routing and firewall zone management.
- Detailed technical reviews of all network and security changes proposed to support agency business requirements.
- Detail packet analysis supporting application, network, and security operations.

Harsco Security, Network Engineer, 2006 – 2007

Consultant for a local business as a networking WAN engineer. Reviewed core infrastructure, implemented HSRP, and configured Multi Home BGP access. Diverse MPLS connections interconnected the enterprise campus core hardware.

- Drafted the corporation's Quality of Service (QoS) standard to support VoIP, videoconferencing, ERP, and other critical business applications.

Susquehanna Communications, Director of Network Engineering, 2003 – 2006

Developed, designed, structured, and managed an organizational strategy for voice, video, and high-speed data, providing support and security over a geographically diverse multiple cable service operation.

UNISYS

Network Engineer

- Implemented a Cisco infrastructure using 76xx border routers, 65xx series Core Layer 3 switching, BGP peering to three upstream providers, and OSPF as the local routing protocol.
- Directed the overall operations of seven large public network infrastructures providing high bandwidth and availability.
- Managed the conversion of a high-speed data product and infrastructure at a newly acquired cable market supporting more than 14,500 HSD subscribers under complex conditions and a tight timeline.
- Supported interactive video data network operations for this conversion.
- Produced capital budgets for key business revenue-generating services in seven separate facilities along with operation figures to maintain and support capital investments.

BlazeNet (Subsidiary of Susquehanna Media Corporation) Team Lead Network Engineer, 1997 – 2003

Designed networking business product offerings that provided a competitive edge over the competition, driving record sales, using Frame Relay, ATM, point-to-point T1 or fraction T1, DSL, cable modems, wireless, and SONET technology. Designed, implemented, and managed a large Web hosting server farm network using Foundry load balancers and a 802.1Q strategy.

- Maximized business sales opportunity by interacting with commercial customers and finding designs and partnerships that generated their highest ROI, which positioned BlazeNet as the preferred vendor.
- Implemented diverse Internet access points for small business by using EIGRP, which provided dynamic bandwidth failover.
- Managed multiple successful business acquisitions for the network conversion, which secured a stronger local community presence and increased revenue potential on capital investments.
- Influenced early adoption of virtual private networking, leveraging the technology in the commercial product offering and providing businesses with an opportunity to reduce or eliminate dedicated telecommunication lines.
- Led the business in network security for internal application access, commercial resale, and product development, which increased uptime and reduced repairs, providing higher efficiency.

Education

Associate's degree in Computer and Electronics, Electronic Institute

Professional Certification

Certifications

- ITIL v3 Foundation Certification, 2012
- Cisco Certified Internetwork Professional (CCIP) Certification – updated, 2012

UNISYS

Network Engineer

- CheckPoint Certified Security Expert (CCSE) Certification, 2008
- CheckPoint Certified Security Administrator (CCSA) Certification, 2007
- Cisco Certified Design Professional (CCDP) Certification – updated, 2012
- Cisco CCDA Certification – updated, 2012
- Cisco Certified Networking Professional (CCNP) Certification – updated, 2012
- Cisco CCNA Certification – updated, 2012
- ISC² Certified Information Systems Security Professional (CISSP), 2012
- GIAC Security Leadership Certificate (GSLC), 2005

Professional Development

Certificates of Completion

- Imperva Application Firewall Operation and Administration, 2012
- ITIL 2011 Foundation, 2012
- BMC BladeLogic BBNA Operation and Administration, 2012
- SANS: Google Hacking / Defense, UNIX Security & Auditing, Security Leadership Essentials for Managers, Legal Issues in Information Technologies, Fundamentals of Information Security Policy, 2005
- ARRIS, CMTS C4 Operations, 2003
- Alvarion, 2.4 GHz Wireless, 2002
- Learning Tree, Solaris Administration, 2001
- Global Knowledge, Cisco CCIE Prep Lab, 2000

This page intentionally left blank.

Patch Management

This page intentionally left blank.

UNISYS

Resource 114

Patch Management

Key Skills and Knowledge

Databases

- Microsoft SQL 2000, 2005, $ 2008
- Oracle 8i & 9i

Hardware

- Cisco routers and Catalyst switches, HP ProLiant GL360 & 380, Dell Power Edge servers, Compaq ProLiant servers, Dell workstations, IBM Thinkpads. IBM 3650s & 3850s, Quantum DLT Libraries, Big-IP (F5), Dell Dimension & Optiplex workstations, Dell & Gateway laptops, BlackBerry 8700 & 8800 series, Palm Tungsten & Treos, video teleconferencing equipment (VSX7000)

Operating Systems

- Windows NT, 9x, XP, 2000, 2003, & 2008 R2, Sun Solaris 7, 8, & 9, Red Hat Linux, Fedora, Novell NetWare 5.x & 6.x.

Software/System Architecture

- HP Insight Manager, HP OpenView, Veritas Backup Exec & NetBackup, J2EE 1.3, Microsoft Office, Microsoft Visual Studio .NET, SharePoint Portal Services, BMC Patrol 7.0, Connect Direct, Axway, SCCM 2007, & SCOM 2007

Programming Languages & Tools

- Treesizepro, BeyondCompare, Httpwatchpro, Idera, Litespeed, C, C++, & Java

Office Productivity Tools

- Microsoft Word, Excel, Access, FrontPage, & Notepad+

Professional Summary

More than 15 years of experience implementing and supporting Windows NT, 2000, 2003, and 2008 R2; Novell; and UNIX networking environments. Excellent understanding and troubleshooting skills in a large-scale enterprise network infrastructure.

- Experienced in the design and implementation od LANS and WANs, including leased lines, Frame Relay, ISDN and switched Ethernet (fast and gigabit), and FibreChannel switches
- Experienced in network, routing, and switching protocols, including TCP/IP (4.0 and 6.0), IPX/SPX, RIP, EIGRP, OSPF, IGRP, BGP, ISDN, and Frame Relay, and integrating IP networks with VoIP-based voice networks
- Solid knowledge of Microsoft Cluster Services, information security, risk management principles, Citrix MetaFrame Presentation Server, Microsoft SharePoint Portal Services, HP OpenView, and other similar tools
- Designed and implemented SAN solutions for clients using SAN hardware (FibreChannel switches and HP storage servers) and software components (Windows 2003 Storage Server and iSCSI).
- Experienced in technical presentations using Microsoft Visio and PowerPoint
- Experienced in DNS; DHCP; WINS; SNMP; NIS; LDAP; SMTP; POP3; IMAP; NTP; NAT; VPN; BIND; Terminal Services; Exchange Server 5.5, 2000, and 2003; Citrix Presentation Server, Xen desktop, SiteMinder; Microsoft Cluster Services, and RAID 10 and 5
- Implemented Linux Networks successfully — Linux as E-mail server, Web server, and Samba server for Windows network connectivity
- Handle large Enterprise networks for more than 50,000 users.

Professional Experience

Patch Management Consultant, Commonwealth of Pennsylvania, Sr. Infrastructure Engineer, Harrisburg, PA, 2012 – Present

Testing, Supporting, and Deploying Microsoft and third-Party Security patches, including Service Packs in different enterprise environments like Development, Stage, and Production using System Center Configuration Manager (SCCM 2007 R2). Process service tickets (in Remedy) in a 5,000-server environment; perform change management, problem management, and configuration management. Provide 24x7x365 application user support. Assign on-call rotation schedules to team members. Monitor the performance of servers (application clusters, database, BizTalk, and Web), and event logs. Track various issues and problems using Microsoft Terminal

Services and the Windows PerfMon tool.

- Create and manage system center deployments using SCCM 2007; consolidate and clean up collections periodically.
- Design, plan, and architect large-enterprise Windows environments with experience in managing and implementing large-scale servers in a production data center environment.
- Use experience with Infrastructure design, Active Directory implementation, system builds, performance monitoring and tuning, application and server high availability, and strong knowledge of disaster recovery.
- Underwent training programs in BMC BladeLogic Server Automation and ADDM (Asset Discovery and Deployment Manager). Created patch deployment packages in BladeLogic for deployment in the lab environment.
- Develop and manage patch release strategies and production delivery schedules for software applications.
- Troubleshoot performance-related issue in the IIS application.
- Verify security logs on different region servers for tracking user logins and logouts to the system, including unsuccessful login attempts. Load balanced and performance tune Web Server farms using SiteMinder 6.

Bank of New York Mellon, Sr. Infrastructure Consultant, King of Prussia, PA, 2010 – 2011

Tested and supported banking applications (ASP.NET) in different enterprise environments like development, QA, mirror, stage, and production, including trade floor support. Processed service tickets (in Seapine Test Track) in a 5,000-server environment. Implemented change management, problem management, and configuration management. Provided 24x7x365 application user support. Assigned on-call rotation schedules to team members. Maintained the performance of servers (application clusters, database, BizTalk, and Web) and event logs. Tracked various issues and problems with Microsoft Terminal Services and the Windows PerfMon tool. Applied service packs, hot fixes, and patches monthly through SMS 2007 to application and Web servers in all the testing and production environments.

- Designed, planned, and architected large enterprise Windows environments, managed and implemented large-scale servers in a production data center environment.
- Acquired experience with Infrastructure design, Active Directory implementation, system builds, performance monitoring and tuning, and application and server high availability. Acquired strong knowledge of disaster recovery.
- Created, ran, and maintained thousands of batch job schedules using ADVSYSCON Active Batch software on Web and SQL servers in all regions. Escalated issues and problems to various Global Operational

UNISYS

Resource 114

Patch Management

Services teams in King of Prussia or Pittsburgh.

- Actively participated in data center migration and relocation, including application and business process discovery, scheduling, physical move execution and vendor certification. Also participated in migrating applications from Windows 2003 and 2008 as well as IIS 6 and 7 platforms.
- Scheduled, configured, and maintained transmission jobs on Axway/Sterling Connect Direct software for clients like SunTrust, Genworth, ETrade, and FiServ. Set up NDM/FTP and subscriptions to leased lines from Verizon and AT&T.
- Created packages in BladeLogic for deployments and upgrades of various .NET applications.
- Troubleshot performance-related issues in the IIS application.
- Rolled SiteMinder out on the IIS server; troubleshot connectivity issues with these master server.
- Performed weekly and monthly application migrations (code moves as well as database fixes and updates) in production environments. Maintained Web sites quarterly. Monitored Web site traffic periodically with Truesight Coradiant.
- Backed up servers using NetBackup software, including monitoring backup logs and troubleshooting backup and restore errors. Created and executed disaster recovery preventive maintenance procedures at the Philadelphia site.
- Verifed security logs on different region servers for tracking user logins and logouts to the system, including unsuccessful login attempts. Load balanced and performance tuned Web server farms using SiteMinder v 6. Installing and configuring policy servers.
- Performed complete Active Directory administration, network conversions, remote access and system security using HP OpenView and IPsec.
- Installed and configured certificates on Windows production and test boxes for SSL connectivity to the portal sites (http://www.advisorport.com).
- Installed, configured, and administered SQL Server 2000 and 2005 and processes, including process monitoring using the Idera SQL tool and database core administration. Worked extensively with SQL Enterprise Manager; created databases, tables, views, and stored procedures. Backing up and restoring databases using Litespeed for SQL software was an integral part of the job.
- Created and administered virtual machines using VMware ESX Server 3.5. Worked extensively with VMware Infrastructure Client and administered Virtual Center 2.5.

Credit Suisse, Application Support Specialist, New York, NY, 2009 – 2010

UNISYS

Resource 114

Patch Management

Tested, deployed, and supported security management products in different enterprise environments such as QA, staging, and production using the Repliweb tool. Processed service tickets (ith Remedy 6.0 and 7.0) in a 5,000-server environment; implemented change management, problem and configuration management. Provided 24x7x365 application user support in the Americas, Europe, and Asia. Gathered functional requirements for the security product (Lumension). Prepared technical documentation for release to the various support teams, including branch support. Identified users for user acceptance testing of the product.

- Installed, configured, and maintained application servers using Windows 2008 Virtual Workstations application servers on HP DL 580s as well as SharePoint team Web sites. Load balanced the IIS 6.0 and 7.0 Web farm.
- Deployed content, both IIS Metabase and .NET assemblies, using Repliweb 4.1.1. Configured distribution and replication jobs.
- Assisted with and developed a process flow for automating content deployments across various environments such as QA, staging, and production.
- Created and modified vbscripts and batch scripts for automating the Windows environment.
- Deployed Lumension successfully in Altiris pushes to 25,000 clients, including laptops, workstations, and virtual desktops in the Americas region.
- Installed and configured SQL Server 2000 and 2005 clusters and processes, including process monitoring and database administration.
- Extensively used the Active Directory CSFB tool for issuing group memberships to aid users in application access. Remotely accessed user machines with Carbon Copy and fixed problems.
- Thoroughly tested Lumension on various USB devices like memory sticks, BlackBerry SD cards, smart phones, and hard drives. Sought users' acceptance for the product from the support teams.
- Identified and whitelisted about 50 BlackBerry device models including 8800s, 9000s, 9500s, and 9700s. Used Lumension Security Management Console to generate reports executing queries from SQL 2000 and 2005 databases. Administered and troubleshot Lumension application server problems.

Ernst & Young LLC, Systems Administrator, Secaucus, NJ, 2007 – 2009

Tested and supported gT&E (global time and expense) and eRooms SharePoint sites and applications in different enterprise environments like development, QA, and production. Processed service tickets (with Remedy 6.0 and 7.0) in a 5,000-server environment; implemented change management, problem management, and configuration management. Performed 24x7x365 application user support in the Americas (Region 1),

UNISYS

Resource 114

Patch Management

Europe (Region 2), and Asia (Region 3). Assigned 2-week on-call rotation schedules to team members.

- Monitored performance of servers (application, database, BizTalk and Web), and event logs. Tracked various issues and problems using Microsoft Terminal Services and the Windows PerfMon tool. Applied service packs, hot fixes, and patches monthly through SMS 2007 to the gT&E and eRooms servers in all the testing and production environments.
- Tested and monitored simple Web transaction response time and availability with BMC Patrol 7.1. Monitored applications, storage, and system devices.
- Created, ran, and maintained thousands of batch job schedules with Control-M agent 6.2 software on Web and SQL servers in all regions (1, 2, and 3). Escalated issues and problems to various Global Operational Services teams in Secaucus or worldwide.
- Changed application, SQL, and cluster services passwords quarterly for all IIS 6.0, application, and database cluster servers enterprise-wide information security policy.
- Connected to Oracle database servers using Oracle Enterprise Manager or SQLPlus on Oracle client software for performing application server tasks.
- Performed weekly gT&E migrations (code moves as well as database fixes and updates) in production environments. Performed monthly eRooms code moves (deployed extensions) in production environments in all three regions.
- Backed up servers using NetBackup software, including monitoring backup logs and troubleshooting backup and restore errors. Created and executed disaster recovery preventive maintenance procedures in gT&E regions 1, 2, and 3.
- Verified security logs on different region servers for tracking user logins (SSO) and logouts to the system, including unsuccessful login attempts. Load balanced and performance tuned Web servers with SiteMinder 6.
- Performed complete Active Directory administration, network conversions, remote access, and system security with HP OpenView and IPsec.
- Installed and configured certificates on Windows and UNIX boxes for SSL connectivity to the portal sites.
- Implemented and maintained DNS services on Linux servers.
- Created and modified cleanup DOS scripts to VB scripts for automating the Windows environment.
- Created and maintained documentation for various operating environments in Microsoft Visio 2003, Microsoft Project 2003, and Wintel.
- Installed, configured, and administered SQL Server 2000 and 2005 and processes, including process monitoring and database core administration. Worked extensively with SQL Enterprise Manager.

Created databases, tables, views, and stored procedures. Backingup and restoring databases was an integral part of the job.

- Configured SAN HBA cards on servers, including resolving any connectivity issues. Allocated SAN drive space of up to 500 gigs depending on requirements.
- Created and administered virtual machines using VMware ESX Server 3.5. Worked extensively with VMware Infrastructure Client; administered Virtual Center 2.5.

Maine Center for Disease Control, Server Administrator, Augusta, ME, 2007 – 2007

Supported IPHIS (Integrated Patient Health Information Systems) in different testing environments like development, staging, standby, and production. Processed service tickets (using Footprints) in a 200-server environment. Implemented change management, problem management, and configuration management. Provided desktop support with LANdesk and in person for all local and remote end users.

- Monitored servers (application, database, integration, and IIS 6.0) and event logs, tracked various problems. Applied service packs and hot fixes to IPHIS in all the testing environments. Started and stopped the WebLogic Server instances on the server.
- Ran scheduled tasks daily like Msgin, Msgout, MasterETL, and Drop_create_tables. Traced the log files. Escalated issues and problems to Office of Information Technology, State of Maine.
- Changed database schema owner passwords, Web servers, Sun One Directory Server Manager passwords, and batch process login accounts.
- Connected to Oracle database servers using Oracle Enterprise Manager or SQLPlus on Oracle client software for performing application server tasks.
- Installed and configured Terminal Services (Application Server mode) and SSL VPNs on Windows 2003 servers.
- Installed and configured BIND 7 DNS server for providing a naming service on the IPv6 network and the Internet.
- Installed and configured Rhapsody licenses on the integration server.
- Configured and monitored WSUS on Windows 2003 Server for patch management.
- Monitored and fixed synchronizing issues between the application server and the integration server.
- Backed up servers with Veritas Enterprise BackExec client software, including monitoring backup logs and troubleshooting backup and restore errors.
- Verified security logs on different servers for tracking user logins and logouts to the system, including unsuccessful login attempts.

UNISYS

Resource 114

Patch Management

- Extensively used RSA Database Administration for issuing security tokens to facility users for application access.
- Installed and configured certificates on Windows and UNIX boxes for SSL connectivity to the Maine's iphis portal.
- Created and modifying vbscripts, wscripts for automating Windows environment.

New York State/Office of Mental Health, Network Administrator
Manhattan, NY, 2006 – 2007

Processed service tickets in a 500-server environment; implemented change management, problem management, and configuration management. Provided desktop support with LANdesk and in person for all local and remote end users. Assisted a group of four to five members in Windows 2000 Professional, 98, and Me rollouts to Windows XP Professional. Configured and administered Windows 2000 and 2003 and Solaris 8 and 9 Servers.

- Configured Novell NetWare Cluster Services on a two-node Dell PowerEdge 2600 server for file and print services.
- Worked with Windows Active Directory and Novell e-Directory services to maintain facility users and resources. Also worked with iManager to install and configure Novell NetWare printers.
- Monitored and fixed synchronization issues between Active Directory and e-Directory using IDM.
- Monitored the performance of servers (application, database, and Web) and event logs. Tracked various issues and problems via MS Terminal Services and BMC Patrol 7.0.
- Worked extensively with Novell GroupWise 7.0.1 for messaging services in the facility.
- Configured and maintained Microsoft Exchange 2000 and 2003 in the facility. Worked extensively with Microsoft Exchange Service Manager (ESM). Worked with storage groups, mailbox, and public folder store administration.
- Performed complete Active Directory administration, network conversions, remote access, and system security with HP OpenView and IPsec.
- Implemented VLANs and Spanning Tree protocol on the LAN using VLSMs. Maintained network cabling for Ethernet connectivity to workstations using CAT3 and 5e cables.
- Maintained GroupWise, including post office rebuilds, DST remediations, and day-to-day administration.
- Supported OMH applications like CAIRS, CONCERTS, Meds Manager, and RAS.
- Installed, configured, and administered SQL Server 2000 and 2005 and processes, including process monitoring and database core

administration. Worked extensively with SQL Service Manager and Enterprise Manager.

- Extensively used RSA database administration for issuing security tokens to facility users for application access.
- Configured and maintained BlackBerrys and Palm Treo desktops for users in the facility.
- Wrote vbscripts and wscripts for automating the Windows environment.
- Configured and maintained SharePoint team Web sites and load balanced the IIS 6.0 and 7.0 Web farm.
- Monitored and implemented video teleconferencing service for the facility, including troubleshooting over ISDN lines.
- Configured Toshiba telephones for users, including backups of AMANDA voicemail.
- Installed and configured WSUS on Windows 2003 Server for patch management.
- Managed patches, Microsoft and Microsoft Office updates, Novell service updates, and hot fixes on servers including Firmware updates.
- Configured desktops for remote connectivity of applications using secure gateway.
- Administered the Novell servers through AdRemote console software.
- Backed up Novell servers using Veritas Enterprise BackExec client software, including monitoring backup logs and troubleshooting backup and restore errors.

Hanover Insurance Group, Server Administrator, Worcester, MA, 2006 – 2006

Processed service tickets in a 500-server environment, change management, problem management, and configuration management. Provided desktop support over the phone and in person for all local and remote end users. Configured and administered Solaris 9 as well as SunFire V480R and V440R servers.

- Configured Microsoft Windows 2003 Cluster Services on a two-node HP DL360 server for file services. Designed Microsoft Print Cluster Services on HP DL360 servers.
- Installed and configured Microsoft SharePoint services with MSDE on the primary domain controller. Organized corporate documentation, including contacts and meetings, using SharePoint Services.
- Added groups and resources under Veritas Cluster Server 4.0.
- Installed and configured BIND 7 DNS Server for providing a naming service on the IPv4 network and the Internet.
- Created and administered virtual servers using VMware ESX Server and load balancing. Moved GSX servers to the ESX farm.

UNISYS

Resource 114

Patch Management

- Developed Shell scripts, Perl scripts for automating, reported, and scheduled jobs using CRON and AT.
- Installed and configured WebSphere AS 5.1 on Windows 2000 Advanced Server SP3, including Web and SOAP Services.
- Deployed Web components (servlets and JSP files) on the application server.
- Managed patches, Microsoft and Microsoft Office updates, and hot fixes on servers; updated Firmware.
- Configured and administered Terminal Services (Application Server mode) and Citrix Metaframe presentation services on Microsoft XP Professional desktops for remote connectivity of applications using Secure Gateway.
- Installed, configured, and administered SQL Server 2000 and processes, including process monitoring.
- Installed and configured SAMBA services on Linux servers for connecting to Windows machines.
- Backed up servers using Tivoli Storage Manager Client software on IBM 800 and 8300 storage systems.
- Maintained DHCP, DNS, and WINS servers.
- Configured DFS for sharing folders and files over the enterprise network.
- Gathered and prepared technical documentation in Microsoft Visio software.

Varsitybooks Inc, Network/System Administrator, Washington, DC, 2005 – 2006

Configured and administered Windows 2000 and 2003, Wintel servers on HP DL blade servers, and Windows XP Professional workstations, including Dell and IBM ThinkPads. Installed and configured Microsoft SharePoint services on the Primary domain controller. Installing and configuring Solaris 9 on SunFire servers, including patching.

- Administered and configured the volumes using Veritas volume managers according to the customer's requirements.
- Performed complete Active Directory administration, network conversions, remote access, and system security using HP Insight Manager and IPsec.
- Worked with a system monitor to tune performance, thereby identifying potential bottlenecks.
- Configured and administered Terminal Services (Application Server mode) and VPN on Windows 2003 servers.
- Load balanced and performance tuned Web servers using a Big-IP F5 load balancer.
- Configured and administered .NET Framework Application Server on IIS 6.0 Server. Worked in XML to validate the configuration files.

UNISYS

Resource 114

Patch Management

- Administered and monitored the Big-IP load balancers for dynamic load balancing of the varsitybooks Web site.
- Installed, configured, and administered SQL Server 2000 and processes, including process monitoring.
- Backed up servers using BrightStor ARCserve backup software.
- Installed and configured DNS, NIS, and NFS servers.
- Installed and configured WebSphere AS 5.1 on Windows 2000 Advanced Server 5.1.
- Installed and configured Web and SOAP Services on application servers.
- Assisted in deploying applications on application servers.
- Gathered and prepared technical documentation for a simple disk-to-disk, disk-to-tape HP SAN solution for the production environment.
- Provided desktop support over the phone and in person for all local and remote end users.

American Florists Inc, Network/System Administrator, Boston, MA, 2005 – 2005

Upgraded a Windows NT network to Windows 2003. Migrated data server using the Aelita migration suite, including building trusts. Worked with 1,000 to1,500 users. Configured and administered Windows 2003 servers and Windows XP, 2000 Professional, NT, XP, 98, and 95 workstations.

- Worked with a system monitor in .NET application performance tuning.
- Wrote vbscripts and wscripts for automating the Windows environment.
- Performed complete Active Directory administration, network conversions, remote access, and system security using HP OpenView and IPsec.
- Installed and configured Terminal Services (Application Server mode), VPN, Web Server, and a Watchguard firewall on Windows 2003 servers.
- Backed up, restored, load balanced, performance tuned Web and app servers.
- Migrated Micrsoft Exchange Server 5.5 to version 2000 and eventually to Exchange Server 2003.
- Installed and configured RPC over HTTP for Exchange 2003 Server Services.
- Worked with Windows 2003 Cluster Server Administrator to administer clusters. Created nodes and resources as part of cluster server management.
- Configured and administered Ecommerce 2002 and BizTalk servers for Web and SOAP Services.
- Configured RAID volumes with Veritas Volume Manager.
- Maintained DHCP, DNS, and WINS servers.

UNISYS

Resource 114

Patch Management

- Developed Shell scripts and Perl scripts for automating, reporting, and scheduling jobs using CRON and AT.

Adelphi Academy, Network/System Administrator, New York, NY, 2001 – 2005

Upgraded a Windows NT network to Windows 2003. Migrated data from Windows NT to Windows 2003 Server using the NetIQ migration suite, including building trusts. Configured and administered Windows 2000 cluster servers and Windows XP, 2000 Professional, NT, XP, 98, and 95 workstations. Worked with more than 2,000 users and workstations.

- Executed vbscripts and wscripts using WMI.
- Configured send mail, fetch mail, and a virtual user and aliases table for enabling e-mail for users from multiple domains with SMTP, IMAP, and POP3 protocol support.
- Implemented and maintained IGRP between the head office and branches on Cisco 1700 through 2500 series routers using leased lines for WAN connectivity and Catalyst switches for LAN connectivity.
- Installed and configured a Sun StorEdge 3310 and 3510 storage area network.
- Installed and configured Terminal Services (Application Server mode), VPN, Web server, and a firewall on Windows 2003 servers.
- Installed, configured, and administered WebSphere Application Server, HTTP Web Server, and Secure Way Directory (LDAP) for e-product development.
- Resolved Windows and UNIX connectivity issues using SAMBA.
- Monitored jobs on SQL server 2000 databases.
- Performed backups, restores, load balancing, and performance tuning of Web and app servers.

Education

- Master's in Computer Engineering, Fairleigh Dickinson University, NJ
- Master's degree in Physics, Andhra Pradesh, India
- Bachelor's degree in Physics, Andhra Pradesh, India

Professional Certification

- Microsoft Certified Professional Systems Engineer (MCSE)
- Microsoft Certified Professional (MCP + I)

This page intentionally left blank.

UNISYS

Project Manager

This page intentionally left blank.

UNISYS

Resource 133

Project Manager (Client Service Manager)

Domain Expertise & Solutions

- Public Sector
- Infrastructure

Project and Program Management

- Proposal Development
- Scope Management
- Time Management
- Cost Management
- HR Management
- Communications Management
- Risk Management
- 3rd Party Management
- Procurement Management
- Documentation

Professional Association

- Certified Project Management Professional by Project Management Institute (1279344)
- Member of the Project Management Institute (1080310)
- ITIL V3 Foundation (March 2012)

Awards

- 2012 Outstanding Leadership and Innovation ("Ollie") award winner for participation on Mobile Video Recorder project for the Pennsylvania State Police

Professional Summary

More than 20 years with Unisys in departmental management, project management, business development, sales and marketing.

Project Experience

Unisys, Commonwealth Technology Center, Project Manager, Harrisburg PA, 2012 – Present

A member of the Commonwealth's PMO, responsibilities include management of projects for the Web hosting environment and coordination and stakeholder communications for operational and project activity for select state agencies.

Unisys, Commonwealth Technology Center Web Hosting, Client Service Manager, 2008 – 2012

Project responsibilities include management of the client service management program, service management for assigned state agencies, management of assigned projects, and development of monthly reports for the Commonwealth's CTO.

Unisys, Pennsylvania State Police, CLEAN, Project Coordinator, Harrisburg PA, 2008 -2008

Project responsibilities were focused primarily on project initiation and execution. Activities included setting up team room and related processes, drafting many of the project documents, including the project management plan and subsidiary plans, and coordinating schedules and resources for testing.

Unisys, Office of Administration, Showcase, Project Manager, Harrisburg PA, 2008 -- 2009

Project management responsibilities included project initiating, planning, executing, monitoring and controlling, and closing. Project scope included setting up and executing a media relations program to increase awareness of the Commonwealth's IT initiatives and successes to create a positive public image.

Unisys, Department of Revenue, Customer Service, Project Manager, Harrisburg PA, 2008 - 2008

Project management responsibilities included project initiating, planning, executing, monitoring and controlling, and closing. Project scope included the analysis of DOR's customer interaction points with the objective of identifying issues and recommending ways to improve customer service.

Unisys, DLI UCMS Portal Implementation, Project Manager, Harrisburg PA, 2007-2008

Project management responsibilities included monitoring and controlling project work, managing communications, documenting issues, and coordinating

UNISYS

Resource 133

Project Manager (Client Service Manager)

activities between the Office of Administration and OA and Department of Labor & Industry. Project scope included the implementation of a portal (staging and production environments) in OA's Enterprise Server Farm for DLI's new application for unemployment compensation.

Unisys, Microsoft Exchange 2007 Migration, Project Manager, Harrisburg PA, 2008 - 2008

Project management responsibilities included monitoring and controlling project work, administering the project plan, and managing stakeholder communications for IT managers at 47 state agencies. Project scope included migration of 80,000 mailboxes to a new MS Exchange 2007 messaging infrastructure, the largest such migration in North America at the time.

Unisys, Web Application Hosting and Messaging, Project Manager, Harrisburg PA, 2002 - 2007

Project management responsibilities included cost, scope, human resource, and procurement management for 26 full-time resources. The Enterprise Server Farm had more than 600 servers and 200 Web-facing applications.

Unisys, Infrastructure Management, Performance Manager, Harrisburg PA, 2004 - 2007

Project management responsibilities included project initiating, planning, executing, and monitoring and controlling, with emphasis on integration, scope, cost, quality, human resource, communications and procurement management. The infrastructure included Nortel switches, Cisco routers, CheckPoint/Nokia firewalls and servers from several manufacturers.

Unisys, Security Assessment, State Police, Project Manager, Harrisburg PA, 2005 - 2005

Project management responsibilities included project initiating, planning, executing, and monitoring and controlling, and closing, with emphasis on integration, scope, time, cost, quality, risk, and communications management. Unisys used manual methods and automated tools to identify known vulnerabilities in the State Police's networked environment and recommended strategies to transfer, minimize, accept, and eliminate risk associated with those vulnerabilities.

Unisys, Telcove, PA Office of Administration, Project Manager, Harrisburg PA, 2005 - 2005

Project management responsibilities included project initiating, planning, executing and monitoring and controlling, with emphasis on integration, scope, time, cost, quality, risk, and communications management. Working as a subcontractor to Telcove, the Commonwealth's primary telecommunications supplier, Unisys led a project to develop a Certificate Policy (CP) and Certification Practice Statement (CPS) for the issuance of Verisign Certificates

UNISYS

Resource 133

Project Manager (Client Service Manager)

supporting an enterprise VPN solution for Commonwealth employees and contractors.

Unisys, Managed Voting Services for PA, Program Developer, Harrisburg PA, 2005 - 2005

Unisys developed a services program to assist Pa. counties with compliance to the U.S. Help America Vote Act. Unisys' program included consulting, deployment, outreach and training services, as well as new voting technology solutions from AccuPoll Systems. Responsibilities included the definition of communications and training requirements and development of related solutions, pricing and proposals.

Unisys, Telcove VPN Pilot for Office of Administration, Project Manager, Harrisburg PA, 2005 - 2005

Project management responsibilities included project initiating, planning, executing, and monitoring and controlling, and closing, with emphasis on integration, scope, time, cost, quality, risk, and communications management. Working as a subcontractor to Telcove, the Commonwealth's primary telecommunications supplier, Unisys provided a suite of services for the implementation of a VPN pilot using Verisign certificates for Pa.'s Office of Administration and State Police. The project entailed the configuration and installation of Cisco VPN technology and integration with Commonwealth and Verisign systems for the issuance of certificates for the Pa. State Police VPN users.

Unisys Commercial Sales, Portfolio Sales Executive, Harrisburg PA, 1989 - 2002

Responsibilities included identification, qualification and winning of new business in the corporate network and desktop services marketplace. Exceed annual quotas for revenue, margin and customer satisfaction.

- 1998 North American Salesman of the Year
- Achieved quota for four consecutive years
- Exceeded 200 percent of quota in 2000
- Managed U.S. public relations efforts for $2 billion customer services division, supporting new product offerings, customer meetings and executive communications
- Develop communications plans and create brochures and other marketing materials for Unisys customer services division. Create, edit and publish Unisys NewsNet, a daily internal employee newsletter

Education

- Master's Degree, Journalism, Temple University, July 1990
- Bachelor's Degree, Liberal Arts, Franklin & Marshall, May 1983

UNISYS

Resource 133

Project Manager (Client Service Manager)

Professional Training

- Project Management Professional (PMP) Certification Prep (PMBOK® Guide -Third Edition-aligned)
- Project Cost Management (PMBOK® Guide -Third Edition-aligned)
- Project Scope Management (PMBOK® Guide - Third Edition-aligned)
- Project Integration Management (PMBOK® Guide - Third Edition-aligned)
- Project Time Management (PMBOK® Guide - Third Edition-aligned)
- Project Management Essentials (PMBOK® Guide - Third Edition-aligned)
- Project Risk Management Workshop
- Project Feedback Program
- ITIL Foundations
- Internet Security: An Overview
- Unisys Six Sigma Lean White Belt
- Financial Requirements and Setup for Project Managers
- Project Reporting for Project Managers
- Revenue, Invoicing, and Costing Concepts for Project Managers
- Introduction to 3D-VE and 3D Blueprinting
- 3D-VE Infrastructure Modeling and Traceability
- Introduction to Business Architecture At Unisys v2.0
- Getting Started with Rational(R) RequisitePro(R)
- Principles of Modeling
- Principles of Rational Unified Process
- Getting Started With Rational ClearCase® v2002
- Introduction to Business Blueprinting
- Managed Services

UNISYS

INFO-MATRIX CORPORATION

Resource 134

Project Manager

Key Skills and Knowledge

- Cisco CCNA
- *Project Management Professional* (*PMP*)
- Microsoft Certified System Engineer

Professional Summary

Professional with over 15 years of IT experience. Proficient with networks and network administration. A PMP certified professional and Microsoft Certified Systems Engineer.

Employment History and Related Experience

Essential Enterprise Solutions ,System Administrator, Mechanicsburg, PA, 2012-2012

Manage Windows servers, Work helpdesk, Manage Cisco and NetGear switches and Firewalls, and Document the layout of the network

Cumberland County IMTO Dept., Technical Manager/Network Administrator, Carlisle, PA, 1997-2012

Run the day to day operations at Cumberland County, Assist in the development of long term solutions for Cumberland County, Support eight other employees with help when needed

- Assisted with the designing and implementation of an Microsoft IP network
- Developed and implemented an E-mail and Proxy server
- Troubleshooting software
- Worked with all Windows operating system, Office 97/XP/2010, WordPerfect

Cumberland County Sheriff's Dept., Security Officer, Carlisle, PA, 1996-1997

Maintaining Security and discipline in the county buildings and Register and assist visitors for meetings

Education

- New Horizons, Mechanicsburg, PA, Microsoft Server 2008
- Guidance Software, Sterling, VA, PC, Internet and E-mail Forensics
- National White Collar Crime Center, Fairmont, WV, BDRA and ADRA
- Intellimark, Mechanicsburg, PA, System Management Server
- Computer Learning Network, Camp Hill, PA, Diploma in Microsystems Technology

Resource 134

Project Manager

Certifications

- Central Pennsylvania College, Summerdale, PA, Cisco CCNA
- New Horizons, Mechanicsburg, PA, Project Management Professional (PMP)
- New Horizons, Mechanicsburg, PA, Microsoft Certified System Engineer

UNISYS

Resource 135

Project Manager

Key Skills and Knowledge

- Domain Expertise & Solutions
- Project and Program Management
- Communication and Networking
- Hardware
- Operating Systems
- Software/System Architecture
- Call Center and Help Desk
- Office Productivity Tools
- Technical Documentation

Professional Summary

An experienced leader in global, national and regional operations with a proven track record of driving cost efficiencies while expanding the scope and quality of services. Disciplined approach to project management that provides on time, on budget, zero defect delivery. Skilled in employee performance management, goal setting and driving collaborative team work.

- Production Assurance / Incident and Problem Management
- Root Cause Analysis
- Process development and improvement based on ITIL standards
- Performance Management
- Disciplined operational support and project management
- Core infrastructure management
- Enterprise server operations
- Merger integration and business unit IT consolidation
- Payment Card Industry (PCI) vulnerability remediation
- National Institute of Standards and Technology (NIST) remediation
- Microsoft Active Directory
  - Microsoft Public Key Infrastructure (PKI) and Certificate Services
  - Microsoft Systems Center Operations Manager 2007 (SCOM)
- Microsoft Systems Center Configuration Manager 2007 (SCCM)
- Microsoft Windows Server 2003 and 2008 R2 Enterprise
- Microsoft Internet Information Services 6.0, 7.5 (IIS)
- VMware/VSphere

Professional Experience

Unisys, Commonwealth of Pennsylvania Office of Administration, Operations Manager, Harrisburg, PA, 2007-Present

Responsible for the day-to-day operational support and project management of over 3000 servers hosted at the Commonwealth of Pennsylvania's Enterprise Data Center.

- Microsoft Active Directory Domain Services (AD DS)
- Microsoft Public Key Infrastructure (PKI)
- Microsoft System Center Operations Manager (SCOM)
- Microsoft Windows server 2003 and 2008 R2
- Microsoft Internet Information Services (IIS)
- Payment Card Industry (PCI) vulnerability remediation

JP Morgan Chase & Company, Infrastructure Director, Columbus, Ohio, 2001–2007

Responsible for the day to day operational support and availability of JP Morgan Chase's national centralized file and print server environment, encompassing

UNISYS

Resource 135

Project Manager

over 1000 infrastructure servers. Responsible for establishing organizational goals, translating organizational goals to individual employee goals, achieving goals, motivating employees, employee performance reviews and hiring and termination decisions. Participated in daily production meetings with each major JP Morgan Chase line of business to discuss priority one service issues and service improvement programs.

- Achieved an 81.1% reduction of priority one incident volumes, and a 90.9% reduction in customer outage minutes January 2006 versus January 2007.
- Change Management success rate exceeded 99.5%.
- Consistently exceeded customer service level agreements for server availability, client impact outage minutes and average time to repair.
- Participated in the design and implementation of the global active directory infrastructure
- Implemented and supported IIS Web servers for Web hosting functions
- Implemented and provided ongoing support for Microsoft Operations Manager (MOM) infrastructure for server monitoring.
- Implemented and provided on-going support for Microsoft Systems Management Server (SMS) infrastructure for application distribution.
- Implemented and provided ongoing support for Microsoft high availability clusters.
- Implemented and provided ongoing support for disaster recovery configurations.
- Developed and implemented server patch management systems to quickly and efficiently patch servers for CSIRT vulnerabilities within tight service level agreements, mitigating risk to the firm.
- Developed internal applications to monitor server configuration management and server backup success.
- Developed and implemented weekly and monthly reporting metrics for server key performance indicators. This data was used to proactively develop internal service improvement programs.
- Developed process documentation for standard operating procedures.
- Successfully passed all IT Risk audits driven by SOX requirements.

DAT Enterprises, Inc., President, Clayton, NJ, 2000–2001

Successfully implemented a secure information systems architecture between FirstUSA (A Bank One / JPMorgan Chase credit card company) and their First Values marketing partners for the secure transfer of card holder information. This high profile contract was in response to pending government legislation. The project was implemented ahead of time, under budget and with zero defects.

- Represented Lockheed Martin in new business proposal development.
- Developed proposals that required end-to-end documented IT support processes and procedures.

UNISYS

Resource 135

Project Manager

- Developed plans to implement automated systems monitoring solutions, escalated support teams and a help desk to provide front line support.

Computer Methods Corporation, Consultant, Mount Laurel, NJ, 1997– 2000

Represented Computer Sciences Corporation (CSC) as a Project Manager and technical lead under their contracted outsourcing agreement with E.I. DuPont. Responsible for the successful implementation of over 50 technology projects.

- Led a team that successfully implemented an SAP R3 infrastructure for DuPont Automotive at 12 North American locations.
- Led a team that successfully performed a technology refresh of 500 laptops for the DuPont-Merck pharmaceuticals sales force. The laptop standard build was designed to support the Siebol CRM solution. In conjunction with the laptop refresh, migrated the sales force from Microsoft Exchange to Lotus Notes. The migrations occurred over two one-week periods at remote locations (Chicago & Las Vegas). The result of this project resulted in an outsourcing agreement between CSC and E. I. DuPont Merck.

Lockheed Martin Technology Services, Engineer, Cherry Hill, NJ, 1987–1997

Engineer responsible for the deployment of complex Digital Equipment Corporation (DEC) VAX based computing systems at various locations around the globe. Accountable for all phases of the deployment including implementation, user acceptance testing and final site acceptance testing..

United States Navy, Cryptologic Maintenance Technician, 1981– 1987

Work center supervisor for a team of nine cryptologic maintenance technicians. Responsible for the day to day operational support of complex VAX based computing systems that utilized one of the government's first secure global TCP/IP networks. Maintained a Top Secret/SCI security clearance.

Education

- Currently pursuing a Bachelor of Science degree at Millersville University
- US Navy, Advanced Computer & Electronics Training – 1983
- Manheim Township High School, Neffsville, Pennsylvania - 1981

Professional Certification

- PMP certification from PMI.org
- Information Technology Infrastructure Library Foundations ITIL V3

UNISYS

Resource 135

Project Manager

- Microsoft Certified IT Professional (MCITP) – Windows 2008 Enterprise Administrator
- Microsoft Certified Systems Engineer W2K3 MCSE
- Microsoft Certified Systems Engineer W2K MCSE
- Certified Novell Engineer 5.x CNE5
- Microsoft Certified Systems Engineer NT4 MCSE
- Certified Novell Engineer 4.x CNE4

Technical Writer

This page intentionally left blank.

UNISYS

Resource 136

Technical Writer

Key Skills and Knowledge

- Technical Writing
- SharePoint
- ITIL Certified
- MS – Office 2007 – Word, PowerPoint, Excel.
- Microsoft SharePoint
- Adobe Photoshop
- Adobe Acrobat
- Robo-Help
- Visio Professional
- MS Outlook
- Web Design
- Microsoft Expression Web

Professional Summary

20+ years of experience managing and solving business problems with technology solutions such as databases, Web sites, and SharePoint sites. Gifted Technical writer; Subject Matter Expert for the creation and maintenance of Management and Procedures Manual, Disaster Recovery Manual, Remedy Help Desk Support User Guide, Communications Management Plan, Pennsylvania Pharmaceutical Rebate Information Management System User Manual, and the Operator Reference Manuals for the Data PowerHouse at Willow Oak.

- Create PowerPoint presentations for prospective clients.
- Format and clean up presentations for Unisys Teams.
- Create graphics and .pdf files for Unisys Teams.
- Manage access and maintain the SharePoint Intranet Web site for the Unisys Harrisburg Data Center.

Manage access and maintain the extranet Web site where all our reports are located and allow access to Commonwealth employees and IBM employees.

Employment History and Related Experience

Unisys, Data PowerHouse, Technical Writer / Web Designer, Harrisburg PA, 2001 - Present

Create and maintain technical documentation for the Data PowerHouse at the Harrisburg Data Center. Responsible for the following manuals:

- Management and Procedures Manual. This manual reflects the procedures for the Outsourcing Program between Unisys and the Commonwealth of Pennsylvania. I improved the process for updating this manual by working closely with Unisys and IBM staff members. I created a timeline and enforced the need to have the manual updated in a timely manner to meet audit deadlines.
- Disaster Recovery Manual for all State Agencies. This manual is for documenting the strategies, personnel, procedures, and resources for the continuation of data processing services in the event of total destruction or temporary disablement of the Commonwealth Data PowerHouse at the Willow Oak Service Center located in Harrisburg, Pa.
- Remedy Help Desk Support User Guide. This manual is for a formal tracking system used by the Commonwealth of Pennsylvania Data Center Project and Unisys Corporation. This system was used for tracking system records, reviews, monitors and reports hardware, software procedural and documentation problems.
- Communications Management Plan: This manual defines the management interfaces that would be utilized to exchange relevant contract information between Unisys and IBM.

UNISYS

Resource 136

Technical Writer

- Operator Reference Manuals for the Data PowerHouse at Willow Oak: These manuals are used to help the Operators in the Data Center perform their job functions for the Data PowerHouse. I maintain manuals for each State Agency.
- Pennsylvania Pharmaceutical Rebate Information Management System User Manual: This training manual is used by Unisys to administer the PA PROMISe™ Drug Rebate System.
- Operator Reference Manuals for the Data PowerHouse at Willow Oak: These manuals are used to help the Operators in the Data Center perform their job functions for the Data PowerHouse. I maintain manuals for each State Agency.
- Create PowerPoint presentations for prospective clients.
- Format and clean up presentations for Unisys Teams.
- Create graphics and .pdf files for Unisys Teams.
- Manage access and maintain the SharePoint Intranet Web site for the Unisys Harrisburg Data Center.
- Manage access and maintain the extranet Web site where all our reports are located and allow access to Commonwealth employees and IBM employees.

NorSoft, Inc, Web Designer, Camp Hill, PA, 1999-2000

Create and maintain Web sites for NorSoft clients: Create and maintain client server Web-based help files for Auntie Anne's franchising application. Created Web-based application screens for ScriptFast and Clark Worldwide Transportation

AMP, Inc., Systems and Procedures Analyst, II, Harrisburg, PA, 1992 - 1999

Designed and maintained multiple Web sites for corporate Intranet. Technical writer for corporate standards and procedures. Developed and implemented Web sites for various departments. Redesigning these sites allowed the users to find information more efficiently.

- Redesigned client server methodology into .pdf format for the corporate Intranet. This provided the users a more efficient way to print out all or part of the document.
- Created GUI standards for client server applications. Researched various GUI standards resources and developed a quick reference guide.
- Developed a manual for corporate server standards. Converted this manual from word format to .pdf format and incorporated it into our Web site. This allowed for quick and easy access and the most current version was always on the Web for analysts to use when configuring a new server.
- Designed and maintained multiple Web sites for corporate Intranet. Created help systems for Windows95 applications. Supported mainframe printer assignment system.
- Created windows help using Robo-Help software, critiqued GUI designs for Client Server applications, Client server application testing, created training materials for Client Server applications.
- Developed manual and on-line help for Migration Request Express system.

UNISYS

Resource 136

Technical Writer

MR/X is a tool that provides migration control capability for IBM/MVS application systems developers and support staff. Received a certificate of commendation for this team effort.

- Designed a printer assignment manual and on-line help which decreased user problem calls by 50%; Provided technical support for mainframe help system. Submitted a series of JCL jobs to migrate the on-line help for corporate CICS applications, maintained CICS Programmers Analyst manual.
- Created a windows help file using Robo-Help for corporate mainframe methodology. Provided technical support for Printer Assignment System and technical documentation using MS/Word.

Other Employment

- A. Peters, Inc. Allentown, Pa., Keypunch Operator, 1977 - 1982
- Library Processing Systems Allentown, Pa., Keypunch Operator, 1969 - 1977

Education

Unisys University - Set Goals and Prioritize Your Use of Time 2006		Knowledge Soft - Intermediate HTML - 1997
Unisys University -The Basics of Listening 2006		Knowledge Soft - Authoring HTML - 1996
Unisys University -Listening for Higher Purposes 2006		AMP - Network Infrastructure - 1996
Unisys University -Effective Listening Skills Simulation 2006		Executrain - Word 6.0 Advanced - 1995
Unisys University -Major Time Management Challenges 2006		Solutions - RoboHelp - 1995
Unisys University -Listening for Comprehension 2006		Executrain - Excel 5.x Beginning Spreadsheet – 1995
Unisys University -Enhancing Your Listening Skills 2006		HACC - CIS110 Intro. to Microcomputer nformation - 1994
Unisys University -Analyze Your Use of Time 2006		Executrain - Intermediate MS Windows - 1994
Unisys University - Introduction to Business Blueprinting - 2003		Executrain - Harvard Graphics 3.0 - 1994
Microsoft PowerPoint 2000 – Advanced Unisys CBT - 2000		Executrain - Intermediate DOS - 1994

UNISYS

Resource 136

Technical Writer

Participating in Project Teams - Unisys CBT - 2000		Executrain - Advanced WordPerfect - 1994
Penn State University - Webmaster Certification - 2000		AMP - Team Building - 1994
Human Factors - How To Design Usable Web sites - 1999		HACC - Word, Lotus, Dbase - 1993
Knowledge Soft - FrontPage98 - Advanced - 1998		Executrain - Microsoft Windows - 1993
Knowledge Soft - FrontPage98 - Introduction - 1998		Executrain - Advanced WordPerfect - 1993
Knowledge Soft - Effective GUI Design - 1998		Executrain - Put It In Writing - 1992
Executrain - Using Your Professional Energy – 1998		Executrain - Introduction to PC/MS-DOS - 1992
Knowledge Soft - Advanced HTML - 1997		Executrain - Interactive Easyflow - 1990

Certifications

- ITIL certified: July 18, 2012

UNISYS

Resource 137

Technical Writer

Security Clearance

- Information Security Training for Commonwealth of PA DPH - 2012
- Centralized Clearance for Data PowerHouse Facility -2012

Key Skills and Knowledge

- Technical Writing and Documentation Specialist
- SharePoint Site Collection Administrator
- Document Project Management
- Communication and Networking

Office Productivity Tools

- Microsoft Office Suite – Word, Excel, Power Point, Visio, Project Plan, Outlook (expert level)
- HTML / RoboHelp (Web builder)
- MS SharePoint 2010
- MS SharePoint Designer 2010
- MS SharePoint Workspace 2010

Professional Summary

An interactive Senior Technical Writer and Documentation Specialist with a highly skilled background in the technical writing field.

- Create, analyze and manage supporting documentation for all levels within the business and technical environment.
- Skilled at extracting business and technical information, analyzing and manipulating application software, and writing documentation for business processes, functional requirements, technical specifications, procedures, policies, work instructions, user guides, and online help documentation.
- Manage large quantities of many types of documentation including SharePoint administration and Web portal document publishing.
- Act as editor for technical documentation such as SOPs, ROEs, Installation and Configuration, Requirements, Project Management Methodology, Annual Business Report for our division, as well as other supporting documentation for all areas of the technical and business process.

Professional Experience

Unisys, Data PowerHouse Contract, Harrisburg PA, 2009 to Present

Create / Edit Documentation; Work with Subject Matter Experts using MS Office Tools to create and edit Installation, Configuration, Statement of Procedure, Rules of Engagement, Functional Specifications, schematics, presentations, spreadsheets and various process documentation. Develop and Maintain Document Templates; Create and maintain consistent document templates for Installation, Configuration, Statement of Procedure, Rules of Engagement, Functional Specifications, schematics, presentations, spreadsheets reports and process documentation.

- Document Review and Tracking Plan; Track priority documents throughout their life cycle. Ensure document versions are updated and maintained. Send notifications for document review and approvals. Store documents in SharePoint document repository.
- SharePoint Site Collection Administrator and Developer; Build SharePoint site and maintain structure, Grant security access to site, libraries, folders, and documents, Load documentation to site and work with other divisions for mass migrations, Make changes to the site structure as required. Support SharePoint upgrade activities, Provide troubleshooting for SharePoint issues, Develop libraries, lists and workflows as required
- Update and Maintain Client Web Portal Pages; Update information to the Web portal for our data center division; Maintain links and the associated documents

UNISYS

Resource 137

Technical Writer

Work with higher level team to produce documents to their common standards and provide support for redesign activities

- Create, Distribute and Maintain Management Reports; Produce monthly CTO (Chief Technical Officer) report that summarizes operations metrics for our data center division
- Create Annual Report for the Enterprise Technology Services Office; Produce annual report detailing projects, metrics, and summary of costs
- Create Newsletter; Develop newsletter to reach out to our clients and provide current information about service offerings and support provided by our data center division.
- Manage Open House for the Enterprise Data Center; Produce agenda and track activities; Create and edit documentation: Handouts, posters, signage, etc; Order food, send invitations, track attendees, plan space set up and provide support as required
- Incident and Problem Management Support; Provide support in creating and maintaining incident and problem management documentation to the most current standards; Create *After Action Report (AAR)* template; Fill out report with preliminary information; Meet with Subject Matter Subjects to complete report; Track incidents on a summary spreadsheet; Maintain all of the information in SharePoint
- Post Outage and Maintenance Notifications in Internal Database; Review production maintenance and outage notifications and post the pertinent notifications into the database for reporting purposes
- Update Division Organization Chart, Team Member, Emergency Contact Information and On-Call Calendar; Update organization chart for our data center division; Update staff, contact, and team information as required; Update Emergency Contact List; Update Team On Call Calendar
- Track and Update Status of Solution Proposals; Assist in developing proposal template; Track solution proposals and load all documents into SharePoint; Provide editing when required
- Data Analysis; analyze content and ensure that all relevant data is included. If not send requests for updates to the responsible team members and track the completion of those updates;
- Data Analysis; provide field descriptions and data mapping outline for all fields preparing for a move to another implementation tool; Provide Network Availability figures for fiscal year against overall versus individual agency figures;Create a data flow that depicts the task efforts of all team members and how long it takes to complete each technical task, working with each team member to gather the information

UNISYS

Resource 137

Technical Writer

Other Employment History

- ARCUS – July 2007 to May 2009
- Computer Task Group (Consultant to IBM) - Feb 1999 to July 2007
- GPU Nuclear (Three Mile Island) – Mar 1978 to Feb 1999

Education

- Annville Cleona High School
- Harrisburg Area Community College – Business Management (Associate Level)
- Columbia Southern University – Business Management

Professional Certification

- ITIL Foundation Certificate
- Dale Carnegie Management Development Certificate
- Team and Leadership Certification

This page intentionally left blank.

6.0 Training

6. TRAINING 6-3

TRAINING DESCRIPTIONS 6-9

This page intentionally left blank.

6. Training

RFP	*Requirement*
II-6	*Training. If appropriate, indicate recommended training of Commonwealth personnel. Include the Commonwealth personnel to be trained, the number to be trained, duration of the program, place of training, curricula, training materials to be used, number and frequency of sessions, and number and level of instructors.*

Unisys is committed to a high-quality training program customized to meet the needs of Commonwealth staff. We believe strongly it is an investment in your most important resource, Human Capital, and provides a strong foundation to meet the high expectations outlined in the RFP.

This section includes a foldout that clearly describes the training to be offered by Unisys, including the Commonwealth personnel to be trained, the number to be trained, duration of the program, place of training, curricula, training materials to be used, number and frequency of sessions, and number and level of instructors.

Our objectives for training are centered on People, Process, and Technology.

People: Develop the necessary staff skills to transform to the new ITIL-based operating model.

Process: Teach the new processes and procedures necessary to correctly implement the contract provisions.

Technology: Provide an understanding of the technology that will be used for the service catalogue, reporting, and other features of our proposal.

Our training strategy is to build staff capability so the Commonwealth can become self-sufficient as quickly as possible. We also recognize there is an ongoing need for refresher training for new employees as well as training for new processes and technologies, especially during the periods of continual improvement.

Unisys Training Experience: Unisys has a rich history of providing training for many decades, including significant experience with educating staff from many state governments and federal agencies. Therefore, we draw on this experience and the expertise of those whose entire mission is education and training. The roles of each of our training team partners are defined below.

Harrisburg University of Science and Technology (HU): Unisys has teamed with HU to bring tremendous value to the Commonwealth. As an educational institution that emphasizes adult learners and collaboration with business as part of its core mission, HU not only brings specific expertise in education and lifelong learning for professionals in science and technology fields, it also has a refreshing ability to be

nimble, entrepreneurial, and innovative in how it works with its partners. Unisys will leverage HU's expertise in principles and techniques for adult learning and the effective use of learning and emerging technologies, its modern educational facilities, and convenient location in downtown Harrisburg

""Harrisburg University is extremely proud to work with the Unisys team on this transformative initiative. Unisys has brought thought-leadership to our university and we look forward to working with them and our state government leaders to make this initiative successful."

—Eric D. Darr, Ph.D.
President of Harrisburg University of Science and Technology

The overall training approach will be managed by a Harrisburg University Training Specialist under the direction of the Unisys Program Management Office (TPMO) staff. Also, the training specialist will gather the evaluations from each class and evaluate them for quality improvement opportunities. The Unisys Team will use HU's course registration, tracking processes, and tools as well as take advantage of HU's expertise to develop and deliver select courseware. Wherever possible, the Unisys Team will use the best commercially available courseware and delivery methods. The Training Specialist will be the primary liaison between our local team and HU.

HU will coordinate training registration for all programs taught by HU or on behalf of HU. This includes providing for online registration, sending confirmation details to participants, providing customer service for training participants, and maintaining a roster of registered and completed participants. Several of our training events will be held at the HU campus, providing an environment that is conveniently accessed and conducive to learning for Commonwealth attendees. Selected training events will be recorded and made available on the Unisys Knowledge Management Portal for future Commonwealth access.

Government Technology Institute: Hosted by HU, the Government Technology Institute (GTI) provides executive training for IT leaders in state government and a venue for public sector innovation. Many Commonwealth employees are becoming increasingly familiar with HU through positive firsthand experience in the educational programs, as participants in professional development, graduate programs, or educational programs of the GTI. GTI co-directors and HU staff continue to work closely with Commonwealth government leaders to develop programs in response to needs presented by executives in CoPA agencies and the Office of Administration. These connections have led to successful new programs such as the Certified Government CIO (CGCIO) program, the Government IT Manager (GITM) certificate program, and Innovate PA, a developing series of seminars and workshops on applying the process of innovation to state government. About 50 senior IT leaders from state government participate in the CGCIO and GITM programs. Many more attend the innovation workshops.

The perspectives and experience of the GTI co-directors, gained from successful careers in state and federal government and now as educators, are an advantage for HU in understanding the needs of the CoPA IT workforce. Under the leadership of Charles Gerhards and Barbara Shelton, the GTI has produced programs that are becoming well known among the Commonwealth IT community and highly regarded as high-quality educational experiences. In fact, members of the Governor's administration are frequent guest presenters in the programs.

We also see value supporting other HU programs that can directly or indirectly build skills such as project management. One such program is the Project Manager Partners Forum known as PM Partners. HU provides Unisys and the Commonwealth with a no-cost partnership between the local Project Management Institute chapter, the Office of Administration, Office of Information Technology, and HU. This Project Manager Development Forum occurs at HU each quarter and allows Commonwealth project managers to work collaboratively with peers, HU faculty, and project management professionals in the PMI chapter to discuss and develop advanced project management skills. This too has generated many positive experiences among Commonwealth IT professionals at all levels of state government.

The training program described in this section will be broken out with a focus solely on **Commonwealth Training.** The Commonwealth Training program was designed with the following goals:

- Deliver detailed information on key deliverables to confirm the Commonwealth's understanding of our technology, plans, and procedures to best take advantage of services provided on the engagement
- Verify that Commonwealth stakeholders at all levels have a thorough understanding of the engagement's change procedures and fee structures
- Provide the Commonwealth with demonstrations of tools and portals that contain information germane to the operation of its business
- Facilitate a common understanding of the flow of ITIL process requests and approvals, and the leveraging of our ITSM tools to promote process discipline and compliance
- Provide transparency of Data Center Services procedures and pricing of services and educate Commonwealth stakeholders on how to access the information.

Table 6-1 provides a high-level view of the training topics for Commonwealth personnel that are detailed in the foldout.

Table 6-1. Training Topics for Commonwealth Personnel

Commonwealth Training Topic	High-level Curriculum Content
EDC Assessment Review	Assessment results and recommendations
Technology and Architecture Overview	Review of all aspects of data center and technology architecture overview and roadmap
Co-location Service Offering	Review of service offering and how to leverage
Commonwealth Computing Procedures Manual Training	Overview of the manual's structure; how to access and use the manual
Security Management Plan	Service offering overview
Security Risk and Vulnerability Assessment Report	Process overview, assessment results, roadmap, and remediation plan
Contract Management Training	Review of contract terms and the change control process
Financial Management Training	Fee structure, consumptive model, and invoicing process
Data Center Services Reporting	Review of reports available and portal usage procedures
Knowledge Management Portal	Review of portal usage and content available
Security Training	Security tools, functions, reports, and escalation process
Performance Monitoring Training	Review of performance management tools, reporting, and support
Continuous Service Improvement & Innovation Program (CSIIP)	Program overview, CoPA and Unisys roles, governance, and critical success factors
Disaster Recovery Planning Process and Tools	Overview of Disaster Recovery scope, declaration, plan development, and testing
Service Catalog Training	Review of services available, request process, and tool usage
Transition Executive Briefing	Program overview, key program activities, roles, responsibilities, schedule, and deliverable acceptance process
IT Service Management Workshops	In-depth review of change and release, incident, problem, asset and configuration database management; capacity; and service level and availability management process training

Experience Delivering Training

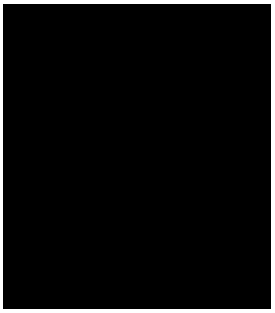
The Unisys philosophy is that effective training and knowledge transfer is key to a successful engagement of this magnitude. The Unisys Team, through Unisys University and our association with Harrisburg University, possesses extensive experience in delivering various training programs to many Commonwealth of Pennsylvania agencies. Over our 50-year relationship with the Commonwealth, we have provided a variety of training to support a number of agencies and engagements, including:

- Pennsylvania State Police—Computerized Criminal History Records Information system
- Pennsylvania State Police—Commonwealth Law Enforcement
- Pennsylvania Department of Revenue—Enterprise Communications System

- Pennsylvania Public Utility Commission—InfoMap System
- Pennsylvania Department of Transportation—ITSM Lessons Learned with department leaders
- Office of Administration, Office for Information Technology—Executive Briefings on Service Management, IT Security, and Cloud/Self-provisioning technologies.

Unisys will provide a formal and structured training plan as outlined in this section. Note that we are proposing some training through our approach to continuous improvement, as outlined in Section 4 of this proposal. As part of our Continual Service Improvement and Innovation Program (CSIIP), Unisys will conduct regular Innovation Workshops for Commonwealth staff focused on innovative technology evaluation, opportunity identification, categorization, and prioritization followed by the development of high-level business cases and implementation roadmaps for the most promising technologies and opportunities for improvement of Commonwealth operations.

"When I think of training, I believe that effective training uses active learning techniques, providing as much hands-on as possible with the most relevant examples to the learner. At Unisys we incorporate problem-based learning and we focus on real tasks during training that may involve multiple software applications or technologies. We time the training appropriately so that learners can put their new knowledge to use immediately. We develop training to support multiple learning styles (visual, auditory, and kinesthetic learners) and respect the different means of learning, from in-person structured group sessions to online quick tips. We set goals for the learners prior to training and then measure progress during and after training. Having worked in environments where technology and systems are evolving, I know the importance of training to keep staff current. Our plan for this contract will get it done."



[redacted]
Engagement Executive
Unisys

This page intentionally left blank.

Training Descriptions

Training Requirement	Category	Personnel to be Trained	# to be Trained	Program Duration	Training Location	Curricula	Training Materials	# & Frequency of Sessions	# & Level of Instructors
Data Center Computing Services Offering, Architecture & Transition									
Data Center Computing Service Catalog	Process	OA and Agency Representatives	100	3 hours	Harrisburg University	Data Center Computing Services Available, Service Request Process, How to use Service Catalog, Demonstration	Presentation Handout	1 Initial	1 Senior
Limited-Use Colocation Services	Deliverable	OA and Agency Representatives	100	2 hours	Harrisburg University	Service Offering Overview: How to use	Presentation Handout	1 Initial	1 Senior
Multi-Data Center Technology and Architecture Overview (2+ Architecture) (Sch. K D-01) - Network and Security Architecture Overview - Data Center Architecture and Technology - Technology Architecture and Refresh Approach (Sch. K D-03) - IT Service Continuity Architecture and Plan Overview (Sch. K D-04)	Deliverable	OA and Agency Representatives	100	4 hours	Harrisburg University	Overview of 2+ Datacenter, network, security architecture and technology implementation roadmap Technology Overview Technology Roadmap	Presentation Handout	1 Initial	1 Senior
Quarterly Multi-Data Center Technology and Architecture Overview (2+ Architecture)	Deliverable	OA and Agency Representatives	100	2 hours	Harrisburg University	Changes to 2+ Datacenter, network, security architecture and technology implementation roadmap, Technology Overview Technology Roadmap	Presentation Handout	4/year	1 Senior
EDC Assessment Overview	Deliverable	OA CIO and CTO	2	3 hours	CoPA	EDC Assessment Results: Recommendations for Security, HVAC, and Power Upgrades required, Physical Access requirements, Monitoring and Operating the installed infrastructure	Presentation Handout	1 Initial	1 Senior
Transition Program Executive Workshop: What to Expect During Transition (Sch. K D-05)	Transition	OA and Agency Representatives	100	3 hours	Harrisburg University	Transition Program overview: Key Program Activities, Roles and Responsibilities, Schedule, Deliverable Acceptance Process	Presentation Handout	1 Initial	1 Senior
Data Center Computing Services Processes and Tools									
Commonwealth Computing Procedures Manual Training (Sch. K D-02)	Process	OA and Agency Representatives	100	2 hours	Harrisburg University	Overview of CCPM: How to Access Detail and Use	Presentation Handout	1 Initial	1 Senior
Security Management Plan Overview (Sch. K D-07)	Deliverable	OA and Agency CISO	25	2 hours	CoPA	Service Offering Overview	Presentation Handout	1 Initial	1 Senior
Security Risk and Vulnerability Assessment Report (Sch. K D-09)	Deliverable	OA and Agency CISO	25	2 hours	CoPA	Assessment Process Overview: Risk and Vulnerability Results, Roadmap and Remediation Plan	Presentation Handout	1 Initial	1 Senior

Training Requirement	Category	Personnel to be Trained	# to be Trained	Program Duration	Training Location	Curricula	Training Materials	# & Frequency of Sessions	# & Level of Instructors
Security Training (Sch. F 3.2.4.6)	Tools	OA and Agency Representatives	100	2 hours	Web Based	Security Tools Used, Security Functions, Reports, Escalation Process	Presentation Handout	1 Initial	1 Senior
Data Center Services Reporting Overview	Tools	OA and Agency Representatives	100	2 hours	Web Based	Portal Usage and Reports Available	Presentation Handout	1 Initial	1 Senior
Knowledge Management Portal (Sch. K D-02.20)	Tools	OA and Agency Representatives	100	2 hours	Web Based	Portal Usage and Content Available	Presentation Handout	1 Initial	1 Senior
Performance Monitoring Training (Sch. F 3.2.2.6)	Tools	OA and Agency Representatives	100	2 hours	Web Based	Performance Management Tools, Reporting, Usage Support	Presentation Handout	1 Initial	1 Senior
Continuous Service Improvement & Innovation Plan	Quality	OA and Agency Representatives	100	2 hours	Web Based	Program Overview: CoPA and Unisys Roles, Critical Success Factors, Governance	Presentation Handout	1 Initial	1 Senior
Disaster Recovery Planning Process and Tool Training	Disaster Recovery	OA and Agency DR Representatives	50	3 hours	Web Based	Disaster Recovery Scope, Declaration, DR Plan, Development/Review, DR Testing	Presentation Handout	1 Initial	1 Senior
Contract Management Training	Contract	OA and Agency Contract Staff	25	2 hours	CoPA	Contract Terms: Change Control Process, Vendor Contract Staff Responsibilities	Presentation Handout	1 Initial	1 Senior
Financial Management Training	Contract	OA and Agency Contract Staff	25	2 hours	CoPA	Fee Structure, Consumptive Model Process, Invoicing Process, Remedy System Usage	Presentation Handout	1 Initial	1 Senior
IT Service Management Workshops									
Change and Release Management Training	Process	OA and Agency Representatives	50	3 hours	Harrisburg University	Change Management Process: Change types, Approvals, Escalations, Enterprise Change Windows	Presentation Handout	1 Initial	1 Senior
Incident Management Training	Process	OA and Agency Representatives	50	3 hours	Harrisburg University	Incident Management Process: Communications, Incident Reports, Process Metrics, Roles & Responsibilities	Presentation Handout	1 Initial	1 Senior
Problem Management Training	Process	OA and Agency Representatives	50	3 hours	Harrisburg University	Problem Management Process: Problem Reports, Process Metrics, Roles & Responsibilities	Presentation Handout	1 Initial	1 Senior
Asset Management and CMDB Training	Process	OA and Agency Representatives	50	3 hours	Harrisburg University	Asset Management Process: Process Metrics, Reports, Roles & Responsibilities, CI Reconciliation	Presentation Handout	1 Initial	1 Senior
Capacity Management Training	Process	OA and Agency Representatives	50	3 hours	Harrisburg University	Capacity Management Process: Process Metrics, Reports, Roles & Responsibilities	Presentation Handout	1 Initial	1 Senior
Service Level and Availability Management Training	Process	OA and Agency Representatives	50	3 hours	Harrisburg University	Service Level/Availability Management Process: Service Level Reports, Process Metrics, Roles & Responsibilities	Presentation Handout	1 Initial	1 Senior

--Redacted—

7.0 Financial Capability

(Redacted pursuant to 65 P.S. § 67.708(b)(26), which exempts the financial information of a bidder or offeror requested in an invitation for bid or request for proposals to demonstrate the bidder's or offeror's economic capability)

8.0 Objections and Additions to Contract Terms and Conditions

8. OBJECTIONS AND ADDITIONS TO CONTRACT TERMS AND CONDITIONS 8-3

This page intentionally left blank.

8. Objections and Additions to Contract Terms and Conditions

RFP	*Requirement*
II-8	*Objections and Additions to Contract Terms and Conditions. The Offeror will identify which, if any, of the terms and conditions (contained in Appendix A) it would like to negotiate and what additional terms and conditions the Offeror would like to add to the standard contract terms and conditions. The Offeror's failure to make a submission under this paragraph will result in its waiving its right to do so later, but the Issuing Office may consider late objections and requests for additions if to do so, in the Issuing Office's sole discretion, would be in the best interest of the Commonwealth. The Issuing Office may, in its sole discretion, accept or reject any requested changes to the standard contract terms and conditions. The Offeror shall not request changes to the other provisions of the RFP, nor shall the Offeror request to completely substitute its own terms and conditions for Appendix A. All terms and conditions must appear in one integrated contract. The Issuing Office will not accept references to the Offeror's, or any other, online guides or online terms and conditions contained in any proposal.* *Regardless of any objections set out in its proposal, the Offeror must submit its proposal, including the cost proposal, on the basis of the terms and conditions set out in Appendix A.* *The Issuing Office will reject any proposal that is conditioned on the negotiation of the terms and conditions set out in Appendix A or to other provisions of the RFP as specifically identified above.*

As requested by the Request for Proposal, there are terms and conditions in the RFP (Appendix A and related Exhibits and Schedules) that Unisys would like to negotiate with the Commonwealth, and there are additional terms and conditions that Unisys would like to add to the contract. As per the RFP instructions, these areas of concern are included within Section 8 of our Response. Unisys' approach was to use the "comments" functionality within Word which we believe will help assist in the Commonwealth's review process. These comments should not be considered as a replacement or including the Unisys standard contractual language as this is not allowed within the Request for Proposal guidelines. Unisys does refer to the existing contractual language in a number of comments with the intent that this will expedite the negotiation process as these areas have already been mutually agreed by both parties in the recent past.

Also, please note that within Appendix G, there are areas that should be considered as Trade Secret and / or Confidential Proprietary Information. As a result, a redacted version of the Request for Proposal response has been included.

Finally, Unisys has indicated in our proposal submission that we are not participating in the COSTARS program for this Commonwealth procurement. Unisys would be interested in discussing and possibly revisiting this decision later during the procurement process.

This page intentionally left blank.

CONTRACT TERMS AND CONDITIONS

Data Center Computing Services
RFP #6100022698

TABLE OF CONTENTS

1. CONTRACT TERM 1
2. PURCHASE ORDERS 2
3. IDENTIFICATION NUMBER 3
4. ORDER OF PRECEDENCE, DEFINITIONS AND CONSTRUCTION 3
5. CONTRACT INTEGRATION 4
6. SERVICES 5
7. EQUIPMENT 8
8. COMMONWEALTH THIRD PARTY SOFTWARE 9
9. DATA SECURITY 10
10. CONDUCT OF SERVICES 12
11. QUALITY ASSURANCE AND INTERNAL CONTROLS 13
12. SERVICE LOCATIONS 14
13. CONDITIONS OF CONTRACTOR'S OCCUPANCY OF COMMONWEALTH-PROVIDED REAL PROPERTY 17
14. TRANSITION 19
15. DISASTER RECOVERY AND BUSINESS CONTINUITY 23
16. PRIME CONTRACTOR RESPONSIBILITIES 25
17. KEY POSITIONS/CONTRACTOR PERSONNEL 25
18. THIRD PARTY SERVICES 27
19. COMPENSATION 28
20. FEES 28
21. PAYMENT SCHEDULE AND INVOICES 29
22. INSPECTION AND ACCEPTANCE 30
23. SERVICE LEVELS 31
24. LIQUIDATED DAMAGES 32
25. CONTINUOUS IMPROVEMENT AND BENCHMARKING 33
26. GOVERNANCE 36
27. CHANGE CONTROL 36
28. NOTICE OF DELAYS 38
29. NOTICE 38
30. DEFAULT 38
31. STEP-IN RIGHTS 41
32. TERMINATION 41
33. TERMINATION ASSISTANCE 45
34. CONTRACT CONTROVERSIES 52

35. COMMONWEALTH HELD HARMLESS 53
36. LIMITATION OF LIABILITY 53
37. CONFIDENTIALITY 55
38. SENSITIVE INFORMATION 58
39. PATENT, COPYRIGHT, TRADEMARK, AND TRADE SECRET PROTECTION 59
40. PROPRIETARY RIGHTS 62
41. PUBLICATION RIGHTS AND/OR COPYRIGHTS 65
42. REPORTS AND DATA 66
43. SECURITY AND PROTECTION OF INFORMATION 67
44. BACKGROUND CHECKS 68
45. INSURANCE 68
46. WARRANTIES 70
47. CONTRACTOR RESPONSIBILITY PROGRAM 72
48. OFFSET PROVISION FOR COMMONWEALTH CONTRACTS 73
49. TAXES-FEDERAL, STATE, AND LOCAL 73
50. POLICIES AND PROCEDURES 74
51. AUDIT OBLIGATIONS 74
52. VIRUS AND MALICIOUS CODE 77
53. THE AMERICANS WITH DISABILITIES ACT 78
54. NONDISCRIMINATION CLAUSE/SEXUAL HARASSMENT CLAUSE 78
55. CONTRACTOR INTEGRITY PROVISIONS 79
56. RIGHT-TO-KNOW LAW 85
57. ENVIRONMENTAL PROTECTION 87
58. ASSIGNABILITY 87
59. INDEPENDENT CAPACITY OF CONTRACTOR 88
60. THIRD PARTY BENEFICIARIES 88
61. CERTIFICATION REGARDING SUSPENSION 88
62. SUSPENSION OF SUBCONTRACTORS 88
63. ASSIGNMENT OF RIGHTS UNDER THE ANTITRUST LAWS 89
64. SIGNIFICANT EVENTS 89
65. FORCE MAJEURE 89
66. CONFLICT OF INTEREST 90
67. OFFICIALS NOT TO BENEFIT 90
68. CONSENTS, APPROVALS, NOTICES AND REQUESTS 90
69. REQUIRED CONSENTS 90
71. EXAMINATION OF RECORDS 92
72. SURVIVAL 92

73. SEVERABILITY 92
74. WAIVER 92
75. PERIOD OF PERFORMANCE 92
76. SPECIAL REQUIREMENTS 92
77. GOVERNING LAW 93
78. COMPLIANCE WITH LAWS 93
79. SMALL DIVERSE BUSINESS COMMITMENT 93
80. ACKNOWLEDGEMENT 93
81. COVENANT OF FURTHER ASSURANCES 94
82. COVENANT OF GOOD FAITH 94
83. AMENDMENTS 94
84. ENTIRE CONTRACT 94
APPENDIX A - BUSINESS ASSOCIATE APPENDIX LANGUAGE 1

TABLE OF SCHEDULES

SCHEDULE A - DEFINED TERMS

SCHEDULE B - GOVERNANCE

SCHEDULE C – SERVICES CATALOG

SCHEDULE D - TRANSITION MILESTONES

SCHEDULE E – DATACENTER LOCATIONS

SCHEDULE F – COPA DATACENTER STATEMENT OF WORK

SCHEDULE G - STAFFING PLAN AND KEY POSITIONS

SCHEDULE H - COMMONWEALTH COMPUTING PROCEDURES MANUAL

SCHEDULE I - OFFEROR PRICING FORMS

SCHEDULE J.1 - SERVICE LEVEL MANAGEMENT

SCHEDULE J.2 - DATACENTER SERVICE LEVEL MATRIX

SCHEDULE J.3 - DATACENTER SLA DEFINITIONS

SCHEDULE K - KEY PROGRAM DELIVERABLES

SCHEDULE L – APPROVED SUBCONTRACTORS

SCHEDULE M – DETAILED TRANSITION PLAN

TERMS AND CONDITIONS

1. CONTRACT TERM

a) The term of the Contract shall commence on the Effective Date and shall end in seven (7) years ("the Expiration Date"), subject to the other provisions of the Contract. The Effective Date shall be: a) the date the Contract has been fully executed by the Contractor and by the Commonwealth and all approvals required by Commonwealth contracting procedures have been obtained or b) the date referenced in the Contract, whichever is later. The Contract shall not be a legally binding contract until after the fully-executed Contract has been sent to the Contractor.

b) The Commonwealth may, in its sole discretion, renew the Contract for three (3) one (1) year periods, or any combination thereof, on the terms and conditions in force at the date of the renewal and utilizing pricing to be negotiated but consistent with and no less favorable than the pricing in force at the date of the renewal. Further, the Commonwealth reserves the right to extend this Contract or any part of this Contract up to three (3) months, or as necessary to prevent a lapse in Contract coverage.

~~b)~~c) The Commonwealth reserves the right to execute the Contract, Purchase Orders or any follow-up Contract documents in ink or electronically. The Contractor understands and agrees that the receipt of an electronically-printed Contract with the printed name of the Commonwealth purchasing agent constitutes a valid, binding contract with the Commonwealth. The printed name of the purchasing agent on the Contract represents the signature of that individual who is authorized to bind the Commonwealth to the obligations contained in the Contract. The printed name also indicates that all approvals required by Commonwealth contracting procedures have been obtained.

~~c)~~d) The Contractor shall not start performance, and the Commonwealth shall not be liable to pay the Contractor for any supply furnished or work performed or expenses incurred, until all of the following have occurred:

(1) The Effective Date has arrived;

(2) The Contractor has received a copy of the fully executed Contract (or written notice from the Commonwealth that the Contract has been fully executed); and

(3) The Contractor has received a Purchase Order or other written notice to proceed signed by the Commonwealth Contracting Officer.

Comment [A1]: Contractor proposes first year pricing can remain the same unless partial contract, then additional discussion will be required for solution, T&Cs and pricing Years 2 and 3 require additional discussion regarding capital assets and increase costs related to cost of living changes

No Commonwealth employee has the authority to verbally direct the commencement of any work or delivery of any supply under this Contract prior to the Effective Date.

2. PURCHASE ORDERS

a) The Commonwealth may issue Purchase Orders against the Contract. These orders constitute the Contractor's authority to make delivery. All Purchase Orders received by the Contractor up to and including the expiration date of the Contract are acceptable and must be performed in accordance with the Contract. Contractors are not permitted to accept Purchase Orders which require performance in excess of those performance time periods specified in the Contract. Each Purchase Order will be deemed to incorporate the terms and conditions set forth in the Contract.

b) Purchase Orders will not include an ink signature by the Commonwealth. The electronically-printed name of the purchaser represents the signature of the individual who has the authority, on behalf of the Commonwealth, to authorize the Contractor to proceed.

c) Purchase Orders may be issued electronically or through facsimile equipment. The electronic transmission of a purchase order shall require acknowledgement of receipt of the transmission by the Contractor.

d) Contractor's acknowledgment of receipt of the electronic or facsimile transmission of the Purchase Order shall constitute receipt of an order.

e) Purchase Orders received by the Contractor after 4:00 p m. will be considered received the following business day.

f) The Commonwealth and the Contractor specifically agree as follows:

(1) No handwritten signature shall be required in order for the Contract or Purchase Order to be legally enforceable.

(2) Upon receipt of a Purchase Order, the Contractor shall promptly and properly transmit an acknowledgement in return. Any order which is issued electronically shall not give rise to any obligation to deliver on the part of the Contractor, or any obligation to receive and pay for delivered products on the part of the Commonwealth, unless and until the Commonwealth agency transmitting the order has properly received an acknowledgement.

(3) The parties agree that no writing shall be required in order to make the order legally binding. The parties hereby agree not to contest the validity or enforceability of the Contract or a genuine Purchase

Order or acknowledgement that have been issued electronically under the provisions of a statute of frauds or any other applicable law relating to whether certain agreements shall be in writing and signed by the party bound thereby. The Contract and any genuine Purchase Order or acknowledgement issued electronically, if introduced as evidence on paper in any judicial, arbitration, mediation, or administrative proceedings, will be admissible as between the parties to the same extent and under the same conditions as other business records originated and maintained in documentary form. Neither party shall contest the admissibility of copies of the Contract or any genuine Purchase Order or acknowledgements under either the business records exception to the hearsay rule or the best evidence rule on the basis that the Contract or Purchase Order or acknowledgement were not in writing or signed by the parties. A Purchase Order or acknowledgment shall be deemed to be genuine for all purposes if it is transmitted to the location designated for such documents.

(4) Each party will immediately take steps to verify any document that appears to be obviously garbled in transmission or improperly formatted to include re-transmission of any such document if necessary.

g) Purchase Orders under five thousand dollars ($5,000) in total amount may also be made using a Commonwealth Procurement VISA Card in person or by telephone. When an order is placed by telephone, the Commonwealth agency shall provide the agency name, employee name, credit card number, and expiration date of the card. The Contractor agrees to accept payment through the use of the Commonwealth Procurement VISA card.

Comment [A2]: Contractor believes this will not be applicable due to dollar amount limit If there are purchases at this level whereby Commonwealth wishes to use VISA card, then Contractor and Commonwealth will agree at that time if this payment process will be acceptable

3. IDENTIFICATION NUMBER

The Contractor must have a SAP Vendor Number.

4. ORDER OF PRECEDENCE, DEFINITIONS AND CONSTRUCTION

a) If any conflicts or discrepancies should arise in the terms and conditions of this Contract, or the interpretation thereof, the order of precedence shall be:

(1) This Contract (first, the Contract, including the terms and conditions, second the Schedules and Appendices); then

(2) The Contractor's Proposal (including the clarifications and the Best and Final Offer), as accepted by the Commonwealth; and then

(3) The RFP.

Comment [A3]: Contractor believes this Contract should stand alone and therefore will not require reference to the Proposal nor RFP

b) Except as otherwise expressly provided in the Contract, all capitalized terms used in the Contract shall have the meanings set forth in *Schedule A* (Defined Terms).

c) Interpretation:

(1) The terms defined in the Contract include the plural as well as the singular and the derivatives of such terms. Unless otherwise expressly stated, the words "herein," "hereof," and "hereunder" and other words of similar import refer to the Contract as a whole and not to any particular Paragraph, Section, subsection or other subdivision. The words "include" and "including" shall not be construed as terms of limitation.

(2) Headings preceding the text of Paragraphs or Sections, and headings to Schedules and Appendices, the table of contents and the table of Schedules and Appendices included in or attached to the Contract are used for convenience only and are not to be considered in construing or interpreting the Contract.

(3) References to any law refer to such law in changed or supplemented form, or to a newly adopted law replacing a previous law.

(4) Except as may be expressly set forth herein, all references to time herein refer to Eastern Standard Time or Eastern Daylight Time, as applicable.

d) The Contract includes each Schedule, Exhibit and Appendix referenced herein, all of which are incorporated into the Contract by this reference

Comment [A4]: Contractor proposes that definitions in Schedule A will need to be revised and updated as appropriate once the parties have discussed and revised the provisions of this Appendix A

5. CONTRACT INTEGRATION

a) This Contract, including the Contract signature pages, together with the Contractor's Proposal, the Contractor's clarifications and the Contractor's Best and Final Offer, and the RFP and addenda thereto that are incorporated herein by reference, constitutes the final, complete, and exclusive Contract between the parties containing all the terms and conditions agreed to by the parties.

b) All representations, understandings, promises, and agreements pertaining to the subject matter of this Contract made prior to or at the time this Contract is executed are superseded by this Contract.

c) There are no conditions precedent to the performance of this Contract except as expressly set forth herein.

Comment [A5]: Similar to comment A3 - The RFP and Proposals should be superseded by this Contract We want one integrated document to contain all of the agreements between the Parties The various documents might well conflict with one another See Section 84 which conflicts with this provision

d) No contract terms or conditions are applicable to this Contract except as they are expressly set forth herein.

6. SERVICES

a) The Contractor agrees to provide the Services to the Commonwealth as such services are defined in this Contract, the RFP and the Contractor's Proposal, and in accordance with the terms of this Contract.

b) The Contractor shall provide to Commonwealth the following Services pursuant to the terms of the Contract:

(1) Commencing as of the Effective Date, the Transition Services set forth in *Section 14* (Transition) and *Schedule D* (Transition Milestones);

(2) Commencing as of the Effective Date and continuing until the Expiration Date:

1. The services, function and responsibilities described in the Contract, including the Services set forth in (Services Catalog) and *Schedule F* (Statement of Work);

2. Any incidental services, functions or responsibilities not specifically described in the Contract, but which are inherent or required for the proper performance and delivery of the Services; and

3. The services, functions and responsibilities related to those categories of Services which Contractor is assuming pursuant to the Contract; and

(3) Commencing upon written notice by Commonwealth to Contractor in accordance with *Section 33* (Termination Assistance).

c) The services set forth in (1) through (3) above shall be collectively referenced as the "Services," as they may evolve during the Term of the Contract or be supplemented, enhanced, modified or replaced pursuant to the terms hereof. The Services provided under this Contract are not exclusive to Contractor. The Commonwealth may in-source or re-procure any or all of the Services.

d) The Commonwealth may request a change to the Services through a "*Request for Services*" to increase or decrease the amount of the Services provided under this Contract, according to Commonwealth's demand for the Services. The parties shall use the Change Control Procedures to implement the changes required by the *Request for Services* and revise the Fees as applicable.

Comment [A6]: Contractor agrees as long as it is inherent to the performance of the Services

Comment [A7]: Contractor requests additional discussion on minimum baseline commitment as minimum requirement is not an unusual practice in industry and allows for best competitive pricing Similar concepts of non-exclusivity contained in Sections 18(a) and 76

Comment [A8]: Contractor requests that in-source and re-procure will require a form of termination for convenience fee structure due to investment required by Contractor and additional conversation may be required regarding Fee Structure for the remaining Services

Comment [A9]: Contractor proposes decreasing volume may be acceptable but to a minimum baseline This concept requires more discussion

Comment [A10]: Contractor proposes adding an "Additional Services" provision like Sec 3 02 of existing contract associated to "out of scope" Services

e) Except as may be necessary on an emergency basis to maintain the continuity of the Services or in the event of a declared disaster, Contractor shall not, without Commonwealth's written consent, modify (1) the composition of the Services, (2) the manner in which the Services are to be provided or delivered if such modification would have an adverse effect on the operations of Commonwealth, or (3) the applicable Services Levels.

f) Except as otherwise expressly provided in this Contract, Contractor is responsible for providing, and is financially and operationally responsible for, the Facilities, Personnel, Equipment, Materials, technical knowledge, expertise and other resources necessary to provide the Services (including all upgrades, improvements, replacements and additions to such resources).

g) Contractor acknowledges that Commonwealth encourages Contractor to provide the Services in a shared data processing environment, if such environment will materially reduce Commonwealth's costs under this Contract and can be accomplished within the confidentiality and physical security constraints imposed upon Contractor elsewhere in this Contract. Accordingly, upon the migration of any of Commonwealth's data processing to a Contractor Services Location, Contractor may provide the related Services from such Contractor Services Location in a shared data processing environment if Contractor reasonably believes such environment will materially reduce Commonwealth's costs under this Contract and if such shared environment and Contractor's use thereof to provide the Services otherwise comports with the terms of this Contract. Commonwealth reserves to itself the right of prior approval of any third party proposed by Contractor to share such data processing environment, such approval not to be unreasonably withheld. Contractor acknowledges that Commonwealth will be entitled to withhold its approval of any such third party if, among other things, there is no or insufficient economic benefit to Commonwealth from the proposed sharing arrangement or if any federal or state confidentiality issues are not resolved to the satisfaction of the applicable federal or state governmental entity.

h) **Technical Architecture and Product Standards**. As part of the Services, Contractor shall suggest to Commonwealth information management technical architecture and product standards to be in effect at the Contractor Services Locations during the Term and the parties shall work together in good faith to develop information management technical architecture and product standards that are mutually acceptable to the parties and consistent with the Services Levels then in effect.

i) **Remote Access Capabilities**. As part of the Services, Contractor shall provide remote access capabilities for use by authorized personnel of the Commonwealth. All such remote access capabilities shall meet or exceed all Commonwealth technology and security standards as set forth in *Section 12* (Service Locations).

j) **Contractor Licenses and Permits**. As part of the Services, Contractor is responsible for obtaining, and has financial responsibility for, all necessary licenses, consents, approvals, permits and authorizations that are legally required to be obtained in order for Contractor to perform the Services. Commonwealth shall reasonably cooperate with and assist Contractor in obtaining any such licenses, consents, approvals, permits and authorizations. Notwithstanding the foregoing, Commonwealth will retain responsibility for obtaining, and the financial responsibility for, all necessary licenses, consents, approvals, permits and authorizations necessary to enable Contractor and its subcontractors to use the Commonwealth Software to the extent necessary for Contractor's performance of the Services and with Contractor's cooperation as further described in *Section 8* (Commonwealth Third Party Software), and Contractor will cooperate, and will cause the Contractor agents to cooperate, in good faith and at no additional cost to Commonwealth, in obtaining such licenses, consents, approvals, permits and authorizations.

k) **Changes in Law and Regulations**. Each party shall identify, and notify the other party of, any changes in applicable statutes, regulations, or policies that may directly or indirectly relate to Contractor's performance of the Services. Contractor and Commonwealth shall work together to identify any impact of such changes upon Commonwealth's use, or Contractor's delivery, of the Services. Contractor shall be responsible for any fines and penalties arising from its noncompliance with any such identified statutes, regulations, or policies relating to the business of providing the Services and shall not be responsible for any fines and penalties assessed against Commonwealth by federal governmental entities from Commonwealth's noncompliance with any federal legislative enactments or federal regulatory requirements relating to Commonwealth's operations that does not result from Contractor's actions or inactions under this Contract. As part of the Services, Contractor shall, if possible, perform the Services regardless of changes in legislative enactments or regulatory requirements. If such changes prevent Contractor from performing any of its obligations under this Contract or increase Contractor's costs in connection therewith, Contractor shall provide written notice thereof to Commonwealth within five (5) days of learning of the change and, if possible, will develop and implement a suitable workaround until such time as Contractor can fully perform its obligations under this Contract without such workaround. Contractor shall bear any costs relating to any legislative enactments and regulatory requirements relating to its business, and Commonwealth shall bear all reasonable out of pocket expenses, excluding attorneys fees, incurred by Contractor relating to legislative enactments and regulatory requirements that require modification of the Services by Contractor. If the parties are unable to agree as to the allocation of such costs, the changes and costs that are the subject of this *Section 6(k)* shall be subject to the Change Control Procedures.

Comment [A11]: Contractor proposes this section should be limited to policies which have the force of law like statutes and regulations

l) **Access**. Upon Contractor's receipt of appropriate, advance notice (which except in an emergency situation shall not be less than three (3) business days) and subject to Contractor's reasonable security requirements, authorized representatives of Commonwealth, Commonwealth agents and agents of the Federal government shall be permitted access to any Contractor Services Location.

7. Equipment

Contractor shall provide the Services using the Equipment. Commonwealth shall provide Contractor with the required access and authorization to use the Commonwealth Machines.

Comment [A12]: Contractor proposes definition of Equipment will need to be discussed as the current proposed definition is too broad (for example, personal computers, cell phone, etc)

Comment [A13]: Contractor proposes that this section seems to be inconsistent with the direction of the type of Managed Services contract that is required within the RFP It is proposed to review this section to validate based on the Services requested

a) **Replacement and Upgrades of the Equipment**.

(1) Contractor shall maintain, replace and upgrade the Contractor Machines at its sole cost and expense. At its sole cost and expense, Contractor shall maintain the Commonwealth Machines and shall replace each Commonwealth Machine at its respective end of life or as otherwise required to provide the Services. All replacements and upgrades shall be addressed through the Change Control Procedure. Commonwealth agencies will work closely with the Office of Administration and Contractor to accurately plan for any additional just-in-time technology refresh and upgrade deployment as may be necessary for Contractor to perform the Services in accordance with the Services Levels while meeting new or increased demands of the agencies. Contractor acknowledges that all such replacements and upgrades shall consist of the then current technology; that is, Contractor will not extend use of then obsolete technology by increasing its capacity with additional hardware capacity if newer, proven technology is then available. In the case of all such replacement or upgrades, Contractor shall provide advance notice via the Change Control Procedure, reasonable under the circumstances to Commonwealth, and such replacement or upgrade shall be subject to Commonwealth's approval, including, without limitation, the approval of the contemplated implementation schedule and cost. If Commonwealth withholds its approval of such replacement, upgrade or contemplated schedule, the Contractor Project Manager and the Commonwealth Project Manager, in good faith and subject to the Change Control Procedures, will determine the appropriate adjustments to the Services Levels.

(2) In addition to the foregoing obligations of Contractor under this *Section 7* (Equipment). Contractor shall provide Commonwealth with information regarding additional Improved Technology for Commonwealth's evaluation in connection with the Services, to the

extent then known to Contractor, and shall meet with Commonwealth at least two (2) times during each Contract year to inform Commonwealth of any Improved Technology Contractor is developing or information processing trends and directions of which Contractor is aware. Upon the existence of any such additional Improved Technology that the parties believe would materially improve the performance, or reduce the cost, of the Services, (other than the required upgrades and replacements provided for above), the parties will meet and discuss in good faith the terms upon which such Improved Technology may be implemented into the Services. The parties acknowledge their intent, in such discussions, to develop terms for such implementation that will result in an equal sharing by the parties of the net economic benefit that is expected to result therefrom with the Fees adjusted accordingly (after taking into account Contractor's cost of the related hardware, software and implementation efforts). Upon any such projected reduction of the cost of the Services, the parties, working together in good faith, shall revise the Fees accordingly.

b) **Equipment Maintenance**. As part of the Services, Contractor shall provide to Commonwealth maintenance and support services in respect of the Equipment and shall, at its own cost and expense, maintain and support the Contractor Machines as necessary for Contractor to perform the Services in accordance with the Services Levels. All costs and expenses incurred in connection with the provision of maintenance and support services in respect of the Equipment (including third party maintenance fees) shall be the responsibility of Contractor.

8. THIRD PARTY SOFTWARE

a) As part of the Services, Contractor shall have operational responsibility for the Commonwealth Third Party Software for which Commonwealth has a valid license and current maintenance agreement ("Commonwealth Third Party Software") and shall be responsible for applying upgrades, enhancements and fixes as provided and directed by the applicable agency. The Commonwealth shall have financial responsibility for any Commonwealth Third Party Software license, upgrade, maintenance and support fees, except that Contractor shall be responsible for any third-party consulting fees in connection with the installation or implementation of any software upgrade, revision or replacement required by Contractor.

b) As part of the Services, Contractor shall have financial, administration, operational and maintenance responsibility for all Contractor Software and Third Party Software provided by the Contractor as part of the Services, including but not limited to the Third Party Software listed in *Exhibit B.4.*

Comment [A14]: Contractor proposes that the words "provided by the Contractor as part of the Services" is added after the words Contractor Software

c) As part of the Services, except for the cost of the license, Contractor shall have financial, administration, operational and maintenance responsibility for the Third

Party Software listed in *Exhibit B.10*, for which the Commonwealth has a valid license ("Hybrid Third Party Software").

d) The Contractor shall not require the Commonwealth to sign a software license agreement for any Contractor Software or Third Party Software, including but not limited to any click through agreement or other terms purported to apply to the software.

Comment [A15]: Contractor would like to understand the Commonwealth's intent with this language

e) The Commonwealth will continue to support and maintain the software owned by the Commonwealth ("Commonwealth Proprietary Software") as necessary for Contractor's performance of the Services.

9. DATA SECURITY

a) Commonwealth will retain administration of logical and data access security, and Contractor will host Commonwealth security applications software utilized by the Commonwealth in managing logical and data access security, and will not implement configurations that would prevent Commonwealth from managing logical and data access security. As part of the Services, Contractor shall implement and maintain the Commonwealth's safeguards against the disclosure, destruction, loss or alteration of the Commonwealth Data in the possession of Contractor in accordance with the terms of this Contract and with Commonwealth's other security policies and procedures provided, in writing, to Contractor. In any event, Contractor, as part of the Services, is required to meet or exceed the most stringent of any applicable federal or state law, statute, rule or regulation applicable to Contractor's and/or Contractor's Agents possession of, or access to, any Commonwealth Data (which includes *Section 12(d)*, herein). All changes or additions to any such Commonwealth security policies or procedure or any changes to any applicable federal or state law, statute, rule or regulation shall be implemented by Contractor. Any changes or additions which result in a material additional cost to Contractor shall be subject to the Change Control Procedures. To the degree such change applies to other Contractor customers, Contractor will mitigate the Commonwealth's economic exposure to additional cost by equitably spreading the additional cost of compliance to its multiple customers.

b) The Contractor shall not store the Commonwealth Data outside of the continental United States of America.

c) All of Contractor's activities relating to the safeguarding of Commonwealth Data shall be subject to periodic review and monitoring by Commonwealth and related Federal agencies, and Contractor shall cooperate fully with all such reviews and monitoring. In addition to, and not in limitation of, any restrictions set forth elsewhere in this Contract, Contractor shall have operational access to the Commonwealth Data only on an as-needed basis.

d) Upon request at any time during the term of this Contract, or upon termination, cancellation, expiration or other conclusion of the Contract, Contractor shall return the Commonwealth Data to the Commonwealth or, at the Commonwealth's request, destroy the Data. If the Commonwealth requests Contractor to destroy the Data, the Commonwealth shall have the right to conduct an audit to ensure the Data has been destroyed. This provision shall also apply to all Commonwealth Data that is in the possession of subcontractors or agents of Contractor. Contractor shall complete such return or destruction within ten (10) days of the request or after the conclusion of this Contract. Within such ten (10) day period, Contractor shall certify in writing to Commonwealth that such return or destruction has been completed. Contractor shall make available to the Commonwealth for a complete and secure (i.e. encrypted and appropriately authenticated) download file of the Commonwealth Data in XML format, or such other format as specified by the Commonwealth, including all schema and transformation definitions and/or delimited text files with documented, detailed schema definitions along with attachments in their native format. Contractor shall be available to answer questions about data schema, transformations, and other elements required to fully understand and utilize the Commonwealth's data file. Unless the Commonwealth agrees or specifies otherwise, the Contractor shall also deliver to the Commonwealth any copies, duplicates, summaries, abstracts or other representations of any such Commonwealth Data or any part thereof, in whatever form, then in the Contractor's possession or control in accordance with the "NIST Guidelines for Media Sanitization" (SP 800-88).

Comment [A16]: This subject is repeated in 37g and 42d, which is somewhat contradictory 42d is similar to current contract language Contractor proposes deleting this section and maintaining section 42d

e) Contractor shall comply with all state and Federal data breach laws, including but not limited to the Commonwealth Breach of Personal Information Notification Act (73 P.S. § §2301 *et seq*.). In the event Contractor or any of Contractor's Agents discover or are notified of a data breach or potential breach of security involving any of the Commonwealth Data, Contractor shall immediately notify the Commonwealth Project Manager and the Commonwealth's Chief Information Security Officer of the same and describe the nature of the breach, the Data compromised, the involved parties, mitigation efforts, and corrective actions to be taken by the Contractor. In addition, at Commonwealth's request and at Contractor's sole cost and expense, Contractor shall:

Comment [A17]: Contractor agrees to comply to applicable state and Federal laws as it relates to the delivery of Contractor Services

(1) Promptly provide Commonwealth Data security reports to Commonwealth in a form to be agreed upon by Commonwealth and Contractor; and

(2) Cooperate with any efforts by Commonwealth to investigate or prosecute any breach of security of the Commonwealth Data; and

(3) Provide credit monitoring services to all individuals or organizations that may be impacted by the security breach.

Contractor shall be solely responsible for any costs, losses or damages actually incurred by the Commonwealth due to Personal Information being accessed, used, released, disclosed and/or acquired in an unauthorized manner while in the possession and control of the Contractor or its employees, agents, and/or subcontractors. In the event of any data breach by Contractor or any of the Contractor Agents involving any of the Commonwealth Data, Contractor shall be assessed a credit against Fees due for Service provided during the period of breach of security.

f) Credit Card Information

(1) By providing the Services under this Contract, the Contractor may create, receive, or have access to credit card records or record systems containing cardholder data including credit card numbers (collectively the "Cardholder Data"). Contractor shall comply with the Payment Card Industry Data Security Standard ("PCI DSS") requirements for Cardholder Data that are prescribed by the payment brands (including but not limited to Visa, MasterCard, American Express, and Discover), as they may be amended from time to time. Contractor acknowledges and agrees that Cardholder Data may only be used for assisting in completing a card transaction, for fraud control services, for loyalty programs, or as specifically agreed to by the payment brands, for purposes of this Contract or as required by applicable law.

(2) Contractor shall conform to and comply with the PCI DSS standards as defined by The PCI Security Standards Council at: https://www.pcisecuritystandards.org/security_standards/index.php. Contractor shall monitor these PCI DSS standards and will promptly notify the Commonwealth if its practices should not conform to such standards. Contractor shall provide a letter of certification to attest to meeting this requirement within one week of Contractor's receipt of the annual PCI DSS compliance report.

Comment [A18]: Contractor should be responsible for the costs described in this paragraph only where due to Contractor's breach Also, Contractor proposes a cap similar to the current contract be incorporated in this Contract

Comment [A19]: Contractor proposes that the specific remedies resulting from a data breach should be discussed and negotiated as part of the limitation of liability discussion Contractor proposes this should be a damages claim, not a credit against fees

Comment [A20]: Contractor believes this may not apply within Services today, and so should be handled via change control at agency direction/request if and when it is needed

Comment [A21]: Contractor shall comply with PCI DSS however the Commonwealth will need to interpret and notify Contractor what requirements that need to be followed Change Control Procedure will be implemented whenever changes are required

10. CONDUCT OF SERVICES

a) Following execution of the Contract, Contractor shall proceed diligently with all Services and shall perform such Services with qualified personnel, in accordance with the completion criteria set forth in the Contract.

b) The Contractor's Services hereunder shall be monitored by the Commonwealth and the Commonwealth's designated representatives. If the Commonwealth reasonably determines that the Contractor has not performed to the requirements in the Contract or has otherwise exposed the Commonwealth to material risk, the Commonwealth and the Contractor will attempt to reach agreement with respect to such matter. Failure of the Commonwealth or the

Contractor to arrive at such mutual determinations shall be a dispute concerning a question of fact within the meaning of *Section 34* (Contract Controversies) of this Contract.

c) As part of the Services, Contractor shall conduct enterprise-wide Commonwealth Satisfaction Surveys, which surveys shall be conducted annually until completion of the Transition. Upon completion of the Transition, Contractor shall conduct the Commonwealth Satisfaction Surveys semi-annually for two years and annually thereafter.

11. QUALITY ASSURANCE AND INTERNAL CONTROLS

a) Contractor will develop and implement quality assurance and internal controls, including implementing tools and methodologies, to ensure that the Services are performed in an accurate and timely manner, in accordance with the Contract. Without limiting the foregoing, Contractor will:

(1) Maintain a strong control environment in day-to-day operations;

(2) Develop and execute a process to ensure regular internal control self-assessments are performed with respect to all Services and report the outcome of such self-assessments to the Commonwealth;

(3) Maintain an internal audit function sufficient to monitor the processes and systems used to provide the Services (i.e., perform audits, track control measures, communicate status to management, drive corrective action, etc.); and

(4) Provide to Commonwealth a summary of audit activity performed, associated significant findings, status of follow-up activity, summary of control incidents (i.e., frauds, conflict of interest situations, etc.) and related corrective action, every six (6) months.

b) As part of the Services and included in the Fees, Contractor shall:

(1) Implement and maintain independently audited quality certification (ISO 27001, ISO 9001 and ISO/IEC 20000 accreditation) and provide copies of its certification under such program and also any relevant audit or report documentation whenever so requested by the Commonwealth.

(2) Maintain valid security certifications including CISSP (Certified Information Systems Security Professional) or Comp TIA-Security+ or CASP and provide copies of its certification under such program and also any relevant documentation whenever so requested by the Commonwealth.

(3) Maintain compliance with Federal and State mandated policies including CJIS (Criminal Justice Information Services) and CHRIA (Criminal History Record Information Act) and provide copies of any relevant documentation whenever so requested by the Commonwealth.

(4) Undertake at least annually, and shall cause to be undertaken by Contractor's material subcontractors, a SSAE 16 Type II audit that covers the common controls for any Contractor sites where Contractor performs work for the Commonwealth; provide the reports from such audits to the Commonwealth; and perform these SSAE 16 Type II audits at such time(s) that shall mean the audit report is recent enough for Commonwealth to rely upon it in meeting its reporting obligations.

Comment [A22]: [illegible] A

12. SERVICE LOCATIONS

a) **Services Locations**. The Services shall be provided from and to the Service Locations as detailed in *Schedule E* (Datacenter Locations). Contractor shall not (1) provide the Services from a location other than a Service Location or (2) use the Commonwealth Enterprise Data Center to provide services to a third party without Commonwealth's consent. Authorized representatives of Commonwealth, Commonwealth agents and agents of the Federal government shall be permitted access to any Services Location, subject to the terms of *Section 12(d)*.

b) **Location of Performance.** Except where Contractor obtains the Commonwealth's prior written approval, Contractor shall perform all of the Services only from or at locations within the geographic boundaries of the continental United States. Any Commonwealth approval for the performance of Services outside of the continental United States shall be limited to the specific instance and scope of such written approval, including the types of Services and locations involved.

c) Right to Audit and Inspect:

(1) The Contractor shall permit the Commonwealth (or a third-party provider selected by the Commonwealth) to perform an onsite inspection of the Contractor's Service Locations, infrastructure and security practices as reasonably requested by the Commonwealth, but no more than once per month.

Comment [A23]: Contractor proposes 2 inspections per year as long as inspections are not disruptive to Contractor Services

(2) The Commonwealth shall have the right to request third-party audits and/or certifications related to each Serve Location's infrastructure and security, including penetration testing and vulnerability assessments. Any reports produced from these audits

and certifications will be provided to the Commonwealth for review at no cost.

(3) The Contractor shall provide the Commonwealth infrastructure and security specifications in written format for each Service Location as requested and at no cost to the Commonwealth.

(4) The Contractor shall provide the Commonwealth access to the performance records of the Contractor, as well as access to daily and weekly service quality statistics as requested and at no cost to the Commonwealth.

d) Security Procedures

(1) As part of the Services, Contractor shall maintain and enforce environmental and physical security standards and procedures at each of the Contractor Services Locations and shall comply with environmental and physical security procedures as described in *Schedule F* (COPA Datacenter Statement of Work) and pursuant to the physical security and environmental chapters of the Commonwealth Computing Procedures Manual, which compliance will be confirmed by Contractor's SSAE 16 Type II audit report which will be delivered to the Commonwealth. If the Commonwealth requests any changes to environmental and security standards after the Effective Date and such changes would subject Contractor to material additional costs, those changes will be addressed through the Change Control Procedures. In addition, each Contractor Services Location must meet a minimum of Class C2 controlled access protection as defined in the Federal Department of Defense Trusted Computer System Evaluation (DOD 5200.28-STD).

(2) Each Commonwealth Agency's specific security requirements must be satisfied prior to the migration of its data or processing activities to any Contractor Services Location, including any facilities to be used to support Disaster Recovery. Contractor shall maintain a log recording all entry to any Contractor Services Location, which log shall at all times be subject to Commonwealth review and audit. All of Contractor's security procedures required under this Contract shall be subject to periodic review by Commonwealth, any Commonwealth Agency or any agency of the United States federal government directly or indirectly having any dealings with any Commonwealth Agency.

(3) Contractor, as part of the Services, shall address any concerns any such reviewing entity may have regarding those security procedures and, if Commonwealth is not the reviewing entity, shall promptly

inform Commonwealth of the expressed concerns and its plans to address the same. Contractor acknowledges that, because Commonwealth is a governmental entity, Commonwealth is subject to various federal and state statutory and regulatory confidentiality and security requirements, all of which will be binding upon Contractor during the Term. This Contract and the business relationship between Commonwealth and Contractor will be subject to review and approval by impacted Commonwealth Agencies and impacted federal agencies and other entities. At a minimum, Contractor will be required to comply with the Privacy Act of 1974, as amended (42 U.S.C.A. 2000, *et seq.*), the Drivers Privacy Protection Act, as amended (18 U.S.C.A. 2721, *et seq.*), the Tax Information Security Guidelines promulgated by the Internal Revenue Service; and various confidentiality regulations promulgated by the U.S. Department of Health and Human Services, all as though Contractor were a governmental entity. Contractor will also be required to comply with the Health Insurance Portability and Accountability Act of 1996, Pub.L. 104-191 (HIPAA) and the regulations promulgated related thereto (45 C.F.R. 160.101, *et seq.*) as a Business Associate as that term is defined by HIPAA according to the Business Associate Contract included as Appendix A (which Contract shall apply to covered portions of the Commonwealth as a hybrid entity as agencies direct, and which Contract shall govern only insofar as no other more stringent law otherwise applies to that data, and only insofar as the Contract does not conflict with more stringent provisions of this Amendment, where "more stringent" is defined as in 45 C.F.R. 160.202). If and only to the extent specifically required in writing by a federal agency, in order for Contractor to be granted operational access to Commonwealth Data in connection with its performance of the Services, Contractor may be appointed as an agent of Commonwealth for the limited purpose of having operational access to certain Commonwealth Data not as a contractor of Commonwealth, but as an agent of Commonwealth having an agent's fiduciary obligations to Commonwealth as its principal. Contractor shall deliver to Commonwealth written notice of any breach of such security standards and procedures of which Contractor then has knowledge, which notice shall be delivered as promptly as is reasonable under the circumstances. Any breach by Contractor of such security standards or procedures under this *Section 12(d)* shall be subject to the provisions of *Section 30* (Default). As more fully set forth in *Section 59* (Independent Capacity of Contractor), parties to this Contract agree that the Services performed by the Contractor under the terms of this Contract are performed as an independent contractor.

Comment [A24]: Contractor proposes this reference should be to 32(c)

13. CONDITIONS OF CONTRACTOR'S OCCUPANCY OF COMMONWEALTH-PROVIDED REAL PROPERTY

a) General

(1) The Contractor shall use and occupy the property provided by the Commonwealth (the "Enterprise Data Center") continuously as a data processing center and for related administrative uses. No other use shall be permitted. A summary of the Enterprise Data Center is attached to the RFP and incorporated herein as *Exhibit D.7* (EDC Summary and Requirements).

(2) The Contractor shall have the sole responsibility to comply with all federal, state, and municipal laws, ordinances and regulations in its use and occupancy of the property.

(3) The Contractor agrees to accept the property in an "as-is" condition. The Contractor agrees that the Commonwealth extends no warranty of any kind, express or implied, in regard to the property provided to the Contractor for its use.

(4) The Commonwealth is immune from the payment of real estate taxes. If any relevant taxing authority deems the use of the property by the Contractor to cause the property to become taxable, the Contractor shall have sole responsibility for the timely payment of any tax levied. Payment of such taxes may be temporarily withheld if Contractor is, in good faith, contesting the assessment or tax in a court of competent jurisdiction.

(5) The Contractor agrees that this Contract does not grant or otherwise convey any legal interest in the real property to the Contractor.

b) Upkeep and Improvements

Comment [A25]: Contractor proposes additional language to be added whereby ordinary wear and tear excepted

(1) The Contractor, at its sole cost and expense, is responsible for all maintenance, security and upkeep of the property under its control. The Contractor agrees to keep the property in substantially the same condition as it was upon the Effective Date of the Contract.

(2) Except for minor, non-structural alterations costing less than $10,000, any and all Contractor alterations and additions to the Property shall be performed in accordance with plans and specifications prepared by a Pennsylvania-licensed architect and/or engineer. The Contractor shall submit plans and specifications to the Office of Administration and the Department of General Services concurrently for approval prior to initiation of

construction. Any and all alterations to the Property shall be performed in a good and workmanlike manner, in conformity with all laws, rules, ordinances and other requirements of all governmental entities having jurisdiction. The Department of General Services and the Office of Administration reserve the right to specify standards that must be maintained for any alterations and additions to the Property.

(3) The Contractor is solely responsible for all costs and expenses associated with any Contractor alterations or additions.

(4) The Contractor shall fully comply with Pennsylvania law governing contracting for construction, alteration or repair of a public building, including but not limited to the Prevailing Wage Act, Steel Products Procurement Act, and the Uniform Construction Code.

(5) To the fullest extent permitted by law, all Contractor contracts for alterations and additions must include a "No-Lien" clause requiring that the Property be kept free from mechanics' or materialmens' liens and that the parties must file the necessary documentation in the appropriate public offices to effectuate waivers of contractors', mechanics' and materialmens' liens.

(6) Any and all alterations and additions made to the property by either the Contractor or the Commonwealth shall become part of the real estate and become the property of the Commonwealth.

c) Utilities

Contractor shall have installed, at its sole cost, separate electric meters and distribution panels to support the raised floor compute space. The Contractor will be responsible to timely reimburse the Commonwealth for electricity consumed in the raised floor compute space.

d) Reserve Account

Contractor shall establish a capital improvement fund ("Reserve Account") into which Contractor shall deposit monthly ($84,000) dollars. The Reserve Account shall be cumulative, intended for capital improvements or major repairs to the Enterprise Data Center and disbursements from which shall be made only upon mutual agreement of the Commonwealth and the Contractor. Any remaining sums in the Reserve Account at termination of this Agreement shall be paid or credited to the Commonwealth. In the event that at any time during the term of this Contract sums in the Reserve Account are insufficient to

cover the cost of an agreed-to capital improvement or major repair, Contractor shall be reimbursed by the Commonwealth in an amount equal to such insufficiency. Contractor shall provide the Commonwealth at least semi-annually a report of all activity in the Reserve Account.

e) Termination Assistance

Contractor shall vacate the Enterprise Data Center and return to the Commonwealth, if not previously returned, any resources that are implicated by the relevant Assistance Event, as described in *Section 33* (Termination Assistance), and that are owned, leased or licensed by the Commonwealth or any Commonwealth Contractor, including the Commonwealth owned or leased Equipment, the Commonwealth Owned Materials and the Commonwealth licensed Materials, in condition at least as good as the condition of such facilities and resources when they were made available to Contractor, ordinary wear and tear excepted. Such facilities and resources shall be vacated and/or returned as of the later of the effective date of the relevant Assistance Event and the completion of the Termination Assistance requiring such facilities or resources.

14. TRANSITION

a) **Transition.** Contractor shall perform the Transition Services, including provision of the deliverables described in the Detailed Transition Plan. Contractor shall accomplish the Transition in a transparent, seamless, orderly, and uninterrupted manner. Contractor's responsibilities with respect to the transition include:

(1) Transfer of the Services to Contractor and subsequent transition of the Services to realize any planned cost reductions and Service performance improvements in accordance with the Transition Plans agreed to by Commonwealth and including a number of Transition Milestones;

(2) Performing the transition without disruption to Commonwealth's operations;

(3) Assuming responsibility for all costs associated with the transition; and

(4) Otherwise performing such transition and migration tasks as are necessary to enable Contractor to provide the Services in accordance with the terms of the Contract, including the applicable Service Levels.

b) **Transition Plan.** The preliminary Transition Plan is attached to this Contract as part of Contractor's Proposal. Contractor shall complete, and submit to

Commonwealth for review a final Detailed Transition Plan on or before the date set forth in *Schedule D* (Transition Milestones). If a Detailed Transition Plan submitted by Contractor is not acceptable to Commonwealth, Contractor will address and resolve any questions or concerns Commonwealth may have and will promptly incorporate any modifications, additions or deletions requested by Commonwealth. Contractor will revise and resubmit the Detailed Transition Plan until accepted by Commonwealth. Upon Commonwealth's acceptance, the Detailed Transition Plan shall automatically be incorporated into this Contract as *Schedule M* (Detailed Transition Plan) and shall supersede and replace all prior Transition Plans. The Detailed Transition Plan shall detail the specific activities to be performed by each Party, and, unless otherwise requested by Contractor and agreed to by Commonwealth in its sole discretion, shall be consistent in all material respects with any preliminary Transition Plan, including with respect to the activities, deliverables, Transition Milestones, and Transition Milestone Credits described therein. The Detailed Transition Plan may thereafter be amended as mutually agreed by the Parties.

Comment [A26]: Contractor proposes that this is subject to Contractor mutual agreement which will not be unreasonably withheld

The Parties recognize and agree that time is of the essence for a successful Transition and have designated certain actions and projects in the Detailed Transition Plan as Transition Milestones ("Transition Milestones"). Contractor shall achieve all such Transition Milestone by the date corresponding thereto in *Schedule D* (Transition Milestones). Without limiting the foregoing, the Detailed Transition Plan shall specify, among other things,

Comment [A27]: Contractor proposes that time is of the essence is not an appropriate concept in this type of Services agreement

1. the deliverables to be completed by Contractor,

2. the date(s) by which each such activity or deliverable is to be completed (the "Transition Milestones"),

3. a process and set of standards to which Contractor shall adhere in the performance of the Transition Services and that shall enable Commonwealth to determine whether Contractor has successfully completed the transition and the activities and deliverables associated with each Transition Milestone,

4. any transition responsibilities to be performed or transition resources to be provided by Commonwealth and/or Commonwealth Customers,

5. any transition responsibilities to be performed or transition resources to be provided by another Commonwealth Contractor, and

6. a detailed description of the processes and procedures that Contractor will implement (and associated implementation schedules) to effect the seamless integration and coordination

of the Services with related services to be provided by other Commonwealth Contractors.

The Detailed Transition Plan shall identify any related documents contemplated by this Contract and/or required to effectuate the transition that shall be executed by either of the Parties.

c) **Performance**. Contractor shall perform the Transition Services in accordance with the timetable and the Transition Milestones set forth in the Transition Detailed Plan. Contractor shall assist Commonwealth in connection with Commonwealth's evaluation or testing of the deliverables set forth in the Detailed Transition Plan. Except as otherwise expressly stipulated in the Detailed Transition Plan, Contractor shall perform the Transition Services in a manner that shall not (i) disrupt or have an unnecessary adverse impact on the activities or operations of Commonwealth or the Commonwealth Customers, (ii) degrade the Services then being received by Commonwealth or the Commonwealth Customers or (iii) disrupt or interfere with the ability of Commonwealth or the Commonwealth Customers to obtain the full benefit of the Services. In Contractor's performance and completion of Transition Services, no functionality of Commonwealth's then current business operations or environment will be discontinued until Contractor demonstrates to Commonwealth's reasonable satisfaction that the affected processes and operations have been successfully migrated to Contractor's target environment and are functioning properly in that environment.

Comment [A28]: Contractor requests a material qualification to be included in subsection ii and iii

Without limiting its obligations or responsibilities, prior to undertaking any transition activity, Contractor shall discuss with Commonwealth and the relevant Commonwealth Customers all known Commonwealth and Commonwealth Customer-specific material risks and shall not proceed with such activity until Commonwealth is reasonably satisfied with the plans with regard to such risks (provided that, neither Contractor's disclosure of any such risks to Commonwealth, nor Commonwealth's acquiescence in Contractor's plans, shall operate or be construed as limiting Contractor's responsibility under this Contract). Contractor will, at Commonwealth's request, participate in transition meetings with other Commonwealth Contractors. Commonwealth reserves the right to monitor, test and otherwise observe and participate in transition. Contractor will notify Commonwealth without delay if any Commonwealth monitoring, testing or participation has caused (or Contractor expects it to cause) a problem or delay in transition and work with Commonwealth to prevent or circumvent the problem or delay.

d) **Reports**. Beginning on the Effective Date, Contractor shall meet at least weekly with the Commonwealth to report on Contractor's progress in performing its responsibilities and meeting the timetable and Transition Milestones set forth in the Detailed Transition Plan. Contractor also shall provide written reports to Commonwealth at least weekly regarding such

matters, and shall provide oral reports more frequently if requested by Commonwealth. Promptly upon receiving any information indicating that Contractor may not perform its responsibilities or meet the timetable or Transition Milestones set forth in the Detailed Transition Plan, Contractor shall notify Commonwealth of such delays and shall identify for Commonwealth's consideration and approval specific measures to address such delays and mitigate the risks associated therewith.

e) **Notification of Problems**. Contractor shall provide to Commonwealth written notice of any acts or omissions (whether by Commonwealth, a Commonwealth Contractor, subcontractor or any third party), any failure to perform any of each such party's obligations under the Contract and any other events that may affect Contractor's performance of the Transition Services. Contractor shall provide such written notice within thirty (30) days after Contractor first knew or should have known of such acts, omissions, or failures or other events. Such written notice shall describe in reasonable detail such acts, omissions, failures or other events and the manner in which the foregoing may affect Contractor's performance.

Comment [A29]: Contractor proposes that Contractor will be reimbursed for Contractor costs and relieved for failure to perform Contractor's obligation if such costs or failure are due to such acts, omissions, or failures

f) **Corrective Action Plan**. In the event that either (1) the Commonwealth determines that Contractor has failed or is reasonably likely to fail to deliver the Transition Services, or (2) Contractor has determined that it has failed or is reasonably likely to fail to deliver the Transition Services, then Commonwealth or Contractor, as applicable, will notify the other Party of such failure (a "Transition CAP Notice"). Concurrently with such notice, Contractor will:

1. immediately take steps to mitigate any harmful effects of such failure, and
2. (promptly (and in any event as soon as reasonably practical) perform a Root Cause Analysis and prepare a Corrective Action Plan with respect to such failure, and
3. take all actions necessary to prevent its recurrence, including, without limitation, providing all additional resources necessary to resolve such failure.

If in Commonwealth's sole discretion any such Corrective Action Plan is not adequately addressing the failure, Contractor shall revise the Corrective Action Plan until it is accepted by the Commonwealth. In the event that Contractor is unable to complete the Transition Services on or before the dates specified in the Detailed Transition Plan (a "Transition Failure Event"), then Contractor will meet with Commonwealth to develop a workaround plan to address the Transition Failure Event, which plan may include, at Commonwealth's option, obtaining the services to workaround the Transition Failure Event from another Commonwealth contractor and/or the incumbent contractor. If the Commonwealth elects to obtain such services from another contractor and/or

Comment [A30]: Contractor requests to removing "sole" and replace with "reasonable"

the incumbent contractor, the Commonwealth will equitably adjust the Fees to reflect the reduction in Services being provided by Contractor.

g) **Failure to Meet Transition Milestones**. Neither the Transition Services nor the activities and deliverables associated with individual Transition Milestones shall be deemed complete until Commonwealth's acceptance of such activities and deliverables. If Contractor fails to meet a Transition Milestone, Contractor shall pay Commonwealth the applicable Milestone Credits specified in *Schedule D* (Transition Milestones) or the Detailed Transition Plan that are associated with such Transition Services.

h) **Additional Remedies**. In the event that Contractor fails to identify and resolve any problems that may impede or delay the timely completion of each task in the Detailed Transition Plan, without prejudice to Commonwealth's other rights and remedies under the Contract or at law or equity, (i) Contractor will provide, at its sole cost and expense, all such additional resources as are necessary to identify and resolve any problems that may impede or delay the timely completion of each task in the Detailed Transition Plan, and (ii) Commonwealth may equitably reduce the Fees set forth in *Schedule I* (Offeror Pricing Forms) in an amount reasonably estimated by Commonwealth to account for the Services that Commonwealth is not receiving or did not receive.

i) **Suspension or Delay of Transition Services.** Commonwealth reserves the right, in its sole discretion, to suspend or delay the performance of the Transition Services and/or the transition of all or any part of the Services. If Commonwealth elects to exercise this right and Commonwealth's decision is based in material part on concerns about Contractor's ability to perform material aspects of the Transition Services or Contractor's failure to perform its obligations under this Contract, the Commonwealth shall not incur any additional Fees or reimbursable expenses in connection with such decision, provided that Commonwealth shall work in good faith with Contractor to minimize the period of any such suspension or delay.

15. DISASTER RECOVERY AND BUSINESS CONTINUITY

a) Disaster Recovery Plan.

(1) Jointly with the Commonwealth, Contractor shall at least annually review and update the disaster recovery plan, it being understood and agreed that the parties will work together and cooperate in good faith on any such review or updated of the disaster recovery plans.

(2) With the Commonwealth's support as specified in the disaster recovery plan, Contractor shall every six (6) months test the operability of the disaster recovery plan then in effect.

Comment [A31]: Contractor believes unilateral deduction of Fees by Commonwealth is not an appropriate remedy, this should be a damages claim

Comment [A32]: For clarity purposes, if the Transition failure event is caused by the Commonwealth, the Commonwealth will not be able to obtain such services from another vendor and Contractor may process Change Control related to any additional costs it incurred

Comment [A33]: Contractor proposes cure periods for missed milestones

Comment [A34]: Contractor requests that Commonwealth will reimburse Contractor for any delays caused by the Commonwealth

1. Within fifteen (15) business days of completion of a disaster recovery test, Contractor will certify to Commonwealth that the disaster recovery plan was fully, timely and successfully implemented, or, if the disaster recovery plan was not fully, timely and successfully implemented, report all deficiencies (including root cause analysis) and corrective actions, and certify that such corrective actions addressed all deficiencies; and

2. Annually and at additional times at the request of Commonwealth, Contractor will certify to Commonwealth that that any applicable third-party business recovery center agreement remains in full force and effect without any default, including payment, thereunder by any party thereto, and that Commonwealth is entitled, pursuant to the terms of the business recovery center agreement, to assume that agreement upon the expiration or termination of this Contract.

b) Disaster Recovery Event.

(1) As part of the Services, Contractor shall have responsibility for executing the disaster recovery plan relating to the Services as described in *Schedule F* (COPA Datacenter Statement of Work). Contractor shall immediately provide Commonwealth with notice of the occurrence of any disaster affecting the provision or receipt of all or any material portion of the Services and implement the disaster recovery plan then in effect. Contractor agrees to utilize the disaster recovery planning methodology software then utilized by Commonwealth in connection with activities contemplated under this *Section 15* (Disaster Recovery and Business Continuity).

(2) Contractor shall reinstitute the Services as promptly as possible but in any event within subscribed restitution hours, as set forth in the disaster recovery plan then in effect, after the occurrence of a disaster. If the Services are not fully reinstituted within the subscribed restitution hours the Commonwealth shall have the right to terminate this Contract for critical failure pursuant to the provisions of *Section 32(c)*, and Contractor shall, prior to or at the expiration of the applicable restitution period, deliver to Commonwealth a written report detailing the cause of the disaster, Contractor's plans to reinstitute the Services and its anticipated schedule to do so. Thereafter, Contractor and Commonwealth shall develop a plan to reinstitute the Services as promptly as is possible under the circumstances, with Contractor making such reinstitution its highest priority. Contractor shall prepare and deliver to Commonwealth

Comment [A35]: Contractor proposes that Contractor is relieved to the extent Commonwealth causes the failure

Comment [A36]: Contractor suggesting deleting the highlighted words “with Contractor… priority ”

updated reports such that Commonwealth shall at all times be fully informed as to the status of Contractor's efforts and anticipated schedule to reinstitute the Services. In the event that any Contractor Machines are required to be replaced as a result of the disaster, Contractor shall replace such Contractor Machines with current or Improved Technology to the extent then available and compatible with the associated application(s). Any Contractor obligations to implement a disaster recovery plan set forth in this paragraph can be triggered by a notice of disaster provided to Contractor by Commonwealth.

Comment [A37]: Contractor proposes that Contractor should be able to replace with any equipment that enables Contractor to meet Service Levels, regardless of current or improved technology based on the Managed Services contract type

16. PRIME CONTRACTOR RESPONSIBILITIES

The Contractor will be responsible for all Services in this Contract whether or not Contractor provides them directly. Further, the Contractor is the sole point of contact with regard to all contractual matters, including payment of any and all charges resulting from the Contract.

17. KEY POSITIONS/CONTRACTOR PERSONNEL

a) **Contractor Project Manager and Transition Project Manager**.

(1) Upon the Effective Date, the Contractor shall appoint the Contractor Project Manager identified in its proposal, who on a full-time basis shall be in charge of implementing the Services. Contractor shall replace the Contractor Project Manager only when required or permitted pursuant to *Section 17(c)*. The Contractor Project Manager shall at all times be subject to Commonwealth's continuing approval.

(2) Upon the Effective Date he Contractor shall appoint the Transition Project Manager identified in its proposal, who will have the responsibilities set forth in *Schedule F* (COPA Datacenter Statement of Work). Contractor shall replace the Transition Project Manager only when required or permitted pursuant to *Section 17(c)*. The Contractor Project Manager shall at all times be subject to Commonwealth's continuing approval.

b) **Key Positions**. The positions identified in *Schedule G* (Staffing Plan and Key Positions), are designated by Commonwealth and Contractor as key positions within the Contractor's Personnel. All of the Key Employees shall be dedicated to the Commonwealth account on a full-time basis. The Commonwealth Project Manager and the Contractor Project Manager shall meet once every Contract Year thereafter or upon the request of either the Commonwealth Project Manager or the Contractor Project Manager to update the list of the Key Employees. Each Key Employee shall at all times be subject to Commonwealth's continuing approval. Except for a replacement or reassignment of a Key Employee pursuant to *Section 17(c)*, Contractor shall not reassign or replace any Key Employee. As

more fully set forth in *Section 59* (Independent Capacity of Contractor), parties to this Contract agree that the Services performed by the Contractor under the terms of this Contract are performed as an independent contractor.

c) **Reassignment Waivers**. Contractor shall not reassign or replace the Contractor Project Manager or any Contractor Services Location Manager during the first eighteen (18) months of his or her assignment as the Contractor Project Manager or a Contractor Services Location Manager unless Commonwealth consents to such reassignment or replacement or unless the individual (1) voluntarily resigns from Contractor, (2) is dismissed by Contractor for cause, or (3) is unable to work due to his or her death or disability. In addition, Contractor shall, in connection with its assignment of other Key Employees, use commercially reasonable efforts to assure the greatest degree of continuity possible among such Key Employees. If, in any instance, Commonwealth withholds or withdraws its approval of any employee or representative of Contractor for the performance of the Services, including without limitation, the Contractor Project Manager, any Contractor Services Location Manager or any other Key Employee, Contractor promptly shall reassign and replace such employee or representative

Comment [A38]: Contractor proposes adding language to include "displays unsatisfactory performance" as included in current contract

d) **Subcontractors**. The Contractor may subcontract any portion of the Services described in this Contract to third parties selected by Contractor and approved in writing by the Commonwealth, which approval will not be unreasonably withheld. Approved Subcontractors will be listed on *Schedule L* (Approved Subcontractors). Notwithstanding the above, if Contractor has disclosed the identity of Subcontractor(s) together with the scope of work to be subcontracted in the Contractor's Proposal, award of the Contract is deemed approval of all named Subcontractors for the specified scope of work and a separate approval is not required. The existence of any subcontract shall not change the obligations of Contractor to the Commonwealth under this Contract. Upon written request of the Commonwealth, the Contractor shall promptly provide the Commonwealth with a copy of any specified subcontract agreement between the Contractor and the subcontractor. If Commonwealth reasonably determines that a subcontractor should no longer be retained by Contractor due to material performance deficiencies arising from the subcontractor's performance, the Commonwealth reserves the right, for good cause, to require that the Contractor remove a subcontractor from the project. As more fully set forth in *Section 59* (Independent Capacity of Contractor), parties to this Contract agree that the Services performed by the Contractor under the terms of this Contract are performed as an independent contractor.

Comment [A39]: Contractor proposes that except to the extent required by law, economic terms shall not be discussed

e) **Managerial Control**. Subject to the other provisions of this Contract, including without limitation, provisions regarding security procedures and government security clearance and the other provisions of this *Section 17* (Key Positions/Contractor Personnel) Contractor shall have complete managerial control over its employees, and Contractor may dismiss, promote, replace or reassign a member of the Contractor Personnel; provided, however, that unless otherwise agreed to by Commonwealth, Contractor shall deliver a notice to

Commonwealth before or immediately after dismissing any member of the Contractor's Personnel. In addition, Contractor shall deliver to Commonwealth written notice of any criminal activities undertaken by, or alleged to have been undertaken by, any member of the Contractor Personnel and of which Contractor then has knowledge, which notice shall be delivered as promptly as is reasonable under the circumstances, and Contractor will cooperate fully with any investigation undertaken by or through Commonwealth in respect of such actual or alleged criminal activities.

Comment [A40]: To the extent permissible by law

f) **Conduct of Contractor Personnel**. While at the Commonwealth Services Locations and the Contractor Services locations, Contractor's personnel, subcontractors and agents (1) shall comply with all lawful requests, rules and regulations of Commonwealth regarding personal and professional conduct (including the wearing of a particular uniform, identification badge or personal protective equipment and adhering to security regulations and general safety practices or procedures) and (2) otherwise shall conduct themselves in a businesslike manner.

g) **Unsatisfactory Conduct**. If the Commonwealth determines in its sole discretion that a particular Contractor employee or subcontractor is not conducting himself or herself in an appropriate manner, Commonwealth may provide Contractor with notice of such conduct. Upon receipt of such notice, Contractor shall promptly investigate the matter and take appropriate action, which may include (1) removing the offending individual from the project and replacing him or her with a similarly qualified individual or (2) taking other appropriate disciplinary action to prevent a reoccurrence. In the event there are repeat violations of this *Section 17(g)* by a particular Contractor employee, contractor or subcontractor, Contractor shall promptly remove him or her from the project as set forth above.

h) **Confidentiality.** Contractor shall:

(1) Cause each Contractor Personnel to maintain and enforce the confidentiality provisions of the Contract both during and after their assignment to the Commonwealth account; and

(2) Enter into, or shall have entered into, an agreement with each Contractor Personnel member which assigns, transfers and conveys to Contractor all of such employee's right, title and interest in and to any materials created pursuant to the Contract, including all rights of patent, copyright, trade secret or other proprietary rights in and to such materials.

18. THIRD PARTY SERVICES

a) Commonwealth shall have the right, in its sole discretion, to contract with any number of third parties to perform Services which would otherwise fall within the

terms of this Contract. In the event Commonwealth contracts with a third party to perform any service on behalf of or for Commonwealth, Contractor, as part of the Services, shall cooperate with Commonwealth and such third party to the extent reasonably required by Commonwealth, including provision of (i) existing written requirements, standards and policies for systems operations so that the enhancements or developments of such third party may be operated by, and will be compatible with the operations of, Contractor, (ii) assistance and support services to such third party, and (iii) such access to the Systems as may be reasonably required by such third party (subject to all security standards, licenses, confidentiality restrictions and other standards and procedures then in effect at each of the Services Locations) to develop, test and deploy the service contracted for by Commonwealth. In addition thereto, Contractor shall not commit or permit any act which will unduly interfere with the performance of work by Commonwealth employees or any such third party, and Commonwealth will not commit or permit any act which will interfere with Contractor's performance of the Services. All additional out-of-scope support costs, excluding attorney fees, incurred by Contractor as a result of a Commonwealth contract with a third party will be handled in accordance with the Change Control Procedures.

Comment [A41]: Similar to the current contract, the right to contract with third parties should be limited to out-of-scope services The Commonwealth separately has the right to terminate the Contract for convenience

b) Throughout the Term, but not more than once every six months, Commonwealth may request that Contractor work together with Commonwealth and/or third parties to identify ways to achieve reductions in the cost of Service delivery and corresponding reductions in the price(s) quoted in the Contract. If so requested by Commonwealth, Contractor will, at its own expense, promptly prepare a detailed proposal identifying all viable means of achieving the desired reductions without (to the extent practically possible) adversely impacting business objectives or requirements identified by Commonwealth. Commonwealth shall not be obligated to accept or implement any such proposal.

19. COMPENSATION

In consideration of Contractor providing the Services, subject to the terms of this Contract, Commonwealth shall pay to Contractor the Fees as set out at *Schedule I* (Offeror Pricing Forms). All items shall be performed within the time period(s) specified in the Contract. The Contractor shall be compensated only for items supplied and performed to the satisfaction of the Commonwealth

Comment [A42]: Commonwealth should be based on the Contractor compliance with the obligations under this Contract

20. FEES

a) **Service Fees**. In consideration of Contractor providing the Services, subject to the terms of this Contract, Commonwealth shall pay to Contractor the Fees pursuant to *Schedule I* (Offeror Pricing Forms).

b) **Cost of Living Adjustment.** The Fees shall not be subject to any cost of living or inflationary adjustment or any other adjustment based on Contractor's costs to provide the Services.

c) **Expenses**. Except as expressly provided otherwise in this Contract, expenses of Contractor relating to the Services are included in the Fees, and no such expenses or other costs or fees shall be reimbursed by Commonwealth unless agreed to by Commonwealth in writing. The Contractor shall not be allowed or paid travel or per diem expenses unless agreed to by Commonwealth in writing.

d) **Pro-ration**. All periodic Fees or charges under this Contract are to be computed on a calendar month basis and shall be prorated on a per diem basis for any partial month.

e) **Unused Credits**. Any unused credits against future payments owed to either party by the other pursuant to this Contract shall be paid to the applicable party within forty-five (45) days after the expiration or termination for any reason of Contractor's obligation to provide the Services or of this Contract. This *Section 20(e)* shall survive the expiration or any termination of this Contract.

f) **Pricing Protection**. Notwithstanding anything to the contrary elsewhere in this Contract, the Fees shall in no event and at no time during the Term exceed Contractor's then lowest charges for such services to Contractor's state governmental customers generally receiving comparable goods and services at comparable volumes and upon material terms and conditions comparable to those contained in this Contract and pursuant to an outsourcing agreement dated after the Effective Date. Upon Commonwealth's request from time to time, and in any event on each anniversary of the Effective Date, Contractor shall advise Commonwealth in writing that this *Section 20(f)*has not been contradicted by any transaction entered into by Contractor on or after the Effective Date. If Contractor is unable to provide such written notice because of a transaction entered into by Contractor contradicting this *Section 20(f)*, Contractor shall offer to Commonwealth an adjustment to the Fees to correct such contradiction.

Comment [A43]: Similar to current contract, Contractor proposes pricing protection applies only to time & materials fees

21. PAYMENT SCHEDULE AND INVOICES

a) **Service Fees**. On or before the 15th day of each calendar month of the Term, Contractor shall provide Commonwealth with a single invoice for the Service Fees. Each such invoice shall include the Fees, if applicable, for the then current month, as well as any Service Level Credits then payable by Contractor or refundable by Commonwealth, or other reimbursable charges to Commonwealth for Services actually rendered prior to the date of such invoice.

b) **Detailed Invoices.** Contractor shall provide on the monthly invoices varying degrees of detail (e.g., per agency, end-user, department, project, site) as specified in *Schedule H* (Commonwealth Computing Procedures Manual). The Detailed Invoice will be delivered both in an electronic format compatible with the

Commonwealth's Invoice Processing System and a summary Invoice will be delivered for Management and Budgeting Purposes.

c) **Time of Payment**. Any sum due Contractor pursuant to any such invoice shall be due and payable on the last business day of the calendar month following the calendar month during which such invoice was delivered to Commonwealth. (e.g., an invoice delivered to Commonwealth on July 15, 2015 will be due and payable on August 31, 2015, the last business day of August, 2015.) In the event any invoices remain unpaid after such due date, the Commonwealth may pay interest as determined by the Secretary of Budget in accordance with Act No. 266 of 1982 and regulations promulgated pursuant thereto. Contractor shall continue to provide the Services even in the event payment is delayed or is not made in timely fashion.

Comment [A44]: Contractor proposes this provision to be adjusted to the current contract language

Comment [A45]: Contractor proposes this to be subject to Section 32 (f)

d) **Fee Dispute**. During the pendency of a dispute between Commonwealth and Contractor pursuant to which Commonwealth, in good faith, believes it is entitled to withhold, and does withhold, payment, Contractor shall continue to fully provide the Services and otherwise fully perform its obligations under this Contract.

Comment [A46]: Contractor proposes current contract language which includes limiting disputed amounts to 10% of the monthly invoice

22. INSPECTION AND ACCEPTANCE

Comment [A47]: Contractor proposes using the term Deliverables instead of Services within this Section 22

a) Acceptance of Services related to transition will occur in accordance with the Acceptance Criteria set out in *Schedule D* (Transition Milestones) and the Detailed Transition Plan.

b) Acceptance of Services other than those related to transition will occur in accordance with the Commonwealth Computing Procedures Manual.

c) If the Services are in compliance with the specifications, then the Commonwealth shall provide the Contractor with Commonwealth's written conditional acceptance of the Services. If the Services are not in compliance with the specifications, then the Commonwealth shall provide the Contractor with Commonwealth's written rejection of the Service. Payment will only be made if the Commonwealth has accepted the Service through written acceptance.

d) If the Services do not meet an accessibility standard as set out in ITB-ACC001, the Contractor must provide written justification for its failure to meet the standard. The justification must provide specific details as to why the standard has not been met. The Commonwealth may either waive the requirement as not applicable to the Commonwealth's business requirements or require that the Contractor provide an acceptable alternative. Any Commonwealth waiver of the requirement must be in writing.

e) Unless otherwise set forth in the Commonwealth Computing Procedures Manual (*Schedule H*), upon the Contractor's receipt of the Commonwealth's written notice of rejection, which must identify the reasons for the failure of the Services to comply with the Contract, the Contractor shall have fifteen (15) business days, or such other time as the Commonwealth and Contractor may agree is reasonable, within which to correct all such failures, and resubmit the corrected Services, certifying to the Commonwealth, in writing, that the failures have been corrected, and that the Services have been brought into compliance with the Contract. Upon receipt of such corrected and resubmitted Service and certification, the Commonwealth shall have thirty (30) business days to test the corrected Service to confirm that it is in compliance with the Contract. If the corrected Service is in compliance with the Contract, then the Commonwealth shall provide the Contractor with Commonwealth's acceptance of the Service.

f) If, in the opinion of the Commonwealth, the corrected Service still contains material failures, the Commonwealth may either:

(1) Repeat the procedure set forth above; or

(2) Terminate the Contract in accordance with *Section 32* (Termination).

23. SERVICE LEVELS

a) The Contractor shall comply with the procedures and requirements of *Schedule J.1* (Service Level Management), *Schedule J.2* (Datacenter Service Level Matrix), and *Schedule J.3* (Datacenter SLA Definitions) during the term of the Contract.

All Services without expressly defined Service Levels must be performed at least to the same degree of accuracy, completeness, efficiency, quality and timeliness as is provided by well-managed suppliers providing services similar to the Services, so long as such performance is operationally reasonable. For where there are expressly defined Service Levels, or where performance can be reasonably reported, Contractor will measure and report its performance against these standards on at least a monthly basis, except as may otherwise be agreed between the Parties in respect of Services performed less frequently than monthly.

Comment [A48]: Contractor proposes that a few SLA definition and targets are reviewed between the Commonwealth and Contractor to validate that these SLA targets are industry standard, which Contractor will commit to industry standard definitions and targets Also, J-1 should be reviewed at this time due to the interdependencies of Schedules J-1, J-2 and J-3

Comment [A49]: Contractor proposes that the Service Level terminology is generic and would like to discuss the purpose of this language as well as definition of each adjective

Comment [A50]: Contractor proposes deleting the language "or where performance can be reasonably reported"

b) The Commonwealth's acceptance of any Service Level Credit shall not bar or impair Commonwealth's rights and remedies in respect of the failure or root cause as set forth elsewhere in this Contract, including without limitation claims for liquidated damages, injunctive relief and termination rights, provided however, Service level Credits paid would be credited against any such claim for damages.

c) The Commonwealth's acceptance of any Service Level credit shall not bar or impair Commonwealth's rights and remedies in respect of the failure or root cause as set forth elsewhere in this Contract, including without limitation claims for damages, injunctive relief and termination rights, provided however, Service level credits paid would be credited against any such claim for damages.

24. LIQUIDATED DAMAGES

a) By accepting this Contract, the Contractor agrees to the delivery requirements of this Contract. If a Contract schedule is not met, including Transition Milestones set out in Transition Plan, the delay will interfere with the Commonwealth's program. In the event of any such delay, it would be impractical and extremely difficult to establish the actual damage for which the Contractor is the material cause. The Commonwealth and the Contractor therefore agree that, in the event of any such delay the amount of damage shall be the amount set forth in this *Section 24* and agree that the Contractor shall pay such amount as liquidated damages, not as a penalty.

Comment [A51]: Contractor suggests changing "will" to "may" as the delay may not interfere

b) The amount of liquidated damages for failure to meet Transition Milestones is set forth in *Schedule D* (Transition Milestones).

c) If, *Schedule D* (Transition Milestones) indicates that Contractor may earn back liquidated damages, then Contractor shall have the time specified in *Schedule D* (Transition Milestones), as indicated, to meet the Acceptance Criteria for the Transition Milestone and earn back the Milestone Credit. If Contractor fails to meet the Acceptance Criteria within 30 days following the Milestone Due Date or, if an earn back period is specified, then 30 days following the end of the specified earn back period, the Commonwealth, at no additional expense and at its option, may either:

Comment [A52]: Contractor proposes that failure must be material

(1) Immediately terminate the Contract and all software, documentation, reports, Developed Materials and any other materials provided for or created for the Commonwealth as a result of this Contract shall be given to the Commonwealth, and the Commonwealth shall be entitled to its remedies under Subsection 24(c); or

(2) Order the Contractor to continue with no decrease in effort until the work is completed in a manner acceptable to the Commonwealth or until the Commonwealth terminates the Contract. If the Contract is continued, the liquidated damages will also continue until the work is completed.

d) Liquidated damages shall be paid by the Contractor and collected by the Commonwealth by deducting them from the invoices submitted under this Contract or any other contract Contractor has with the Commonwealth, by

collecting them through the performance security, if any, or by billing the Contractor as a separate item.

e) To the extent that the delay is caused by the Commonwealth, as described in *Schedule D* (Transition Milestones), no liquidated damages will be applied.

Comment [A53]: Contractor proposes adding "or its third party contractors or agents"

f) Contractor shall not be liable for liquidated damages if the delay to the Contract arises out of causes beyond the control of and without the fault or negligence of the Contractor and/or its subcontractors. Such causes may include, but are not limited to, acts of God or of the public enemy, fires, floods, epidemics, quarantine restrictions, strikes, work stoppages, freight embargoes, acts of terrorism, and unusually severe weather; but in every case, the delay must be beyond the control of, and without the fault or negligence of, the Contractor and/or its subcontractors. The Contractor shall notify the Commonwealth immediately in writing of its inability to perform because of a cause beyond the control of the Contractor.

g) If the delays are caused by the default of a Subcontractor, and if such default arises out of causes beyond the control of both the Contractor and Subcontractor, and without their fault or negligence, the Contractor shall not be liable for liquidated damages for delays, unless the supplies or services to be furnished by the Subcontractor were obtainable from other sources in sufficient time to permit the Contractor to meet the required performance schedule.

25. CONTINUOUS IMPROVEMENT AND BENCHMARKING

a) **Benchmark Overview**. Prior to the expiration of the second anniversary of the Effective Date, Commonwealth and Contractor shall establish the details of the Benchmarking Process intended to ensure that Contractor provides Commonwealth with technology and Services Levels equal to or greater than other organizations receiving similar services. The parties acknowledge and agree that the benchmarking process is intended to assist Commonwealth in making decisions necessary to balance the desire for then current technology against the cost and uncertain performance of newly evolving technology.

b) **Benchmarker**. The Benchmark shall be conducted by a Benchmarker selected by the Commonwealth, subject to Contractor's approval thereof, in writing, such approval not to be unreasonably withheld, delayed or conditioned. The fees and expenses charged by the Benchmarker shall be paid by Commonwealth. Contractor shall at its expense cooperate with and assist the Benchmarker and any other third parties involved in the Benchmarking process, including meeting with Commonwealth and the Benchmarker before and throughout the Benchmarking Process and providing data relating to the provision of the Services, as requested by Commonwealth or the Benchmarker.

c) **Benchmark**. If Commonwealth undertakes the Benchmarking, Commonwealth and Contractor, in good faith, shall attempt to agree upon the period during which the Benchmarking shall be conducted. If the parties are unable to so agree, Commonwealth shall specify the relevant period, subject to Contractor's approval thereof, in writing, such approval not to be unreasonably withheld, delayed or conditioned.

d) **Benchmark Information**. Commonwealth and Contractor shall jointly determine the Benchmark Information with appropriate input from the Benchmarker. Commonwealth and Contractor shall (1) review the Benchmark Information, and (2) schedule a meeting to address any issues either party may have with the Benchmark Information. Contractor shall provide the Benchmark Information at no additional cost to Commonwealth; provided, however, that if Commonwealth wishes the Benchmarker to use information which Contractor does not otherwise have access to in the course of its business, Commonwealth shall provide such information at its own cost and Contractor may use such information but, unless Commonwealth expressly agrees otherwise in writing, only in connection with providing the Services.

e) **Benchmarking Results**. Within thirty (30) days after the completion of Benchmarking, the Benchmarker shall deliver the Benchmark Results to the Commonwealth Project Manager and the Contractor Project Manager for distribution to the members of the Management Committee.

f) **Benchmark Results Review Period and Adjustments**. The members of the Management Committee shall utilize the Benchmark Review Period to review such Benchmark Results, and the Management Committee shall meet during the Benchmark Review Period to collectively assess the Benchmark Results.

g) **Disputes of Benchmark Results**. Either Commonwealth or Contractor may in good faith dispute the Benchmark Results, in writing, prior to the expiration of the Benchmark Review Period. Any such notice of dispute issued by either party shall include a description of the nature of such dispute in sufficient detail so as to enable the Benchmarker and the other party to assess the motive and merit of the dispute. Within ten (10) days after receipt of such notice, the parties shall cause the Benchmarker to issue a written response addressing the dispute, and if such dispute requires a change to any of the Benchmark Results, the Benchmarker shall be directed to issue revised Benchmark Results. Upon issuing such revised Benchmark Results, Commonwealth and Contractor, as applicable, shall have another Benchmark Review Period to review the revised Benchmark Results in accordance with *Section 25(f)*. In the event either party disputes the revised Benchmark Results within the second Benchmark Review Period or if the parties are unable to agree as to the need for revised Benchmark Results, original Benchmark Results or the revised Benchmark Results, as the case may be, shall be subject to the contract controversy procedures set forth in *Section 34* (Contract Controversies).

h) **Benchmarking: Price Protection**. In addition to the Benchmarking provided for in this *Section 25* (Continuous Improvement and Benchmarking), no earlier than sixty (60) days after the end of Year 2 of this Contract, and no more frequently than annually thereafter, the Commonwealth may engage a Benchmarker, in accordance with the provisions of this *Section 25* (Continuous Improvement and Benchmarking) for the purpose of assessing the extent to which the prices paid for the Services hereunder are comparable to prices of a comparable reference group of clients for Services. This Benchmarking Price Protection process shall be an objective measurement and comparison process utilizing baseline methods and industry standards. The parties acknowledge and agree that this Benchmarking Price Protection process is intended to assure the Commonwealth that pricing and pricing models employed in this engagement are consistent with the reference group throughout the later years of the Contract, as it may be extended or renewed.

Comment [A54]: As per existing contract, Contractor proposes this should be limited to bi-annually

i) **Benchmark: Pricing Adjustments**. If the results of a Benchmarking Price Protection analysis, as reflected in written Benchmarking Results delivered to Contractor, reveal that amounts to be paid under the terms of the Contract for Services exceed by a factor of ten percent (10%) or more than the average of amounts paid by the reference group for comparable services (the "Market Rate"), the Commonwealth may elect to renegotiate those prices. When notified of the Commonwealth's intent to renegotiate the prices, the Contractor shall, as soon as practical following notification of the Commonwealth's intent, negotiate in good faith with Commonwealth for the adjustment and reduction of fees for the Services. If an agreement is reached for a pricing adjustment such agreement will be effective as of the date of delivery of the Benchmarking (Price Protection) Results. If the parties are unable to agree to a pricing adjustment within sixty (60) days after delivery of the Benchmarking (Price Protection) Results, the matter shall be submitted to the various dispute resolution procedures contained in *Section 34* (Contract Controversies) of the Contract. If the dispute resolution procedure results in a pricing adjustment, that adjustment will be effective as of the date of delivery of the Benchmarking (Price Protection) Results. In no event will Contractor increase the Fees as a result of any review pursuant to this *Section 25* (Continuous Improvement and Benchmarking).

j) **Annual Best Practices Reviews.** Within thirty (30) days of each anniversary of the Effective Date, Contractor shall, in accordance with procedures agreed upon by the Commonwealth Project Manager and the Contractor Project Manager, identify for Commonwealth any best practices that have emerged (within Contractor's organization or, to the knowledge of Contractor, within the processing services outsourcing market generally), that, if implemented by the Contractor would materially benefit the Commonwealth in terms of price reductions or performance improvement. If requested by Commonwealth, within sixty (60) days Contractor shall provide Commonwealth with proposals

for the implementation of such best practices in a manner consistent with the Change Control Procedures of the Contract. If approved by Commonwealth, Contractor shall implement such best practices on behalf of Commonwealth as expeditiously as possible.

26. GOVERNANCE

Provisions for the governance of this Contract and the Services delivered pursuant hereto are set forth in *Schedule B* (Governance) to this Contract.

27. CHANGE CONTROL

a) Change Control Procedures. The following Change Control Procedures will apply if either party wishes to implement or have Contractor implement a Change. The requesting Party will forward to the other party a Change Order which will include the following:

(1) Project identification
(2) Originator's name and title
(3) The date of the Change Order
(4) A description of the proposed change
(5) The reason for the proposed change

For Contractor, all Change Orders must be directed to Contractor's Project Manager. For Commonwealth, all Change Orders must be directed to or originate from the Commonwealth Project Manager.

(1) For any Contractor-initiated Change Order, Commonwealth shall have the option of accepting or rejecting that Change Order.

(2) Contractor will assign a number to and log each Change Order.

(3) All Change Orders will be categorized by Commonwealth as Priority 1 (urgent), Priority 2 (ordinary) or Priority 3 (low).

(4) Contractor will make reasonable efforts to investigate the impact of the Change Order on the Fees, timetable, specifications, Services, Service Levels, terms and conditions and, the relative obligations of the parties under this Contract and the (the "Impact Study") in accordance with a schedule that reflects the applicable priority category.

(5) Contractor will inform Commonwealth if there will be any charges for Contractor Services in conducting the Impact Study and Commonwealth will decide whether Contractor should conduct the Impact Study. Contractor shall be entitled hereunder to charge Commonwealth only for those expenses incurred by Contractor in

connection with the conduct of the Impact Study that are (i) Contractor's out-of-pocket expenses paid by Contractor to third parties (other than Contractor's or any Contractor's Agent's employees) for expertise not otherwise possessed by or available to Contractor or (ii) for employees of Contractor or any Contractor Agent not theretofore engaged in the provision of the Services. In order for any of the foregoing expenses to be reimbursable to Contractor, Contractor must first provide an estimate thereof to Commonwealth and obtain from Commonwealth its prior written approval thereof. If Contractor provides any such estimate and Commonwealth does not approve the estimated expenses, Contractor shall not be obligated to proceed with the Impact Study. In all cases, Contractor shall make a good faith effort to maximize its use of its employees and the employees of Contractors Agents then engaged in the provision of the Services to the extent Contractor can do so without adversely affecting its ability to provide the Services in accordance with the Services Levels. Any disputes between the parties regarding the validity, estimated amount or actual amount of any reimbursable expenses shall be subject to the dispute resolution provisions of *Section 34* (Contract Controversies).

(6) If both parties agree on the Impact Study and any necessary Changes to the Services, the relative obligations of the parties under this Contract, and the Fees, a Change Order will be issued to reflect the agreed to Changes.

(7) If the parties cannot agree upon the Impact Study or the resultant Changes to this Contract, any Commonwealth-initiated Change Order will nevertheless be implemented at Commonwealth's option and Contractor shall perform the Services, and either party may elect to have all outstanding related matters treated as a dispute between the parties under *Section 34* (Contract Controversies). During the pendency of any such dispute, Commonwealth shall pay to Contractor any undisputed amounts. Any changes to Service Levels which are required by the implementation of the Changes, will be reflected in the Change Order that is issued.

Comment [A55]: Contractor proposes to discuss the scenario where the dispute is regarding the price of the change order

b) All Changes shall be made pursuant to the Change Control Procedures. Contractor shall:

(1) schedule all Changes so as not to interrupt or unduly interfere with Commonwealth's operations,

(2) prepare and deliver to Commonwealth each month a ninety-day rolling schedule for ongoing proposed and approved and planned Changes,

(3) review and determine the cause of any failed Changes and deviations from scheduled Changes, and

(4) document and provide to the Management Committee and to the Commonwealth Project Manager, individually, same-day notification (which may be given orally provided that such oral notice is confirmed in writing to such persons within three (3) Commonwealth business days) of all changes performed on an emergency basis to maintain the continuity of the Services.

c) Without limiting any other provision of this Contract, the following Schedules may be modified through the Change Control Procedures set forth in this *Section 27* (Change Control):

- Schedule C – Services Catalog
- Schedule E – Datacenter Locations
- Schedule G – Staffing Plan and Key Positions
- Schedule J.1 – Service Level Management
- Schedule J.2 – Datacenter Service Level Matrix
- Schedule J.3 – Datacenter SLA Definitions
- Schedule H – Commonwealth Computing Procedures Manual

28. NOTICE OF DELAYS

Whenever the Contractor encounters any difficulty that delays or threatens to delay the timely performance of this Contract (including actual or potential labor disputes), the Contractor shall immediately give notice thereof in writing to the Commonwealth stating all relevant information with respect thereto. Such notice shall not in any way constitute a basis for an extension of the delivery schedule or be construed as a waiver by the Commonwealth of any rights or remedies to which it is entitled by law or pursuant to provisions of this Contract. Failure to give such notice, however, may be grounds for denial of any request for an extension of the delivery schedule because of such delay. If an extension of the delivery schedule is granted, it will be done consistent with *Section 27*(Change Control).

29. NOTICE

Any written notice to any party under this Contract shall be deemed sufficient if delivered personally, or by facsimile, telecopy, electronic or digital transmission (provided such delivery is confirmed), or by a recognized overnight courier service (e.g., DHL, Federal Express, etc.), with confirmed receipt, or by certified or registered United States mail, postage prepaid, return receipt requested, sent to the address such party may designate by notice given pursuant to this section.

30. DEFAULT

Comment [A56]: Contractor proposes deleting section 30 as Defaults are already covered in section 32 (c)

a) The Commonwealth may, subject to the provisions of *Section 28* (Notice of Delays), and in addition to its other rights under the Contract, declare the Contractor in default by written notice thereof to the Contractor, and terminate for cause (as provided in *Section 32* (Termination) the whole or any part of this Contract and shall further have the right to seek damages from Contractor for any of the following reasons:

(1) Failure to begin work within the time specified in the Contract or as otherwise specified;

(2) Failure to successfully complete a Major Milestone in accordance with the agreed Transition or Transition Plans or to complete specified work in accordance with the Contract terms;

(3) Multiple failures over time of a single Service Level or a pattern of failure over time across multiple Service Levels (a Service Level Termination Event); this will include failures of Service Levels and Key Service Levels;

(4) Failure to make agreed-upon adjustments to the fees or Service Levels in accordance with the outcome of Benchmarking Procedures;

(5) Failure or refusal to remove material, or remove and replace any work rejected as defective or unsatisfactory;

(6) Abandonment or willful refusal to provide the Services or any part of the Services;

(7) Failure to perform its responsibilities under any Business Continuity or Disaster Recovery Plans, including such Business Continuity or Disaster Recovery Plans that apply to Contractor's own locations used for the delivery of the Services;

(8) Insolvency or bankruptcy;

(9) Assignment made for the benefit of creditors;

(10) Failure or refusal within 30 days after written notice by the Contracting Officer, of the Contractor to make payment or show cause why payment should not be made, of any amounts due for materials furnished, labor supplied or performed, for equipment rentals, or for utility services rendered;

(11) Failure to protect, to repair, or to make good any damage or injury to property as required under the terms of this Contract;

(12) Breaches of covenants, agreements, obligations, representations or warranties in the Contract occurring simultaneously or over time, whether or not each such breach is a material breach, and whether or not each such breach was cured, that taken together constitute a material breach of the Contract after Contractor has been made aware of such breaches, on an individual basis. Regardless of any other provision in this Contract to the contrary no cure period is available to Contractor should the Commonwealth terminate under this *Section 30(a)(12)*;

(13) An act or omission of Contractor in the performance of this Contract, which is not otherwise explicitly required or permitted under this Contract, and which results in any Regulatory Entity notifying Commonwealth that it is subjecting the Commonwealth to a hearing or tribunal or withdrawing any license granted to Commonwealth or Contractor and such hearing, tribunal or withdrawal would have a material and adverse effect on Commonwealth's operations or business or the Services. Regardless of any other provision in this Contract the contrary no cure period is available to Contractor should the Commonwealth terminate under this *Section 30(a)(13)*;

b) In the event that the Commonwealth terminates this Contract in whole or in part as provided in Subparagraph (a) above, the Commonwealth may procure, upon such terms and in such manner as it determines, services similar or identical to those so terminated, and the Contractor shall be liable to the Commonwealth for any reasonable excess costs for such similar or identical services included within the terminated part of the Contract.

c) If the Contract is terminated as provided in Subparagraph (a) above, the Commonwealth, in addition to any other rights provided in this *Section 30* (Default), may require the Contractor to transfer title and deliver immediately to the Commonwealth in the manner and to the extent directed by the Commonwealth, such partially completed work, including, where applicable, reports, working papers and other documentation, as the Contractor has specifically produced or specifically acquired for the performance of such part of the Contract as has been terminated. Except as provided below, payment for completed work accepted by the Commonwealth shall be at the Contract price. Except as provided below, payment for partially completed work including, where applicable, reports and working papers, delivered to and accepted by the Commonwealth shall be in an amount agreed upon by the Contractor and the Commonwealth. The Commonwealth may withhold from amounts otherwise due the Contractor for such completed or partially completed work, such sum as the Commonwealth determines to be necessary to protect the Commonwealth against loss.

d) The rights and remedies of the Commonwealth provided in this *Section 30* (Default) shall not be exclusive and are in addition to any other rights and remedies provided by law or under this Contract.

e) The Commonwealth's failure to exercise any rights or remedies provided in this *Section 30* (Default) shall not be construed to be a waiver by the Commonwealth of its rights and remedies in regard to the event of default or any succeeding event of default.

f) Following exhaustion of the Contractor's administrative remedies as set forth in *Section 34* (Contract Controversies), the Contractor's exclusive remedy shall be to seek damages in the Board of Claims.

31. STEP-IN RIGHTS

a) In the event that Contractor is failing to deliver all or part of the Services, the Commonwealth shall give the Contractor notice of the failure. The Contractor shall have fifteen (15) days to provide the Commonwealth with a correction plan. If the correction plan is not received within fifteen (15) days or the failure is not corrected within thirty (30) days of the notice provided under this paragraph, Commonwealth may assign Commonwealth staff or third parties to step-in and perform failing elements of the Services, to the extent those Services are listed below, until such time as Contractor can demonstrate the ability to resume provision of such Services. Provided, however, that if in the Commonwealth's sole discretion the failure creates an emergency, no notice is required for the Commonwealth to exercise its rights under this paragraph.

(1) Co-location services;
(2) Management of Commonwealth owned equipment located within the Enterprise Data Center;
(3) Network Connectivity between the Commonwealth and the Contractor's datacenter(s); and
(4) Disaster Recovery Services.

b) All costs associated with the exercise of such step-in rights shall be borne by Contractor.

c) Commonwealth's exercise of its step-in rights shall not constitute a waiver by Commonwealth of any termination rights or rights to pursue a claim for damages arising out of the failure that led to the step-in rights being exercised.

32. TERMINATION

(a) For Convenience

Comment [A57]: Contractor proposes additional language to clearly state length of time, and minimal financial impacts required by both parties and the achievements required for the step out to occur

Comment [A58]: Propose additional conversation of the activities for step in for Co-location services and Disaster Recovery Services as these activities could be in a shared facility

(1) The Commonwealth may terminate this Contract without cause by giving Contractor thirty (30) calendar days prior written notice (Notice of Termination) whenever the Commonwealth shall determine that such termination is in the best interest of the Commonwealth (Termination for Convenience). Any such termination shall be effected by delivery to the Contractor of a Notice of Termination specifying the extent to which performance under this Contract is terminated either in whole or in part and the date on which such termination becomes effective.

In the event of termination hereunder, Contractor shall receive payment for the following:

(i) all Services performed consistent with the terms of the Contract prior to the effective date of termination;

(ii) all actual and reasonable costs incurred by Contractor as a result of the termination of the Contract; and

In no event shall the Contractor be paid for any loss of anticipated profit (by the Contractor or any Subcontractor), loss of use of money, or administrative or overhead costs.

Failure to agree on any termination costs shall be a dispute handled in accordance with *Section 34* (Contract Controversies) of this Contract.

(2) The Contractor shall cease Services as of the date set forth in the Notice of Termination, and shall be paid only for such Services as have already been satisfactorily rendered up to and including the termination date set forth in said notice, or as may be otherwise provided for in said Notice of Termination, and for such services performed during the thirty (30) calendar day notice period, if such services are requested by the Commonwealth, for the collection, assembling, and transmitting to the Commonwealth of at least all materials, manuals, magnetic media, studies, drawings, computations, maps, supplies, and survey notes including field books, which were obtained, prepared, or developed as part of the Services required under this Contract.

(3) The above shall not be deemed to limit the Commonwealth's right to terminate this Contract for any reason as permitted by the other provisions of this Contract, or under applicable law.

(b) Non-Appropriation

Any payment obligation or portion thereof of the Commonwealth created by this Contract is conditioned upon the availability and appropriation of funds. When funds (state or federal) are not appropriated or otherwise made available to

Comment [A59]: As consistent with current Contract, Contractor suggests 180 day prior written notice

Comment [A60]: Contractor proposes partial termination will result in a separate termination fee schedule and will require further clarification of scope

Comment [A61]: Contractor proposes a termination fee schedule to be included in the contract

support continuation of performance in a subsequent fiscal year period, the Commonwealth shall have the right to terminate the Contract. The Contractor shall be reimbursed in the same manner as that described in this section related to Termination for Convenience to the extent that appropriated funds are available.

(c) Default

The Commonwealth may, in addition to its other rights under this Contract, terminate this Contract in whole or in part by providing written notice of default to the Contractor if the Contractor materially fails to perform its obligations under the Contract and does not cure such failure within thirty (30) days or, if a cure within such period is not practical, commence a good faith effort to cure such failure to perform within the specified period or such longer period as the Commonwealth may specify in the written notice specifying such failure, and diligently and continuously proceed to complete the cure. The Contracting Officer shall provide any notice of default or written cure notice for Contract terminations.

(1) Subject to *Section 36* (Limitation of Liability) of this Contract, in the event the Commonwealth terminates this Contract in whole or in part as provided in this Subsection 32(c), the Commonwealth may procure services similar to those so terminated, and the Contractor, in addition to liability for any liquidated damages, shall be liable to the Commonwealth for the difference between the Contract price for the terminated portion of the services and the actual and reasonable cost (but in no event greater than the fair market value) of producing substitute equivalent services for the terminated services, provided that the Contractor shall continue the performance of this Contract to the extent not terminated under the provisions of this section.

(2) Except with respect to defaults of Subcontractors, the Contractor shall not be liable for any excess costs if the failure to perform the Contract arises out of causes beyond the control of the Contractor. Such causes may include, but are not limited to, acts of God or of the public enemy, fires, floods, epidemics, quarantine restrictions, strikes, work stoppages, freight embargoes, acts of terrorism, and unusually severe weather. The Contractor shall notify the Commonwealth Contracting Officer promptly in writing of its inability to perform because of a cause beyond the control of the Contractor.

(3) Nothing in this *Subsection 32(c)* shall abridge the Commonwealth's right to suspend, debar, or take other administrative action against the Contractor.

Comment [A62]: Contractor proposes the termination should be mutual and limited to material breach of the agreement

Comment [A63]: Contractor recommends cure period of 45 days as is in the current contract

(4) If it is later determined that the Commonwealth erred in terminating the Contract for default, then the Contract shall be deemed to have been terminated for convenience under Subsection (a).

(5) If this Contract is terminated as provided by this Subsection 31(c), the Commonwealth may, in addition to any other rights provided in this Subsection, and subject to *Section 40* (Proprietary Rights) of this Contract, require the Contractor to deliver to the Commonwealth in the manner and to the extent directed by the Contracting Officer, such reports and other documentation as the Contractor has specifically produced or specifically acquired for the performance of such part of the Contract as has been terminated. Payment for such reports and documentation will be made consistent with the Contract.

(d) In the event that Contractor becomes insolvent for any reason whatsoever, or makes an assignment for the benefit of creditors, or has a receiver appointed, or if it is declared as bankrupt under the laws of the United States, or if a petition of reorganization or rearrangement is filed against it under the bankruptcy laws, Commonwealth shall have the exclusive option of continuing with Contractor or its successors or assigns or trustee in bankruptcy under the terms and conditions of this Contract for the full remaining term of this Contract, or continuing with Contractor or its successors or assigns or trustee in bankruptcy under the terms and conditions of this Contract for such period of time as is necessary or desirable to terminate this Contract.

(e) In the event of the sale by Contractor of all or substantially all of its assets (in a single transaction or a series of related transactions) or the sale of a controlling interest in Contractor's outstanding stock, Contractor shall be entitled to assign this Contract to its successor upon written notice thereof to Commonwealth. Commonwealth shall be entitled to receive from Contractor, upon Commonwealth's request, such information as is reasonably requested by Commonwealth to enable Commonwealth to assess the financial, technical and management capabilities of such successor to assume Contractor's obligations under this Contract. If Commonwealth determines, in the exercise of its reasonable discretion, that such successor does not or may not have such requisite financial, technical or management capabilities, and if Commonwealth informs Contractor thereof in writing and describing in reasonable detail its basis therefore, then, and only then, such assignment by Contractor shall be subject to Commonwealth's prior written consent, which consent may be withheld, delayed or conditioned in Commonwealth's sole discretion. If Commonwealth withholds such consent, then Commonwealth shall have the exclusive option of continuing under the terms and conditions of this Contract with Contractor or its successors or assigns for the full remaining term of this Contract, or continuing under the terms and conditions of this Contract with Contractor or its successors or assigns for such period of time as is necessary or desirable to terminate this Contract.

Comment [A64]: Contractor suggests using language in current contract where Termination Fees should be payable if Commonwealth elects to terminate for anything other than non-appropriation

(f) In the event Commonwealth fails to pay undisputed Fees for twelve (12) consecutive months, Contractor may terminate this Contract for its convenience. In such event, notwithstanding any other provision of this Contract to the contrary, Contractor shall be released from any obligation to provide further Services pursuant to this Contract.

(g) The rights and remedies of the Commonwealth provided in this Section shall not be exclusive and are in addition to any other rights and remedies provided by law or under this Contract.

(h) The Commonwealth's failure to exercise any rights or remedies provided in this Section shall not be construed to be a waiver by the Commonwealth of its rights and remedies in regard to the event of default or any succeeding event of default.

(i) In no event shall the Contractor be paid for any loss of anticipated profit (by the Contractor or any Subcontractor), loss of use of money, or administrative or overhead costs. Any dispute regarding termination costs shall be a dispute handled in accordance with *Section 34* (Contract Controversies) of this Contract.

(j) Following exhaustion of the Contractor's administrative remedies as set forth in *Section 34* (Contract Controversies), the Contractor's exclusive remedy shall be to seek damages in the Board of Claims.

Comment [A65]: Contractor suggests using current contract language and stating 9 months rather than 12

Comment [A66]: Contractor proposes this subsection is made mutual as well as (h)

Comment [A67]: Based on Contractors proposal in subsection 32(g) that remedies should be non-exclusive, this subsection (j) would be deleted

33. TERMINATION ASSISTANCE

a) **General.** Upon the Commonwealth's request, Contractor shall provide Termination Assistance Services directly to the Commonwealth, or to any replacement provider designated by the Commonwealth, any successors or assigns of such entities or any of their designee(s). Contractor shall take all necessary and appropriate actions to accomplish a complete, timely, and seamless transition of any Terminated Services from Contractor to the Commonwealth, or to any replacement provider designated by the Commonwealth, without material interruption of or material adverse impact on the Terminated Services or any other services provided by third-parties or Services that Contractor shall continue to provide (each transition, an "Assistance Event"). Contractor shall cooperate with the Commonwealth and any new Contractor and otherwise promptly take all steps required or reasonably requested to assist the Commonwealth in effecting a complete and timely Termination Assistance Services of any Terminated Services. Contractor shall provide all information regarding the Terminated Services or as otherwise needed for Termination Assistance Services, including data conversion, interface specifications, and related professional services. Contractor shall provide for the prompt and orderly conclusion of all Terminated Services, as the Commonwealth may direct, including completion or partial completion of projects, documentation of work in process, and other measures to assure an orderly transition to the Commonwealth or the Commonwealth's designee. Contractor's obligation to provide the Services shall not cease until a Assistance Event satisfactory to the Commonwealth,

including the performance by Contractor of all asset-transfers and other obligations of Contractor provided in this *Section 33* (Termination Assistance), has been completed in accordance with mutually agreed to completion or acceptance criteria or if no agreed acceptance criteria exist, then to the Commonwealth's reasonable satisfaction.

(i) **Period of Provision**. Contractor shall provide Termination Assistance Services commencing on the date a determination is made by the Commonwealth that there shall be an Assistance Event**.**

(ii) **Notice of an Assistance Event.** The Commonwealth will provide Contractor with written notice of an Assistance Event. Such notice will include a description of the Services that are to be terminated or discontinued, the affected Commonwealth Agencies, and the anticipated effective date of the Assistance Event. The Commonwealth may modify or update any of the information provided in the initial notice of an Assistance Event from time to time by a supplemental notice from the Commonwealth to Contractor.

(iii) **Extension of Services**. The Commonwealth may elect, upon thirty (30) days prior notice to Contractor, to extend the period for performance of Termination Assistance Services (in whole or in part), in its sole discretion, provided that the total of all such extensions shall not result in Termination Assistance Services being performed beyond twenty-four (24) months following the effective date of the applicable Assistance Event without Contractor's consent. In each case, if the Commonwealth provides less than thirty (30) days prior notice of an extension, Contractor shall nonetheless use reasonable efforts to comply with the Commonwealth's request and provide the requested Services.

(iv) **Firm Commitment**. Contractor shall provide Termination Assistance Services regardless of the reason for the Assistance Event

Comment [A68]: As stated in our current contract, Contractor would propose to include "If this Contract is terminated due to failure by Commonwealth to pay amounts owed hereunder, Commonwealth will pay monthly in advance for Termination Assistance Services "

(v) **Performance**. Contractor shall provide all Termination Assistance Services subject to and in accordance with the terms and conditions of this Contract. Contractor shall perform Termination Assistance Services with at least the same degree of accuracy, quality, completeness, timeliness, responsiveness and resource efficiency as it is or was required to provide the same or similar Services in accordance with this Contract. The quality and level of performance of Termination Assistance Services provided by Contractor shall continue to meet or exceed the Service Levels and shall not be degraded or deficient in any respect. Service Level Credits shall be assessed for any failure to meet Service Levels during any period in which Termination Assistance Services are provided. If any period for performing any Termination

Comment [A69]: Contractor proposes further discussion on SLAs during termination assistance as this will depend on the assistance being requested of Contractor as well as the Services provided by new vendor or Commonwealth

Assistance Services extends beyond the expiration or the effective date of any termination of this Contract, the provisions of this Contract shall remain in full effect for the duration of such period.

b) **Scope.** As part of the Termination Assistance Services, Contractor shall timely transfer the control and responsibility for Services previously performed by or for Contractor to the Commonwealth and/or its designee(s), and upon Commonwealth request, shall execute any documents reasonably necessary to effect such transfers. Contractor shall also provide any and all information and assistance requested by the Commonwealth required for:

(i) the Systems and processes associated with the Services to operate and be maintained and enhanced efficiently;

(ii) the Services to continue without interruption or adverse effect; and

(iii) the orderly transfer of the Services (or replacement or supplemental services) to the Commonwealth and/or its designee(s).

c) **General Support**. Contractor shall:

(i) assist the Commonwealth and/or its designee(s) in developing a written plan for the migration of the Services to the Commonwealth and/or its designee(s), which plan shall include (as requested by the Commonwealth) capacity planning, process planning, facilities planning, human resources planning, technology planning, telecommunications planning and other planning necessary to effect the transition,

(ii) perform programming and consulting services as requested to assist in implementing the transition plan,

(iii) train personnel designated by the Commonwealth and/or its designee(s) in the use of any processes or associated Equipment, Materials, Systems or tools used in connection with the provision of the Services as needed for such personnel to assume responsibility for performance of the Services,

(iv) provide a catalog of all processes, Materials, the Commonwealth Data, Equipment, Software, Third Party Contracts and tools used to provide the Services,

(v) provide machine readable and printed listings and associated documentation for source code for Software owned by the Commonwealth and source code to which the Commonwealth is entitled under this Contract and assist in its re-configuration,

(vi) provide technical documentation for Software used by Contractor to provide the Services as needed for continuing performance of the Services,

(vii) analyze and report on the space required for the Commonwealth Data and the Software needed to provide the Services,

(viii) assist in the execution of a parallel operation, data migration and testing process until the successful completion of the transition to the Commonwealth and/or its designee(s),

(ix) create and provide copies of the Commonwealth Data in the format and on the media requested by the Commonwealth and/or its designee(s),

(x) provide a complete and up-to-date, electronic copy of the Commonwealth Procedure Manual in the format and on the media requested by the Commonwealth and/or its designee(s) and

(xi) provide other technical and process assistance, documentation and information as requested by the Commonwealth and/or its designee(s).

d) **Personnel**.

(i) **List of Contractor Personnel**. Contractor shall promptly provide to the Commonwealth a list, organized by location, of the Contractor Personnel dedicated (fifty percent (50%) or more) to the performance of the Services that are implicated by each Assistance Event. Such list shall, subject to applicable privacy laws, specify each such Contractor Personnel's name, job title, compensation package, leave status, years of service and job responsibilities. The Commonwealth agrees not to disseminate the personally identifiable information contained in such list without Contractor's consent. Contractor shall not terminate, reassign or otherwise remove from the performance of the Services any such dedicated Contractor Personnel until after the end of the applicable Termination Assistance Services period.

~~(i)~~(ii) **Right to Hire**. The Commonwealth and/or its designee(s) shall be permitted, without interference (including through counter-offers) from Contractor (subject to *Section 33(d)(iii)* below), to meet with, solicit and hire, effective after the later of (i) the date of the Commonwealth's notice of an Assistance Event and (ii) the completion of the Termination Assistance Services requiring such Contractor Personnel, any Contractor Personnel dedicated to the performance of the Services during the twelve (12) month period prior to the date of the Commonwealth's notice of an Assistance Event who are implicated by that Assistance Event. Contractor hereby waives its rights, if any, under contracts with such Contractor Personnel restricting the ability of such Contractor Personnel to be recruited or hired by the Commonwealth

Comment [A70]: Contractor proposes that the Contractor will provide the CCPM based on the then existing format and media

Comment [A71]: Proposed personnel who are solely dedicated rather than using 50% or more as a basis

Comment [A72]: Contractor proposes further discussion as personnel may not be required or may legitimately be subject to termination due to performance before end of Termination Assistance period

Comment [A73]: Contractor agrees as long as the deployment of the contractor assigned resource does not interfere with the contractors ability to continue to meet service obligations and service level requirements for service delivery to the commonwealth

and/or its designee(s) (including waiving any right to restrict such personnel via non-compete agreements or other contractual means). Contractor shall provide the Commonwealth and/or its designee(s) with reasonable assistance in their efforts to meet with, solicit and hire such Contractor Personnel, and shall give the Commonwealth and/or its designee(s) reasonable access to such Contractor Personnel for interviews, evaluations and recruitment. The Commonwealth shall endeavor, and shall cause its designee(s) to endeavor, to conduct the above-described activities in a manner that is not unnecessarily disruptive of Contractor's performance of its obligations under this Contract.

e) **Software and Developed Documentation**. The Contractor shall provide the Commonwealth with all Software and Developed Documentation as set forth in *Section 40* (Proprietary Rights).

f) **Equipment**.

(i) **List of Equipment**. Contractor shall promptly provide to the Commonwealth a list, organized by location, of the Equipment that is implicated by each Assistance Event. Such list shall specify information reasonably requested by the Commonwealth, including all fields tracked by Contractor in any asset management system used by Contractor for tracking and managing Equipment, such Equipment's function, manufacturer, model number, age, and other pertinent information.

(ii) **Right to Acquire**. The Commonwealth and/or its designee(s) shall have the right (but not the obligation) to purchase or assume the lease for any or all Equipment that is owned or leased by Contractor which is used in the provision of the Services and that is implicated by the relevant Assistance Event. Such Equipment shall be transferred in good working condition, reasonable wear and tear excepted, as of the later of the effective date of the relevant Assistance Event and the completion of the Termination Assistance Services requiring such Equipment. Contractor shall maintain such Equipment through the date of transfer so as to be eligible for the applicable manufacturer's maintenance program. In the case of Contractor-owned Equipment (including Equipment owned by Contractor Affiliates and Subcontractors and further including any such Equipment leased to Contractor), Contractor (or such Affiliate or Subcontractor) shall grant to the Commonwealth, and/or its designee(s) a warranty of title and a warranty that such Equipment is free and clear of all liens, security interests and other encumbrances. Such conveyance by Contractor (or Affiliate or Subcontractor) to the Commonwealth and/or its designee(s) shall be at fair market value (as shall be determined by an agreed-upon appraisal). At the Commonwealth's request, the Parties shall negotiate in good

Comment [A74]: Contractor proposes adding language stating that this should only be related to "solely" used for the Commonwealth

faith and agree upon the form and structure of the purchase. In the case of leased Equipment, Contractor shall (1) represent and warrant that the lease is not in default, (2) represent and warrant that all payments thereunder have been made through the date of transfer and (3) notify the Commonwealth and/or its designee(s) of any lessor defaults of which it is aware at the time.

g) **Third Party Contracts.** Contractor shall promptly, but no less than thirty (30) days from the Commonwealth's issuance of notice of an Assistance Event provide to the Commonwealth a list of the Third Party Contracts that are implicated by the relevant Assistance Event. Contractor shall, at the Commonwealth's request, cause the parties to such Third Party Contracts to permit the Commonwealth and/or its designee(s) to assume prospectively any or all such Third Party Contracts or to enter into new contracts with the Commonwealth and/or its designees on substantially the same terms and conditions, including price. Contractor shall transfer or assign those Third Party Contracts that the Commonwealth elects to assume prospectively to the Commonwealth and/or its designee(s) as of the later of the effective date of the relevant Assistance Event and the completion of the Termination Assistance requiring such Third Party Contracts. Such transfers or assignments shall be on terms and conditions acceptable to all applicable parties, provided that (A) there shall be no fee, charge or other amount imposed on the Commonwealth and/or its designee(s) by Contractor or the counter-parties to such Third Party Contracts for such transfer or assignment and (B) Contractor shall: (1) promptly cure and, in accordance with *Section 32(c)*, indemnify the Commonwealth against any default under such Third Party Contracts relating to the period prior to such transfer or assignment; (2) represent and warrant that all payments thereunder through the date of transfer or assignment are current; and (3) notify the Commonwealth and/or its designee(s) of any counter-party's default with respect to such Third Party Contracts of which it is aware at the time of such transfer or assignment.

Comment [A75]: Contractor will attempt however cannot guarantee third party contracts will accept this language

Contractor will request, with respect to any contracts applicable to Contractor Third Party Software being provided to Commonwealth and being used by Contractor to perform the Services, that the third party agree in writing that it will permit the assignment or transfer of the applicable agreement with Contractor to Commonwealth at the termination or expiration of this Contract. If any such third party refuses to provide such a written agreement, then Contractor will notify Commonwealth of this fact. Upon any such notification by Contractor, Commonwealth shall notify Contractor in writing whether Contractor may use such third party in connection with Contractor's performance of the Services. If Contractor is notified by Commonwealth that it must not use such third party services, then Contractor will make commercially reasonable efforts to locate an alternate third party provider, but Contractor is not responsible for any additional third-party costs that may result from using an alternate provider. If no alternate provider can be located by Contractor, Contractor will so notify Commonwealth and the parties, both acting in good faith and through their respective project

managers, will attempt to resolve the issue. The Contractor will not be responsible for any fees associated with the assignment or transfer of the license to the Commonwealth or for any breach by such third party of its agreement regarding the assignment or transfer.

h) **Other Subcontracts and Third Party Contracts**. With respect to Third Party Contracts implicated by the relevant Assistance Event that are not otherwise transferred or assigned to the Commonwealth and/or its designee(s) pursuant to *Section 33(g)*, Contractor shall make available to the Commonwealth and/or its designee(s), pursuant to reasonable terms and conditions, any third party services then being utilized by Contractor in the performance of the Services. Contractor shall retain the right to utilize any such third party services in connection with the performance of services for other Contractor customers. The Commonwealth shall retain the right to contract directly with any third party previously utilized by Contractor to perform any Services.

Comment [A76]: Contractor requires more discussion as we don't understand Commonwealth's intent with this section

i) **Rates and Charges**. Except as provided in this Subsection and *Section 33(j)*, Contractor shall provide all Termination Assistance Services at no additional charge. The Parties anticipate that Termination Assistance Services requested by the Commonwealth shall be provided by Contractor using Contractor Personnel already assigned to the performance of the Services and without adversely affecting Contractor's ability to meet its performance obligations. To the extent the Commonwealth requests that Contractor perform only a portion (but not all) of the Services included in a particular Fee, the amount to be paid by the Commonwealth shall be equitably adjusted downward in proportion to the portion of the Services that Contractor shall not be providing.

Comment [A77]: Contractor proposes to add language that if such services can't be provided using existing resources without affecting Contractor's ability to meet SLAs, Commonwealth will pay for such additional resources or Contractor has relief from SLAs

Comment [A78]: Contractor proposes that fees may be reduced however it will be based on then Services required rather than a pre-determined amount

j) **Proprietary Communications Network**. If Contractor uses a proprietary communications network to provide the Services, then for a period of up to two (2) years following the effective date of the relevant Assistance Event, Contractor shall, if requested by the Commonwealth, continue to provide such proprietary communications network and other network Services to the Commonwealth, the Commonwealth and/or its designee at the rates, and subject to the terms and conditions, set forth in this Contract.

k) **Resources.** Contractor shall maintain capability on at least thirty (30) days notice at all times during the Term to deploy all necessary resources to perform any Termination Assistance Services.

l) **Information.** At the Commonwealth's request, Contractor shall provide to and/or make available for the Commonwealth review, at Contractor's sole cost and expense, any and all reports, data and information that the Commonwealth deems necessary in order to evaluate all options related to an Assistance Event. Contractor shall provide all such reports, data and information regardless of whether the Commonwealth has provided notice of or otherwise declared an Assistance Event.

Comment [A79]: Contractor proposes that this subsection should apply to the information within Contactors possession only

Comment [A80]: Contractor proposes that if this is information in addition to steady state reports, Contractor should be paid for costs incurred

Breach. Contractor acknowledges and agrees that, upon any breach or threatened breach by Contractor of its obligations under this *Section 33* (Termination Assistance), Commonwealth shall be entitled to seek injunctive relief, including an order of specific performance. The provisions of this *Section 33* (Termination Assistance) will survive any expiration of the Term and any termination of this Contract.

34. CONTRACT CONTROVERSIES

a) All disputes between the parties arising under or relating to this Contract shall initially be referred in writing by either party to the Contractor Project Manager and the Commonwealth Project Manager. If the Contractor Project Manager and the Commonwealth Project Manager are unable to resolve the dispute within ten (10) Commonwealth business day(s) after referral of the matter to them or upon the earlier request by either the Contractor Project Manager or the Commonwealth Project Manager, the parties shall submit the dispute to the Management Committee for immediate review.

b) Within ten (10) Commonwealth business days after any dispute between the parties is submitted to the Management Committee pursuant to Subparagraph 30(a), the Management Committee shall meet for the purpose of attempting to resolve such dispute. At any meeting of the Management Committee at which more than one (1) dispute will be considered, Commonwealth may establish the order in which such disputes shall be addressed. If the Management Committee is unable to resolve a dispute within fifteen (15) Commonwealth business days after the date of the initial meeting of the Management Committee during which such dispute was considered, the Management Committee shall immediately notify Commonwealth and Contractor pursuant to Subparagraph 30(c).

c) In the event of a controversy or claim arising from the Contract that has not been resolved by the above process, the Contractor must, within six (6) months, file a written claim with the contracting officer for a determination. The claim shall state all grounds upon which the Contractor asserts a controversy exists

(1) The Commonwealth shall review timely-filed claims and issue a final determination, in writing, regarding the claim. The final determination shall be issued within 120 days of the receipt of the claim, unless extended by consent of the contracting officer and the Contractor. The Commonwealth shall send its written determination to the Contractor. If the Commonwealth fails to issue a final determination within the 120 days (unless extended by consent of the parties), the claim shall be deemed denied. The Commonwealth's determination shall be the final order of the purchasing agency.

Comment [A81]: Contractor proposes to be consistent to current contract the Contractor has a right to judicial review beyond the Board of Claims

(2) Within fifteen (15) days of the mailing date of the determination denying a claim or within one hundred thirty five (135) days of filing a claim if no extension is agreed to by the parties, whichever occurs first, the Contractor may file a statement of claim with the Commonwealth Board of Claims.

d) Each of Commonwealth and Contractor acknowledge that the provision of the Services is critical to the operations of Commonwealth. Accordingly, in the event of a dispute between Commonwealth and Contractor arising under or relating to this Contract, Contractor shall continue to provide the Services in accordance with the terms of this Contract during the pendency of the resolution of such dispute, including the final judicial resolution thereof by Commonwealth's Board of Claims or any appeal thereof, and Commonwealth shall compensate the Contractor pursuant to the terms of the Contract.

35. COMMONWEALTH HELD HARMLESS

Comment [A82]: Contractor proposes that this section be discussed with the Commonwealth to provide an indemnification section that is similar to our current Contract

a) The Contractor shall hold the Commonwealth harmless from and indemnify the Commonwealth against any and all third party claims, demands and actions based upon or arising out of any activities performed by the Contractor and its employees and agents under this Contract, provided the Commonwealth gives Contractor prompt notice of any such claim of which it learns. Pursuant to the Commonwealth Attorneys Act (71 P.S. § 732-101, et seq.), the Office of Attorney General (OAG) has the sole authority to represent the Commonwealth in actions brought against the Commonwealth. The OAG may, however, in its sole discretion and under such terms as it deems appropriate, delegate its right of defense. If OAG delegates the defense to the Contractor, the Commonwealth will cooperate with all reasonable requests of Contractor made in the defense of such suits.

b) Notwithstanding the above, neither party shall enter into any settlement without the other party's written consent, which shall not be unreasonably withheld. The Commonwealth may, in its sole discretion, allow the Contractor to control the defense and any related settlement negotiations.

36. LIMITATION OF LIABILITY

Comment [A83]: Contractor proposes that this section be discussed with the Commonwealth to include language that is similar to our current Contract For example, limitation of liability for direct damages is last 12 months charges, which is consistent with industry practice

a) The Contractor's liability to the Commonwealth under this Contract shall be limited to the value of the contract. This limitation will apply, except as otherwise stated in this *Section 36* (Limitation of Liability), regardless of the form of action, whether in contract or in tort, including negligence and whether related to direct, consequential, exemplary or punitive damages.

b) This limitation does not apply to damages for:

(1) Bodily injury

(2) Death;

(3) Intentional injury;

(4) Damage to real property or tangible personal property for which the Contractor is legally liable; or

(5) The Contractor's indemnity of the Commonwealth for patent, copyright, trade secret or trademark protection;

(6) Third party claims related to confidential or proprietary data misuse of confidential information or data;

(7) Milestone Credits, provided, however that payment will accrue against the cap;

(8) Commonwealth's losses resulting from Contractor's gross negligence, willful misconduct; or

(9) Contractor's costs incurred for notification, mitigation, and credit monitoring services required due to a security breach; or

(10) The Commonwealth costs, losses or damages incurred due to Personal Information being accessed, used, released, disclosed and/or acquired in an unauthorized manner while in the control of the Contractor; or

(11) Contractor's abandonment of any Services, wrongful termination of the Contract or willful refusal to provide Termination Assistance Services.

c) Except as provided for in *Section 36(c)(1) through (4)*, neither Party will be liable for indirect, incidental, special, consequential, exemplary or punitive damages arising out of or relating to the Contract :

(1) Additional costs to maintain the Services arising from a default by Contractor including the cost of work-arounds;

(2) Loss of or corruption to Commonwealth data including, without limitation, the cost and expense of rectification of the data arising out of a default (including for recovering, reconstructing, reformatting or reloading data), but only to the extent such damages arise out of the failure of Contractor to comply with its obligations under *Section 52* (Virus and Malicious Code);

(3) Expenditure or charges incurred by Commonwealth and rendered necessary as a result of a default by Contractor; and

(4) Any regulatory losses, fines, expenses or other losses suffered by Commonwealth as a result of Contractor's failure to comply with any law or regulation

37. CONFIDENTIALITY

a) For purposes of this Contract, *"Confidential Information"* of a party shall mean (1) with respect to Commonwealth, all Commonwealth Data and other information of Commonwealth or any Commonwealth agency or any private individual, organization or public agency, in each case to the extent such information and documentation is not permitted to be disclosed to third parties under local, Commonwealth or Federal laws and regulations or pursuant to any policy adopted by Commonwealth or pursuant to the terms of any third-party agreement to which Commonwealth is a party and (2) with respect to Contractor, all information identified in writing by Contractor as confidential or proprietary to Contractor, its subcontractors or licensors.

Comment [A84]: Contractor proposes using the current contract definition for Confidential Information as that definition is more complete

b) All Confidential Information relating to a party shall be held in confidence by the other party to the same extent and in at least the same manner as such party protects its own confidential or proprietary information. Neither party shall disclose, publish, release, transfer or otherwise make available any Confidential Information of the other party in any form to, or for the use or benefit of, any person or entity without the other party's consent. Subject to the other provisions of this Contractor, each party shall, however, be permitted to disclose relevant aspects of the other party's Confidential Information to its officers, agents, subcontractors and employees and to the officers, agents, subcontractors and employees of its corporate affiliates or subsidiaries to the extent that such disclosure is reasonably necessary for the performance of its duties and obligations under this Contract; provided, however, that such party shall take all reasonable measures to ensure that Confidential Information of the other party is not disclosed or duplicated in contravention of the provisions of this Contractor by such officers, agents, subcontractors and employees and that such party shall be responsible for any unauthorized disclosure of the Confidential Information of the other party by such officers, agents, subcontractors or employees; and further provided, that if the disclosure is by the Commonwealth to another contractor or sub-contractor, such disclosure is subject to a suitable non-disclosure agreement. The obligations in this Paragraph shall not restrict any disclosure by either party pursuant to any applicable law, or in accordance with the order of any court or government agency of competent jurisdiction (provided that the disclosing party shall give prompt notice to the non-disclosing party of such order) and, except to

the extent provided otherwise by any applicable law, shall not apply with respect to information which:

(1) is developed by the other party without violating the disclosing party's proprietary rights,

(2) is or becomes publicly known (other than through unauthorized disclosure),

(3) is disclosed by the owner of such information to a third party free of any obligation of confidentiality,

(4) is already known by such party without an obligation of confidentiality other than pursuant to this Contractor or any confidentiality Contractor entered into before the Effective Date between Commonwealth and Contractor, or

(5) is rightfully received by the disclosing party free of any obligation of confidentiality.

The confidentiality period for Confidential Information which is related to hardware, software, technical specifications, and methods and processes related to data processing and/or computing shall continue from the date of disclosure until two years following expiration or termination of this Contract. The immediately preceding sentence shall not release or relax, in whole or in part, Contractor's confidentiality obligations with respect to information pertaining to any private individual or, with respect to any Commonwealth Agency, information or documentation which is not permitted to be disclosed to third parties under local, Commonwealth or Federal laws and regulations or pursuant to the terms of any third party Contractor to which Commonwealth is a party.

Nothing in this *Section 37(b)* shall supersede or limit, or be deemed to supersede or limit, any other provision of this Contract pertaining to confidentiality or disclosure of any Commonwealth Data or to any security procedures required to be followed by Contractor or its employees and other representatives. In addition to the confidentiality and non-disclosure and other restrictive provisions of this *Section 37(b)* and elsewhere in this Contract, Contractor shall be subject to, and shall be required to abide by, the provisions set forth in the *Exhibits* to the RFP, all of which are required to be incorporated into this Contract to satisfy the requirements of a particular Commonwealth Agency, a particular agency of the Federal government with whom Commonwealth interacts or other third party.

c) Each party shall:

(1) Notify the other party promptly of any known unauthorized possession, use or knowledge of the other party's Confidential Information by any person or entity.

(2) Promptly furnish to the other party full details known by such party relating to the unauthorized possession, use or knowledge thereof and shall use reasonable efforts to assist the other party in investigating or preventing the recurrence of any unauthorized possession, use or knowledge of the other party's Confidential Information.

(3) Use reasonable efforts to cooperate with the other party in any litigation and investigation against third parties deemed necessary by the other party to protect its proprietary rights.

(4) Promptly use all reasonable efforts to prevent a recurrence of any such unauthorized possession, use or knowledge of the other party's Confidential Information.

d) Each party shall bear the cost it incurs as a result of compliance with this Paragraph. The obligations in this Paragraph shall not restrict any disclosure by either party pursuant to any applicable law or pursuant to the order of any court or other legal process or government agency of competent jurisdiction (provided that the disclosing party shall give prompt notice to the non-disclosing party of such order).

e) There shall be no restriction with respect to the use or disclosure of any ideas, concepts, know-how or data processing techniques developed alone or jointly with Commonwealth in connection with Services provided to Commonwealth under this Contractor.

f) The Contractor shall use the following process when submitting information to the Commonwealth it believes to be confidential and/or proprietary information or trade secrets:

Comment [A85]: Contractor proposes deletion as what is to be treated as confidential information is already defined

(1) Prepare an un-redacted version of the appropriate document, and

(2) Prepare a redacted version of the document that redacts the information that is asserted to be confidential or proprietary information or a trade secret, and

(3) Prepare a signed written statement that states:

(i) the attached document contains confidential or proprietary information or trade secrets;

(ii) the Contractor is submitting the document in both redacted and un-redacted format in accordance with 65 P.S. § 67.707(b); and

(iii) the Contractor is requesting that the document be considered exempt under 65 P.S. § 67.708(b)(11) from public records requests.

(4) Submit the two documents with the signed written statement to the Commonwealth.

g) When the Contract expires or terminates, and at any other time at the written request of the Commonwealth, the Contractor must promptly return to the Commonwealth all of the Commonwealth's Confidential Information and Data (and all copies of this information) that is in the Contractor's possession or control, in whatever form. Unless the Commonwealth agrees or specifies otherwise, the Contractor shall also deliver to the Commonwealth or, if requested by the Commonwealth, delete or destroy any copies, duplicates, summaries, abstracts or other representations of any such Confidential Information or any part thereof, in whatever form, then in the Contractor's possession or control in accordance with the "NIST Guidelines for Media Sanitization" (SP 800-88).

Comment [A86]: Contractor proposes mutual requirement to return the other parties confidential information

Comment [A87]: Contractor proposes an exception to the obligation to return or destroy data to the extent it is (1) embedded in records or documents maintained in the normal course of business, or (2) otherwise retained for legal, regulatory, or archival purposes

38. SENSITIVE INFORMATION

a) The Contractor shall not publish or otherwise disclose, except to the Commonwealth or the Contractor's subcontractors, any information or data obtained hereunder from private individuals, organizations, or public agencies, in a way that allows the information or data furnished by or about any particular person or establishment to be identified.

b) The parties shall not use or disclose any information about a recipient receiving services from, or otherwise enrolled in, a Commonwealth program affected by or benefiting from services under this Contract for any purpose not connected with the parties' Contract responsibilities.

c) Contractor, as directed, shall comply with all federal or state laws and regulations related to the use of information that constitutes protected health information (PHI) as defined by the regulations promulgated pursuant to the *Health Insurance Portability and Accountability Act* (HIPAA). By signing this Contract, the Contractor agrees to the terms of the Business Associates Contract, which is incorporated into this Contract as Appendix A. If Contract Participant, or relevant portion thereof, is a Covered Entity as defined in HIPAA, and the Contractor is performing the work of a Business Associate, the Contract Participant will fill in the blanks in the attached Appendix. It is understood that Appendix A is only applicable if the Contract Participant indicates in writing to Contractor, specifying the work and scope intended to be

subject to a Business Associates Contract, and only to the extent that Contractor and the Contract Participant agree in writing as to the specific application of Appendix A and the Business Associate Contract. If not applicable to the entire Contract Participant, Appendix A is only applicable with respect to the internal entities indicated by the Contract Participant and agreed to by the Contractor.

d) Contractor will comply with all obligations applicable to it under all applicable data protection legislation in relation to all personal data that is processed by it in the course of performing its obligations under this Contract including by:

(1) Maintaining a valid and up to date registration or notification under the data protection legislation; and

(2) Complying with all data protection legislation applicable to cross border data flows of personal data and required security measures for personal data.

39. PATENT, COPYRIGHT, TRADEMARK, AND TRADE SECRET PROTECTION

a) The Contractor shall hold the Commonwealth harmless from any suit or proceeding which may be brought by a third party against the Commonwealth, its departments, officers or employees for the alleged infringement of any United States or foreign patents, copyrights, or trademarks, or for a misappropriation of trade secrets arising out of performance of this Contract, including all work, services, materials, reports, studies, and computer programs provided by the Contractor, and in any such suit or proceeding will satisfy any final award for such infringement, including costs. The Commonwealth agrees to give Contractor prompt notice of any such claim of which it learns. Pursuant to the Commonwealth Attorneys Act 71 P.S. § 732-101, *et seq*., the Office of Attorney General (OAG) has the sole authority to represent the Commonwealth in actions brought against the Commonwealth. The OAG may, however, in its sole discretion and under the terms it deems appropriate, delegate its right of defense. If OAG delegates the defense to the Contractor, the Commonwealth will cooperate with all reasonable requests of Contractor made in the defense of such suits. No settlement which prevents the Commonwealth from continuing to use the Developed Materials as provided herein shall be made without the Commonwealth's prior written consent. In all events, the Commonwealth shall have the right, , to participate in the defense of any such suit or proceeding through counsel of its own choosing. It is expressly agreed by the Contractor that, in the event it requests that the Commonwealth to provide support to the Contractor in defending any such claim, the Contractor shall reimburse the Commonwealth for all reasonable expenses (including attorneys' fees, if such are made necessary by the Contractor's request) incurred by the Commonwealth for such support. If OAG does not delegate the defense of the matter, the Contractor's obligation to

Comment [A88]: Contractor proposes clarification and add the word "Contractors" performance

Comment [A89]: Contractor proposes adding the words ", at its expense,"

indemnify ceases. The Contractor will, at its expense, provide whatever cooperation OAG requests in the defense of the suit.

b) The Contractor agrees to exercise reasonable due diligence to prevent claims of infringement on the rights of third parties. The Contractor certifies that, in all respects applicable to this Contract, it has exercised and will continue to exercise due diligence to ensure that all works produced under this Contract do not infringe on the patents, copyrights, trademarks, trade secrets or other proprietary interests of any kind which may be held by third parties.

Comment [A90]: Contractor proposes that section b) be deleted

c) If the defense of the suit is delegated to the Contractor, the Contractor shall pay all damages and costs finally awarded therein against the Commonwealth, when such damages and costs are required to be paid. If information and assistance are furnished by the Commonwealth at the Contractor's written request, it shall be at the Contractor's expense, but the responsibility for such expense shall be only that within the Contractor's written authorization.

d) If the products, materials, reports, studies, or computer programs furnished hereunder become subject to a claim of infringement of a United States patent, copyright, or trademark, or for a misappropriation of trade secret, or if any of the products, materials, reports, studies or computer programs provided by the Contractor are in such suit or proceeding held to constitute infringement and the use or publication thereof is enjoined, then without diminishing the Contractor's obligation to satisfy any final award, the Contractor may, at its option and expense, substitute functional equivalents for the alleged infringing products, materials, reports, studies, or computer programs or, at the Contractor's option and expense, obtain the rights for the Commonwealth to continue the use of such products, materials, reports, studies, or computer programs

Comment [A91]: Contractor proposes adding the following at the end of the sentence "or modify them so that they are no longer infringing " Section 39 (e) can then be deleted

e) If any of the products, materials, reports, studies, or computer programs provided by the Contractor are in such suit or proceeding held to constitute infringement and the use or publication thereof is enjoined, the Contractor shall, at its own expense and at its option, either procure the right to publish or continue use of such infringing products, materials, reports, studies, or computer programs, replace them with non-infringing items, or modify them so that they are no longer infringing.

f) If the Contractor is unable to do any of the preceding, the Contractor agrees to pay the Commonwealth:

(1) Any amounts paid by the Commonwealth less a reasonable amount based on the acceptance and use of the deliverable;

(2) Any license fee less an amount for the period of usage of any software; and

(3) The prorated portion of any Fees representing the time remaining in any period of service for which payment was made.

g) The obligations of the Contractor under this Section 45 (Patent, Copyright, Trademark, and Trade Secret Protection) continue without time limit and survive the termination of this Contract.

h) Notwithstanding the above, the Contractor shall have no obligation for:

(1) Modification of any product, service, or deliverable provided by the Commonwealth or any third party, except for the Contractor or any of its Subcontractors;

(2) Any material provided by the Commonwealth to the Contractor and incorporated into, or used to prepare, a product, service, or deliverable;

(3) Use of the product, service, or deliverable in other than its specified operating environment;

(4) The combination, operation, or use of the product, service, or deliverable with other products, services, or deliverables not provided by the Contractor as a system or the combination, operation, or use of the product, service, or deliverable, with any products, data, or apparatus that the Contractor did not provide;

(5) Infringement of a non-Contractor product alone;

(6) The Commonwealth's distribution, marketing or use beyond the scope contemplated by the Contract;

(7) The Commonwealth's failure to use corrections or enhancements made available to the Commonwealth by the Contractor at no charge;

Comment [A92]: Contractor propose deleting "at no charge"

(8) Any infringement or claim thereof against the Commonwealth brought prior to the execution of this Contract, unless the infringement or claim relates to services provided by Contractor under another contract with the Commonwealth; or

(9) Infringement related to content provided by or on behalf of the Commonwealth, except as provided by the Contractor or any of its Subcontractors or suppliers.

i) The obligation to defend and indemnify the Commonwealth, under the terms of this *Section 39* (Patent, Copyright, Trademark, and Trade Secret Protection), shall be the Contractor's sole and exclusive obligation and the Commonwealth's sole and exclusive remedy against the Contractor for the infringement or misappropriation of intellectual property.

40. PROPRIETARY RIGHTS

a) **Commonwealth Software**. As between Commonwealth and Contractor, all Commonwealth Software shall be and shall remain the exclusive property of Commonwealth or its licensors, and Contractor shall have no rights or interests in the Commonwealth Software by virtue of this Contract except as described in this *Section 40* (Proprietary Rights) or elsewhere in this Contract. Commonwealth hereby grants to Contractor, at no cost to Contractor, for the limited purpose of providing the Services, a nonexclusive, nontransferable, royalty-free right (subject to the terms of any third party agreement to which Commonwealth is a party and which theretofore is disclosed to Contractor) to (1) have access to the Commonwealth Software, (2) copy the Commonwealth Software for archival purposes or as may otherwise be required by this Contract, (3) modify the Commonwealth Software as required by this Contract, if permitted by the Software licensing terms and pursuant to the terms of Commonwealth Third Party Software license agreement, if applicable, and (4) sublicense Contractor's subcontractors approved by Commonwealth to do any of the foregoing; provided, however, that neither Contractor nor any of its subcontractors may decompile or reverse engineer, or attempt to decompile or reverse engineer, any of the Commonwealth Software.

As of the Effective Date and subject to the terms of any third party agreement to which Commonwealth is a party, (1) Commonwealth shall, at no cost to Contractor, provide Contractor with access to the Commonwealth Software in the form in use by Commonwealth as of the Effective Date and (2) Contractor, as part of the Services, shall compile and, as changes are made, update a list of all of the Commonwealth Software then in use by Contractor or any of its subcontractors in connection with Contractor's performance of the Services. Upon the expiration or termination for any reason of Contractor's obligation to provide the Services or of this Contract, the rights granted to Contractor in this *Section 40(a)* shall immediately revert to Commonwealth or Commonwealth's designee, and Contractor forthwith shall, at no cost to Commonwealth, deliver to Commonwealth all of the Commonwealth Software (including any related source code and object code in Contractor's possession or under its control) in the form in use as of the effective date of such expiration or termination, together with a current copy of the list of Commonwealth Software in use as of the date of such expiration or termination. Concurrently therewith, Contractor shall destroy or erase all other copies of any of the Commonwealth Software then in Contractor's possession or under its control unless otherwise instructed by Commonwealth; provided, however, pursuant to and if permitted by the Commonwealth's license agreement for Commonwealth Third Party Software, if applicable, that

Contractor may retain one archival copy of such Commonwealth Software, including the Developed Software, until the later of six (6) years after such expiration or termination of this Contract and the final resolution of any actively asserted pending disputes between the parties, such retention being for the sole purpose of establishing Contractor's performance under this Contract.

b) **Contractor Software and Contractor Tools**. As between Commonwealth and Contractor, all Contractor Software and Contractor Tools shall be and shall remain the exclusive property of Contractor, and Commonwealth shall have no rights or interests in the Contractor Software or the Contractor Tools by virtue of this Contract except as described in this *Section 40(b)*. As part of the Services, Contractor shall during the Term (1) use the Contractor Software and the Contractor Tools to provide the Services, (2) make available the commercially available Contractor Software and the commercially available Contractor Tools to Commonwealth for use by Commonwealth solely in connection with the Services, and (3) maintain on Commonwealth's premises and make available to Commonwealth upon Commonwealth's request from time to time, for archival purposes only, a copy of the Contractor Software and the Contractor Tools owned by Contractor or its subcontractors and then being used by Contractor to provide the Services.

Upon the expiration or termination for any reason of Contractor's obligation to provide the Services under this Contract and at the request of Commonwealth, Contractor shall, subject to mutually agreed terms and conditions, (1) grant, or cause its subcontractors to grant, to Commonwealth a nonexclusive, nontransferable license to use and, if permitted by the terms of mutually agreed terms and conditions relating thereto, modify and make derivative works of, and unless Commonwealth terminates this Contract pursuant to the terms of *Section 32(a),(b), or (f)* to grant to third parties engaged by Commonwealth the right to use and, if permitted by mutually agreed terms and conditions relating thereto, modify and make derivative works of, all or any portion of the commercially available Contractor Software and the commercially available Contractor Tools owned by Contractor or its subcontractors theretofore being used by Contractor in connection with the Services, the foregoing rights being granted to the extent reasonably necessary to facilitate Commonwealth's or such third party's performance of the activities or services substantially equivalent to the Services to be provided by Contractor under this Contract immediately prior to such expiration or termination and (2) deliver to Commonwealth the object code version of such commercially available Contractor Software and such commercially available Contractor Tools in the form being used by Contractor in connection with the Services immediately prior to such expiration or termination.

It is understood and agreed by Contractor that the rights granted to Commonwealth hereunder in respect of the commercially available Contractor Software and the commercially available Contractor Tools shall not restrict Commonwealth from using such Contractor Software and such Contractor Tools

in the manner in which such items were used by Contractor and its subcontractors to provide the Services immediately prior to the expiration or termination of this Contract. The foregoing obligations of Contractor shall be subject to mutually agreed terms and conditions. In consideration of the grant to Commonwealth of the foregoing license, Commonwealth shall be assessed license fees hereunder not in excess of any license fees therefor being offered, as of the date of termination, by Contractor or its subcontractors, to their respective state governmental customers generally, unless Commonwealth terminates this Contract pursuant to the terms of *Section 32(a),(b) or (f)*, in which case the then-prevailing license fees of Contractor and its subcontractors, as applicable, shall apply. The foregoing shall not limit or otherwise affect Commonwealth's obligations to pay third party assignment or transfer fees as contemplated in *Section 33* (Termination Assistance); provided, however, that Commonwealth shall not be assessed any additional fees in respect thereof by Contractor.

c) **Developed Documentation.** Documentation developed by Contractor specifically for the Commonwealth in connection with its performance under this Contract is the sole and exclusive property of the Commonwealth and shall be considered "works made for hire" under the United States Copyright Act of 1976, as amended, 17 United States Code. In the event that the documentation does not fall within the specifically enumerated works that constitute works made for hire under the United States copyright laws, Contractor agrees to assign and, upon their authorship or creation, expressly and automatically assigns all copyright interests, proprietary rights, trade secrets, and other right, title, and interest in and to such documentation to Commonwealth. Commonwealth shall have all rights accorded an owner of copyright under the United States copyright laws including, but not limited to, the exclusive right to reproduce the documentation in multiple copies, the right to distribute, copies by sales or other transfers, the right to register all copyrights in its own name as author in the United States and in foreign countries, the right to prepare derivative works based upon the Creative Works and the right to display the documentation. Upon completion or termination of this Contract, all working papers, files and other documents related to the documentation shall immediately be delivered by Contractor to the Commonwealth. Contractor warrants that the documentation is original and does not infringe any copyright, patent, trademark, or other intellectual property right of any third party and are in conformance with the intellectual property laws of the United States. Provided however that Commonwealth's sole remedy for breach of this warranty is the indemnity contained in *Section 39* (Patent, Copyright, Trademark, and Trade Secret Protection).

d) All literary works, or other works of authorship (such as application programs, listings, programming tools, documentation, reports, drawings, procedure manuals and similar works) ("Developed Materials") developed hereunder shall be treated in accordance with the following general principles:

Comment [A93]: Contractor proposes that this is limited to those required to be developed under the Contract and paid for by the Commonwealth Ownership and license rights need to be clarified

(1) If and to the extent Developed Materials modify, improve or enhance software programs generally licensed by Contractor to end-users, then such Developed Materials shall be the property of Contractor and Contractor hereby grants to Commonwealth a perpetual, non-exclusive, nontransferable, royalty-free license to use such Developed Materials in Commonwealth's receipt and use of the Services;

(2) If and to the extent Developed Materials modify, improve or enhance software or other materials owned by Commonwealth or licensed to Commonwealth by a third party (i.e., a licensor other than Contractor or any Contractor agent), then such modification, improvement or enhancement and all related intellectual property rights therein shall, as between Commonwealth and Contractor, be the property of Commonwealth;

(3) If and to the extent Developed Materials constitute a newly created software program or module, and if Commonwealth funds the development cost thereof to any extent, then such software program or module and all related intellectual property rights therein shall be the property of Commonwealth; and

(4) If and to the extent Developed Materials constitute documentation, reports, drawings, procedure manuals and similar works, such Developed Materials shall be the property of Commonwealth. Contractor will not place trademarks or copyright notices on any such Developed Materials.

Comment [A94]: Contractor propose 40(d)(4) and 40(d)(5) should be limited to documentation, reports, data, etc generated for the Commonwealth as part of the Services

(5) Any data related to the use of the Services by the Commonwealth shall be the property of the Commonwealth. For this purpose, data includes ordering information, inventories, etc. At the end of the Contract, regardless of how it is ended, or at any time requested by the Commonwealth, the Contractor will provide the Commonwealth with such data in a format specified by the Commonwealth.

Comment [A95]: Contractor proposes Contractor return data in format then in use as of the date of the end of the contract This change is to be consistent with language in Section 42(d)

e) **Residual Knowledge**. Either Party, in the course of conducting business, may use any ideas, concepts, and know-how, relating to the Services which Contractor or Commonwealth (alone or jointly with the Commonwealth) develops or learns in connection with Contractor's provision of Services to Commonwealth under this Contract.

41. PUBLICATION RIGHTS AND/OR COPYRIGHTS

Comment [A96]: Contractor is uncertain of the purpose of this section and would like to discuss further with Commonwealth

a) The Contractor shall not publish any of the results of the work, which identify the Commonwealth, without the written permission of the Commonwealth. The publication shall include the following statement: "The opinions, findings, and conclusions expressed in this publication are those of the author and not

necessarily those of the Commonwealth of Pennsylvania." The Contractor shall not include in the documentation any copyrighted matter, unless the Contractor provides the Commonwealth with written permission of the copyright owner.

b) Except as otherwise provided in *Section 40* (Proprietary Rights) and the confidentiality provisions of *Section 37* (Confidentiality), the Commonwealth shall have unrestricted authority to reproduce, distribute, and use any submitted report or data designed or developed and delivered to the Commonwealth as part of the performance of the Contract.

c) Rights and obligations of the parties under this *Section 41* (Publication Rights and/or Copyrights) survive the termination of this Contract.

42. REPORTS AND DATA

a) Data. Commonwealth shall supply to Contractor the Commonwealth Data in the form maintained by the Commonwealth on such time schedules as may be agreed to by Commonwealth and Contractor from time to time. All Commonwealth Data is and shall remain the property of Commonwealth. Subject to *Section 40* (Proprietary Rights), the Commonwealth Data shall not be (1) used by Contractor or Contractor Agents other than in connection with providing the Services, and then only in accordance with the terms of this Contract, (2) disclosed, sold, assigned, leased or otherwise provided to third parties by Contractor or Contractor Agents without Commonwealth's consent and any applicable consent required by any federal governmental entity, or (3) commercially exploited by or on behalf of Contractor or Contractor Agents.

b) Reports. As part of the Services, Contractor shall provide the Reports, in electronic form, to Commonwealth. The Reports shall be prepared by Contractor and provided to the Commonwealth in a manner readable by a normal Windows based personal computer. Acceptable formats include but are not limited to: Adobe Acrobat (PDF), Microsoft Word, Microsoft Excel, Microsoft PowerPoint, Text, Comma Separated Values (CSV).

c) Correction of Errors. In the event of any errors or inaccuracies in any of the Commonwealth Data or the Reports, or any other data processing errors or unexpected interruptions (e.g., "abends" or "freeze"), Contractor and Commonwealth shall work together in good faith, using all reasonable efforts and commencing immediately upon the discovery of the situation, to correct such error, inaccuracy or interruption. The foregoing obligations of Contractor under this *Section 42(c)* shall be subject to any limitations placed upon Contractor's access to the Commonwealth Data by Commonwealth or pursuant to this Contract. Promptly upon the completion of the correction of such error, inaccuracy or interruption, the Commonwealth Project Manager and the Contractor Project Manager shall meet to determine and document the cause

thereof. If the error, inaccuracy or interruption is determined to be caused by the error, negligence or omission of Contractor to perform an obligation under this Contract, there shall be no charge to Commonwealth for Contractor's participation in such correction. If the error, inaccuracy or interruption is determined to be caused by the error, negligence or omission of Commonwealth to perform an obligation under this Contract, Commonwealth shall reimburse Contractor for Contractor's out-of-pocket expenses paid by Contractor to third parties (other than Contractor's or any Contractor's Agent's employees) for expertise not otherwise possessed by or available to Contractor and Contractor's expenses for its employees or the employees of any Contractor agent not theretofore engaged in the provision of the Services.

d) Return of Data. At no cost to Commonwealth and as part of the Services, Contractor shall, upon Commonwealth's request at any time and at the cessation of the Termination Assistance, (1) promptly return to Commonwealth, in the format and on the media in use as of the date of the request, all or the requested portion of the Commonwealth Data then in Contractor's possession or under its control and (2) erase or destroy all or the requested portion of Commonwealth Data then in Contractor's possession or under its control. Commonwealth Data returned to the Commonwealth must be in a form that is freely accessible to the Commonwealth and not in a Contractor proprietary format.

43. SECURITY AND PROTECTION OF INFORMATION

a) At all times during the Term, Contractor shall provide all Services, and use all resources related thereto, in a secure manner and in accordance with the Commonwealth's security requirements, including the prevention and detection of fraud, abuse, or other inappropriate use or access of systems and networks by all appropriate means, including network management and maintenance applications and tools, and the use of appropriate encryption technologies. In addition, all Contractor personnel (including personnel of any Subcontractors) shall be subject to and shall at all times conform to the Commonwealth's laws, rules, and requirements for the protection of premises, materials, equipment, and personnel, as they have been previously disclosed to Contractor in writing, including those set forth in the *Exhibits* to the RFP. Any violations or disregard of these rules shall be cause for denial of access by such personnel to the Commonwealth's property. Contractor shall exercise due care and diligence to prevent any injury to person or damage to property while on the Commonwealth's premises. The operation of Contractor vehicles or private vehicles of Contractor personnel on the Commonwealth's property shall conform to posted and other regulations and safe driving practices. Vehicular accidents on the Commonwealth's property and involving Contractor personnel shall be reported promptly to the appropriate Commonwealth's security personnel.

Comment [A97]: Contractor proposes deleting "in a secure manner" as the language it will already be in accordance to the Commonwealth security requirements

Comment [A98]: Contractor requests that security requirements be documented as part of contract, with any subsequent changes handled via Change Control procedures

b) The Pennsylvania State Police's Criminal Justice Information Services Policy ("CJIS Policy"), is set forth in *Exhibits G.6 and G.7*, and is hereby incorporated by this reference into this Contract. Contractor acknowledges and agrees that it is bound by all applicable provisions of the CJIS Policy. Contractor and the Commonwealth further agree that, in accordance with the CJIS Policy, the Commonwealth does not anticipate and will not authorize any requests to Contractor for the criminal history record information covered by the CJIS Policy, because Contractor is performing an IT support function. The Commonwealth's Office of Attorney General's CHRIA Handbook, attached as *Exhibit G.12* to the RFP, is also incorporated by reference into this Contract. Contractor acknowledges and agrees that it is bound by all applicable provisions of the CHRIA Handbook.

.

44. BACKGROUND CHECKS

a) The Contractor must, at its expense, arrange for a background check for each of its employees, as well as for the employees of its subcontractors, who will have access to Commonwealth Services Locations, either through on site or remote access. Background checks will not be conducted by the Commonwealth but rather will be conducted by Contractor or its subcontractors according to Contractor policy and practice and consistent with ITB-SEC009. The background check must be conducted prior to initial access by a Contractor Personnel and every two (2) years thereafter or at a longer interval if required by applicable law.

b) Before the Commonwealth will permit Contractor Personnel access to Commonwealth facilities, the Contractor must provide written confirmation to the office designated by the agency that the background check has been conducted. If, at any time, it is discovered that Contractor Personnel has a criminal record that includes a felony or misdemeanor involving terroristic threats, violence, use of a lethal weapon, or breach of trust/fiduciary responsibility; or which raises concerns about building, system, or personal security, or is otherwise job-related, the Contractor shall notify the Commonwealth Contracting Officer immediately, shall not assign that employee to any Commonwealth facilities, shall remove any access privileges already given to the employee, and shall not permit that employee remote access to Commonwealth facilities or systems, unless the agency consents, in writing, prior to the access being provided. The agency may withhold its consent at its sole discretion. Failure of the Contractor to comply with the terms of this Paragraph may result in default of the Contractor under its Contract with the Commonwealth.

c) The Commonwealth specifically reserves the right of the Commonwealth to conduct background checks over and above that described herein.

45. INSURANCE

a) Contractor Insurance Requirements. During the Contract Term, Contractor shall maintain at its own expense, insurance of the type and in the amounts specified below and issued by companies authorized to conduct such business under the laws of Pennsylvania:

(1) Statutory workers' compensation in accordance with all applicable Federal, state and local requirements, and employer liability in an amount not less than $2,000,000 per occurrence;

(2) Comprehensive general public liability (including contractual liability insurance) in an amount not less than $5,000,000 per occurrence;

(3) Comprehensive automobile liability covering all vehicles that Contractor owns, hires, or leases in an amount not less than $5,000,000 per occurrence (combined single limit for bodily injury and property damages).

(4) Personal property insurance, on a replacement basis, covering all of Contractor's and Contractor's Agents' personal property located at any Contractor Services Location.

(5) Professional liability/error & omission in the aggregate amount of not less than $15,000,000.

(6) Comprehensive crime insurance in an amount of not less than $15,000,000 per claim.

(7) Network/Cyber Liability Insurance (including coverage for Technology Professional Liability if not covered under Contractor's Professional Liability/Errors and Omissions Insurance referenced above) in the amount of $20,000,000, per occurrence.

(8) Umbrella/excess in an aggregate amount of not less than $30,000,000.

b) Insurance Requirements for Subcontractors. During the Contract Term, Contractor shall require each of its subcontractors listed in *Schedule L* (Approved Subcontractors) and any other subcontractors performing any Services on-site at any of the Contractor Services Locations, to maintain at their own expense or Contractor's expense, insurance of the type and in the amounts specified below:

(1) Statutory workers' compensation in accordance with all applicable Federal, state and local requirements, and employer liability in an amount not less than $1,000,000 per occurrence;

(2) Comprehensive general public liability (including contractual liability insurance) in an amount not less than $2,000,000 per occurrence;

(3) If any of the subcontractor personnel will be on-site at any of the Commonwealth's or Contractor's facilities, comprehensive automobile liability covering all vehicles owned, hired or leased by that Subcontractor and in an amount not less than $2,000,000 per occurrence (combined single limit for bodily injury and property damages);

(4) If the subcontractor personnel will be on-site at any of Commonwealth's or Contractor's facilities, personal property

(5) insurance, on a replacement basis, covering all of that Subcontractor's personal property located at any such facilities; and

(6) Network/Cyber Liability Insurance (including coverage for Technology Professional Liability if not covered under Contractor's Professional Liability/Errors and Omissions Insurance referenced above) in the amount of $10,000,000, per occurrence; and

(7) Errors & Omissions liability in the amount of $2,000,000 each claim and aggregate (if applicable).

c) Prior to the expiration of any then effective insurance policy, Contractor shall furnish to Commonwealth certificates of insurance or other appropriate documentation (including evidence of renewal of insurance) evidencing all coverage referenced in this *Section 45* (Insurance), as applicable, and naming Commonwealth as an additional insured to the extent of Contractor's indemnities contained in this Contract. Contractor shall have included in all policies of insurance required hereunder a waiver by the insurer of all right of subrogation against Commonwealth in connection with any loss or damage thereby insured against. Such certificates or other documentation will include a provision whereby thirty (30) days' notice must be received by Commonwealth prior to coverage cancellation or alteration of the coverage by either Contractor or its subcontractors or the applicable insurer. Such cancellation or alteration shall not relieve Contractor of its continuing obligation to maintain insurance coverage in accordance with this *Section 45*(Insurance).

d) For purposes hereof, Contractor and such subcontractors may maintain "umbrella" insurance policies to fulfill the foregoing insurance requirements, as appropriate.

46. WARRANTIES

Comment [A99]: Contractor proposes dividing Section 46 into 2 parts Representation in Section a and Covenants in Section b Subsection 5 through 11 should be Covenants

a) Contractor represents, warrants and covenants that as of the Contract's Effective Date:

(1) It is a corporation duly incorporated, validly existing, and in good standing under the laws of _____..

(2) It has all requisite corporate power and authority to execute, deliver, and perform its obligations under this Contract.

(3) Contractor is duly licensed, authorized and qualified to do business and is in good standing in Pennsylvania and in every other jurisdiction where Services will be performed by Contractor pursuant to this Contract in which a license, authorization or qualification is required for the ownership or leasing of its assets or the transaction of business of the character transacted by it except where the failure to be so licensed, authorized or qualified would not have a material adverse effect on Contractor's ability to fulfill its obligations under this Contract.

(4) The execution, delivery and performance of this Contract by Contractor has been duly authorized by Contractor.

(5) Contractor shall comply with all applicable Federal, state and local laws and regulations applicable to Contractor and shall obtain all applicable permits and licenses required of Contractor in connection with its obligations under this Contract.

Comment [A100]: Contractor proposes to delete this section 5 as it appears redundant with Section 78

(6) Contractor has not disclosed any Confidential Information of Commonwealth.

(7) The Contractor Software does not and will not, and the Developed Software and the Services will not, infringe upon the proprietary rights of any third party, provided that Contractor will have no obligation with respect to any losses to the extent the same arise out of or in connection with Commonwealth's modification or misuse of equipment, systems, programs, or products or Commonwealth's combination, operation or use with devices, data, equipment, systems, programs or products not furnished by Contractor under this Contract.

(8) Contractor Personnel and Subcontractors that Contractor will use to provide and perform the Services have and during the Term will have, the suitable knowledge, skills, experience, qualifications and resources to provide and perform the Services:

1. In accordance with the Contract; and

2. In a diligent, workmanlike manner with due care and skill, consistent with the required level of quality and performance and in accordance with the Service Levels.

(9) The Services will comply with standards set in the Commonwealth's IT Bulletins as issued from time to time, and all internal policies and procedures as set from time to time and as a provided to Contractor.

(10) Contractor shall cooperate fully with Commonwealth and with any third party appointed by Commonwealth to the extent that such cooperation may be necessary to permit Commonwealth or such third parties to complete any work related to or impacted by the Services provided to Commonwealth by Contractor under the Contract.

(11) Contractor shall collaborate fully with Commonwealth or with any third party appointed by Commonwealth to the extent that such cooperation may be necessary to permit Commonwealth or such third parties to in-source or transfer to a third party any aspect of the Services then provided by Contractor under the Contract.

b) Commonwealth represents, warrants and covenants that as of the Contract's Effective Date:

(1) It is a sovereign entity and has all requisite power and authority to execute, deliver, and perform its obligations under this Contract.

(2) It has, or at any time of provision to Contractor, will have the right to use and to disclose to Contractor and Contractor Agents and to allow Contractor and Contractor Agents to use in accordance with the terms of this Contract any Commonwealth Software so disclosed to Contractor.

Comment [A101]: Contractor proposes deleting this subsection 9 as standards should be included within this Contract and any changes to the standards should be processed via Change Control

Comment [A102]: Contractor proposes having reciprocal representations and warranties similar to current contract provision 26 01

47. CONTRACTOR RESPONSIBILITY PROGRAM

a) The Contractor certifies, for itself and all its subcontractors, that as of the date of its execution of this Bid/Contract, that neither the Contractor, nor any subcontractors, nor any suppliers are under suspension or debarment by the Commonwealth or any governmental entity, instrumentality, or authority and, if the Contractor cannot so certify, then it agrees to submit, along with its Bid, a written explanation of why such certification cannot be made.

b) The Contractor must also certify, in writing, that as of the date of its execution of this Bid/Contract, it has no tax liabilities or other Commonwealth obligations.

c) The Contractor's obligations pursuant to these provisions are ongoing from and after the effective date of the contract through the termination date thereof.

Accordingly, the Contractor shall have an obligation to inform the Commonwealth if, at any time during the term of the Contract, it becomes delinquent in the payment of taxes, or other Commonwealth obligations, or if it or any of its subcontractors are suspended or debarred by the Commonwealth, the federal government, or any other state or governmental entity. Such notification shall be made within 15 days of the date of suspension or debarment.

d) The failure of the Contractor to notify the Commonwealth of its suspension or debarment by the Commonwealth, any other state, or the federal government shall constitute an event of default of the Contract with the Commonwealth.

e) The Contractor agrees to reimburse the Commonwealth for the reasonable costs of investigation incurred by the Office of State Inspector General for investigations of the Contractor's compliance with the terms of this or any other agreement between the Contractor and the Commonwealth, which results in the suspension or debarment of the Contractor. Such costs shall include, but shall not be limited to, salaries of investigators, including overtime; travel and lodging expenses; and expert witness and documentary fees. The Contractor shall not be responsible for investigative costs for investigations that do not result in the Contractor's suspension or debarment.

f) The Contractor may obtain a current list of suspended and debarred Commonwealth contractors by either searching the internet at *http://www.dgs.state.pa.us* or contacting the:

Department of General Services
Office of Chief Counsel
603 North Office Building
Harrisburg, PA 17125
Telephone No. (717) 783-6472
FAX No. (717) 787-9138

48. OFFSET PROVISION FOR COMMONWEALTH CONTRACTS

The Contractor agrees that the Commonwealth may set off the amount of any state tax liability or other obligation of the Contractor or its subsidiaries to the Commonwealth against any payments due the Contractor under any contract with the Commonwealth.

49. TAXES-FEDERAL, STATE, AND LOCAL

a) **Commonwealth Exemption**. No taxes from which the Commonwealth is exempt shall be included in the Fee. The Commonwealth is exempt from all excise taxes imposed by the Internal Revenue Service and has accordingly registered with the Internal Revenue Service to make tax-free purchases under registration No. 23-23740001-K. With the exception of purchases of the

following items, no exemption certificates are required and none will be issued: undyed diesel fuel, tires, trucks, gas-guzzler emergency vehicles, and sports fishing equipment. The Commonwealth is also exempt from Pennsylvania sales tax, local sales tax, public transportation assistance taxes, and fees and vehicle rental tax. The Department of Revenue regulations provide that exemption certificates are not required for sales made to governmental entities and none will be issued.

b) **Contractor Taxes**. Fees are inclusive of any applicable sales, use, personal property and other taxes attributable to periods on or after the Effective Date and based upon or measured by Contractor's cost in acquiring or providing equipment, materials, supplies or services furnished or used by Contractor in performing or furnishing the Services, including without limitation, all personal property and use taxes, if any, due on Contractor Machines.

c) **Segregation of Fees**. Commonwealth and Contractor shall cooperate to segregate the Fees into the following separate payment streams: (1) those for Services, and (2) those for which Contractor functions merely as a paying agent for Commonwealth in receiving goods, supplies, or services (including leasing and licensing arrangements).

50. POLICIES AND PROCEDURES

Contractor shall comply with the most stringent of:

Comment [A103]: Suggest removing "most stringent"

a) Commonwealth standards set out in IT Bulletins, standards and procedures related to the Services, including but not limited to those governing security, treatment of personal information, quality, change, and problem management, safety, data privacy and data security, and pervasive and transaction controls; provided, however that the Contractor may submit a request under *Section 27* (Change Control), if it believes that it has incurred costs or delay in complying with this Section due to changes in the IT Bulletins, standards and procedures related to the Services; or

b) The policies, standard and procedures that are generally adopted by leading providers of Services similar in scope, scale and geographic coverage to the outsourced Services.

51. AUDIT OBLIGATIONS

a) SINGLE AUDIT ACT OF 1984

In compliance with the *Single Audit Act of 1984*, the Contractor agrees to the following:

(1) This Contract is subject to audit by federal and state agencies or their authorized representative in accordance with the auditing standards promulgated by the Comptroller General of the United States and specified in *Government Auditing Standards*, 1994 Revisions (Yellow Book).

(2) The audit requirement of this Contract will be satisfied if a single audit is performed under the provisions of the *Single Audit Act of 1984, 31 U.S.C. § 7501, et seq*., and all rules and regulations promulgated pursuant to the Act.

(3) The Commonwealth reserves the right for federal and state agencies or their authorized representatives to perform additional audits of a financial/compliance, economy/efficiency, or program results nature, if deemed necessary.

(4) The Contractor further agrees to comply with requirements that may be issued by the state agency upon receipt of additional guidance received from the federal government regarding the *Single Audit Act of 1984.*

b) Access by Commonwealth

(1) **Processing**. Upon reasonable written notice from Commonwealth, Contractor and Contractor Agents shall provide such auditors and inspectors with access to the Services Locations and the Software and the Machines for the purpose of performing audits or inspections of the Services and the operations of Commonwealth and Contractor, subject always to Contractor's reasonable security requirements. Contractor shall provide, and shall cause Contractor Agents to provide, to such auditors and inspectors any reasonable assistance that they may require. If any such audit results in Contractor being notified that it or any Contractor Agent is not in compliance with any law, regulation, audit requirement or generally accepted accounting principle relating to the Services, Contractor shall, and shall cause such Contractor Agent to, promptly take actions to comply with such law, regulation, audit requirement or generally accepted accounting principle. Commonwealth shall bear the expense of any such compliance that is (1) required by a law, regulation or other audit requirement relating to Commonwealth's operations to the extent the same was first enacted on or after the Effective Date or (2) necessary due to Commonwealth's noncompliance with any law, regulation or audit requirement imposed on Commonwealth. Contractor shall bear the expense of any such response that is (1) required by a law, regulation or other audit requirement relating to Contractor's business or enacted prior to the Effective Date, (2) to be performed by

Contractor as part of the Services, or (3) necessary due to Contractor's noncompliance with any law, regulation or audit requirement imposed on Contractor. As part of the Services, Contractor shall provide to Commonwealth summary data of those portions of Contractor's and Contractor Agents' internal audit reports relating solely to the Services.

(2) **Fees**. Upon reasonable written notice from Commonwealth, Contractor shall provide such auditors and inspectors with access to such financial records and supporting documentation as may reasonably be requested by Commonwealth, and such auditors and inspectors may audit the Fees charged to Commonwealth to determine that such Fees are accurate and in accordance with this Contract.

(3) **Overcharges**. If, as a result of such audit, Commonwealth determines that Contractor has overcharged Commonwealth, Commonwealth shall notify Contractor of the amount of such overcharge and Contractor shall promptly pay to Commonwealth the amount of the overcharge, plus interest at the rate of six percent (6%) per annum, calculated from the date of receipt by Contractor of the overcharged amount until the date of repayment to Commonwealth. In the event any such audit reveals an overcharge to Commonwealth during any calendar month during the Term exceeding fifteen percent (15%) of all Fees in the aggregate paid by Commonwealth in respect of such calendar month, Contractor shall reimburse Commonwealth for the cost of such audit. If as a result of such audit, Commonwealth or Contractor determines that Contractor has undercharged Commonwealth, Commonwealth shall promptly pay to Contractor the amount of such undercharge, without interest. Any disagreement between the parties with regard to the results of any such audit shall be treated as a dispute between the parties subject to the provisions of *Section 34* (Contract Controversies).

(4) **Record Retention**. As part of the Services, Contractor shall (1) retain records and supporting documentation sufficient to document the Services and the Fees paid or payable by Commonwealth under this Contract for at least three (3) years after the expiration or termination of this Contract or until all questioned items relating to such records and documentation are resolved by the parties, whichever is later, and (2) upon notice from Commonwealth, provide such auditors and inspectors as are designated by Commonwealth with reasonable access to such records and documentation for inspection, audit and reproduction. Such records and documentation shall be in such detail as will properly reflect, in accordance with generally accepted accounting principles, all charges claimed under the provisions of this Contract. Any such records which relate to litigation or the settlement

of claims arising out of the performance of this Contract, or any Fees as to which exception has been taken by the auditors, shall be retained by Contractor until such litigation, claims, or exceptions have been finally resolved. Such audit shall not require Contractor to disclose cost, profit and overhead data, including direct and indirect rates, markups, profit margins or confidential employee records or other trade secret information.

(5) **Inclusion in Subcontracts**. The provisions of this *Section 51* (Audit Obligations), except for *Section 51(b)3*, shall be applicable to and included in each subcontract under this Contract.

52. VIRUS AND MALICIOUS CODE

(a) The Contractor shall be liable for any damage to any data and/or software owned or licensed by the Commonwealth if the Contractor or any of its employees, subcontractors or consultants introduces a virus or malicious, mischievous or destructive programming into the Commonwealth's software or computer networks and has failed to comply with the Commonwealth software security standards. The Commonwealth must demonstrate that the Contractor or any of its employees, subcontractors or consultants introduced the virus or malicious, mischievous or destructive programming. The Contractor's liability shall cease if the Commonwealth has not fully complied with its own software security standards.

(b) The Contractor shall be liable for any damages incurred by the Commonwealth including, but not limited to, the expenditure of Commonwealth funds to eliminate or remove a computer virus or malicious, mischievous or destructive programming that result from the Contractor's failure to take proactive measures to keep virus or malicious, mischievous or destructive programming from originating from the Contractor or any of its employees, subcontractors or consultants through appropriate firewalls and maintenance of anti-virus software and software security updates (such as operating systems security patches, etc.).

(c) In the event of destruction or modification of software, the Contractor shall eliminate the virus, malicious, mischievous or destructive programming, restore the Commonwealth's software, and be liable to the Commonwealth for any resulting damages.

(d) The Contractor shall be responsible for reviewing Commonwealth software security standards and complying with those standards.

(e) The Commonwealth may, at any time, audit, by a means deemed appropriate by the Commonwealth, any computing devices being used by representatives of the Contractor to provide Services to the Commonwealth for the sole purpose of determining whether those devices have anti-virus software with current virus

signature files and the current minimum operating system patches or workarounds have been installed. Devices found to be out of compliance will immediately be disconnected and will not be permitted to connect or reconnect to the Commonwealth network until the proper installations have been made.

(f) The Contractor may use the anti-virus software used by the Commonwealth to protect Contractor's computing devices used in the course of providing services to the Commonwealth. It is understood that the Contractor may not install the software on any computing device not being used to provide services to the Commonwealth, and that all copies of the software will be removed from all devices upon termination of this Contract.

(g) The Commonwealth will not be responsible for any damages to the Contractor's computers, data, software, etc. caused as a result of the installation of the Commonwealth's anti-virus software or monitoring software on the Contractor's computers.

53. THE AMERICANS WITH DISABILITIES ACT

During the term of this Contract, the Contractor agrees as follows:

(h) Pursuant to federal regulations promulgated under the authority of *The Americans With Disabilities Act*, 28 C.F.R.§ 35.101, *et seq*., the Contractor understands and agrees that no individual with a disability shall, on the basis of the disability, be excluded from participation in this Contract or from activities provided for under this Contract. As a condition of accepting and executing this Contract, the Contractor agrees to comply with the *General Prohibitions Against Discrimination*, 28 C.F.R. § 35.130, and all other regulations promulgated under Title II of *The Americans With Disabilities Act* which are applicable to the benefits, services, programs, and activities provided by the Commonwealth of Pennsylvania through Contracts with outside Contractors.

(i) The Contractor shall be responsible for and agrees to indemnify and hold harmless the Commonwealth of Pennsylvania from losses, damages, expenses claims, demands, suits, and actions brought by any party against the Commonwealth of Pennsylvania as a result of the Contractor's failure to comply with the provisions of subsection (a) above.

54. NONDISCRIMINATION CLAUSE/SEXUAL HARASSMENT CLAUSE

The Contractor agrees:

a) In the hiring of any employee(s) for the manufacture of supplies, performance of work, or any other activity required under the contract or any subcontract, the Contractor, each subcontractor, or any person acting on behalf of the Contractor or subcontractor shall not, by reason of gender, race, creed, or color,

discriminate against any citizen of this Commonwealth who is qualified and available to perform the work to which the employment relates.

b) Neither the Contractor nor any subcontractor nor any person on their behalf shall in any manner discriminate against or intimidate any employee involved in the manufacture of supplies, the performance of work, or any other activity required under the contract on account of gender, race, creed, or color.

c) The Contractor and each subcontractor shall establish and maintain a written sexual harassment policy and shall inform their employees of the policy. The policy must contain a notice that sexual harassment will not be tolerated and employees who practice it will be disciplined.

d) The Contractor and each subcontractor shall not discriminate by reason of gender, race, creed, or color against any subcontractor or supplier who is qualified to perform the work to which the contracts relates.

e) The Contractor and each subcontractor shall, within the time periods requested by the Commonwealth, furnish all necessary employment documents and records and permit access to their books, records, and accounts by the contracting agency and the Bureau of Small Business Opportunities (BSBO), for purpose of ascertaining compliance with provisions of this Nondiscrimination/Sexual Harassment Clause. Within fifteen (15) days after award of any contract, the Contractor shall be required to complete, sign and submit Form STD-21, the "Initial Contract Compliance Data" form. If the contract is a construction contract, then the Contractor shall be required to complete, sign and submit Form STD-28, the "Monthly Contract Compliance Report for Construction Contractors", each month no later than the 15th of the month following the reporting period beginning with the initial job conference and continuing through the completion of the project. Those contractors who have fewer than five employees or whose employees are all from the same family or who have completed the Form STD-21 within the past 12 months may, within the 15 days, request an exemption from the Form STD-21 submission requirement from the contracting agency.

f) The Contractor shall include the provisions of this Nondiscrimination/Sexual Harassment Clause in every subcontract so that those provisions applicable to subcontractors will be binding upon each subcontractor.

g) The Commonwealth may cancel or terminate the contract and all money due or to become due under the contract may be forfeited for a violation of the terms and conditions of this Nondiscrimination/Sexual Harassment Clause. In addition, the agency may proceed with debarment or suspension and may place the Contractor in the Contractor Responsibility File.

55. CONTRACTOR INTEGRITY PROVISIONS

It is essential that those who seek to contract with the Commonwealth of Pennsylvania observe high standards of honesty and integrity. They must conduct themselves in a manner that fosters public confidence in the integrity of the Commonwealth procurement process.

In furtherance of this policy, Contractor agrees to the following:

(a) Contractor shall maintain the highest standards of honesty and integrity during the performance of this contract and shall take no action in violation of state or federal laws or regulations or any other applicable laws or regulations, or other requirements applicable to Contractor or that govern contracting with the Commonwealth.

(b) Contractor shall establish and implement a written business integrity policy, which includes, at a minimum, the requirements of these provisions as they relate to Contractor employee activity with the Commonwealth and Commonwealth employees, and which is distributed and made known to all Contractor employees.

(c) Contractor, its affiliates, agents and employees shall not influence, or attempt to influence, any Commonwealth employee to breach the standards of ethical conduct for Commonwealth employees set forth in the *Public Official and Employees Ethics Act, 65 Pa.C.S. §§1101 et seq.*; the *State Adverse Interest Act, 71 P.S. §776.1 et seq.*; and the *Governor's Code of Conduct, Executive Order 1980-18, 4 Pa. Code §7.151 et seq.*, or to breach any other state or federal law or regulation.

(d) Contractor, its affiliates, agents and employees shall not offer, give, or agree or promise to give any gratuity to a Commonwealth official or employee or to any other person at the direction or request of any Commonwealth official or employee.

(e) Contractor, its affiliates, agents and employees shall not offer, give, or agree or promise to give any gratuity to a Commonwealth official or employee or to any other person, the acceptance of which would violate the *Governor's Code of Conduct, Executive Order 1980-18, 4 Pa. Code §7.151 et seq.* or any statute, regulation, statement of policy, management directive or any other published standard of the Commonwealth.

(f) Contractor, its affiliates, agents and employees shall not, directly or indirectly, offer, confer, or agree to confer any pecuniary benefit on anyone as consideration for the decision, opinion, recommendation, vote, other exercise of discretion, or violation of a known legal duty by any Commonwealth official or employee.

(g) Contractor, its affiliates, agents, employees, or anyone in privity with him or her shall not accept or agree to accept from any person, any gratuity in connection with the performance of work under the contract, except as provided in the contract.

(h) Contractor shall not have a financial interest in any other contractor, subcontractor, or supplier providing services, labor, or material on this project, unless the financial interest is disclosed to the Commonwealth in writing and the Commonwealth consents to Contractor's financial interest prior to Commonwealth execution of the contract. Contractor shall disclose the financial interest to the Commonwealth at the time of bid or proposal submission, or if no bids or proposals are solicited, no later than Contractor's submission of the contract signed by Contractor.

(i) Contractor, its affiliates, agents and employees shall not disclose to others any information, documents, reports, data, or records provided to, or prepared by, Contractor under this contract without the prior written approval of the Commonwealth, except as required by the *Pennsylvania Right-to-Know Law, 65 P.S. §§ 67.101-3104*, or other applicable law or as otherwise provided in this contract. Any information, documents, reports, data, or records secured by Contractor from the Commonwealth or a third party in connection with the performance of this contract shall be kept confidential unless disclosure of such information is:

(1) Approved in writing by the Commonwealth prior to its disclosure; or

(2) Directed by a court or other tribunal of competent jurisdiction unless the contract requires prior Commonwealth approval; or

(3) Required for compliance with federal or state securities laws or the requirements of national securities exchanges; or

(4) Necessary for purposes of Contractor's internal assessment and review; or

(5) Deemed necessary by Contractor in any action to enforce the provisions of this contract or to defend or prosecute claims by or against parties other than the Commonwealth; or

(6) Permitted by the valid authorization of a third party to whom the information, documents, reports, data, or records pertain: or

(7) Otherwise required by law.

(j) Contractor certifies that neither it nor any of its officers, directors, associates, partners, limited partners or individual owners has been officially notified of, charged with, or convicted of any of the following and agrees to immediately

Comment [A104]: Contractor proposes deleting this section (i), since this is covered in detail in Section 37

Comment [A105]: Contractor proposes that the Commonwealth is protected by the compliance with laws provisions

notify the Commonwealth agency contracting officer in writing if and when it or any officer, director, associate, partner, limited partner or individual owner has been officially notified of, charged with, convicted of, or officially notified of a governmental determination of any of the following:

(1) Commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements or receiving stolen property.

(2) Commission of fraud or a criminal offense or other improper conduct or knowledge of, approval of or acquiescence in such activities by Contractor or any affiliate, officer, director, associate, partner, limited partner, individual owner, or employee or other individual or entity associated with:

i. obtaining;

ii. attempting to obtain; or

iii. performing a public contract or subcontract.

Contractor's acceptance of the benefits derived from the conduct shall be deemed evidence of such knowledge, approval or acquiescence.

(3) Violation of federal or state antitrust statutes.

(4) Violation of any federal or state law regulating campaign contributions.

(5) Violation of any federal or state environmental law.

(6) Violation of any federal or state law regulating hours of labor, minimum wage standards or prevailing wage standards; discrimination in wages; or child labor violations.

(7) Violation of the *Act of June 2, 1915 (P.L.736, No. 338)*, known as the *Workers' Compensation Act*, 77 P.S. 1 *et seq.*

(8) Violation of any federal or state law prohibiting discrimination in employment.

(9) Debarment by any agency or department of the federal government or by any other state.

(10) Any other crime involving moral turpitude or business honesty or integrity.

Contractor acknowledges that the Commonwealth may, in its sole discretion, terminate the contract for cause upon such notification or when the Commonwealth otherwise learns that Contractor has been officially notified, charged, or convicted.

(k) If this contract was awarded to Contractor on a non-bid basis, Contractor must, (as required by *Section 1641* of the *Pennsylvania Election Code*) file a report of political contributions with the Secretary of the Commonwealth on or before February 15 of the next calendar year. The report must include an itemized list of all political contributions known to Contractor by virtue of the knowledge possessed by every officer, director, associate, partner, limited partner, or individual owner that has been made by:

(1) Any officer, director, associate, partner, limited partner, individual owner or members of the immediate family when the contributions exceed an aggregate of one thousand dollars ($1,000) by any individual during the preceding year; or

(2) Any employee or members of his immediate family whose political contribution exceeded one thousand dollars ($1,000) during the preceding year.

To obtain a copy of the reporting form, Contractor shall contact the Bureau of Commissions, Elections and Legislation, Division of Campaign Finance and Lobbying Disclosure, Room 210, North Office Building, Harrisburg, PA 17120.

(l) Contractor shall comply with requirements of the *Lobbying Disclosure Act, 65 Pa.C.S. § 13A01 et seq*., and the regulations promulgated pursuant to that law. Contractor employee activities prior to or outside of formal Commonwealth procurement communication protocol are considered lobbying and subjects the Contractor employees to the registration and reporting requirements of the law. Actions by outside lobbyists on Contractor's behalf, no matter the procurement stage, are not exempt and must be reported.

(m) When Contractor has reason to believe that any breach of ethical standards as set forth in law, the Governor's Code of Conduct, or in these provisions has occurred, or may occur, including but not limited to contact by a Commonwealth officer or employee which, if acted upon, would violate such ethical standards, Contractor shall immediately notify the Commonwealth contracting officer or Commonwealth Inspector General in writing.

Comment [A106]: Contractor proposes more specific language regarding the role(s) within the Contractor organization and it is based on factual circumstances

(n) Contractor, by submission of its bid or proposal and/or execution of this contract and by the submission of any bills, invoices or requests for payment pursuant to the contract, certifies and represents that it has not violated any of these contractor integrity provisions in connection with the submission of the bid or proposal, during any contract negotiations or during the term of the contract.

Comment [A107]: Contractor proposes deleting subsection (n)

(o) Contractor shall cooperate with the Office of Inspector General in its investigation of any alleged Commonwealth employee breach of ethical standards and any alleged Contractor non-compliance with these provisions. Contractor agrees to make identified Contractor employees available for interviews at reasonable times and places. Contractor, upon the inquiry or request of the Office of Inspector General, shall provide, or if appropriate, make promptly available for inspection or copying, any information of any type or form deemed relevant by the Inspector General to Contractor's integrity and compliance with these provisions. Such information may include, but shall not be limited to, Contractor's business or financial records, documents or files of any type or form that refers to or concern this contract.

(p) For violation of any of these Contractor Integrity Provisions, the Commonwealth may terminate this and any other contract with Contractor, claim liquidated damages in an amount equal to the value of anything received in breach of these provisions, claim damages for all additional costs and expenses incurred in obtaining another contractor to complete performance under this contract, and debar and suspend Contractor from doing business with the Commonwealth. These rights and remedies are cumulative, and the use or non-use of any one shall not preclude the use of all or any other. These rights and remedies are in addition to those the Commonwealth may have under law, statute, regulation, or otherwise.

(q) For purposes of these Contractor Integrity Provisions, the following terms shall have the meanings found in this Section (q).

(1) "Confidential information" means information that a) is not already in the public domain; b) is not available to the public upon request; c) is not or does not become generally known to Contractor from a third party without an obligation to maintain its confidentiality; d) has not become generally known to the public through an act or omission of Contractor; or e) has not been independently developed by Contractor without the use of confidential information of the Commonwealth.

(2) **"**Consent" means written permission signed by a duly authorized officer or employee of the Commonwealth, provided that where the material facts have been disclosed, in writing, by pre-qualification, bid, proposal, or contractual terms, the Commonwealth shall be deemed to have consented by virtue of execution of this contract.

(3) **"**Contractor" means the individual or entity that has entered into this contract with the Commonwealth, including those directors, officers, partners, managers, and owners having more than a five percent interest in Contractor.

(4) "Financial interest" means:

Comment [A108]: Contractor proposes that specific type of exclusions should be identified For example, attorney / client privileges

Comment [A109]: Contractor proposes that a termination right of this Contract only should apply only if "material breach", and that damages should be subject to the liability provisions

i. Ownership of more than a five percent interest in any business; or

ii. Holding a position as an officer, director, trustee, partner, employee, or holding any position of management.

(5) "Gratuity" means tendering, giving or providing anything of more than nominal monetary value including, but not limited to, cash, travel, entertainment, gifts, meals, lodging, loans, subscriptions, advances, deposits of money, services, employment, or contracts of any kind. The exceptions set forth in the *Governor's Code of Conduct, Executive Order 1980-18*, the *4 Pa. Code §7.153(b)*, shall apply.

(6) "Immediate family" means a spouse and any unemancipated child.

(7) "Non-bid basis" means a contract awarded or executed by the Commonwealth with Contractor without seeking bids or proposals from any other potential bidder or offeror.

(8) "Political contribution" means any payment, gift, subscription, assessment, contract, payment for services, dues, loan, forbearance, advance or deposit of money or any valuable thing, to a candidate for public office or to a political committee, including but not limited to a political action committee, made for the purpose of influencing any election in the Commonwealth of Pennsylvania or for paying debts incurred by or for a candidate or committee before or after any election.

56. RIGHT-TO-KNOW LAW

(a) The Pennsylvania Right-to-Know Law, 65 P.S. §§ 67.101-3104, ("RTKL") applies to this Contract.

(b) If the Commonwealth requires the Contractor's assistance in any matter arising out of the RTKL related to this Contract, it shall notify the Contractor using the legal contact information provided in this Contract. The Contractor, at any time, may designate a different contact for such purpose upon reasonable prior written notice to the Commonwealth.

(c) Upon written notification from the Commonwealth that it requires the Contractor's assistance in responding to a request under the RTKL for information related to this Contract that may be in the Contractor's possession, constituting, or alleged to constitute, a public record in accordance with the RTKL ("Requested Information"), the Contractor shall:

(1) Provide the Commonwealth, within ten (10) calendar days after receipt of written notification, access to, and copies of, any document or information in the Contractor's possession arising out of this Contract that the

Commonwealth reasonably believes is Requested Information and may be a public record under the RTKL; and

(2) Provide such other assistance as the Commonwealth may reasonably request, in order to comply with the RTKL with respect to this Contract.

(d) If the Contractor considers the Requested Information to include a request for a Trade Secret or Confidential Proprietary Information, as those terms are defined by the RTKL, or other information that the Contractor considers exempt from production under the RTKL, the Contractor must notify the Commonwealth and provide, within seven (7) calendar days of receiving the written notification, a written statement signed by a representative of the Contractor explaining why the requested material is exempt from public disclosure under the RTKL.

(e) The Commonwealth will rely upon the written statement from the Contractor in denying a RTKL request for the Requested Information unless the Commonwealth determines that the Requested Information is clearly not protected from disclosure under the RTKL. Should the Commonwealth determine that the Requested Information is clearly not exempt from disclosure, the Contractor shall provide the Requested Information within five (5) business days of receipt of written notification of the Commonwealth's determination.

(f) If the Contractor fails to provide the Requested Information within the time period required by these provisions, the Contractor shall indemnify and hold the Commonwealth harmless for any damages, penalties, costs, detriment or harm that the Commonwealth may incur as a result of the Contractor's failure, including any statutory damages assessed against the Commonwealth.

Comment [A110]: Contractor proposes limiting the indemnity obligation to just government fines and penalties assessed against the Commonwealth and capping this indemnity obligation

(g) The Commonwealth will reimburse the Contractor for any costs associated with complying with these provisions only to the extent allowed under the fee schedule established by the Office of Open Records or as otherwise provided by the RTKL if the fee schedule is inapplicable.

(h) The Contractor may file a legal challenge to any Commonwealth decision to release a record to the public with the Office of Open Records, or in the Pennsylvania Courts, however, the Contractor shall indemnify the Commonwealth for any legal expenses incurred by the Commonwealth as a result of such a challenge and shall hold the Commonwealth harmless for any damages, penalties, costs, detriment or harm that the Commonwealth may incur as a result of the Contractor's failure, including any statutory damages assessed against the Commonwealth, regardless of the outcome of such legal challenge. As between the parties, the Contractor agrees to waive all rights or remedies that may be available to it as a result of the Commonwealth's disclosure of Requested Information pursuant to the RTKL.

Comment [A111]: Contractor proposes the deletion of subsection (h) as it is inappropriate to indemnify Commonwealth in the event Contractor challenge a disclosure by Commonwealth under the RTKL, even if Contractor wins the challenge; nor is it reasonable to waive all Contractor rights from any disclosure by Commonwealth under the RTKL

(i) The Contractor's duties relating to the RTKL are continuing duties that survive the expiration of this Contract and shall continue as long as the Contractor has Requested Information in its possession.

57. ENVIRONMENTAL PROTECTION

In carrying out this Contract, the Contractor shall minimize pollution and shall strictly comply with all applicable environmental laws and regulations, including the *Clean Streams Law*, Act of June 22, 1937, as amended; the *Pennsylvania Solid Waste Management Act*, Act of July 7, 1980 (P.L. 380, No. 97), as amended; and the *Dam Safety and Encroachment Act*, Act of November 26, 1978 (P.L. 1375, No. 325), as amended.

58. ASSIGNABILITY

a) This Contract may not be assigned by Contractor, either in whole or in part without the prior written consent of the Commonwealth, which consent shall not be unreasonably withheld, conditioned, or delayed. Transfer of the majority of the stock or the majority of the assets of a corporation, or other change of ownership will be deemed an assignment. In the event that Contractor requests the right to assign this Contract, including an assignment to an affiliate or subsidiary, Contractor will provide the Commonwealth with copies of the following documents (to the extent they exist): most recent audited financial statements and such other documents as Commonwealth reasonably deems necessary. Within thirty (30) days of such notice, the Commonwealth shall provide its written decision regarding the requested assignment.

b) Subject to the terms and conditions of this *Section 58* (Assignability), the Contract is binding upon the parties and their respective successors and assigns.

c) Any assignment consented to by the Commonwealth shall be evidenced by a written assignment agreement executed by the Contractor and its assignee in which the assignee agrees to be legally bound by all of the terms and conditions of the Contract and to assume the duties, obligations, and responsibilities being assigned. In addition, the assignee must execute a contract with the Commonwealth in the same form as this Contract.

d) Notwithstanding the foregoing, the Contractor may, without the consent of the Commonwealth, assign its rights to payment to be received under the Contract, provided that the Contractor provides written notice of such assignment to the Commonwealth together with a written acknowledgement from the assignee that any such payments are subject to all of the terms and conditions of the Contract.

e) A change of name by the Contractor, following which the Contractor's federal identification number remains unchanged, is not considered to be an assignment. The Contractor shall give the Commonwealth written notice of any such change of name.

59. INDEPENDENT CAPACITY OF CONTRACTOR

a) The parties to this Contract agree that the Services performed by the Contractor under the terms of this Contract are performed as an independent contractor and nothing contained in this Contract shall be construed to make either Contractor or Commonwealth partners, joint venturers, principals, agents or employees of the other, except only to the extent that Contractor is expressly appointed under the Contract to act as the agent of Commonwealth and, in those cases, only to the limited extent of such express appointment. No officer, director, employee, agent, affiliate or contractor retained by Contractor to perform work on Commonwealth's behalf hereunder shall be deemed to be an employee, agent or contractor of Commonwealth. Neither party shall have any right, power or authority, express or implied, to bind the other. As between Contractor and Commonwealth, Contractor is solely responsible for payment of all income, disability, withholding and other employment taxes, and all medical benefit premiums, vacation pay, sick pay and other fringe benefits resulting from Contractor's retention of any such officers, directors, employees, agents or contractors.

b) Except as otherwise provided by the terms of this Contract, the Commonwealth shall have no control over the manner in which the contractual Services are performed by the Contractor, or any subcontractor. Any job specifications or standards of work attached to or incorporated into this Contract or any subcontracting restrictions contained in this Contract shall not be construed as the Commonwealth's direction or control over the manner of the performance of Services provided by the Contractor.

60. THIRD PARTY BENEFICIARIES

Each party intends that this Contract shall not benefit, or create any right or cause of action in or on behalf of, any person or entity other than Commonwealth and Contractor.

61. CERTIFICATION REGARDING SUSPENSION

Contractor certificates that it is not currently under suspension or debarment by Commonwealth, any other state, or the Federal government.

62. SUSPENSION OF SUBCONTRACTORS

If Contractor enters into any subcontracts or employs under this Contract any subcontractor's individuals who are currently suspended or debarred by Commonwealth

or the Federal government or who become suspended or debarred by Commonwealth or the Federal government during the term of this Contract or any extensions or renewals thereof, Commonwealth shall have the right to require Contractor to terminate such subcontracts or employment.

63. ASSIGNMENT OF RIGHTS UNDER THE ANTITRUST LAWS

It is recognized that in actual economic practice, overcharges by Contractor's suppliers resulting from violations of state and federal antitrust laws are in fact borne by the Commonwealth. As part of the consideration for the award of this Contract, and intending to be legally bound, the Contractor assigns to the Commonwealth all rights, title, and interest in and to any claims Contractor now has or may hereafter acquire under state and federal antitrust laws relating to the goods and services which are provided by the Contractor under this Contract.

64. SIGNIFICANT EVENTS

Commonwealth requires the right to adjust the scope or volume of Services to be provided in response to an event, or series of events taken together, that have or will have a significant and sustained impact on Commonwealth's demand for the Services, and requires Contractor to equitably adjust the price for the Services to reflect any such changes to the scope or volume of the Services.

Comment [A112]: Contractor requests additional discussion on the "adjust the scope or volume of Services" as minimum requirement is not an unusual practice in industry and allows for best competitive pricing

65. FORCE MAJEURE

No failure or delay by Contractor in the performance of its obligations pursuant to this Contract shall be deemed a default of this Contract or a ground for termination hereunder (except as provided in this Section 65 (Force Majeure) to the extent such failure or delay is due to a Force Majeure Event and such Force Majeure Event could not have been prevented by Contractor's reasonable precautions or efforts to mitigate damage. The occurrence of a Force Majeure Event does not limit or otherwise affect Contractor's obligation to provide normal recovery procedures and any disaster recovery services described in Section 15 (Disaster Recovery and Business Continuity) to the extent such obligations are not directly precluded by the occurrence of that Force Majeure Event. The occurrence of a Force Majeure Event in respect of another customer of Contractor does not constitute a Force Majeure Event under this Contract, except to the extent such customer and Commonwealth experience the same Force Majeure Event at a site shared by Commonwealth and such other customer. The party delayed by a Force Majeure Event shall immediately orally notify the other party (to be confirmed in a written notice within three (3) business days after the inception of such delay) of the occurrence of a Force Majeure Event and describe in reasonable detail the nature of the Force Majeure Event. From and after becoming aware of a Force Majeure Event, the party delayed thereby shall undertake all commercially reasonable measures (including the use of alternative sources for products and services and workaround plans) to mitigate the impact and duration of the Force Majeure Event, and such party shall consistently and diligently prosecute such measures until the Force Majeure Event is relieved. If

Contractor does not fulfill its obligations under the immediately preceding sentence and, as a result thereof, such Force Majeure Event precludes Contractor from delivering the Services for more than forty five (45) days, Commonwealth may terminate this Contract for cause under Section 32(c), but without regard to any additional cure periods provided for therein. In any other case in which a Force Majeure Event precludes Contractor from delivering the Services for more than forty-five (45) days (without consideration of any such Services performed from a business recovery center under Section 15 (Disaster Recovery and Business Continuity)), Commonwealth may terminate this Contract for convenience under Section 32(a), but without regard to any notice period or additional cure periods provided for therein. In the event of a Force Majeure Event, Contractor shall not increase the Fees under this Contract or charge Commonwealth usage fees in addition to the Fees except for applicable disaster recovery declaration and usage fees in accordance with the provisions of Section 15 (Disaster Recovery and Business Continuity).

Comment [A113]: Contractor proposes to reference only critical services within this section (for example, those covered by Disaster Recovery) Commonwealth can terminate the Contract but not via section 32 (c) Commonwealth can terminate via section 32 (a) with a reduced termination fee

66. CONFLICT OF INTEREST

Contractor, by signing this Contract, covenants that it has no undisclosed public or private interest, direct or indirect, and shall not acquire directly or indirectly any such interest, and that Contractor has no association, direct or indirect, which interest or association does or may conflict in any manner with the performance of the Services or any other obligations of Contractor under this Contract. Any such conflicts shall be disclosed to Commonwealth, and Commonwealth shall determine whether such conflict is cause for termination of this Contract. Contractor further covenants that, in the performance of this Contract, no person having such interest shall be employed by or associated with Contractor.

67. OFFICIALS NOT TO BENEFIT

No official or employee of the Commonwealth and no member of its General Assembly who exercises any functions or responsibilities under this Contract shall participate in any decision relating to this Contract which affects their personal interest or the interest of any corporation, partnership, or association in which they are, directly or indirectly, interested; nor shall any such official or employee of the Commonwealth or member of its General Assembly have any interest, direct or indirect, in this Contract or the proceeds thereof.

68. CONSENTS, APPROVALS, NOTICES AND REQUESTS

Unless otherwise specified in this Contract, all consents, approvals, notices and requests, acceptances or similar actions to be given by either party under this Contract shall not be unreasonably withheld, delayed or conditioned and each party shall make only reasonable requests under this Contract.

69. REQUIRED CONSENTS

The Commonwealth, with reasonable assistance at no additional cost by Contractor and its agents shall obtain all consents, approvals, authorizations, notices, requests and acknowledgements necessary to allow Contractor to use the Commonwealth Software, the Commonwealth Machines and the services under Commonwealth's third party service contracts, all to the extent necessary to enable Contractor to provide the Services to Commonwealth. Commonwealth shall be responsible for all costs and expenses imposed by third parties in connection with obtaining any such consents. Contractor shall obtain all consents, approvals, authorizations, notices, requests and acknowledgements necessary to allow (1) Contractor to use the Contractor Software, the Developed Software and the Contractor Machines to provide the Services to Commonwealth, and (2) Commonwealth to use the Contractor Software in accordance with the terms of this Contract upon the expiration or termination for any reason of Contractor's obligation to provide the Services or of this Contract. Contractor shall be responsible for all costs and expenses imposed by a third party in connection with any such consents described in the foregoing clause (1). Commonwealth's costs and expenses under the foregoing clause (2) shall be governed by the terms of *Section 40(b).02*. Each party shall cooperate with and assist the other party in obtaining the consents contemplated in this *Section 69* (Required Consents).

70. REQUIREMENTS FOR INFORMATION IN LEGAL PROCEEDINGS

a) If the Commonwealth notifies Contractor, or Contractor is otherwise aware, that particular Commonwealth Confidential Information may be within attorney-client or work-product privileges of the Commonwealth, then regardless of any applicable exclusions, Contractor (i) shall not disclose such the Confidential Information or take any other action that would result in waiver of such privileges and (ii) shall instruct all Contractor Personnel who may have access to such communications to maintain privileged material as strictly confidential and otherwise protect the Commonwealth privileges.

b) To the extent requested by the Commonwealth, Contractor shall comply with the Commonwealth's litigation response plan, including policies and procedures to prepare for and respond to discovery requests, subpoenas, investigatory demands, and other requirements for information related to legal and regulatory proceedings, as such plan may be revised from time to time, including preparing for and complying with requirements for preservation and production of data in connection with legal and regulatory proceedings and government investigations. Upon receipt of any request, demand, notice, subpoena, order or other legal information request relating to legal proceedings or investigations by third parties relating to any Materials, the Confidential Information or related Systems in Contractor possession, Contractor shall immediately notify the Commonwealth and provide the Commonwealth with a copy of all documentation of such legal information request, to the extent Contractor legally may do so and shall cooperate with the Commonwealth in responding to such request, demand, notice, subpoena, order or other legal information request.

c) Contractor 's cost of complying with this section shall be at no additional charge to the Commonwealth.

Comment [A114]: Proposed Contractors compliance should be limited to reasonable assistance utilizing existing resources If additional resources are required, it is subject to Change Control procedures

71. EXAMINATION OF RECORDS

The Commonwealth may, at reasonable times and places, audit the books and records of Contractor or its subcontractors to the extent that the books and records relate to the performance of the contract. Contractor shall maintain books and records related to the Contract for a period of three years from the date of final payment under the Contract. Contractor shall include a requirement in agreements with subcontractors that requires the subcontractor to maintain its records for the same length of time.

72. SURVIVAL

Sections 4, 33, 35, 36, 37, 38, 38, 40, 41, 47, 48, 49, 52, 53, 72 shall survive the expiration or termination of the Contract.

73. SEVERABILITY

If any provision of this Contract is held by a court of competent jurisdiction to be contrary to law, then the remaining provisions of this Contract or the application of such provision to persons or circumstances other than those as to which it is invalid or unenforceable shall not be affected thereby, and each such provision of this Contract shall be valid and enforceable to the extent permitted by law.

74. WAIVER

No delay or omission by either party to exercise any right or power it has under this Contract shall impair or be construed as a waiver of such right or power. A waiver by any party of any breach or covenant shall not be construed to be a waiver of any succeeding breach or any other covenant. All waivers must be in writing and signed by the party waiving its rights.

75. PERIOD OF PERFORMANCE

The Contractor, for the life of this Contract, shall complete all Services as specified under the terms of this Contract. In no event shall the Commonwealth be responsible or liable to pay for any Services provided by the Contractor prior to the Effective Date, and the Contractor hereby waives any claim or cause of action for any such Services.

76. SPECIAL REQUIREMENTS

Comment [A115]: Contractor request clarification of this section

The Commonwealth reserves the right to purchase Services covered under this Contract through other procurement methods whenever the Commonwealth deems it to be in its best interest.

77. GOVERNING LAW

This Contract shall be interpreted in accordance with and governed by the laws of the Commonwealth of Pennsylvania, without giving effect to its conflicts of law provisions. Except as set forth in *Section 34* (Contract Controversies), Commonwealth and Contractor agree that the courts of the Commonwealth of Pennsylvania and the federal courts of the Middle District of Pennsylvania shall have exclusive jurisdiction over disputes under this Contract and the resolution thereof. Any legal action relating to this Contract must be brought in Dauphin County, Pennsylvania, and the parties agree that jurisdiction and venue in such courts is appropriate.

78. COMPLIANCE WITH LAWS

a) The Contractor shall comply with all federal, state, and local laws applicable to its work, including, but not limited to, all statutes, regulations and rules that are in effect as of the Effective Date of the Contract and shall procure at its expense all licenses and all permits necessary for the fulfillment of its obligation.

b) If any existing law, regulation or policy is changed or if any new law, regulation or policy is enacted that affects the Services provided under this Contract, the parties to the Contract shall modify this Contract, via *Section 27* (Change Control), to the extent reasonably necessary to:

(1) Ensure that such Services will be in full compliance with such laws, regulations and/or policies; and

(2) Modify the rates applicable to such Services; and

(3) Address any schedule impacts.

Comment [A116]: Contractor proposes to differentiate between Contractor Laws (those applicable to provider of IT services) and Commonwealth Laws

79. SMALL DIVERSE BUSINESS COMMITMENT

Contractor shall meet and maintain the commitments to small diverse businesses in the Small Diverse Business ("SDB") portion of its Proposal. Any proposed change to a SDB commitment must be submitted to the DGS Bureau of Small Business Opportunities ("BSBO"), which will make a recommendation as to a course of action to the Commonwealth Contracting Officer. Contractor shall complete the Prime Contractor's Quarterly Utilization Report and submit it to the Commonwealth Contracting Officer and BSBO within ten (10) workdays at the end of each calendar quarter that the Contract is in effect.

80. ACKNOWLEDGEMENT

Commonwealth and Contractor each acknowledge that the limitations and exclusions contained in this Contract have been the subject of active and complete negotiation between the parties and represent the parties' Contract based upon the level of risk to

Commonwealth and Contractor associated with their respective obligations under this Contract and the payments to be made to Contractor and credits to be issued to, and Services to be provided to, Commonwealth pursuant to this Contract. The parties agree that the terms and conditions of this Contract shall not be construed in favor of or against any party by reason of the extent to which any party or its professional advisors participated in the preparation of this Contract.

81. COVENANT OF FURTHER ASSURANCES

Commonwealth and Contractor covenant and agree that, subsequent to the execution and delivery of this Contract and without any additional consideration, each of Commonwealth and Contractor will execute and deliver any further legal instruments and perform any commercially reasonable acts which are or may become necessary to effectuate the purposes of this Contract.

82. COVENANT OF GOOD FAITH

Each Party agrees that, in its respective dealings with the other Party under or in connection with this Contract, it shall act in good faith.

83. AMENDMENTS

No amendment to, or change, waiver, or discharge of, any provision of this Contract shall be valid unless in writing and signed by an authorized representative of the party against which such amendment, change, waiver or discharge is sought to be enforced.

84. ENTIRE CONTRACT

This Contract is the entire Contract between the parties with respect to its subject matter, and there are no other representations, understandings or Contracts between the parties relative to such subject matter

APPENDIX A - BUSINESS ASSOCIATE APPENDIX LANGUAGE

COMMONWEALTH OF PENNSYLVANIA
BUSINESS ASSOCIATE AGREEMENT

WHEREAS, the ***[name of program and/or Department]*** (Covered Entity) and Contractor (Business Associate) intend to protect the privacy and security of certain Protected Health Information (PHI) to which Business Associate may have access in order to provide goods or services to or on behalf of Covered Entity, in accordance with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5 (Feb. 17, 2009), the HIPAA Privacy Rule (Privacy Rule), 45 C.F.R. Parts 160 and 164, and the HIPAA Security Rule (Security Rule), 45 C.F.R. Parts 160, 162 and 164, and all other applicable laws; and

WHEREAS, Business Associate may receive PHI from Covered Entity, or may create or obtain PHI from other parties for use on behalf of Covered Entity, which PHI can be used or disclosed only in accordance with this Agreement and the standards established by applicable laws; and

WHEREAS, Business Associate may receive PHI from Covered Entity, or may create or obtain PHI from other parties for use on behalf of Covered Entity that is in electronic form, which PHI must be handled in accordance with this Agreement and the standards established by HIPAA and the Security Rule and other applicable laws; and

NOW, THEREFORE, the parties to this Agreement set forth the following as the terms and conditions of their understanding.

1. Definitions.

a) "Breach" shall have the meaning assigned to such term at 42 USCS § 17921 and HIPAA regulations at 45 C.F.R. § 164.402.

b) "Business Associate" shall have the meaning given to such term under the Privacy and Security Rules, including but not limited to, 45 C.F.R. §160.103.

c) "Covered Entity" shall have the meaning given to such term under the Privacy and Security Rules, including, but not limited to, 45 C.F.R. §160.103.

d) "HIPAA" shall mean the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191.

e) "Privacy Rule" shall mean the standards for privacy of individually identifiable health information in 45 C.F.R. Parts 160 and 164.

f) "Protected Health Information" or "PHI" shall have the meaning given to such term under HIPAA and the HIPAA Regulations in 45 C.F.R. Parts 160, 162 and 164, including, but not limited to 45 C.F.R. §160.103.

g) "Security Rule" shall mean the security standards in 45 C.F.R. Parts 160, 162 and 164.

Comment [A117]: Contractor will comply with all federal or state laws applicable to its use or disclosure of information that constitutes personal health information (PHI) as defined by the Health Insurance Portability and Accountability Act (H PAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5 (Feb. 17, 2009), the H PAA Privacy Rule (Privacy Rule), 45 C F.R. Parts 160 and 164, and the H PAA Security Rule (Security Rule), 45 C F.R. Parts 160, 162 and 164. Contractor understands that, as part of its Contract with the Commonwealth, that it will be required to agree to terms and conditions of a Business Associate Agreement. Contractor has reviewed the Commonwealth's terms Appendix A of the Contract Terms and Conditions, and believes some aspects of the terms require discussion and clarification between the parties so that provisions are consistent with and don't extend beyond the requirements of the applicable privacy laws, and believes some of the provisions need adjustment so that they are appropriate to the nature and extent of the Provider's access to personal health information and individual record sets. Contractor proposes to discuss these concerns and negotiate certain clarifications in the terms of this section upon award

h) Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5 (Feb. 17, 2009), the HIPAA Privacy Rule (Privacy Rule), 45 C.F.R. Parts 160 and 164, and the HIPAA Security Rule (Security Rule), 45 C.F.R. Parts 160, 162 and 164.

2. Stated Purposes For Which Business Associate May Use Or Disclose PHI. The Parties hereby agree that Business Associate shall be permitted to use and/or disclose PHI provided by or obtained on behalf of Covered Entity for purposes state in Attachment 1 , except as otherwise stated in this Agreement.

NO OTHER USES OR DISCLOSURES OF PHI ARE PERMITTED.

3. BUSINESS ASSOCIATE OBLIGATIONS:

i) Security and Privacy Provisions Applicable to Business Associate. Business Associate shall abide by the security and privacy provisions applicable to Covered Entities which are made applicable to the Business Associate by 42 USCS § 17931 and 17934.

j) Limits On Use And Further Disclosure Established By Agreement And Law. Business Associate hereby agrees that the PHI provided by, or created or obtained on behalf of Covered Entity shall not be further used or disclosed other than as permitted or required by this Agreement or as Required by Law.

k) Appropriate Safeguards. Business Associate shall establish and maintain appropriate safeguards to prevent any use or disclosure of PHI other than as provided for by this Agreement. Appropriate safeguards shall include implementing administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI that is created, received, maintained, or transmitted on behalf of the Covered Entity.

l) Reports Of Improper Use Or Disclosure. Business Associate hereby agrees that it shall report to the Covered Entity's Privacy Officer, or his designee**,** and the Covered entity's legal office, within two (2) days of discovery any Breach or use or disclosure of PHI not provided for or allowed by this Agreement (unless some more stringent standard applies under this Agreement). Business Associate agrees to conduct reasonable diligence to discover improper use or disclosure of PHI.

.

Such notification shall be written and shall include the identification of each individual whose unsecured PHI has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, or disclosed during the improper use or disclosure or Breach. An improper use or disclosure or Breach shall be treated as discovered by the Business Associate on the first day on which it is known to the Business Associate (including any person other than the person committing the Breach, that is an employee, officer, or other agent of the Business Associate) or should reasonably have been known to the Business Associate (or such person) to have occurred.

d) Reports Of Security Incidents. In addition to following the Breach notification requirements in section 13402 of the HITECH Act and related regulations and guidance, Business Associate shall report to Covered Entity's Privacy Officer, or his designee, within two (2) days of discovery any Security Incident of which it becomes aware.

e) Subcontractors And Agents. Business Associate hereby agrees that any time PHI is provided or made available to any subcontractors or agents, Business Associate shall provide only the minimum necessary PHI for the purpose of the covered transaction and shall first enter into a subcontract or contract with the subcontractor or agent that contains the same terms, conditions and restrictions on the use and disclosure of PHI as contained in this Agreement.

f) Right Of Access To PHI. Business Associate hereby agrees to allow an individual who is the subject of PHI maintained in a designated record set, to have access to and copy that individual's PHI within five (5) business days of receiving a written request from the Covered Entity or individual. Business Associate shall provide PHI in the format requested, unless it cannot readily be produced in such format, in which case it shall be provided in standard hard copy. If any individual requests from Business Associate or its agents or subcontractors access to PHI, Business Associate shall notify Covered Entity of same within two (2) business days. Business associate shall further conform with and meet all of the requirements of 45 C.F.R. §164.524, 42 USCS § 17936(e), and other applicable laws.

g) Amendment And Incorporation Of Amendments. Within five (5) business days of receiving a request from Covered Entity for an amendment of PHI maintained in a designated record set, Business Associate shall make the PHI available and incorporate the amendment to enable Covered Entity to comply with 45 C.F.R. §164.526 and other applicable laws. If any individual requests an amendment from Business Associate or its agents or subcontractors, Business Associate shall notify Covered Entity within five (5) business days.

h) Provide Accounting Of Disclosures. Business Associate agrees to maintain a record of all disclosures of PHI in accordance with 45 C.F.R. §164.528, 42 USCS § 17935(c), and other applicable laws. Such records shall include, for each disclosure, the date of the disclosure, the name and address of the recipient of the PHI, a description of the PHI disclosed, the name of the individual who is the subject of the PHI disclosed, the purpose of the disclosure, and shall include disclosures made on or after the date that is six (6) years prior to the request or April 14, 2003, whichever is later. Business Associate shall make such record available to the individual or the Covered Entity within five (5) business days of a request for an accounting of disclosures, or within such other time as may be dictated by applicable law.

i) Access To Books And Records. Business Associate hereby agrees to make its internal practices, books, and records relating to the use or disclosure of PHI received from, or created or received by Business Associate on behalf of the Covered Entity, available to the Secretary of Health and Human Services or designee for purposes of determining compliance with the HIPAA Privacy Regulations.

j) Return Or Destruction Of PHI. At termination of this Agreement, Business Associate hereby agrees to return or destroy all PHI provided by or obtained on behalf of Covered Entity. Business Associate agrees not to retain any copies of the PHI after termination of

this Agreement. If return or destruction of the PHI is not feasible, Business Associate agrees to extend the protections of this Agreement to limit any further use or disclosure until such time as the PHI may be returned or destroyed. If Business Associate elects to destroy the PHI, it shall certify to Covered Entity that the PHI has been destroyed.

k) Maintenance of PHI. Notwithstanding Section 5(j) of this Agreement, Business Associate and its subcontractors or agents shall retain all PHI throughout the term of the Agreement and shall continue to maintain the information required under §5(h) of this Agreement for a period of six (6) years after termination of the Agreement, unless Covered Entity and Business Associate agree otherwise.

l) Mitigation Procedures. Business Associate agrees to establish and to provide to Covered Entity upon request, procedures for mitigating, to the maximum extent practicable, any harmful effect from the use or disclosure of PHI in a manner contrary to this Agreement or the Privacy Rule. Business Associate further agrees to mitigate any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of this Agreement or the Privacy Rule.

m) Training. Business Associate will train all members of its workforce on its policies and procedures with respect to PHI as necessary and appropriate for the workforce members to carry out the functions required by this contract.

n) Sanction Procedures. Business Associate agrees that it shall develop and implement a system of sanctions for any employee, subcontractor or agent who violates this Agreement or other applicable laws.

o) Grounds For Breach by Covered Entity. Upon Business Associate's knowledge of a material breach by Commonwealth of this Business Associate Agreement, Business Associate shall notify Commonwealth of such breach and Commonwealth shall have at least thirty (30) days to cure such breach. In the event Commonwealth does not cure the breach~~,~~ Business Associate shall have the right to report the violation to the Secretary. Notwithstanding any other language in this Agreement, the parties agree that termination by the Business Associate is infeasible.

p) Grounds For Breach. Any non-compliance by Business Associate with this Agreement or the Privacy or Security Rules will automatically be considered to be a breach of the Agreement, if Business Associate knew or reasonably should have known of such non-compliance and failed to immediately take reasonable steps to cure the non-compliance. Business Associate shall have thirty (30) days to cure such breach from the date of notice to cure by the Commonwealth. In the event Business Associate does not cure the breach, the Commonwealth shall have the right to immediately terminate this Agreement and the underlying agreement. If termination is infeasible, the Commonwealth shall report the violation to the Secretary.

q) Termination by Commonwealth. Business Associate authorizes termination of this Agreement by the Commonwealth if the Commonwealth determines, in its sole discretion, that the Business Associate has violated a material term of this Agreement.

r) Failure to Perform Obligations. In the event Business Associate fails to perform its obligations under this Agreement, Covered Entity may immediately discontinue providing PHI to Business Associate. Covered Entity may also, at its option, require

Business Associate to submit to a plan of compliance, including monitoring by Covered Entity and reporting by Business Associate, as Covered Entity in its sole discretion determines to be necessary to maintain compliance with this Agreement and applicable law.

s) Privacy Practices. The Department will provide and Business Associate shall immediately begin using any applicable form, including but not limited to, any form used for Notice of Privacy Practices, Accounting for Disclosures, or Authorization, upon the effective date designated by the Program or Department. The Department retains the right to change the applicable privacy practices, documents and forms. The Business Associate shall implement changes as soon as practicable, but not later than 45 days from the date of notice of the change.

4. OBLIGATIONS OF COVERED ENTITY:

a) Provision of Notice of Privacy Practices. Covered Entity shall provide Business Associate with the notice of privacy practices that the Covered Entity produces in accordance with applicable laws, as well as changes to such notice.

b) Permissions. Covered Entity shall provide Business Associate with any changes in, or revocation of, permission by individual to use or disclose PHI of which Covered Entity is aware, if such changes affect Business Associate's permitted or required uses and disclosures.

c) Restrictions. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of PHI that the Covered Entity has agreed to in accordance with 45 C.F.R. §164.522 and other applicable laws, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

5. MISCELLANEOUS:

a) Regulatory References. A reference in this Appendix to a section in the Privacy or Security Rules means the section as in effect or as amended as reasonably determined by the Covered Entity.

b) Amendment. The Parties agree to take such action as is necessary to amend this Appendix from time to time as is necessary for the Covered Entity to comply with the requirements of the Privacy and Security Rules and the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.

c) Survival. The respective rights and obligations of Business Associate under section 5(i) of this Appendix shall survive the termination of the Agreement.

d) Interpretation. Any ambiguity in this Appendix shall be resolved to permit Covered Entity to comply with the Privacy and Security Rules as reasonably determined by the Covered Entity.

e) Changes in Law. Business Associate shall comply with all applicable privacy and security rules and regulations, including but not limited to HIPAA regulations and the HITECH Act and HITECH regulations which are now in effect or which take effect during the term of this contract.

Attachment 1 to Commonwealth of Pennsylvania Business Associate Agreement

Permitted Uses and Disclosures
of Protected Health Information

1. Purpose of Disclosure of PHI to Business Associate: To allow _____ to meet the requirements of Agreement # _____.

2. Information to be Disclosed to Business Associate: _____.

Use to Effectuate Purpose of Agreement: _____ may use and disclose PHI to the extent contemplated by Agreement #_____ ,and as permitted by law with Commonwealth approval and

9.0 Required Forms

9. REQUIRED FORMS 9-3

9.1 DOMESTIC WORKFORCE UTILIZATION CERTIFICATION (RFP APPENDIX D) 9-5
9.2 COSTARS PROGRAM ELECTION TO PARTICIPATE (RFP APPENDIX E) 9-7
9.3 TRADE SECRET FORM (RFP APPENDIX G) 9-9
9.4 LOBBYING CERTIFICATION AND DISCLOSURE OF LOBBYING ACTIVITIES (RFP APPENDIX H) 9-11

This page intentionally left blank.

9. Required Forms

Unisys includes the following forms:

- Domestic Workforce Utilization Certification (RFP Appendix D)
- Costars Program Election To Participate (RFP Appendix E)
- Trade Secret Form (RFP Appendix G)
- Lobbying Certification And Disclosure Of Lobbying Activities (RFP Appendix H).

This page intentionally left blank.

9.1 Domestic Workforce Utilization Certification (RFP Appendix D)

RFP	*Requirement*
II-11	*Domestic Workforce Utilization Certification. Complete and sign the Domestic Workforce Utilization Certification contained in Appendix D of this RFP. Offerors who seek consideration for this criterion must submit in hardcopy the signed Domestic Workforce Utilization Certification Form in the same sealed envelope with the Technical Submittal.*

This page intentionally left blank.

9.2 Costars Program Election to Participate (RFP Appendix E)

RFP	*Requirement*
II-12	*COSTARS Program Election to Participate. Offerors electing to permit COSTARS members to participate in this Contract should complete and sign the COSTARS Program Election to Participate form contained in Appendix E of this RFP. If the Offeror is asserting that it is a Department of General Services Certified Small Business, also provide an active Department of General Services Small Business Certification. Submit the form and the certification, as applicable, in the same sealed envelope with the Technical Submittal only if the Offeror elects to participate in the program.*

Unisys has indicated in our proposal submission that we are not participating in the COSTARS program for this Commonwealth procurement. Unisys would be interested in discussing and possibly revisiting this decision later during the procurement process.

This page intentionally left blank.

9.3 Trade Secret Form (RFP Appendix G)

This page intentionally left blank.

9.4 Lobbying Certification and Disclosure of Lobbying Activities (RFP Appendix H)

RFP	*Requirement*
II-13	*This Project may be funded, in whole or in part, with federal monies. Public Law 101-121, Section 319, prohibits federal funds from being expended by the recipient or by any lower tier sub-recipients of a federal contract, grant, loan, or a cooperative agreement to pay any person for influencing, or attempting to influence a federal agency or Congress in connection with the awarding of any federal contract, the making of any federal grant or loan, or entering into any cooperative agreement. Offerors who submit proposals in response to this RFP must sign the "Lobbying Certification Form," (attached as Appendix H) and, if applicable, complete the "Disclosure of Lobbying Activities" form available at: http://www.whitehouse.gov/omb/assets/omb/grants/sfllin.pdf.*

This page intentionally left blank.

Trade Secret/Confidential Proprietary Information Notice

Instructions:

The Commonwealth may not assert on behalf of a third party an exception to the public release of materials that contain trade secrets or confidential proprietary information unless the materials are accompanied, at the time they are submitted, by this form or a document containing similar information.

It is the responsibility of the party submitting this form to ensure that all statements and assertions made below are legally defensible and accurate. The Commonwealth will not provide a submitting party any advice with regard to trade secret law.

Name of submitting party:

Contact information for submitting party:

Unisys Corporation
Attention : Mr [redacted]
4750 Lindle Road, Suite 301
Harrisburg, PA 17111
Telephone: (717) 526-1267
E-Mail: [redacted]

Please provide a brief overview of the materials that you are submitting (e.g. bid proposal, grant application, technical schematics):

Request for Proposal - Data Center Computing Services

Please provide a brief explanation of why the materials are being submitted to the Commonwealth (e.g. response to bid #12345, application for grant XYZ being offered by the Department of Health, documents required to be submitted under law ABC)

Response to Request for Proposal #6100022698

Please provide a list detailing which portions of the material being submitted you believe constitute a trade secret or confidential proprietary information, and please provide an explanation of why you think those materials constitute a trade secret or confidential proprietary information. Also, please mark the submitted material in such a way to allow a reviewer to easily distinguish between the parts referenced below. (You may attach additional pages if needed)

Note: The following information will not be considered a trade secret or confidential proprietary information:

- Any information submitted as part of a vendor's cost proposal
- Information submitted as part of a vendor's technical response that does not pertain to specific business practices or product specification
- Information submitted as part of a vendor's technical or disadvantaged business response that is otherwise publicly available or otherwise easily obtained
- Information detailing the name, quantity, and price paid for any product or service being purchased by the Commonwealth

Page Number	Description	Explanation
Section 4.5.2	Contact Information for References	Private information that our clients do not want publicized.
Schedule J.3	SL20 and SL21 Description of Figures J-31 & J-33	Description references actual Commonwealth data and the Commonwealth may not want this to be known.
Schedule F, 3.2.2.3	Appendix to Item #2C	Actual DPH Capacity Planning Report that the Commonwealth may not want to provide.

Acknowledgment

The undersigned party hereby agrees that it has read and completed this form, and has marked the material being submitted in accordance with the instructions above. The undersigned party acknowledges that the Commonwealth is not liable for the use or disclosure of trade secret data or confidential proprietary information that has not been clearly marked as such, and which was not accompanied by a specific explanation included with this form.

The undersigned agrees to defend any action seeking release of the materials it believes to be trade secret or confidential, and indemnify and hold harmless the Commonwealth, its agents and employees, from any judgments awarded against the Commonwealth in favor of the party requesting the materials, and any and all costs connected with that defense. This indemnification survives so long as the Commonwealth has possession of the submitted material, and will apply to all costs unless and until the undersigned provides a written statement or similar notice to the Commonwealth stating that it no longer wishes to exempt the submitted material from public disclosure.

The undersigned acknowledges that the Commonwealth is required to keep all records for at least as long as specified in its published records retention schedule.

The undersigned acknowledges that the Commonwealth reserves the right to reject the undersigned's claim of trade secret/confidential proprietary information if the Commonwealth determines that the undersigned has not met the burden of establishing that the information constitutes a trade secret or is confidential. The undersigned also acknowledges that if only a certain part of the submitted material is found to constitute a trade secret or is confidential, the remainder of the submitted material will become public; only the protected information will be removed and remain nonpublic.

If being submitted electronically, the undersigned agrees that the mark below is a valid electronic signature.

[redacted] Vice President 6-18-2013

Signature Title Date

APPENDIX D

DOMESTIC WORKFORCE UTILIZATION CERTIFICATE

DOMESTIC WORKFORCE UTILIZATION CERTIFICATION FOR MULTIPLE AWARD CONTRACTS (07/24/09)

To the extent permitted by the laws and treaties of the United States, this certification will be used by the Agency in making a best value selection for each particular assignment. Each quote will be evaluated for its commitment to use the domestic workforce in the fulfillment of the contract. Maximum consideration will be given to those suppliers who will perform the contracted direct labor exclusively within the geographical boundaries of the United States or within the geographical boundaries of a country that is a party to the World Trade Organization Government Procurement Agreement. Those who propose to perform a portion of the direct labor outside of the United States and not within the geographical boundaries of a party to the World Trade Organization Government Procurement Agreement will receive a correspondingly smaller score for this criterion. In order to be eligible for any consideration for this criterion, suppliers must complete and sign the following certification. This certification will be included as a contractual obligation when the contract is executed. Failure to complete and sign this certification will result in no consideration being given to the supplier for this criterion.

I, Reed Laughlin, Vice President of Unisys Corporation a Delaware corporation or other legal entity, ("Contractor") located at 801 Lakeview Drive, Blue Bell, PA 19422, having a Social Security or Federal Identification Number of [redacted] do hereby certify and represent to the Commonwealth of Pennsylvania ("Commonwealth") (Check **one** of the boxes below):

X All of the direct labor performed within the scope of services under the contract will be performed exclusively within the geographical boundaries of the United States or one of the following countries that is a party to the World Trade Organization Government Procurement Agreement: Aruba, Austria, Belgium, Bulgaria, Canada, Chinese Taipei, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hong Kong, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Latvia, Liechtenstein, Lithuania, Luxemburg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Singapore, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, and the United Kingdom

OR

_____ **percent (_____%) [Contractor must specify the percentage]** of the direct labor performed within the scope of services under the contract will be performed within the geographical boundaries of the United States or within the geographical boundaries of one of the countries listed above that is a party to the World Trade Organization Government Procurement Agreement. Please identify the direct labor performed under the contract that will be performed outside the United States and not within the geographical boundaries of a party to the World Trade Organization Government Procurement Agreement and identify the country where the direct labor will be performed:

_____

_____

[Use additional sheets if necessary]

The Department of General Services **[or other purchasing agency]** shall treat any misstatement as fraudulent concealment of the true facts punishable under Section 4904 of the *Pennsylvania Crimes Code*, Title 18, of Pa. Consolidated Statutes.

Attest or Witness:

[redacted] 6/18/2013

Signature/Date

Jeffrey R. Carlson SR Eng. Mgr.

Printed Name/Title

Unisys Corporation

[redacted] 6-18-2013

Signature/Date

Reed Laughlin, Vice President

Printed Name/Title

APPENDIX H

Lobbying Certification Form

Certification for Contracts, Grants, Loans, and Cooperative Agreements

The undersigned certifies, to the best of his or her knowledge and belief, that:

(1) No federal appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of any agency, a member of Congress , an officer or employee of Congress, or an employee of a member of Congress in connection with the awarding of any federal contract, the making of any federal grant, the making of any federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any federal contract, grant, loan, or cooperative agreement.

(2) **If any** funds other than federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a member of Congress, an officer or employee of Congress, or an employee of a member of Congress in connection with this federal contract, grant, loan, or cooperative agreement, the undersigned shall complete and submit Standard Form-LLL, "Disclosure of Lobbying Activities," in accordance with its instructions.

(3) The undersigned shall require that the language of this certification be included in the award documents for all subawards at all tiers (including subcontracts, subgrants, and contracts under grants, loans, and cooperative agreements) and that all subrecipients shall certify and disclose accordingly.

This certification is a material representation of fact upon which reliance is placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed under Section 1352, Title 31, U.S. Code. Any person who fails to file the required certification shall be subject to a civil penalty of not less than $10,000 and not more than **$100,000** for such failure.

SIGNATURE [redacted]

TITLE: Vice President

DATE: June 18. 2013

APPENDIX E

COSTARS PROGRAM QUESTIONNAIRE

COSTARS PROGRAM QUESTIONNAIRE

If your firm is awarded a Contract, does it agree to sell the awarded items/services at the same prices and/or discounts, and in accordance with the contractual terms and conditions, to registered COSTARS Members who elect to participate in the contract? If your answer is "YES", your firm agrees to pay the applicable Administrative Fee ($1500 or $500 for Qualified Small Businesses) at the beginning of each contract year and upon each contract renewal date.

Please Answer: **YES _____** **NO X**

If you are asserting that your firm is a Qualified Small Business, have you completed, signed and included with your bid the required Department of General Services Small Business Certification form?

Please Answer: **YES _____** **NO _____**

Unisys Corporation
Corporate or Legal Entity Name

[redacted] 6-18-2013
Signature/Date

Reed Laughlin, Vice President
Printed Name/Title

10.0 Appendices

10. APPENDICES (MANDATORY REQUIREMENTS) 10-3

10.1 APPENDIX A - MANDATORY REQUIREMENTS (EVAL CRITERIA III-1) 10-3
10.1.1 ISO 27001Certification 10-5
10.1.2 ISO 9001 Certification 10-7
10.1.3 ISO/IEC 20000 Certifications 10-9
10.1.4 SSAE 16 Audit Findings Report 10-11
10.1.5 Six Sigma Certifications / Assessments / Evaluations 10-15
10.1.6 ITIL Certifications / Assessments / Evaluations 10-17

This page intentionally left blank.

10. Appendices (Mandatory Requirements)

10.1 Appendix A - Mandatory Requirements (Eval criteria III-1)

RFP	*Requirement*
	Offerors must provide the copies of the ISO 27001, ISO 9001 and ISO/IEC 20000 certifications and SSAE 16 audit findings report as an appendix to the Offeror's technical submittal. The appendix must be titled "Mandatory Requirements."

This page intentionally left blank.

10.1.1 ISO 27001Certification

On the pages that follow please find our Certificate of Registration — Information Security Management System ISO/SEC 27001:2005. Certification Numbers: IS 534949 ([redacted] and IS 552072 (Harrisburg).

10.1.1a.pdf

10.1.1b.pdf

10.1.1a

INTENTIONALLY OMITTED

10.1.1b

INTENTIONALLY OMITTED

This page intentionally left blank.

10.1.2 ISO 9001 Certification

On the pages that follow please find the certification and annexes that Unisys has implemented and maintains a Quality Management System.

10.1.2a.pdf

10.1.2a

INTENTIONALLY OMITTED

This page intentionally left blank.

10.1.3 ISO/IEC 20000 Certifications

On the pages that follow please find the certification and annexes that Unisys has implemented and maintains a Service Management System.

10.1.3a.pdf

10.1.3a

INTENTIONALLY OMITTED

This page intentionally left blank.

10.1.4 SSAE 16 Audit Findings Report

On the pages that follow please find an independent auditor's report on a Description of service organization's system and Suitability of the Design and Operating Effectiveness of Controls – September 1, 2011 through August 31, 2012.

Data Center Hosting Services

Unisys [redacted]
44665 Guildford Drive
[redacted] 20147

10.1.4a.pdf

10.1.4a

INTENTIONALLY OMITTED

This page intentionally left blank.

On the pages that follow please find an independent auditor's report on a description of Unisys Corporation's System and on the Suitability of the Design and Operating Effectiveness of Controls – January 1, 2012 through September 30, 2012.

Global Managed Services (GMS) – Standard Data Centers

Unisys [redacted]
3199 Pilot Knob Road
[redacted] 55121

10.1.4b.pdf

Password UnisysDC2012_18

10.1.4b

INTENTIONALLY OMITTED

This page intentionally left blank.

10.1.5 Six Sigma Certifications / Assessments / Evaluations

Since 2005, Unisys has adopted the Six Sigma Lean methodology and embedded the methodologies and skills across our organization. For example, Six Sigma Lean methods and techniques underpin our Continual Service Improvement and Innovation Program (CSIIP) process and SEO. Our Root Cause Analysis methodologies (such as those for defect reduction) follow the Plan-Do-Check-Act (PDCA) Cycle and use Six Sigma Lean tools such as the fishbone diagram, graphical analysis, mistake-proofing, hypothesis testing, correlation/regression, value stream mapping, and Failure Mode and Effects Analysis (FMEA). Also, key leaders at the Unisys PMO are trained in Six Sigma Lean and, if appropriate, will have access to a Six Sigma Black Belt resource. Our Black Belts across the globe are trained as facilitators for collaborative events such as Kaizen and Innovation Workshops.

Unisys Six Sigma efforts focus on improving customer satisfaction, operational excellence, and overall efficiency of operations that reduce cost. We have a comprehensive Six Sigma Lean training curriculum with instructor-led and self-paced classes in topics such as Define, Measure, Analyze, Improve, and Control (DMAIC); statistical analysis; Lean thinking; Kaizen methods; and A3 problem-solving at the Yellow Belt, Green Belt, and Black Belt levels.

This page intentionally left blank.

10.1.6 ITIL Certifications / Assessments / Evaluations

IT Infrastructure Library (ITIL®) processes are well known as the de facto standard for service delivery and support in most IT organizations. Not only did Unisys implement these processes, but over the past few years we also developed procedures and work instructions that complement the ITIL v3 Framework. These procedures and instructions take a process from a best practice to a powerful daily tool used throughout our global delivery organization. The supporting tools are aligned, consolidated, and rationalized so that we can leverage the long history and legacy of service delivery with the process framework. The processes and procedures that we implement are Incident, Problem, Change, Release, Configuration, Request, and Asset Management. The global ITSM 7.6 toolset and all Service Delivery and Service Management functions support all processes.

IT Service Management practices guide our governance model, which fosters direct communications between our customers and Unisys at planned intervals, at various levels (from working to executive level) based on measurable and quantifiable targets.

Unisys Certifications

Certification and Standards	How they Apply at Unisys
ITIL V3	ITIL (the IT Infrastructure Library) is the most widely accepted approach to IT Service Management in the world. ITIL provides a cohesive set of best practices drawn from the public and private sectors worldwide. It is supported by a comprehensive qualifications program, accredited training organizations, and implementation and assessment tools. Best practice processes are promoted in ITIL support and supported by ISO 20000. Unisys is proud to be a truly global ITIL V3 compliant service provider—we can provide one global service delivery experience throughout all our Managed Services Centers and Data Centers. Fifty five Unisys resources dedicated to the Commonwealth are ITIL V3 certifications

This page intentionally left blank.

REQUEST FOR PROPOSALS FOR

Data Center Computing Services

ISSUING OFFICE

Commonwealth Of Pennsylvania
Office of Administration
Office for Information Technology

RFP 6100022698

DATE OF ISSUANCE

11/30/12

REQUEST FOR PROPOSALS FOR

Data Center Computing Services

TABLE OF CONTENTS

CALENDAR OF EVENTS **ix**

Part I—GENERAL INFORMATION **1**

Part II—PROPOSAL REQUIREMENTS **17**

Part III—CRITERIA FOR SELECTION **23**

Part IV—WORK STATEMENT **28**

APPENDIX A - CONTRACT TERMS AND CONDITIONS

SCHEDULES TO THE CONTRACT TERMS AND CONDITIONS:

SCHEDULE A - DEFINED TERMS

SCHEDULE B - GOVERNANCE

SCHEDULE C – SERVICES CATALOG

SCHEDULE D - TRANSITION MILESTONES

SCHEDULE E - DATACENTER LOCATIONS

SCHEDULE F - COPA DATACENTER STATEMENT OF WORK

SCHEDULE G - STAFFING PLAN AND KEY POSITIONS

SCHEDULE H - COMMONWEALTH COMPUTING PROCEDURES MANUAL

SCHEDULE I - OFFEROR PRICING FORMS

SCHEDULE J.1 - SERVICE LEVEL MANAGEMENT

SCHEDULE J.2 - DATACENTER SERVICE LEVEL MATRIX

SCHEDULE J.3 - DATACENTER SLA DEFINITIONS

SCHEDULE K - KEY PROGRAM DELIVERABLES

SCHEDULE L – APPROVED SUBCONTRACTORS

SCHEDULE M – DETAILED TRANSITION PLAN

APPENDIX B - PROPOSAL COVER SHEET

APPENDIX C – PROJECT REFERENCES

APPENDIX D - DOMESTIC WORKFORCE UTILIZATION CERTIFICATION

APPENDIX E - COSTARS PROGRAM QUESTIONNAIRE

APPENDIX F - NON-DISCLOSURE AGREEMENT

APPENDIX G - TRADE SECRETS FORM

APPENDIX H - LOBBYING CERTIFICATION FORM

APPENDIX I – QUESTIONS SUBMITTAL FORM

APPENDIX J - SDB LETTER OF INTENT

EXHIBIT A - COMMONWEALTH NETWORK ENVIRONMENT

EXHIBIT B.1 - DPH - ASSET LIST

EXHIBIT B.2 - DPH -COMMONWEALTH OWNED DPH IT ASSETS

EXHIBIT B.3 - DPH - COMMONWEALTH SOFTWARE ASSET LISTING

EXHIBIT B.4 - DPH - THIRD PARTY SOFTWARE

EXHIBIT B.5 - DPH - AGENCY DISASTER RECOVERY MATRIX

EXHIBIT B.6 - DPH - COPA NETWORK

EXHIBIT B.7 – DPH - IBM MF SW INVENTORY V3

EXHIBIT B.8 – DPH - UNISYS SOFTWARE - DORADO LIBRA

EXHIBIT B.9 – DPH – RECOVERY TIME OBJECTIVES

EXHIBIT B.10 – DPH – HYBRID THIRD PARTY SOFTWARE

EXHIBIT C.1 - DPW - ROOM 105 AND CAO SERVERS - STORAGE

EXHIBIT C.2 - DPW - APPLICATION INVENTORY TEMPLATE

EXHIBIT C.3 - DPW - METRICS Q2-2012

EXHIBIT C.4 - DPW - DPH ASSET LIST

EXHIBIT C.5 - DPW - COPA SOFTWARE ASSET UNISYS

EXHIBIT C.6 - DPW - ENVIRONMENTS

EXHIBIT C.7 - DPW - HCSIS APPLICATION TECH ARCHITECTURE

EXHIBIT C.8 - DPW - ICIS APPLICATION TECH ARCHITECTURE

EXHIBIT C.9 - DPW - PACSES APPLICATION TECH ARCHITECTURE

EXHIBIT C.10 -DPW - PELICAN APPLICATION TECH ARCHITECTURE

EXHIBIT C.11 - DPW - IT SYSTEMS OVERVIEW

EXHIBIT C.12 – DPW - ENVIRONMENTS_V25_UPDATED_03-20-2013

EXHIBIT C.13 – DPW – PRODUCTS ON MAINFRAMES

EXHIBIT D.1 - EDC - SERVER INVENTORY

EXHIBIT D.2 - EDC - SWITCH INVENTORY

EXHIBIT D.3 - EDC - STORAGE

EXHIBIT D.4 - EDC – APPLICATION SERVER AGENCY REPORT

EXHIBIT D.5 - EDC - DOT DATACENTER INVENTORY

EXHIBIT D.6 - EDC - IBM MAINTENANCE QUOTE

EXHIBIT D.7 - EDC FACILITY SUMMARY AND REQUIREMENTS

EXHIBIT D.8 – EDC SINGLE LINE ELECTRICAL DRAWING

EXHBIT D.9 – EDC MSL FLOOR PLAN ROOM 182.183 A

EXHBIT D.10 – EDC CR2 FLOOR PLAN ROOM 182.183 B

EXHBIT D.11 – EDC MS FLOOR PLAN ROOM 182.183 C

EXHBIT D.12 – EDC ELECTRICAL FAILURE SEQUENCE

EXHIBIT D.13 – EDC BUSINESS PARTNER CIRCUITS

EXHIBIT D.14 - EDC HARDWARE WARRANTY INFORMATION

EXHIBIT D.15 - EDC ELECTRICAL SYSTEM TESTING RESULTS

EXHIBIT E.1 - DLI - DATACENTER INVENTORY TEMPLATE

EXHIBIT E.2 - DLI - APPLICATION INVENTORY B

EXHIBIT E.3 - DLI - DPH COPA SOFTWARE ASSET IBM

EXHIBIT E.4 - DLI - BOE INFRASTRUCTURE

EXHIBIT E.5 - DLI - BWC HANDS

EXHIBIT E.6 - DLI - BWC WEB

EXHIBIT E.7 - DLI - CIMS INFRASTRUCTURE

EXHIBIT E.8 - DLI - CWDS ENVIRONMENTS

EXHIBIT E.9 - DLI - DEPT WEB INFRASTRUCTURE

EXHIBIT E.10 - DLI - NETWORK

EXHIBIT E.11 - DLI - DNS-DHCP-IPAM

EXHIBIT E.12 - DLI - DNS-SMTP

EXHIBIT E.13 - DLI - FILENET INFRASTRUCTURE

EXHIBIT E.14 - DLI - FTP ROUTING

EXHIBIT E.15 - DLI - IAM INFRASTRUCTURE

EXHIBIT E.16 - DLI - IRS 1099

EXHIBIT E.17 - DLI - DC LAYOUT

EXHIBIT E.18 - DLI - I PORTAL INFRASTRUCTURE

EXHIBIT E.19 - DLI - SAN STORAGE

EXHIBIT E.20 - DLI - VMWARE ENVIRONMENTS

EXHIBIT E.21 - DLI - LOADRUNNER

EXHIBIT E.22 - DLI - NETWORK ARCHITECTURE

EXHIBIT E.23 - DLI - QC & RATIONAL INFRASTRUCTURE

EXHIBIT E.24 - DLI - QUALITYCENTER

EXHIBIT E.25 - DLI - REMEDY INFRASTRUCTURE

EXHIBIT E.26 - DLI - SCOM POC DIAGRAM

EXHIBIT E.27 - DLI - SERVER OPERATIONS ARCHITECTURE

EXHIBIT E.28 - DLI - SRM LAYOUT

EXHIBIT E.29 - DLI - SWIF

EXHIBIT E.30 - DLI - TFS-SP INFRASTRUCTURE

EXHIBIT E.31 - DLI - TIVOLI ARCHITECTURE

EXHIBIT E.32 - DLI - UC CLAIMS INFRASTRUCTURE

EXHIBIT E.33 - DLI - UC TELCO LAYOUT

EXHIBIT E.34 - DLI - UCMS INFRASTRUCTURE

EXHIBIT E.35 - DLI - UCTIDES COLO DIAGRAM

EXHIBIT E.36 - DLI - VI5 INFRASTRUCTURE

EXHIBIT E.37 - DLI - WCAB INFRASTRUCTURE

EXHIBIT E.38 - DLI - WCAIS ENVIRONMENTS

EXHIBIT E.39 - DLI - WEBMETHODS INFRASTRUCTURE

EXHIBIT E.40 - DLI - WIAFMS HIGH LEVEL

EXHIBIT E.41- DLI - SERVER FARM TRANSITION APPROACH

EXHIBIT E.42 – DLI – BOIS SOFTWARE LIST

EXHIBIT E.43 – DLI – UC SOFTWARE

EXHIBIT F.1 - DOH - DATACENTER INVENTORY

EXHIBIT F.2 - DOH - DPH ASSET LIST

EXHIBIT F.3 - DOH - DPH COPA SOFTWARE ASSET IBM

EXHIBIT F.4 – DOH – PHYSICAL SERVERS

EXHIBIT G.1 - PSP - DATACENTER HW INVENTORY

EXHIBIT G.2 - PSP - DATACENTER APPLICATION INVENTORY FROM APPLICATION PORTFOLIO

EXHIBIT G.3 - PSP - DPH ASSET LIST

EXHIBIT G.4 - PSP - DPH COPA SOFTWARE ASSET UNISYS

EXHIBIT G.5 - PSP - NETWORK OVERVIEW

EXHIBIT G.6 - PSP - CJIS SECURITY POLICY

EXHIBIT G.7 - PSP - SUMMARY OF CJIS REQUIREMENTS

EXHIBIT G8 - PSP - AFIS

EXHIBIT G.9 - PSP - CCHRI

EXHIBIT G.10 - PSP - CLEAN

EXHIBIT G.11 - PSP - MEGANS' LAW

EXHIBIT G.12 - PSP - CHRIA HANDBOOK

EXHIBIT G.13 - PSP - PICS IVR

EXHIBIT G.14 - PSP - PICS

EXHIBIT G.15 - PSP - TRACS

EXHIBIT G.16 - PSP – MOBILE OFFICE

EXHIBIT H.1 - DOR - DATACENTER INVENTORY

EXHIBIT H.2 - DOR - DPH ASSET LIST

EXHIBIT H.3 - DOR - DPH COPA SOFTWARE ASSET IBM MAINFRAME

EXHIBIT H.4 – DOR - SAP TRM SYSTEM

EXHIBIT H.5 – DOR - CRITICAL TIMEFRAMES FOR DOR-ITS IMPLEMENTATION

EXHIBIT H.6 – DOR - SAP MODULES VERSION

EXHIBIT H.7 – DOR - STRAWBERRY SQUARE NETWORK SUMMARY

EXHIBIT H.8 – DOR - DPH DOR ITS OVERVIEW 2011

EXHIBIT I.1 - IES - DPH COPA OWNED IT ASSETS

EXHIBIT I.2 - IES - APPLICATION INVENTORY

EXHIBIT I.3 - IES - DPH COPA SOFTWARE ASSET UNISYS

EXHIBIT I.4 - IES - DPH - MEASUREMENT REPORT SEPTEMBER 2012

EXHIBIT I.5 - IES - BWA NON-PRODUCTION HARDWARE LIST

EXHIBIT I.6 - IES - BWA PRODUCTION HARDWARE LIST

EXHIBIT I.7 - IES - IES MONITORING OVERVIEW

EXHIBIT I.8 - IES - IES TECHNICAL REFRESH - DPH SAN SWITCHES

EXHIBIT I.9 - IES - IES TECHNICAL REFRESH - DPH SYSTEM P7 SERVERS

EXHIBIT I.10 - IES - IES TECHNICAL REFRESH - DPH SYSTEM-X HARDWARE

EXHIBIT I.11 - IES - IES TECHNICAL REFRESH - DPH XIV DISK STORAGE

EXHIBIT I.12 - IES - SLA SYSTEMGROUPS APPLICATIONS

EXHIBIT I.13 - IES – BWA SYSTEMS SOFTWARE SUBSCRIPTION

EXHIBIT I.14 – IES – IES ANTICIPATED SLA SERVICE LEVELS

EXHIBIT J.1 - SECURITY COMPLIANCE GUIDELINES

EXHIBIT J.2 - ITB SEC022

EXHIBIT J.3 - IRS PUBLICATION 1075 REV 8-2010

EXHIBIT J.4 - SECURITY AGENT STANDARD TOOLS

EXHIBIT K - OA ENTERPRISE ITSM SYSTEM AND VOLUMETRICS

EXHIBIT L - MASTER APPLICATION INVENTORY

EXHIBIT M.1 – DOC AND PBPP - APPLICATIONS

EXHIBIT M.2 – DOC AND PBPP – SERVERS

EXHIBIT M.3 – DOC - EDC PRODUCTION INFRASTRUCTURE - COLO DOCUMENT

EXHIBIT M.4 - DOC EDC DEVELOPMENT INFRASTRUCTURE

EXHIBIT M.5 – PBPP - EDC PRODUCTION SERVERS COLO DOCUMENT

EXHIBIT M.6 - DOC - APPLICATIONS V7

EXHIBIT M.7 – DOC - RACK LOCATIONS FOR SERVERS

EXHIBIT N.1 – PENNDOT - ENTERPRISE NETWORK CONNECTIVITY DIAGRAM

EXHIBIT N.2 – PENNDOT MONITORING

EXHIBIT O - 2012 AGENCY NO MAINTENANCE PERIODS

EXHIBIT P – ENTERPRISE INTERNET BANDWIDTH UTILIZATION

EXHIBIT Q – MAILBOX RESTORE POLICY

EXHIBIT R - TRANSITION CONSIDERATIONS

EXHIBIT S – DATACENTER LOCATIONS

EXHIBIT T – CRITICAL CONFIGURATION CONSIDERATIONS

EXHIBIT U – COPANET LOCATIONS

EXHIBIT V - SCSC - POWER 520 SYSTEM I

CALENDAR OF EVENTS

The Commonwealth will make every effort to adhere to the following schedule:

Activity	Responsibility	Date
Enterprise Data Center (EDC) Tour and Exhibit Distribution	Issuing Office/Potential Offerors	12/12/12 and 12/13/12
Deadline to submit initial questions via email to RA-OITPurchases@state.pa.us.	Potential Offerors	12/21/12 by 1:00 PM EST
Pre-proposal Conference—Location. Forum 500 Walnut St. Harrisburg, PA 17101	Issuing Office/Potential Offerors	1/17/13 @ 9:00 AM EST
Deadline to submit second round questions via email to RA-OITPurchases@state.pa.us	Potential Offerors	2/1/13 by 1:00 PM EST
Answers to second round of questions posted to the DGS website **(**http://www.emarketplace.state.pa.us **)**.	Issuing Office	TBD
Deadline to submit third round questions via email to RA-OITPurchases@state.pa.us	Potential Offerors	2/22/13 by 1:00 PM EST
Answers to third round of questions posted to the DGS website **(**http://www.emarketplace.state.pa.us **)**.	Issuing Office	TBD
Post updated RFP documents including Schedules, Exhibits and answers to all questions received.	Issuing Office	4/17/13
Deadline to submit final questions via email to RA-OITPurchases@state.pa.us	Potential Offerors	4/26/13 by 12:00 PM EST
Answers to final questions posted to the DGS website **(**http://www.emarketplace.state.pa.us **)**.	Issuing Office	5/14/13
Please monitor website for all communications regarding the RFP.	Potential Offerors	Ongoing
Sealed proposal must be received by the Issuing Office at Bureau of IT Procurement c/o Commonwealth Mail Processing Center 2 Technology Park (rear)	Offerors	6/19/13 by 1:00 PM EST

Activity	Responsibility	Date
Attn: IT Procurement 506 Finance Harrisburg PA 17110 Attn: Janis Brown Proposals must be time and date stamped by the facility receiving the proposals. Proposals may only be hand-delivered between 6:00 a.m. and 2:45 p.m., Monday through Friday, excluding Commonwealth holidays.		

PART I

GENERAL INFORMATION

I-1. Purpose. This request for proposals (RFP) provides to those interested in submitting proposals for the subject procurement ("Offerors") sufficient information to enable them to prepare and submit proposals for the Office of Administration's consideration on behalf of the Commonwealth of Pennsylvania ("Commonwealth") to satisfy a need **for Data Center Computing Services** ("Project").

I-2. Issuing Office. The Office of Administration ("Issuing Office") has issued this RFP on behalf of the Commonwealth. The sole point of contact in the Commonwealth for this RFP shall be **Janis Brown, 506 Finance Building, Harrisburg PA, 17120, RA-OITPurchases@pa.gov,** the Issuing Officer for this RFP. Please refer all inquiries to the Issuing Officer.

I-3. Scope. This RFP contains instructions governing the requested proposals, including the requirements for the information and material to be included; a description of the service to be provided; requirements which Offerors must meet to be eligible for consideration; general evaluation criteria; and other requirements specific to this RFP.

I-4. Problem Statement. The current managed datacenter service contract is nearing its end and the Commonwealth is seeking to implement a new datacenter service model that will provide various infrastructures/computing platforms on a consumption basis to service the needs of the Commonwealth in a secure and flexible manner. Additional detail is provided in **Part IV** of this RFP.

I-5. Type of Contract. It is proposed that if the Issuing Office enters into a contract as a result of this RFP, it will be a firm, fixed price contract containing the Contract Terms and Conditions as shown in **Appendix A**. The Issuing Office, in its sole discretion, may undertake negotiations with one or more Offerors whose proposals, in the sole judgment of the Issuing Office, show them to be qualified, responsible and capable of performing the Project.

I-6. Rejection of Proposals. The Issuing Office reserves the right, in its sole and complete discretion, to reject any proposal received as a result of this RFP.

I-7. Incurring Costs. The Issuing Office is not liable for any costs the Offeror incurs in preparation and submission of its proposal, in participating in the RFP process or in anticipation of award of the contract.

I-8. Enterprise Data Center (EDC) Tour. The Issuing Office will hold a tour of the Commonwealth's Enterprise Data Center as specified in the Calendar of Events. The purpose of the tour is to provide a visual inspection of the facility which is required to be utilized by the selected Offeror as a datacenter location for this Project. The tour is **not mandatory**. Tours will be provided on the dates indicated in the Calendar of Events. Tours will be approximately 1 hour in length. Each tour will be limited in size of

participants and will be scheduled on a first come first basis. In order to take part in the EDC tour and reserve a tour time, the Offeror must contact, in advance, the Issuing Officer and provide a list of individuals who will be attending the tour. This tour is limited to **two (2)** individuals per Offeror. Only those named individuals will be given access to the facility.

Pre-proposal Conference. The Issuing Office will hold a Pre-proposal conference as specified in the Calendar of Events. The purpose of this conference is to provide opportunity for clarification of the RFP. Offerors should forward all questions to the Issuing Office in accordance with **Part I, Section I-9** to ensure adequate time for analysis before the Issuing Office provides an answer. Offerors may also ask questions at the conference. In view of the limited facilities available for the conference, Offerors should limit their representation to **two (2)** individuals per Offeror. The Pre-proposal conference is for information only. Any answers furnished during the conference will not be official until they have been verified, in writing, by the Issuing Office. All questions and written answers will be posted on the Department of General Services' ("DGS") website (http://www.emarketplace.state.pa.us) as an addendum to, and shall become part of, this RFP. Attendance at the Pre-proposal Conference is **not mandatory.**

Application and Architectural exhibits Distribution. The information included in the Application and Architectural exhibits is confidential and proprietary. In order for an Offeror to receive access to these exhibits, the Offeror must sign the non-disclosure agreement attached to this RFP as **Appendix F.** The non-disclosure agreement must be signed by an individual that has the authority to bind his or her company. Offerors may provide the signed agreement to the Issuing Officer at the EDC Tour, the Pre-Proposal Conference, or at a separate time as scheduled with the Issuing Officer. The Issuing Officer will distribute the exhibits only to those Offerors that provide a properly executed non-disclosure agreement. Individuals seeking to receive the exhibits will be required to provide contact information to the Issuing Officer including name, address, phone number, email address and title within their respective company, as well as a photo ID. The Commonwealth will provide one copy of the Application and Architectural exhibits per company.

I-9. Questions & Answers. If an Offeror has any questions regarding this RFP, the Offeror must submit the questions by email **(with the subject line "RFP 6100022698 Question")** to the Issuing Officer named in **Part I, Section I-2** of the RFP. All questions must be submitted using **Appendix I – Questions Submittal Form**. Questions must be submitted via email **no later than** the date indicated on the Calendar of Events. The Offeror shall not attempt to contact the Issuing Officer by any other means. The Issuing Officer shall post the answers to the questions on the DGS website by the date stated on the Calendar of Events**.** An Offeror who submits a question *after* the deadline date for receipt of questions indicated on the Calendar of Events assumes the risk that its proposal will not be responsive or competitive because the Commonwealth is not able to respond before the proposal receipt date or in sufficient time for the Offeror to prepare a responsive or competitive proposal. When submitted after the deadline date for receipt of questions indicated on the Calendar of Events, the Issuing Officer *may* respond to questions of an administrative nature by directing the questioning Offeror to specific

provisions in the RFP. To the extent that the Issuing Office decides to respond to a non-administrative question *after* the deadline date for receipt of questions indicated on the Calendar of Events, the answer must be provided to all Offerors through an addendum.

All questions and responses as posted on the DGS website are considered as an addendum to, and part of, this RFP in accordance with RFP **Part I, Section I-10.** Each Offeror shall be responsible to monitor the DGS website for new or revised RFP information. The Issuing Office shall not be bound by any verbal information nor shall it be bound by any written information that is not either contained within the RFP or formally issued as an addendum by the Issuing Office. The Issuing Office does not consider questions to be a protest of the specifications or of the solicitation. The required protest process for Commonwealth procurements is described on the DGS website.

I-10. Addenda to the RFP. If the Issuing Office deems it necessary to revise any part of this RFP before the proposal response date, the Issuing Office will post an addendum to the DGS website at http://www.emarketplace.state.pa.us . It is the Offeror's responsibility to periodically check the website for any new information or addenda to the RFP. Answers to the questions asked during the Questions & Answers period also will be posted to the website as an addendum to the RFP.

I-11. Response Date. To be considered for selection, hard copies of proposals must arrive at the Issuing Office on or before the time and date specified in the RFP Calendar of Events. The Issuing Office will **not** accept proposals via email or facsimile transmission. Offerors who send proposals by mail or other delivery service should allow sufficient delivery time to ensure timely receipt of their proposals. If, due to inclement weather, natural disaster, or any other cause, the Commonwealth office location to which proposals are to be returned is closed on the proposal response date, the deadline for submission will be automatically extended until the next Commonwealth business day on which the office is open, unless the Issuing Office otherwise notifies Offerors by posting an Addendum to the RFP. The hour for submission of proposals shall remain the same. The Issuing Office will reject, unopened, any late proposals.

I-12. Proposals. To be considered, Offerors should submit a complete response to this RFP to the Issuing Office, using the format provided in **Part II**, providing **fourteen (14) paper copies of the Technical Submittal and one (1) paper copy of the Cost Submittal and two (2) paper copies of the Small Diverse Business (SDB) participation submittal.** In addition to the paper copies of the proposal, Offerors shall submit **two (2)complete and exact** copies of the entire proposal (Technical, Cost and SDB submittals, along with all requested documents) on CD-ROM or Flash drive in Microsoft Office or Microsoft Office-compatible format. The electronic copy must be a mirror image of the paper copy and any spreadsheets must be in Microsoft Excel. The Offerors may not lock or protect any cells or tabs. Offerors should ensure that there is no costing information in the technical submittal. Offerors should not reiterate technical information in the cost submittal. The CD or Flash drive should clearly identify the Offeror and include the name and version number of the virus scanning software that was used to scan the CD or Flash drive before it was submitted. The Offeror shall make no other distribution of its proposal to any other Offeror or Commonwealth official or Commonwealth consultant.

Each proposal page should be numbered for ease of reference. An official authorized to bind the Offeror to its provisions must sign the proposal. If the official signs the Proposal Cover Sheet (**Appendix B** to this RFP) and the Proposal Cover Sheet is attached to the Offeror's proposal, the requirement will be met. For this RFP, the proposal must remain valid until a contract is fully executed. If the Issuing Office selects the Offeror's proposal for award, the contents of the selected Offeror's proposal will become, except to the extent the contents are changed through Best and Final Offers or negotiations, contractual obligations.

Each Offeror submitting a proposal specifically waives any right to withdraw or modify it, except that the Offeror may withdraw its proposal by written notice received at the Issuing Office's address for proposal delivery prior to the exact hour and date specified for proposal receipt. An Offeror or its authorized representative may withdraw its proposal in person prior to the exact hour and date set for proposal receipt, provided the withdrawing person provides appropriate identification and signs a receipt for the proposal. An Offeror may modify its submitted proposal prior to the exact hour and date set for proposal receipt only by submitting a new sealed proposal or sealed modification which complies with the RFP requirements.

I-13. Small Diverse Business Information. The Issuing Office encourages participation by small diverse businesses as prime contractors, and encourages all prime contractors to make a significant commitment to use small diverse businesses as subcontractors and suppliers**.**

A Small Diverse Businesses is a DGS-verified minority-owned business, woman-owned business, veteran-owned business or service-disabled veteran-owned business.

A small business is a business in the United States which is independently owned, not dominant in its field of operation, employs no more than 100 full-time or full-time equivalent employees, and earns less than $7 million in gross annual revenues for building design, $20 million in gross annual revenues for sales and services and $25 million in gross annual revenues for those businesses in the information technology sales or service business.

Questions regarding this Program can be directed to:

Department of General Services
Bureau of Small Business Opportunities
Room 611, North Office Building
Harrisburg, PA 17125
Phone: (717) 783-3119
Fax: (717) 787-7052
Email: gs-bsbo@pa.gov
Website: www.dgs.state.pa.us

The Department's directory of BSBO-verified minority, women, veteran and service disabled veteran-owned businesses can be accessed from: Searching for Small Diverse Businesses.

I-14. Economy of Preparation. Offerors should prepare proposals simply and economically, providing a straightforward, concise description of the Offeror's ability to meet the requirements of the RFP.

I-15. Alternate Proposals. The Issuing Office will not accept alternate proposals.

I-16. Discussions for Clarification. Offerors may be required to make an oral or written clarification of their proposals to the Issuing Office to ensure thorough mutual understanding and Offeror responsiveness to the solicitation requirements. The Issuing Office will initiate requests for clarification. Clarifications may occur at any stage of the evaluation and selection process prior to contract execution.

I-17. Prime Contractor Responsibilities. The contract will require the selected Offeror to assume responsibility for all services offered in its proposal whether it produces them itself or by subcontract. The Issuing Office will consider the selected Offeror to be the sole point of contact with regard to contractual matters.

I-18. Proposal Contents.

A. Confidential Information. The Commonwealth is not requesting, and does not require, confidential proprietary information or trade secrets to be included as part of Offerors' submissions in order to evaluate proposals submitted in response to this RFP. Accordingly, except as provided herein, Offerors should not label proposal submissions as confidential or proprietary or trade secret protected. Any Offeror who determines that it must divulge such information as part of its proposal must submit the signed written statement described in subsection c. below and must additionally provide a redacted version of its proposal, which removes only the confidential proprietary information and trade secrets, for required public disclosure purposes.

B. Commonwealth Use. All material submitted with the proposal shall be considered the property of the Commonwealth of Pennsylvania and may be returned only at the Issuing Office's option. The Commonwealth has the right to use any or all ideas not protected by intellectual property rights that are presented in any proposal regardless of whether the proposal becomes part of a contract. Notwithstanding any Offeror copyright and/or trademark designations contained on proposals, the Commonwealth shall have the right to make copies and distribute proposals internally and to comply with public record or other disclosure requirements under the provisions of any Commonwealth or United States statute or regulation, or rule or order of any court of competent jurisdiction.

C. Public Disclosure. After the award of a contract pursuant to this RFP, all proposal submissions are subject to disclosure in response to a request for public records made under the Pennsylvania Right-to-Know-Law, 65 P.S. § 67.101, et seq. If a proposal submission contains confidential proprietary information or trade secrets, a signed written statement to this effect must be provided with the submission in accordance with 65 P.S.

§ 67.707(b) for the information to be considered exempt under 65 P.S. § 67.708(b)(11) from public records requests. If financial capability information is submitted in response to Part II of this RFP such financial capability information is exempt from public records disclosure under 65 P.S. § 67.708(b)(26).

I-19. Best and Final Offers.

A. While not required, the Issuing Office reserves the right to conduct discussions with Offerors for the purpose of obtaining "best and final offers." To obtain best and final offers from Offerors, the Issuing Office may do one or more of the following, in any combination and order:

1. Schedule oral presentations;

2. Request revised proposals;

3. Conduct a reverse online auction; and

4. Enter into pre-selection negotiations.

B. The following Offerors will **not** be invited by the Issuing Office to submit a Best and Final Offer:

1. Those Offerors, which the Issuing Office has determined to be not responsible or whose proposals the Issuing Office has determined to be not responsive.

2. Those Offerors, which the Issuing Office has determined in accordance with **Part III, Section III-5**, from the submitted and gathered financial and other information, do not possess the financial capability, experience or qualifications to assure good faith performance of the contract.

3. Those Offerors whose score for their technical submittal of the proposal is less than 75% of the total amount of technical points allotted to the technical criterion.

The issuing office may further limit participation in the best and final offers process to those remaining responsible offerors which the Issuing Office has, within its discretion, determined to be within the top competitive range of responsive proposals.

C. The Evaluation Criteria found in **Part III, Section III-4**, shall also be used to evaluate the Best and Final offers.

D. Price reductions offered through any reverse online auction shall have no effect upon the Offeror's Technical Submittal. Dollar commitments to Small Diverse Businesses can be reduced only in the same percentage as the percent reduction in the total price offered through any reverse online auction or negotiations.

I-20. News Releases. Offerors shall not issue news releases, Internet postings, advertisements or any other public communications pertaining to this Project without prior written approval of the Issuing Office, and then only in coordination with the Issuing Office.

I-21. Restriction of Contact. From the issue date of this RFP until the Issuing Office selects a proposal for award, the Issuing Officer is the sole point of contact concerning this RFP. Any violation of this condition may be cause for the Issuing Office to reject the offending Offeror's proposal. If the Issuing Office later discovers that the Offeror has engaged in any violations of this condition, the Issuing Office may reject the offending Offeror's proposal or rescind its contract award. Offerors must agree not to distribute any part of their proposals beyond the Issuing Office. An Offeror who shares information contained in its proposal with other Commonwealth personnel and/or competing Offeror personnel may be disqualified.

I-22. Issuing Office Participation. Offerors shall provide all services, supplies, facilities, and other support necessary to complete the identified work, except as otherwise provided in this **Part I, Section I-22**.

I-23. Term of Contract. The term of the contract will commence on the Effective Date and will end in seven (7) years. The Commonwealth, at its sole option, may renew the contract for up to an additional three (3) years. The Commonwealth may exercise the renewal(s) in single or multiple year increments, at any time during the contact term**.** The Issuing Office will fix the Effective Date after the contract has been fully executed by the selected Offeror and by the Commonwealth and all approvals required by Commonwealth contracting procedures have been obtained. The selected Offeror shall not begin to perform or incur any expenses under the contract until (1) the contract Effective Date has arrived; (2) it has received a copy of the fully executed contract; and (3) it has received a purchase order or other written notice to proceed signed by the Contracting Officer.

I-24. Offeror's Representations and Authorizations. By submitting its proposal, each Offeror understands, represents, and acknowledges that:

A. All of the Offeror's information and representations in the proposal are true, correct, material and important, and the Issuing Office may rely upon the contents of the proposal in awarding the contract(s). The Commonwealth shall treat any misstatement, omission or misrepresentation as fraudulent concealment of the true facts relating to the Proposal submission, punishable pursuant to 18 Pa. C.S. § 4904.

B. The Offeror has arrived at the price(s) and amounts in its proposal independently and without consultation, communication, or agreement with any other Offeror or potential offeror.

C. The Offeror has not disclosed the price(s), the amount of the proposal, nor the approximate price(s) or amount(s) of its proposal to any other firm or person who is an Offeror or potential offeror for this RFP, and the Offeror shall not disclose any of these items on or before the proposal submission deadline specified in the Calendar of Events of this RFP.

D. The Offeror has not attempted, nor will it attempt, to induce any firm or person to refrain from submitting a proposal on this contract, or to submit a proposal higher

than this proposal, or to submit any intentionally high or noncompetitive proposal or other form of complementary proposal.

E. The Offeror makes its proposal in good faith and not pursuant to any agreement or discussion with, or inducement from, any firm or person to submit a complementary or other noncompetitive proposal.

F. To the best knowledge of the person signing the proposal for the Offeror, the Offeror, its affiliates, subsidiaries, officers, directors, and employees are not currently under investigation by any Local, State, or Federal governmental agency and have not in the last **four** years been convicted or found liable for any act prohibited by Local, State or Federal law in any jurisdiction, involving conspiracy or collusion with respect to bidding or proposing on any public contract, except as the Offeror has disclosed in its proposal.

G. To the best of the knowledge of the person signing the proposal for the Offeror and except as the Offeror has otherwise disclosed in its proposal, the Offeror has no outstanding, delinquent obligations to the Commonwealth including, but not limited to, any state tax liability not being contested on appeal or other obligation of the Offeror that is owed to the Commonwealth.

H. The Offeror is not currently under suspension or debarment by the Commonwealth, any other state or the federal government, and if the Offeror cannot so certify, then it shall submit along with its proposal a written explanation of why it cannot make such certification.

I. The Offeror has not made, under separate contract with the Issuing Office, any recommendations to the Issuing Office concerning the need for the services described in its proposal or the specifications for the services described in the proposal. (*See* Pennsylvania State Adverse Interest Act)

J. Each Offeror, by submitting its proposal, authorizes Commonwealth agencies to release to the Commonwealth information concerning the Offeror's Pennsylvania taxes, unemployment compensation and workers' compensation liabilities.

K. Until the selected Offeror receives a fully executed and approved written contract from the Issuing Office, there is no legal and valid contract, in law or in equity. The selected Offeror shall not begin to perform or incur any expenses under the contract until (1) the contract Effective Date has arrived; (2) it has received a copy of the fully executed contract; and (3) it has received a purchase order or other written notice to proceed signed by the Contracting Officer.

I-25. Notification of Selection.

A. **Contract Negotiations.** The Issuing Office will notify all Offerors in writing of the Offeror selected for contract negotiations after the Issuing Office has determined, taking into consideration all of the evaluation factors, the proposal that is the most advantageous to the Issuing Office.

B. **Award.** Offerors whose proposals are not selected will be notified when contract negotiations have been successfully completed and the Issuing Office has received the final negotiated contract signed by the selected Offeror.

I-26. Debriefing Conferences. Upon notification of award, Offerors whose proposals were not selected will be given the opportunity to be debriefed. The Issuing Office will schedule the debriefing at a mutually agreeable time. The debriefing will not compare the Offeror with other Offerors, other than the position of the Offeror's proposal in relation to all other Offeror proposals. An Offeror's exercise of the opportunity to be debriefed does not constitute nor toll the time for filing a protest (See Section I-27 of this RFP).

I-27. RFP Protest Procedure.

A. Who May File a Protest. An Offeror or Prospective Offeror which is aggrieved in connection with the RFP or award of the contract may file a protest. An Offeror is an entity which submits a proposal in response to an RFP. A Prospective Offeror is an entity which has not submitted a proposal in response to the RFP. No protest may be filed if the RFP is cancelled or if all proposals received in response to the RFP are rejected.

B. Place for Filing. A protest must be filed with the Agency Head Designee at:

Mr. James E. Henning
Deputy Secretary for Administration
Department of General Services
515 North Office Building
Harrisburg, PA 17125

C. Time for Filing.

1. A Prospective Offeror which is considering filing a proposal must file the protest within seven (7) days after the Prospective Offeror knew or should have known of the facts giving rise to the protest, but in no event later than the proposal submission deadline specified in the RFP.

2. A protest filed by an Offeror which submits a proposal must be filed within seven (7) days after the protesting Offeror knew or should have known of the facts giving rise to the protest, but in no event may an Offeror file a protest later than seven (7) days after the date the notice of award of the contract is posted on the DGS website.

3. The date of filing the protest is the date the Agency Head Designee receives the protest.

4. For purposes of this RFP, to be timely, a protest must be received by 4:00 p.m. of the seventh day.

5. Commonwealth agencies are required by law to disregard any protest received beyond the deadlines established in this Section I-27.

D. Contents of Protest.

6. A protest must be in writing. Hard copy in paper and electronic copy via email are acceptable.

7. A protest shall state all grounds upon which the protesting party asserts that the RFP or contract award was improper.

8. The protesting party may submit with the protest any documents or information it deems relevant.

E. Notice of Protest.

1. The Agency Head Designee will notify the successful Offeror of the protest if contractor selection has already been made.

2. If the Agency Head Designee receives the protest before selection, and he or she determines that substantial issues are raised by the protest, the Agency Head Designee will, in the sole discretion of the Agency Head Designee, notify all Offerors which appear to have a substantial and reasonable prospect of selection, as determined by the Agency Head, that a protest has been filed.

F. Stay of Procurement.

3. The Agency Head designee will promptly decide upon receipt of a timely protest whether or not the award of a contract shall be delayed, or if the protest is timely received after the award, whether the performance of the contract should be suspended.

4. The Issuing Office shall not proceed further with the RFP unless the Agency Head Designee makes a written determination that the protest is clearly without merit or that award of the contract without delay is necessary to protect the substantial interests of the Commonwealth.

G. Response and Reply.

1. Within 15 days of receipt of the protest, a response to the protest may be submitted to the Agency Head Designee. The protesting party must be copied on the response.

2. The protesting party may file a reply to the response within ten days of the date of the response.

H. Procedures.

1. The Agency Head Designee shall review the protest and any response and reply.

2. The Agency Head Designee may request and review such additional documents or information he deems necessary to render a decision and may, at his sole discretion, conduct a hearing.

3. The Agency Head Designee shall provide to the protesting party and the contracting officer a reasonable opportunity to review and address any additional documents or information deemed necessary by the Agency Head Designee to render a decision.

I. Determination.

The Agency Head Designee shall promptly, but in no event later than 60 days from the filing of the protest unless both parties agree to an extension, issue a written determination. The determination shall:

1. State the reason for the decision, and

2. If the determination is a denial of the protest, inform the protesting party of its right to file an action in the Commonwealth Court within fifteen (15) days of the determination mailing date.

3. The Agency Head Designee shall send a copy of the determination to the protesting party and any other person determined by the Agency Head Designee in his sole discretion to be affected by the determination.

I-28. Use of Electronic Versions of this RFP. This RFP is being made available by electronic means. If an Offeror electronically accepts the RFP, the Offeror acknowledges and accepts full responsibility to insure that no changes are made to the RFP. In the event of a conflict between a version of the RFP in the Offeror's possession and the Issuing Office's version of the RFP, the Issuing Office's version shall govern.

I-29. Information Technology Bulletins.

This RFP is subject to the Information Technology Bulletins (ITB's) issued by the Office of Administration, Office for Information Technology (OA-OIT). ITB's may be found at http://www.portal.state.pa.us/portal/server.pt?open=512&objID=416&PageID=210791&mode=2

All proposals must be submitted on the basis that all ITBs are applicable to this procurement. It is the responsibility of the Offeror to read and be familiar with the ITBs. Notwithstanding the foregoing, if the Offeror believes that any ITB is not applicable to this procurement, it must list all such ITBs in its technical submittal, and explain why it believes the ITB is not applicable. The Issuing Office may, in its sole discretion, accept or reject any request that an ITB not be considered to be applicable to the procurement. The Offeror's failure to list an ITB will result in its waiving its right to do so later, unless the Issuing Office, in its sole discretion, determines that it would be in the best interest of the Commonwealth to waive the pertinent ITB.

I-30. COSTARS PROGRAM.

COSTARS Purchasers. Section 1902 of the Commonwealth Procurement Code, 62 Pa.C.S. § 1902 ("Section 1902"), authorizes local public procurement units and state-affiliated entities (together, "COSTARS Members") to participate in Commonwealth procurement contracts that the Department of General Services ("DGS") may choose to make available to COSTARS Members. DGS has identified this Contract as one which will be made available for COSTARS Members' participation.

A. Only those entities registered with DGS are authorized to participate as COSTARS Members in this Contract. A COSTARS Member may be either a local public procurement unit or a state-affiliated entity.

1. **A "local public procurement unit" is:**

   a) Any political subdivision (local government unit), such as a municipality, school district, or commission;
   b) Any public authority (including authorities formed under the Municipality Authorities Act of 1955 or other authorizing legislation, such as the Public Transportation Law or the Aviation Code);
   c) Any tax-exempt, nonprofit educational institution or organization;
   d) Any tax-exempt, nonprofit public health institution or organization;
   e) Any nonprofit fire, rescue, or ambulance company; and
   f) Any other entity that spends public funds for the procurement of supplies, services, and construction (such as a council of governments, an area government, or an organization that receives public grant funds).

2. **A state-affiliated entity is a Commonwealth authority or other Commonwealth entity that is not a Commonwealth agency. The term includes:**

   a) The Pennsylvania Turnpike Commission;
   b) The Pennsylvania Housing Finance Agency;

c) The Pennsylvania Municipal Retirement System;
d) The Pennsylvania Infrastructure Investment Authority;
e) The State Public School Building Authority;
f) The Pennsylvania Higher Education Facilities Authority, and
g) The State System of Higher Education.

The term does not include any court or other officer or agency of the unified judicial system, the General Assembly and its officers and agencies, any State-related institution, or any Commonwealth executive or independent agencies, boards, or commissions not listed above. Statewide "row" offices, including the Auditor General, Attorney General, and State Treasurer **are not** State-affiliated entities under the Procurement Code.

However, elements of the court system, the General Assembly, and independent agencies, boards, or commissions have been deemed eligible for COSTARS membership as entities that spend public funds for the procurement of supplies, services, and construction.

3. A complete list of local public procurement units and state-affiliated entities that have registered with DGS and that are authorized to procure items from the Contract can be found at http://www.dgsweb.state.pa.us/COSTARSReg/Member.aspx

B. COSTARS Members have the option to purchase from this Contract, from any DGS contract established exclusively for COSTARS Members in accordance with the requirements of Section 1902, from any other cooperative procurement contracts, or from their own procurement contracts established in accordance with the applicable laws governing such procurements. The Contractor understands and acknowledges that there is no guarantee that a COSTARS Member will place an order under this Contract, and that the decision to procure from this Contract is within the sole discretion of each COSTARS Member.

C. DGS is acting as a facilitator for COSTARS Members who may wish to purchase under this Contract. COSTARS Members that participate in this Contract and issue purchase orders ("POs") to Contractors are third party beneficiaries who have the right to sue and be sued for breach of this Contract without joining the Commonwealth or DGS as a party. The Commonwealth will not intervene in any action between a Contractor and a COSTARS Member unless substantial interests of the Commonwealth are involved.

D. COSTARS Members electing to participate in this Contract will order items directly from the Contractor and be responsible for payment directly to the Contractor.

E. Those Contractors electing to permit COSTARS Members to procure from this Contract shall pay the Required Administrative Fee applicable to the Contractor's classification:

Contractor Classification	Required Administrative Fee
Department of General Services Certified Small Business Bidder	$500
All Other Bidders	$1,500

1. Each bidder electing to permit COSTARS Members to participate in the Contract must submit the COSTARS Program Election to Participate form with its bid submittal and pay the applicable Administrative Fee upon Contract award in order to sell the awarded items/services to COSTARS Members. If the bidder is a Department of General Services-Certified Small Business, a copy of its active certification must be included with the bid submittal.

2. At the beginning of each Contract year and upon any Contract renewal, the Contractor shall submit a check for the required amount, payable to "Commonwealth of PA". The Contractor must pay the Administrative Fee at each contract renewal date to continue to sell the awarded items/services to COSTARS Members. If the bidder is a Department of General Services-Certified Small Business, a copy of its active certification must be included with the Administrative Fee for each contract year and upon each renewal.

F. DGS has registered the COSTARS name and logo (together, the "COSTARS Brand") as a trademark with the Pennsylvania Department of State. Therefore, the Contractor may use the COSTARS Brand only as permitted under in this Subsection.

1. The Contractor shall pay the Administrative Fee covering its participation in the program, including without limitation any use of the COSTARS Brand, for each year of the Contract period. The fee is payable upon Contract award and prior to the renewal date for each succeeding Contract period.

2. DGS grants the Contractor a nonexclusive license to use the COSTARS Brand, subject to the following conditions:

   a) The Contractor agrees not to transfer to any third party, including without limitation any of its subcontractors or suppliers, any privileges it may have to use the COSTARS Brand under this Contract.

   b) The Contractor agrees not to use the COSTARS Brand to represent or imply any Commonwealth endorsement or approval of its products or services.

   c) The Contractor is permitted to use the COSTARS Brand in broadcast, or Internet media solely in connection with this Contract and any other Contract with the Commonwealth under which it has agreed to make sales to COSTARS Purchasers. The Contractor may use the COSTARS Brand on

business cards, brochures, and other print publications so long as the purpose is to identify the Contractor as a COSTARS vendor, and only so long as the required Contract fee is kept current.

d) Should this Contract terminate for any reason, the Contractor agrees promptly to remove the COSTARS Brand from any and all print and electronic media and to refrain from using the COSTARS Brand for any purpose whatsoever from the date of Contract termination forward.

e) The Contractor agrees to defend, indemnify, and hold harmless the Commonwealth of Pennsylvania and DGS from and against all claims, demands, liabilities, obligations, costs, and expenses of any nature whatsoever arising out of or based upon the Contractor's use of the COSTARS Brand.

f) The Contractor agrees it has no property rights in the use of the COSTARS Brand by virtue of this nonexclusive license. The Contractor expressly waives any claims, including without limitation due process claims that may otherwise be available under the law in the event of any dispute involving these terms of use.

G. The Contractor shall furnish to the DGS COSTARS Program Office a quarterly electronic Contract sales report detailing the previous quarter's Contract purchasing activity, using the form and in the format prescribed by DGS. The Contractor shall submit its completed quarterly report no later than the fifteenth calendar day of the succeeding Contract quarter.

1. The Contractor shall submit the reports via the web-based COSTARS Suppliers' Gateway at www.dgs.state.pa.us/costars. If a Contractor does not have access to the Internet, the Contractor shall send the reports, using the form and in the format prescribed by DGS, on compact disc via US Postal Service to the DGS COSTARS Program Office, Bureau of Procurement, 6th Floor Forum Place, 555 Walnut Street, Harrisburg, PA 17101-1914.

   For each PO received, the Contractor shall include on the report the name and address of each COSTARS-Registered Purchaser that has used the Contract along with the sales date, and dollar volume of sales to the specific Purchaser for the reporting period.

2. DGS may suspend the Contractor's participation in the COSTARS Program for failure to provide the Quarterly Sales Report within the specified time.

H. Additional information regarding the COSTARS Program is available on the DGS COSTARS Website at www.dgs.state.pa.us/costars

1. If the Contractor is aware of any qualified entity not currently registered and wishing to participate in the COSTARS Program, please refer the potential purchaser to the DGS COSTARS Website at www.dgs.state.pa.us/costars, where it may register by completing the online registration form and receiving DGS

confirmation of its registration. To view a list of currently-registered COSTARS member entities, please visit the COSTARS website.

2. Direct all questions concerning the COSTARS Program to:

Department of General Services
COSTARS Program
555 Walnut Street, 6th Floor
Harrisburg, PA 17101
Telephone: 1-866-768-7827
E-mail: GS-PACostars@state.pa.us

PART II

PROPOSAL REQUIREMENTS

Offerors must submit their proposals in the format, including heading descriptions, outlined below. To be considered, the proposal must respond to all requirements in this part of the RFP. Offerors should provide any other information thought to be relevant, but not applicable to the enumerated categories, as an appendix to the Proposal. All cost data relating to this proposal and all Small Diverse Business cost data should be kept separate from and not included in the Technical Submittal. Each Proposal shall consist of the following **three** separately sealed submittals:

A. Technical Submittal, which shall be a response to RFP **Part II, Sections II-1 through II-8**;

B. Small Diverse Business participation submittal, in response to RFP **Part II, Section II-9**; and

C. Cost Submittal, in response to RFP **Part II, Section II-10.**

The Issuing Office reserves the right to request additional information which, in the Issuing Office's opinion, is necessary to assure that the Offeror's competence, number of qualified employees, business organization, and financial resources are adequate to perform according to the RFP.

The Issuing Office may make investigations as deemed necessary to determine the ability of the Offeror to perform the Project, and the Offeror shall furnish to the Issuing Office all requested information and data. The Issuing Office reserves the right to reject any proposal if the evidence submitted by, or investigation of, such Offeror fails to satisfy the Issuing Office that such Offeror is properly qualified to carry out the obligations of the RFP and to complete the Project as specified.

II-1. Statement of the Problem. State in succinct terms your understanding of the problem presented or the service required by this RFP.

II-2. Management Summary. Include a narrative description of the proposed effort and a list of the items to be delivered or services to be provided.

II-3. Work Plan. Describe in narrative form your technical plan for accomplishing the work. Use the task descriptions in **Part IV** of this RFP and **Schedule F** as your reference point. Modifications of the task descriptions are permitted; however, reasons for changes should be fully explained. Indicate the number of person hours allocated to each task. Include a Program Evaluation and Review Technique (PERT) or similar type display, time related, showing each event. If more than one approach is apparent, comment on why you chose this approach.

II-4. Prior Experience.

The Offeror's Background and Qualifications should cover the topics described below.

Overall

The Offeror must provide information describing its background, services, experience, and qualifications relative to the scope of this RFP. Information that will be considered includes the length of the service, service levels, references, and quality of comparable services provided to other clients. The Offeror should also indicate any additional information that will be helpful to the Commonwealth's evaluation.

Corporate Information

The Offeror must provide a narrative describing its background, history, services, and corporate organization. A general overview of the corporate organization is appropriate. If the Offeror is a subsidiary or division of a larger company, this section should concentrate on the operating history of the subsidiary or division which will provide the Services.

Strategic Direction

The Commonwealth places strong emphasis on the need for a long-term strategy. The Offeror should describe its strategic direction, and the implications of that strategy for the Commonwealth.

Dedication to Quality

The Offeror must provide details of its approach to measuring and maintaining high quality services. The Offeror should provide details of any industry-recognized quality standard to which it is, or will become, compliant (including a timeframe for compliance, if not already achieved), as well as any awards received over the past 18 months. Indicate all quality programs that are externally measured (e.g., Six Sigma, ISO 9001:2000) and how such certifications would directly benefit the Commonwealth. A detailed approach and quality plan should be included in the response to this section.

Client References

The Offeror must provide at least three (3) customer references for projects similar to this Project using **Appendix C – Project References**. If the Offeror is using subcontractors to provide a significant portion of services, each subcontractor must also provide at least three (3) references. To the extent possible, references should be selected to represent projects of similar size and complexity to the project described in this RFP. The Commonwealth at its sole discretion may request references from any or all proposed subcontractors.

The Offeror must include a client contact name, title, address, email address and phone number for each of the references provided. The Offeror will provide a brief description of the services provided for each client. The Offeror will also ensure that the

Commonwealth is able to discuss with the client or clients listed, the client's experience with the Offeror's services.

Experience shown should be work done by individuals who will be assigned to this project as well as that of your company. Studies or projects referred to must be identified and the name of the customer shown, including the name, address, and telephone number of the responsible official of the customer, company, or agency who may be contacted.

Subcontractors

The Offeror must provide a list of all proposed subcontractors that will be used as part of the project using **Schedule L – Approved Subcontractors**.

II-5. Personnel. Include the number of executive and professional personnel, analysts, auditors, researchers, programmers, consultants, etc., who will be engaged in the work. Show where these personnel will be physically located during the time they are engaged in the Project. Refer to **Schedule G - Staffing Plan and Key Positions** for key personnel, include the employee's name and, through a resume or similar document, the Project personnel's education and experience in respective Account Role as defined within **Schedule G - Staffing Plan and Key Positions.** Indicate the responsibilities each individual will have in this Project and how long each has been with your company. Identify by name any subcontractors you intend to use and the services they will perform.

II-6. Training. If appropriate, indicate recommended training of Commonwealth personnel. Include the Commonwealth personnel to be trained, the number to be trained, duration of the program, place of training, curricula, training materials to be used, number and frequency of sessions, and number and level of instructors.

II-7. Financial Capability. Describe your company's financial stability and economic capability to perform the contract requirements. Provide your company's financial statements (audited, if available) for the past three fiscal years. Financial statements must include the company's Balance Sheet and Income Statement or Profit/Loss Statements. Also include a Dun & Bradstreet comprehensive report, if available. If your company is a publicly traded company, please provide a link to your financial records on your company website in lieu of providing hardcopies. The Commonwealth reserves the right to request additional information it deems necessary to evaluate an Offeror's financial capability.

The Offeror must be able to demonstrate to the Commonwealth its financial soundness and its ability to remain viable as a provider of the Services over the term of the agreement. The Offeror must provide the following information for Offeror's lines of business that are directly comparable to outsourcing the Services:

- Revenues segmented by managed Datacenter business lines
- Revenues from all lines of business
- Total number of FTEs performing managed Datacenter services
- Locations and number of employees in each location
- Employee turnover rate

- Long-term debt rating (Moody's or S&P)
- Total market capitalization
- Number of customers to which it provides managed Datacenter services
- Length/total expected dollar value of all contracts in force

Offeror shall furnish to the Commonwealth as part of its technical submittal, certificates of insurance or other appropriate documentation evidencing all current insurance coverage.

The Commonwealth in its sole discretion reserves the right to request financial capability information from proposed subcontractors.

II-8. Objections and Additions to Contract Terms and Conditions. The Offeror will identify which, if any, of the terms and conditions (contained in **Appendix A**) it would like to negotiate and what additional terms and conditions the Offeror would like to add to the standard contract terms and conditions. The Offeror's failure to make a submission under this paragraph will result in its waiving its right to do so later, but the Issuing Office may consider late objections and requests for additions if to do so, in the Issuing Office's sole discretion, would be in the best interest of the Commonwealth. The Issuing Office may, in its sole discretion, accept or reject any requested changes to the standard contract terms and conditions. The Offeror shall not request changes to the other provisions of the RFP, nor shall the Offeror request to completely substitute its own terms and conditions for **Appendix A**. All terms and conditions must appear in one integrated contract. The Issuing Office will not accept references to the Offeror's, or any other, online guides or online terms and conditions contained in any proposal.

Regardless of any objections set out in its proposal, the Offeror must submit its proposal, including the cost proposal, on the basis of the terms and conditions set out in **Appendix A**.

The Issuing Office will reject any proposal that is conditioned on the negotiation of the terms and conditions set out in Appendix A or to other provisions of the RFP as specifically identified above.

II-9. Small Diverse Business Participation Submittal.

A. To receive credit for being a Small Diverse Business or for subcontracting with a Small Diverse Business (including purchasing supplies and/or services through a purchase agreement), an Offeror must include proof of Small Diverse Business qualification in the Small Diverse Business participation submittal of the proposal, as indicated below:

- A Small Diverse Business verified by BSBO as a Small Diverse Business must provide a photocopy of their verification letter.

B. In addition to the above verification letter, the Offeror must include in the Small Diverse Business participation submittal of the proposal the following information:

1. Offerors must include a numerical percentage which represents the total percentage of the work (as a percentage of the total amount paid to the Offeror under the contract) that the Offeror commits to paying to Small Diverse Businesses (SDBs) as subcontractors. To support its total percentage SDB subcontractor commitment, Offeror must also include:

   a) The percentage of each subcontract commitment to a Small Diverse Business.

   b) The name of each Small Diverse Business. The Offeror will not receive credit for stating that after the contract is awarded it will find a Small Diverse Business.

   c) The services or supplies each Small Diverse Business will provide, including the timeframe for providing the services or supplies.

   d) The location where each Small Diverse Business will perform services.

   e) The timeframe for each Small Diverse Business to provide or deliver the goods or services.

   f) A completed and signed letter of intent, in the format set forth in Appendix J - SDB Letter of Intent, for each Small Diverse Business.

   g) The name, address and telephone number of the primary contact person for each Small Diverse Business.

2. The total percentages and each SDB subcontractor commitment will become contractual obligations once the contract is fully executed.

3. The name and telephone number of the Offeror's project (contact) person for the Small Diverse Business information.

C. The Offeror is required to submit two copies of its Small Diverse Business participation submittal. The submittal shall be clearly identified as Small Diverse Business information and sealed in its own envelope, separate from the remainder of the proposal.

D. A Small Diverse Business can be included as a subcontractor with as many prime contractors as it chooses in separate proposals.

E. An Offeror that qualifies as a Small Diverse Business and submits a proposal as a prime contractor is not prohibited from being included as a subcontractor in separate proposals submitted by other Offerors.

II-10. Cost Submittal. The information submitted in **Schedule I - Offeror Pricing Forms** shall constitute the Cost Submittal. The Cost Submittal shall be placed in a separate sealed envelope within the sealed proposal, separated from the technical submittal. Offerors should **not** include any assumptions in their cost submittals. If the Offeror includes assumptions in its cost submittal, the Issuing Office may reject the proposal. Offerors should direct in writing to the Issuing Office pursuant to **Part I, Section I-9**, of this RFP any questions about whether a cost or other component is included or applies. All Offerors will then have the benefit of the Issuing Office's written answer so that all proposals are submitted on the same basis.

II-11. Domestic Workforce Utilization Certification. Complete and sign the Domestic Workforce Utilization Certification contained in **Appendix D** of this RFP. Offerors who seek consideration for this criterion must submit in hardcopy the signed Domestic Workforce Utilization Certification Form in the same sealed envelope with the Technical Submittal.

II-12. COSTARS Program Election to Participate. Offerors electing to permit COSTARS members to participate in this Contract should complete and sign the COSTARS Program Election to Participate form contained in **Appendix E** of this RFP. If the Offeror is asserting that it is a Department of General Services Certified Small Business, also provide an active Department of General Services Small Business Certification. Submit the form and the certification, as applicable, in the same sealed envelope with the Technical Submittal only if the Offeror elects to participate in the program.

II-13. Lobbying Certification and Disclosure of Lobbying Activities

This Project may be funded, in whole or in part, with federal monies. Public Law 101-121, Section 319, prohibits federal funds from being expended by the recipient or by any lower tier sub-recipients of a federal contract, grant, loan, or a cooperative agreement to pay any person for influencing, or attempting to influence a federal agency or Congress in connection with the awarding of any federal contract, the making of any federal grant or loan, or entering into any cooperative agreement. Offerors who submit proposals in response to this RFP must sign the "Lobbying Certification Form," (attached as **Appendix H**) and, if applicable, complete the "Disclosure of Lobbying Activities" form available at: http://www.whitehouse.gov/omb/assets/omb/grants/sflllin.pdf.

PART III

CRITERIA FOR SELECTION

III-1. Mandatory Responsiveness Requirements. To be responsive, a proposal must be:

A. Timely received from an Offeror;

B. Properly signed by the Offeror;

C. Submitted by an Offeror that is ISO 27001, ISO 9001 and ISO/IEC 20000 certified;

a. A copy of the certifications must be submitted with the proposal.

D. Submitted by an Offeror that has successfully passed a SSAE 16 audit within twelve (12) months of the proposal due date.

a. A copy of the audit findings report must be submitted with the proposal.

Offerors must provide the copies of the ISO 27001, ISO 9001 and ISO/IEC 20000 certifications and SSAE 16 audit findings report as an appendix to the Offeror's technical submittal. The appendix must be titled "Mandatory Requirements."

III-2. Technical Nonconforming Proposals. The **four (4)** Mandatory Responsiveness Requirements set forth in **Section III-1** above (A-D) are the only RFP requirements that the Commonwealth will consider to be *non-waivable.* The Issuing Office reserves the right, in its sole discretion, to (1) waive any other technical or immaterial nonconformities in an Offeror's proposal, (2) allow the Offeror to cure the nonconformity, or (3) consider the nonconformity in the scoring of the Offeror's proposal.

III-3. Evaluation. The Issuing Office has selected a committee of qualified personnel to review and evaluate timely submitted proposals. Independent of the committee, BSBO will evaluate the Small Diverse Business participation submittal and provide the Issuing Office with a rating for this component of each proposal. The Issuing Office will notify in writing of its selection for negotiation the responsible Offeror whose proposal is determined to be the most advantageous to the Commonwealth as determined by the Issuing Office after taking into consideration all of the evaluation factors.

III-4. Evaluation Criteria. The following criteria will be used in evaluating each proposal:

A. **Technical:** The Issuing Office has established the weight for the Technical criterion for this RFP as **50 %** of the total points. Evaluation will be based upon the following:

- **Proposed Facilities**
- **Offeror Qualification**
- **Personnel Qualifications**
- **Soundness of Approach**
- **Understanding the Problem**

The final Technical scores are determined by giving the maximum number of technical points available to the proposal with the highest raw technical score. The remaining proposals are rated by applying the Technical Scoring Formula set forth at the following webpage: http://www.portal.state.pa.us/portal/server.pt/community/rfp_scoring_formulas_overview/20124.

B. **Cost:** The Issuing Office has established the weight for the Cost criterion for this RFP as **30%** of the total points. The cost criterion is rated by giving the proposal with the lowest total cost the maximum number of Cost points available. The remaining proposals are rated by applying the Cost Formula set forth at the following webpage: http://www.portal.state.pa.us/portal/server.pt/community/rfp_scoring_formulas_overview/20124

C. **Small Diverse Business Participation:** BSBO has established the weight for the Small Diverse Business (SDB) participation criterion for this RFP as **20%** of the total points. Each SDB participation submittal will be rated for its approach to enhancing the utilization of SDBs in accordance with the below-listed priority ranking and subject to the following requirements:

1. To receive credit for an SDB subcontracting commitment, the SDB subcontractor must perform at least fifty percent (50%) of the work subcontracted to it.

2. A significant subcontracting commitment is a minimum of one percent (1%) of the total contract value.

3. A subcontracting commitment less than one percent (1%) of the total contract value is considered nominal and will receive reduced or no additional SDB points depending on the priority ranking.

Priority Rank 1: Proposals submitted by SDBs as prime contractors will receive 150 points. In addition, SDB prime contractors that have significant subcontracting commitments to additional SDBs may receive up to an additional 50 points (200 points total available).

Subcontracting commitments to additional SDBs are evaluated based on the proposal offering the highest total percentage SDB subcontracting commitment. All other Offerors will be scored in proportion to the highest total percentage SDB subcontracting commitment within this ranking. *See formula below.*

Priority Rank 2: Proposals submitted by SDBs as prime contractors, with no or nominal subcontracting commitments to additional SDBs, will receive 150 points.

Priority Rank 3: Proposals submitted by non-small diverse businesses as prime contractors, with significant subcontracting commitments to SDBs, will receive up to 100 points. Proposals submitted with nominal subcontracting commitments to SDBs will

receive points equal to the percentage level of their total SDB subcontracting commitment.

SDB subcontracting commitments are evaluated based on the proposal offering the highest total percentage SDB subcontracting commitment. All other Offerors will be scored in proportion to the highest total percentage SDB subcontracting commitment within this ranking. *See formula below.*

Priority Rank 4: Proposals by non-small diverse businesses as prime contractors with no SDB subcontracting commitments shall receive no points under this criterion.

To the extent that there are multiple SDB Participation submittals in Priority Rank 1 and/or Priority Rank 3 that offer significant subcontracting commitments to SDBs, the proposal offering the highest total percentage SDB subcontracting commitment shall receive the highest score (or additional points) available in that Priority Rank category and the other proposal(s) in that category shall be scored in proportion to the highest total percentage SDB subcontracting commitment. Proportional scoring is determined by applying the following formula:

SDB % Being Scored	*x*	*Points/Additional*	=	*Awarded/Additional*
Highest % SDB Commitment		*Points Available*		*SDB Points*

Priority Rank 1 = 50 Additional Points Available
Priority Rank 3 = 100 Total Points Available

Please refer to the following webpage for an illustrative chart which shows SDB scoring based on a hypothetical situation in which the Commonwealth receives proposals for each Priority Rank:

http://www.portal.state.pa.us/portal/server.pt/community/rfp_scoring_formulas_overview/20124

D. **Domestic Workforce Utilization:** Any points received for the Domestic Workforce Utilization criterion are bonus points in addition to the total points for this RFP. The maximum amount of bonus points available for this criterion is 3% of the total points for this RFP.

To the extent permitted by the laws and treaties of the United States, each proposal will be scored for its commitment to use domestic workforce in the fulfillment of the contract. Maximum consideration will be given to those Offerors who will perform the contracted direct labor exclusively within the geographical boundaries of the United States or within the geographical boundaries of a country that is a party to the World Trade Organization Government Procurement Agreement. Those who propose to perform a portion of the direct labor outside of the United States and not within the geographical boundaries of a party to the World Trade Organization Government Procurement Agreement will receive a correspondingly smaller score for this criterion. See the following webpage for the Domestic Workforce Utilization Formula:

http://www.portal.state.pa.us/portal/server.pt/community/rfp_scoring_formulas_overview/20124. Offerors who seek consideration for this criterion must submit in hardcopy the signed Domestic Workforce Utilization Certification Form in the same sealed envelope with the Technical Submittal. The certification will be included as a contractual obligation when the contract is executed.

III-5. Offeror Responsibility. To be responsible, an Offeror must submit a responsive proposal and possess the capability to fully perform the contract requirements in all respects and the integrity and reliability to assure good faith performance of the contract.

In order for an Offeror to be considered responsible for this RFP and therefore eligible for selection for best and final offers or selection for contract negotiations:

A. The total score for the technical submittal of the Offeror's proposal must be greater than or equal to **75% of the available technical points**; and

B. The Offeror's financial information must demonstrate that the Offeror possesses the financial capability to assure good faith performance of the contract. The Issuing Office will review the Offeror's previous three audited annual financial statements, any additional information received from the Offeror, and any other publicly-available financial information concerning the Offeror, and assess each Offeror's financial capacity based on calculating and analyzing various financial ratios, and comparison with industry standards and trends.

An Offeror which fails to demonstrate sufficient financial capability to assure good faith performance of the contract as specified herein may be considered by the Issuing Office, in its sole discretion, for Best and Final Offers or contract negotiation contingent upon such Offeror providing contract performance security, in a form acceptable to the Issuing Office, for twenty percent (20%) of the contract value for the base term proposed by the Offeror. Based on the financial condition of the Offeror, the Issuing Office may require a certified or bank (cashier's) check, letter of credit, or a performance bond conditioned upon the faithful performance of the contract by the Offeror. The required performance security must be issued or executed by a bank or surety company authorized to do business in the Commonwealth. The cost of the required performance security will be the sole responsibility of the Offeror and cannot increase the Offeror's cost proposal or the contract cost to the Commonwealth.

Further, the Issuing Office will award a contract only to an Offeror determined to be responsible in accordance with the most current version of Commonwealth Management Directive 215.9, Contractor Responsibility Program.

III-6. Final Ranking and Award.

A. After any best and final offer process conducted, the Issuing Office will combine the evaluation committee's final technical scores, BSBO's final small diverse business participation scores, the final cost scores, and (when applicable) the domestic workforce utilization scores, in accordance with the relative weights assigned to these areas as set forth in this Part.

B. The Issuing Office will rank responsible offerors according to the total overall score assigned to each, in descending order.

C. The Issuing Office must select for contract negotiations the offeror with the highest overall score; PROVIDED, HOWEVER, THAT AN AWARD WILL NOT BE MADE TO AN OFFEROR WHOSE PROPOSAL RECEIVED THE LOWEST TECHNICAL SCORE AND HAD THE LOWEST COST SCORE OF THE RESPONSIVE PROPOSALS RECEIVED FROM RESPONSIBLE OFFERORS. IN THE EVENT SUCH A PROPOSAL ACHIEVES THE HIGHEST OVERALL SCORE, IT SHALL BE ELIMINATED FROM CONSIDERATION AND AWARD SHALL BE MADE TO THE OFFEROR WITH THE NEXT HIGHEST OVERALL SCORE.

D. The Issuing Office has the discretion to reject all proposals or cancel the request for proposals, at any time prior to the time a contract is fully executed, when it is in the best interests of the Commonwealth. The reasons for the rejection or cancellation shall be made part of the contract file.

PART IV

WORK STATEMENT

IV-1. Objectives. The objective of this procurement is to enter into a single agreement with a company or consortium of companies (with a single prime) that will provide the entire scope of services detailed within this RFP, which include but is not limited, to replacing the existing DPH, EDC and agency datacenter services. The resulting contract is intended to provide the entire suite of services with common invoicing/billing, communications, governance, management, support organization and interface. Program objectives are described in **Schedule F Section 2.1 Program Objectives.**

IV-2. Nature and Scope of the Project.

The Commonwealth is focused on an agency-wide datacenter modernization initiative. This initiative includes implementing a new datacenter service model that will provide various infrastructures/computing platforms to service the needs of the Commonwealth in a secure and flexible manner.

The Commonwealth currently has six (6) datacenters located within Commonwealth controlled (owned or leased) buildings. These datacenters provide computing services for the Commonwealth as a whole or for a specific agency. The Commonwealth has over the last several years been consolidating its datacenters into one of two enterprise datacenters. One of these datacenters is managed under an agreement with Unisys Corporation and the other is managed by the OA/OIT. The datacenter managed by Unisys Corporation is under an agreement that terminates on December 31, 2014.With more than $1 billion in information technology (IT) investments annually, the Commonwealth of Pennsylvania (Commonwealth) is the equivalent of a Fortune 20 organization providing a diverse portfolio of IT services and solutions to its 12.3 million citizens and business customers worldwide. Prior to 2006, these services and solutions were offered by more than 45 individual agencies, boards and commissions; each operating under its own mission and business objectives.

Executive Order 2004-8, as amended May 9, 2007, addresses the need for coordinated IT planning and resource utilization by directing the consolidation of agency information technology organizations under the Office for Information Technology.

As a result of this directive, the Commonwealth's approach to IT was published. The Chief Information Officer issued an IT Strategic Plan for 2012-2015. This plan can be viewed in its entirety at:

http://www.portal.state.pa.us/portal/server.pt/document/1218867/it_strategic_plan_2012-15_pdf

IV-3. Requirements. The following sections set forth the requirements of the Project. Offerors must address each requirement:

A. **Business and Technical Requirements.**

The business and technical requirements are detailed in **Schedule F** of this RFP.

B. **Office Location.**

The selected Offeror must maintain an office in the Harrisburg, PA area during the term of the contract. If the selected Offeror does not currently have an office in the Harrisburg, PA area, it must establish an office within two (2) months of award of the contract.

C. **Proposed Services.**

The selected Offeror shall not significantly alter or discontinue any Service defined in this RFP or proposed by the Offeror without prior written authorization from the Commonwealth.

D. **Service Catalog**

The Offeror must provide the Services listed in Schedule C - Services Catalog.

E. **Payment for Services**

The selected Offeror may bill for a Service, including those transitioned from the EDC, DPH or a Commonwealth Agency datacenter, once the Commonwealth accepts the Service via ITSM.

F. **Emergency Preparedness.**

To support continuity of operations during an emergency, including a pandemic, the Commonwealth needs a strategy for maintaining operations for an extended period of time. One part of this strategy is to ensure that essential contracts that provide critical business services to the Commonwealth have planned for such an emergency and put contingencies in place to provide needed goods and services.

1. Describe Offeror anticipates such a crisis will impact its operations.

2. Describe Offeror's emergency response continuity of operations plan. Please attach a copy of the plan, or at a minimum, summarize how the plan addresses the following aspects of pandemic preparedness:

   a) Employee training (describe Offeror's training plan, and how frequently it plan will be shared with employees)

   b) Identified essential business functions and key employees (within Offeror's organization) necessary to carry them out

   c) Contingency plans for:

      i.) How Offeror will handle staffing issues when a portion of key employees are incapacitated due to illness.

      ii.) How Offeror employees will carry out the essential functions if contagion control measures prevent them from coming to the primary workplace.

d) How Offeror will communicate with staff and suppliers when primary communications systems are overloaded or otherwise fail, including key contacts, chain of communications (including suppliers), etc.

e) How and when Offeror's emergency plan will be tested, and if the plan will be tested by a third-party.

IV-4. Tasks.

A. **Schedule F** of this RFP details the specific tasks and requirements that encompass the Project. The selected Offeror shall perform the tasks set forth in **Schedule F**.

B. **Schedules J.1, J.2, and J.3** details the Service Levels required by the Commonwealth.

IV-5. Reports and Project Control.

A. **Task Plans.** A work plan for each task that identifies the work elements of each task, the resources assigned to the task, and the time allotted to each element and the deliverable items to be produced. Where appropriate, a PERT or GANTT chart display should be used to show project, task, and time relationship. This Plan should identify the Offer's PMO establishment, Major Transition Tasks, and Major Steady State events throughout the term of this engagement.

B. **Status Reports.** Monthly progress reports covering activities, problems, risks and recommendations. This report should be keyed to the work plan the Offeror developed in its proposal, as amended or approved by the Issuing Office. During the Transition period of this project additional progress reports are required.

Monthly Service Level, Change Management, Incident/Problem, Operational, and Billing Reports are to be provided. These reports will be developed in cooperation with the Commonwealth during the early stages of the engagement.

C. **Problem Identification Reports.** An "as required" report, identifying problem areas. The report should describe the problem and its impact on the overall project and on each affected task. It should list possible courses of action with advantages and disadvantages of each, and include Offeror recommendations with supporting rationale.

IV-6. Contract Requirements—Small Diverse Business Participation.

All contracts containing Small Diverse Business participation must also include a provision requiring the selected contractor to meet and maintain those commitments made to Small Diverse Businesses at the time of proposal submittal or contract negotiation, unless a change in the commitment is approved by the BSBO. All contracts containing Small Diverse Business participation must include a provision requiring Small Diverse Business subcontractors to perform at least **50%** of the subcontracted work.

The selected contractor's commitments to Small Diverse Businesses made at the time of proposal submittal or contract negotiation shall, to the extent so provided in the commitment, be maintained throughout the term of the contract and through any renewal or extension of the contract. Any proposed change must be submitted to BSBO, which will make a recommendation to the Contracting Officer regarding a course of action.

If a contract is assigned to another contractor, the new contractor must maintain the Small Diverse Business participation of the original contract.

The selected contractor shall complete the Prime Contractor's Quarterly Utilization Report (or similar type document containing the same information) and submit it to the contracting officer of the Issuing Office and BSBO within **ten** (**10)** workdays at the end of each quarter the contract is in force. This information will be used to determine the actual dollar amount paid to Small Diverse Business subcontractors and suppliers. Also, this information will serve as a record of fulfillment of the commitment the selected contractor made and for which it received Small Diverse Business participation points. If there was no activity during the quarter then the form must be completed by stating "No activity in this quarter."

NOTE: EQUAL EMPLOYMENT OPPORTUNITY AND CONTRACT COMPLIANCE STATEMENTS REFERRING TO COMPANY EQUAL EMPLOYMENT OPPORTUNITY POLICIES OR PAST CONTRACT COMPLIANCE PRACTICES DO NOT CONSTITUTE PROOF OF SMALL DIVERSE BUSINESS STATUS OR ENTITLE AN OFFEROR TO RECEIVE CREDIT FOR SMALL DIVERSE BUSINESS UTILIZATION.

Request for Proposal

RFP # 6100022698

Commonwealth of Pennsylvania
Office of Administration
Office for Information Technology
Data Center Computing Services

APPENDIX A

CONTRACT TERMS AND CONDITIONS

TABLE OF CONTENTS

1. CONTRACT TERM 1
2. PURCHASE ORDERS 2
3. IDENTIFICATION NUMBER 3
4. ORDER OF PRECEDENCE, DEFINITIONS AND CONSTRUCTION 3
5. CONTRACT INTEGRATION 4
6. SERVICES 5
7. EQUIPMENT 8
8. THIRD PARTY SOFTWARE 9
9. DATA SECURITY 10
10. CONDUCT OF SERVICES 12
11. QUALITY ASSURANCE AND INTERNAL CONTROLS 13
12. SERVICE LOCATIONS 14
13. CONDITIONS OF CONTRACTOR'S OCCUPANCY OF COMMONWEALTH-PROVIDED REAL PROPERTY 17
14. TRANSITION 19
15. DISASTER RECOVERY AND BUSINESS CONTINUITY 23
16. PRIME CONTRACTOR RESPONSIBILITIES 25
17. KEY POSITIONS/CONTRACTOR PERSONNEL 25
18. THIRD PARTY SERVICES 27
19. COMPENSATION 28
20. FEES 28
21. PAYMENT SCHEDULE AND INVOICES 29
22. INSPECTION AND ACCEPTANCE 30
23. SERVICE LEVELS 31
24. LIQUIDATED DAMAGES 32
25. CONTINUOUS IMPROVEMENT AND BENCHMARKING 33
26. GOVERNANCE 36
27. CHANGE CONTROL 36
28. NOTICE OF DELAYS 38
29. NOTICE 38
30. DEFAULT 38
31. STEP-IN RIGHTS 41
32. TERMINATION 41
33. TERMINATION ASSISTANCE 45
34. CONTRACT CONTROVERSIES 52

35. COMMONWEALTH HELD HARMLESS 53
36. LIMITATION OF LIABILITY 53
37. CONFIDENTIALITY 55
38. SENSITIVE INFORMATION 58
39. PATENT, COPYRIGHT, TRADEMARK, AND TRADE SECRET PROTECTION 59
40. PROPRIETARY RIGHTS 61
41. PUBLICATION RIGHTS AND/OR COPYRIGHTS 65
42. REPORTS AND DATA 66
43. SECURITY AND PROTECTION OF INFORMATION 67
44. BACKGROUND CHECKS 68
45. INSURANCE 68
46. WARRANTIES 70
47. CONTRACTOR RESPONSIBILITY PROGRAM 72
48. OFFSET PROVISION FOR COMMONWEALTH CONTRACTS 73
49. TAXES-FEDERAL, STATE, AND LOCAL 73
50. POLICIES AND PROCEDURES 74
51. AUDIT OBLIGATIONS 74
52. VIRUS AND MALICIOUS CODE 77
53. THE AMERICANS WITH DISABILITIES ACT 78
54. NONDISCRIMINATION CLAUSE/SEXUAL HARASSMENT CLAUSE 78
55. CONTRACTOR INTEGRITY PROVISIONS 79
56. RIGHT-TO-KNOW LAW 85
57. ENVIRONMENTAL PROTECTION 86
58. ASSIGNABILITY 87
59. INDEPENDENT CAPACITY OF CONTRACTOR 87
60. THIRD PARTY BENEFICIARIES 88
61. CERTIFICATION REGARDING SUSPENSION 88
62. SUSPENSION OF SUBCONTRACTORS 88
63. ASSIGNMENT OF RIGHTS UNDER THE ANTITRUST LAWS 88
64. SIGNIFICANT EVENTS 89
65. FORCE MAJEURE 89
66. CONFLICT OF INTEREST 90
67. OFFICIALS NOT TO BENEFIT 90
68. CONSENTS, APPROVALS, NOTICES AND REQUESTS 90
69. REQUIRED CONSENTS 90
71. EXAMINATION OF RECORDS 91
72. SURVIVAL 92

73. SEVERABILITY 92
74. WAIVER 92
75. PERIOD OF PERFORMANCE 92
76. SPECIAL REQUIREMENTS 92
77. GOVERNING LAW 92
78. COMPLIANCE WITH LAWS 93
79. SMALL DIVERSE BUSINESS COMMITMENT 93
80. ACKNOWLEDGEMENT 93
81. COVENANT OF FURTHER ASSURANCES 93
82. COVENANT OF GOOD FAITH 94
83. AMENDMENTS 94
84. ENTIRE CONTRACT 94
APPENDIX A - BUSINESS ASSOCIATE APPENDIX LANGUAGE 1

TABLE OF SCHEDULES

SCHEDULE A - DEFINED TERMS

SCHEDULE B - GOVERNANCE

SCHEDULE C – SERVICES CATALOG

SCHEDULE D - TRANSITION MILESTONES

SCHEDULE E – DATACENTER LOCATIONS

SCHEDULE F – COPA DATACENTER STATEMENT OF WORK

SCHEDULE G - STAFFING PLAN AND KEY POSITIONS

SCHEDULE H - COMMONWEALTH COMPUTING PROCEDURES MANUAL

SCHEDULE I - OFFEROR PRICING FORMS

SCHEDULE J.1 - SERVICE LEVEL MANAGEMENT

SCHEDULE J.2 - DATACENTER SERVICE LEVEL MATRIX

SCHEDULE J.3 - DATACENTER SLA DEFINITIONS

SCHEDULE K - KEY PROGRAM DELIVERABLES

SCHEDULE L – APPROVED SUBCONTRACTORS

SCHEDULE M – DETAILED TRANSITION PLAN

TERMS AND CONDITIONS

1. CONTRACT TERM

(a) The term of the Contract shall commence on the Effective Date and shall end in seven (7) years ("the Expiration Date"), subject to the other provisions of the Contract. The Effective Date shall be: a) the date the Contract has been fully executed by the Contractor and by the Commonwealth and all approvals required by Commonwealth contracting procedures have been obtained or b) the date referenced in the Contract, whichever is later. The Contract shall not be a legally binding contract until after the fully-executed Contract has been sent to the Contractor.

(b) The Commonwealth may, in its sole discretion, renew the Contract for three (3) one (1) year periods, or any combination thereof, on the terms and conditions in force at the date of the renewal and utilizing pricing to be negotiated but consistent with and no less favorable than the pricing in force at the date of the renewal. Further, the Commonwealth reserves the right to extend this Contract or any part of this Contract up to three (3) months, or as necessary to prevent a lapse in Contract coverage.

(c) The Commonwealth reserves the right to execute the Contract, Purchase Orders or any follow-up Contract documents in ink or electronically. The Contractor understands and agrees that the receipt of an electronically-printed Contract with the printed name of the Commonwealth purchasing agent constitutes a valid, binding contract with the Commonwealth. The printed name of the purchasing agent on the Contract represents the signature of that individual who is authorized to bind the Commonwealth to the obligations contained in the Contract. The printed name also indicates that all approvals required by Commonwealth contracting procedures have been obtained.

(d) The Contractor shall not start performance, and the Commonwealth shall not be liable to pay the Contractor for any supply furnished or work performed or expenses incurred, until all of the following have occurred:

(1) The Effective Date has arrived;

(2) The Contractor has received a copy of the fully executed Contract (or written notice from the Commonwealth that the Contract has been fully executed); and

(3) The Contractor has received a Purchase Order or other written notice to proceed signed by the Commonwealth Contracting Officer.

No Commonwealth employee has the authority to verbally direct the commencement of any work or delivery of any supply under this Contract prior to the Effective Date.

2. PURCHASE ORDERS

(a) The Commonwealth may issue Purchase Orders against the Contract. These orders constitute the Contractor's authority to make delivery. All Purchase Orders received by the Contractor up to and including the expiration date of the Contract are acceptable and must be performed in accordance with the Contract. Contractors are not permitted to accept Purchase Orders which require performance in excess of those performance time periods specified in the Contract. Each Purchase Order will be deemed to incorporate the terms and conditions set forth in the Contract.

(b) Purchase Orders will not include an ink signature by the Commonwealth. The electronically-printed name of the purchaser represents the signature of the individual who has the authority, on behalf of the Commonwealth, to authorize the Contractor to proceed.

(c) Purchase Orders may be issued electronically or through facsimile equipment. The electronic transmission of a purchase order shall require acknowledgement of receipt of the transmission by the Contractor.

(d) Contractor's acknowledgment of receipt of the electronic or facsimile transmission of the Purchase Order shall constitute receipt of an order.

(e) Purchase Orders received by the Contractor after 4:00 p.m. will be considered received the following business day.

(f) The Commonwealth and the Contractor specifically agree as follows:

(1) No handwritten signature shall be required in order for the Contract or Purchase Order to be legally enforceable.

(2) Upon receipt of a Purchase Order, the Contractor shall promptly and properly transmit an acknowledgement in return. Any order which is issued electronically shall not give rise to any obligation to deliver on the part of the Contractor, or any obligation to receive and pay for delivered products on the part of the Commonwealth, unless and until the Commonwealth agency transmitting the order has properly received an acknowledgement.

(3) The parties agree that no writing shall be required in order to make the order legally binding. The parties hereby agree not to contest the validity or enforceability of the Contract or a genuine Purchase

Order or acknowledgement that have been issued electronically under the provisions of a statute of frauds or any other applicable law relating to whether certain agreements shall be in writing and signed by the party bound thereby. The Contract and any genuine Purchase Order or acknowledgement issued electronically, if introduced as evidence on paper in any judicial, arbitration, mediation, or administrative proceedings, will be admissible as between the parties to the same extent and under the same conditions as other business records originated and maintained in documentary form. Neither party shall contest the admissibility of copies of the Contract or any genuine Purchase Order or acknowledgements under either the business records exception to the hearsay rule or the best evidence rule on the basis that the Contract or Purchase Order or acknowledgement were not in writing or signed by the parties. A Purchase Order or acknowledgment shall be deemed to be genuine for all purposes if it is transmitted to the location designated for such documents.

(4) Each party will immediately take steps to verify any document that appears to be obviously garbled in transmission or improperly formatted to include re-transmission of any such document if necessary.

(g) Purchase Orders under five thousand dollars ($5,000) in total amount may also be made using a Commonwealth Procurement VISA Card in person or by telephone. When an order is placed by telephone, the Commonwealth agency shall provide the agency name, employee name, credit card number, and expiration date of the card. The Contractor agrees to accept payment through the use of the Commonwealth Procurement VISA card.

3. IDENTIFICATION NUMBER

The Contractor must have a SAP Vendor Number.

4. ORDER OF PRECEDENCE, DEFINITIONS AND CONSTRUCTION

(a) If any conflicts or discrepancies should arise in the terms and conditions of this Contract, or the interpretation thereof, the order of precedence shall be:

(1) This Contract (first, the Contract, including the terms and conditions, second the Schedules and Appendices); then

(2) The Contractor's Proposal (including the clarifications and the Best and Final Offer), as accepted by the Commonwealth; and then

(3) The RFP.

(b) Except as otherwise expressly provided in the Contract, all capitalized terms used in the Contract shall have the meanings set forth in *Schedule A* (Defined Terms).

(c) Interpretation:

(1) The terms defined in the Contract include the plural as well as the singular and the derivatives of such terms. Unless otherwise expressly stated, the words "herein," "hereof," and "hereunder" and other words of similar import refer to the Contract as a whole and not to any particular Paragraph, Section, subsection or other subdivision. The words "include" and "including" shall not be construed as terms of limitation.

(2) Headings preceding the text of Paragraphs or Sections, and headings to Schedules and Appendices, the table of contents and the table of Schedules and Appendices included in or attached to the Contract are used for convenience only and are not to be considered in construing or interpreting the Contract.

(3) References to any law refer to such law in changed or supplemented form, or to a newly adopted law replacing a previous law.

(4) Except as may be expressly set forth herein, all references to time herein refer to Eastern Standard Time or Eastern Daylight Time, as applicable.

(d) The Contract includes each Schedule, Exhibit and Appendix referenced herein, all of which are incorporated into the Contract by this reference

5. CONTRACT INTEGRATION

(a) This Contract, including the Contract signature pages, together with the Contractor's Proposal, the Contractor's clarifications and the Contractor's Best and Final Offer, and the RFP and addenda thereto that are incorporated herein by reference, constitutes the final, complete, and exclusive Contract between the parties containing all the terms and conditions agreed to by the parties.

(b) All representations, understandings, promises, and agreements pertaining to the subject matter of this Contract made prior to or at the time this Contract is executed are superseded by this Contract.

(c) There are no conditions precedent to the performance of this Contract except as expressly set forth herein.

(d) No contract terms or conditions are applicable to this Contract except as they are expressly set forth herein.

6. SERVICES

(a) The Contractor agrees to provide the Services to the Commonwealth as such services are defined in this Contract, the RFP and the Contractor's Proposal, and in accordance with the terms of this Contract.

(b) The Contractor shall provide to Commonwealth the following Services pursuant to the terms of the Contract:

(1) Commencing as of the Effective Date, the Transition Services set forth in *Section 14* (Transition) and *Schedule D* (Transition Milestones);

(2) Commencing as of the Effective Date and continuing until the Expiration Date:

(i) The services, function and responsibilities described in the Contract, including the Services set forth in (Services Catalog) and *Schedule F* (Statement of Work);

(ii) Any incidental services, functions or responsibilities not specifically described in the Contract, but which are inherent or required for the proper performance and delivery of the Services; and

(iii) The services, functions and responsibilities related to those categories of Services which Contractor is assuming pursuant to the Contract; and

(3) Commencing upon written notice by Commonwealth to Contractor in accordance with *Section 33* (Termination Assistance).

(c) The services set forth in (1) through (3) above shall be collectively referenced as the "Services," as they may evolve during the Term of the Contract or be supplemented, enhanced, modified or replaced pursuant to the terms hereof. The Services provided under this Contract are not exclusive to Contractor. The Commonwealth may in-source or re-procure any or all of the Services.

(d) The Commonwealth may request a change to the Services through a "*Request for Services*" to increase or decrease the amount of the Services provided under this Contract, according to Commonwealth's demand for the Services. The parties shall use the Change Control Procedures to implement the changes required by the *Request for Services* and revise the Fees as applicable.

(e) Except as may be necessary on an emergency basis to maintain the continuity of the Services or in the event of a declared disaster, Contractor shall not, without Commonwealth's written consent, modify (1) the composition of the Services, (2) the manner in which the Services are to be provided or delivered if such modification would have an adverse effect on the operations of Commonwealth, or (3) the applicable Services Levels.

(f) Except as otherwise expressly provided in this Contract, Contractor is responsible for providing, and is financially and operationally responsible for, the Facilities, Personnel, Equipment, Materials, technical knowledge, expertise and other resources necessary to provide the Services (including all upgrades, improvements, replacements and additions to such resources).

(g) Contractor acknowledges that Commonwealth encourages Contractor to provide the Services in a shared data processing environment, if such environment will materially reduce Commonwealth's costs under this Contract and can be accomplished within the confidentiality and physical security constraints imposed upon Contractor elsewhere in this Contract. Accordingly, upon the migration of any of Commonwealth's data processing to a Contractor Services Location, Contractor may provide the related Services from such Contractor Services Location in a shared data processing environment if Contractor reasonably believes such environment will materially reduce Commonwealth's costs under this Contract and if such shared environment and Contractor's use thereof to provide the Services otherwise comports with the terms of this Contract. Commonwealth reserves to itself the right of prior approval of any third party proposed by Contractor to share such data processing environment, such approval not to be unreasonably withheld. Contractor acknowledges that Commonwealth will be entitled to withhold its approval of any such third party if, among other things, there is no or insufficient economic benefit to Commonwealth from the proposed sharing arrangement or if any federal or state confidentiality issues are not resolved to the satisfaction of the applicable federal or state governmental entity.

(h) **Technical Architecture and Product Standards**. As part of the Services, Contractor shall suggest to Commonwealth information management technical architecture and product standards to be in effect at the Contractor Services Locations during the Term and the parties shall work together in good faith to develop information management technical architecture and product standards that are mutually acceptable to the parties and consistent with the Services Levels then in effect.

(i) **Remote Access Capabilities**. As part of the Services, Contractor shall provide remote access capabilities for use by authorized personnel of the Commonwealth. All such remote access capabilities shall meet or exceed all Commonwealth technology and security standards as set forth in *Section 12* (Service Locations).

(j) **Contractor Licenses and Permits**. As part of the Services, Contractor is responsible for obtaining, and has financial responsibility for, all necessary licenses, consents, approvals, permits and authorizations that are legally required to be obtained in order for Contractor to perform the Services. Commonwealth shall reasonably cooperate with and assist Contractor in obtaining any such licenses, consents, approvals, permits and authorizations. Notwithstanding the foregoing, Commonwealth will retain responsibility for obtaining, and the financial responsibility for, all necessary licenses, consents, approvals, permits and authorizations necessary to enable Contractor and its subcontractors to use the Commonwealth Software to the extent necessary for Contractor's performance of the Services and with Contractor's cooperation as further described in *Section 8* (Commonwealth Third Party Software), and Contractor will cooperate, and will cause the Contractor agents to cooperate, in good faith and at no additional cost to Commonwealth, in obtaining such licenses, consents, approvals, permits and authorizations.

(k) **Changes in Law and Regulations**. Each party shall identify, and notify the other party of, any changes in applicable statutes, regulations, or policies that may directly or indirectly relate to Contractor's performance of the Services. Contractor and Commonwealth shall work together to identify any impact of such changes upon Commonwealth's use, or Contractor's delivery, of the Services. Contractor shall be responsible for any fines and penalties arising from its noncompliance with any such identified statutes, regulations, or policies relating to the business of providing the Services and shall not be responsible for any fines and penalties assessed against Commonwealth by federal governmental entities from Commonwealth's noncompliance with any federal legislative enactments or federal regulatory requirements relating to Commonwealth's operations that does not result from Contractor's actions or inactions under this Contract. As part of the Services, Contractor shall, if possible, perform the Services regardless of changes in legislative enactments or regulatory requirements. If such changes prevent Contractor from performing any of its obligations under this Contract or increase Contractor's costs in connection therewith, Contractor shall provide written notice thereof to Commonwealth within five (5) days of learning of the change and, if possible, will develop and implement a suitable workaround until such time as Contractor can fully perform its obligations under this Contract without such workaround. Contractor shall bear any costs relating to any legislative enactments and regulatory requirements relating to its business, and Commonwealth shall bear all reasonable out of pocket expenses, excluding attorneys fees, incurred by Contractor relating to legislative enactments and regulatory requirements that require modification of the Services by Contractor. If the parties are unable to agree as to the allocation of such costs, the changes and costs that are the subject of this *Section 6(k)* shall be subject to the Change Control Procedures.

(l) **Access**. Upon Contractor's receipt of appropriate, advance notice (which except in an emergency situation shall not be less than three (3) business days) and subject to Contractor's reasonable security requirements, authorized representatives of Commonwealth, Commonwealth agents and agents of the Federal government shall be permitted access to any Contractor Services Location.

7. Equipment

Contractor shall provide the Services using the Equipment. Commonwealth shall provide Contractor with the required access and authorization to use the Commonwealth Machines.

(a) **Replacement and Upgrades of the Equipment**.

(1) Contractor shall maintain, replace and upgrade the Contractor Machines at its sole cost and expense. At its sole cost and expense, Contractor shall maintain the Commonwealth Machines and shall replace each Commonwealth Machine at its respective end of life or as otherwise required to provide the Services. All replacements and upgrades shall be addressed through the Change Control Procedure. Commonwealth agencies will work closely with the Office of Administration and Contractor to accurately plan for any additional just-in-time technology refresh and upgrade deployment as may be necessary for Contractor to perform the Services in accordance with the Services Levels while meeting new or increased demands of the agencies. Contractor acknowledges that all such replacements and upgrades shall consist of the then current technology; that is, Contractor will not extend use of then obsolete technology by increasing its capacity with additional hardware capacity if newer, proven technology is then available. In the case of all such replacement or upgrades, Contractor shall provide advance notice via the Change Control Procedure, reasonable under the circumstances to Commonwealth, and such replacement or upgrade shall be subject to Commonwealth's approval, including, without limitation, the approval of the contemplated implementation schedule and cost. If Commonwealth withholds its approval of such replacement, upgrade or contemplated schedule, the Contractor Project Manager and the Commonwealth Project Manager, in good faith and subject to the Change Control Procedures, will determine the appropriate adjustments to the Services Levels.

(2) In addition to the foregoing obligations of Contractor under this *Section 7* (Equipment). Contractor shall provide Commonwealth with information regarding additional Improved Technology for Commonwealth's evaluation in connection with the Services, to the extent then known to Contractor, and shall meet with Commonwealth

at least two (2) times during each Contract year to inform Commonwealth of any Improved Technology Contractor is developing or information processing trends and directions of which Contractor is aware. Upon the existence of any such additional Improved Technology that the parties believe would materially improve the performance, or reduce the cost, of the Services, (other than the required upgrades and replacements provided for above), the parties will meet and discuss in good faith the terms upon which such Improved Technology may be implemented into the Services. The parties acknowledge their intent, in such discussions, to develop terms for such implementation that will result in an equal sharing by the parties of the net economic benefit that is expected to result therefrom with the Fees adjusted accordingly (after taking into account Contractor's cost of the related hardware, software and implementation efforts). Upon any such projected reduction of the cost of the Services, the parties, working together in good faith, shall revise the Fees accordingly.

(b) **Equipment Maintenance**. As part of the Services, Contractor shall provide to Commonwealth maintenance and support services in respect of the Equipment and shall, at its own cost and expense, maintain and support the Contractor Machines as necessary for Contractor to perform the Services in accordance with the Services Levels. All costs and expenses incurred in connection with the provision of maintenance and support services in respect of the Equipment (including third party maintenance fees) shall be the responsibility of Contractor.

8. THIRD PARTY SOFTWARE

(a) As part of the Services, Contractor shall have operational responsibility for the Commonwealth Third Party Software for which Commonwealth has a valid license and current maintenance agreement ("Commonwealth Third Party Software") and shall be responsible for applying upgrades, enhancements and fixes as provided and directed by the applicable agency. The Commonwealth shall have financial responsibility for any Commonwealth Third Party Software license, upgrade, maintenance and support fees, except that Contractor shall be responsible for any third-party consulting fees in connection with the installation or implementation of any software upgrade, revision or replacement required by Contractor.

(b) As part of the Services, Contractor shall have financial, administration, operational and maintenance responsibility for all Contractor Software and Third Party Software provided by the Contractor as part of the Services, including but not limited to the Third Party Software listed in *Exhibit B.4.*

(c) As part of the Services, except for the cost of the license, Contractor shall have financial, administration, operational and maintenance responsibility for the Third

Party Software listed in *Exhibit B.10,* for which the Commonwealth has a valid license ("Hybrid Third Party Software").

(d) The Contractor shall not require the Commonwealth to sign a software license agreement for any Contractor Software or Third Party Software, including but not limited to any click through agreement or other terms purported to apply to the software.

(e) The Commonwealth will continue to support and maintain the software owned by the Commonwealth ("Commonwealth Proprietary Software") as necessary for Contractor's performance of the Services.

9. DATA SECURITY

(a) Commonwealth will retain administration of logical and data access security, and Contractor will host Commonwealth security applications software utilized by the Commonwealth in managing logical and data access security, and will not implement configurations that would prevent Commonwealth from managing logical and data access security. As part of the Services, Contractor shall implement and maintain the Commonwealth's safeguards against the disclosure, destruction, loss or alteration of the Commonwealth Data in the possession of Contractor in accordance with the terms of this Contract and with Commonwealth's other security policies and procedures provided, in writing, to Contractor. In any event, Contractor, as part of the Services, is required to meet or exceed the most stringent of any applicable federal or state law, statute, rule or regulation applicable to Contractor's and/or Contractor's Agents possession of, or access to, any Commonwealth Data (which includes *Section 12(d)*, herein). All changes or additions to any such Commonwealth security policies or procedure or any changes to any applicable federal or state law, statute, rule or regulation shall be implemented by Contractor. Any changes or additions which result in a material additional cost to Contractor shall be subject to the Change Control Procedures. To the degree such change applies to other Contractor customers, Contractor will mitigate the Commonwealth's economic exposure to additional cost by equitably spreading the additional cost of compliance to its multiple customers.

(b) The Contractor shall not store the Commonwealth Data outside of the continental United States of America.

(c) All of Contractor's activities relating to the safeguarding of Commonwealth Data shall be subject to periodic review and monitoring by Commonwealth and related Federal agencies, and Contractor shall cooperate fully with all such reviews and monitoring. In addition to, and not in limitation of, any restrictions set forth elsewhere in this Contract, Contractor shall have operational access to the Commonwealth Data only on an as-needed basis.

(d) Upon request at any time during the term of this Contract, or upon termination, cancellation, expiration or other conclusion of the Contract, Contractor shall return the Commonwealth Data to the Commonwealth or, at the Commonwealth's request, destroy the Data. If the Commonwealth request Contractor to destroy the Data, the Commonwealth shall have the right to conduct an audit to ensure the Data has been destroyed. This provision shall also apply to all Commonwealth Data that is in the possession of subcontractors or agents of Contractor. Contractor shall complete such return or destruction within ten (10) days of the request or after the conclusion of this Contract. Within such ten (10) day period, Contractor shall certify in writing to Commonwealth that such return or destruction has been completed. Contractor shall make available to the Commonwealth for a complete and secure (i.e. encrypted and appropriately authenticated) download file of the Commonwealth Data in XML format, or such other format as specified by the Commonwealth, including all schema and transformation definitions and/or delimited text files with documented, detailed schema definitions along with attachments in their native format. Contractor shall be available to answer questions about data schema, transformations, and other elements required to fully understand and utilize the Commonwealth's data file. Unless the Commonwealth agrees or specifies otherwise, the Contractor shall also deliver to the Commonwealth any copies, duplicates, summaries, abstracts or other representations of any such Commonwealth Data or any part thereof, in whatever form, then in the Contractor's possession or control in accordance with the "NIST Guidelines for Media Sanitization" (SP 800-88).

(e) Contractor shall comply with all state and Federal data breach laws, including but not limited to the Commonwealth Breach of Personal Information Notification Act (73 P.S. § §2301 *et seq*.). In the event Contractor or any of Contractor's Agents discover or are notified of a data breach or potential breach of security involving any of the Commonwealth Data, Contractor shall immediately notify the Commonwealth Project Manager and the Commonwealth's Chief Information Security Officer of the same and describe the nature of the breach, the Data compromised, the involved parties, mitigation efforts, and corrective actions to be taken by the Contractor. In addition, at Commonwealth's request and at Contractor's sole cost and expense, Contractor shall:

(1) Promptly provide Commonwealth Data security reports to Commonwealth in a form to be agreed upon by Commonwealth and Contractor; and

(2) Cooperate with any efforts by Commonwealth to investigate or prosecute any breach of security of the Commonwealth Data; and

(3) Provide credit monitoring services to all individuals or organizations that may be impacted by the security breach.

Contractor shall be solely responsible for any costs, losses or damages actually incurred by the Commonwealth due to Personal Information being accessed, used, released, disclosed and/or acquired in an unauthorized manner while in the possession and control of the Contractor or its employees, agents, and/or subcontractors. In the event of any data breach by Contractor or any of the Contractor Agents involving any of the Commonwealth Data, Contractor shall be assessed a credit against Fees due for Service provided during the period of breach of security.

(f) Credit Card Information

(1) By providing the Services under this Contract, the Contractor may create, receive, or have access to credit card records or record systems containing cardholder data including credit card numbers (collectively the "Cardholder Data"). Contractor shall comply with the Payment Card Industry Data Security Standard ("PCI DSS") requirements for Cardholder Data that are prescribed by the payment brands (including but not limited to Visa, MasterCard, American Express, and Discover), as they may be amended from time to time. Contractor acknowledges and agrees that Cardholder Data may only be used for assisting in completing a card transaction, for fraud control services, for loyalty programs, or as specifically agreed to by the payment brands, for purposes of this Contract or as required by applicable law.

(2) Contractor shall conform to and comply with the PCI DSS standards as defined by The PCI Security Standards Council at: https://www.pcisecuritystandards.org/security_standards/index.php. Contractor shall monitor these PCI DSS standards and will promptly notify the Commonwealth if its practices should not conform to such standards. Contractor shall provide a letter of certification to attest to meeting this requirement within one week of Contractor's receipt of the annual PCI DSS compliance report.

10. CONDUCT OF SERVICES

(a) Following execution of the Contract, Contractor shall proceed diligently with all Services and shall perform such Services with qualified personnel, in accordance with the completion criteria set forth in the Contract.

(b) The Contractor's Services hereunder shall be monitored by the Commonwealth and the Commonwealth's designated representatives. If the Commonwealth reasonably determines that the Contractor has not performed to the requirements in the Contract or has otherwise exposed the Commonwealth to material risk, the Commonwealth and the Contractor will attempt to reach agreement with respect to such matter. Failure of the Commonwealth or the

Contractor to arrive at such mutual determinations shall be a dispute concerning a question of fact within the meaning of *Section 34* (Contract Controversies) of this Contract.

(c) As part of the Services, Contractor shall conduct enterprise-wide Commonwealth Satisfaction Surveys, which surveys shall be conducted annually until completion of the Transition. Upon completion of the Transition, Contractor shall conduct the Commonwealth Satisfaction Surveys semi-annually for two years and annually thereafter.

11. QUALITY ASSURANCE AND INTERNAL CONTROLS

(a) Contractor will develop and implement quality assurance and internal controls, including implementing tools and methodologies, to ensure that the Services are performed in an accurate and timely manner, in accordance with the Contract. Without limiting the foregoing, Contractor will:

(1) Maintain a strong control environment in day-to-day operations;

(2) Develop and execute a process to ensure regular internal control self-assessments are performed with respect to all Services and report the outcome of such self-assessments to the Commonwealth;

(3) Maintain an internal audit function sufficient to monitor the processes and systems used to provide the Services (i.e., perform audits, track control measures, communicate status to management, drive corrective action, etc.); and

(4) Provide to Commonwealth a summary of audit activity performed, associated significant findings, status of follow-up activity, summary of control incidents (i.e., frauds, conflict of interest situations, etc.) and related corrective action, every six (6) months.

(b) As part of the Services and included in the Fees, Contractor shall:

(1) Implement and maintain independently audited quality certification (ISO 27001, ISO 9001 and ISO/IEC 20000 accreditation) and provide copies of its certification under such program and also any relevant audit or report documentation whenever so requested by the Commonwealth.

(2) Maintain valid security certifications including CISSP (Certified Information Systems Security Professional) or Comp TIA-Security+ or CASP and provide copies of its certification under such program and also any relevant documentation whenever so requested by the Commonwealth.

(3) Maintain compliance with Federal and State mandated policies including CJIS (Criminal Justice Information Services) and CHRIA (Criminal History Record Information Act) and provide copies of any relevant documentation whenever so requested by the Commonwealth.

(4) Undertake at least annually, and shall cause to be undertaken by Contractor's material subcontractors, a SSAE 16 Type II audit that covers the common controls for any Contractor sites where Contractor performs work for the Commonwealth; provide the reports from such audits to the Commonwealth; and perform these SSAE 16 Type II audits at such time(s) that shall mean the audit report is recent enough for Commonwealth to rely upon it in meeting its reporting obligations.

12. SERVICE LOCATIONS

(a) **Services Locations**. The Services shall be provided from and to the Service Locations as detailed in *Schedule E* (Datacenter Locations). Contractor shall not (1) provide the Services from a location other than a Service Location or (2) use the Commonwealth Enterprise Data Center to provide services to a third party without Commonwealth's consent. Authorized representatives of Commonwealth, Commonwealth agents and agents of the Federal government shall be permitted access to any Services Location, subject to the terms of *Section 12(d)*.

(b) **Location of Performance.** Except where Contractor obtains the Commonwealth's prior written approval, Contractor shall perform all of the Services only from or at locations within the geographic boundaries of the continental United States. Any Commonwealth approval for the performance of Services outside of the continental United States shall be limited to the specific instance and scope of such written approval, including the types of Services and locations involved.

(c) Right to Audit and Inspect:

(1) The Contractor shall permit the Commonwealth (or a third-party provider selected by the Commonwealth) to perform an onsite inspection of the Contractor's Service Locations, infrastructure and security practices as reasonably requested by the Commonwealth, but no more than once per month.

(2) The Commonwealth shall have the right to request third-party audits and/or certifications related to each Serve Location's infrastructure and security, including penetration testing and vulnerability assessments. Any reports produced from these audits

and certifications will be provided to the Commonwealth for review at no cost.

(3) The Contractor shall provide the Commonwealth infrastructure and security specifications in written format for each Service Location as requested and at no cost to the Commonwealth.

(4) The Contractor shall provide the Commonwealth access to the performance records of the Contractor, as well as access to daily and weekly service quality statistics as requested and at no cost to the Commonwealth.

(d) Security Procedures

(1) As part of the Services, Contractor shall maintain and enforce environmental and physical security standards and procedures at each of the Contractor Services Locations and shall comply with environmental and physical security procedures as described in *Schedule F* (COPA Datacenter Statement of Work) and pursuant to the physical security and environmental chapters of the Commonwealth Computing Procedures Manual, which compliance will be confirmed by Contractor's SSAE 16 Type II audit report which will be delivered to the Commonwealth. If the Commonwealth requests any changes to environmental and security standards after the Effective Date and such changes would subject Contractor to material additional costs, those changes will be addressed through the Change Control Procedures. In addition, each Contractor Services Location must meet a minimum of Class C2 controlled access protection as defined in the Federal Department of Defense Trusted Computer System Evaluation (DOD 5200.28-STD).

(2) Each Commonwealth Agency's specific security requirements must be satisfied prior to the migration of its data or processing activities to any Contractor Services Location, including any facilities to be used to support Disaster Recovery. Contractor shall maintain a log recording all entry to any Contractor Services Location, which log shall at all times be subject to Commonwealth review and audit. All of Contractor's security procedures required under this Contract shall be subject to periodic review by Commonwealth, any Commonwealth Agency or any agency of the United States federal government directly or indirectly having any dealings with any Commonwealth Agency.

(3) Contractor, as part of the Services, shall address any concerns any such reviewing entity may have regarding those security procedures and, if Commonwealth is not the reviewing entity, shall promptly

inform Commonwealth of the expressed concerns and its plans to address the same. Contractor acknowledges that, because Commonwealth is a governmental entity, Commonwealth is subject to various federal and state statutory and regulatory confidentiality and security requirements, all of which will be binding upon Contractor during the Term. This Contract and the business relationship between Commonwealth and Contractor will be subject to review and approval by impacted Commonwealth Agencies and impacted federal agencies and other entities. At a minimum, Contractor will be required to comply with the Privacy Act of 1974, as amended (42 U.S.C.A. 2000, *et seq.*), the Drivers Privacy Protection Act, as amended (18 U.S.C.A. 2721, *et seq.*), the Tax Information Security Guidelines promulgated by the Internal Revenue Service; and various confidentiality regulations promulgated by the U.S. Department of Health and Human Services, all as though Contractor were a governmental entity. Contractor will also be required to comply with the Health Insurance Portability and Accountability Act of 1996, Pub.L. 104-191 (HIPAA) and the regulations promulgated related thereto (45 C.F.R. 160.101, *et seq.*) as a Business Associate as that term is defined by HIPAA according to the Business Associate Contract included as Appendix A (which Contract shall apply to covered portions of the Commonwealth as a hybrid entity as agencies direct, and which Contract shall govern only insofar as no other more stringent law otherwise applies to that data, and only insofar as the Contract does not conflict with more stringent provisions of this Amendment, where "more stringent" is defined as in 45 C.F.R. 160.202). If and only to the extent specifically required in writing by a federal agency, in order for Contractor to be granted operational access to Commonwealth Data in connection with its performance of the Services, Contractor may be appointed as an agent of Commonwealth for the limited purpose of having operational access to certain Commonwealth Data not as a contractor of Commonwealth, but as an agent of Commonwealth having an agent's fiduciary obligations to Commonwealth as its principal. Contractor shall deliver to Commonwealth written notice of any breach of such security standards and procedures of which Contractor then has knowledge, which notice shall be delivered as promptly as is reasonable under the circumstances. Any breach by Contractor of such security standards or procedures under this *Section 12(d)* shall be subject to the provisions of *Section 30* (Default). As more fully set forth in *Section 59* (Independent Capacity of Contractor), parties to this Contract agree that the Services performed by the Contractor under the terms of this Contract are performed as an independent contractor.

13. CONDITIONS OF CONTRACTOR'S OCCUPANCY OF COMMONWEALTH-PROVIDED REAL PROPERTY

(a) General

(1) The Contractor shall use and occupy the property provided by the Commonwealth (the "Enterprise Data Center") continuously as a data processing center and for related administrative uses. No other use shall be permitted. A summary of the Enterprise Data Center is attached to the RFP and incorporated herein as *Exhibit D.7* (EDC Summary and Requirements).

(2) The Contractor shall have the sole responsibility to comply with all federal, state, and municipal laws, ordinances and regulations in its use and occupancy of the property.

(3) The Contractor agrees to accept the property in an "as-is" condition. The Contractor agrees that the Commonwealth extends no warranty of any kind, express or implied, in regard to the property provided to the Contractor for its use.

(4) The Commonwealth is immune from the payment of real estate taxes. If any relevant taxing authority deems the use of the property by the Contractor to cause the property to become taxable, the Contractor shall have sole responsibility for the timely payment of any tax levied. Payment of such taxes may be temporarily withheld if Contractor is, in good faith, contesting the assessment or tax in a court of competent jurisdiction.

(5) The Contractor agrees that this Contract does not grant or otherwise convey any legal interest in the real property to the Contractor.

(b) Upkeep and Improvements

(1) The Contractor, at its sole cost and expense, is responsible for all maintenance, security and upkeep of the property under its control. The Contractor agrees to keep the property in substantially the same condition as it was upon the Effective Date of the Contract.

(2) Except for minor, non-structural alterations costing less than $10,000, any and all Contractor alterations and additions to the Property shall be performed in accordance with plans and specifications prepared by a Pennsylvania-licensed architect and/or engineer. The Contractor shall submit plans and specifications to the Office of Administration and the Department of General Services concurrently for approval prior to initiation of

construction. Any and all alterations to the Property shall be performed in a good and workmanlike manner, in conformity with all laws, rules, ordinances and other requirements of all governmental entities having jurisdiction. The Department of General Services and the Office of Administration reserve the right to specify standards that must be maintained for any alterations and additions to the Property.

(3) The Contractor is solely responsible for all costs and expenses associated with any Contractor alterations or additions.

(4) The Contractor shall fully comply with Pennsylvania law governing contracting for construction, alteration or repair of a public building, including but not limited to the Prevailing Wage Act, Steel Products Procurement Act, and the Uniform Construction Code.

(5) To the fullest extent permitted by law, all Contractor contracts for alterations and additions must include a "No-Lien" clause requiring that the Property be kept free from mechanics' or materialmens' liens and that the parties must file the necessary documentation in the appropriate public offices to effectuate waivers of contractors', mechanics' and materialmens' liens.

(6) Any and all alterations and additions made to the property by either the Contractor or the Commonwealth shall become part of the real estate and become the property of the Commonwealth.

(c) Utilities

Contractor shall have installed, at its sole cost, separate electric meters and distribution panels to support the raised floor compute space. The Contractor will be responsible to timely reimburse the Commonwealth for electricity consumed in the raised floor compute space.

(d) Reserve Account

Contractor shall establish a capital improvement fund ("Reserve Account") into which Contractor shall deposit monthly ($84,000) dollars. The Reserve Account shall be cumulative, intended for capital improvements or major repairs to the Enterprise Data Center and disbursements from which shall be made only upon mutual agreement of the Commonwealth and the Contractor. Any remaining sums in the Reserve Account at termination of this Agreement shall be paid or credited to the Commonwealth. In the event that at any time during the term of this Contract sums in the Reserve Account are insufficient to

cover the cost of an agreed-to capital improvement or major repair, Contractor shall be reimbursed by the Commonwealth in an amount equal to such insufficiency. Contractor shall provide the Commonwealth at least semi-annually a report of all activity in the Reserve Account.

(e) Termination Assistance

Contractor shall vacate the Enterprise Data Center and return to the Commonwealth, if not previously returned, any resources that are implicated by the relevant Assistance Event, as described in *Section 33* (Termination Assistance), and that are owned, leased or licensed by the Commonwealth or any Commonwealth Contractor, including the Commonwealth owned or leased Equipment, the Commonwealth Owned Materials and the Commonwealth licensed Materials, in condition at least as good as the condition of such facilities and resources when they were made available to Contractor, ordinary wear and tear excepted. Such facilities and resources shall be vacated and/or returned as of the later of the effective date of the relevant Assistance Event and the completion of the Termination Assistance requiring such facilities or resources.

14. TRANSITION

(a) **Transition.** Contractor shall perform the Transition Services, including provision of the deliverables described in the Detailed Transition Plan. Contractor shall accomplish the Transition in a transparent, seamless, orderly, and uninterrupted manner. Contractor's responsibilities with respect to the transition include:

(1) Transfer of the Services to Contractor and subsequent transition of the Services to realize any planned cost reductions and Service performance improvements in accordance with the Transition Plans agreed to by Commonwealth and including a number of Transition Milestones;

(2) Performing the transition without disruption to Commonwealth's operations;

(3) Assuming responsibility for all costs associated with the transition; and

(4) Otherwise performing such transition and migration tasks as are necessary to enable Contractor to provide the Services in accordance with the terms of the Contract, including the applicable Service Levels.

(b) **Transition Plan.** The preliminary Transition Plan is attached to this Contract as part of Contractor's Proposal. Contractor shall complete, and submit to

Commonwealth for review a final Detailed Transition Plan on or before the date set forth in *Schedule D* (Transition Milestones). If a Detailed Transition Plan submitted by Contractor is not acceptable to Commonwealth, Contractor will address and resolve any questions or concerns Commonwealth may have and will promptly incorporate any modifications, additions or deletions requested by Commonwealth. Contractor will revise and resubmit the Detailed Transition Plan until accepted by Commonwealth. Upon Commonwealth's acceptance, the Detailed Transition Plan shall automatically be incorporated into this Contract as *Schedule M* (Detailed Transition Plan) and shall supersede and replace all prior Transition Plans. The Detailed Transition Plan shall detail the specific activities to be performed by each Party, and, unless otherwise requested by Contractor and agreed to by Commonwealth in its sole discretion, shall be consistent in all material respects with any preliminary Transition Plan, including with respect to the activities, deliverables, Transition Milestones, and Transition Milestone Credits described therein. The Detailed Transition Plan may thereafter be amended as mutually agreed by the Parties.

The Parties recognize and agree that time is of the essence for a successful Transition and have designated certain actions and projects in the Detailed Transition Plan as Transition Milestones (“Transition Milestones”). Contractor shall achieve all such Transition Milestone by the date corresponding thereto in *Schedule D* (Transition Milestones). Without limiting the foregoing, the Detailed Transition Plan shall specify, among other things,

(i) the deliverables to be completed by Contractor,

(ii) the date(s) by which each such activity or deliverable is to be completed (the "Transition Milestones"),

(iii) a process and set of standards to which Contractor shall adhere in the performance of the Transition Services and that shall enable Commonwealth to determine whether Contractor has successfully completed the transition and the activities and deliverables associated with each Transition Milestone,

(iv) any transition responsibilities to be performed or transition resources to be provided by Commonwealth and/or Commonwealth Customers,

(v) any transition responsibilities to be performed or transition resources to be provided by another Commonwealth Contractor, and

(vi) a detailed description of the processes and procedures that Contractor will implement (and associated implementation schedules) to effect the seamless integration and coordination

of the Services with related services to be provided by other Commonwealth Contractors.

The Detailed Transition Plan shall identify any related documents contemplated by this Contract and/or required to effectuate the transition that shall be executed by either of the Parties.

(c) **Performance**. Contractor shall perform the Transition Services in accordance with the timetable and the Transition Milestones set forth in the Transition Detailed Plan. Contractor shall assist Commonwealth in connection with Commonwealth's evaluation or testing of the deliverables set forth in the Detailed Transition Plan. Except as otherwise expressly stipulated in the Detailed Transition Plan, Contractor shall perform the Transition Services in a manner that shall not (i) disrupt or have an unnecessary adverse impact on the activities or operations of Commonwealth or the Commonwealth Customers, (ii) degrade the Services then being received by Commonwealth or the Commonwealth Customers or (iii) disrupt or interfere with the ability of Commonwealth or the Commonwealth Customers to obtain the full benefit of the Services. In Contractor's performance and completion of Transition Services, no functionality of Commonwealth's then current business operations or environment will be discontinued until Contractor demonstrates to Commonwealth's reasonable satisfaction that the affected processes and operations have been successfully migrated to Contractor's target environment and are functioning properly in that environment.

Without limiting its obligations or responsibilities, prior to undertaking any transition activity, Contractor shall discuss with Commonwealth and the relevant Commonwealth Customers all known Commonwealth and Commonwealth Customer-specific material risks and shall not proceed with such activity until Commonwealth is reasonably satisfied with the plans with regard to such risks (provided that, neither Contractor's disclosure of any such risks to Commonwealth, nor Commonwealth's acquiescence in Contractor's plans, shall operate or be construed as limiting Contractor's responsibility under this Contract). Contractor will, at Commonwealth's request, participate in transition meetings with other Commonwealth Contractors. Commonwealth reserves the right to monitor, test and otherwise observe and participate in transition. Contractor will notify Commonwealth without delay if any Commonwealth monitoring, testing or participation has caused (or Contractor expects it to cause) a problem or delay in transition and work with Commonwealth to prevent or circumvent the problem or delay.

(d) **Reports**. Beginning on the Effective Date, Contractor shall meet at least weekly with the Commonwealth to report on Contractor's progress in performing its responsibilities and meeting the timetable and Transition Milestones set forth in the Detailed Transition Plan. Contractor also shall provide written reports to Commonwealth at least weekly regarding such

matters, and shall provide oral reports more frequently if requested by Commonwealth. Promptly upon receiving any information indicating that Contractor may not perform its responsibilities or meet the timetable or Transition Milestones set forth in the Detailed Transition Plan, Contractor shall notify Commonwealth of such delays and shall identify for Commonwealth's consideration and approval specific measures to address such delays and mitigate the risks associated therewith.

(e) **Notification of Problems**. Contractor shall provide to Commonwealth written notice of any acts or omissions (whether by Commonwealth, a Commonwealth Contractor, subcontractor or any third party), any failure to perform any of each such party's obligations under the Contract and any other events that may affect Contractor's performance of the Transition Services. Contractor shall provide such written notice within thirty (30) days after Contractor first knew or should have known of such acts, omissions, or failures or other events. Such written notice shall describe in reasonable detail such acts, omissions, failures or other events and the manner in which the foregoing may affect Contractor's performance.

(f) **Corrective Action Plan**. In the event that either (1) the Commonwealth determines that Contractor has failed or is reasonably likely to fail to deliver the Transition Services, or (2) Contractor has determined that it has failed or is reasonably likely to fail to deliver the Transition Services, then Commonwealth or Contractor, as applicable, will notify the other Party of such failure (a "Transition CAP Notice"). Concurrently with such notice, Contractor will:

(i) immediately take steps to mitigate any harmful effects of such failure, and

(ii) (promptly (and in any event as soon as reasonably practical) perform a Root Cause Analysis and prepare a Corrective Action Plan with respect to such failure, and

(iii) take all actions necessary to prevent its recurrence, including, without limitation, providing all additional resources necessary to resolve such failure.

If in Commonwealth's sole discretion any such Corrective Action Plan is not adequately addressing the failure, Contractor shall revise the Corrective Action Plan until it is accepted by the Commonwealth. In the event that Contractor is unable to complete the Transition Services on or before the dates specified in the Detailed Transition Plan (a "Transition Failure Event"), then Contractor will meet with Commonwealth to develop a workaround plan to address the Transition Failure Event, which plan may include, at Commonwealth's option, obtaining the services to workaround the Transition Failure Event from another Commonwealth contractor and/or the incumbent contractor. If the Commonwealth elects to obtain such services from another contractor and/or

the incumbent contractor, the Commonwealth will equitably adjust the Fees to reflect the reduction in Services being provided by Contractor.

(g) **Failure to Meet Transition Milestones**. Neither the Transition Services nor the activities and deliverables associated with individual Transition Milestones shall be deemed complete until Commonwealth's acceptance of such activities and deliverables. If Contractor fails to meet a Transition Milestone, Contractor shall pay Commonwealth the applicable Milestone Credits specified in *Schedule D* (Transition Milestones) or the Detailed Transition Plan that are associated with such Transition Services.

(h) **Additional Remedies**. In the event that Contractor fails to identify and resolve any problems that may impede or delay the timely completion of each task in the Detailed Transition Plan, without prejudice to Commonwealth's other rights and remedies under the Contract or at law or equity, (i) Contractor will provide, at its sole cost and expense, all such additional resources as are necessary to identify and resolve any problems that may impede or delay the timely completion of each task in the Detailed Transition Plan, and (ii) Commonwealth may equitably reduce the Fees set forth in *Schedule I* (Offeror Pricing Forms) in an amount reasonably estimated by Commonwealth to account for the Services that Commonwealth is not receiving or did not receive.

(i) **Suspension or Delay of Transition Services.** Commonwealth reserves the right, in its sole discretion, to suspend or delay the performance of the Transition Services and/or the transition of all or any part of the Services. If Commonwealth elects to exercise this right and Commonwealth's decision is based in material part on concerns about Contractor's ability to perform material aspects of the Transition Services or Contractor's failure to perform its obligations under this Contract, the Commonwealth shall not incur any additional Fees or reimbursable expenses in connection with such decision, provided that Commonwealth shall work in good faith with Contractor to minimize the period of any such suspension or delay.

15. DISASTER RECOVERY AND BUSINESS CONTINUITY

(a) Disaster Recovery Plan.

(1) Jointly with the Commonwealth, Contractor shall at least annually review and update the disaster recovery plan, it being understood and agreed that the parties will work together and cooperate in good faith on any such review or updated of the disaster recovery plans.

(2) With the Commonwealth's support as specified in the disaster recovery plan, Contractor shall every six (6) months test the operability of the disaster recovery plan then in effect.

(i) Within fifteen (15) business days of completion of a disaster recovery test, Contractor will certify to Commonwealth that the disaster recovery plan was fully, timely and successfully implemented, or, if the disaster recovery plan was not fully, timely and successfully implemented, report all deficiencies (including root cause analysis) and corrective actions, and certify that such corrective actions addressed all deficiencies; and

(ii) Annually and at additional times at the request of Commonwealth, Contractor will certify to Commonwealth that that any applicable third-party business recovery center agreement remains in full force and effect without any default, including payment, thereunder by any party thereto, and that Commonwealth is entitled, pursuant to the terms of the business recovery center agreement, to assume that agreement upon the expiration or termination of this Contract.

(b) Disaster Recovery Event.

(1) As part of the Services, Contractor shall have responsibility for executing the disaster recovery plan relating to the Services as described in *Schedule F* (COPA Datacenter Statement of Work). Contractor shall immediately provide Commonwealth with notice of the occurrence of any disaster affecting the provision or receipt of all or any material portion of the Services and implement the disaster recovery plan then in effect. Contractor agrees to utilize the disaster recovery planning methodology software then utilized by Commonwealth in connection with activities contemplated under this *Section 15* (Disaster Recovery and Business Continuity).

(2) Contractor shall reinstitute the Services as promptly as possible but in any event within subscribed restitution hours, as set forth in the disaster recovery plan then in effect, after the occurrence of a disaster. If the Services are not fully reinstituted within the subscribed restitution hours the Commonwealth shall have the right to terminate this Contract for critical failure pursuant to the provisions of *Section 32(c)*, and Contractor shall, prior to or at the expiration of the applicable restitution period, deliver to Commonwealth a written report detailing the cause of the disaster, Contractor's plans to reinstitute the Services and its anticipated schedule to do so. Thereafter, Contractor and Commonwealth shall develop a plan to reinstitute the Services as promptly as is possible under the circumstances, with Contractor making such reinstitution its highest priority. Contractor shall prepare and deliver to Commonwealth

updated reports such that Commonwealth shall at all times be fully informed as to the status of Contractor's efforts and anticipated schedule to reinstitute the Services. In the event that any Contractor Machines are required to be replaced as a result of the disaster, Contractor shall replace such Contractor Machines with current or Improved Technology to the extent then available and compatible with the associated application(s). Any Contractor obligations to implement a disaster recovery plan set forth in this paragraph can be triggered by a notice of disaster provided to Contractor by Commonwealth.

16. PRIME CONTRACTOR RESPONSIBILITIES

The Contractor will be responsible for all Services in this Contract whether or not Contractor provides them directly. Further, the Contractor is the sole point of contact with regard to all contractual matters, including payment of any and all charges resulting from the Contract.

17. KEY POSITIONS/CONTRACTOR PERSONNEL

(a) **Contractor Project Manager and Transition Project Manager**.

(1) Upon the Effective Date, the Contractor shall appoint the Contractor Project Manager identified in its proposal, who on a full-time basis shall be in charge of implementing the Services. Contractor shall replace the Contractor Project Manager only when required or permitted pursuant to *Section 17(c)*. The Contractor Project Manager shall at all times be subject to Commonwealth's continuing approval.

(2) Upon the Effective Date he Contractor shall appoint the Transition Project Manager identified in its proposal, who will have the responsibilities set forth in *Schedule F* (COPA Datacenter Statement of Work). Contractor shall replace the Transition Project Manager only when required or permitted pursuant to *Section 17(c)*. The Contractor Project Manager shall at all times be subject to Commonwealth's continuing approval.

(b) **Key Positions**. The positions identified in *Schedule G* (Staffing Plan and Key Positions), are designated by Commonwealth and Contractor as key positions within the Contractor's Personnel. All of the Key Employees shall be dedicated to the Commonwealth account on a full-time basis. The Commonwealth Project Manager and the Contractor Project Manager shall meet once every Contract Year thereafter or upon the request of either the Commonwealth Project Manager or the Contractor Project Manager to update the list of the Key Employees. Each Key Employee shall at all times be subject to Commonwealth's continuing approval. Except for a replacement or reassignment of a Key Employee pursuant to *Section 17(c)*, Contractor shall not reassign or replace any Key Employee. As

more fully set forth in *Section 59* (Independent Capacity of Contractor), parties to this Contract agree that the Services performed by the Contractor under the terms of this Contract are performed as an independent contractor.

(c) **Reassignment Waivers**. Contractor shall not reassign or replace the Contractor Project Manager or any Contractor Services Location Manager during the first eighteen (18) months of his or her assignment as the Contractor Project Manager or a Contractor Services Location Manager unless Commonwealth consents to such reassignment or replacement or unless the individual (1) voluntarily resigns from Contractor, (2) is dismissed by Contractor for cause, or (3) is unable to work due to his or her death or disability. In addition, Contractor shall, in connection with its assignment of other Key Employees, use commercially reasonable efforts to assure the greatest degree of continuity possible among such Key Employees. If, in any instance, Commonwealth withholds or withdraws its approval of any employee or representative of Contractor for the performance of the Services, including without limitation, the Contractor Project Manager, any Contractor Services Location Manager or any other Key Employee, Contractor promptly shall reassign and replace such employee or representative.

(d) **Subcontractors**. The Contractor may subcontract any portion of the Services described in this Contract to third parties selected by Contractor and approved in writing by the Commonwealth, which approval will not be unreasonably withheld. Approved Subcontractors will be listed on *Schedule L* (Approved Subcontractors). Notwithstanding the above, if Contractor has disclosed the identity of Subcontractor(s) together with the scope of work to be subcontracted in the Contractor's Proposal, award of the Contract is deemed approval of all named Subcontractors for the specified scope of work and a separate approval is not required. The existence of any subcontract shall not change the obligations of Contractor to the Commonwealth under this Contract. Upon written request of the Commonwealth, the Contractor shall promptly provide the Commonwealth with a copy of any specified subcontract agreement between the Contractor and the subcontractor. If Commonwealth reasonably determines that a subcontractor should no longer be retained by Contractor due to material performance deficiencies arising from the subcontractor's performance, the Commonwealth reserves the right, for good cause, to require that the Contractor remove a subcontractor from the project. As more fully set forth in *Section 59* (Independent Capacity of Contractor), parties to this Contract agree that the Services performed by the Contractor under the terms of this Contract are performed as an independent contractor.

(e) **Managerial Control**. Subject to the other provisions of this Contract, including without limitation, provisions regarding security procedures and government security clearance and the other provisions of this *Section 17* (Key Positions/Contractor Personnel) Contractor shall have complete managerial control over its employees, and Contractor may dismiss, promote, replace or reassign a member of the Contractor Personnel; provided, however, that unless

otherwise agreed to by Commonwealth, Contractor shall deliver a notice to Commonwealth before or immediately after dismissing any member of the Contractor's Personnel. In addition, Contractor shall deliver to Commonwealth written notice of any criminal activities undertaken by, or alleged to have been undertaken by, any member of the Contractor Personnel and of which Contractor then has knowledge, which notice shall be delivered as promptly as is reasonable under the circumstances, and Contractor will cooperate fully with any investigation undertaken by or through Commonwealth in respect of such actual or alleged criminal activities.

(f) **Conduct of Contractor Personnel**. While at the Commonwealth Services Locations and the Contractor Services locations, Contractor's personnel, subcontractors and agents (1) shall comply with all lawful requests, rules and regulations of Commonwealth regarding personal and professional conduct (including the wearing of a particular uniform, identification badge or personal protective equipment and adhering to security regulations and general safety practices or procedures) and (2) otherwise shall conduct themselves in a businesslike manner.

(g) **Unsatisfactory Conduct**. If the Commonwealth determines in its sole discretion that a particular Contractor employee or subcontractor is not conducting himself or herself in an appropriate manner, Commonwealth may provide Contractor with notice of such conduct. Upon receipt of such notice, Contractor shall promptly investigate the matter and take appropriate action, which may include (1) removing the offending individual from the project and replacing him or her with a similarly qualified individual or (2) taking other appropriate disciplinary action to prevent a reoccurrence. In the event there are repeat violations of this *Section 17(g)* by a particular Contractor employee, contractor or subcontractor, Contractor shall promptly remove him or her from the project as set forth above.

(h) **Confidentiality.** Contractor shall:

(1) Cause each Contractor Personnel to maintain and enforce the confidentiality provisions of the Contract both during and after their assignment to the Commonwealth account; and

(2) Enter into, or shall have entered into, an agreement with each Contractor Personnel member which assigns, transfers and conveys to Contractor all of such employee's right, title and interest in and to any materials created pursuant to the Contract, including all rights of patent, copyright, trade secret or other proprietary rights in and to such materials.

18. THIRD PARTY SERVICES

(a) Commonwealth shall have the right, in its sole discretion, to contract with any number of third parties to perform Services which would otherwise fall within the terms of this Contract. In the event Commonwealth contracts with a third party to perform any service on behalf of or for Commonwealth, Contractor, as part of the Services, shall cooperate with Commonwealth and such third party to the extent reasonably required by Commonwealth, including provision of (i) existing written requirements, standards and policies for systems operations so that the enhancements or developments of such third party may be operated by, and will be compatible with the operations of, Contractor, (ii) assistance and support services to such third party, and (iii) such access to the Systems as may be reasonably required by such third party (subject to all security standards, licenses, confidentiality restrictions and other standards and procedures then in effect at each of the Services Locations) to develop, test and deploy the service contracted for by Commonwealth. In addition thereto, Contractor shall not commit or permit any act which will unduly interfere with the performance of work by Commonwealth employees or any such third party, and Commonwealth will not commit or permit any act which will interfere with Contractor's performance of the Services. All additional out-of-scope support costs, excluding attorney fees, incurred by Contractor as a result of a Commonwealth contract with a third party will be handled in accordance with the Change Control Procedures.

(b) Throughout the Term, but not more than once every six months, Commonwealth may request that Contractor work together with Commonwealth and/or third parties to identify ways to achieve reductions in the cost of Service delivery and corresponding reductions in the price(s) quoted in the Contract. If so requested by Commonwealth, Contractor will, at its own expense, promptly prepare a detailed proposal identifying all viable means of achieving the desired reductions without (to the extent practically possible) adversely impacting business objectives or requirements identified by Commonwealth. Commonwealth shall not be obligated to accept or implement any such proposal.

19. COMPENSATION

In consideration of Contractor providing the Services, subject to the terms of this Contract, Commonwealth shall pay to Contractor the Fees as set out at *Schedule I* (Offeror Pricing Forms). All items shall be performed within the time period(s) specified in the Contract. The Contractor shall be compensated only for items supplied and performed to the satisfaction of the Commonwealth.

20. FEES

(a) **Service Fees**. In consideration of Contractor providing the Services, subject to the terms of this Contract, Commonwealth shall pay to Contractor the Fees pursuant to *Schedule I* (Offeror Pricing Forms).

(b) **Cost of Living Adjustment.** The Fees shall not be subject to any cost of living or inflationary adjustment or any other adjustment based on Contractor's costs to provide the Services.

(c) **Expenses**. Except as expressly provided otherwise in this Contract, expenses of Contractor relating to the Services are included in the Fees, and no such expenses or other costs or fees shall be reimbursed by Commonwealth unless agreed to by Commonwealth in writing. The Contractor shall not be allowed or paid travel or per diem expenses unless agreed to by Commonwealth in writing.

(d) **Pro-ration**. All periodic Fees or charges under this Contract are to be computed on a calendar month basis and shall be prorated on a per diem basis for any partial month.

(e) **Unused Credits**. Any unused credits against future payments owed to either party by the other pursuant to this Contract shall be paid to the applicable party within forty-five (45) days after the expiration or termination for any reason of Contractor's obligation to provide the Services or of this Contract. This *Section 20(e)* shall survive the expiration or any termination of this Contract.

(f) **Pricing Protection**. Notwithstanding anything to the contrary elsewhere in this Contract, the Fees shall in no event and at no time during the Term exceed Contractor's then lowest charges for such services to Contractor's state governmental customers generally receiving comparable goods and services at comparable volumes and upon material terms and conditions comparable to those contained in this Contract and pursuant to an outsourcing agreement dated after the Effective Date. Upon Commonwealth's request from time to time, and in any event on each anniversary of the Effective Date, Contractor shall advise Commonwealth in writing that this *Section 20(f)*has not been contradicted by any transaction entered into by Contractor on or after the Effective Date. If Contractor is unable to provide such written notice because of a transaction entered into by Contractor contradicting this *Section 20(f)*, Contractor shall offer to Commonwealth an adjustment to the Fees to correct such contradiction.

21. PAYMENT SCHEDULE AND INVOICES

(a) **Service Fees**. On or before the 15th day of each calendar month of the Term, Contractor shall provide Commonwealth with a single invoice for the Service Fees. Each such invoice shall include the Fees, if applicable, for the then current month, as well as any Service Level Credits then payable by Contractor or refundable by Commonwealth, or other reimbursable charges to Commonwealth for Services actually rendered prior to the date of such invoice.

(b) **Detailed Invoices.** Contractor shall provide on the monthly invoices varying degrees of detail (e.g., per agency, end-user, department, project, site) as specified in *Schedule H* (Commonwealth Computing Procedures Manual). The Detailed Invoice will be delivered both in an electronic format compatible with the

Commonwealth's Invoice Processing System and a summary Invoice will be delivered for Management and Budgeting Purposes.

(c) **Time of Payment**. Any sum due Contractor pursuant to any such invoice shall be due and payable on the last business day of the calendar month following the calendar month during which such invoice was delivered to Commonwealth. (e.g., an invoice delivered to Commonwealth on July 15, 2015 will be due and payable on August 31, 2015, the last business day of August, 2015.) In the event any invoices remain unpaid after such due date, the Commonwealth may pay interest as determined by the Secretary of Budget in accordance with Act No. 266 of 1982 and regulations promulgated pursuant thereto. Contractor shall continue to provide the Services even in the event payment is delayed or is not made in timely fashion.

(d) **Fee Dispute**. During the pendency of a dispute between Commonwealth and Contractor pursuant to which Commonwealth, in good faith, believes it is entitled to withhold, and does withhold, payment, Contractor shall continue to fully provide the Services and otherwise fully perform its obligations under this Contract.

22. INSPECTION AND ACCEPTANCE

(a) Acceptance of Services related to transition will occur in accordance with the Acceptance Criteria set out in *Schedule D* (Transition Milestones) and the Detailed Transition Plan.

(b) Acceptance of Services other than those related to transition will occur in accordance with the Commonwealth Computing Procedures Manual.

(c) If the Services are in compliance with the specifications, then the Commonwealth shall provide the Contractor with Commonwealth's written conditional acceptance of the Services. If the Services are not in compliance with the specifications, then the Commonwealth shall provide the Contractor with Commonwealth's written rejection of the Service. Payment will only be made if the Commonwealth has accepted the Service through written acceptance.

(d) If the Services do not meet an accessibility standard as set out in ITB-ACC001, the Contractor must provide written justification for its failure to meet the standard. The justification must provide specific details as to why the standard has not been met. The Commonwealth may either waive the requirement as not applicable to the Commonwealth's business requirements or require that the Contractor provide an acceptable alternative. Any Commonwealth waiver of the requirement must be in writing.

(e) Unless otherwise set forth in the Commonwealth Computing Procedures Manual (*Schedule H*), upon the Contractor's receipt of the Commonwealth's written notice of rejection, which must identify the reasons for the failure of the Services to comply with the Contract, the Contractor shall have fifteen (15) business days, or such other time as the Commonwealth and Contractor may agree is reasonable, within which to correct all such failures, and resubmit the corrected Services, certifying to the Commonwealth, in writing, that the failures have been corrected, and that the Services have been brought into compliance with the Contract. Upon receipt of such corrected and resubmitted Service and certification, the Commonwealth shall have thirty (30) business days to test the corrected Service to confirm that it is in compliance with the Contract. If the corrected Service is in compliance with the Contract, then the Commonwealth shall provide the Contractor with Commonwealth's acceptance of the Service.

(f) If, in the opinion of the Commonwealth, the corrected Service still contains material failures, the Commonwealth may either:

(1) Repeat the procedure set forth above; or

(2) Terminate the Contract in accordance with *Section 32* (Termination).

23. SERVICE LEVELS

(a) The Contractor shall comply with the procedures and requirements of *Schedule J.1* (Service Level Management), *Schedule J.2* (Datacenter Service Level Matrix), and *Schedule J.3* (Datacenter SLA Definitions) during the term of the Contract.

(b) All Services without expressly defined Service Levels must be performed at least to the same degree of accuracy, completeness, efficiency, quality and timeliness as is provided by well-managed suppliers providing services similar to the Services, so long as such performance is operationally reasonable. For where there are expressly defined Service Levels, or where performance can be reasonably reported, Contractor will measure and report its performance against these standards on at least a monthly basis, except as may otherwise be agreed between the Parties in respect of Services performed less frequently than monthly.

(c) The Commonwealth's acceptance of any Service Level Credit shall not bar or impair Commonwealth's rights and remedies in respect of the failure or root cause as set forth elsewhere in this Contract, including without limitation claims for liquidated damages, injunctive relief and termination rights, provided however, Service level Credits paid would be credited against any such claim for damages.

(d) The Commonwealth's acceptance of any Service Level credit shall not bar or impair Commonwealth's rights and remedies in respect of the failure or root cause as set forth elsewhere in this Contract, including without limitation claims for damages, injunctive relief and termination rights, provided however, Service level credits paid would be credited against any such claim for damages.

24. LIQUIDATED DAMAGES

(a) By accepting this Contract, the Contractor agrees to the delivery requirements of this Contract. If a Contract schedule is not met, including Transition Milestones set out in Transition Plan, the delay will interfere with the Commonwealth's program. In the event of any such delay, it would be impractical and extremely difficult to establish the actual damage for which the Contractor is the material cause. The Commonwealth and the Contractor therefore agree that, in the event of any such delay the amount of damage shall be the amount set forth in this *Section 24* and agree that the Contractor shall pay such amount as liquidated damages, not as a penalty.

(b) The amount of liquidated damages for failure to meet Transition Milestones is set forth in *Schedule D* (Transition Milestones).

(c) If, *Schedule D* (Transition Milestones) indicates that Contractor may earn back liquidated damages, then Contractor shall have the time specified in *Schedule D* (Transition Milestones), as indicated, to meet the Acceptance Criteria for the Transition Milestone and earn back the Milestone Credit. If Contractor fails to meet the Acceptance Criteria within 30 days following the Milestone Due Date or, if an earn back period is specified, then 30 days following the end of the specified earn back period, the Commonwealth, at no additional expense and at its option, may either:

(1) Immediately terminate the Contract and all software, documentation, reports, Developed Materials and any other materials provided for or created for the Commonwealth as a result of this Contract shall be given to the Commonwealth, and the Commonwealth shall be entitled to its remedies under Subsection 24(c); or

(2) Order the Contractor to continue with no decrease in effort until the work is completed in a manner acceptable to the Commonwealth or until the Commonwealth terminates the Contract. If the Contract is continued, the liquidated damages will also continue until the work is completed.

(d) Liquidated damages shall be paid by the Contractor and collected by the Commonwealth by deducting them from the invoices submitted under this Contract or any other contract Contractor has with the Commonwealth, by collecting them through the performance security, if any, or by billing the Contractor as a separate item.

(e) To the extent that the delay is caused by the Commonwealth, as described in *Schedule D* (Transition Milestones), no liquidated damages will be applied.

(f) Contractor shall not be liable for liquidated damages if the delay to the Contract arises out of causes beyond the control of and without the fault or negligence of the Contractor and/or its subcontractors. Such causes may include, but are not limited to, acts of God or of the public enemy, fires, floods, epidemics, quarantine restrictions, strikes, work stoppages, freight embargoes, acts of terrorism, and unusually severe weather; but in every case, the delay must be beyond the control of, and without the fault or negligence of, the Contractor and/or its subcontractors. The Contractor shall notify the Commonwealth immediately in writing of its inability to perform because of a cause beyond the control of the Contractor.

(g) If the delays are caused by the default of a Subcontractor, and if such default arises out of causes beyond the control of both the Contractor and Subcontractor, and without their fault or negligence, the Contractor shall not be liable for liquidated damages for delays, unless the supplies or services to be furnished by the Subcontractor were obtainable from other sources in sufficient time to permit the Contractor to meet the required performance schedule.

25. CONTINUOUS IMPROVEMENT AND BENCHMARKING

(a) **Benchmark Overview**. Prior to the expiration of the second anniversary of the Effective Date, Commonwealth and Contractor shall establish the details of the Benchmarking Process intended to ensure that Contractor provides Commonwealth with technology and Services Levels equal to or greater than other organizations receiving similar services. The parties acknowledge and agree that the benchmarking process is intended to assist Commonwealth in making decisions necessary to balance the desire for then current technology against the cost and uncertain performance of newly evolving technology.

(b) **Benchmarker**. The Benchmark shall be conducted by a Benchmarker selected by the Commonwealth, subject to Contractor's approval thereof, in writing, such approval not to be unreasonably withheld, delayed or conditioned. The fees and expenses charged by the Benchmarker shall be paid by Commonwealth. Contractor shall at its expense cooperate with and assist the Benchmarker and any other third parties involved in the Benchmarking process, including meeting with Commonwealth and the Benchmarker before and throughout the Benchmarking Process and providing data relating to the provision of the Services, as requested by Commonwealth or the Benchmarker.

(c) **Benchmark**. If Commonwealth undertakes the Benchmarking, Commonwealth and Contractor, in good faith, shall attempt to agree upon the period during which the Benchmarking shall be conducted. If the parties are unable to so agree,

Commonwealth shall specify the relevant period, subject to Contractor's approval thereof, in writing, such approval not to be unreasonably withheld, delayed or conditioned.

(d) **Benchmark Information**. Commonwealth and Contractor shall jointly determine the Benchmark Information with appropriate input from the Benchmarker. Commonwealth and Contractor shall (1) review the Benchmark Information, and (2) schedule a meeting to address any issues either party may have with the Benchmark Information. Contractor shall provide the Benchmark Information at no additional cost to Commonwealth; provided, however, that if Commonwealth wishes the Benchmarker to use information which Contractor does not otherwise have access to in the course of its business, Commonwealth shall provide such information at its own cost and Contractor may use such information but, unless Commonwealth expressly agrees otherwise in writing, only in connection with providing the Services.

(e) **Benchmarking Results**. Within thirty (30) days after the completion of Benchmarking, the Benchmarker shall deliver the Benchmark Results to the Commonwealth Project Manager and the Contractor Project Manager for distribution to the members of the Management Committee.

(f) **Benchmark Results Review Period and Adjustments**. The members of the Management Committee shall utilize the Benchmark Review Period to review such Benchmark Results, and the Management Committee shall meet during the Benchmark Review Period to collectively assess the Benchmark Results.

(g) **Disputes of Benchmark Results**. Either Commonwealth or Contractor may in good faith dispute the Benchmark Results, in writing, prior to the expiration of the Benchmark Review Period. Any such notice of dispute issued by either party shall include a description of the nature of such dispute in sufficient detail so as to enable the Benchmarker and the other party to assess the motive and merit of the dispute. Within ten (10) days after receipt of such notice, the parties shall cause the Benchmarker to issue a written response addressing the dispute, and if such dispute requires a change to any of the Benchmark Results, the Benchmarker shall be directed to issue revised Benchmark Results. Upon issuing such revised Benchmark Results, Commonwealth and Contractor, as applicable, shall have another Benchmark Review Period to review the revised Benchmark Results in accordance with *Section 25(f)*. In the event either party disputes the revised Benchmark Results within the second Benchmark Review Period or if the parties are unable to agree as to the need for revised Benchmark Results, original Benchmark Results or the revised Benchmark Results, as the case may be, shall be subject to the contract controversy procedures set forth in *Section 34* (Contract Controversies).

(h) **Benchmarking: Price Protection**. In addition to the Benchmarking provided for in this *Section 25* (Continuous Improvement and Benchmarking), no earlier

than sixty (60) days after the end of Year 2 of this Contract, and no more frequently than annually thereafter, the Commonwealth may engage a Benchmarker, in accordance with the provisions of this *Section 25* (Continuous Improvement and Benchmarking) for the purpose of assessing the extent to which the prices paid for the Services hereunder are comparable to prices of a comparable reference group of clients for Services. This Benchmarking Price Protection process shall be an objective measurement and comparison process utilizing baseline methods and industry standards. The parties acknowledge and agree that this Benchmarking Price Protection process is intended to assure the Commonwealth that pricing and pricing models employed in this engagement are consistent with the reference group throughout the later years of the Contract, as it may be extended or renewed.

(i) **Benchmark: Pricing Adjustments**. If the results of a Benchmarking Price Protection analysis, as reflected in written Benchmarking Results delivered to Contractor, reveal that amounts to be paid under the terms of the Contract for Services exceed by a factor of ten percent (10%) or more than the average of amounts paid by the reference group for comparable services (the "Market Rate"), the Commonwealth may elect to renegotiate those prices. When notified of the Commonwealth's intent to renegotiate the prices, the Contractor shall, as soon as practical following notification of the Commonwealth's intent, negotiate in good faith with Commonwealth for the adjustment and reduction of fees for the Services. If an agreement is reached for a pricing adjustment such agreement will be effective as of the date of delivery of the Benchmarking (Price Protection) Results. If the parties are unable to agree to a pricing adjustment within sixty (60) days after delivery of the Benchmarking (Price Protection) Results, the matter shall be submitted to the various dispute resolution procedures contained in *Section 34* (Contract Controversies) of the Contract. If the dispute resolution procedure results in a pricing adjustment, that adjustment will be effective as of the date of delivery of the Benchmarking (Price Protection) Results. In no event will Contractor increase the Fees as a result of any review pursuant to this *Section 25* (Continuous Improvement and Benchmarking).

(j) **Annual Best Practices Reviews.** Within thirty (30) days of each anniversary of the Effective Date, Contractor shall, in accordance with procedures agreed upon by the Commonwealth Project Manager and the Contractor Project Manager, identify for Commonwealth any best practices that have emerged (within Contractor’s organization or, to the knowledge of Contractor, within the processing services outsourcing market generally), that, if implemented by the Contractor would materially benefit the Commonwealth in terms of price reductions or performance improvement. If requested by Commonwealth, within sixty (60) days Contractor shall provide Commonwealth with proposals for the implementation of such best practices in a manner consistent with the Change Control Procedures of the Contract. If approved by Commonwealth,

Contractor shall implement such best practices on behalf of Commonwealth as expeditiously as possible.

26. GOVERNANCE

Provisions for the governance of this Contract and the Services delivered pursuant hereto are set forth in *Schedule B* (Governance) to this Contract.

27. CHANGE CONTROL

(a) Change Control Procedures. The following Change Control Procedures will apply if either party wishes to implement or have Contractor implement a Change. The requesting Party will forward to the other party a Change Order which will include the following:

(1) Project identification
(2) Originator's name and title
(3) The date of the Change Order
(4) A description of the proposed change
(5) The reason for the proposed change

For Contractor, all Change Orders must be directed to Contractor's Project Manager. For Commonwealth, all Change Orders must be directed to or originate from the Commonwealth Project Manager.

(1) For any Contractor-initiated Change Order, Commonwealth shall have the option of accepting or rejecting that Change Order.

(2) Contractor will assign a number to and log each Change Order.

(3) All Change Orders will be categorized by Commonwealth as Priority 1 (urgent), Priority 2 (ordinary) or Priority 3 (low).

(4) Contractor will make reasonable efforts to investigate the impact of the Change Order on the Fees, timetable, specifications, Services, Service Levels, terms and conditions and, the relative obligations of the parties under this Contract and the (the "Impact Study") in accordance with a schedule that reflects the applicable priority category.

(5) Contractor will inform Commonwealth if there will be any charges for Contractor Services in conducting the Impact Study and Commonwealth will decide whether Contractor should conduct the Impact Study. Contractor shall be entitled hereunder to charge Commonwealth only for those expenses incurred by Contractor in connection with the conduct of the Impact Study that are (i) Contractor's out-of-pocket expenses paid by Contractor to third parties

(other than Contractor's or any Contractor's Agent's employees) for expertise not otherwise possessed by or available to Contractor or (ii) for employees of Contractor or any Contractor Agent not theretofore engaged in the provision of the Services. In order for any of the foregoing expenses to be reimbursable to Contractor, Contractor must first provide an estimate thereof to Commonwealth and obtain from Commonwealth its prior written approval thereof. If Contractor provides any such estimate and Commonwealth does not approve the estimated expenses, Contractor shall not be obligated to proceed with the Impact Study. In all cases, Contractor shall make a good faith effort to maximize its use of its employees and the employees of Contractors Agents then engaged in the provision of the Services to the extent Contractor can do so without adversely affecting its ability to provide the Services in accordance with the Services Levels. Any disputes between the parties regarding the validity, estimated amount or actual amount of any reimbursable expenses shall be subject to the dispute resolution provisions of *Section 34* (Contract Controversies).

(6) If both parties agree on the Impact Study and any necessary Changes to the Services, the relative obligations of the parties under this Contract, and the Fees, a Change Order will be issued to reflect the agreed to Changes.

(7) If the parties cannot agree upon the Impact Study or the resultant Changes to this Contract, any Commonwealth-initiated Change Order will nevertheless be implemented at Commonwealth's option and Contractor shall perform the Services, and either party may elect to have all outstanding related matters treated as a dispute between the parties under *Section 34* (Contract Controversies). During the pendency of any such dispute, Commonwealth shall pay to Contractor any undisputed amounts. Any changes to Service Levels which are required by the implementation of the Changes, will be reflected in the Change Order that is issued.

(b) All Changes shall be made pursuant to the Change Control Procedures. Contractor shall:

(1) schedule all Changes so as not to interrupt or unduly interfere with Commonwealth's operations,

(2) prepare and deliver to Commonwealth each month a ninety-day rolling schedule for ongoing proposed and approved and planned Changes,

(3) review and determine the cause of any failed Changes and deviations from scheduled Changes, and

(4) document and provide to the Management Committee and to the Commonwealth Project Manager, individually, same-day notification (which may be given orally provided that such oral notice is confirmed in writing to such persons within three (3) Commonwealth business days) of all changes performed on an emergency basis to maintain the continuity of the Services.

(c) Without limiting any other provision of this Contract, the following Schedules may be modified through the Change Control Procedures set forth in this *Section 27* (Change Control):

- Schedule C – Services Catalog
- Schedule E – Datacenter Locations
- Schedule G – Staffing Plan and Key Positions
- Schedule J.1 – Service Level Management
- Schedule J.2 – Datacenter Service Level Matrix
- Schedule J.3 – Datacenter SLA Definitions
- Schedule H – Commonwealth Computing Procedures Manual

28. NOTICE OF DELAYS

Whenever the Contractor encounters any difficulty that delays or threatens to delay the timely performance of this Contract (including actual or potential labor disputes), the Contractor shall immediately give notice thereof in writing to the Commonwealth stating all relevant information with respect thereto. Such notice shall not in any way constitute a basis for an extension of the delivery schedule or be construed as a waiver by the Commonwealth of any rights or remedies to which it is entitled by law or pursuant to provisions of this Contract. Failure to give such notice, however, may be grounds for denial of any request for an extension of the delivery schedule because of such delay. If an extension of the delivery schedule is granted, it will be done consistent with *Section 27*(Change Control).

29. NOTICE

Any written notice to any party under this Contract shall be deemed sufficient if delivered personally, or by facsimile, telecopy, electronic or digital transmission (provided such delivery is confirmed), or by a recognized overnight courier service (e.g., DHL, Federal Express, etc.), with confirmed receipt, or by certified or registered United States mail, postage prepaid, return receipt requested, sent to the address such party may designate by notice given pursuant to this section.

30. DEFAULT

(a) The Commonwealth may, subject to the provisions of *Section 28* (Notice of Delays), and in addition to its other rights under the Contract, declare the Contractor in default by written notice thereof to the Contractor, and terminate

for cause (as provided in *Section 32* (Termination) the whole or any part of this Contract and shall further have the right to seek damages from Contractor for any of the following reasons:

(1) Failure to begin work within the time specified in the Contract or as otherwise specified;

(2) Failure to successfully complete a Major Milestone in accordance with the agreed Transition or Transition Plans or to complete specified work in accordance with the Contract terms;

(3) Multiple failures over time of a single Service Level or a pattern of failure over time across multiple Service Levels (a Service Level Termination Event); this will include failures of Service Levels and Key Service Levels;

(4) Failure to make agreed-upon adjustments to the fees or Service Levels in accordance with the outcome of Benchmarking Procedures;

(5) Failure or refusal to remove material, or remove and replace any work rejected as defective or unsatisfactory;

(6) Abandonment or willful refusal to provide the Services or any part of the Services;

(7) Failure to perform its responsibilities under any Business Continuity or Disaster Recovery Plans, including such Business Continuity or Disaster Recovery Plans that apply to Contractor's own locations used for the delivery of the Services;

(8) Insolvency or bankruptcy;

(9) Assignment made for the benefit of creditors;

(10) Failure or refusal within 30 days after written notice by the Contracting Officer, of the Contractor to make payment or show cause why payment should not be made, of any amounts due for materials furnished, labor supplied or performed, for equipment rentals, or for utility services rendered;

(11) Failure to protect, to repair, or to make good any damage or injury to property as required under the terms of this Contract;

(12) Breaches of covenants, agreements, obligations, representations or warranties in the Contract occurring simultaneously or over time,

whether or not each such breach is a material breach, and whether or not each such breach was cured, that taken together constitute a material breach of the Contract after Contractor has been made aware of such breaches, on an individual basis. Regardless of any other provision in this Contract to the contrary no cure period is available to Contractor should the Commonwealth terminate under this *Section 30(a)(12)*;

(13) An act or omission of Contractor in the performance of this Contract, which is not otherwise explicitly required or permitted under this Contract, and which results in any Regulatory Entity notifying Commonwealth that it is subjecting the Commonwealth to a hearing or tribunal or withdrawing any license granted to Commonwealth or Contractor and such hearing, tribunal or withdrawal would have a material and adverse effect on Commonwealth's operations or business or the Services. Regardless of any other provision in this Contract the contrary no cure period is available to Contractor should the Commonwealth terminate under this *Section 30(a)(13)*;

(b) In the event that the Commonwealth terminates this Contract in whole or in part as provided in Subparagraph (a) above, the Commonwealth may procure, upon such terms and in such manner as it determines, services similar or identical to those so terminated, and the Contractor shall be liable to the Commonwealth for any reasonable excess costs for such similar or identical services included within the terminated part of the Contract.

(c) If the Contract is terminated as provided in Subparagraph (a) above, the Commonwealth, in addition to any other rights provided in this *Section 30* (Default), may require the Contractor to transfer title and deliver immediately to the Commonwealth in the manner and to the extent directed by the Commonwealth, such partially completed work, including, where applicable, reports, working papers and other documentation, as the Contractor has specifically produced or specifically acquired for the performance of such part of the Contract as has been terminated. Except as provided below, payment for completed work accepted by the Commonwealth shall be at the Contract price. Except as provided below, payment for partially completed work including, where applicable, reports and working papers, delivered to and accepted by the Commonwealth shall be in an amount agreed upon by the Contractor and the Commonwealth. The Commonwealth may withhold from amounts otherwise due the Contractor for such completed or partially completed work, such sum as the Commonwealth determines to be necessary to protect the Commonwealth against loss.

(d) The rights and remedies of the Commonwealth provided in this *Section 30* (Default) shall not be exclusive and are in addition to any other rights and remedies provided by law or under this Contract.

(e) The Commonwealth's failure to exercise any rights or remedies provided in this *Section 30* (Default) shall not be construed to be a waiver by the Commonwealth of its rights and remedies in regard to the event of default or any succeeding event of default.

(f) Following exhaustion of the Contractor's administrative remedies as set forth in *Section 34* (Contract Controversies), the Contractor's exclusive remedy shall be to seek damages in the Board of Claims.

31. STEP-IN RIGHTS

(a) In the event that Contractor is failing to deliver all or part of the Services, the Commonwealth shall give the Contractor notice of the failure. The Contractor shall have fifteen (15) days to provide the Commonwealth with a correction plan. If the correction plan is not received within fifteen (15) days or the failure is not corrected within thirty (30) days of the notice provided under this paragraph, Commonwealth may assign Commonwealth staff or third parties to step-in and perform failing elements of the Services, to the extent those Services are listed below, until such time as Contractor can demonstrate the ability to resume provision of such Services. Provided, however, that if in the Commonwealth's sole discretion the failure creates an emergency, no notice is required for the Commonwealth to exercise its rights under this paragraph.

(1) Co-location services;
(2) Management of Commonwealth owned equipment located within the Enterprise Data Center;
(3) Network Connectivity between the Commonwealth and the Contractor's datacenter(s); and
(4) Disaster Recovery Services.

(b) All costs associated with the exercise of such step-in rights shall be borne by Contractor.

(c) Commonwealth's exercise of its step-in rights shall not constitute a waiver by Commonwealth of any termination rights or rights to pursue a claim for damages arising out of the failure that led to the step-in rights being exercised.

32. TERMINATION

(a) For Convenience

(1) The Commonwealth may terminate this Contract without cause by giving Contractor thirty (30) calendar days prior written notice (Notice of Termination) whenever the Commonwealth shall determine that such termination is in the best interest of the Commonwealth (Termination for Convenience). Any such termination shall be effected by delivery to the Contractor of a Notice of Termination specifying the extent to which performance under this Contract is terminated either in whole or in part and the date on which such termination becomes effective.

In the event of termination for convenience, Contractor shall receive a termination for convenience fee ("Termination for Convenience Fee").

The Termination for Convenience Fee shall equal the applicable amount set out in Tab #6 of Schedule I (Termination Fees) minus the value of all Services performed by the Contractor consistent with the terms of the Contract prior to the effective date of termination.

In no event shall the Contractor be paid for any loss of anticipated profit (by the Contractor or any Subcontractor), loss of use of money, or administrative or overhead costs.

Failure to agree on any termination costs shall be a dispute handled in accordance with *Section 34* (Contract Controversies) of this Contract.

(2) The Contractor shall cease Services as of the date set forth in the Notice of Termination, and shall be paid only for such Services as have already been satisfactorily rendered up to and including the termination date set forth in said notice, or as may be otherwise provided for in said Notice of Termination, and for such services performed during the thirty (30) calendar day notice period, if such services are requested by the Commonwealth, for the collection, assembling, and transmitting to the Commonwealth of at least all materials, manuals, magnetic media, studies, drawings, computations, maps, supplies, and survey notes including field books, which were obtained, prepared, or developed as part of the Services required under this Contract.

(3) The above shall not be deemed to limit the Commonwealth's right to terminate this Contract for any reason as permitted by the other provisions of this Contract, or under applicable law.

(b) Non-Appropriation

Any payment obligation or portion thereof of the Commonwealth created by this Contract is conditioned upon the availability and appropriation of funds. When funds (state or federal) are not appropriated or otherwise made available to support continuation of performance in a subsequent fiscal year period, the

Commonwealth shall have the right to terminate the Contract. The Contractor shall be reimbursed in the same manner as that described in this section related to Termination for Convenience to the extent that appropriated funds are available.

(c) Default

The Commonwealth may, in addition to its other rights under this Contract, terminate this Contract in whole or in part by providing written notice of default to the Contractor if the Contractor materially fails to perform its obligations under the Contract and does not cure such failure within thirty (30) days or, if a cure within such period is not practical, commence a good faith effort to cure such failure to perform within the specified period or such longer period as the Commonwealth may specify in the written notice specifying such failure, and diligently and continuously proceed to complete the cure. The Contracting Officer shall provide any notice of default or written cure notice for Contract terminations.

(1) Subject to *Section 36* (Limitation of Liability) of this Contract, in the event the Commonwealth terminates this Contract in whole or in part as provided in this Subsection 32(c), the Commonwealth may procure services similar to those so terminated, and the Contractor, in addition to liability for any liquidated damages, shall be liable to the Commonwealth for the difference between the Contract price for the terminated portion of the services and the actual and reasonable cost (but in no event greater than the fair market value) of producing substitute equivalent services for the terminated services, provided that the Contractor shall continue the performance of this Contract to the extent not terminated under the provisions of this section.

(2) Except with respect to defaults of Subcontractors, the Contractor shall not be liable for any excess costs if the failure to perform the Contract arises out of causes beyond the control of the Contractor. Such causes may include, but are not limited to, acts of God or of the public enemy, fires, floods, epidemics, quarantine restrictions, strikes, work stoppages, freight embargoes, acts of terrorism, and unusually severe weather. The Contractor shall notify the Commonwealth Contracting Officer promptly in writing of its inability to perform because of a cause beyond the control of the Contractor.

(3) Nothing in this *Subsection 32(c)* shall abridge the Commonwealth's right to suspend, debar, or take other administrative action against the Contractor.

(4) If it is later determined that the Commonwealth erred in terminating the Contract for default, then the Contract shall be deemed to have been terminated for convenience under Subsection (a).

(5) If this Contract is terminated as provided by this Subsection 31(c), the Commonwealth may, in addition to any other rights provided in this Subsection, and subject to *Section 40* (Proprietary Rights) of this Contract, require the Contractor to deliver to the Commonwealth in the manner and to the extent directed by the Contracting Officer, such reports and other documentation as the Contractor has specifically produced or specifically acquired for the performance of such part of the Contract as has been terminated. Payment for such reports and documentation will be made consistent with the Contract.

(d) In the event that Contractor becomes insolvent for any reason whatsoever, or makes an assignment for the benefit of creditors, or has a receiver appointed, or if it is declared as bankrupt under the laws of the United States, or if a petition of reorganization or rearrangement is filed against it under the bankruptcy laws, Commonwealth shall have the exclusive option of continuing with Contractor or its successors or assigns or trustee in bankruptcy under the terms and conditions of this Contract for the full remaining term of this Contract, or continuing with Contractor or its successors or assigns or trustee in bankruptcy under the terms and conditions of this Contract for such period of time as is necessary or desirable to terminate this Contract.

(e) In the event of the sale by Contractor of all or substantially all of its assets (in a single transaction or a series of related transactions) or the sale of a controlling interest in Contractor's outstanding stock, Contractor shall be entitled to assign this Contract to its successor upon written notice thereof to Commonwealth. Commonwealth shall be entitled to receive from Contractor, upon Commonwealth's request, such information as is reasonably requested by Commonwealth to enable Commonwealth to assess the financial, technical and management capabilities of such successor to assume Contractor's obligations under this Contract. If Commonwealth determines, in the exercise of its reasonable discretion, that such successor does not or may not have such requisite financial, technical or management capabilities, and if Commonwealth informs Contractor thereof in writing and describing in reasonable detail its basis therefore, then, and only then, such assignment by Contractor shall be subject to Commonwealth's prior written consent, which consent may be withheld, delayed or conditioned in Commonwealth's sole discretion. If Commonwealth withholds such consent, then Commonwealth shall have the exclusive option of continuing under the terms and conditions of this Contract with Contractor or its successors or assigns for the full remaining term of this Contract, or continuing under the terms and conditions of this Contract with Contractor or its successors or assigns for such period of time as is necessary or desirable to terminate this Contract.

(f) In the event Commonwealth fails to pay undisputed Fees for twelve (12) consecutive months, Contractor may terminate this Contract for its convenience. In such event,

notwithstanding any other provision of this Contract to the contrary, Contractor shall be released from any obligation to provide further Services pursuant to this Contract.

(g) The rights and remedies of the Commonwealth provided in this Section shall not be exclusive and are in addition to any other rights and remedies provided by law or under this Contract.

(h) The Commonwealth's failure to exercise any rights or remedies provided in this Section shall not be construed to be a waiver by the Commonwealth of its rights and remedies in regard to the event of default or any succeeding event of default.

(i) In no event shall the Contractor be paid for any loss of anticipated profit (by the Contractor or any Subcontractor), loss of use of money, or administrative or overhead costs. Any dispute regarding termination costs shall be a dispute handled in accordance with *Section 34* (Contract Controversies) of this Contract.

(j) Following exhaustion of the Contractor's administrative remedies as set forth in *Section 34* (Contract Controversies), the Contractor's exclusive remedy shall be to seek damages in the Board of Claims.

33. TERMINATION ASSISTANCE

(a) **General.** Upon the Commonwealth's request, Contractor shall provide Termination Assistance Services directly to the Commonwealth, or to any replacement provider designated by the Commonwealth, any successors or assigns of such entities or any of their designee(s). Contractor shall take all necessary and appropriate actions to accomplish a complete, timely, and seamless transition of any Terminated Services from Contractor to the Commonwealth, or to any replacement provider designated by the Commonwealth, without material interruption of or material adverse impact on the Terminated Services or any other services provided by third-parties or Services that Contractor shall continue to provide (each transition, an "Assistance Event"). Contractor shall cooperate with the Commonwealth and any new Contractor and otherwise promptly take all steps required or reasonably requested to assist the Commonwealth in effecting a complete and timely Termination Assistance Services of any Terminated Services. Contractor shall provide all information regarding the Terminated Services or as otherwise needed for Termination Assistance Services, including data conversion, interface specifications, and related professional services. Contractor shall provide for the prompt and orderly conclusion of all Terminated Services, as the Commonwealth may direct, including completion or partial completion of projects, documentation of work in process, and other measures to assure an orderly transition to the Commonwealth or the Commonwealth's designee. Contractor's obligation to provide the Services shall not cease until a Assistance Event satisfactory to the Commonwealth, including the performance by Contractor of all asset-transfers and other obligations of Contractor provided in this *Section 33* (Termination Assistance),

has been completed in accordance with mutually agreed to completion or acceptance criteria or if no agreed acceptance criteria exist, then to the Commonwealth's reasonable satisfaction.

(i) **Period of Provision**. Contractor shall provide Termination Assistance Services commencing on the date a determination is made by the Commonwealth that there shall be an Assistance Event**.**

(ii) **Notice of an Assistance Event.** The Commonwealth will provide Contractor with written notice of an Assistance Event. Such notice will include a description of the Services that are to be terminated or discontinued, the affected Commonwealth Agencies, and the anticipated effective date of the Assistance Event. The Commonwealth may modify or update any of the information provided in the initial notice of an Assistance Event from time to time by a supplemental notice from the Commonwealth to Contractor.

(iii) **Extension of Services**. The Commonwealth may elect, upon thirty (30) days prior notice to Contractor, to extend the period for performance of Termination Assistance Services (in whole or in part), in its sole discretion, provided that the total of all such extensions shall not result in Termination Assistance Services being performed beyond twenty-four (24) months following the effective date of the applicable Assistance Event without Contractor's consent. In each case, if the Commonwealth provides less than thirty (30) days prior notice of an extension, Contractor shall nonetheless use reasonable efforts to comply with the Commonwealth's request and provide the requested Services.

(iv) **Firm Commitment**. Contractor shall provide Termination Assistance Services regardless of the reason for the Assistance Event.

(v) **Performance**. Contractor shall provide all Termination Assistance Services subject to and in accordance with the terms and conditions of this Contract. Contractor shall perform Termination Assistance Services with at least the same degree of accuracy, quality, completeness, timeliness, responsiveness and resource efficiency as it is or was required to provide the same or similar Services in accordance with this Contract. The quality and level of performance of Termination Assistance Services provided by Contractor shall continue to meet or exceed the Service Levels and shall not be degraded or deficient in any respect. Service Level Credits shall be assessed for any failure to meet Service Levels during any period in which Termination Assistance Services are provided. If any period for performing any Termination Assistance Services extends beyond the expiration or the effective date of any termination of this Contract, the provisions of this Contract shall remain in full effect for the duration of such period.

(b) **Scope.** As part of the Termination Assistance Services, Contractor shall timely transfer the control and responsibility for Services previously performed by or for Contractor to the Commonwealth and/or its designee(s), and upon Commonwealth request, shall execute any documents reasonably necessary to effect such transfers. Contractor shall also provide any and all information and assistance requested by the Commonwealth required for:

(i) the Systems and processes associated with the Services to operate and be maintained and enhanced efficiently;

(ii) the Services to continue without interruption or adverse effect; and

(iii) the orderly transfer of the Services (or replacement or supplemental services) to the Commonwealth and/or its designee(s).

(c) **General Support**. Contractor shall:

(i) assist the Commonwealth and/or its designee(s) in developing a written plan for the migration of the Services to the Commonwealth and/or its designee(s), which plan shall include (as requested by the Commonwealth) capacity planning, process planning, facilities planning, human resources planning, technology planning, telecommunications planning and other planning necessary to effect the transition,

(ii) perform programming and consulting services as requested to assist in implementing the transition plan,

(iii) train personnel designated by the Commonwealth and/or its designee(s) in the use of any processes or associated Equipment, Materials, Systems or tools used in connection with the provision of the Services as needed for such personnel to assume responsibility for performance of the Services,

(iv) provide a catalog of all processes, Materials, the Commonwealth Data, Equipment, Software, Third Party Contracts and tools used to provide the Services,

(v) provide machine readable and printed listings and associated documentation for source code for Software owned by the Commonwealth and source code to which the Commonwealth is entitled under this Contract and assist in its re-configuration,

(vi) provide technical documentation for Software used by Contractor to provide the Services as needed for continuing performance of the Services,

(vii) analyze and report on the space required for the Commonwealth Data and the Software needed to provide the Services,

(viii) assist in the execution of a parallel operation, data migration and testing process until the successful completion of the transition to the Commonwealth and/or its designee(s),

(ix) create and provide copies of the Commonwealth Data in the format and on the media requested by the Commonwealth and/or its designee(s),

(x) provide a complete and up-to-date, electronic copy of the Commonwealth Procedure Manual in the format and on the media requested by the Commonwealth and/or its designee(s) and

(xi) provide other technical and process assistance, documentation and information as requested by the Commonwealth and/or its designee(s).

(d) **Personnel**.

(i) **List of Contractor Personnel**. Contractor shall promptly provide to the Commonwealth a list, organized by location, of the Contractor Personnel dedicated (fifty percent (50%) or more) to the performance of the Services that are implicated by each Assistance Event. Such list shall, subject to applicable privacy laws, specify each such Contractor Personnel's name, job title, compensation package, leave status, years of service and job responsibilities. The Commonwealth agrees not to disseminate the personally identifiable information contained in such list without Contractor's consent. Contractor shall not terminate, reassign or otherwise remove from the performance of the Services any such dedicated Contractor Personnel until after the end of the applicable Termination Assistance Services period.

(ii) **Right to Hire**. The Commonwealth and/or its designee(s) shall be permitted, without interference (including through counter-offers) from Contractor (subject to *Section 33(d)(iii)* below), to meet with, solicit and hire, effective after the later of (i) the date of the Commonwealth's notice of an Assistance Event and (ii) the completion of the Termination Assistance Services requiring such Contractor Personnel, any Contractor Personnel dedicated to the performance of the Services during the twelve (12) month period prior to the date of the Commonwealth's notice of an Assistance Event who are implicated by that Assistance Event. Contractor hereby waives its rights, if any, under contracts with such Contractor Personnel restricting the ability of such Contractor Personnel to be recruited or hired by the Commonwealth and/or its designee(s) (including waiving any right to restrict such personnel via non-compete agreements or other contractual means). Contractor shall provide the Commonwealth and/or its designee(s) with reasonable assistance in their efforts to meet with, solicit and hire such

Contractor Personnel, and shall give the Commonwealth and/or its designee(s) reasonable access to such Contractor Personnel for interviews, evaluations and recruitment. The Commonwealth shall endeavor, and shall cause its designee(s) to endeavor, to conduct the above-described activities in a manner that is not unnecessarily disruptive of Contractor's performance of its obligations under this Contract.

(e) **Software and Developed Documentation**. The Contractor shall provide the Commonwealth with all Software and Developed Documentation as set forth in *Section 40* (Proprietary Rights).

(f) **Equipment**.

(i) **List of Equipment**. Contractor shall promptly provide to the Commonwealth a list, organized by location, of the Equipment that is implicated by each Assistance Event. Such list shall specify information reasonably requested by the Commonwealth, including all fields tracked by Contractor in any asset management system used by Contractor for tracking and managing Equipment, such Equipment's function, manufacturer, model number, age, and other pertinent information.

(ii) **Right to Acquire**. The Commonwealth and/or its designee(s) shall have the right (but not the obligation) to purchase or assume the lease for any or all Equipment that is owned or leased by Contractor which is used in the provision of the Services and that is implicated by the relevant Assistance Event. Such Equipment shall be transferred in good working condition, reasonable wear and tear excepted, as of the later of the effective date of the relevant Assistance Event and the completion of the Termination Assistance Services requiring such Equipment. Contractor shall maintain such Equipment through the date of transfer so as to be eligible for the applicable manufacturer's maintenance program. In the case of Contractor-owned Equipment (including Equipment owned by Contractor Affiliates and Subcontractors and further including any such Equipment leased to Contractor), Contractor (or such Affiliate or Subcontractor) shall grant to the Commonwealth, and/or its designee(s) a warranty of title and a warranty that such Equipment is free and clear of all liens, security interests and other encumbrances. Such conveyance by Contractor (or Affiliate or Subcontractor) to the Commonwealth and/or its designee(s) shall be at fair market value (as shall be determined by an agreed-upon appraisal). At the Commonwealth's request, the Parties shall negotiate in good faith and agree upon the form and structure of the purchase. In the case of leased Equipment, Contractor shall (1) represent and warrant that the lease is not in default, (2) represent and warrant that all payments thereunder have been made through the date of transfer and (3) notify

the Commonwealth and/or its designee(s) of any lessor defaults of which it is aware at the time.

(g) **Third Party Contracts.** Contractor shall promptly, but no less than thirty (30) days from the Commonwealth's issuance of notice of an Assistance Event provide to the Commonwealth a list of the Third Party Contracts that are implicated by the relevant Assistance Event. Contractor shall, at the Commonwealth's request, cause the parties to such Third Party Contracts to permit the Commonwealth and/or its designee(s) to assume prospectively any or all such Third Party Contracts or to enter into new contracts with the Commonwealth and/or its designees on substantially the same terms and conditions, including price. Contractor shall transfer or assign those Third Party Contracts that the Commonwealth elects to assume prospectively to the Commonwealth and/or its designee(s) as of the later of the effective date of the relevant Assistance Event and the completion of the Termination Assistance requiring such Third Party Contracts. Such transfers or assignments shall be on terms and conditions acceptable to all applicable parties, provided that (A) there shall be no fee, charge or other amount imposed on the Commonwealth and/or its designee(s) by Contractor or the counter-parties to such Third Party Contracts for such transfer or assignment and (B) Contractor shall: (1) promptly cure and, in accordance with *Section 32(c)*, indemnify the Commonwealth against any default under such Third Party Contracts relating to the period prior to such transfer or assignment; (2) represent and warrant that all payments thereunder through the date of transfer or assignment are current; and (3) notify the Commonwealth and/or its designee(s) of any counter-party's default with respect to such Third Party Contracts of which it is aware at the time of such transfer or assignment.

Contractor will request, with respect to any contracts applicable to Contractor Third Party Software being provided to Commonwealth and being used by Contractor to perform the Services, that the third party agree in writing that it will permit the assignment or transfer of the applicable agreement with Contractor to Commonwealth at the termination or expiration of this Contract. If any such third party refuses to provide such a written agreement, then Contractor will notify Commonwealth of this fact. Upon any such notification by Contractor, Commonwealth shall notify Contractor in writing whether Contractor may use such third party in connection with Contractor's performance of the Services. If Contractor is notified by Commonwealth that it must not use such third party services, then Contractor will make commercially reasonable efforts to locate an alternate third party provider, but Contractor is not responsible for any additional third-party costs that may result from using an alternate provider. If no alternate provider can be located by Contractor, Contractor will so notify Commonwealth and the parties, both acting in good faith and through their respective project managers, will attempt to resolve the issue. The Contractor will not be responsible for any fees associated with the assignment or transfer of the license to the Commonwealth or for any breach by such third party of its agreement regarding the assignment or transfer.

(h) **Other Subcontracts and Third Party Contracts**. With respect to Third Party Contracts implicated by the relevant Assistance Event that are not otherwise transferred or assigned to the Commonwealth and/or its designee(s) pursuant to *Section 33(g)*, Contractor shall make available to the Commonwealth and/or its designee(s), pursuant to reasonable terms and conditions, any third party services then being utilized by Contractor in the performance of the Services. Contractor shall retain the right to utilize any such third party services in connection with the performance of services for other Contractor customers. The Commonwealth shall retain the right to contract directly with any third party previously utilized by Contractor to perform any Services.

(i) **Rates and Charges**. Except as provided in this Subsection and *Section 33(j)*, Contractor shall provide all Termination Assistance Services at no additional charge. The Parties anticipate that Termination Assistance Services requested by the Commonwealth shall be provided by Contractor using Contractor Personnel already assigned to the performance of the Services and without adversely affecting Contractor's ability to meet its performance obligations. To the extent the Commonwealth requests that Contractor perform only a portion (but not all) of the Services included in a particular Fee, the amount to be paid by the Commonwealth shall be equitably adjusted downward in proportion to the portion of the Services that Contractor shall not be providing.

(j) **Proprietary Communications Network**. If Contractor uses a proprietary communications network to provide the Services, then for a period of up to two (2) years following the effective date of the relevant Assistance Event, Contractor shall, if requested by the Commonwealth, continue to provide such proprietary communications network and other network Services to the Commonwealth, the Commonwealth and/or its designee at the rates, and subject to the terms and conditions, set forth in this Contract.

(k) **Resources.** Contractor shall maintain capability on at least thirty (30) days notice at all times during the Term to deploy all necessary resources to perform any Termination Assistance Services.

(l) **Information.** At the Commonwealth's request, Contractor shall provide to and/or make available for the Commonwealth review, at Contractor's sole cost and expense, any and all reports, data and information that the Commonwealth deems necessary in order to evaluate all options related to an Assistance Event. Contractor shall provide all such reports, data and information regardless of whether the Commonwealth has provided notice of or otherwise declared an Assistance Event.

(m) **Breach**. Contractor acknowledges and agrees that, upon any breach or threatened breach by Contractor of its obligations under this *Section 33* (Termination Assistance), Commonwealth shall be entitled to seek injunctive relief, including an order of specific performance. The provisions of this *Section 33* (Termination

Assistance) will survive any expiration of the Term and any termination of this Contract.

34. CONTRACT CONTROVERSIES

(a) All disputes between the parties arising under or relating to this Contract shall initially be referred in writing by either party to the Contractor Project Manager and the Commonwealth Project Manager. If the Contractor Project Manager and the Commonwealth Project Manager are unable to resolve the dispute within ten (10) Commonwealth business day(s) after referral of the matter to them or upon the earlier request by either the Contractor Project Manager or the Commonwealth Project Manager, the parties shall submit the dispute to the Management Committee for immediate review.

(b) Within ten (10) Commonwealth business days after any dispute between the parties is submitted to the Management Committee pursuant to Subparagraph 30(a), the Management Committee shall meet for the purpose of attempting to resolve such dispute. At any meeting of the Management Committee at which more than one (1) dispute will be considered, Commonwealth may establish the order in which such disputes shall be addressed. If the Management Committee is unable to resolve a dispute within fifteen (15) Commonwealth business days after the date of the initial meeting of the Management Committee during which such dispute was considered, the Management Committee shall immediately notify Commonwealth and Contractor pursuant to Subparagraph 30(c).

(c) In the event of a controversy or claim arising from the Contract that has not been resolved by the above process, the Contractor must, within six (6) months, file a written claim with the contracting officer for a determination. The claim shall state all grounds upon which the Contractor asserts a controversy exists

(1) The Commonwealth shall review timely-filed claims and issue a final determination, in writing, regarding the claim. The final determination shall be issued within 120 days of the receipt of the claim, unless extended by consent of the contracting officer and the Contractor. The Commonwealth shall send its written determination to the Contractor. If the Commonwealth fails to issue a final determination within the 120 days (unless extended by consent of the parties), the claim shall be deemed denied. The Commonwealth's determination shall be the final order of the purchasing agency.

(2) Within fifteen (15) days of the mailing date of the determination denying a claim or within one hundred thirty five (135) days of filing a claim if no extension is agreed to by the parties, whichever

occurs first, the Contractor may file a statement of claim with the Commonwealth Board of Claims.

(d) Each of Commonwealth and Contractor acknowledge that the provision of the Services is critical to the operations of Commonwealth. Accordingly, in the event of a dispute between Commonwealth and Contractor arising under or relating to this Contract, Contractor shall continue to provide the Services in accordance with the terms of this Contract during the pendency of the resolution of such dispute, including the final judicial resolution thereof by Commonwealth's Board of Claims or any appeal thereof, and Commonwealth shall compensate the Contractor pursuant to the terms of the Contract.

35. COMMONWEALTH HELD HARMLESS

(a) The Contractor shall hold the Commonwealth harmless from and indemnify the Commonwealth against any and all third party claims, demands and actions based upon or arising out of any activities performed by the Contractor and its employees and agents under this Contract, provided the Commonwealth gives Contractor prompt notice of any such claim of which it learns. Pursuant to the Commonwealth Attorneys Act (71 P.S. § 732-101, et seq.), the Office of Attorney General (OAG) has the sole authority to represent the Commonwealth in actions brought against the Commonwealth. The OAG may, however, in its sole discretion and under such terms as it deems appropriate, delegate its right of defense. If OAG delegates the defense to the Contractor, the Commonwealth will cooperate with all reasonable requests of Contractor made in the defense of such suits.

(b) Notwithstanding the above, neither party shall enter into any settlement without the other party's written consent, which shall not be unreasonably withheld. The Commonwealth may, in its sole discretion, allow the Contractor to control the defense and any related settlement negotiations.

36. LIMITATION OF LIABILITY

(a) The Contractor's liability to the Commonwealth under this Contract shall be limited to the value of the contract. This limitation will apply, except as otherwise stated in this *Section 36* (Limitation of Liability), regardless of the form of action, whether in contract or in tort, including negligence and whether related to direct, consequential, exemplary or punitive damages.

(b) This limitation does not apply to damages for:

(1) Bodily injury;

(2) Death;

(3) Intentional injury;

(4) Damage to real property or tangible personal property for which the Contractor is legally liable; or

(5) The Contractor's indemnity of the Commonwealth for patent, copyright, trade secret or trademark protection;

(6) Third party claims related to confidential or proprietary data misuse of confidential information or data;

(7) Milestone Credits, provided, however that payment will accrue against the cap;

(8) Commonwealth's losses resulting from Contractor's gross negligence, willful misconduct; or

(9) Contractor's costs incurred for notification, mitigation, and credit monitoring services required due to a security breach; or

(10) The Commonwealth costs, losses or damages incurred due to Personal Information being accessed, used, released, disclosed and/or acquired in an unauthorized manner while in the control of the Contractor; or

(11) Contractor's abandonment of any Services, wrongful termination of the Contract or willful refusal to provide Termination Assistance Services.

(c) Except as provided for in *Section 36(c)(1) through (4)*, neither Party will be liable for indirect, incidental, special, consequential, exemplary or punitive damages arising out of or relating to the Contract:

(1) Additional costs to maintain the Services arising from a default by Contractor including the cost of work-arounds;

(2) Loss of or corruption to Commonwealth data including, without limitation, the cost and expense of rectification of the data arising out of a default (including for recovering, reconstructing, reformatting or reloading data), but only to the extent such damages arise out of the failure of Contractor to comply with its obligations under *Section 52* (Virus and Malicious Code);

(3) Expenditure or charges incurred by Commonwealth and rendered necessary as a result of a default by Contractor; and

(4) Any regulatory losses, fines, expenses or other losses suffered by Commonwealth as a result of Contractor's failure to comply with any law or regulation.

37. CONFIDENTIALITY

(a) For purposes of this Contract, "*Confidential Information*" of a party shall mean (1) with respect to Commonwealth, all Commonwealth Data and other information of Commonwealth or any Commonwealth agency or any private individual, organization or public agency, in each case to the extent such information and documentation is not permitted to be disclosed to third parties under local, Commonwealth or Federal laws and regulations or pursuant to any policy adopted by Commonwealth or pursuant to the terms of any third-party agreement to which Commonwealth is a party and (2) with respect to Contractor, all information identified in writing by Contractor as confidential or proprietary to Contractor, its subcontractors or licensors.

(b) All Confidential Information relating to a party shall be held in confidence by the other party to the same extent and in at least the same manner as such party protects its own confidential or proprietary information. Neither party shall disclose, publish, release, transfer or otherwise make available any Confidential Information of the other party in any form to, or for the use or benefit of, any person or entity without the other party's consent. Subject to the other provisions of this Contractor, each party shall, however, be permitted to disclose relevant aspects of the other party's Confidential Information to its officers, agents, subcontractors and employees and to the officers, agents, subcontractors and employees of its corporate affiliates or subsidiaries to the extent that such disclosure is reasonably necessary for the performance of its duties and obligations under this Contract; provided, however, that such party shall take all reasonable measures to ensure that Confidential Information of the other party is not disclosed or duplicated in contravention of the provisions of this Contractor by such officers, agents, subcontractors and employees and that such party shall be responsible for any unauthorized disclosure of the Confidential Information of the other party by such officers, agents, subcontractors or employees; and further provided, that if the disclosure is by the Commonwealth to another contractor or sub-contractor, such disclosure is subject to a suitable non-disclosure agreement. The obligations in this Paragraph shall not restrict any disclosure by either party pursuant to any applicable law, or in accordance with the order of any court or government agency of competent jurisdiction (provided that the disclosing party shall give prompt notice to the non-disclosing party of such order) and, except to the extent provided otherwise by any applicable law, shall not apply with respect to information which:

(1) is developed by the other party without violating the disclosing party's proprietary rights,

(2) is or becomes publicly known (other than through unauthorized disclosure),

(3) is disclosed by the owner of such information to a third party free of any obligation of confidentiality,

(4) is already known by such party without an obligation of confidentiality other than pursuant to this Contractor or any confidentiality Contractor entered into before the Effective Date between Commonwealth and Contractor, or

(5) is rightfully received by the disclosing party free of any obligation of confidentiality.

The confidentiality period for Confidential Information which is related to hardware, software, technical specifications, and methods and processes related to data processing and/or computing shall continue from the date of disclosure until two years following expiration or termination of this Contract. The immediately preceding sentence shall not release or relax, in whole or in part, Contractor's confidentiality obligations with respect to information pertaining to any private individual or, with respect to any Commonwealth Agency, information or documentation which is not permitted to be disclosed to third parties under local, Commonwealth or Federal laws and regulations or pursuant to the terms of any third party Contractor to which Commonwealth is a party.

Nothing in this *Section 37(b)* shall supersede or limit, or be deemed to supersede or limit, any other provision of this Contract pertaining to confidentiality or disclosure of any Commonwealth Data or to any security procedures required to be followed by Contractor or its employees and other representatives. In addition to the confidentiality and non-disclosure and other restrictive provisions of this *Section 37(b)* and elsewhere in this Contract, Contractor shall be subject to, and shall be required to abide by, the provisions set forth in the *Exhibits* to the RFP, all of which are required to be incorporated into this Contract to satisfy the requirements of a particular Commonwealth Agency, a particular agency of the Federal government with whom Commonwealth interacts or other third party.

(c) Each party shall:

(1) Notify the other party promptly of any known unauthorized possession, use or knowledge of the other party's Confidential Information by any person or entity.

(2) Promptly furnish to the other party full details known by such party relating to the unauthorized possession, use or knowledge thereof and shall use reasonable efforts to assist the other party in investigating or

preventing the recurrence of any unauthorized possession, use or knowledge of the other party's Confidential Information.

(3) Use reasonable efforts to cooperate with the other party in any litigation and investigation against third parties deemed necessary by the other party to protect its proprietary rights.

(4) Promptly use all reasonable efforts to prevent a recurrence of any such unauthorized possession, use or knowledge of the other party's Confidential Information.

(d) Each party shall bear the cost it incurs as a result of compliance with this Paragraph. The obligations in this Paragraph shall not restrict any disclosure by either party pursuant to any applicable law or pursuant to the order of any court or other legal process or government agency of competent jurisdiction (provided that the disclosing party shall give prompt notice to the non-disclosing party of such order).

(e) There shall be no restriction with respect to the use or disclosure of any ideas, concepts, know-how or data processing techniques developed alone or jointly with Commonwealth in connection with Services provided to Commonwealth under this Contractor.

(f) The Contractor shall use the following process when submitting information to the Commonwealth it believes to be confidential and/or proprietary information or trade secrets:

(1) Prepare an un-redacted version of the appropriate document, and

(2) Prepare a redacted version of the document that redacts the information that is asserted to be confidential or proprietary information or a trade secret, and

(3) Prepare a signed written statement that states:

(i) the attached document contains confidential or proprietary information or trade secrets;

(ii) the Contractor is submitting the document in both redacted and un-redacted format in accordance with 65 P.S. § 67.707(b); and

(iii) the Contractor is requesting that the document be considered exempt under 65 P.S. § 67.708(b)(11) from public records requests.

(4) Submit the two documents with the signed written statement to the Commonwealth.

(g) When the Contract expires or terminates, and at any other time at the written request of the Commonwealth, the Contractor must promptly return to the Commonwealth all of the Commonwealth's Confidential Information and Data (and all copies of this information) that is in the Contractor's possession or control, in whatever form. Unless the Commonwealth agrees or specifies otherwise, the Contractor shall also deliver to the Commonwealth or, if requested by the Commonwealth, delete or destroy any copies, duplicates, summaries, abstracts or other representations of any such Confidential Information or any part thereof, in whatever form, then in the Contractor's possession or control in accordance with the "NIST Guidelines for Media Sanitization" (SP 800-88).

38. SENSITIVE INFORMATION

(a) The Contractor shall not publish or otherwise disclose, except to the Commonwealth or the Contractor's subcontractors, any information or data obtained hereunder from private individuals, organizations, or public agencies, in a way that allows the information or data furnished by or about any particular person or establishment to be identified.

(b) The parties shall not use or disclose any information about a recipient receiving services from, or otherwise enrolled in, a Commonwealth program affected by or benefiting from services under this Contract for any purpose not connected with the parties' Contract responsibilities.

(c) Contractor, as directed, shall comply with all federal or state laws and regulations related to the use of information that constitutes protected health information (PHI) as defined by the regulations promulgated pursuant to the *Health Insurance Portability and Accountability Act* (HIPAA). By signing this Contract, the Contractor agrees to the terms of the Business Associates Contract, which is incorporated into this Contract as Appendix A. If Contract Participant, or relevant portion thereof, is a Covered Entity as defined in HIPAA, and the Contractor is performing the work of a Business Associate, the Contract Participant will fill in the blanks in the attached Appendix. It is understood that Appendix A is only applicable if the Contract Participant indicates in writing to Contractor, specifying the work and scope intended to be subject to a Business Associates Contract, and only to the extent that Contractor and the Contract Participant agree in writing as to the specific application of Appendix A and the Business Associate Contract. If not applicable to the entire Contract Participant, Appendix A is only applicable with respect to the internal entities indicated by the Contract Participant and agreed to by the Contractor.

(d) Contractor will comply with all obligations applicable to it under all applicable data protection legislation in relation to all personal data that is processed by it in the course of performing its obligations under this Contract including by:

(1) Maintaining a valid and up to date registration or notification under the data protection legislation; and

(2) Complying with all data protection legislation applicable to cross border data flows of personal data and required security measures for personal data.

39. PATENT, COPYRIGHT, TRADEMARK, AND TRADE SECRET PROTECTION

(a) The Contractor shall hold the Commonwealth harmless from any suit or proceeding which may be brought by a third party against the Commonwealth, its departments, officers or employees for the alleged infringement of any United States or foreign patents, copyrights, or trademarks, or for a misappropriation of trade secrets arising out of performance of this Contract, including all work, services, materials, reports, studies, and computer programs provided by the Contractor, and in any such suit or proceeding will satisfy any final award for such infringement, including costs. The Commonwealth agrees to give Contractor prompt notice of any such claim of which it learns. Pursuant to the Commonwealth Attorneys Act 71 P.S. § 732-101, *et seq.*, the Office of Attorney General (OAG) has the sole authority to represent the Commonwealth in actions brought against the Commonwealth. The OAG may, however, in its sole discretion and under the terms it deems appropriate, delegate its right of defense. If OAG delegates the defense to the Contractor, the Commonwealth will cooperate with all reasonable requests of Contractor made in the defense of such suits. No settlement which prevents the Commonwealth from continuing to use the Developed Materials as provided herein shall be made without the Commonwealth's prior written consent. In all events, the Commonwealth shall have the right to participate in the defense of any such suit or proceeding through counsel of its own choosing. It is expressly agreed by the Contractor that, in the event it requests that the Commonwealth to provide support to the Contractor in defending any such claim, the Contractor shall reimburse the Commonwealth for all reasonable expenses (including attorneys' fees, if such are made necessary by the Contractor's request) incurred by the Commonwealth for such support. <u>If OAG does not delegate the defense of the matter, the Contractor's obligation to indemnify ceases</u>. The Contractor will, at its expense, provide whatever cooperation OAG requests in the defense of the suit.

(b) The Contractor agrees to exercise reasonable due diligence to prevent claims of infringement on the rights of third parties. The Contractor certifies that, in all respects applicable to this Contract, it has exercised and will continue to exercise due diligence to ensure that all works produced under this Contract do

not infringe on the patents, copyrights, trademarks, trade secrets or other proprietary interests of any kind which may be held by third parties.

(c) If the defense of the suit is delegated to the Contractor, the Contractor shall pay all damages and costs finally awarded therein against the Commonwealth, when such damages and costs are required to be paid. If information and assistance are furnished by the Commonwealth at the Contractor's written request, it shall be at the Contractor's expense, but the responsibility for such expense shall be only that within the Contractor's written authorization.

(d) If the products, materials, reports, studies, or computer programs furnished hereunder become subject to a claim of infringement of a United States patent, copyright, or trademark, or for a misappropriation of trade secret, or if any of the products, materials, reports, studies or computer programs provided by the Contractor are in such suit or proceeding held to constitute infringement and the use or publication thereof is enjoined, then without diminishing the Contractor's obligation to satisfy any final award, the Contractor may, at its option and expense, substitute functional equivalents for the alleged infringing products, materials, reports, studies, or computer programs or, at the Contractor's option and expense, obtain the rights for the Commonwealth to continue the use of such products, materials, reports, studies, or computer programs.

(e) If any of the products, materials, reports, studies, or computer programs provided by the Contractor are in such suit or proceeding held to constitute infringement and the use or publication thereof is enjoined, the Contractor shall, at its own expense and at its option, either procure the right to publish or continue use of such infringing products, materials, reports, studies, or computer programs, replace them with non-infringing items, or modify them so that they are no longer infringing.

(f) If the Contractor is unable to do any of the preceding, the Contractor agrees to pay the Commonwealth:

(1) Any amounts paid by the Commonwealth less a reasonable amount based on the acceptance and use of the deliverable;

(2) Any license fee less an amount for the period of usage of any software; and

(3) The prorated portion of any Fees representing the time remaining in any period of service for which payment was made.

(g) The obligations of the Contractor under this Section 45 (Patent, Copyright, Trademark, and Trade Secret Protection) continue without time limit and survive the termination of this Contract.

(h) Notwithstanding the above, the Contractor shall have no obligation for:

(1) Modification of any product, service, or deliverable provided by the Commonwealth or any third party, except for the Contractor or any of its Subcontractors;

(2) Any material provided by the Commonwealth to the Contractor and incorporated into, or used to prepare, a product, service, or deliverable;

(3) Use of the product, service, or deliverable in other than its specified operating environment;

(4) The combination, operation, or use of the product, service, or deliverable with other products, services, or deliverables not provided by the Contractor as a system or the combination, operation, or use of the product, service, or deliverable, with any products, data, or apparatus that the Contractor did not provide;

(5) Infringement of a non-Contractor product alone;

(6) The Commonwealth's distribution, marketing or use beyond the scope contemplated by the Contract;

(7) The Commonwealth's failure to use corrections or enhancements made available to the Commonwealth by the Contractor at no charge;

(8) Any infringement or claim thereof against the Commonwealth brought prior to the execution of this Contract, unless the infringement or claim relates to services provided by Contractor under another contract with the Commonwealth; or

(9) Infringement related to content provided by or on behalf of the Commonwealth, except as provided by the Contractor or any of its Subcontractors or suppliers.

(i) The obligation to defend and indemnify the Commonwealth, under the terms of this *Section 39* (Patent, Copyright, Trademark, and Trade Secret Protection), shall be the Contractor's sole and exclusive obligation and the Commonwealth's sole and exclusive remedy against the Contractor for the infringement or misappropriation of intellectual property.

40. PROPRIETARY RIGHTS

(a) **Commonwealth Software**. As between Commonwealth and Contractor, all Commonwealth Software shall be and shall remain the exclusive property of Commonwealth or its licensors, and Contractor shall have no rights or interests in the Commonwealth Software by virtue of this Contract except as described in this *Section 40* (Proprietary Rights) or elsewhere in this Contract. Commonwealth hereby grants to Contractor, at no cost to Contractor, for the limited purpose of providing the Services, a nonexclusive, nontransferable, royalty-free right (subject to the terms of any third party agreement to which Commonwealth is a party and which theretofore is disclosed to Contractor) to (1) have access to the Commonwealth Software, (2) copy the Commonwealth Software for archival purposes or as may otherwise be required by this Contract, (3) modify the Commonwealth Software as required by this Contract, if permitted by the Software licensing terms and pursuant to the terms of Commonwealth Third Party Software license agreement, if applicable, and (4) sublicense Contractor's subcontractors approved by Commonwealth to do any of the foregoing; provided, however, that neither Contractor nor any of its subcontractors may decompile or reverse engineer, or attempt to decompile or reverse engineer, any of the Commonwealth Software.

As of the Effective Date and subject to the terms of any third party agreement to which Commonwealth is a party, (1) Commonwealth shall, at no cost to Contractor, provide Contractor with access to the Commonwealth Software in the form in use by Commonwealth as of the Effective Date and (2) Contractor, as part of the Services, shall compile and, as changes are made, update a list of all of the Commonwealth Software then in use by Contractor or any of its subcontractors in connection with Contractor's performance of the Services. Upon the expiration or termination for any reason of Contractor's obligation to provide the Services or of this Contract, the rights granted to Contractor in this *Section 40(a)* shall immediately revert to Commonwealth or Commonwealth's designee, and Contractor forthwith shall, at no cost to Commonwealth, deliver to Commonwealth all of the Commonwealth Software (including any related source code and object code in Contractor's possession or under its control) in the form in use as of the effective date of such expiration or termination, together with a current copy of the list of Commonwealth Software in use as of the date of such expiration or termination. Concurrently therewith, Contractor shall destroy or erase all other copies of any of the Commonwealth Software then in Contractor's possession or under its control unless otherwise instructed by Commonwealth; provided, however, pursuant to and if permitted by the Commonwealth's license agreement for Commonwealth Third Party Software, if applicable, that Contractor may retain one archival copy of such Commonwealth Software, including the Developed Software, until the later of six (6) years after such expiration or termination of this Contract and the final resolution of any actively asserted pending disputes between the parties, such retention being for the sole purpose of establishing Contractor's performance under this Contract.

(b) **Contractor Software and Contractor Tools**. As between Commonwealth and Contractor, all Contractor Software and Contractor Tools shall be and shall remain the exclusive property of Contractor, and Commonwealth shall have no rights or interests in the Contractor Software or the Contractor Tools by virtue of this Contract except as described in this *Section 40(b)*. As part of the Services, Contractor shall during the Term (1) use the Contractor Software and the Contractor Tools to provide the Services, (2) make available the commercially available Contractor Software and the commercially available Contractor Tools to Commonwealth for use by Commonwealth solely in connection with the Services, and (3) maintain on Commonwealth's premises and make available to Commonwealth upon Commonwealth's request from time to time, for archival purposes only, a copy of the Contractor Software and the Contractor Tools owned by Contractor or its subcontractors and then being used by Contractor to provide the Services.

Upon the expiration or termination for any reason of Contractor's obligation to provide the Services under this Contract and at the request of Commonwealth, Contractor shall, subject to mutually agreed terms and conditions, (1) grant, or cause its subcontractors to grant, to Commonwealth a nonexclusive, nontransferable license to use and, if permitted by the terms of mutually agreed terms and conditions relating thereto, modify and make derivative works of, and unless Commonwealth terminates this Contract pursuant to the terms of *Section 32(a),(b), or (f)* to grant to third parties engaged by Commonwealth the right to use and, if permitted by mutually agreed terms and conditions relating thereto, modify and make derivative works of, all or any portion of the commercially available Contractor Software and the commercially available Contractor Tools owned by Contractor or its subcontractors theretofore being used by Contractor in connection with the Services, the foregoing rights being granted to the extent reasonably necessary to facilitate Commonwealth's or such third party's performance of the activities or services substantially equivalent to the Services to be provided by Contractor under this Contract immediately prior to such expiration or termination and (2) deliver to Commonwealth the object code version of such commercially available Contractor Software and such commercially available Contractor Tools in the form being used by Contractor in connection with the Services immediately prior to such expiration or termination.

It is understood and agreed by Contractor that the rights granted to Commonwealth hereunder in respect of the commercially available Contractor Software and the commercially available Contractor Tools shall not restrict Commonwealth from using such Contractor Software and such Contractor Tools in the manner in which such items were used by Contractor and its subcontractors to provide the Services immediately prior to the expiration or termination of this Contract. The foregoing obligations of Contractor shall be subject to mutually agreed terms and conditions. In consideration of the grant to Commonwealth of the foregoing license, Commonwealth shall be assessed license fees hereunder not in excess of any license fees therefor being offered, as of the date of

termination, by Contractor or its subcontractors, to their respective state governmental customers generally, unless Commonwealth terminates this Contract pursuant to the terms of *Section 32(a),(b) or (f)*, in which case the then-prevailing license fees of Contractor and its subcontractors, as applicable, shall apply. The foregoing shall not limit or otherwise affect Commonwealth's obligations to pay third party assignment or transfer fees as contemplated in *Section 33* (Termination Assistance); provided, however, that Commonwealth shall not be assessed any additional fees in respect thereof by Contractor.

(c) **Developed Documentation.** Documentation developed by Contractor specifically for the Commonwealth in connection with its performance under this Contract is the sole and exclusive property of the Commonwealth and shall be considered "works made for hire" under the United States Copyright Act of 1976, as amended, 17 United States Code. In the event that the documentation does not fall within the specifically enumerated works that constitute works made for hire under the United States copyright laws, Contractor agrees to assign and, upon their authorship or creation, expressly and automatically assigns all copyright interests, proprietary rights, trade secrets, and other right, title, and interest in and to such documentation to Commonwealth. Commonwealth shall have all rights accorded an owner of copyright under the United States copyright laws including, but not limited to, the exclusive right to reproduce the documentation in multiple copies, the right to distribute, copies by sales or other transfers, the right to register all copyrights in its own name as author in the United States and in foreign countries, the right to prepare derivative works based upon the Creative Works and the right to display the documentation. Upon completion or termination of this Contract, all working papers, files and other documents related to the documentation shall immediately be delivered by Contractor to the Commonwealth. Contractor warrants that the documentation is original and does not infringe any copyright, patent, trademark, or other intellectual property right of any third party and are in conformance with the intellectual property laws of the United States. Provided however that Commonwealth's sole remedy for breach of this warranty is the indemnity contained in *Section 39* (Patent, Copyright, Trademark, and Trade Secret Protection).

(d) All literary works, or other works of authorship (such as application programs, listings, programming tools, documentation, reports, drawings, procedure manuals and similar works) ("Developed Materials") developed hereunder shall be treated in accordance with the following general principles:

(1) If and to the extent Developed Materials modify, improve or enhance software programs generally licensed by Contractor to end-users, then such Developed Materials shall be the property of Contractor and Contractor hereby grants to Commonwealth a perpetual, non-exclusive, nontransferable, royalty-free license to use such Developed Materials in Commonwealth's receipt and use of the Services;

(2) If and to the extent Developed Materials modify, improve or enhance software or other materials owned by Commonwealth or licensed to Commonwealth by a third party (i.e., a licensor other than Contractor or any Contractor agent), then such modification, improvement or enhancement and all related intellectual property rights therein shall, as between Commonwealth and Contractor, be the property of Commonwealth;

(3) If and to the extent Developed Materials constitute a newly created software program or module, and if Commonwealth funds the development cost thereof to any extent, then such software program or module and all related intellectual property rights therein shall be the property of Commonwealth; and

(4) If and to the extent Developed Materials constitute documentation, reports, drawings, procedure manuals and similar works, such Developed Materials shall be the property of Commonwealth. Contractor will not place trademarks or copyright notices on any such Developed Materials.

(5) Any data related to the use of the Services by the Commonwealth shall be the property of the Commonwealth. For this purpose, data includes ordering information, inventories, etc. At the end of the Contract, regardless of how it is ended, or at any time requested by the Commonwealth, the Contractor will provide the Commonwealth with such data in a format specified by the Commonwealth.

(e) **Residual Knowledge**. Either Party, in the course of conducting business, may use any ideas, concepts, and know-how, relating to the Services which Contractor or Commonwealth (alone or jointly with the Commonwealth) develops or learns in connection with Contractor's provision of Services to Commonwealth under this Contract.

41. PUBLICATION RIGHTS AND/OR COPYRIGHTS

(a) The Contractor shall not publish any of the results of the work, which identify the Commonwealth, without the written permission of the Commonwealth. The publication shall include the following statement: "The opinions, findings, and conclusions expressed in this publication are those of the author and not necessarily those of the Commonwealth of Pennsylvania." The Contractor shall not include in the documentation any copyrighted matter, unless the Contractor provides the Commonwealth with written permission of the copyright owner.

(b) Except as otherwise provided in *Section 40* (Proprietary Rights) and the confidentiality provisions of *Section 37* (Confidentiality), the Commonwealth shall have unrestricted authority to reproduce, distribute, and use any submitted report or data designed or developed and delivered to the Commonwealth as part of the performance of the Contract.

(c) Rights and obligations of the parties under this *Section 41* (Publication Rights and/or Copyrights) survive the termination of this Contract.

42. REPORTS AND DATA

(a) Data. Commonwealth shall supply to Contractor the Commonwealth Data in the form maintained by the Commonwealth on such time schedules as may be agreed to by Commonwealth and Contractor from time to time. All Commonwealth Data is and shall remain the property of Commonwealth. Subject to *Section 40* (Proprietary Rights), the Commonwealth Data shall not be (1) used by Contractor or Contractor Agents other than in connection with providing the Services, and then only in accordance with the terms of this Contract, (2) disclosed, sold, assigned, leased or otherwise provided to third parties by Contractor or Contractor Agents without Commonwealth's consent and any applicable consent required by any federal governmental entity, or (3) commercially exploited by or on behalf of Contractor or Contractor Agents.

(b) Reports. As part of the Services, Contractor shall provide the Reports, in electronic form, to Commonwealth. The Reports shall be prepared by Contractor and provided to the Commonwealth in a manner readable by a normal Windows based personal computer. Acceptable formats include but are not limited to: Adobe Acrobat (PDF), Microsoft Word, Microsoft Excel, Microsoft PowerPoint, Text, Comma Separated Values (CSV).

(c) Correction of Errors. In the event of any errors or inaccuracies in any of the Commonwealth Data or the Reports, or any other data processing errors or unexpected interruptions (e.g., "abends" or “freeze”), Contractor and Commonwealth shall work together in good faith, using all reasonable efforts and commencing immediately upon the discovery of the situation, to correct such error, inaccuracy or interruption. The foregoing obligations of Contractor under this *Section 42(c)* shall be subject to any limitations placed upon Contractor's access to the Commonwealth Data by Commonwealth or pursuant to this Contract. Promptly upon the completion of the correction of such error, inaccuracy or interruption, the Commonwealth Project Manager and the Contractor Project Manager shall meet to determine and document the cause thereof. If the error, inaccuracy or interruption is determined to be caused by the error, negligence or omission of Contractor to perform an obligation under this Contract, there shall be no charge to Commonwealth for Contractor's participation in such correction. If the error, inaccuracy or interruption is determined to be caused by the error, negligence or omission of

Commonwealth to perform an obligation under this Contract, Commonwealth shall reimburse Contractor for Contractor's out-of-pocket expenses paid by Contractor to third parties (other than Contractor's or any Contractor's Agent's employees) for expertise not otherwise possessed by or available to Contractor and Contractor's expenses for its employees or the employees of any Contractor agent not theretofore engaged in the provision of the Services.

(d) Return of Data. At no cost to Commonwealth and as part of the Services, Contractor shall, upon Commonwealth's request at any time and at the cessation of the Termination Assistance, (1) promptly return to Commonwealth, in the format and on the media in use as of the date of the request, all or the requested portion of the Commonwealth Data then in Contractor's possession or under its control and (2) erase or destroy all or the requested portion of Commonwealth Data then in Contractor's possession or under its control. Commonwealth Data returned to the Commonwealth must be in a form that is freely accessible to the Commonwealth and not in a Contractor proprietary format.

43. SECURITY AND PROTECTION OF INFORMATION

(a) At all times during the Term, Contractor shall provide all Services, and use all resources related thereto, in a secure manner and in accordance with the Commonwealth's security requirements, including the prevention and detection of fraud, abuse, or other inappropriate use or access of systems and networks by all appropriate means, including network management and maintenance applications and tools, and the use of appropriate encryption technologies. In addition, all Contractor personnel (including personnel of any Subcontractors) shall be subject to and shall at all times conform to the Commonwealth's laws, rules, and requirements for the protection of premises, materials, equipment, and personnel, as they have been previously disclosed to Contractor in writing, including those set forth in the *Exhibits* to the RFP. Any violations or disregard of these rules shall be cause for denial of access by such personnel to the Commonwealth's property. Contractor shall exercise due care and diligence to prevent any injury to person or damage to property while on the Commonwealth's premises. The operation of Contractor vehicles or private vehicles of Contractor personnel on the Commonwealth's property shall conform to posted and other regulations and safe driving practices. Vehicular accidents on the Commonwealth's property and involving Contractor personnel shall be reported promptly to the appropriate Commonwealth's security personnel.

(b) The Pennsylvania State Police's Criminal Justice Information Services Policy ("CJIS Policy"), is set forth in *Exhibits G.6 and G.7*, and is hereby incorporated by this reference into this Contract. Contractor acknowledges and agrees that it is bound by all applicable provisions of the CJIS Policy. Contractor and the Commonwealth further agree that, in accordance with the CJIS Policy, the Commonwealth does not anticipate and will not authorize any

requests to Contractor for the criminal history record information covered by the CJIS Policy, because Contractor is performing an IT support function. The Commonwealth's Office of Attorney General's CHRIA Handbook, attached as *Exhibit G.12* to the RFP, is also incorporated by reference into this Contract. Contractor acknowledges and agrees that it is bound by all applicable provisions of the CHRIA Handbook.

.

44. BACKGROUND CHECKS

(a) The Contractor must, at its expense, arrange for a background check for each of its employees, as well as for the employees of its subcontractors, who will have access to Commonwealth Services Locations, either through on site or remote access. Background checks will not be conducted by the Commonwealth but rather will be conducted by Contractor or its subcontractors according to Contractor policy and practice and consistent with ITB-SEC009. The background check must be conducted prior to initial access by a Contractor Personnel and every two (2) years thereafter or at a longer interval if required by applicable law.

(b) Before the Commonwealth will permit Contractor Personnel access to Commonwealth facilities, the Contractor must provide written confirmation to the office designated by the agency that the background check has been conducted. If, at any time, it is discovered that Contractor Personnel has a criminal record that includes a felony or misdemeanor involving terroristic threats, violence, use of a lethal weapon, or breach of trust/fiduciary responsibility; or which raises concerns about building, system, or personal security, or is otherwise job-related, the Contractor shall notify the Commonwealth Contracting Officer immediately, shall not assign that employee to any Commonwealth facilities, shall remove any access privileges already given to the employee, and shall not permit that employee remote access to Commonwealth facilities or systems, unless the agency consents, in writing, prior to the access being provided. The agency may withhold its consent at its sole discretion. Failure of the Contractor to comply with the terms of this Paragraph may result in default of the Contractor under its Contract with the Commonwealth.

(c) The Commonwealth specifically reserves the right of the Commonwealth to conduct background checks over and above that described herein.

45. INSURANCE

(a) Contractor Insurance Requirements. During the Contract Term, Contractor shall maintain at its own expense, insurance of the type and in the amounts specified below and issued by companies authorized to conduct such business under the laws of Pennsylvania:

(1) Statutory workers' compensation in accordance with all applicable Federal, state and local requirements, and employer liability in an amount not less than $2,000,000 per occurrence;

(2) Comprehensive general public liability (including contractual liability insurance) in an amount not less than $5,000,000 per occurrence;

(3) Comprehensive automobile liability covering all vehicles that Contractor owns, hires, or leases in an amount not less than $5,000,000 per occurrence (combined single limit for bodily injury and property damages).

(4) Personal property insurance, on a replacement basis, covering all of Contractor's and Contractor's Agents' personal property located at any Contractor Services Location.

(5) Professional liability/error & omission in the aggregate amount of not less than $15,000,000.

(6) Comprehensive crime insurance in an amount of not less than $15,000,000 per claim.

(7) Network/Cyber Liability Insurance (including coverage for Technology Professional Liability if not covered under Contractor's Professional Liability/Errors and Omissions Insurance referenced above) in the amount of $20,000,000, per occurrence.

(8) Umbrella/excess in an aggregate amount of not less than $30,000,000.

(b) Insurance Requirements for Subcontractors. During the Contract Term, Contractor shall require each of its subcontractors listed in *Schedule L* (Approved Subcontractors) and any other subcontractors performing any Services on-site at any of the Contractor Services Locations, to maintain at their own expense or Contractor's expense, insurance of the type and in the amounts specified below:

(1) Statutory workers' compensation in accordance with all applicable Federal, state and local requirements, and employer liability in an amount not less than $1,000,000 per occurrence;

(2) Comprehensive general public liability (including contractual liability insurance) in an amount not less than $2,000,000 per occurrence;

(3) If any of the subcontractor personnel will be on-site at any of the Commonwealth's or Contractor's facilities, comprehensive automobile liability covering all vehicles owned, hired or leased by that Subcontractor and in an amount not less than $2,000,000 per

occurrence (combined single limit for bodily injury and property damages);

(4) If the subcontractor personnel will be on-site at any of Commonwealth's or Contractor's facilities, personal property insurance, on a replacement basis, covering all of that Subcontractor's personal property located at any such facilities; and

(5) Network/Cyber Liability Insurance (including coverage for Technology Professional Liability if not covered under Contractor's Professional Liability/Errors and Omissions Insurance referenced above) in the amount of $10,000,000, per occurrence; and

(6) Errors & Omissions liability in the amount of $2,000,000 each claim and aggregate (if applicable).

(c) Prior to the expiration of any then effective insurance policy, Contractor shall furnish to Commonwealth certificates of insurance or other appropriate documentation (including evidence of renewal of insurance) evidencing all coverage referenced in this *Section 45* (Insurance), as applicable, and naming Commonwealth as an additional insured to the extent of Contractor's indemnities contained in this Contract. Contractor shall have included in all policies of insurance required hereunder a waiver by the insurer of all right of subrogation against Commonwealth in connection with any loss or damage thereby insured against. Such certificates or other documentation will include a provision whereby thirty (30) days' notice must be received by Commonwealth prior to coverage cancellation or alteration of the coverage by either Contractor or its subcontractors or the applicable insurer. Such cancellation or alteration shall not relieve Contractor of its continuing obligation to maintain insurance coverage in accordance with this *Section 45*(Insurance).

(d) For purposes hereof, Contractor and such subcontractors may maintain "umbrella" insurance policies to fulfill the foregoing insurance requirements, as appropriate.

46. WARRANTIES

(a) Contractor represents, warrants and covenants that as of the Contract's Effective Date:

(1) It is a corporation duly incorporated, validly existing, and in good standing under the laws of _____.

(2) It has all requisite corporate power and authority to execute, deliver, and perform its obligations under this Contract.

(3) Contractor is duly licensed, authorized and qualified to do business and is in good standing in Pennsylvania and in every other jurisdiction where Services will be performed by Contractor pursuant to this Contract in which a license, authorization or qualification is required for the ownership or leasing of its assets or the transaction of business of the character transacted by it except where the failure to be so licensed, authorized or qualified would not have a material adverse effect on Contractor's ability to fulfill its obligations under this Contract.

(4) The execution, delivery and performance of this Contract by Contractor has been duly authorized by Contractor.

(5) Contractor shall comply with all applicable Federal, state and local laws and regulations applicable to Contractor and shall obtain all applicable permits and licenses required of Contractor in connection with its obligations under this Contract.

(6) Contractor has not disclosed any Confidential Information of Commonwealth.

(7) The Contractor Software does not and will not, and the Developed Software and the Services will not, infringe upon the proprietary rights of any third party, provided that Contractor will have no obligation with respect to any losses to the extent the same arise out of or in connection with Commonwealth's modification or misuse of equipment, systems, programs, or products or Commonwealth's combination, operation or use with devices, data, equipment, systems, programs or products not furnished by Contractor under this Contract.

(8) Contractor Personnel and Subcontractors that Contractor will use to provide and perform the Services have and during the Term will have, the suitable knowledge, skills, experience, qualifications and resources to provide and perform the Services:

(i) In accordance with the Contract; and

(ii) In a diligent, workmanlike manner with due care and skill, consistent with the required level of quality and performance and in accordance with the Service Levels.

(9) The Services will comply with standards set in the Commonwealth’s IT Bulletins as issued from time to time, and all internal policies and procedures as set from time to time and as a provided to Contractor.

(10) Contractor shall cooperate fully with Commonwealth and with any third party appointed by Commonwealth to the extent that such cooperation may be necessary to permit Commonwealth or such third parties to complete any work related to or impacted by the Services provided to Commonwealth by Contractor under the Contract.

(11) Contractor shall collaborate fully with Commonwealth or with any third party appointed by Commonwealth to the extent that such cooperation may be necessary to permit Commonwealth or such third parties to in-source or transfer to a third party any aspect of the Services then provided by Contractor under the Contract.

(b) Commonwealth represents, warrants and covenants that as of the Contract's Effective Date:

(1) It is a sovereign entity and has all requisite power and authority to execute, deliver, and perform its obligations under this Contract.

(2) It has, or at any time of provision to Contractor, will have the right to use and to disclose to Contractor and Contractor Agents and to allow Contractor and Contractor Agents to use in accordance with the terms of this Contract any Commonwealth Software so disclosed to Contractor.

47. CONTRACTOR RESPONSIBILITY PROGRAM

(a) The Contractor certifies, for itself and all its subcontractors, that as of the date of its execution of this Bid/Contract, that neither the Contractor, nor any subcontractors, nor any suppliers are under suspension or debarment by the Commonwealth or any governmental entity, instrumentality, or authority and, if the Contractor cannot so certify, then it agrees to submit, along with its Bid, a written explanation of why such certification cannot be made.

(b) The Contractor must also certify, in writing, that as of the date of its execution of this Bid/Contract, it has no tax liabilities or other Commonwealth obligations.

(c) The Contractor's obligations pursuant to these provisions are ongoing from and after the effective date of the contract through the termination date thereof. Accordingly, the Contractor shall have an obligation to inform the Commonwealth if, at any time during the term of the Contract, it becomes delinquent in the payment of taxes, or other Commonwealth obligations, or if it or any of its subcontractors are suspended or debarred by the Commonwealth, the federal government, or any other state or governmental entity. Such

notification shall be made within 15 days of the date of suspension or debarment.

(d) The failure of the Contractor to notify the Commonwealth of its suspension or debarment by the Commonwealth, any other state, or the federal government shall constitute an event of default of the Contract with the Commonwealth.

(e) The Contractor agrees to reimburse the Commonwealth for the reasonable costs of investigation incurred by the Office of State Inspector General for investigations of the Contractor's compliance with the terms of this or any other agreement between the Contractor and the Commonwealth, which results in the suspension or debarment of the Contractor. Such costs shall include, but shall not be limited to, salaries of investigators, including overtime; travel and lodging expenses; and expert witness and documentary fees. The Contractor shall not be responsible for investigative costs for investigations that do not result in the Contractor's suspension or debarment.

(f) The Contractor may obtain a current list of suspended and debarred Commonwealth contractors by either searching the internet at *http://www.dgs.state.pa.us* or contacting the:

Department of General Services
Office of Chief Counsel
603 North Office Building
Harrisburg, PA 17125
Telephone No. (717) 783-6472
FAX No. (717) 787-9138

48. OFFSET PROVISION FOR COMMONWEALTH CONTRACTS

The Contractor agrees that the Commonwealth may set off the amount of any state tax liability or other obligation of the Contractor or its subsidiaries to the Commonwealth against any payments due the Contractor under any contract with the Commonwealth.

49. TAXES-FEDERAL, STATE, AND LOCAL

(a) **Commonwealth Exemption**. No taxes from which the Commonwealth is exempt shall be included in the Fee. The Commonwealth is exempt from all excise taxes imposed by the Internal Revenue Service and has accordingly registered with the Internal Revenue Service to make tax-free purchases under registration No. 23-23740001-K. With the exception of purchases of the following items, no exemption certificates are required and none will be issued: undyed diesel fuel, tires, trucks, gas-guzzler emergency vehicles, and sports fishing equipment. The Commonwealth is also exempt from Pennsylvania sales tax, local sales tax, public transportation assistance taxes, and fees and vehicle rental tax. The Department of Revenue regulations provide that exemption

certificates are not required for sales made to governmental entities and none will be issued.

(b) **Contractor Taxes**. Fees are inclusive of any applicable sales, use, personal property and other taxes attributable to periods on or after the Effective Date and based upon or measured by Contractor's cost in acquiring or providing equipment, materials, supplies or services furnished or used by Contractor in performing or furnishing the Services, including without limitation, all personal property and use taxes, if any, due on Contractor Machines.

(c) **Segregation of Fees**. Commonwealth and Contractor shall cooperate to segregate the Fees into the following separate payment streams: (1) those for Services, and (2) those for which Contractor functions merely as a paying agent for Commonwealth in receiving goods, supplies, or services (including leasing and licensing arrangements).

50. POLICIES AND PROCEDURES

Contractor shall comply with the most stringent of:

(a) Commonwealth standards set out in IT Bulletins, standards and procedures related to the Services, including but not limited to those governing security, treatment of personal information, quality, change, and problem management, safety, data privacy and data security, and pervasive and transaction controls; provided, however that the Contractor may submit a request under *Section 27* (Change Control), if it believes that it has incurred costs or delay in complying with this Section due to changes in the IT Bulletins, standards and procedures related to the Services; or

(b) The policies, standard and procedures that are generally adopted by leading providers of Services similar in scope, scale and geographic coverage to the outsourced Services.

51. AUDIT OBLIGATIONS

(a) SINGLE AUDIT ACT OF 1984

In compliance with the *Single Audit Act of 1984*, the Contractor agrees to the following:

(1) This Contract is subject to audit by federal and state agencies or their authorized representative in accordance with the auditing standards promulgated by the Comptroller General of the United States and specified in *Government Auditing Standards*, 1994 Revisions (Yellow Book).

(2) The audit requirement of this Contract will be satisfied if a single audit is performed under the provisions of the *Single Audit Act of 1984, 31 U.S.C.* § *7501, et seq.,* and all rules and regulations promulgated pursuant to the Act.

(3) The Commonwealth reserves the right for federal and state agencies or their authorized representatives to perform additional audits of a financial/compliance, economy/efficiency, or program results nature, if deemed necessary.

(4) The Contractor further agrees to comply with requirements that may be issued by the state agency upon receipt of additional guidance received from the federal government regarding the *Single Audit Act of 1984.*

(b) Access by Commonwealth

(1) **Processing**. Upon reasonable written notice from Commonwealth, Contractor and Contractor Agents shall provide such auditors and inspectors with access to the Services Locations and the Software and the Machines for the purpose of performing audits or inspections of the Services and the operations of Commonwealth and Contractor, subject always to Contractor's reasonable security requirements. Contractor shall provide, and shall cause Contractor Agents to provide, to such auditors and inspectors any reasonable assistance that they may require. If any such audit results in Contractor being notified that it or any Contractor Agent is not in compliance with any law, regulation, audit requirement or generally accepted accounting principle relating to the Services, Contractor shall, and shall cause such Contractor Agent to, promptly take actions to comply with such law, regulation, audit requirement or generally accepted accounting principle. Commonwealth shall bear the expense of any such compliance that is (1) required by a law, regulation or other audit requirement relating to Commonwealth's operations to the extent the same was first enacted on or after the Effective Date or (2) necessary due to Commonwealth's noncompliance with any law, regulation or audit requirement imposed on Commonwealth. Contractor shall bear the expense of any such response that is (1) required by a law, regulation or other audit requirement relating to Contractor's business or enacted prior to the Effective Date, (2) to be performed by Contractor as part of the Services, or (3) necessary due to Contractor's noncompliance with any law, regulation or audit requirement imposed on Contractor. As part of the Services, Contractor shall provide to Commonwealth summary data of those portions of Contractor's and Contractor Agents' internal audit reports relating solely to the Services.

(2) **Fees**. Upon reasonable written notice from Commonwealth, Contractor shall provide such auditors and inspectors with access to such financial records and supporting documentation as may reasonably be requested by Commonwealth, and such auditors and inspectors may audit the Fees charged to Commonwealth to determine that such Fees are accurate and in accordance with this Contract.

(3) **Overcharges**. If, as a result of such audit, Commonwealth determines that Contractor has overcharged Commonwealth, Commonwealth shall notify Contractor of the amount of such overcharge and Contractor shall promptly pay to Commonwealth the amount of the overcharge, plus interest at the rate of six percent (6%) per annum, calculated from the date of receipt by Contractor of the overcharged amount until the date of repayment to Commonwealth. In the event any such audit reveals an overcharge to Commonwealth during any calendar month during the Term exceeding fifteen percent (15%) of all Fees in the aggregate paid by Commonwealth in respect of such calendar month, Contractor shall reimburse Commonwealth for the cost of such audit. If as a result of such audit, Commonwealth or Contractor determines that Contractor has undercharged Commonwealth, Commonwealth shall promptly pay to Contractor the amount of such undercharge, without interest. Any disagreement between the parties with regard to the results of any such audit shall be treated as a dispute between the parties subject to the provisions of *Section 34* (Contract Controversies).

(4) **Record Retention**. As part of the Services, Contractor shall (1) retain records and supporting documentation sufficient to document the Services and the Fees paid or payable by Commonwealth under this Contract for at least three (3) years after the expiration or termination of this Contract or until all questioned items relating to such records and documentation are resolved by the parties, whichever is later, and (2) upon notice from Commonwealth, provide such auditors and inspectors as are designated by Commonwealth with reasonable access to such records and documentation for inspection, audit and reproduction. Such records and documentation shall be in such detail as will properly reflect, in accordance with generally accepted accounting principles, all charges claimed under the provisions of this Contract. Any such records which relate to litigation or the settlement of claims arising out of the performance of this Contract, or any Fees as to which exception has been taken by the auditors, shall be retained by Contractor until such litigation, claims, or exceptions have been finally resolved. Such audit shall not require Contractor to disclose cost, profit and overhead data, including direct and indirect rates,

markups, profit margins or confidential employee records or other trade secret information.

(5) **Inclusion in Subcontracts**. The provisions of this *Section 51* (Audit Obligations), except for *Section 51(b)3*, shall be applicable to and included in each subcontract under this Contract.

52. VIRUS AND MALICIOUS CODE

(a) The Contractor shall be liable for any damage to any data and/or software owned or licensed by the Commonwealth if the Contractor or any of its employees, subcontractors or consultants introduces a virus or malicious, mischievous or destructive programming into the Commonwealth's software or computer networks and has failed to comply with the Commonwealth software security standards. The Commonwealth must demonstrate that the Contractor or any of its employees, subcontractors or consultants introduced the virus or malicious, mischievous or destructive programming. The Contractor's liability shall cease if the Commonwealth has not fully complied with its own software security standards.

(b) The Contractor shall be liable for any damages incurred by the Commonwealth including, but not limited to, the expenditure of Commonwealth funds to eliminate or remove a computer virus or malicious, mischievous or destructive programming that result from the Contractor's failure to take proactive measures to keep virus or malicious, mischievous or destructive programming from originating from the Contractor or any of its employees, subcontractors or consultants through appropriate firewalls and maintenance of anti-virus software and software security updates (such as operating systems security patches, etc.).

(c) In the event of destruction or modification of software, the Contractor shall eliminate the virus, malicious, mischievous or destructive programming, restore the Commonwealth's software, and be liable to the Commonwealth for any resulting damages.

(d) The Contractor shall be responsible for reviewing Commonwealth software security standards and complying with those standards.

(e) The Commonwealth may, at any time, audit, by a means deemed appropriate by the Commonwealth, any computing devices being used by representatives of the Contractor to provide Services to the Commonwealth for the sole purpose of determining whether those devices have anti-virus software with current virus signature files and the current minimum operating system patches or workarounds have been installed. Devices found to be out of compliance will immediately be disconnected and will not be permitted to connect or reconnect to the Commonwealth network until the proper installations have been made.

(f) The Contractor may use the anti-virus software used by the Commonwealth to protect Contractor's computing devices used in the course of providing services to the Commonwealth. It is understood that the Contractor may not install the software on any computing device not being used to provide services to the Commonwealth, and that all copies of the software will be removed from all devices upon termination of this Contract.

(g) The Commonwealth will not be responsible for any damages to the Contractor's computers, data, software, etc. caused as a result of the installation of the Commonwealth's anti-virus software or monitoring software on the Contractor's computers.

53. THE AMERICANS WITH DISABILITIES ACT

During the term of this Contract, the Contractor agrees as follows:

(h) Pursuant to federal regulations promulgated under the authority of *The Americans With Disabilities Act*, 28 C.F.R.§ 35.101, *et seq*., the Contractor understands and agrees that no individual with a disability shall, on the basis of the disability, be excluded from participation in this Contract or from activities provided for under this Contract. As a condition of accepting and executing this Contract, the Contractor agrees to comply with the *General Prohibitions Against Discrimination*, 28 C.F.R. § 35.130, and all other regulations promulgated under Title II of *The Americans With Disabilities Act* which are applicable to the benefits, services, programs, and activities provided by the Commonwealth of Pennsylvania through Contracts with outside Contractors.

(i) The Contractor shall be responsible for and agrees to indemnify and hold harmless the Commonwealth of Pennsylvania from losses, damages, expenses claims, demands, suits, and actions brought by any party against the Commonwealth of Pennsylvania as a result of the Contractor's failure to comply with the provisions of subsection (a) above.

54. NONDISCRIMINATION CLAUSE/SEXUAL HARASSMENT CLAUSE

The Contractor agrees:

(a) In the hiring of any employee(s) for the manufacture of supplies, performance of work, or any other activity required under the contract or any subcontract, the Contractor, each subcontractor, or any person acting on behalf of the Contractor or subcontractor shall not, by reason of gender, race, creed, or color, discriminate against any citizen of this Commonwealth who is qualified and available to perform the work to which the employment relates.

(b) Neither the Contractor nor any subcontractor nor any person on their behalf shall in any manner discriminate against or intimidate any employee involved

in the manufacture of supplies, the performance of work, or any other activity required under the contract on account of gender, race, creed, or color.

(c) The Contractor and each subcontractor shall establish and maintain a written sexual harassment policy and shall inform their employees of the policy. The policy must contain a notice that sexual harassment will not be tolerated and employees who practice it will be disciplined.

(d) The Contractor and each subcontractor shall not discriminate by reason of gender, race, creed, or color against any subcontractor or supplier who is qualified to perform the work to which the contracts relates.

(e) The Contractor and each subcontractor shall, within the time periods requested by the Commonwealth, furnish all necessary employment documents and records and permit access to their books, records, and accounts by the contracting agency and the Bureau of Small Business Opportunities (BSBO), for purpose of ascertaining compliance with provisions of this Nondiscrimination/Sexual Harassment Clause. Within fifteen (15) days after award of any contract, the Contractor shall be required to complete, sign and submit Form STD-21, the "Initial Contract Compliance Data" form. If the contract is a construction contract, then the Contractor shall be required to complete, sign and submit Form STD-28, the "Monthly Contract Compliance Report for Construction Contractors", each month no later than the 15th of the month following the reporting period beginning with the initial job conference and continuing through the completion of the project. Those contractors who have fewer than five employees or whose employees are all from the same family or who have completed the Form STD-21 within the past 12 months may, within the 15 days, request an exemption from the Form STD-21 submission requirement from the contracting agency.

(f) The Contractor shall include the provisions of this Nondiscrimination/Sexual Harassment Clause in every subcontract so that those provisions applicable to subcontractors will be binding upon each subcontractor.

(g) The Commonwealth may cancel or terminate the contract and all money due or to become due under the contract may be forfeited for a violation of the terms and conditions of this Nondiscrimination/Sexual Harassment Clause. In addition, the agency may proceed with debarment or suspension and may place the Contractor in the Contractor Responsibility File.

55. CONTRACTOR INTEGRITY PROVISIONS

It is essential that those who seek to contract with the Commonwealth of Pennsylvania observe high standards of honesty and integrity. They must conduct themselves in a manner that fosters public confidence in the integrity of the Commonwealth procurement process.

In furtherance of this policy, Contractor agrees to the following:

(a) Contractor shall maintain the highest standards of honesty and integrity during the performance of this contract and shall take no action in violation of state or federal laws or regulations or any other applicable laws or regulations, or other requirements applicable to Contractor or that govern contracting with the Commonwealth.

(b) Contractor shall establish and implement a written business integrity policy, which includes, at a minimum, the requirements of these provisions as they relate to Contractor employee activity with the Commonwealth and Commonwealth employees, and which is distributed and made known to all Contractor employees.

(c) Contractor, its affiliates, agents and employees shall not influence, or attempt to influence, any Commonwealth employee to breach the standards of ethical conduct for Commonwealth employees set forth in the *Public Official and Employees Ethics Act, 65 Pa.C.S. §§1101 et seq.*; the *State Adverse Interest Act, 71 P.S. §776.1 et seq.*; and the *Governor's Code of Conduct, Executive Order 1980-18, 4 Pa. Code §7.151 et seq.*, or to breach any other state or federal law or regulation.

(d) Contractor, its affiliates, agents and employees shall not offer, give, or agree or promise to give any gratuity to a Commonwealth official or employee or to any other person at the direction or request of any Commonwealth official or employee.

(e) Contractor, its affiliates, agents and employees shall not offer, give, or agree or promise to give any gratuity to a Commonwealth official or employee or to any other person, the acceptance of which would violate the *Governor's Code of Conduct, Executive Order 1980-18, 4 Pa. Code §7.151 et seq.* or any statute, regulation, statement of policy, management directive or any other published standard of the Commonwealth.

(f) Contractor, its affiliates, agents and employees shall not, directly or indirectly, offer, confer, or agree to confer any pecuniary benefit on anyone as consideration for the decision, opinion, recommendation, vote, other exercise of discretion, or violation of a known legal duty by any Commonwealth official or employee.

(g) Contractor, its affiliates, agents, employees, or anyone in privity with him or her shall not accept or agree to accept from any person, any gratuity in connection with the performance of work under the contract, except as provided in the contract.

(h) Contractor shall not have a financial interest in any other contractor, subcontractor, or supplier providing services, labor, or material on this project, unless the financial interest is disclosed to the Commonwealth in writing and the Commonwealth consents to Contractor's financial interest prior to Commonwealth execution of the contract. Contractor shall disclose the financial interest to the Commonwealth at the time of bid or proposal submission, or if no bids or proposals are solicited, no later than Contractor's submission of the contract signed by Contractor.

(i) Contractor, its affiliates, agents and employees shall not disclose to others any information, documents, reports, data, or records provided to, or prepared by, Contractor under this contract without the prior written approval of the Commonwealth, except as required by the *Pennsylvania Right-to-Know Law, 65 P.S. §§ 67.101-3104*, or other applicable law or as otherwise provided in this contract. Any information, documents, reports, data, or records secured by Contractor from the Commonwealth or a third party in connection with the performance of this contract shall be kept confidential unless disclosure of such information is:

(1) Approved in writing by the Commonwealth prior to its disclosure; or

(2) Directed by a court or other tribunal of competent jurisdiction unless the contract requires prior Commonwealth approval; or

(3) Required for compliance with federal or state securities laws or the requirements of national securities exchanges; or

(4) Necessary for purposes of Contractor's internal assessment and review; or

(5) Deemed necessary by Contractor in any action to enforce the provisions of this contract or to defend or prosecute claims by or against parties other than the Commonwealth; or

(6) Permitted by the valid authorization of a third party to whom the information, documents, reports, data, or records pertain: or

(7) Otherwise required by law.

(j) Contractor certifies that neither it nor any of its officers, directors, associates, partners, limited partners or individual owners has been officially notified of, charged with, or convicted of any of the following and agrees to immediately notify the Commonwealth agency contracting officer in writing if and when it or any officer, director, associate, partner, limited partner or individual owner has been officially notified of, charged with, convicted of, or officially notified of a governmental determination of any of the following:

(1) Commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements or receiving stolen property.

(2) Commission of fraud or a criminal offense or other improper conduct or knowledge of, approval of or acquiescence in such activities by Contractor or any affiliate, officer, director, associate, partner, limited partner, individual owner, or employee or other individual or entity associated with:

i. obtaining;

ii. attempting to obtain; or

iii. performing a public contract or subcontract.

Contractor's acceptance of the benefits derived from the conduct shall be deemed evidence of such knowledge, approval or acquiescence.

(3) Violation of federal or state antitrust statutes.

(4) Violation of any federal or state law regulating campaign contributions.

(5) Violation of any federal or state environmental law.

(6) Violation of any federal or state law regulating hours of labor, minimum wage standards or prevailing wage standards; discrimination in wages; or child labor violations.

(7) Violation of the *Act of June 2, 1915 (P.L.736, No. 338),* known as the *Workers' Compensation Act*, 77 P.S. 1 *et seq.*

(8) Violation of any federal or state law prohibiting discrimination in employment.

(9) Debarment by any agency or department of the federal government or by any other state.

(10) Any other crime involving moral turpitude or business honesty or integrity.

Contractor acknowledges that the Commonwealth may, in its sole discretion, terminate the contract for cause upon such notification or when the Commonwealth otherwise learns that Contractor has been officially notified, charged, or convicted.

(k) If this contract was awarded to Contractor on a non-bid basis, Contractor must, (as required by *Section 1641* of the *Pennsylvania Election Code*) file a report of political contributions with the Secretary of the Commonwealth on or before February 15 of the next calendar year. The report must include an itemized list of all political contributions known to Contractor by virtue of the knowledge possessed by every officer, director, associate, partner, limited partner, or individual owner that has been made by:

(1) Any officer, director, associate, partner, limited partner, individual owner or members of the immediate family when the contributions exceed an aggregate of one thousand dollars ($1,000) by any individual during the preceding year; or

(2) Any employee or members of his immediate family whose political contribution exceeded one thousand dollars ($1,000) during the preceding year.

To obtain a copy of the reporting form, Contractor shall contact the Bureau of Commissions, Elections and Legislation, Division of Campaign Finance and Lobbying Disclosure, Room 210, North Office Building, Harrisburg, PA 17120.

(l) Contractor shall comply with requirements of the *Lobbying Disclosure Act, 65 Pa.C.S. § 13A01 et seq.*, and the regulations promulgated pursuant to that law. Contractor employee activities prior to or outside of formal Commonwealth procurement communication protocol are considered lobbying and subjects the Contractor employees to the registration and reporting requirements of the law. Actions by outside lobbyists on Contractor's behalf, no matter the procurement stage, are not exempt and must be reported.

(m) When Contractor has reason to believe that any breach of ethical standards as set forth in law, the Governor's Code of Conduct, or in these provisions has occurred or may occur, including but not limited to contact by a Commonwealth officer or employee which, if acted upon, would violate such ethical standards, Contractor shall immediately notify the Commonwealth contracting officer or Commonwealth Inspector General in writing.

(n) Contractor, by submission of its bid or proposal and/or execution of this contract and by the submission of any bills, invoices or requests for payment pursuant to the contract, certifies and represents that it has not violated any of these contractor integrity provisions in connection with the submission of the bid or proposal, during any contract negotiations or during the term of the contract.

(o) Contractor shall cooperate with the Office of Inspector General in its investigation of any alleged Commonwealth employee breach of ethical standards and any alleged Contractor non-compliance with these provisions. Contractor agrees to make identified Contractor employees available for interviews at reasonable times

and places. Contractor, upon the inquiry or request of the Office of Inspector General, shall provide, or if appropriate, make promptly available for inspection or copying, any information of any type or form deemed relevant by the Inspector General to Contractor's integrity and compliance with these provisions. Such information may include, but shall not be limited to, Contractor's business or financial records, documents or files of any type or form that refers to or concern this contract.

(p) For violation of any of these Contractor Integrity Provisions, the Commonwealth may terminate this and any other contract with Contractor, claim liquidated damages in an amount equal to the value of anything received in breach of these provisions, claim damages for all additional costs and expenses incurred in obtaining another contractor to complete performance under this contract, and debar and suspend Contractor from doing business with the Commonwealth. These rights and remedies are cumulative, and the use or non-use of any one shall not preclude the use of all or any other. These rights and remedies are in addition to those the Commonwealth may have under law, statute, regulation, or otherwise.

(q) For purposes of these Contractor Integrity Provisions, the following terms shall have the meanings found in this Section (q).

(1) "Confidential information" means information that a) is not already in the public domain; b) is not available to the public upon request; c) is not or does not become generally known to Contractor from a third party without an obligation to maintain its confidentiality; d) has not become generally known to the public through an act or omission of Contractor; or e) has not been independently developed by Contractor without the use of confidential information of the Commonwealth.

(2) **"**Consent" means written permission signed by a duly authorized officer or employee of the Commonwealth, provided that where the material facts have been disclosed, in writing, by pre-qualification, bid, proposal, or contractual terms, the Commonwealth shall be deemed to have consented by virtue of execution of this contract.

(3) **"**Contractor" means the individual or entity that has entered into this contract with the Commonwealth, including those directors, officers, partners, managers, and owners having more than a five percent interest in Contractor.

(4) "Financial interest" means:

i. Ownership of more than a five percent interest in any business; or

ii. Holding a position as an officer, director, trustee, partner, employee, or holding any position of management.

(5) "Gratuity" means tendering, giving or providing anything of more than nominal monetary value including, but not limited to, cash, travel, entertainment, gifts, meals, lodging, loans, subscriptions, advances, deposits of money, services, employment, or contracts of any kind. The exceptions set forth in the *Governor's Code of Conduct, Executive Order 1980-18*, the *4 Pa. Code §7.153(b)*, shall apply.

(6) "Immediate family" means a spouse and any unemancipated child.

(7) "Non-bid basis" means a contract awarded or executed by the Commonwealth with Contractor without seeking bids or proposals from any other potential bidder or offeror.

(8) "Political contribution" means any payment, gift, subscription, assessment, contract, payment for services, dues, loan, forbearance, advance or deposit of money or any valuable thing, to a candidate for public office or to a political committee, including but not limited to a political action committee, made for the purpose of influencing any election in the Commonwealth of Pennsylvania or for paying debts incurred by or for a candidate or committee before or after any election.

56. RIGHT-TO-KNOW LAW

(a) The Pennsylvania Right-to-Know Law, 65 P.S. §§ 67.101-3104, ("RTKL") applies to this Contract.

(b) If the Commonwealth requires the Contractor's assistance in any matter arising out of the RTKL related to this Contract, it shall notify the Contractor using the legal contact information provided in this Contract. The Contractor, at any time, may designate a different contact for such purpose upon reasonable prior written notice to the Commonwealth.

(c) Upon written notification from the Commonwealth that it requires the Contractor's assistance in responding to a request under the RTKL for information related to this Contract that may be in the Contractor's possession, constituting, or alleged to constitute, a public record in accordance with the RTKL ("Requested Information"), the Contractor shall:

(1) Provide the Commonwealth, within ten (10) calendar days after receipt of written notification, access to, and copies of, any document or information in the Contractor's possession arising out of this Contract that the Commonwealth reasonably believes is Requested Information and may be a public record under the RTKL; and

(2) Provide such other assistance as the Commonwealth may reasonably request, in order to comply with the RTKL with respect to this Contract.

(d) If the Contractor considers the Requested Information to include a request for a Trade Secret or Confidential Proprietary Information, as those terms are defined by the RTKL, or other information that the Contractor considers exempt from production under the RTKL, the Contractor must notify the Commonwealth and provide, within seven (7) calendar days of receiving the written notification, a written statement signed by a representative of the Contractor explaining why the requested material is exempt from public disclosure under the RTKL.

(e) The Commonwealth will rely upon the written statement from the Contractor in denying a RTKL request for the Requested Information unless the Commonwealth determines that the Requested Information is clearly not protected from disclosure under the RTKL. Should the Commonwealth determine that the Requested Information is clearly not exempt from disclosure, the Contractor shall provide the Requested Information within five (5) business days of receipt of written notification of the Commonwealth's determination.

(f) If the Contractor fails to provide the Requested Information within the time period required by these provisions, the Contractor shall indemnify and hold the Commonwealth harmless for any damages, penalties, costs, detriment or harm that the Commonwealth may incur as a result of the Contractor's failure, including any statutory damages assessed against the Commonwealth.

(g) The Commonwealth will reimburse the Contractor for any costs associated with complying with these provisions only to the extent allowed under the fee schedule established by the Office of Open Records or as otherwise provided by the RTKL if the fee schedule is inapplicable.

(h) The Contractor may file a legal challenge to any Commonwealth decision to release a record to the public with the Office of Open Records, or in the Pennsylvania Courts, however, the Contractor shall indemnify the Commonwealth for any legal expenses incurred by the Commonwealth as a result of such a challenge and shall hold the Commonwealth harmless for any damages, penalties, costs, detriment or harm that the Commonwealth may incur as a result of the Contractor's failure, including any statutory damages assessed against the Commonwealth, regardless of the outcome of such legal challenge. As between the parties, the Contractor agrees to waive all rights or remedies that may be available to it as a result of the Commonwealth's disclosure of Requested Information pursuant to the RTKL.

(i) The Contractor's duties relating to the RTKL are continuing duties that survive the expiration of this Contract and shall continue as long as the Contractor has Requested Information in its possession.

57. ENVIRONMENTAL PROTECTION

In carrying out this Contract, the Contractor shall minimize pollution and shall strictly comply with all applicable environmental laws and regulations, including the *Clean Streams Law,* Act of June 22, 1937, as amended; the *Pennsylvania Solid Waste Management Act,* Act of July 7, 1980 (P.L. 380, No. 97), as amended; and the *Dam Safety and Encroachment Act,* Act of November 26, 1978 (P.L. 1375, No. 325), as amended.

58. ASSIGNABILITY

(a) This Contract may not be assigned by Contractor, either in whole or in part without the prior written consent of the Commonwealth, which consent shall not be unreasonably withheld, conditioned, or delayed. Transfer of the majority of the stock or the majority of the assets of a corporation, or other change of ownership will be deemed an assignment. In the event that Contractor requests the right to assign this Contract, including an assignment to an affiliate or subsidiary, Contractor will provide the Commonwealth with copies of the following documents (to the extent they exist): most recent audited financial statements and such other documents as Commonwealth reasonably deems necessary. Within thirty (30) days of such notice, the Commonwealth shall provide its written decision regarding the requested assignment.

(b) Subject to the terms and conditions of this *Section 58* (Assignability), the Contract is binding upon the parties and their respective successors and assigns.

(c) Any assignment consented to by the Commonwealth shall be evidenced by a written assignment agreement executed by the Contractor and its assignee in which the assignee agrees to be legally bound by all of the terms and conditions of the Contract and to assume the duties, obligations, and responsibilities being assigned. In addition, the assignee must execute a contract with the Commonwealth in the same form as this Contract.

(d) Notwithstanding the foregoing, the Contractor may, without the consent of the Commonwealth, assign its rights to payment to be received under the Contract, provided that the Contractor provides written notice of such assignment to the Commonwealth together with a written acknowledgement from the assignee that any such payments are subject to all of the terms and conditions of the Contract.

(e) A change of name by the Contractor, following which the Contractor's federal identification number remains unchanged, is not considered to be an assignment. The Contractor shall give the Commonwealth written notice of any such change of name.

59. INDEPENDENT CAPACITY OF CONTRACTOR

(a) The parties to this Contract agree that the Services performed by the Contractor under the terms of this Contract are performed as an independent contractor and nothing contained in this Contract shall be construed to make either Contractor or Commonwealth partners, joint venturers, principals, agents or employees of the other, except only to the extent that Contractor is expressly appointed under the Contract to act as the agent of Commonwealth and, in those cases, only to the limited extent of such express appointment. No officer, director, employee, agent, affiliate or contractor retained by Contractor to perform work on Commonwealth's behalf hereunder shall be deemed to be an employee, agent or contractor of Commonwealth. Neither party shall have any right, power or authority, express or implied, to bind the other. As between Contractor and Commonwealth, Contractor is solely responsible for payment of all income, disability, withholding and other employment taxes, and all medical benefit premiums, vacation pay, sick pay and other fringe benefits resulting from Contractor's retention of any such officers, directors, employees, agents or contractors.

(b) Except as otherwise provided by the terms of this Contract, the Commonwealth shall have no control over the manner in which the contractual Services are performed by the Contractor, or any subcontractor. Any job specifications or standards of work attached to or incorporated into this Contract or any subcontracting restrictions contained in this Contract shall not be construed as the Commonwealth's direction or control over the manner of the performance of Services provided by the Contractor.

60. THIRD PARTY BENEFICIARIES

Each party intends that this Contract shall not benefit, or create any right or cause of action in or on behalf of, any person or entity other than Commonwealth and Contractor.

61. CERTIFICATION REGARDING SUSPENSION

Contractor certificates that it is not currently under suspension or debarment by Commonwealth, any other state, or the Federal government.

62. SUSPENSION OF SUBCONTRACTORS

If Contractor enters into any subcontracts or employs under this Contract any subcontractor's individuals who are currently suspended or debarred by Commonwealth or the Federal government or who become suspended or debarred by Commonwealth or the Federal government during the term of this Contract or any extensions or renewals thereof, Commonwealth shall have the right to require Contractor to terminate such subcontracts or employment.

63. ASSIGNMENT OF RIGHTS UNDER THE ANTITRUST LAWS

It is recognized that in actual economic practice, overcharges by Contractor's suppliers resulting from violations of state and federal antitrust laws are in fact borne by the Commonwealth. As part of the consideration for the award of this Contract, and intending to be legally bound, the Contractor assigns to the Commonwealth all rights, title, and interest in and to any claims Contractor now has or may hereafter acquire under state and federal antitrust laws relating to the goods and services which are provided by the Contractor under this Contract.

64. SIGNIFICANT EVENTS

Commonwealth requires the right to adjust the scope or volume of Services to be provided in response to an event, or series of events taken together, that have or will have a significant and sustained impact on Commonwealth's demand for the Services, and requires Contractor to equitably adjust the price for the Services to reflect any such changes to the scope or volume of the Services.

65. FORCE MAJEURE

No failure or delay by Contractor in the performance of its obligations pursuant to this Contract shall be deemed a default of this Contract or a ground for termination hereunder (except as provided in this *Section 65* (Force Majeure) to the extent such failure or delay is due to a Force Majeure Event and such Force Majeure Event could not have been prevented by Contractor's reasonable precautions or efforts to mitigate damage. The occurrence of a Force Majeure Event does not limit or otherwise affect Contractor's obligation to provide normal recovery procedures and any disaster recovery services described in *Section 15* (Disaster Recovery and Business Continuity) to the extent such obligations are not directly precluded by the occurrence of that Force Majeure Event. The occurrence of a Force Majeure Event in respect of another customer of Contractor does not constitute a Force Majeure Event under this Contract, except to the extent such customer and Commonwealth experience the same Force Majeure Event at a site shared by Commonwealth and such other customer. The party delayed by a Force Majeure Event shall immediately orally notify the other party (to be confirmed in a written notice within three (3) business days after the inception of such delay) of the occurrence of a Force Majeure Event and describe in reasonable detail the nature of the Force Majeure Event. From and after becoming aware of a Force Majeure Event, the party delayed thereby shall undertake all commercially reasonable measures (including the use of alternative sources for products and services and workaround plans) to mitigate the impact and duration of the Force Majeure Event, and such party shall consistently and diligently prosecute such measures until the Force Majeure Event is relieved. If Contractor does not fulfill its obligations under the immediately preceding sentence and, as a result thereof, such Force Majeure Event precludes Contractor from delivering the Services for more than forty five (45) days, Commonwealth may terminate this Contract for cause under *Section 32(c)*, but without regard to any additional cure periods provided for therein. In any other case in which a Force Majeure Event precludes Contractor from delivering the Services for more than forty-five (45) days (without consideration of any such Services performed from a business recovery center under *Section 15* (Disaster Recovery and Business Continuity)), Commonwealth may

terminate this Contract for convenience under *Section 32(a)*, but without regard to any notice period or additional cure periods provided for therein. In the event of a Force Majeure Event, Contractor shall not increase the Fees under this Contract or charge Commonwealth usage fees in addition to the Fees except for applicable disaster recovery declaration and usage fees in accordance with the provisions of *Section 15* (Disaster Recovery and Business Continuity).

66. CONFLICT OF INTEREST

Contractor, by signing this Contract, covenants that it has no undisclosed public or private interest, direct or indirect, and shall not acquire directly or indirectly any such interest, and that Contractor has no association, direct or indirect, which interest or association does or may conflict in any manner with the performance of the Services or any other obligations of Contractor under this Contract. Any such conflicts shall be disclosed to Commonwealth, and Commonwealth shall determine whether such conflict is cause for termination of this Contract. Contractor further covenants that, in the performance of this Contract, no person having such interest shall be employed by or associated with Contractor.

67. OFFICIALS NOT TO BENEFIT

No official or employee of the Commonwealth and no member of its General Assembly who exercises any functions or responsibilities under this Contract shall participate in any decision relating to this Contract which affects their personal interest or the interest of any corporation, partnership, or association in which they are, directly or indirectly, interested; nor shall any such official or employee of the Commonwealth or member of its General Assembly have any interest, direct or indirect, in this Contract or the proceeds thereof.

68. CONSENTS, APPROVALS, NOTICES AND REQUESTS

Unless otherwise specified in this Contract, all consents, approvals, notices and requests, acceptances or similar actions to be given by either party under this Contract shall not be unreasonably withheld, delayed or conditioned and each party shall make only reasonable requests under this Contract.

69. REQUIRED CONSENTS

The Commonwealth, with reasonable assistance at no additional cost by Contractor and its agents shall obtain all consents, approvals, authorizations, notices, requests and acknowledgements necessary to allow Contractor to use the Commonwealth Software, the Commonwealth Machines and the services under Commonwealth's third party service contracts, all to the extent necessary to enable Contractor to provide the Services to Commonwealth. Commonwealth shall be responsible for all costs and expenses imposed by third parties in connection with obtaining any such consents. Contractor shall obtain all consents, approvals, authorizations, notices, requests and acknowledgements necessary to allow (1) Contractor to use the Contractor Software, the Developed Software and the

Contractor Machines to provide the Services to Commonwealth, and (2) Commonwealth to use the Contractor Software in accordance with the terms of this Contract upon the expiration or termination for any reason of Contractor's obligation to provide the Services or of this Contract. Contractor shall be responsible for all costs and expenses imposed by a third party in connection with any such consents described in the foregoing clause (1). Commonwealth's costs and expenses under the foregoing clause (2) shall be governed by the terms of *Section 40(b).02*. Each party shall cooperate with and assist the other party in obtaining the consents contemplated in this *Section 69* (Required Consents).

70. REQUIREMENTS FOR INFORMATION IN LEGAL PROCEEDINGS

(a) If the Commonwealth notifies Contractor, or Contractor is otherwise aware, that particular Commonwealth Confidential Information may be within attorney-client or work-product privileges of the Commonwealth, then regardless of any applicable exclusions, Contractor (i) shall not disclose such the Confidential Information or take any other action that would result in waiver of such privileges and (ii) shall instruct all Contractor Personnel who may have access to such communications to maintain privileged material as strictly confidential and otherwise protect the Commonwealth privileges.

(b) To the extent requested by the Commonwealth, Contractor shall comply with the Commonwealth's litigation response plan, including policies and procedures to prepare for and respond to discovery requests, subpoenas, investigatory demands, and other requirements for information related to legal and regulatory proceedings, as such plan may be revised from time to time, including preparing for and complying with requirements for preservation and production of data in connection with legal and regulatory proceedings and government investigations. Upon receipt of any request, demand, notice, subpoena, order or other legal information request relating to legal proceedings or investigations by third parties relating to any Materials, the Confidential Information or related Systems in Contractor possession, Contractor shall immediately notify the Commonwealth and provide the Commonwealth with a copy of all documentation of such legal information request, to the extent Contractor legally may do so and shall cooperate with the Commonwealth in responding to such request, demand, notice, subpoena, order or other legal information request.

(c) Contractor's cost of complying with this section shall be at no additional charge to the Commonwealth.

71. EXAMINATION OF RECORDS

The Commonwealth may, at reasonable times and places, audit the books and records of Contractor or its subcontractors to the extent that the books and records relate to the performance of the contract. Contractor shall maintain books and records related to the Contract for a period of three years from the date of final payment under the Contract.

Contractor shall include a requirement in agreements with subcontractors that requires the subcontractor to maintain its records for the same length of time.

72. SURVIVAL

Sections 4, 33, 35, 36, 37, 38, 38, 40, 41, 47, 48, 49, 52, 53, 72 shall survive the expiration or termination of the Contract.

73. SEVERABILITY

If any provision of this Contract is held by a court of competent jurisdiction to be contrary to law, then the remaining provisions of this Contract or the application of such provision to persons or circumstances other than those as to which it is invalid or unenforceable shall not be affected thereby, and each such provision of this Contract shall be valid and enforceable to the extent permitted by law.

74. WAIVER

No delay or omission by either party to exercise any right or power it has under this Contract shall impair or be construed as a waiver of such right or power. A waiver by any party of any breach or covenant shall not be construed to be a waiver of any succeeding breach or any other covenant. All waivers must be in writing and signed by the party waiving its rights.

75. PERIOD OF PERFORMANCE

The Contractor, for the life of this Contract, shall complete all Services as specified under the terms of this Contract. In no event shall the Commonwealth be responsible or liable to pay for any Services provided by the Contractor prior to the Effective Date, and the Contractor hereby waives any claim or cause of action for any such Services.

76. SPECIAL REQUIREMENTS

The Commonwealth reserves the right to purchase Services covered under this Contract through other procurement methods whenever the Commonwealth deems it to be in its best interest.

77. GOVERNING LAW

This Contract shall be interpreted in accordance with and governed by the laws of the Commonwealth of Pennsylvania, without giving effect to its conflicts of law provisions. Except as set forth in *Section 34* (Contract Controversies), Commonwealth and Contractor agree that the courts of the Commonwealth of Pennsylvania and the federal courts of the Middle District of Pennsylvania shall have exclusive jurisdiction over disputes under this Contract and the resolution thereof. Any legal action relating to this Contract must be brought in Dauphin County, Pennsylvania, and the parties agree that jurisdiction and venue in such courts is appropriate.

78. COMPLIANCE WITH LAWS

(a) The Contractor shall comply with all federal, state, and local laws applicable to its work, including, but not limited to, all statutes, regulations and rules that are in effect as of the Effective Date of the Contract and shall procure at its expense all licenses and all permits necessary for the fulfillment of its obligation.

(b) If any existing law, regulation or policy is changed or if any new law, regulation or policy is enacted that affects the Services provided under this Contract, the parties to the Contract shall modify this Contract, via *Section 27* (Change Control), to the extent reasonably necessary to:

(1) Ensure that such Services will be in full compliance with such laws, regulations and/or policies; and

(2) Modify the rates applicable to such Services; and

(3) Address any schedule impacts.

79. SMALL DIVERSE BUSINESS COMMITMENT

Contractor shall meet and maintain the commitments to small diverse businesses in the Small Diverse Business ("SDB") portion of its Proposal. Any proposed change to a SDB commitment must be submitted to the DGS Bureau of Small Business Opportunities ("BSBO"), which will make a recommendation as to a course of action to the Commonwealth Contracting Officer. Contractor shall complete the Prime Contractor's Quarterly Utilization Report and submit it to the Commonwealth Contracting Officer and BSBO within ten (10) workdays at the end of each calendar quarter that the Contract is in effect.

80. ACKNOWLEDGEMENT

Commonwealth and Contractor each acknowledge that the limitations and exclusions contained in this Contract have been the subject of active and complete negotiation between the parties and represent the parties' Contract based upon the level of risk to Commonwealth and Contractor associated with their respective obligations under this Contract and the payments to be made to Contractor and credits to be issued to, and Services to be provided to, Commonwealth pursuant to this Contract. The parties agree that the terms and conditions of this Contract shall not be construed in favor of or against any party by reason of the extent to which any party or its professional advisors participated in the preparation of this Contract.

81. COVENANT OF FURTHER ASSURANCES

Commonwealth and Contractor covenant and agree that, subsequent to the execution and delivery of this Contract and without any additional consideration, each of Commonwealth and Contractor will execute and deliver any further legal instruments and perform any commercially reasonable acts which are or may become necessary to effectuate the purposes of this Contract.

82. COVENANT OF GOOD FAITH

Each Party agrees that, in its respective dealings with the other Party under or in connection with this Contract, it shall act in good faith.

83. AMENDMENTS

No amendment to, or change, waiver, or discharge of, any provision of this Contract shall be valid unless in writing and signed by an authorized representative of the party against which such amendment, change, waiver or discharge is sought to be enforced.

84. ENTIRE CONTRACT

This Contract is the entire Contract between the parties with respect to its subject matter, and there are no other representations, understandings or Contracts between the parties relative to such subject matter

APPENDIX A - BUSINESS ASSOCIATE APPENDIX LANGUAGE

COMMONWEALTH OF PENNSYLVANIA
BUSINESS ASSOCIATE AGREEMENT

WHEREAS, the ***[name of program and/or Department]*** (Covered Entity) and Contractor (Business Associate) intend to protect the privacy and security of certain Protected Health Information (PHI) to which Business Associate may have access in order to provide goods or services to or on behalf of Covered Entity, in accordance with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5 (Feb. 17, 2009), the HIPAA Privacy Rule (Privacy Rule), 45 C.F.R. Parts 160 and 164, and the HIPAA Security Rule (Security Rule), 45 C.F.R. Parts 160, 162 and 164, and all other applicable laws; and

WHEREAS, Business Associate may receive PHI from Covered Entity, or may create or obtain PHI from other parties for use on behalf of Covered Entity, which PHI can be used or disclosed only in accordance with this Agreement and the standards established by applicable laws; and

WHEREAS, Business Associate may receive PHI from Covered Entity, or may create or obtain PHI from other parties for use on behalf of Covered Entity that is in electronic form, which PHI must be handled in accordance with this Agreement and the standards established by HIPAA and the Security Rule and other applicable laws; and

NOW, THEREFORE, the parties to this Agreement set forth the following as the terms and conditions of their understanding.

1. Definitions.

a) "Breach" shall have the meaning assigned to such term at 42 USCS § 17921 and HIPAA regulations at 45 C.F.R. § 164.402.

b) "Business Associate" shall have the meaning given to such term under the Privacy and Security Rules, including but not limited to, 45 C.F.R. §160.103.

c) "Covered Entity" shall have the meaning given to such term under the Privacy and Security Rules, including, but not limited to, 45 C.F.R. §160.103.

d) "HIPAA" shall mean the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191.

e) "Privacy Rule" shall mean the standards for privacy of individually identifiable health information in 45 C.F.R. Parts 160 and 164.

f) "Protected Health Information" or "PHI" shall have the meaning given to such term under HIPAA and the HIPAA Regulations in 45 C.F.R. Parts 160, 162 and 164, including, but not limited to 45 C.F.R. §160.103.

g) "Security Rule" shall mean the security standards in 45 C.F.R. Parts 160, 162 and 164.

h) Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5 (Feb. 17, 2009), the HIPAA Privacy Rule (Privacy Rule), 45 C.F.R. Parts 160 and 164, and the HIPAA Security Rule (Security Rule), 45 C.F.R. Parts 160, 162 and 164.

2. Stated Purposes For Which Business Associate May Use Or Disclose PHI. The Parties hereby agree that Business Associate shall be permitted to use and/or disclose PHI provided by or obtained on behalf of Covered Entity for purposes state in Attachment 1 , except as otherwise stated in this Agreement.

NO OTHER USES OR DISCLOSURES OF PHI ARE PERMITTED.

3. BUSINESS ASSOCIATE OBLIGATIONS:

i) Security and Privacy Provisions Applicable to Business Associate. Business Associate shall abide by the security and privacy provisions applicable to Covered Entities which are made applicable to the Business Associate by 42 USCS § 17931 and 17934.

j) Limits On Use And Further Disclosure Established By Agreement And Law. Business Associate hereby agrees that the PHI provided by, or created or obtained on behalf of Covered Entity shall not be further used or disclosed other than as permitted or required by this Agreement or as Required by Law.

k) Appropriate Safeguards. Business Associate shall establish and maintain appropriate safeguards to prevent any use or disclosure of PHI other than as provided for by this Agreement. Appropriate safeguards shall include implementing administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI that is created, received, maintained, or transmitted on behalf of the Covered Entity.

l) Reports Of Improper Use Or Disclosure. Business Associate hereby agrees that it shall report to the Covered Entity's Privacy Officer, or his designee**,** and the Covered entity's legal office, within two (2) days of discovery any Breach or use or disclosure of PHI not provided for or allowed by this Agreement (unless some more stringent standard applies under this Agreement). Business Associate agrees to conduct reasonable diligence to discover improper use or disclosure of PHI.

Such notification shall be written and shall include the identification of each individual whose unsecured PHI has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, or disclosed during the improper use or disclosure or Breach. An improper use or disclosure or Breach shall be treated as discovered by the Business Associate on the first day on which it is known to the Business Associate (including any person other than the person committing the Breach, that is an employee,

officer, or other agent of the Business Associate) or should reasonably have been known to the Business Associate (or such person) to have occurred.

d) Reports Of Security Incidents. In addition to following the Breach notification requirements in section 13402 of the HITECH Act and related regulations and guidance, Business Associate shall report to Covered Entity's Privacy Officer, or his designee, within two (2) days of discovery any Security Incident of which it becomes aware.

e) Subcontractors And Agents. Business Associate hereby agrees that any time PHI is provided or made available to any subcontractors or agents, Business Associate shall provide only the minimum necessary PHI for the purpose of the covered transaction and shall first enter into a subcontract or contract with the subcontractor or agent that contains the same terms, conditions and restrictions on the use and disclosure of PHI as contained in this Agreement.

f) Right Of Access To PHI. Business Associate hereby agrees to allow an individual who is the subject of PHI maintained in a designated record set, to have access to and copy that individual's PHI within five (5) business days of receiving a written request from the Covered Entity or individual. Business Associate shall provide PHI in the format requested, unless it cannot readily be produced in such format, in which case it shall be provided in standard hard copy. If any individual requests from Business Associate or its agents or subcontractors access to PHI, Business Associate shall notify Covered Entity of same within two (2) business days. Business associate shall further conform with and meet all of the requirements of 45 C.F.R. §164.524, 42 USCS § 17936(e), and other applicable laws.

g) Amendment And Incorporation Of Amendments. Within five (5) business days of receiving a request from Covered Entity for an amendment of PHI maintained in a designated record set, Business Associate shall make the PHI available and incorporate the amendment to enable Covered Entity to comply with 45 C.F.R. §164.526 and other applicable laws. If any individual requests an amendment from Business Associate or its agents or subcontractors, Business Associate shall notify Covered Entity within five (5) business days.

h) Provide Accounting Of Disclosures. Business Associate agrees to maintain a record of all disclosures of PHI in accordance with 45 C.F.R. §164.528, 42 USCS § 17935(c), and other applicable laws. Such records shall include, for each disclosure, the date of the disclosure, the name and address of the recipient of the PHI, a description of the PHI disclosed, the name of the individual who is the subject of the PHI disclosed, the purpose of the disclosure, and shall include disclosures made on or after the date that is six (6) years prior to the request or April 14, 2003, whichever is later. Business Associate shall make such record available to the individual or the Covered Entity within five (5) business days of a request for an accounting of disclosures, or within such other time as may be dictated by applicable law.

i) Access To Books And Records. Business Associate hereby agrees to make its internal practices, books, and records relating to the use or disclosure of PHI received from, or created or received by Business Associate on behalf of the Covered Entity, available to the Secretary of Health and Human Services or designee for purposes of determining compliance with the HIPAA Privacy Regulations.

j) Return Or Destruction Of PHI. At termination of this Agreement, Business Associate hereby agrees to return or destroy all PHI provided by or obtained on behalf of Covered Entity. Business Associate agrees not to retain any copies of the PHI after termination of this Agreement. If return or destruction of the PHI is not feasible, Business Associate agrees to extend the protections of this Agreement to limit any further use or disclosure until such time as the PHI may be returned or destroyed. If Business Associate elects to destroy the PHI, it shall certify to Covered Entity that the PHI has been destroyed.

k) Maintenance of PHI. Notwithstanding Section 5(j) of this Agreement, Business Associate and its subcontractors or agents shall retain all PHI throughout the term of the Agreement and shall continue to maintain the information required under §5(h) of this Agreement for a period of six (6) years after termination of the Agreement, unless Covered Entity and Business Associate agree otherwise.

l) Mitigation Procedures. Business Associate agrees to establish and to provide to Covered Entity upon request, procedures for mitigating, to the maximum extent practicable, any harmful effect from the use or disclosure of PHI in a manner contrary to this Agreement or the Privacy Rule. Business Associate further agrees to mitigate any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of this Agreement or the Privacy Rule.

m) Training. Business Associate will train all members of its workforce on its policies and procedures with respect to PHI as necessary and appropriate for the workforce members to carry out the functions required by this contract.

n) Sanction Procedures. Business Associate agrees that it shall develop and implement a system of sanctions for any employee, subcontractor or agent who violates this Agreement or other applicable laws.

o) Grounds For Breach by Covered Entity. Upon Business Associate's knowledge of a material breach by Commonwealth of this Business Associate Agreement, Business Associate shall notify Commonwealth of such breach and Commonwealth shall have at least thirty (30) days to cure such breach. In the event Commonwealth does not cure the breach~~,~~ Business Associate shall have the right to report the violation to the Secretary. Notwithstanding any other language in this Agreement, the parties agree that termination by the Business Associate is infeasible.

p) Grounds For Breach. Any non-compliance by Business Associate with this Agreement or the Privacy or Security Rules will automatically be considered to be a breach of the Agreement, if Business Associate knew or reasonably should have known of such non-compliance and failed to immediately take reasonable steps to cure the non-compliance. Business Associate shall have thirty (30) days to cure such breach from the date of notice to cure by the Commonwealth. In the event Business Associate does not cure the breach, the Commonwealth shall have the right to immediately terminate this Agreement and the underlying agreement. If termination is infeasible, the Commonwealth shall report the violation to the Secretary.

q) Termination by Commonwealth. Business Associate authorizes termination of this Agreement by the Commonwealth if the Commonwealth determines, in its sole discretion, that the Business Associate has violated a material term of this Agreement.

r) Failure to Perform Obligations. In the event Business Associate fails to perform its obligations under this Agreement, Covered Entity may immediately discontinue providing PHI to Business Associate. Covered Entity may also, at its option, require Business Associate to submit to a plan of compliance, including monitoring by Covered Entity and reporting by Business Associate, as Covered Entity in its sole discretion determines to be necessary to maintain compliance with this Agreement and applicable law.

s) Privacy Practices. The Department will provide and Business Associate shall immediately begin using any applicable form, including but not limited to, any form used for Notice of Privacy Practices, Accounting for Disclosures, or Authorization, upon the effective date designated by the Program or Department. The Department retains the right to change the applicable privacy practices, documents and forms. The Business Associate shall implement changes as soon as practicable, but not later than 45 days from the date of notice of the change.

4. OBLIGATIONS OF COVERED ENTITY:

a) Provision of Notice of Privacy Practices. Covered Entity shall provide Business Associate with the notice of privacy practices that the Covered Entity produces in accordance with applicable laws, as well as changes to such notice.

b) Permissions. Covered Entity shall provide Business Associate with any changes in, or revocation of, permission by individual to use or disclose PHI of which Covered Entity is aware, if such changes affect Business Associate's permitted or required uses and disclosures.

c) Restrictions. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of PHI that the Covered Entity has agreed to in accordance with 45 C.F.R. §164.522 and other applicable laws, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

5. MISCELLANEOUS:

a) Regulatory References. A reference in this Appendix to a section in the Privacy or Security Rules means the section as in effect or as amended as reasonably determined by the Covered Entity.

b) Amendment. The Parties agree to take such action as is necessary to amend this Appendix from time to time as is necessary for the Covered Entity to comply with the requirements of the Privacy and Security Rules and the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.

c) Survival. The respective rights and obligations of Business Associate under section 5(i) of this Appendix shall survive the termination of the Agreement.

d) Interpretation. Any ambiguity in this Appendix shall be resolved to permit Covered Entity to comply with the Privacy and Security Rules as reasonably determined by the Covered Entity.

e) Changes in Law. Business Associate shall comply with all applicable privacy and security rules and regulations, including but not limited to HIPAA regulations and the HITECH Act and HITECH regulations which are now in effect or which take effect during the term of this contract.

Attachment 1 to Commonwealth of Pennsylvania Business Associate Agreement

Permitted Uses and Disclosures
of Protected Health Information

1. Purpose of Disclosure of PHI to Business Associate: To allow _____ to meet the requirements of Agreement # _____.

2. Information to be Disclosed to Business Associate: _____.

Use to Effectuate Purpose of Agreement: _____ may use and disclose PHI to the extent contemplated by Agreement #_____ ,and as permitted by law with Commonwealth approval and

APPENDIX B - PROPOSAL COVER SHEET
COMMONWEALTH OF PENNSYLVANIA
OFFICE OF ADMINISTRATION – OFFICE FOR INFORMATION TECHNOLOGY
RFP# 6100022698

Enclosed in three separately sealed submittals is the proposal of the Offeror identified below for the above-referenced RFP:

Offeror Information:	
Offeror Name	
Offeror Mailing Address	
Offeror Website	
Offeror Contact Person	
Contact Person's Phone Number	
Contact Person's Facsimile Number	
Contact Person's E-Mail Address	
Offeror Federal ID Number	
Offeror SAP/SRM Vendor Number	

Submittals Enclosed and Separately Sealed:	
□	Technical Submittal
□	Disadvantaged Business Submittal
□	Cost Submittal

Signature	
Signature of an official authorized to bind the Offeror to the provisions contained in the Offeror's proposal:	
Printed Name	
Title	

FAILURE TO COMPLETE, SIGN AND RETURN THIS FORM WITH THE OFFEROR'S PROPOSAL MAY RESULT IN THE REJECTION OF THE OFFEROR'S PROPOSAL

□

□□□□□□□□□□□□□□□□□□□□

Name of Client & Project Title	□□□□□□□□□□□□□□□□□□□□

APPENDIX D

DOMESTIC WORKFORCE UTILIZATION CERTIFICATE

DOMESTIC WORKFORCE UTILIZATION CERTIFICATION FOR MULTIPLE AWARD CONTRACTS (07/24/09)

To the extent permitted by the laws and treaties of the United States, this certification will be used by the Agency in making a best value selection for each particular assignment. Each quote will be evaluated for its commitment to use the domestic workforce in the fulfillment of the contract. Maximum consideration will be given to those suppliers who will perform the contracted direct labor exclusively within the geographical boundaries of the United States or within the geographical boundaries of a country that is a party to the World Trade Organization Government Procurement Agreement. Those who propose to perform a portion of the direct labor outside of the United States and not within the geographical boundaries of a party to the World Trade Organization Government Procurement Agreement will receive a correspondingly smaller score for this criterion. In order to be eligible for any consideration for this criterion, suppliers must complete and sign the following certification. This certification will be included as a contractual obligation when the contract is executed. Failure to complete and sign this certification will result in no consideration being given to the supplier for this criterion.

I, _____**[title]** of _____**[name of Contractor]** a _____ **[place of incorporation]** corporation or other legal entity, ("Contractor") located at _____ **[address],** having a Social Security or Federal Identification Number of _____, do hereby certify and represent to the Commonwealth of Pennsylvania ("Commonwealth") (Check **one** of the boxes below):

☐ All of the direct labor performed within the scope of services under the contract will be performed exclusively within the geographical boundaries of the United States or one of the following countries that is a party to the World Trade Organization Government Procurement Agreement: Aruba, Austria, Belgium, Bulgaria, Canada, Chinese Taipei, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hong Kong, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Latvia, Liechtenstein, Lithuania, Luxemburg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Singapore, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, and the United Kingdom

OR

☐ _____ **percent** (_____**%**) **[Contractor must specify the percentage]** of the direct labor performed within the scope of services under the contract will be performed within the geographical boundaries of the United States or within the geographical boundaries of one of the countries listed above that is a party to the World Trade Organization Government Procurement Agreement. Please identify the direct labor performed under the contract that will be performed outside the United States and not within the geographical boundaries of a party to the World Trade Organization Government Procurement Agreement and identify the country where the direct labor will be performed:

_____

_____

[Use additional sheets if necessary]

The Department of General Services **[or other purchasing agency]** shall treat any misstatement as fraudulent concealment of the true facts punishable under Section 4904 of the *Pennsylvania Crimes Code*, Title 18, of Pa. Consolidated Statutes.

Attest or Witness:

_____
Corporate or Legal Entity's Name

_____
Signature/Date

_____
Signature/Date

_____
Printed Name/Title

_____
Printed Name/Title

APPENDIX E

COSTARS PROGRAM QUESTIONNAIRE

COSTARS PROGRAM QUESTIONNAIRE

If your firm is awarded a Contract, does it agree to sell the awarded items/services at the same prices and/or discounts, and in accordance with the contractual terms and conditions, to registered COSTARS Members who elect to participate in the contract? If your answer is "YES", your firm agrees to pay the applicable Administrative Fee ($1500 or $500 for Qualified Small Businesses) at the beginning of each contract year and upon each contract renewal date.

Please Answer: YES _____ NO _____

If you are asserting that your firm is a Qualified Small Business, have you completed, signed and included with your bid the required Department of General Services Small Business Certification form?

Please Answer: YES _____ NO _____

_____

Corporate or Legal Entity Name

_____

Signature/Date

_____

Printed Name/Title

Request for Proposal

RFP # 6100022698

Commonwealth of Pennsylvania
Office of Administration
Office for Information Technology
Data Center Computing Services

Appendix F

NON-DISCLOSURE AGREEMENT

NON-DISCLOSURE AGREEMENT

1. _____ (Company) wishes to receive certain trade secrets, confidential and proprietary information (hereinafter collectively "Information") pertaining to the **Data Center Computing Services RFP 6100022698** (the "RFP"). This exchange includes all communication of Information between the parties in any form whatsoever, including oral, written and machine readable form, pertaining to the above.

2. Company wishes to receive the Information for the sole purpose of submitting a proposal in response to the Commonwealth's RFP.

3. Disclosure of Information by the Commonwealth is in strictest confidence and thus Company understands that it will:

   a) Not disclose to any other person the Information

   b) Use at least the same degree of care to maintain the Information secret as the Company uses in maintaining as secret its own secret information, but always at least a reasonable degree of care;

   c) Use the Information only for the above purposes;

   d) Restrict disclosure of the Information solely to those employees of Company having a need to know such Information in order to accomplish the purpose stated above;

   e) Advise each such employee, before he or she receives access to the Information, of the obligations of Company under this Agreement, and require each such employee to maintain those obligations;

   f) Within fifteen (15) days following request of the Commonwealth, return to the Commonwealth all documentation, copies, notes, diagrams, computer memory media and other materials containing any portion of the Information, or confirm to the Commonwealth, in writing, the destruction of such materials; and

   g) Immediately upon sale of Company or merger of Company with a third party, return to the Commonwealth all documentation, copies, notes, diagrams, computer memory media and other materials containing any portion of the Information, or confirm to the Commonwealth, in writing, the destruction of such materials.

4. This Agreement imposes no obligation on Company with respect to any portion of the Information received from the Commonwealth which (a)(1) was known to the Company prior to disclosure by the Commonwealth and (2) as to which the Company has no obligation not to disclose or use it, (b) is lawfully obtained by the Company from a third party under no obligation of confidentiality, (c) is or becomes generally known or available other than by unauthorized disclosure, (d) is independently developed by the Company or (e) is generally disclosed by the Commonwealth to third parties without any obligation on the third parties.

5. The Information shall remain the sole property of the Commonwealth or the originating agency.

6. In the event of a breach or threatened breach or intended breach of this Agreement by Company, the Commonwealth, in addition to any other rights and remedies available to it at law or in equity, shall be entitled to preliminary and final injunctions, enjoining and restraining such breach or threatened breach or intended breach.

7. Company understands that the Commonwealth may not own the intellectual property rights in all of the information that it provides to Company.

8. The validity, construction, and performance of this Agreement are governed by the laws of the Commonwealth of Pennsylvania.

9. The rights and obligations of the Company under this Agreement may not be sold, assigned or otherwise transferred.

This Agreement is binding upon the Company, and upon the directors, officers, employees and agent of the Company. This Agreement is effective as of the date of execution by the Company and will continue indefinitely, unless terminated on thirty (30) days written notice by either party. However, Company's obligations of confidentiality and restrictions on use of the Information disclosed by Commonwealth shall survive termination of this Agreement.

Signature and Certification by Company

I certify that I have the authority to bind the Company to this Agreement. I have read and understand the certifications and understanding set out in this document. I further understand that I, by signing this document, I make the acknowledgement and certifications and confirm the understandings herein subject to the provisions and penalties of *18 Pa.C.S. Section 4904 (unsworn falsification to authorities).*

Signature (Must be an original ink signature) Date

Trade Secret/Confidential Proprietary Information Notice

Instructions:

The Commonwealth may not assert on behalf of a third party an exception to the public release of materials that contain trade secrets or confidential proprietary information unless the materials are accompanied, at the time they are submitted, by this form or a document containing similar information.

It is the responsibility of the party submitting this form to ensure that all statements and assertions made below are legally defensible and accurate. The Commonwealth will not provide a submitting party any advice with regard to trade secret law.

Name of submitting party:

Contact information for submitting party:

Please provide a brief overview of the materials that you are submitting (e.g. bid proposal, grant application, technical schematics):

Please provide a brief explanation of why the materials are being submitted to the Commonwealth (e.g. response to bid #12345, application for grant XYZ being offered by the Department of Health, documents required to be submitted under law ABC)

Please provide a list detailing which portions of the material being submitted you believe constitute a trade secret or confidential proprietary information, and please provide an explanation of why you think those materials constitute a trade secret or confidential proprietary information. Also, please mark the submitted material in such a way to allow a reviewer to easily distinguish between the parts referenced below. (You may attach additional pages if needed)

Note: The following information will not be considered a trade secret or confidential proprietary information:

- Any information submitted as part of a vendor's cost proposal
- Information submitted as part of a vendor's technical response that does not pertain to specific business practices or product specification
- Information submitted as part of a vendor's technical or disadvantaged business response that is otherwise publicly available or otherwise easily obtained
- Information detailing the name, quantity, and price paid for any product or service being purchased by the Commonwealth

Page Number	Description	Explanation

Acknowledgment

The undersigned party hereby agrees that it has read and completed this form, and has marked the material being submitted in accordance with the instructions above. The undersigned party acknowledges that the Commonwealth is not liable for the use or disclosure of trade secret data or confidential proprietary information that has not been clearly marked as such, and which was not accompanied by a specific explanation included with this form.

The undersigned agrees to defend any action seeking release of the materials it believes to be trade secret or confidential, and indemnify and hold harmless the Commonwealth, its agents and employees, from any judgments awarded against the Commonwealth in favor of the party requesting the materials, and any and all costs connected with that defense. This indemnification survives so long as the Commonwealth has possession of the submitted material, and will apply to all costs unless and until the undersigned provides a written statement or similar notice to the Commonwealth stating that it no longer wishes to exempt the submitted material from public disclosure.

The undersigned acknowledges that the Commonwealth is required to keep all records for at least as long as specified in its published records retention schedule.

The undersigned acknowledges that the Commonwealth reserves the right to reject the undersigned's claim of trade secret/confidential proprietary information if the Commonwealth determines that the undersigned has not met the burden of establishing that the information constitutes a trade secret or is confidential. The undersigned also acknowledges that if only a certain part of the submitted material is found to constitute a trade secret or is confidential, the remainder of the submitted material will become public; only the protected information will be removed and remain nonpublic.

If being submitted electronically, the undersigned agrees that the mark below is a valid electronic signature.

Signature	Title	Date

APPENDIX H

Lobbying Certification Form

Certification for Contracts, Grants, Loans, and Cooperative Agreements

The undersigned certifies, to the best of his or her knowledge and belief, that:

(1) No federal appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of any agency, a member of Congress , an officer or employee of Congress, or an employee of a member of Congress in connection with the awarding of any federal contract, the making of any federal grant, the making of any federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any federal contract, grant, loan, or cooperative agreement.

(2) **If any** funds other than federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a member of Congress, an officer or employee of Congress, or an employee of a member of Congress in connection with this federal contract, grant, loan, or cooperative agreement, the undersigned shall complete and submit Standard Form-LLL, "Disclosure of Lobbying Activities," in accordance with its instructions.

(3) The undersigned shall require that the language of this certification be included in the award documents for all subawards at all tiers (including subcontracts, subgrants, and contracts under grants, loans, and cooperative agreements) and that all subrecipients shall certify and disclose accordingly.

This certification is a material representation of fact upon which reliance is placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed under Section 1352, Title 31, U.S. Code. Any person who fails to file the required certification shall be subject to a civil penalty of not less than $10,000 and not more than **$100,000** for such failure.

SIGNATURE: _____

TITLE: _____

DATE: _____

pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

QUESTIONS SUBMITTAL FORM FOR REQUEST FOR PROPOSAL DATA CENTER COMPUTING SERVICES (6100022698)
Appendix I

I. Vendor Contact Information (please provide contact information for one person responsible for coordinating your responses for this RFP).	
Name of contact	
Name of company	
Contact's title	
Telephone	
Email	

Number	Document	Section	Page Number	Question
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				

pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

QUESTIONS SUBMITTAL FORM FOR REQUEST FOR PROPOSAL DATA CENTER COMPUTING SERVICES (6100022698)

Appendix I

Number	Document	Section	Page Number	Question
14.				
15.				
16.				
17.				
18.				
19.				
20.				
21.				
22.				
23.				
24.				
25.				
26.				
27.				
28.				
29.				
30.				
31.				
32.				

pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

QUESTIONS SUBMITTAL FORM FOR REQUEST FOR PROPOSAL DATA CENTER COMPUTING SERVICES (6100022698)
Appendix I

Number	Document	Section	Page Number	Question
33.				
34.				
35.				
36.				
37.				
38.				
39.				
40.				
41.				
42.				
43.				
44.				
45.				
46.				
47.				
48.				
49.				
50.				

[DATE]

[SDB Contact Name
Title
SDB Company Name
Address
City, State, Zip]

Dear [SDB Contact Name]:

This letter serves as confirmation of the intent of [Offeror] to utilize [Small Diverse Business (SDB)] on RFP [RFP number and Title] issued by the [Commonwealth agency name].

If [Offeror] is the successful vendor, [SDB] shall provide [identify the work, goods or services the SDB will perform, and the timeframe during the term of the contract and any option/renewal periods when the work, goods or services will be performed or provided].

These services represent [identify fixed numerical percentage commitment] of the total amount [Offeror] will be paid under the initial term of the contract. The dollar value that the fixed percentage commitment represents will depend on the final negotiated contract pricing and actual contract usage or volume.

[SDB] represents that it meets the small diverse business requirements set forth in the RFP and all required documentation has been provided to [Offeror] for its SDB submission.

We look forward to the opportunity to serve the [Commonwealth agency name] on this project. If you have any questions concerning our small diverse business commitment, please feel free to contact me at the number below.

Sincerely,

Acknowledged,

Offeror Name	SDB Name
Title	Title
Company	Company
Phone number	Phone number

Request for Proposal

RFP # 6100022698

Commonwealth of Pennsylvania

Office of Administration

Office for Information Technology

Data Center Computing Services

Schedule A
DEFINED TERMS

Table of Contents

ABBREVIATIONS AND ACRONYMS 3
DEFINITIONS 6

Abbreviations and Acronyms

Abbreviation / Acronym	Description
ADA	The Americans With Disabilities Act, 28 C.F.R. § 35.101 et seq.
ADM	Application Development and Maintenance
BSBO	Bureau of Small Business Opportunities
BYOD	Bring Your Own Device
CAB	Change Advisory Board
CCPM	Commonwealth Computing Procedures Manual
CHRIA	Criminal History Record Information Act
CI	Configuration Item
CJIS	Criminal Justice Information Services
CMDB	Configuration Management Database
CMs	Critical Measurements
COPANET	Commonwealth Network
CTC	Commonwealth Technology Center
DBA	Database Administration
DGS	Department of General Services
DGS	Department of General Services
DLI	Department of Labor and Industry
DOC	Department of Corrections
DOH	Department of Health
DOR	Department of Revenue
DOT	Department of Transportation
DPH	Data Power House

Abbreviation / Acronym	Description
DPW	Department of Public Welfare
DR	Disaster Recovery
EDC	Enterprise Data Center
FIPS	Federal Information Processing Standards
FIRPA	Family Educational Rights and Privacy Act
GLBA	Gramm-Leach-Bliley Act of 1999
HIPAA	Health Insurance Portability and Accountability Act
HLE	High Level Estimate
HVAC	Heating, Ventilation, and Air Conditioning
IES	Integrated Enterprise Services
IFL	Integrated Facility for Linux
ITB	Information Technologies Bulletin
ITIL	Information Technology Infrastructure Library
ITSM	Information Technologies Service Management
KM	Key Measurement
KMP	Knowledge Management Portal
LPAR	Logical Partition
OA	Office of Administration
OA/OIT	Office of Administration / Office for Information Technologies
OAG	Office of Attorney General
OIG	Office of Inspector General
PCI	Payment Card Industry
PCI DSS	Payment Card Industry Data Security Standard

Abbreviation / Acronym	Description
PHI	Protected Health Information
PIP	Private IP
PMO	Program Management Office
PSP	Pennsylvania State Police
PUE	Power Usage Effectiveness
RFP	Request For Proposal
RTK	Right-to-Know
RTKL	Right-to-Know Law
RTO	Return To Operations
SDB	Small Diverse Business
SDLC	Systems Development Life Cycle
SLA	Service Level Agreement
SOW	Statement of Work
SOX	Sarbanes-Oxley Act of 2002
SSAE16	Statement on Standards for Attestation Engagements no. 16
TPMO	Transition Program Management Office
UPS	Uninterruptable Power Supply
VRF	Virtual Routing and Forwarding

DEFINITIONS

The following defined terms shall have the meanings specified below:

Term	Definition
24 x 7 x 365	A continuous, non-stop period of time.
Acceptance Criteria	The list of predetermined objectives that define the minimum capabilities or work results that is acceptable to the Commonwealth.
Acceptance Testing Plan	A mutually agreed plan that includes the testing of application infrastructure performance characteristics prior to migrating each of the current application workloads to the Offeror's infrastructure.
Agency Agencies	One or more administration division(s) of the Commonwealth of Pennsylvania.
Application Development and Maintenance (ADM)	The work needed to create, update and maintain software applications.
Application Infrastructure Availability	A Service Level that measures the percentage of time the Applications is available during the applicable Measurement Window. Availability is determined by whether the application residing on any of the associated server instances is available to users as defined within the CMDB.
Assistance Event	A single necessary and appropriate action to accomplish a complete, timely, and seamless transition of any Terminated Services from Offeror to the Commonwealth, or to any replacement provider designated by the Commonwealth, without material interruption of or material adverse impact on the Terminated Services or any other services provided by third-parties or Services that Offeror shall continue to provide
At Risk Amount	The amount that the Offeror will have at risk for all Service Level Credits in each month.
Availability	The time a service or application is fully functional (available) to perform the functions it is designed to produce.
Baseline Data	The actual data measured during a Measurement Period or applicable historical data of the Commonwealth.

Term	Definition
Baseline Security Risk and Vulnerability Assessment	The assessment of must include a roadmap and project plan to make any required security modifications.
Benchmark Results	The details of the Benchmarking Process intended to ensure that Offeror provides Commonwealth with technology and Services at Service Levels equal to or greater than other organizations receiving similar services.
Benchmark Review Period	The period to review such Benchmark Reports to assess the Benchmark Results.
Benchmarker	An independent third-party that undertakes Benchmarking.
Benchmarking	The objective measurement and comparison process (utilizing resource baselines and industry standards) utilized by a Benchmarker to benchmark the quality of the Services and the Fees by Statement of Work or Statement of Works.
Benchmarking Price Protection	The process of an objective measurement and comparison process utilizing baseline methods and industry standards to determine pricing as more fully set forth within Section 25 of Appendix A (Terms and Conditions).
Bureau of Small Business Opportunities (BSBO)	A Bureau within the Commonwealth's Department of General Services responsible for certifying a small diverse businesses as a DGS-certified minority-owned business, woman-owned business, service-disabled veteran-owned business or veteran-owned business, or United States Small Business Administration-certified 8(a) small disadvantaged business concern, that qualifies as a small business.
Business Continuity Plan	The plan set out to continue business operations of the Commonwealth in the event of a declared disaster.
Business Partner	A third party entity that does business with the Commonwealth.
Capacity On Demand	A type of Service that its capacity can be modified in an automated process with a short implementation time.
Card Holder Data	Credit card records or record systems containing cardholder data including credit card numbers.

Term	Definition
Change	An alteration in specifications, services, delivery point, rate of delivery, period of performance, price, or other provisions of the Contract changes accomplished by mutual action of the parties to the Contract.
Change Advisory Board	A group of individuals authorized to approve or reject individual service and infrastructure changes and to set and guide the Change process.
Change Control Procedures	The procedures used to modify sections of the Contract or modify the configuration of an infrastructure component of a Service.
Change Management	The process responsible for controlling the lifecycle of all changes, enabling beneficial changes to be made with minimum interruption to the Services.
Change Order	The documentation used to request, validate, negotiate and approve a change to the sections of the Contract.
Change Proposal	The document presented to the Commonwealth by the Offeror to start the Change Control Procedures.
Change Request	The type of request created and processed within the Commonwealth's ITSM system to request authorization to modify an infrastructure component of a Service.
Co-location	The capability to provide space, power, and cooling to an asset that is not owned by the Offeror.
Comma Separated Values (CSV)	A type of Text file where the values are delineated with a comma.
Commonwealth	The Commonwealth of Pennsylvania.
Commonwealth Computing Procedures Manual (CCPM)	A date detailed description of all processes and procedures used to support the computing needs of the Commonwealth via the Offerors Knowledge/Service Portal. The CCPM contains specific sections dedicated to the operational procedures for each Commonwealth datacenter customer.
Commonwealth Computing Services	The centralized computing capabilities of the Commonwealth that includes Mainframe, Midrange and x86 based servers and the supporting infrastructure.

Term	Definition
Commonwealth Contracting Officer	The person authorized to administer this Contract for the Commonwealth and to make written determinations with respect to the Contract.
Commonwealth Customers	The end users deriving benefits from the services provided from this contract.
Commonwealth Project Manager	The individual within the Commonwealth that is responsible for managing the Contract.
Commonwealth Proprietary Software	The software owned by the Commonwealth.
Commonwealth Technology Center (CTC)	The Commonwealth's datacenter and adjacent offices located at 1 Technology Park Drive, Harrisburg, PA 17110. Also known as "1 Tech Park" or the EDC.
Commonwealth Third Party Software	Third Party Software for which the Commonwealth has a valid license and current maintenance agreement.
Confidential Information.	With regard to the Commonwealth, the data and other information of the Commonwealth or any private individual, organization or public agency, in each case to the extent such information and documentation is not permitted to be disclosed to third parties under local, Commonwealth or Federal laws and regulations or pursuant to any policy adopted by the Commonwealth or pursuant to the terms of any third-party agreement to which Commonwealth is a party. With regard to the Contractor, all Contractor Software and all Contractor documentation and manuals not made available in the ordinary course of business (except those items developed by Contractor specifically to deliver Services to the Commonwealth pursuant to this Contract), and any other information identified in writing by Contractor as confidential or proprietary to Contractor, its subcontractors or licensors.
Confidential Proprietary Information	All Contractor Software and all Contractor documentation and manuals not made available in the ordinary course of business (except those items developed by Contractor specifically to deliver Services to the Commonwealth pursuant to this Contract), and any other information identified in writing by Contractor as confidential or proprietary to Contractor, its subcontractors or licensors.

Term	Definition
Configuration Items (CI)	The database record(s) indicating the interrelationships and configuration of a service, hardware component, application, and software
Configuration Management Database (CMDB)	The repository of configuration information related to all the components of the Offeror's datacenter services solution. It contains the details of each of the configuration items (CI) in the IT infrastructure. The CMDB helps provide the relationships between these components (e.g. Application Infrastructure) and track their configuration. The CMDB is a fundamental component of the ITIL framework's Configuration Management process.
Contract	Means the agreement for provision of Services executed on [ ] between Offeror and Commonwealth of which this document is a part of.
Contractor	*The Offeror awarded the Contract.*
Contractor Software	The software owned by the Contractor.
Contractor Tools	All Tools owned or licensed by Contractor or its agents and used by Contractor or its agents to provide the Services.
COPANET	The Commonwealth's private Fiber network.
Criminal History Record Information Act (CHRIA)	Chapter 91 of the Crimes Code of Pennsylvania and Pennsylvania Consolidated Statues Annotated, 18 Pa. C.S.A. 9101 et. seq.
Criminal Justice Information Services (CJIS)	The policy that provides Criminal Justice Agencies and Noncriminal Justice Agencies with a minimum set of security requirements for the access to Federal Bureau of Investigation Criminal Justice Information Services (CJIS) Division systems and information and to protect and safeguard Criminal Justice Information.
Critical Application	Those applications designated as "Critical Applications" in the Commonwealth Compute Process Manual (CCPM)
Critical Measurements (CM)	Performance measurements defined for the most important service areas

Term	Definition
Critical Services	Those services designated as "Critical Services" in a Commonwealth Compute Process Manual (CCPM)
Data Gathering	The work effort of collecting information to discover and document a process, a procedure, or the configuration of a Service.
Data Power House (DPH)	The Commonwealth accepted term encompassing the current managed datacenter contract, Services, and location.
Database Administration (DBA)	The function of implementing, configuring, monitoring, and troubleshooting structured data in a common platform/application.
Datacenter Architecture	The resulting equipment and associated network infrastructure viewed as an entire collection of services.
Days	Calendar days, unless specifically indicated otherwise.
Degraded Condition	A Service that tests as fully operational but is degraded below user expectations across a significant segment of the user population as determined by the Commonwealth.
Deliverable	A Milestone or Service that is subject to acceptance testing in the Acceptance Testing Plan.
Developed Documentation	Documentation developed by Contractor specifically for the Commonwealth in connection with its performance under this Contract as more fully set forth in Section 40 of Appendix A (Terms and Conditions).
Developed Materials	All literary works, or other works of authorship (such as application programs, listings, programming tools, documentation, reports, drawings, procedure manuals and similar works) developed under the Contract, as more fully set forth in Section 40 of Appendix A (Terms and Conditions)
Disaster Recovery Plan	The plan created to restore Services to the Commonwealth in the event of a declared disaster.
Disaster Recovery (DR)	A series of events to restore a service or equipment in the advent of a major system or network failure, or a natural or man-made event that denies service for an extended period of time.

Term	Definition
Documentation	All written materials, work papers, configurations and manuals (including the CCPM) prepared by or on behalf of the Contractor or any of the Contractor's Agents pursuant to the Contract as more fully set forth in Section 40 of Appendix A (Terms and Conditions)..
Downtime	The duration a service or equipment is not fully functional based on the requirements of the service or equipment.
Earn Back	The Offeror's opportunity to earn back Service Level Credits on Required Service Level Defaults, in accordance with Schedule J.1 (Datacenter Service Level Management)
Effective Date	The date the Commonwealth and the Offeror complete the approval and signature of the resulting Contract for this Procurement, as more fully set forth in Section 1 of Appendix A (Terms and Conditions).
Enterprise Data Center (EDC)	The Commonwealth's datacenter and adjacent offices located at 1 Technology Park Drive, Harrisburg, PA 17110.
Enterprise Remedy	The Commonwealth's ITSM system that manages and tracks the workflows and approvals for Incidents, Changes, Problems, CMDB and SLA's.
Equipment	All computing, networking, telecommunications and other equipment (hardware and firmware) procured, provided, operated, supported, or used by Offeror in connection with the Services, including but not limited to: a) mainframe, midrange, server and distributed computing equipment and associated attachments, features, accessories, peripheral devices and cabling, b) personal computers, laptop computers, workstations and personal data devices and associated attachments, features, accessories, printers, multi-functional printers, peripheral or network devices and cabling, and c) voice, data, video and wireless telecommunications and network and monitoring equipment and associated attachments, features, accessories, cell phones, peripheral devices and cabling.

Term	Definition
ERP systems	Systems that integrate internal and external management information across an entire organization, typically including finance, accounting, sales, service, and customer relationship management, etc.
Expiration Date	The end of the Contract Term, as more fully set forth in Section 1 of Appendix A (Terms and Conditions).
Federal Information Processing Standards (FIPS)	Standards and guidelines that are developed by the National Institute of Standards and Technology (NIST) for Federal computer systems. Under the Information Technology Management Reform Act (Public Law 104-106), the Secretary of Commerce approves standards and guidelines that are developed by the National Institute of Standards and Technology (NIST) for Federal computer systems. These standards and guidelines are issued by NIST as Federal Information Processing Standards (FIPS) for use government-wide. NIST develops FIPS when there are compelling Federal government requirements such as for security and interoperability and there are no acceptable industry standards or solutions.
Fees	The fees and any other amounts payable by Commonwealth to Offeror.
Force Majeure Event	An event or effect that cannot be reasonably anticipated or controlled, as more fully set forth in Section 65 of Appendix A (Terms and Conditions).
High Level Estimate (HLE)	Used when the Commonwealth has a clear technical direction and needs rough estimates on the cost of implementing the Service. HLEs may be used to attach a cost estimate to a prior conceptualization or technical opinion produced by the Offeror.
Hybrid Third Party Software	Third Party Software for which the Commonwealth has a valid license, and except for the cost of the license, the contractor shall have financial, administration, operational and maintenance responsibility.
Improved Technology	Any new commercially available information processing technology developments, including new software and hardware developments, that could reasonably be expected to have a positive impact on the Services in terms of increased efficiency or reduced cost.

Term	Definition
Incident	An ITIL term use to describe a failure or loss of capabilities of a Service where a temporary work around is not available or not in place.
Information Technology Infrastructure Library (ITIL)	A cohesive set of best practices, drawn from the public and private sectors internationally.
Information Technology Service Management (ITSM)	A best practice approach driven both by technology and organizational environments on managing IT services as a whole.
IT Bulletins	Information Technology (IT) bulletins which are issued by the Governor's Office of Administration to set IT policy.
Key Measurements (KMs)	Performance target measurements for non-critical service areas.
Key Personnel	The Offeror's named staff that the Commonwealth determined to be critical to the success of the Project and require the Offeror to provide as defined and governed in Schedule G – Staffing Plan and Key Positions.
Key Positions	The positions that the Commonwealth determined to be critical to the success of the Project and require the Offeror to provide as defined and governed in Schedule G – Staffing Plan and Key Positions
Knowledge/Service Management Portal (KMP)	A software recording tool the Offeror uses to record all incidents, problems, service requests, change requests, and configuration information. All updates to the records, contacts with clients or vendors, and resolutions will be recorded in a real-time and consistent manner.
Management Committee	A committee comprised of ten members, five of whom shall be appointed by Commonwealth and five of whom shall be appointed by Offeror from Offeror's executive management staff.
Market Rate	The average of amounts paid by the reference group for comparable services.

Term	Definition
Measurement Period	The nine (9) consecutive months of measurements during which Baseline Data will be measured, which may be used by the Commonwealth and the Offeror to determine Service Level Target and/or Minimum Service Levels. The Offeror will measure, collect and report to the Commonwealth the relevant measurements during such period.
Measurement Window	Shall mean the periodic evaluation and reporting frequency for each individual Service Level as specified in Schedule J.2 (Datacenter Service Level Matrix) (*e.g.*, monthly, quarterly, semi-annually, annually).
Milestone	A Transition Milestone, Transformation Milestone or Critical Milestone
Milestone Credit	The invoice credits due the Commonwealth if the Offeror fails to attain a Milestone defined in Schedule D - Transition Milestones.
Milestone Credit	The credit to be paid by Offeror for missing a Transition Milestone, as set out in Schedule D (Transition Milestones).
Milestone Due Date	The date the Offeror will not exceed as specified within Schedule D (Transition Milestones).
Monitoring System	The hardware and software used to monitor the performance, capacity, and other events occurring around or within a service provided to the Commonwealth.
OA Service Desk	The department responsible for Tier I troubleshooting support to the end users by taking requests from end-users and performing triage on the request and escalate as necessary
Offeror Personnel	The personnel of Offeror and its Subcontractors who provide or are involved in the provision of the Services.
Offeror Services Locations	The service locations owned, leased or under the control of Offeror or its subcontractors that are set forth in Schedule E (Datacenter Locations).
Offeror's Proposal	The proposal submitted by the selected Offeror in response to the RFP.

Term	Definition
Office of Administration	An organization within the Commonwealth that provides information technology, human resource, records management, and continuity of government services
Office of Attorney General (OAG)	The office of Pennsylvania's top law enforcement official, which has a wide range of responsibility to protect and serve the citizens and agencies of the Commonwealth.
Office of Inspector General	An organization within the Commonwealth that works to prevent or find fraud, waste, and abuse in the Commonwealth's programs, operations, and contracts.
Outage	Any service interruption that is or may be experienced by the end-users of the service, application, or equipment.
P Series Servers	A general reference to the IBM collection of servers that typically operate on the AIX operating system.
Payment Card Industry Data Security Standard (PCI DSS)	An actionable framework for developing a robust payment card data security process -- including prevention, detection and appropriate reaction to security incidents.
Pennsylvania	The Commonwealth of Pennsylvania.
Pennsylvania Election Code	The act of June 3, 1937 (P.L.1333, No.320), known as the Pennsylvania Election Code.
Pennsylvania Right-to-Know Law ("RTKL")	The Pennsylvania Right-to-Know Law, 65 P.S. §§ 67.101-3104.
Power Usage Effectiveness ratio (PUE)	A ratio that represents the amount of power consumption of compute versus the total power consumption of a facility as defined by the Green Grid consortium.
Prevailing Wage Act	The Pennsylvania Prevailing Wage Act (43 P.S. §§ 165-1 through 165-17).
Problem	An ITIL term use to describe a failure or loss of capabilities of a Service where a temporary work around is in place.
Program Management Office (PMO)	The organization with governance, implementation, and management of the overall engagement.

Term	Definition
Project	This Data Center Computing Services procurement and resulting program supporting the Contract that is the results of this procurement.
Protected Health Information (PHI)	The meaning given to such term under HIPAA and the HIPAA Regulations in 45 C.F.R. Parts 160, 162 and 164, including, but not limited to 45 C.F.R. §160.103
Purchase Order	Orders made in accordance with the ordering process set forth in Section 2 of Appendix A (Terms and Conditions).
Regulatory Entity	Any supervisory or governmental agency, body or authority having regulatory or supervisory authority over the Commonwealth, its agencies, the Offeror and subcontractor's assets, resources or business and over the Services, including any organization reporting to such bodies.
Remote Hands Support	Shall mean the Time and Material effort by the Offeror to provide technical support to the Commonwealth in the support of the equipment in co-location
Request for Criminal Record Check	The form and procedure for looking up and compiling criminal records, commercial records and financial records of an individual, a more fully set forth at Section 44 of Appendix A (Terms and Conditions).
Request for Service	The process used by the Commonwealth to order an addition, modification, or removal of a Service component or configuration using the Service Catalog.
Required Service Level	The expected level of performance for a CM or a KM, as applicable, as set forth in Schedule J.1 (Service Level Methodology).
Required Service Level Default	A recurring failure of the Offeror to meet the Required Service Level for the same CM or KM three (3) times, and each subsequent failure thereafter, during a Service Level Reporting Period
Reserve Account	A capital improvement fund into which Offeror shall deposit quarterly as specified in Section 13 of Appendix A (Terms and Conditions).
RFP	The Request for Proposal (RFP 6100022698) issued by the Commonwealth for Data Center Computing Services.

Term	Definition
Run Book	A book containing all of the information needed to perform day-to-day operations and to respond to emergency situations. This information must include the following: •Resource information about the data center and its hardware and software •Process information, including step-by-step procedures for operational and emergency processes
SAP Vendor Number	A vendor identification number for the Commonwealth's SAP ordering and payment processing systems.
Service Catalog	A listing of Services with pricing and descriptions that are available to the Commonwealth for delivery by the Offeror.
Service Desk	The organization that interfaces with end-users on service requests and trouble reporting.
Service Level	The quality and response standards set for the Offeror's performance of the Services delivered and are defined in Schedules Schedule J.1 - Datacenter Service Level Management, Schedule J.2 - Datacenter Service Level Matrix, and Schedule J.3 - Datacenter SLA Definitions.
Service Level Agreements (SLA's)	A collection of Service Level commitments provided by the Offeror with associated cures.
Service Level Credit	The credits due the Commonwealth in the even the Offeror fails to meet the SLA objectives defined in Schedules Schedule J.1 - Datacenter Service Level Management, Schedule J.2 - Datacenter Service Level Matrix, and Schedule J.3 - Datacenter SLA Definitions.
Service Level Default	A single failure of the Offeror to meet the applicable Minimum Service Level for a specific CM or KM in the applicable Measurement Window (*e.g.*, monthly).
Service Level Default	Failure to meet the Required Service Level.
Service Level Termination Event	Multiple failures over time of a single Service Level or a pattern of failure over time across multiple Service Levels.

Term	Definition
Service Outage	Any event that unexpectedly denies a service's full functionality to the end-users.
Service(s)	The services, function and responsibilities described in the Contract, including the Services set forth in (Services Catalog) and Schedule F (Statement of Work).
Services Locations	The Commonwealth Services Locations and the Offeror Services Locations as agreed upon by the parties as listed in Schedule E (Datacenter Locations).
Small Diverse Business (SDB)	A minority, woman, veteran or service-disabled veteran business enterprise as determined by BSBO.
Software	A collection of one or more programs, databases or microprograms fixed in any tangible medium of expression that comprises a sequence of instructions (source code) to carry out a process in, or convertible into, a form executable by an electronic computer (object code).
SSAE 16	A service organization reporting standard for performing an examination of a service organization's controls and processes. (Statement on Standards for Attestation Engagements (SSAE) No. 16)
Standard Service Request	A service request that is routine in nature and not requiring extensive engineering or solutioning to develop the request.
Statement of Work	The Services, function and responsibilities described in the Agreement, including the services set forth in Schedule F (COPA Datacenter Statement of Work).
Subcontractors	A third party (including an affiliate of Offeror) to which Offeror subcontracts or otherwise delegates its obligations to perform the Services.
Systems Development Life Cycle (SDLC)	A methodology used to create or modify a software application or system.

Term	Definition
Targeted Application Infrastructure	Used to describe a particular Offeror's application's infrastructure related components or configuration items (CIs) When measuring actual application infrastructure related availability it is important to look at all the components that make up the application infrastructure such as all Servers, Storage, Networking, Firewalls, etc. components as defined in the CMDB.
Term	The duration the Contact between the Commonwealth and the Contractor, as more fully set forth in Appendix A (Terms and Conditions).
Terminated Services	Any Service(s) terminated by the Commonwealth.
Termination Assistance Services	All necessary and appropriate actions to accomplish a complete, timely, and seamless transition of any Terminated Services from Offeror to the Commonwealth, or to any replacement provider designated by the Commonwealth.
Termination for Convenience Fees	A fee due to the Contractor in the event the Commonwealth terminates the Contract for convenience, as more fully set forth in Section 32(a) of Appendix A (Terms and Conditions).
Text	A data format that information can be stored that is usable by a standard personal computer
Third Party Software	All Software products (and all modifications, replacements, upgrades, enhancements, documentation, materials and media related thereto) that are provided under license or lease by a third party to Contractor or Commonwealth.
Tier III Datacenter Rating	Uptime Institute Tier Standard: Topology, TIA-942 Telecommunications Infrastructure Standard for Data Centers, and BICSI 002-2011 Data Center Design and Implementation Best Practices.
Tiered Disaster Recovery	A Disaster Recovery plan that allows for multiple Return to Operation (RTO) timeframes to satisfy varying Commonwealth requirements.
Time	Eastern Time (Standard or Daylight Savings time, as applicable)

Term	Definition
Tools	Any tools, either in object code or source code form, which Offeror has previously developed, or which Offeror independently develops or licenses from a third party, excluding any tools that Offeror creates pursuant to this Contract. Offeror Tools includes but is not limited to, methodologies, information, concepts, toolbars for maneuvering between pages, search engines, JAVA applets, and ActiveX controls.
Transition Milestone	Those tasks and associated completion dates set forth in Schedule D (Transition Milestones).
Transition Orders	The orders for existing Commonwealth services that will be placed to transition those services into the contract.
Transition Plan	The plan set out and agreed to by the parties in Schedule M – Detailed Transition Plan detailing the activities, timescales and responsibilities for transitioning the services from Commonwealth to Offeror, including Transition Milestones.
Transition Program Management Office (TPMO)	The organization responsible for transitioning services to the Offeror's control. The TPMO will provide program management Services to deliver architecture, transition plan integration, and organizational change management, as well as quality assurance, verification of testing, financial oversight, and operational readiness for the Mainframe and Server transition/consolidation program.
Transition Services	Means the transition activities, functions and deliverables described in the Detailed Transition Plan and such other tasks as are necessary to enable Offeror to provide the Services.
Vulnerability Analyses	A security analysis to determine the possibility of an unauthorized intrusion, loss of data, denial of service or other security breach.
x86	A series of computer microprocessor instruction set architectures based on the Intel 8086 CPU.
XML	A data format standard allowing computing systems to exchange information over a data connection.

Request for Proposal

RFP # 6100022698

Commonwealth of Pennsylvania

Office of Administration

Office for Information Technology

Data Center Computing Services

SCHEDULE B

GOVERNANCE

1. **Management Meetings**. There shall be weekly meetings of the Management Committee during the Transition Period and monthly meetings thereafter. The purpose of such meetings shall be to (1) track the progress of the Transition and Transformation Plan, (2) review Contractor's performance of the Services Levels, (3) resolve disputes, (4) track the progress of the Services and other projects, (5) coordinate and plan for any new hardware or software acquisitions and service deployments, and (6) address any other matters properly brought before the Management Committee.

2. **Management Committee**. "*Management Committee"* shall be a committee comprised of ten members, five of whom shall be appointed by Commonwealth and five of whom shall be appointed by Contractor from Contractor's executive management staff. Commonwealth and Contractor shall each have one (1) vote with respect to matters that are brought before the Management Committee for resolution. Commonwealth shall designate one of its members on the Management Committee to act as the chairperson of the Management Committee. Both Commonwealth and Contractor can change the individuals on the Management Committee on an as-needed basis. The Management Committee shall be authorized and responsible for (1) generally overseeing the performance of this Contract, (2) providing input and advise to the Governor's Office of Administration regarding Commonwealth's strategic and tactical decisions in respect of the Services, the Systems and any other aspect of the business relationship between Commonwealth and Contractor under this Contract, and (3) monitoring and attempting to resolve disputes regarding the provision of the Services and the Services Levels.

3. **Commonwealth Computing Procedures Manual**. For each Commonwealth Agency and as part of the Services, Contractor shall establish procedures pursuant to which Contractor proposes that policies of Commonwealth and Contractor will be adhered to during the Term for the Commonwealth, and shall deliver to Commonwealth, not later than thirty (30) days prior to the commencement of the activities contemplated under the Transition Plan for the Commonwealth's approval or comment, a draft Commonwealth Computing Procedures Manual generally summarizing (1) the Services, (2) the computer hardware and software environments in which, and the various Services Locations at which, the Services will be performed, (3) the documentation, if any, which provides further details regarding the Services, (4) the procedures Contractor intends to use, and the activities Contractor proposes to undertake, in order to manage the Services, and (5) the procedures of a management reporting system that Contractor will use to manage this Contract and communicate to and with Commonwealth. Commonwealth may, at its request, participate to whatever degree it desires in the preparation of the draft Commonwealth Computing Procedures Manual. Contractor may periodically propose and, at the request of Commonwealth, shall promptly propose updates of the Commonwealth Computing Procedures Manual to reflect any changes in the operations or procedures described therein, all of which proposed changes shall be subject to Commonwealth's approval or comment. Reference Schedule H - Commonwealth Computing Procedures Manual for additional details.

Request for Proposal

RFP # 6100022698

Commonwealth of Pennsylvania

Office of Administration

Office for Information Technology

Data Center Computing Services

SCHEDULE C

SERVICES CATALOG

The Service Catalog in this Schedule C is identical to Schedule I Configuration Definitions, Tab 3 (Technical Rate Card), Tab 4 (Catalog of Services) and Tab 5 (Software), excluding the pricing information. Schedule C is for reference only and an Offeror's proposal shall not include alterations to this schedule.

Schedule I Configuration Definitions

(1) Fully Managed and (2) Managed Only

Servers and Storage Services (x86, p-Series, i-Series)

Servers and Storage services should include the server, disk and backup devices, as well as hardware supplies; software, including operating and data management systems; the facilities, including raised floor and office space; and facilities management.

Unit Prices should include all services costs associated with providing, managing, operating, and transitioning to each technology unit per the RFP requirements Schedule F COPA Datacenter Statement of Work;

3.1 Establish Datacenter Architecture
- 3.1.1 Multi Datacenter Environment (2+ Architecture)
- 3.1.2 Network and Security Architecture
- 3.1.3 Datacenter Architecture and Technology

3.2 Enable Common Service Portfolio

3.2.1 Program & Service Management
- 3.2.1.1 PMO & Contract Management
- 3.2.1.2 Availability/SLA Management
- 3.2.1.3 Change & Release Management
- 3.2.1.4 Service Desk
- 3.2.1.5 Technical Architecture
- 3.2.1.6 Account Management
- 3.2.1.7 Configuration Management
- 3.2.1.8 3rd Party License Management

3.2.2 Technical Services
- 3.2.2.1 Transition Management (New Customer and/or Services)
- 3.2.2.2 Infrastructure Architecture
- 3.2.2.3 Capacity Management
- 3.2.2.4 DR Planning & Testing
- 3.2.2.5 Security Management
- 3.2.2.6 Performance Monitoring & Management

3.2.3 Facilities Management

3.2.3.1 Facilities Architecture / Maintenance
3.2.3.2 Site Operations
3.2.4 Managed Hosting Services
3.2.4.1 Windows Support
3.2.4.2 Storage Management
3.2.4.3 ERP Hosting – SAP / Oracle
3.2.4.4 UNIX Support – AIX / Linux
3.2.4.6 Security & Firewall
3.3 Transition Services
3.3.1 Transition Services – Guiding Principals
3.3.2 Transition Planning/Governance
3.3.2.1 Transition Program Management
3.3.2.2 Security Transition Activities

- Fully Managed Infrastructure is fully owned and managed by the Offeror
- Managed Only Infrastructure is managed by the Service Provider but owned by the Commonwealth and/or a 3rd Party

(3) Limited Co-Lo

Limited Co-Lo is infrastructure that is located in the Service Provider managed datacenter(s). Either owned or managed by the Commonwealth; or 3rd Party.

Limited Co-Lo Services Unit Prices should include all services costs associated with providing, managing, and transitioning to each technology unit per the RFP requirements Schedule F COPA Datacenter Statement of Work Unit Prices should include all services costs associated with providing, managing, operation, and transitioning to each technology unit per the RFP requirements Schedule F COPA Datacenter Statement of Work;

3.1 Establish Datacenter Architecture
3.1.1 Multi Datacenter Environment (2+ Architecture)
3.1.2 Network and Security Architecture
3.1.3 Datacenter Architecture and Technology
3.2 Enable Common Service Portfolio
3.2.1 Program & Service Management
3.2.1.1 PMO & Contract Management
3.2.1.2 Availability/SLA Management
3.2.1.3 Change & Release Management
3.2.1.4 Service Desk
3.2.1.5 Technical Architecture
3.2.1.6 Account Management

3.2.1.7 Configuration Management
3.2.1.8 3rd Party License Management
3.2.2 Technical Services
3.2.2.1 Transition Management (New Customer and/or Services)
3.2.2.2 Infrastructure Architecture
3.2.2.3 Capacity Management
3.2.2.4 DR Planning & Testing
3.2.2.5 Security Management
3.2.2.6 Performance Monitoring & Management
3.2.3 Facilities Management
3.2.3.1 Facilities Architecture / Maintenance
3.2.3.2 Site Operations
3.2.4 Managed Hosting Services
3.2.4.8 Limited-Use Colocation Services
3.3 Transition Services
3.3.1 Transition Services – Guiding Principals
3.3.2 Transition Planning/Governance
3.3.2.1 Transition Program Management
3.3.2.2 Security Transition Activities

(4) Mainframe Services - Include both IBM and Unisys Mainframe services

Mainframe services should include the hardware for the mainframe processing units; disk and backup devices, as well as hardware supplies; software, including operating and data management systems; the facilities, including raised floor and office space; and facilities management in addition to the services described below.

Mainframe Services Unit Prices should include all services costs associated with providing, managing, operating, and transitioning to each technology unit per the RFP requirements Schedule F COPA Datacenter Statement of Work;

3.1 Establish Datacenter Architecture
3.1.1 Multi Datacenter Environment (2+ Architecture)
3.1.2 Network and Security Architecture
3.1.3 Datacenter Architecture and Technology
3.2 Enable Common Service Portfolio
3.2.1 Program & Service Management
3.2.1.1 PMO & Contract Management

3.2.1.2 Availability/SLA Management
3.2.1.3 Change & Release Management
3.2.1.4 Service Desk
3.2.1.5 Technical Architecture
3.2.1.6 Account Management
3.2.1.7 Configuration Management
3.2.1.8 3rd Party License Management

3.2.2 Technical Services
3.2.2.1 Transition Management (New Customer and/or Services)
3.2.2.2 Infrastructure Architecture
3.2.2.3 Capacity Management
3.2.2.4 DR Planning & Testing
3.2.2.5 Security Management
3.2.2.6 Performance Monitoring & Management

3.2.3 Facilities Management
3.2.3.1 Facilities Architecture / Maintenance
3.2.3.2 Site Operations

3.2.4 Managed Hosting Services
3.2.4.2 Storage Management
3.2.4.5 Mainframe Services
3.2.4.6 Security & Firewall

3.3 Transition Services
3.3.1 Transition Services – Guiding Principals
3.3.2 Transition Planning/Governance
3.3.2.1 Transition Program Management
3.3.2.2 Security Transition Activities

- Offerors must also use exhibit B1 DPH Asset List for configuration requirements for mainframe services.

(5) On-Demand (IaaS) Services

On-Demand Unit Prices should include all services costs associated with providing, managing, operating, and transitioning to each technology unit per the RFP requirements Schedule F COPA Datacenter Statement of Work;

3.1 Establish Datacenter Architecture
3.1.1 Multi Datacenter Environment (2+ Architecture)

3.1.2 Network and Security Architecture
3.1.3 Datacenter Architecture and Technology
3.2 Enable Common Service Portfolio
3.2.1 Program & Service Management
3.2.1.1 PMO & Contract Management
3.2.1.2 Availability/SLA Management
3.2.1.3 Change & Release Management
3.2.1.4 Service Desk
3.2.1.5 Technical Architecture
3.2.1.6 Account Management
3.2.1.7 Configuration Management
3.2.1.8 3rd Party License Management
3.2.2 Technical Services
3.2.2.1 Transition Management (New Customer and/or Services)
3.2.2.2 Infrastructure Architecture
3.2.2.3 Capacity Management
3.2.2.4 DR Planning & Testing
3.2.2.5 Security Management
3.2.2.6 Performance Monitoring & Management
3.2.3 Facilities Management
3.2.3.1 Facilities Architecture / Maintenance
3.2.3.2 Site Operations
3.2.5 Capacity on Demand Services
3.2.5.1 Server Capacity on Demand
3.2.5.2 Storage Capacity on Demand
3.2.5.3 DR Infrastructure on Demand
3.2.5.4 Additional Technical Services
3.3 Transition Services
3.3.1 Transition Services – Guiding Principals
3.3.2 Transition Planning/Governance
3.3.2.1 Transition Program Management
3.3.2.2 Security Transition Activities

Schedule I Tab 3. Technical Staff Rate Card

Technical Staff Rate Card
Resource Description
Infrastructure (mainframe, mid-range and x86) Architects/Engineers
Microsoft Product Specialists (e.g. Exchange, SharePoint)
Basis and SAP Oracle support
Performance Specialists
Mainframe Systems Programmers
Batch Administrators
3rd Party Software Product Specialists
System Administrator (Windows, AIX, Linux)
System Administrator (Middleware support)
Storage Administrator
Data Backup Administrator
Database Administrator
Database Architects
Database Analysts
Project Management Support
Network Administrator
Facilities Administrator
Security Administrator
Security Architects
Security Analysts
Asset Management Administrator
Quality Assurance Support
Remedy Support Specialist
IT Service Continuity Specialist

Schedule I Tab 4. Catalog of Services

Field Name ==>	**Product Name**	**Unit**
Description / Use *==>*	*Unique Identifier*	*Unit*
Server - Fully Managed (1)		
x86 Server Configurations (Windows)		
Windows pConfig - 1	2-way Quad-Core 2.0 GHz	Per Server
Windows pConfig - 2, 4, 5	2-way Six-Core 2.4 GHz	Per Server
Windows pConfig - 3	4-way Six-Core 2.0 GHz	Per Server
Windows pConfig - 1, 2, 3, 4, 5	GB RAM	Per GB
Windows pConfig - 1, 2, 4, 5	Mirrored 146 15K Hard Drives	Per Primary + Mirror drive
Windows pConfig - 3	SAN Attached Storage	Per GB
Windows pConfig - 1, 2, 3, 4, 5	Windows Server 2008 R2	Per License
Windows pConfig - 4	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization Site's Local SAN Storage from hourly data synchronization	Per Service
Windows pConfig - 5	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Service
Windows pConfig - 1	Fully Managed (1) - Platinum Tier	Per Config
Windows pConfig - 1	Fully Managed (1) - Gold Tier	Per Config
Windows pConfig - 1	Fully Managed (1) - Silver Tier	Per Config
Windows pConfig - 1	Fully Managed (1) - Bronze Tier	Per Config
Windows pConfig - 1	Fully Managed (1) - Basic Tier	Per Config
Windows pConfig - 2	Fully Managed (1) - Platinum Tier	Per Config
Windows pConfig - 2	Fully Managed (1) - Gold Tier	Per Config
Windows pConfig - 2	Fully Managed (1) - Silver Tier	Per Config
Windows pConfig - 2	Fully Managed (1) - Bronze Tier	Per Config
Windows pConfig - 2	Fully Managed (1) - Basic Tier	Per Config
Windows pConfig - 3	Fully Managed (1) - Platinum Tier	Per Config
Windows pConfig - 3	Fully Managed (1) - Gold Tier	Per Config
Windows pConfig - 3	Fully Managed (1) - Silver Tier	Per Config
Windows pConfig - 3	Fully Managed (1) - Bronze Tier	Per Config
Windows pConfig - 3	Fully Managed (1) - Basic Tier	Per Config
Windows pConfig - 4	Fully Managed (1) - Platinum Tier	Per Config
Windows pConfig - 4	Fully Managed (1) - Gold Tier	Per Config
Windows pConfig - 4	Fully Managed (1) - Silver Tier	Per Config
Windows pConfig - 4	Fully Managed (1) - Bronze Tier	Per Config
Windows pConfig - 4	Fully Managed (1) - Basic Tier	Per Config
Windows pConfig - 5	Fully Managed (1) - Platinum Tier	Per Config
Windows pConfig - 5	Fully Managed (1) - Gold Tier	Per Config
Windows pConfig - 5	Fully Managed (1) - Silver Tier	Per Config
Windows pConfig - 5	Fully Managed (1) - Bronze Tier	Per Config

Field Name ==>	**Product Name**	**Unit**
Description / Use *==>*	*Unique Identifier*	*Unit*
Windows pConfig - 5	Fully Managed (1) - Basic Tier	Per Config
x86 Server Configurations (Linux)		
Linux pConfig - 1	2-way Quad-Core 2.0 GHz	Per Server
Linux pConfig - 2, 4, 5	2-way Six-Core 2.4 GHz	Per Server
Linux pConfig - 3	4-way Six-Core 2.0 GHz	Per Server
Linux pConfig - 1	GB RAM	Per GB
Linux pConfig - 1, 2, 4, 5	Mirrored 146 15K Hard Drives	Per Primary + Mirror drive
Linux pConfig - 3	SAN Attached Storage	Per GB
Linux pConfig - 1, 2, 3, 4 , 5	RedHat or SUSE	Per License
Linux pConfig - 4	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Service
Linux pConfig - 5	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Service
Linux pConfig - 1	Fully Managed (1) - Platinum Tier	Per Config
Linux pConfig - 1	Fully Managed (1) - Gold Tier	Per Config
Linux pConfig - 1	Fully Managed (1) - Silver Tier	Per Config
Linux pConfig - 1	Fully Managed (1) - Bronze Tier	Per Config
Linux pConfig - 1	Fully Managed (1) - Basic Tier	Per Config
Linux pConfig - 2	Fully Managed (1) - Platinum Tier	Per Config
Linux pConfig - 2	Fully Managed (1) - Gold Tier	Per Config
Linux pConfig - 2	Fully Managed (1) - Silver Tier	Per Config
Linux pConfig - 2	Fully Managed (1) - Bronze Tier	Per Config
Linux pConfig - 2	Fully Managed (1) - Basic Tier	Per Config
Linux pConfig - 3	Fully Managed (1) - Platinum Tier	Per Config
Linux pConfig - 3	Fully Managed (1) - Gold Tier	Per Config
Linux pConfig - 3	Fully Managed (1) - Silver Tier	Per Config
Linux pConfig - 3	Fully Managed (1) - Bronze Tier	Per Config
Linux pConfig - 3	Fully Managed (1) - Basic Tier	Per Config
Linux pConfig - 4	Fully Managed (1) - Platinum Tier	Per Config
Linux pConfig - 4	Fully Managed (1) - Gold Tier	Per Config
Linux pConfig - 4	Fully Managed (1) - Silver Tier	Per Config
Linux pConfig - 4	Fully Managed (1) - Bronze Tier	Per Config
Linux pConfig - 4	Fully Managed (1) - Basic Tier	Per Config
Linux pConfig - 5	Fully Managed (1) - Platinum Tier	Per Config
Linux pConfig - 5	Fully Managed (1) - Gold Tier	Per Config
Linux pConfig - 5	Fully Managed (1) - Silver Tier	Per Config
Linux pConfig - 5	Fully Managed (1) - Bronze Tier	Per Config
Linux pConfig - 5	Fully Managed (1) - Basic Tier	Per Config
x86 (Windows) - Virtual Servers		
Windows vConfig - 1	2vCPU	Per Instance

Field Name ==>	**Product Name**	**Unit**
Description / Use *==>*	*Unique Identifier*	*Unit*
Windows vConfig - 2, 4, 5	4vCPU	Per Instance
Windows vConfig - 3	8vCPU	Per Instance
Windows vConfig - 1, 2, 3, 4, 5	GB Ram	Per GB
Windows vConfig - 1, 2, 3, 4, 5	Windows Server 2008 R2	Per License
Windows vConfig - 4	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Config
Windows vConfig - 5	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Config
Windows vConfig - 1	Fully Managed (1) - Platinum Tier	Per Config
Windows vConfig - 1	Fully Managed (1) - Gold Tier	Per Config
Windows vConfig - 1	Fully Managed (1) - Silver Tier	Per Config
Windows vConfig - 1	Fully Managed (1) - Bronze Tier	Per Config
Windows vConfig - 1	Fully Managed (1) - Basic Tier	Per Config
Windows vConfig - 2	Fully Managed (1) - Platinum Tier	Per Config
Windows vConfig - 2	Fully Managed (1) - Gold Tier	Per Config
Windows vConfig - 2	Fully Managed (1) - Silver Tier	Per Config
Windows vConfig - 2	Fully Managed (1) - Bronze Tier	Per Config
Windows vConfig - 2	Fully Managed (1) - Basic Tier	Per Config
Windows vConfig - 3	Fully Managed (1) - Platinum Tier	Per Config
Windows vConfig - 3	Fully Managed (1) - Gold Tier	Per Config
Windows vConfig - 3	Fully Managed (1) - Silver Tier	Per Config
Windows vConfig - 3	Fully Managed (1) - Bronze Tier	Per Config
Windows vConfig - 3	Fully Managed (1) - Basic Tier	Per Config
Windows vConfig - 4	Fully Managed (1) - Platinum Tier	Per Config
Windows vConfig - 4	Fully Managed (1) - Gold Tier	Per Config
Windows vConfig - 4	Fully Managed (1) - Silver Tier	Per Config
Windows vConfig - 4	Fully Managed (1) - Bronze Tier	Per Config
Windows vConfig - 4	Fully Managed (1) - Basic Tier	Per Config
Windows vConfig - 5	Fully Managed (1) - Platinum Tier	Per Config
Windows vConfig - 5	Fully Managed (1) - Gold Tier	Per Config
Windows vConfig - 5	Fully Managed (1) - Silver Tier	Per Config
Windows vConfig - 5	Fully Managed (1) - Bronze Tier	Per Config
Windows vConfig - 5	Fully Managed (1) - Basic Tier	Per Config
x86 (Linux) - Virtual Servers		
Linux vConfig - 1	2vCPU	Per Instance
Linux vConfig - 2, 4, 5	4vCPU	Per Instance
Linux vConfig - 3	8vCPU	Per Instance
Linux vConfig - 1, 2, 3, 4, 5	GB Ram	Per GB
Linux vConfig - 1, 2, 3, 4, 5	RedHat or SUSE	Per License

Field Name ==>	**Product Name**	**Unit**
Description / Use *==>*	*Unique Identifier*	*Unit*
Linux vConfig - 4	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Config
Linux vConfig - 5	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Config
Linux vConfig - 1	Fully Managed (1) - Platinum Tier	Per Config
Linux vConfig - 1	Fully Managed (1) - Gold Tier	Per Config
Linux vConfig - 1	Fully Managed (1) - Silver Tier	Per Config
Linux vConfig - 1	Fully Managed (1) - Bronze Tier	Per Config
Linux vConfig - 1	Fully Managed (1) - Basic Tier	Per Config
Linux vConfig - 2	Fully Managed (1) - Platinum Tier	Per Config
Linux vConfig - 2	Fully Managed (1) - Gold Tier	Per Config
Linux vConfig - 2	Fully Managed (1) - Silver Tier	Per Config
Linux vConfig - 2	Fully Managed (1) - Bronze Tier	Per Config
Linux vConfig - 2	Fully Managed (1) - Basic Tier	Per Config
Linux vConfig - 3	Fully Managed (1) - Platinum Tier	Per Config
Linux vConfig - 3	Fully Managed (1) - Gold Tier	Per Config
Linux vConfig - 3	Fully Managed (1) - Silver Tier	Per Config
Linux vConfig - 3	Fully Managed (1) - Bronze Tier	Per Config
Linux vConfig - 3	Fully Managed (1) - Basic Tier	Per Config
Linux vConfig - 4	Fully Managed (1) - Platinum Tier	Per Config
Linux vConfig - 4	Fully Managed (1) - Gold Tier	Per Config
Linux vConfig - 4	Fully Managed (1) - Silver Tier	Per Config
Linux vConfig - 4	Fully Managed (1) - Bronze Tier	Per Config
Linux vConfig - 4	Fully Managed (1) - Basic Tier	Per Config
Linux vConfig - 5	Fully Managed (1) - Platinum Tier	Per Config
Linux vConfig - 5	Fully Managed (1) - Gold Tier	Per Config
Linux vConfig - 5	Fully Managed (1) - Silver Tier	Per Config
Linux vConfig - 5	Fully Managed (1) - Bronze Tier	Per Config
Linux vConfig - 5	Fully Managed (1) - Basic Tier	Per Config
P-Series Server Configurations		
AIX Config - 1, 2, 3, 4, 5	3.0GHz POWER7	Per Server
AIX Config - 1	Cores	Per .5 Core
AIX Config - 1, 2, 3, 4, 5	GB RAM	Per GB
AIX Config - 1, 2, 3, 4, 5	AIX	Per License
AIX Config - 4	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Config
AIX Config - 5	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Config
AIX Config - 1	Fully Managed (1) - Platinum Tier	Per Config

Field Name ==>	**Product Name**	**Unit**
Description / Use *==>*	*Unique Identifier*	*Unit*
AIX Config - 1	Fully Managed (1) - Gold Tier	Per Config
AIX Config - 1	Fully Managed (1) - Silver Tier	Per Config
AIX Config - 1	Fully Managed (1) - Bronze Tier	Per Config
AIX Config - 1	Fully Managed (1) - Basic Tier	Per Config
AIX Config - 2	Fully Managed (1) - Platinum Tier	Per Config
AIX Config - 2	Fully Managed (1) - Gold Tier	Per Config
AIX Config - 2	Fully Managed (1) - Silver Tier	Per Config
AIX Config - 2	Fully Managed (1) - Bronze Tier	Per Config
AIX Config - 2	Fully Managed (1) - Basic Tier	Per Config
AIX Config - 3	Fully Managed (1) - Platinum Tier	Per Config
AIX Config - 3	Fully Managed (1) - Gold Tier	Per Config
AIX Config - 3	Fully Managed (1) - Silver Tier	Per Config
AIX Config - 3	Fully Managed (1) - Bronze Tier	Per Config
AIX Config - 3	Fully Managed (1) - Basic Tier	Per Config
AIX Config - 4	Fully Managed (1) - Platinum Tier	Per Config
AIX Config - 4	Fully Managed (1) - Gold Tier	Per Config
AIX Config - 4	Fully Managed (1) - Silver Tier	Per Config
AIX Config - 4	Fully Managed (1) - Bronze Tier	Per Config
AIX Config - 4	Fully Managed (1) - Basic Tier	Per Config
AIX Config - 5	Fully Managed (1) - Platinum Tier	Per Config
AIX Config - 5	Fully Managed (1) - Gold Tier	Per Config
AIX Config - 5	Fully Managed (1) - Silver Tier	Per Config
AIX Config - 5	Fully Managed (1) - Bronze Tier	Per Config
AIX Config - 5	Fully Managed (1) - Basic Tier	Per Config
Server - Managed Only (2)		
Server - Managed Only x86 (Windows, Linux)		
	Platinum Tier	Server/Instance
	Gold Tier	Server/Instance
	Silver Tier	Server/Instance
	Bronze Tier	Server/Instance
	Basic Tier	Server/Instance
Server - Managed Only UNIX (IBM P-Series, AIX)		
	Platinum	LPAR
	Gold Tier	LPAR
	Silver Tier	LPAR
	Bronze Tier	LPAR
	Basic Tier	LPAR
Storage and Backup - Fully Managed (1)		
Enterprise Storage		
	* Dedicated - Config 1 - SAN Raid 5	GB
	* Dedicated - Config 2 - SAN Raid 10	GB
	Dedicated - Config 3 - Net Attached	GB

Field Name ==>	Product Name	Unit
Description / Use *==>*	*Unique Identifier*	*Unit*
Tape and Backup		
	** Server Tape Stored	GB Stored
	** Offsite Tape Storage	Tapes
Limited Co-Lo (Data Center Only Charge) (3)		
Limited Co-Lo Configurations		
Co-Lo Config - 1	1/4 Rack Configuration includes: 10U Cabinet Space	Per Config
Co-Lo Config - 2	1/2 Rack Configuration includes: 21U Cabinet Space	Per Config
Co-Lo Config - 3	Full Rack Configuration includes: 42U Cabinet Space	Per Config
Co-Lo Config - 1, 2, 3	Network Bandwidth	Per GB
Co-Lo Config - 1, 2, 3	100Mb/s Uplink	Each
Co-Lo Config - 1, 2, 3	IP Addresses	Each
Co-Lo Config - 1	110V AC Circuits	Per Circuit
Mainframe Services (4)		
IBM Mainframe		
	*** IBM Mainframe Allocated DASD	GB
	IBM Tapes in Storage - VTS	GB
	IBM Offsite Tape Storage	Tape/Reel
IBM Mainframe Configurations		
IBM Mainframe Config - 1	IBM System zEnterprise Processor z/OS	Per MIP
IBM Mainframe Config - 2	IBM System zEnterprise Processor Virtual Linux Prod IFL	Per MIP
IBM Mainframe Config - 3	IBM System zEnterprise Processor Virtual Linux Prod IFLw/ Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per MIP
IBM AS400 Config 1	IBM i Series / AS400	Per CPW
IBM AS400 Config 2	IBM i Series / AS400 w/ Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per CPW
IBM Mainframe Config - 1	Mainframe Services (4) - Platinum Tier	Per Config
IBM Mainframe Config - 1	Mainframe Services (4) - Gold Tier	Per Config
IBM Mainframe Config - 1	Mainframe Services (4) - Basic Tier	Per Config
IBM Mainframe Config - 2	Mainframe Services (4) - Platinum Tier	Per Config
IBM Mainframe Config - 2	Mainframe Services (4) - Gold Tier	Per Config
IBM Mainframe Config - 2	Mainframe Services (4) - Basic Tier	Per Config
IBM Mainframe Config - 3	Mainframe Services (4) - Platinum Tier	Per Config
IBM Mainframe Config - 3	Mainframe Services (4) - Gold Tier	Per Config
IBM Mainframe Config - 3	Mainframe Services (4) - Basic Tier	Per Config

Field Name ==>	**Product Name**	**Unit**
Description / Use *==>*	*Unique Identifier*	*Unit*
IBM AS400 Config 1	Mainframe Services (4) - Platinum Tier	Per Config
IBM AS400 Config 1	Mainframe Services (4) - Gold Tier	Per Config
IBM AS400 Config 1	Mainframe Services (4) - Basic Tier	Per Config
IBM AS400 Config 2	Mainframe Services (4) - Platinum Tier	Per Config
IBM AS400 Config 2	Mainframe Services (4) - Gold Tier	Per Config
IBM AS400 Config 2	Mainframe Services (4) - Basic Tier	Per Config
Unisys Mainframe		
	*** Unisys DASD	GB
	Unisys Tapes in Storage - VTS	GB
	Unisys Offsite Tape Storage	Tape/Reel
Unisys Mainframe Configurations		
Unisys Mainframe Config - 1	Unisys (Clearpath / Dorado)	Per MIP
Unisys Mainframe Config - 2	Unisys (Clearpath / Libra)	Per MIP
Unisys Mainframe Config - 3	Unisys (Clearpath / Dorado) w/ Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per MIP
Unisys Mainframe Config - 4	Unisys (Clearpath / Libra) w/ Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per MIP
Unisys Mainframe Config - 1	Mainframe Services (4) - Platinum Tier	Per Config
Unisys Mainframe Config - 1	Mainframe Services (4) - Gold Tier	Per Config
Unisys Mainframe Config - 1	Mainframe Services (4) - Basic Tier	Per Config
Unisys Mainframe Config - 2	Mainframe Services (4) - Platinum Tier	Per Config
Unisys Mainframe Config - 2	Mainframe Services (4) - Gold Tier	Per Config
Unisys Mainframe Config - 2	Mainframe Services (4) - Basic Tier	Per Config
Unisys Mainframe Config - 3	Mainframe Services (4) - Platinum Tier	Per Config
Unisys Mainframe Config - 3	Mainframe Services (4) - Gold Tier	Per Config
Unisys Mainframe Config - 3	Mainframe Services (4) - Basic Tier	Per Config
Unisys Mainframe Config - 4	Mainframe Services (4) - Platinum Tier	Per Config
Unisys Mainframe Config - 4	Mainframe Services (4) - Gold Tier	Per Config
Unisys Mainframe Config - 4	Mainframe Services (4) - Basic Tier	Per Config
IaaS x86 Server Configurations (Windows)		
IaaS Windows vConfig - 1	2vCPU	Per Server
IaaS Windows vConfig - 2, 4, 5	4vCPU	Per Server
IaaS Windows vConfig - 3	8vCPU	Per Server
IaaS Windows vConfig - 1, 2, 3, 4, 5	GB Ram	Per GB
IaaS Windows vConfig - 1, 2, 3, 4, 5	Windows Server 2008 R2	Per License

Field Name ==>	**Product Name**	**Unit**
Description / Use *==>*	*Unique Identifier*	*Unit*
IaaS Windows vConfig - 4	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Config
IaaS Windows vConfig - 5	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Config
IaaS x86 Server Configurations (Linux)		
IaaS Linux vConfig - 1	2vCPU	Per Server
IaaS Linux vConfig - 2, 4, 5	4vCPU	Per Server
IaaS Linux vConfig - 3	8vCPU	Per Server
IaaS Linux vConfig - 1, 2, 3, 4, 5	GB Ram	Per GB
IaaS Linux vConfig - 1, 2, 3, 4, 5	RedHat or SUSE	Per License
IaaS Linux vConfig - 4	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Config
IaaS Linux vConfig - 5	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Config
IaaS Storage Configurations		
IaaS Storage Config - 1, 2	SAN attached storage	Per GB
IaaS Storage Config - 3	Network Attached Storage	Per GB
IaaS Storage Config - 1	Raid 5	Per GB
IaaS Storage Config - 2	Raid 10	Per GB
IaaS Storage Config - 1, 2	10K - 15K RPM discs	Per GB
IaaS Backup Configurations		
IaaS Backup Config - 1	Remote Offsite backup per GB	Per GB
Reserve Account		
	Reserve Account - Enterprise Datacenter	

Schedule I Tab 5. Software

Third Party Software		
Third Party Software		
Field Name ==>	**Product Name**	**Unit**
Description / Use *==>*	*Unique Identifier*	*Unit*
Vendor	**Product**	
B & L	BL/LIB Tape Library Management System	License
B & L	BL/SCHED Scheduling & Monitoring System	License
BMC Software	BMC AppSight for Windows/.NET - Division Edition	License
BMC Software	BMC AppSight Named Users	License
BMC Software	BMC AppSight QA Users	License
BMC Software	CONTROL-M Enterprise Manager	License
BMC Software	CONTROL-M Full Admin User	License
BMC Software	CONTROL-M Tasks (100 Tasks per Unit)	License
BMC Software	Database Director (D2)	License
BMC Software	Eclipse iBuild	License
BMC Software	Eclipse iChange	License
BMC Software	Eclipse iCheck	License
BMC Software	Eclipse iCopy	License
BMC Software	Eclipse iExtract	License
BMC Software	Eclipse iLM	License
BMC Software	Eclipse iLoad	License
BMC Software	Eclipse iRecover	License
BMC Software	Eclipse iSurvey	License
BMC Software	Eclipse iUnload	License
BMC Software	Mission Control	License
Business Objects	Crystal Reports	License
Bytware Inc.	StandGuard Anti-Virus	License
Citrix	XenApp Advanced (User Counts)	License
Citrix	XenApp Enterprise (User Counts)	License
Computer Associates International, Inc.	CA-Explore for CICS	License
Computer Associates International, Inc.	SOA Security Manager	License
Computer Associates International, Inc.	SOA Security Manager Additional Secured Web Services	License
Computer Associates International, Inc.	SOA Security Manager Additional Users	License
Corticon Technologies	Corticon Business Rules Server – Unlimited CPUs	License
Corticon Technologies	Corticon Server – per Non-Production Server	License

Third Party Software

Third Party Software

Field Name ==>	Product Name	Unit
Description / Use *==>*	*Unique Identifier*	*Unit*
Vendor	**Product**	
Corticon Technologies	Corticon Business Rules Modeling Studio – per Named User	License
CSI International	EPIC	License
CSI International	FAQS/PCS	License
CSI International	FAQS/ASO	License
EMC Corporation	PowerPath	License
EMC Corporation	PowerPath (per CPU)	License
EMC Corporation	Symmetrix® VMAX Fully Automated Storage Tiering for Virtual Pools (FAST VP)	License
EMC Corporation	Vsphere Enterprise Plus	License
Experian QAS	NameSearch - Production (Licensed per Server up to 8 CPU)	License
Experian QAS	NameSearch - Non-Production (Licensed per Server)	License
Formula Consultants, Inc.	Star 1100	License
GlobalScape	CuteFTP Pro 2.0	License
HELPSYS	Robot/Schedule	License
Idea Integration	XGEN	License
Informatica Corporation	SSA-Name 3	License
Infragistics	NetAdvantage for .NET	License
KMSYS Worldwide, Inc.	IQU Plus-1	License
Levi, Ray and Shoup	VPS/PCL	License
Levi, Ray and Shoup	VPS/TCP/IP	License
Levi, Ray and Shoup	VPS/DRS	License
Levi, Ray and Shoup	VPS	License
MacKinney Systems, Inc.	CICS Response Time Monitor	License
Microsoft	BizTalk Adaptor for MQSeries	License
Microsoft	BizTalk Server Enterprise (Single Processor)	License
Microsoft	BizTalk Server Standard (Single Processor)	License
Microsoft	SQL Server CAL	License
Microsoft	SQL Server Enterprise (Single Processor)	License
Microsoft	SQL Server Enterprise	License
Microsoft	SQL Server Standard (Single Processor)	License
Microsoft	SQL Server Standard	License
Microsoft	SQL Server Standard per 2-Core	License
Microsoft	Visual Studio Foundation Server	License
Microsoft	Visual Studio Foundation Server CAL	License

Third Party Software

Third Party Software

Field Name ==>	Product Name	Unit
Description / Use *==>*	*Unique Identifier*	*Unit*
Vendor	**Product**	
Microsoft	Visual Studio Professional with MSDN	License
Microsoft	Windows Server Datacenter Edition (Single Processor)	License
Microsoft	Windows Server Enterprise Edition	License
Microsoft	Windows Server Standard Edition	License
Microsoft	Windows Terminal Service Client Access Licenses	License
Network Associates	McAfee Anti-Virus	License
Novell	Platespin Migrator	License
Novell	SuSE Linux	License
OpenText	Metastorm Integration Manager for CICS (MIM for CICS)	License
Oracle	Oracle Change Management Pack	License
Oracle	Oracle Database 10g Enterprise	License
Oracle	Oracle Database Enterprise Edition	License
Oracle	Oracle Diagnostic Pack	License
Oracle	Oracle Enterprise Linux	License
Oracle	Oracle Exadata Storage Software	License
Oracle	Oracle Partitioning	License
Oracle	Oracle Tuning Pack	License
Oracle	Real Application Cluster - Processor Perpetual	License
Oracle	Spatial and Graph - Processor Perpetual	License
Pitney Bowes	Finalist (Doc Sense)	License
Pitney Bowes	CODE-1 Plus	License
Pitney Bowes	CODE-1 Plus (Test / Development)	License
Pitney Bowes	Online Window for Finalist	License
Quest	Central Performance Suite for SQL Server, Tier A	License
Quest	Central Performance Suite for SQL Server, Tier B	License
Quest	Foglight Database Management Suite for SQL Server	License
Quest	Foglight for SQL Server per CPU Socket	License
Quest	Foglight OS Management per CPU Socket	License
Quest	Foglight Server for FSM	License
RealVNC	VNC Enterprise Edition for Windows	License
Red Hat	Red Hat Enterprise Linux	License

Third Party Software

Third Party Software

Field Name ==>	Product Name	Unit
Description / Use *==>*	*Unique Identifier*	*Unit*
Vendor	**Product**	
Segus Inc.	OPC/Graph	License
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG20	License
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG40	License
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG60	License
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG80	License
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG130	License
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG20	License
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG40	License
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG60	License
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG80	License
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG130	License
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG140	License
Sightline	OS 2200 Interface Agent - MAPPER, SWG20	License
Sightline	OS 2200 Interface Agent - MAPPER, SWG40	License
Sightline	OS 2200 Interface Agent - MAPPER, SWG60	License
Sightline	OS 2200 Interface Agent - MAPPER, SWG80	License
Sightline	OS 2200 Interface Agent - MAPPER, SWG130	License
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG20	License
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG40	License
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG60	License
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG80	License
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG130	License
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG140	License

Third Party Software

Third Party Software

Field Name ==>	Product Name	Unit
Description / Use *==>*	*Unique Identifier*	*Unit*
Vendor	**Product**	
Sightline	OS 2200 Interface Agent - System Log, SWG20	License
Sightline	OS 2200 Interface Agent - System Log, SWG40	License
Sightline	OS 2200 Interface Agent - System Log, SWG60	License
Sightline	OS 2200 Interface Agent - System Log, SWG80	License
Sightline	OS 2200 Interface Agent - System Log, SWG130	License
Sightline	OS 2200 Interface Agent - System Log, SWG140	License
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG20	License
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG40	License
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG60	License
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG80	License
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG130	License
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG140	License
Sightline	OS 2200 Power Agent, SWG20	License
Sightline	OS 2200 Power Agent, SWG40	License
Sightline	OS 2200 Power Agent, SWG60	License
Sightline	OS 2200 Power Agent, SWG80	License
Sightline	OS 2200 Power Agent, SWG130	License
Sightline	OS 2200 Power Agent, SWG140	License
Sightline	OS 2200 Torch Capacity Manager Power Agent, SWG40	License
Sightline	OS 2200 Torch Capacity Manager Power Agent, SWG60	License
Sightline	OS 2200 Torch Capacity Manager Power Agent, SWG130	License
Sightline	OS 2200 Torch Capacity Manager Power Agent, SWG140	License
Sightline	OS 2200 Torch Interface Agent - I/O TRACE, SWG40	License
Sightline	OS 2200 Torch Interface Agent - I/O TRACE, SWG60	License

Third Party Software

Third Party Software

Field Name ==>	Product Name	Unit
Description / Use *==>*	*Unique Identifier*	*Unit*
Vendor	**Product**	
Sightline	OS 2200 Torch Interface Agent - I/O TRACE, SWG130	License
Sightline	OS 2200 Torch Interface Agent - LOG, SWG40	License
Sightline	OS 2200 Torch Interface Agent - LOG, SWG60	License
Sightline	OS 2200 Torch Interface Agent - LOG, SWG130	License
Sightline	OS 2200 Torch Interface Agent - LOG, SWG140	License
Sightline	OS 2200 Torch Interface Agent - MAPPER, SWG40	License
Sightline	OS 2200 Torch Interface Agent - MAPPER, SWG60	License
Sightline	OS 2200 Torch Interface Agent - MAPPER, SWG130	License
Sightline	Windows 2000 Interface Agent - Internet Information Server	License
Sightline	Windows 2000 Interface Agent - .NET	License
Sightline	Windows 2000 Interface Agent - SQL Server	License
Sightline	Windows 2000 Power Agent Upto 32 CPU's	License
SMA	OpCon/xps EXEC LSAM, Group 3	License
SMA	OpCon/xps EXEC LSAM, Group 12	License
SMA	OpCon/xps EXEC LSAM Development, Group 2	License
SMA	OpCon/xps EXEC LSAM Development, Group 12	License
SMA	OpCon/xps Production SAM	License
SMA	OpCon/xps Starter Kit	License
SMA	OpCon/xps User Interface	License
Sybase	EAServer Deploy Advanced - Active	License
Sybase	EAServer Deploy Advanced - Passive	License
Symantec	Backup Exec System Recovery Server	License
Symantec	EndPoint Protection	License
Symantec	Ghost Solution Suite	License
Symantec	NetBackup Client Application and Database Pack, UNX, Tier 3	License
Symantec	NetBackup Client Application and Database Pack, UNX, Tier 4	License

Third Party Software

Third Party Software

Field Name ==>	Product Name	Unit
Description / Use *==>*	*Unique Identifier*	*Unit*
Vendor	**Product**	
Symantec	NetBackup Client Application and Database Pack, WIN, Tier 2	License
Symantec	NetBackup Client Application and Database Pack, WIN, Tier 3	License
Symantec	NetBackup Client Application and Database Pack, WIN, Tier 4	License
Symantec	NetBackup Enterprise Client, UNX, Tier 4	License
Symantec	NetBackup Enterprise Client, WIN, Tier 1	License
Symantec	NetBackup Enterprise Client, WIN, Tier 2	License
Symantec	NetBackup Enterprise Client, WIN, Tier 3	License
Symantec	NetBackup Enterprise Server, WIN, Tier 2	License
Symantec	NetBackup Enterprise Server, WIN, Tier 3	License
Symantec	NetBackup Library Based Tape Drive Option, XPLAT	License
Symantec	NetBackup Media Server Encryption Option (MSEO) WIN, Tier 2	License
Symantec	NetBackup Platform Base, XPLAT (per Terabyte)	License
Symantec	NetBackup Shared Storage Option, XPLAT	License
Symantec	NetBackup Standard Client, XPLAT	License
Symantec	NetBackup Vault Additional Drive Option, XPLAT	License
Symantec	NetBackup Vault Base Option, XPLAT (4 tape drives per license)	License
Symantec	Veritas NetBackup Enterprise Server License, Tier 3	License
Symantec	Veritas NetBackup Windows Client, Tier 4	License
Tone Software Corp.	Dynastep	License
Unicon Group Ltd.	LOUIS II LCOM Host Module	License
Unicon Group Ltd.	LOUIS II Extract & Reporting Module	License
Unicon Group Ltd.	LOUIS II DERIVE Option	License
Unicon Group Ltd.	LOUIS II DMS Interface	License
Unicon Group Ltd.	LOUIS II RDMS Interface	License
Unicon Group Ltd.	LOUIS II RELATE Option	License
VanDyke Technologies	VShell Workgroup Server	License
Veeam	nWorks ESX Monitoring for SCOM	License
Veeam	nWorks Management Pack for VMWare	License
VMware, Inc.	VMware vSphere 4 Enterprise Plus for 1 Processor	License

Third Party Software

Third Party Software

Field Name ==>	Product Name	Unit
Description / Use *==>*	*Unique Identifier*	*Unit*
Vendor	**Product**	
VMware, Inc.	VMware vSphere 5 Enterprise Plus for 1 Processor	License
Winternals	Winternals Administrator's Pak	License
WinZip Computing	Winzip	License
XtremeSoft	AppMetrics	License
USPS	Correct Address	License
IBM	FileNet	License
Microsoft	SharePoint (with SA)	License
IBM	WebSphere MQ (Procesor Value Unit)	License
Xerox	XeroxDocuShare	License

Hybrid Third Party Software

Vendor	Product	
Computer Associates International, Inc.	CA 90's Services (freeware)	License
Computer Associates International, Inc.	Vision Builder	License
Computer Associates International, Inc.	Easytrieve Plus	License
Computer Associates International, Inc.	Easytrieve Plus MVS	License
Computer Associates International, Inc.	Easytrieve Plus IMS	License
Computer Associates International, Inc.	Easytrieve Plus IMS Option MVS	License
Computer Associates International, Inc.	Easytrieve Plus DB2 OPT	License
Computer Associates International, Inc.	Easytrieve Plus DB2 Option MVS	License
Computer Associates International, Inc.	Endevor/MVS Automated Configuration Mgr MVS	License
Computer Associates International, Inc.	Endevor/MVS External Security Int. MVS	License
Computer Associates International, Inc.	Endevor/MVS MVS	License
Computer Associates International, Inc.	Endevor/MVS Extended Processor	License
Computer Associates International, Inc.	CA-Librarian	License
Computer Associates International, Inc.	CA-META COBOL	License
Computer Associates International, Inc.	Panvalet	License
Computer Associates International, Inc.	Panvalet ISPF	License

Third Party Software

Third Party Software

Field Name ==>	Product Name	Unit
Description / Use *==>*	*Unique Identifier*	*Unit*
Vendor	**Product**	
Computer Associates International, Inc.	SORT (INCL DART)	License
Computer Associates International, Inc.	SRAM	License
dotJ Software Inc.	dotJ Custom Tag Library	License
Formula Consultants, Inc.	Star 1100	License
Idea Integration	XGEN	License
Informatica Corporation	Change DataMove for DB2 Source	License
Informatica Corporation	DataMove for DB2 Source	License
Informatica Corporation	Change DataMove	License
Informatica Corporation	DataMove for IMS Source	License
Informatica Corporation	Change DataMove for IMS Source	License
Informatica Corporation	DataMove	License
Informatica Corporation	Change DataMove DB2 Target	License
Informatica Corporation	DataMove DB2 Target	License
Informatica Corporation	Change DataMove/DataMove Target for UDB	License
Informatica Corporation	SSA - Name 3	License
KMSYS Worldwide, Inc.	IQU Plus-1	License
KMSYS Worldwide, Inc.	IQU Reorg Composer	License
KMSYS Worldwide, Inc.	QPLXSS	License
KMSYS Worldwide, Inc.	QPLXSV	License
KMSYS Worldwide, Inc.	QPLXV	License
Microsoft	SQL Server Enterprise	License
SAS Institute, Inc.	Base SAS	License
SAS Institute, Inc.	SAS/ACCESS Interface for IMS	License
SAS Institute, Inc.	SAS/ACCESS DB2	License
SAS Institute, Inc.	SAS/AF	License
SAS Institute, Inc.	SAS/FSP	License
SAS Institute, Inc.	SAS/GRAPH	License
SAS Institute, Inc.	SAS/SHARE	License
SAS Institute, Inc.	SAS/STAT	License
SMA	OpCon/xps EXEC LSAM, Group 3	License
SMA	OpCon/xps EXEC LSAM, Group 8	License
SMA	OpCon/xps EXEC LSAM, Group 14	License
SMA	OpCon/xps Microsoft LSAM	License
SMA	OpCon/xps User Interface	License
Sybase	EAServer Deploy Advanced - Active	License

Third Party Software

Third Party Software

Field Name ==>	Product Name	Unit
Description / Use *==>*	*Unique Identifier*	*Unit*
Vendor	**Product**	
Sybase	EAServer Deploy Advanced - Passive	License
TRILOGexport, Inc.	TriTune Automation Component (APC)	License
Unicon Group Ltd.	LOUIS II Database Gateway	License
Unicon Group Ltd.	LOUIS II DMS Interface	License
Unicon Group Ltd.	LOUIS II Extract & Reporting Module	License
Unicon Group Ltd.	LOUIS II LCOM Host Module	License
Unicon Group Ltd.	LOUIS II MAPPER Interface	License
Unicon Group Ltd.	LOUIS II RDMS Interface	License
Verisign	Secure Site Pro SSL	License
WinZip	Self-Extractor 10-user license	License

Request for Proposal

RFP # 6100022698

Commonwealth of Pennsylvania
Office of Administration
Office for Information Technology

Data Center Computing Services

Schedule D

Transition Milestones

Milestones include the completion of all tasks, deliverables and interim milestones associated with such Milestone as set forth in the Transition Plan. The Earn Back period is thirty (30) calendar days from the Transition Milestone Due Date and applies to those Milestones indicated with "Y" in the Earn Back column. The Acceptance Criteria for each Milestone includes criteria described in Schedule F and Schedule K of the contract.

Note: If a Milestone is dependent on another Milestone and the first Milestone is missed, the subsequent Milestones remain in effect. An example is: if M-3 is missed, M-5 is still enforced.

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
M-1	Key Staffing	30 calendar days from Contract Effective Date	• Key Personnel team completed per Schedule G • staffing plan approved • detailed project organizational chart approved • resumes for each key personnel listed on the team submitted • staff contingency plan approved	$50,000 One-time	N	• Commonwealth review and approval
M-2	Contract Management Plan	60 calendar days from Contract Effective Date	• Delivery and acceptance of the following Deliverables from Schedule K: o D-11.01 o D-11.02	$50,000 One-time	Y	• Commonwealth review and approval
M-3	Datacenter Architecture Plan and Roadmap	90 calendar days from Contract Effective Date	• Delivery and acceptance of the following Deliverables from Schedule K: o D-01.01 o D-01.02 (Initial Deliverable Approval) o D-01.03 (Initial Deliverable Approval) o D-01.04 (Initial Deliverable Approval) o D-01.05 (Initial Deliverable	$150,000 One-time	Y	• Commonwealth review and approval

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			Approval) o D-01.07 o D-03.01 o D-03.04 o D-03.08 o D-04.01 o D-04.05			
M-4	Detailed Transition Plan	180 calendar days from Contract Effective Date	• Completion of Data Gathering o All data gathering checklists completed, validated, reviewed and approved • Completion, submittal and acceptance of data gathering report on B2B interface to Commonwealth's ITSM system that includes interfaces for the following: o Incident Management o Change Management o Problem Management o Known Errors o Request Management o Invoicing Process • Completion and acceptance of the Detailed Transition Plan using Schedule M – Detailed Transition Plan • Delivery and acceptance of the following Deliverables from Schedule K: o D-05.01 o D-05.04 o D-05.10	$250,000 One-time	N	• Commonwealth review and approval

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			o D-10.01 • The Detailed Transition plan must contain: o An **overall (master) plan** which includes but is not limited to: ▪ transition governance plan ▪ transition risk and mitigation plan ▪ due diligence timeline ▪ configuration / testing verification ▪ operational readiness o A **plan by Datacenter** which includes but is not limited to: ▪ transition governance plan ▪ transition risk and mitigation plan ▪ due diligence timeline ▪ configuration / testing verification ▪ operational readiness o A **plan by Agency** which includes but is not limited to: ▪ transition governance plan ▪ transition risk and mitigation plan ▪ due diligence timeline ▪ configuration / testing verification ▪ operational readiness o A **plan by Application** which includes but is not limited to:			

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			▪ transition governance plan ▪ transition risk and mitigation plan ▪ due diligence timeline ▪ configuration / testing verification ▪ operational readiness			
M-5	Commonwealth Compute Process Manual (CCPM)	180 calendar days from Contract Effective Date	• Delivery and acceptance of the following Deliverables from Schedule K: o D-02.01 o D-02.04 o D-02.09 o D-02.15 o D-02.17 o D-02.18 o D-02.23 o D-02.26 o D-02.29 o D-02.32 o D-02.37 o D-02.42 o D-02.47 o D-02.52 o D-02.57 o D-02.62 o D-02.67 o D-02.70 o D-02.75 o D-02.81 • Completion and Acceptance of final	$75,000 One-time	Y	• Commonwealth review and approval

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			CCPM as listed within Schedule L of this contract. This includes but is not limited to: o Incident (including Security) o Problem o Change o Order/Request o Billing o Service Level			
M-6	Network Connectivity	120 calendar days from Contract Effective Date	• Completion and Acceptance of the Network Connectivity to the Commonwealth	$250,000 One-time	N	• Commonwealth review, testing and approval
M-7	Security	180 calendar days from Contract Effective Date	• Completion and acceptance of security architecture, solution, policies and procedures which included but is not limited to: o Delivery and acceptance of the following Deliverables from Schedule K: ▪ D-07.01 ▪ D-07.06 ▪ D-01.03 (Initial Deliverable Approval) ▪ D-09.01 ▪ D-09.02 o Implement security management plan o Implement security and firewall plan o Policies and procedures are in place	$250,000 One-time	N	• Commonwealth review and approval

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			for physical security o Policies and procedures are in place for data and network security o Policies and procedures are in place for personnel security, such as annual background checks o Security assessment is conducted to ensure data safety and confidentiality			
M-8	ITSM System Integration	180 calendar days from Contract Effective Date	• Completion and Acceptance of Integration between Commonwealth's ITSM system and Offeror's ITSM System including but is not limited to: o Incident connectivity has been tested and incidents created and updated on either side flow back and forth between systems o Problem connectivity has been tested and problems created and updated on either side flow back and forth between systems o Change requests connectivity has been tested and requests created and updated on either side flow back and forth between systems o Configuration items in both system CMDBs are reconciled o Test Invoices have been processed through the ITSM system to the Commonwealth's AP system o Reporting from Offeror's ITSM system is available to	$100,000 One-time	Y	• Commonwealth review and approval

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			Commonwealth			
M-9	Financial Management	180 calendar days from Contract Effective Date	• Completion and acceptance of billing process and form of invoice approved • Schedule K Deliverable D-02.01 completed • Process implemented, tested and accepted providing an enterprise bill providing the details required by the Commonwealth	$75,000 One-time	Y	• Commonwealth review and approval
M-10	Operational Readiness	240 calendar days from Contract Effective Date	• Completion and acceptance of an Operational Readiness Report indicating Offeror is "Ready" to transition the Commonwealth's Applications and Services to other Datacenters. This report must include but is not limited to the following: o Delivery and acceptance of the following Deliverables from Schedule K: ▪ D-01.01 ▪ D-01.02 ▪ D-01.03 ▪ D-01.04 ▪ D-01.05 ▪ D-01.06 ▪ D-01.07 o Transition Project Office established and fully staffed o Program plan and architecture developed and approved by the Commonwealth	$150,000 One-time	N	• Commonwealth review and approval

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			o Processes and Tools implemented to support the transition change control, schedule, quality, communications, risk and issue management o Datacenter environment configured , tested and acceptance			
M-11	SSAE 16 Audits of EDC	On the July 31st following the Commonwealth's acceptance of Milestone M-14	• Completion and Issuance of a SSAE-16 Audit Reports as detailed with the Appendix A (Terms and Conditions) on the Commonwealth's EDC Datacenter • Schedule K Deliverable D-08.02	$100,000 One-time	Y	• Commonwealth review and approval
M-12	DPH Transition Completed (1)	18 months from Contract Effective Date	• Completion and acceptance of ALL applications transitioned from the DPH to new Datacenters which includes but is not limited to the following for each application: o High availability, backup and DR are operational for identified systems. o CCPM specific details for application are available in KMP. o Operations dashboards to report immediately on status and alerts for transitioned applications. o Service Level agreements are identified and supporting metrics in place. o System operational for scheduling and	$2,500,000 per month or partial month for six (6) months	N	• Commonwealth review and approval of work product plus assisting in data gathering, planning, ordering, implementing, testing and accepting the transition of the applications

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			tracking of ticket-based tasks and incidents. o System is available to begin data collection to produce configuration, monitoring and management status reports. o Systems with DR plans have an updated DR plan and test scheduled. o Operational support assumed and workloads migrated. • High-Speed direct link to current DPH location is disconnected. • Signoff that all Services provided by DPH have been successfully transitioned			
M-13	DPH Transition Completed (2)	24 months from Contract Effective Date	• Completion and acceptance of ALL applications transitioned from the DPH to new Datacenters which includes but is not limited to: o High availability, backup and DR are operational for identified systems. o CCPM contains specific details for apps transitioned are available in KMP. o Operations dashboards are in place to report immediately on status and alerts for transitioned apps. o Service Level agreements have been identified and supporting metrics in place. o System is operational for scheduling and tracking of ticket-based tasks and incidents. o System available to begin data collection in order to produce	$5,000,000 per month or partial month	N	• Commonwealth review and approval of work product plus assisting in data gathering, planning, ordering, implementing, testing and accepting the transition of the applications

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			configuration, monitoring and management status reports. o Systems with DR plans have a replacement plan and test scheduled. o Operational support has been assumed and workloads migrated. o High-Speed direct link to current DPH location is disconnected. o Signoff that all Services provided by DPH have been successfully transitioned			
M-14	EDC Operational Transition Completed	12/31/2014	• Completion and acceptance of operational control and support of the EDC which includes but is not limited to the following: o Schedule K deliverable D-01 o Schedule K deliverable D-08.01 o Schedule K deliverable D-08.06 o Verification CMDB of record with Offeror's configuration info includes EDC assets and CI's o Service catalogs, processes, and procedures are transitioned o Multi environments/instances are available for identified systems o High availability, backup and DR are operational for identified system o CCPM specific details for applications are available in KMP. o Operations dashboards are in place to report immediately on status and alerts for apps o Service Level agreements have been identified and supporting metrics in	$100,000 per month or partial month	N	• Commonwealth review and approval of work product plus assisting in data gathering, planning, ordering, implementing, testing and accepting the transition of the applications

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			place o System is operational for scheduling and tracking of ticket-based tasks and incidents o System is available to begin data collection in order to produce configuration, monitoring and management status reports o Transition orders completed and accepted by the Commonwealth			
M-15	Department of Labor and Industry Datacenter Transition Completed	30 months from Contract Effective Date	• Completion and acceptance of ALL applications transitioned from the DLI Datacenter to new Datacenters which includes but is not limited to the following: o Service catalogs, processes and procedures fully established, documented and approved o Multi environments and instances are fully functional for transitioned systems o High availability, backup and DR are operational for transitioned systems o CCPM contains specific details for apps transitioned are available in KMP o Operations dashboards are in place to report immediately on status and alerts for transitioned apps o Service Level agreements have been identified and supporting metrics in place o System is operational for scheduling and tracking of ticket-based tasks and incidents o System available to begin data	$1,000 000 One-time	N	• Commonwealth review and approval of work product plus assisting in data gathering, planning, ordering, implementing, testing and accepting the transition of the applications

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			collection in order to produce configuration, monitoring and management status reports o Transition orders completed and accepted by the Commonwealth			
M-16	Department of Revenue Datacenter Transition Completed	30 months from Contract Effective Date	• Completion and acceptance of ALL applications transitioned from the DOR Datacenter to new Datacenters which includes but is not limited to the following: o Service catalogs, processes and procedures fully established, documented and approved o Multi environments and instances are fully functional for transitioned systems o High availability, backup and DR are operational for transitioned systems o CCPM contains specific details for applications transitioned are available in KMP o Operations dashboards are in place to report immediately on status and alerts for transitioned apps o Service Level agreements have been identified and supporting metrics in place o System is operational for scheduling and tracking of ticket-based tasks and incidents o System available to begin data collection in order to produce configuration, monitoring and management status reports o Transition orders completed and	$1,000,000 One-time	N	• Commonwealth review and approval of work product plus assisting in data gathering, planning, ordering, implementing, testing and accepting the transition of the applications

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			accepted by the Commonwealth			
M-17	Pennsylvania State Police Datacenter Transition Completed	30 months from Contract Effective Date	• Completion and acceptance of ALL applications transitioned from the PSP Datacenter to new Datacenters which includes but is not limited to the following: o Service catalogs, processes and procedures fully established, documented and approved o Multi environments and instances are fully functional for transitioned systems o High availability, backup and DR are operational for transitioned systems o CCPM contains specific details for applications transitioned are available in KMP o Operations dashboards are in place to report immediately on status and alerts for transitioned apps o Service Level agreements have been identified and supporting metrics in place o System is operational for scheduling and tracking of ticket-based tasks and incidents o System available to begin data collection in order to produce configuration, monitoring and management status reports o Transition orders completed and accepted by the Commonwealth	$1,000,000 One-time	N	• Commonwealth review and approval of work product plus assisting in data gathering, planning, ordering, implementing, testing and accepting the transition of the applications
M-18	Department of Public Welfare Datacenter	30 months from Contract	• Completion and acceptance of ALL applications transitioned from the DPW Datacenter to new Datacenters which	$1,000,000 One-time	N	• Commonwealth review and approval of work product plus assisting in data

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
	Transition Completed	Effective Date	includes but is not limited to the following: o Service catalogs, processes and procedures fully established, documented and approved o Multi environments and instances are fully functional for transitioned systems o High availability, backup and DR are operational for transitioned systems o CCPM contains specific details for apps transitioned are available in KMP o Operations dashboards are in place to report immediately on status and alerts for transitioned apps o Service Level agreements have been identified and supporting metrics in place o System is operational for scheduling and tracking of ticket-based tasks and incidents o System available to begin data collection in order to produce configuration, monitoring and management status reports o Transition orders completed and accepted by the Commonwealth			gathering, planning, ordering, implementing, testing and accepting the transition of the applications
M-19	Department of Health Datacenter Transition Completed	30 months from Contract Effective Date	• Completion and acceptance of ALL applications transitioned from the DOH Datacenter to new Datacenters which includes but is not limited to the following: o Service catalogs, processes and procedures fully established, documented and approved	$1,000,000 One-time	N	• Commonwealth review and approval of work product plus assisting in data gathering, planning, ordering, implementing, testing and accepting the transition of the applications

Milestone Number	Transition Milestone	Milestone Due Date	Acceptance Criteria	Milestone Credit	Earn Back	Dependency on Commonwealth
			o Multi environments and instances are fully functional for transitioned systems o High availability, backup and DR are operational for transitioned systems o CCPM contains specific details for apps transitioned are available in KMP o Operations dashboards are in place to report immediately on status and alerts for transitioned apps o Service Level agreements have been identified and supporting metrics in place o System is operational for scheduling and tracking of ticket-based tasks and incidents o System available to begin data collection in order to produce configuration, monitoring and management status reports o Transition orders completed and accepted by the Commonwealth			

Request for Proposal

RFP # 6100022698

Commonwealth of Pennsylvania
Office of Administration
Office for Information Technology
Data Center Computing Services

Schedule E

Offeror Datacenter Locations

[The Offeror will list the address of proposed Datacenter locations that will host the Commonwealth's applications and data].

Request for Proposal

RFP # 6100022698

Commonwealth of Pennsylvania

Office of Administration

Office for Information Technology

Data Center Computing Services

Schedule F

COPA Datacenter Statement of Work

Contents

1 Offeror Guidelines 4
1.1 Offeror Instructions 4
2 Program Objectives and Summary Solution Requirements 5
2.1 Program Objectives 5
2.2 Service Level Agreements 7
2.3 Target Solution Requirements Overview 7
2.3.1 Target Datacenter 2+ Architecture 7
2.3.2 IP conversion strategy 8
2.3.3 Common Services Portfolio 9
2.3.4 Data Protection 10
2.3.5 Transition Services 12
3 Tasks 12
3.1 Establish Datacenter Architecture 12
3.1.1 Multi Datacenter Environment (2+ Architecture) 14
3.1.2 Network and Security Architecture 16
3.1.3 Datacenter Architecture and Technology 18
3.2 Enable Common Service Portfolio 22
3.2.1 Program & Service Management 23
3.2.1.1 PMO & Contract Management 23
3.2.1.2 Availability/SLA Management 37
3.2.1.3 Change & Release Management 41
3.2.1.4 Service Desk 44
3.2.1.5 Technical Architecture 49
3.2.1.6 Account Management 55
3.2.1.7 Configuration Management 57
3.2.1.8 3rd Party License Management 60
3.2.2 Technical Services 61
3.2.2.1 Transition Management (New Customer and/or Services) 61

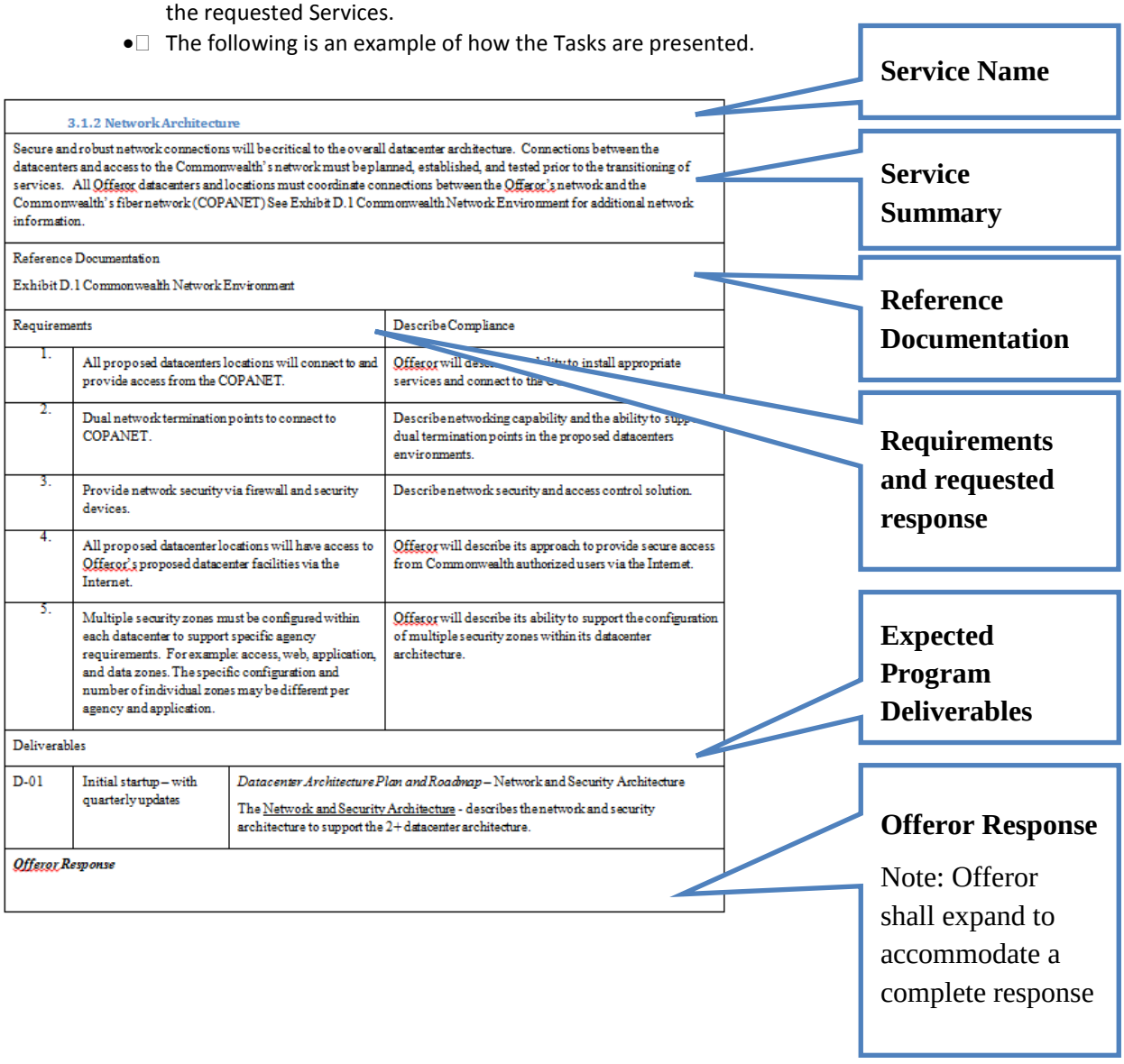
3.2.2.2 Infrastructure Architecture 64
3.2.2.3 Capacity Management 69
3.2.2.4 DR Planning & Testing 72
3.2.2.5 Security Management 76
3.2.2.6 Performance Monitoring & Management 81
3.2.3 Facilities Management 85
3.2.3.1 Facilities Architecture / Maintenance 85
3.2.3.2 Site Operations 89
3.2.4 Managed Hosting Services 95
3.2.4.1 Windows Support 95
3.2.4.2 Storage Management 101
3.2.4.3 ERP Hosting – SAP / Oracle 106
3.2.4.4 UNIX Support – AIX / Linux 111
3.2.4.5 Mainframe Services 117
3.2.4.6 Security & Firewall 124
3.2.4.7 Database Management Services 129
3.2.4.8 Limited-Use Colocation Services 132
3.2.5 Capacity on Demand Services 134
3.2.5.1 Server Capacity on Demand 134
3.2.5.2 Storage Capacity on Demand 137
3.2.5.3 DR Infrastructure on Demand 139
3.2.5.4 Additional Technical Services 141
3.3 Transition Services 142
3.3.1 Transition Services – Guiding Principals 142
3.3.2 Transition Planning/Governance 144
3.3.2.1 Transition Program Management 147
3.3.2.2 Security Transition Activities 154

1 Offeror Guidelines

This Schedule contains the primary scope of Services required to support the Commonwealth's Enterprise Datacenter Services program. The Offeror must respond to the requirements contained in this Schedule according to the instructions provided below.

1.1 Offeror Instructions

- The Offeror's response to the RFP must reflect and comply with the information contained in this Schedule and any Referenced Schedules and Exhibits.
- The Offeror must provide responses to the section 3 Tasks. After reviewing each of the service requirement tables, the Offeror should provide its response. Responses must address the stated requirements as well the additional information on Offeror's approach and how it would deliver the requested Services.
- The following is an example of how the Tasks are presented.



3.1.2 Network Architecture

Secure and robust network connections will be critical to the overall datacenter architecture. Connections between the datacenters and access to the Commonwealth's network must be planned, established, and tested prior to the transitioning of services. All Offeror datacenters and locations must coordinate connections between the Offeror's network and the Commonwealth's fiber network (COPANET) See Exhibit D.1 Commonwealth Network Environment for additional network information.

Reference Documentation

Exhibit D.1 Commonwealth Network Environment

Requirements		Describe Compliance
1.	All proposed datacenters locations will connect to and provide access from the COPANET.	Offeror will desc… ability to install appropriate services and connect to the …
2.	Dual network termination points to connect to COPANET.	Describe networking capability and the ability to supp… dual termination points in the proposed datacenters environments.
3.	Provide network security via firewall and security devices.	Describe network security and access control solution.
4.	All proposed datacenter locations will have access to Offeror's proposed datacenter facilities via the Internet.	Offeror will describe its approach to provide secure access from Commonwealth authorized users via the Internet.
5.	Multiple security zones must be configured within each datacenter to support specific agency requirements. For example: access, web, application, and data zones. The specific configuration and number of individual zones may be different per agency and application.	Offeror will describe its ability to support the configuration of multiple security zones within its datacenter architecture.

Deliverables

D-01	Initial startup – with quarterly updates	*Datacenter Architecture Plan and Roadmap* – Network and Security Architecture The Network and Security Architecture - describes the network and security architecture to support the 2+ datacenter architecture.

Offeror Response

2 Program Objectives and Summary Solution Requirements

2.1 Program Objectives

The Commonwealth is seeking to implement a new datacenter service model that will provide various infrastructures/computing platforms to service the needs of the Commonwealth in a secure and flexible manner. This initiative will realize the following objectives:

- Provide a reliable, flexible, secure, and robust IT infrastructure to support the transformation of the Commonwealth into an information-focused organization.
- Provide a multiple datacenter architecture utilizing the Offeror's proposed datacenter assets that will support the current and future capacity and service level demands.
- Include primary support for the Commonwealth's Enterprise Datacenter (EDC) operations and its computing assets including but not limited to datacenter facilities operations and infrastructure support (see **Exhibits D.1 through D.7** EDC Exhibits for description of the facility, servers, storage and tape equipment).
- Leverage Offeror's established processes and tools necessary to ensure consistent and predictable pricing to facilitate accurate and timely budget projections.
- Provide engineering support that will anticipate changes in business and technical requirements and make recommendations for staying current with industry best practices.
- Ensure that the Offeror's datacenters adhere to the Commonwealth's contractual, regulatory, and policy compliance requirements for security, architecture, and systems development life cycle (SDLC) standards.
- Establish a tiered service/capability to support high-availability hosting, backup, and disaster recovery (DR) Services to maintain continuity of government operations.
- Provide multiple environments and instances to support the enterprise application portfolio. For example; Development, Integration, System / User Acceptance Test (SAT/UAT), Training, load Testing, Pre-Production and Production.
- Continue to consolidate Commonwealth datacenters to achieve cost savings, energy consumption reductions, optimal space utilization, and improvements in IT asset utilization in accordance with the government-wide datacenter consolidation initiative currently underway.

Currently, Commonwealth datacenter resources are decentralized, owned and operated under multiple datacenter service catalogs, processes and procedures. At times, this presents the Commonwealth with barriers to establishing interoperability between datacenters, implementing standard processes and procedures for datacenter oversight, and ensuring compliance with the same standards for datacenter operations. To resolve these issues, the Commonwealth intends, under this single procurement vehicle, to contract with a service provider that currently owns, maintains and operates a group of geographically dispersed world-class datacenters (meeting or exceeding Tier 3 standards) located in the continental United States.

To satisfy the Commonwealth diverse datacenter requirements, the Offeror must be capable of providing the necessary infrastructure for the following critical purposes:

- Provide production, development and hosting of new and legacy business applications and databases that run on mainframes (IBM and Unisys), mid-ranges and distributed platforms
- Support options for high-availability, backup/recovery, and multiple levels of DR Services in support of the Commonwealth.

The Offeror's datacenter architecture must consist of multiple geographically dispersed datacenters, referred below as a 2+ (two-plus) architecture. The Offeror must utilize the EDC as one of its datacenters and propose a minimum of one additional datacenter to meet the 2+ architecture requirement. It is the Offeror's option to utilize the EDC as one of its primary datacenters within its proposed solution. It is the Commonwealth's requirement that the Offeror datacenters will have the ability to provide multiple levels of DR Services in the event of a disaster, which must also include an option to support high availability (HA) application infrastructures.

The Offeror is responsible for ensuring successful delivery of IT infrastructure Services, providing the Commonwealth with visibility into (performance, capacity, security, SLA's etc.), as well as, working in partnership with the Commonwealth as required to ensure seamless operations. In turn, the Commonwealth's role will be to provide oversight to ensure that the Offeror is delivering agreed-upon Services and that the business requirements are clearly communicated and satisfied, and provide timely feedback on contractor performance. Commonwealth agencies, OA/OIT and the Offeror will work together on IT planning, including service and capacity planning, strategic and tactical planning, and IT resource and budget planning. The Commonwealth believes that this combination of industry knowledge, government oversight, and collaboration will result in successful partnership between the private sector and the Commonwealth.

The datacenter approach must provide a computing infrastructure that delivers reliable, effective and technologically current Services seamlessly to the Commonwealth in a cost-effective manner. The cost for those Services must remain less than the cost the Commonwealth would have incurred for providing the same infrastructure itself. Applications hosted in the Offeror's datacenters must meet Quality of Service (QoS) requirements as determined by the Commonwealth agency application owners. The Commonwealth will avoid capital expenditure by acquiring Services through Capacity on Demand. The Commonwealth agencies will consume resources as a service and pay only for those resources that it uses. The Commonwealth and Offeror must engage in proactive oversight of datacenter operations. The Commonwealth requires visibility into the Offeror's management practices and effective monitoring channels that include the following:

- Program and project progress reports that track milestones, deliverables, risks, and financial data.

- Commonwealth Computing Procedures Manual (CCPM) that provides up-to-date detailed description of all processes and procedures used to support the computing needs of the Commonwealth via the Offeror's Knowledge/Service Management Portal (KMP). The CCPM must contain specific sections dedicated to the operational procedures for each Commonwealth datacenter customer.
- Scheduling and tracking of ticket-based tasks and incidents.
- Operations dashboards with status and alerts based on real-time and historic data collected by instruments, agents, scanners, and logs that monitor the hosted applications, batch operations, network, security, and service performance measures.
- Other configuration, monitoring and management status reports as needed.
- Recommendations and offerings by the Offeror for improved processes and procedures for delivery of Services that are based on a program of continuous quality and process improvement as implemented by the Offeror.

2.2 Service Level Agreements

The Commonwealth has proposed a baseline set of Service Levels which the Offeror is required to consider when developing its proposed solution. The Offeror is expected to provide multiple service tiers and associated service levels within each service offered. The Offeror is also required to have or implement a quality and process improvement program that focuses not on just meeting minimum requirements but on meeting or exceeding the target requirements.

2.3 Target Solution Requirements Overview

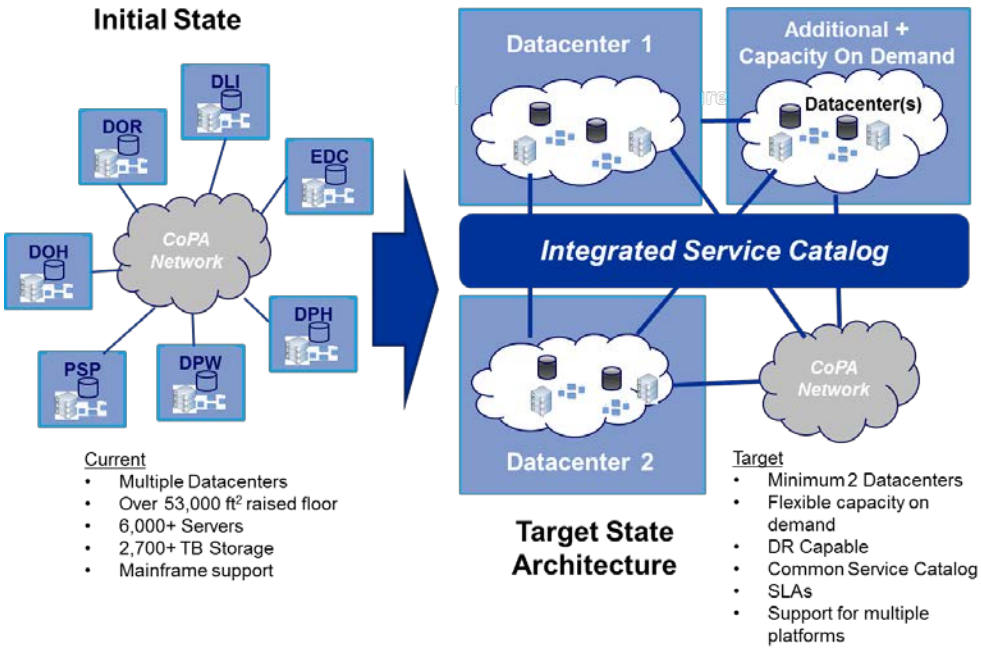
A key outcome of the Commonwealth datacenter strategy is to transition from the current individually managed datacenters with different levels of service to enterprise level datacenter architecture with a common set of basic Services combined with available specialized Services dependent upon specific customer requirements. To facilitate this request for Services, the Commonwealth has structured the solution requirements into three areas, as follows:

- Transition Services;
- Target Datacenter 2+ Architecture (includes operations support for the Commonwealth's EDC); and
- Common Services Portfolio

2.3.1 Target Datacenter 2+ Architecture

The target architecture must leverage a minimum of two geographically separated datacenters located in the continental United States that would allow for enhanced disaster recovery capabilities as well as leverage excess capacity (virtual capacity on demand). The Commonwealth requires that the architecture include operations support for the EDC. The Offeror must explain how it can leverage additional capacity from other datacenter resources within its provider network to satisfy the needs of the Commonwealth. The architecture will include support for multiple computing platforms including but not limited to x86 (physical and

virtual), midrange, mainframes, and storage systems. All of the Commonwealth computing workloads must be transitioned from the current state to the new target state architecture.



The 2+ datacenter architecture must include secure redundant network connections to the Commonwealth's network and the Internet. Offeror network connections must terminate at different end points within the Commonwealth's network. The Offeror is expected to implement a multi DR solution to limit the impact of any disruptive event at any datacenter location. This requirement is targeted for all systems that are currently covered by a DR solution. The solution must also have the capability to support future disaster recovery requirements by providing tiered DR capability within its datacenters.

Each datacenter must have the ability to support multiple security and network zones to support specific agency requirements. For example: access, web, application, and data zones. The specific configuration and number of individual zones may be different per agency and application.

To support the potential of future demand and Services beyond the capacity of the two datacenters, the Offeror must explain how it can leverage additional capacity from other datacenter resources within its provider network.

2.3.2 IP conversion strategy

The Offeror shall provide an IPv6 strategy which includes an enterprise migration plan to take the Commonwealth from the IPv4 address format to the IPv6 format.

The Offeror shall provide an infrastructure and equipment that supports IPv6 andIPv4, except were limited due to the requirement that the Initial transition approach of the Commonwealth's mainframe and SAP environments must be as close to the Commonwealth's current

configuration as possible. As technology refreshes replace this equipment, the infrastructure and equipment shall support IPv6 andIPv4

2.3.3 Common Services Portfolio

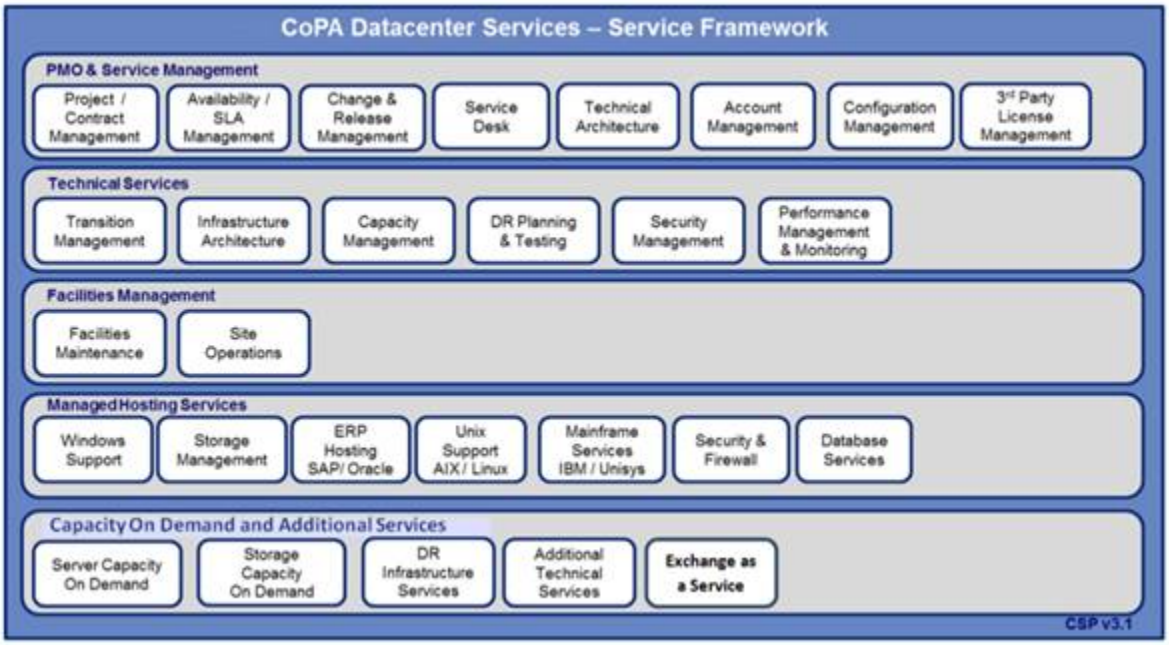
Based on the review of current and future requirements as well as industry offered Services; the following five (5) Key Services Areas will be used as a framework for the new datacenter common portfolio of Services.

Key Service Area Framework

	Key Service Area	Service Overview
1	Program Management Office (PMO) & Service Management	Provides for overall project management and operational service management (e.g. PMO, Account, Availability, Service Level Agreement (SLA))
2	Technical Services	Technical support services resources (e.g. Transition Management, Infrastructure Architecture, Capacity Planning)
3	Facilities Management	Facility operational support services (e.g. Facility Management, Operations Support)
4	Managed Hosting Services	Managed hosting/platform services for existing and future applications (e.g. Windows, Unix, SAP Hosting, Mainframe)
5	Capacity on Demand and Additional Services	Provides for additional capacity on demand offerings to support disaster recovery or increased demand for server and storage infrastructure (e.g. Cloud-centric offerings, Infrastructure as a Service (IaaS), Platform as a Service (PaaS)). Also access to additional skilled technology resources if required.

The Offeror is required to provide a complete set of Services within these service areas. The anticipated target Services are presented below and the requirements are further detailed in the Task section that follows.

Expanded Services Framework



2.3.4 Data Protection

The Offerors solution shall provide security of Commonwealth data. Offerors shall describe how they will ensure that all data (at rest and in transit) is kept secure and confidential. If Offerors proposed solution involves data residing or routing outside the continental United States; the Offeror shall disclose this in their proposal and describe how the data will be kept secure, confidential, and meet the security requirements as described in this RFP.

Offeror shall provide data protection Services including Data Loss Prevention (DLP) and Database Firewall (DBFW) Services to identify, monitor and protect sensitive and confidential Citizen Personal Identifiable Information (PII) in use, data in transit, and data at rest through deep content inspection and analysis of information exchange both at data storage locations and administrative/access endpoints.

Reference Documentation

Requirements	Describe Compliance

1.	DLP • Discover confidential data wherever it is stored, inventory sensitive data, and automatically manage data cleanup. • Monitor confidential data usage and provide enterprise visibility. • Enforce security policies to proactively secure data and prevent confidential data from leaving Commonwealth systems. • Manage policies across the enterprise, remediate and report on incidents, and detect content from centralized management platform.	Offeror must describe their approach to discover, manage, monitor, and enforce security for confidential data to meet Data Loss Prevention requirements.
2.	DBFW • Alert or block database attacks and abnormal access requests, in real time to protect against database attacks including SQL injection, Buffer overflow, Denial of Service. • Detect and patch database software vulnerabilities • Provide both agent based and network based database activity monitoring. • Audit all access to sensitive data by privileged and application users, and enforce corporate policies on data usage • Provide centralized management and advanced analytics • Discover new databases and database objects in scope for security and compliance projects and automatically apply appropriate protection and audit policies	Offeror must describe their approach to alert, detect, audit, monitor, manage, and discover attacks to meet Database Firewall requirements.
Deliverables		
Deliverables are defined in **Schedule K – Key Program Deliverables**		
Offeror Response		

2.3.5 Transition Services

Transition to the new baseline datacenter architecture and common Services portfolio must be carefully planned and executed. The Offeror is required to provide a proven methodology and plan to establish the target environment and then conduct an orderly transition of existing infrastructure and Services to the new environment.

The Offeror must transition Services from the incumbent contractor where there is an incumbent contractor, as well as, transitioning Services located at the Commonwealth managed datacenters. The Offeror must identify critical success factors and risk mitigation strategies, and describe how it will coordinate and manage other Commonwealth contractor related activities impacting the Offeror's plan. The Offeror must provide an estimate of any required Commonwealth resources, including the skills needed and the duration required for each of the resources required in order for the Offeror to implement its solution. The Commonwealth expects to provide limited resources.

The Offeror must thoroughly plan, evaluate and propose comprehensive and realistic activities and timeframes for accomplishment of transition activities given identified parameters within the Commonwealth's requirements as described in Schedule K - Key Program Deliverables and Schedule D - Transition Milestones.

3 Tasks

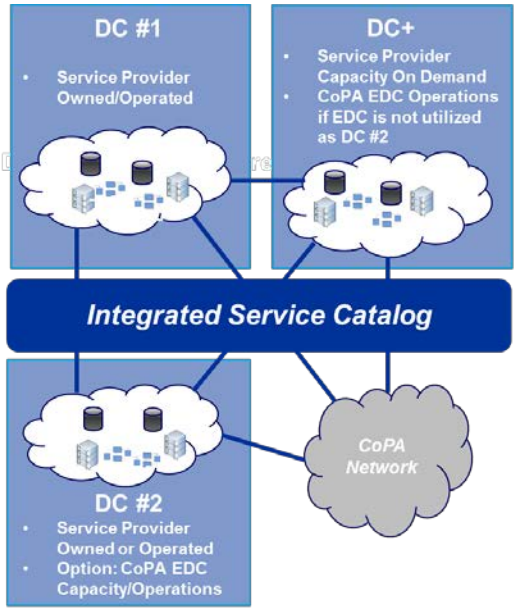
The Commonwealth has provided detailed information on the current environment for computing (mainframe, mid-range, x86, etc.), data storage, data backup (tape and other) and other datacenter related equipment in the referenced Exhibits. The Offeror shall utilize this information as the baseline requirement (in terms of Services, quantities and bandwidth) for developing its proposal.

3.1 Establish Datacenter Architecture

The Offeror must provide a multi-datacenter, multi-platform solution that will support the migration of all of the Commonwealth's current workloads. In order to support future Services, the Offeror must develop a proposal which will lead the Commonwealth into the future, and be able to address all current and future datacenter requirements. The Offeror must propose cost-effective, efficient, and forward-looking technologies for integrating Services and incorporate these technologies into its proposal. The Offeror must also address how it will allow for service updates and new technology offerings. The Offeror must describe how it will perform sizing exercises for different infrastructure to ensure the Commonwealth is getting a minimum of "like for like" or increased computing capabilities.

Baseline Architecture

In an effort to simplify the administration of IT assets, reduce IT costs, improve the provisioning of IT Services, and, in general improve the quality of IT Operations, the Commonwealth has established a preferred datacenter baseline target state architecture.



Baseline Datacenter Architecture

- Minimum 2 Datacenters
- Manage the CoPA EDC within architecture
- Flexible capacity on demand
- Redundant Secure Network Links between Datacenters and CoPA Network
- DR Capable
- Common Service Catalog
- SLAs
- Support for multiple platforms

The datacenter baseline target state architecture is based on a shared Services model in which a minimum of two geographically-separate datacenters (includes operations support for the EDC) provide a wide range of common IT Services to the Commonwealth. While not necessarily mirror images of each other, each datacenter must be capable of supporting critical Commonwealth processing in the event the other datacenter goes offline (as, for example, in the event of a datacenter disaster). To address the need for additional capacity and new Services over time the Offeror may propose additional capacity beyond the two datacenters with secure connections to other Offeror capacity.

Initially, this target datacenter combination would host the Commonwealth's existing collection of shared information systems and currently outsourced Services. Over a prescribed period of time, the new datacenter architecture must support the transition of additional IT workloads presently being processed at a variety of datacenters owned and operated by Commonwealth agencies, thus permitting these datacenters to be decommissioned.

3.1.1 Multi Datacenter Environment (2+ Architecture)

The Offeror must provide a multi datacenter environment. All datacenters will be managed and maintained by the Offeror, including the Commonwealth's EDC and may be either a standalone facility, or integrated into existing qualified facilities. The multi datacenter environment is to facilitate high availability, capacity on demand, and the recovery of applications and Services that are deemed critical to the Commonwealth. The multi datacenter requirement is to provide a minimum of two datacenters. The Offeror may propose additional capacity and Services utilizing additional facilities beyond the two required datacenters.

Reference Documentation

Schedule E – Datacenter Locations

Exhibit A - Commonwealth Network Environment

Exhibit(s) D.1 through D.15 – Enterprise Datacenter (EDC) Exhibits

	Requirements	Describe Compliance
1.	The Offeror's datacenter architecture must consist of multiple geographically disbursed datacenters. Any datacenters being used in a back-up function must be at least 50 miles apart from the associated primary location for the service.	Offeror must describe the process of establishing a multi datacenter environment, including facility management, resource sharing, operational coordination, and inter-datacenter communications. Provide proposed datacenter architecture and locations. Using **Schedule E – Datacenter locations**, the Offeror must list the address of all proposed Datacenter locations that will host the Commonwealth's applications and data.
2.	Tier III equivalent datacenter facilities proposed by the Offeror must have had consistent availability of 99.99% in the past six months as of December 31, 2011.	Offeror must provide current availability reports of its proposed datacenter(s) with its submittal.
3.	The EDC assets will be managed and maintained by the Offeror. The current maintenance contract for the EDC servers is scheduled to expire on June 30, 2014.	Offeror must describe its approach to transition operations and management of the EDC infrastructure from the Commonwealth to the Offeror's support Services and how it intend to address the server maintenance expiration issue.

4.	Each datacenters will have the capability to provide DR for the other, for identified critical applications.	Offeror must describe the process of providing DR for critical applications from one datacenter to the other. Also, describe additional DR Services if included in the overall proposed offering.
5.	Datacenter sustainability.	Offeror must describe its methods of achieving datacenter sustainability, such as realizing a low Power Usage Effectiveness (PUE) ratio.
6.	Robust physical security, including biometric access control, video surveillance, and routine security officer patrols.	Offeror must describe its security methods and techniques that will be used to protect Commonwealth computing assets and ensure compliance with Commonwealth security requirements.
7.	In a datacenter environment that hosts both Commonwealth and non-Commonwealth clients, segregation of Commonwealth data, and computing resources from other clients' data and computing resources. The Offeror is required to provide system and data segregation between different agency application environments. Note: The Offeror may not use the EDC to provide services to Non-Commonwealth clients. The Commonwealth may permit the Offeror to provide services to COSTARS members if written permission is granted by the Commonwealth.	Offeror must describe its approach to provide Services in the event a datacenter will be shared with a non-Commonwealth client, describe how segregation of resources will be achieved and maintained. Offeror must describe how systems and data segregation can be maintained between different agency application infrastructure environments.
8.	Elastic datacenter infrastructures to accommodate variable workloads.	Offeror must describe its computing and networking capabilities that will accommodate the growth or contraction of workloads.

9.	24/7/365 staffing.	Offeror must describe the staffing model used to provide 24/7/365 staffing. Operations staff, technical support staff, security staff, and management. Offeror must address how it plan to manage security/background checks, monitoring and reporting on employees and how it will coordinate those requirements with Criminal Justice agencies.
10.	Common work and meeting space.	Offeror must describe its capabilities to accommodate meeting and workspace for Commonwealth and Offeror IT staff and management.
Deliverables		
Deliverables are defined in **Schedule K – Key Program Deliverables**		
Offeror Response		

3.1.2 Network and Security Architecture

Secure and robust network connections are critical to the overall datacenter architecture. Connections between the datacenters and access to the Commonwealth's network must be planned, established, and tested prior to the transitioning of Services. All Offeror datacenters and locations must coordinate connections between the Offeror's network and the Commonwealth's fiber network (COPANET).

Reference Documentation

Exhibit A - Commonwealth Network Environment

Exhibit P – Enterprise Internet Bandwidth Utilization

Requirements		Describe Compliance
1.	All proposed datacenter locations will connect to and provide access from COPANET.	Offeror must describe its approach to connect to COPANET.

2.	Dual network termination points to connect to COPANET.	Offeror must describe its networking capability and the ability to support dual termination points in the proposed datacenters environments.
3.	Provide network security via firewall and security devices.	Offeror must describe its network security and access control solution.
4.	All proposed Offeror's datacenter facilities will have secure Internet access capabilities. Internet access must provide virus and intrusion protection systems with reporting capabilities.	Offeror must describe its approach to providing secure access from Commonwealth authorized users via the Internet. The Offeror must describe its approach to providing virus and intrusion protection and reporting.
5.	Multiple security zones must be configured within each datacenter to support specific agency requirements. For example: access, web, application, and data zones. The specific configuration and number of individual zones may be different per agency and application.	Offeror must describe its ability to support the configuration of multiple security zones within its datacenter architecture.
6.	Secure connections are required for traffic that may traverse between Datacenters and between Datacenters and Commonwealth. Encryption shall be a minimum of 128-bit and must be FIPS 140-2 certified to meet Criminal Justice Information Services (CJIS) requirements. (Refer to Pennsylvania State Police (PSP) Summary of CJIS Requirements and CJIS Security Policy.)	Offeror must describe its ability to provide secure network connectivity that meets the standards outlined in the requirement.

7.	Remote access to datacenters supporting CJIS systems must meet minimum security requirements identified in CJIS Security Policy. These requirements include but are not limited to identifying remote user's identity, IP address and connection must be FIPS 140-2 certified with a minimum of 128-bit encryption.	Offeror must describe its ability to comply with the security policies described in this requirement,

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

3.1.3 Datacenter Architecture and Technology

The Offeror must evaluate the Commonwealth computing infrastructure(s) and develop and implement an IT architecture that will support all current systems and applications, utilizing existing and/or underutilized technologies where appropriate, to provide a high level of quality computing Services to the Commonwealth, in a cost effective manner. An overall review of all Commonwealth computing Services is required, as the requirement is to consolidate all Commonwealth based computing Services into the Offeror's datacenter architecture. This architecture design is to include the current DR programs and structure and will be implemented along with the production and testing environments.

The Offeror must provide a multi-platform solution that will support the migration of all of the Commonwealth's current workloads. The Offeror must address in its design how it will create a target environment that will minimize application latency concerns.

The Offeror must also develop a proposed infrastructure environment, which will lead the Commonwealth into the future, and be able to address all current and future datacenter requirements.

Reference Documentation

Exhibit A - Commonwealth Network Environment

Exhibit(s) B.1 through B.6 - Data PowerHouse (DPH) Exhibits

Exhibit(s) C.1 through C.13 - Department of Public Welfare (DPW) Exhibits

Exhibit(s) D.1 through D.15 - Enterprise Datacenter (EDC) Exhibits

Exhibit(s) E.1 through E.43 - Department of Labor & Industry (DLI) Exhibits

Exhibit(s) F.1 through F.4 - Department of Health (DOH) Exhibits

Exhibit(s) G.1 through G.16 - PA State Police (PSP) Exhibits

Exhibit(s) H.1 through H.8 - Department of Revenue (DOR) Exhibits

Exhibit(s) I.1 through I.13 - Commonwealth SAP Environment - Integrated Enterprise Services (IES) Exhibits

Exhibit L - Master Application Inventory

Schedule J.1 - Datacenter Service Level Management

Exhibit(s) M.1 through M.7 - Department of Corrections (DOC) and Pennsylvania Board of Probation and Parole (PBPP) Exhibits

Exhibit(s) N.1 through N.2 - PennDOT Exhibits

Requirements		Describe Compliance
1.	Develop the architecture and define the technology that will be used in the target datacenter environment to support the Commonwealth computing systems.	Offeror must describe the overall architecture and technologies that will be required to run the computing requirements for the Commonwealth.
2.	Provide all technical system support and reporting including: • Multi-Platform Systems Support • Multi-Tiered Storage Management • Network Management • Security Management • Capacity planning • Performance analysis and tuning • Technology Refresh/Life Cycle Management • Annual Audits and Certifications	Offeror must describe overall strategy to provide these Services for each component of its supporting architecture.

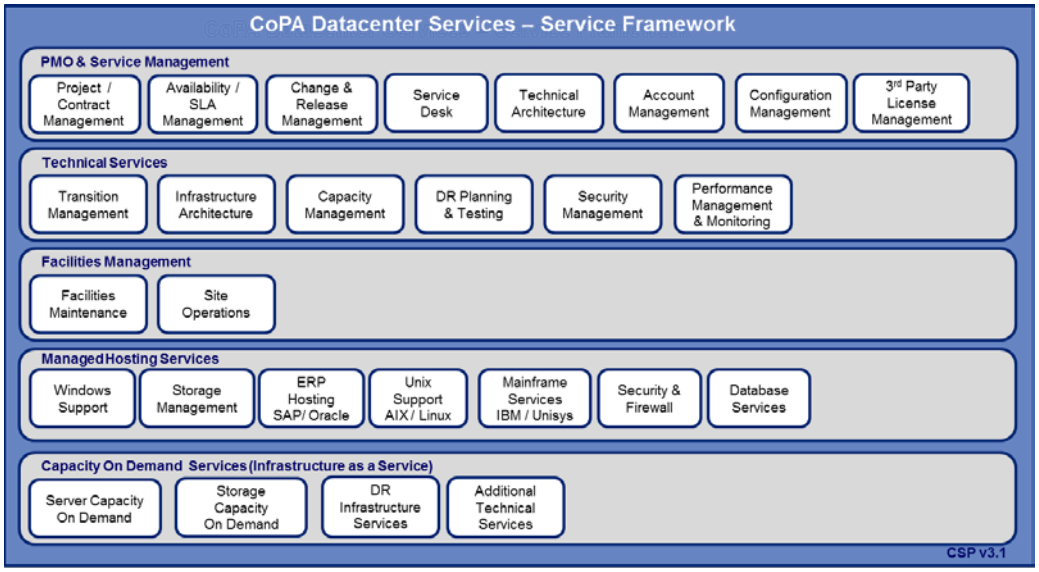
3.	Provide a storage management approach which meets the Commonwealth's needs. The storage management approach shall include, but not be limited to, the following: • **Basic** – based on Pay-As-You-Go allocation model with no upfront resource allocation and resources are reserved on demand per workload. (shared, multitenant) • **Committed** – based on Allocation Pool allocation model which gives a minimal initial commitment of resources plus the ability to burst above that minimum if additional capacity is needed – usually a percentage of resources reserved for agency with over-allocation. (shared, multitenant) • **Dedicated** – based on Reservation Pool allocation model – 100% of resources are reservation–guaranteed. (dedicated, single tenant)	Offeror must describe overall strategy to provide these Services for storage management.
4.	Provide real-time monitoring and monthly reporting of system availability, performance, utilization, and efficiency.	Offeror must describe its overall strategy to provide real-time scheduled system performance, operations, monitoring and capacity reporting for the entire datacenter architecture. Offeror must describe its strategy to support or provide real-time system and/or application monitoring

5.	Disaster Recovery - Design a tiered DR solution to ensure that applications and associated hardware that currently have an active DR plan will continue to have offsite Services available in the event of a primary system outage. The tiered DR solution must include an option to support high availability (HA) architectures. Include tiered DR solution in the overall datacenter architecture design.	Offeror must describe its tiered approach to supporting the Disaster Recovery needs of the Commonwealth.
6.	Configuration Item Reconciliation The Offeror must perform an initial asset review of the targeted inventory for all datacenter configuration items (CI) that will be managed. The Offeror must reconcile and validate that appropriate relationships exist for all datacenter configuration information in the Configuration Management Database (CMDB) system. Offeror must ensure that CIs are properly mapped in order to support the established Service Level Agreements (SLAs). The Offeror will be required to provide an automated interface between its CMDB and the Commonwealth's CMDB.	Offeror must describe its approach to gathering this configuration information.
Deliverables		
Deliverables are defined in **Schedule K – Key Program Deliverables**		
Offeror Response		

3.2 Enable Common Service Portfolio

The Commonwealth currently bases its service management practices on the Information Technology Infrastructure Library (ITIL) v3, a worldwide recognized best-practice framework for the management and delivery of IT Services throughout their full life cycle. Accordingly, the Commonwealth requires that the Offeror's service management practices be based on the ITIL v3 framework and guidance. The Datacenter Architecture, which conforms to a service-oriented structure, is prescribed by the Commonwealth common service framework. The common service framework is comprised of 27 discrete IT Services divided into five (5) categories of service:

- **PMO & Service Management** – This category of service defines the overall datacenter management structure, including interactions with the Commonwealth and business partners.
- **Technical Services** – This category of service defines the datacenter architecture, and prescribes standards for datacenter continuity and security. This level also defines the workload transition process, for when Commonwealth Agencies migrate applications to the new datacenter computing Services model.
- **Facilities Management** – This category of service defines day-to-day datacenter operations and maintenance.
- **Managed Hosting Services** – This category of service defines a set of Commonwealth enterprise datacenter managed Services, each designed to accommodate the specific needs of the Commonwealth.
- **Capacity On Demand and Additional Services** – This category of service defines a set of infrastructure as a service (IaaS) offerings, each designed to provide just-in-time resources to the Commonwealth.



3.2.1 Program & Service Management

3.2.1.1 PMO & Contract Management

The PMO & Contract Management service is responsible for the overall program, projects, and contract elements, and will maintain an active working relationship with the Commonwealth project team. Offeror must assign an executive management team that will drive the processes to complete the due diligence required to make informed decisions and Services offerings that will meet the needs and requests of the Commonwealth. This executive team will also provide ongoing direction and leadership supporting the contract and designated Services, for the duration of the Contract.

The Offeror is required to provide and maintain operational, technical, and management staff contacts so that it is clear to the Commonwealth whom is the most direct contact for each operational area.

Reference Documentation

Schedule H - CCPM Commonwealth Computing Procedures Manual

Requirements		Describe Compliance
1.	Establish and maintain a program and project management framework, throughout the term of the contract.	Offeror must describe its proposed program and project management framework that will be used to support this contract.
2.	Establish and maintain a protocol for project estimation: ▪ Scope ▪ Hardware / Software ▪ Manpower to develop, test and implement ▪ All other resources required	Offeror must describe a project estimation protocol suitable for Commonwealth data-center migration projects.

3.	Collaboration meetings, technical exchanges, and forums – Through established procedures and meetings address in good faith all issues, needs, technical exchanges and forums with the Commonwealth team. Provide the technical knowledge, and knowledgeable staff, to effectively support and guide the Commonwealth's technology needs.	Offeror must describe how it will accomplish this.
4.	Translate the Datacenter contract requirements into measurable service level objectives, and codify those requirements by creating a set of service level agreements.	Offeror must provide examples of actual datacenter service level agreements, appropriately redacted to preserve client anonymity.
5.	Establish interim contract management procedures during the transition of datacenter Services. All interim contract management procedures must be negotiated in good faith and approved by both parties.	Offeror must describe an interim procedure to monitor and manage service delivery (conforming to Commonwealth policies and procedures) including but not limited to the following; Problem Management, Change Management, Service Level monitoring and reporting, physical and logical security, project management, etc. while the service is transitioned from the Commonwealth to the Offeror.
6.	Establish and maintain a process for change management for the Datacenter contract as requested or required. The final process developed must be coordinated with the Commonwealth contract compliance group and mutually agreed to by both parties.	Offeror must describe its proposed contract change management process.

7.	Subcontractor Relationship Management - Establish and enforce standards for ensuring subcontractor performance. The Offeror is responsible for all Services provided by subcontractors.	Offeror must describe its subcontractor relationship management process.
8.	Offeror must have experience in managing and supporting Managed Service Solutions for Datacenter Infrastructure Services.	Offeror must document its qualifications within its proposal.
9.	Offeror must have the capability to provide mainframe (IBM & Unisys) Services to support the current and future needs of the Commonwealth.	Offeror must document its qualifications within its proposal.
10.	Offeror must have experience managing and supporting SAP/Oracle ERP environments.	Offeror must document its qualifications within its proposal.
11.	Offeror must be an established firm which has provided hosted datacenter Services for a period exceeding three years	Offeror must document its qualifications within its proposal.
12.	Offeror must currently operate at least 3 Datacenters. Each of those datacenters have to have been operational for at least one (1) year and have a minimum five (5) clients hosted at each.	Offeror must document its qualifications within its proposal.

13.	Offeror must have experience handling comprehensive on-site operations and maintenance of Datacenter Physical Infrastructure Services. The Services must have been provided for a continuous period of at least one year during the last three years ending 2011. The Services may not have been terminated before completion of the relevant contract.	Offeror must document its qualifications within its proposal.
Deliverables		
Deliverables are defined in **Schedule K – Key Program Deliverables**		
Offeror Response		

3.2.1.1.1 Financial Management

The Offeror must provide financial management for Services to provide accurate and cost effective stewardship of IT assets and resources. Financial management will be used to plan, control, and recover costs expended in providing the Services. Overall, the goal of financial management is to offer a truly transparent analysis of the Commonwealth spending on Services. In many cases, this analysis of efficiency will be used to create intelligent, metric-based cost-reduction strategies.

Clear and transparent invoicing, both for the Commonwealth and for individual agencies, will be required to insure integrity and accountability of all invoices. It is expected that invoicing may vary somewhat on a monthly basis whenever Services are either increased or decreased.

The Offeror is expected to work with the Commonwealth to identify major investments as part of the budgetary planning process. The Commonwealth will review strategic and tactical objectives as indicated in the planning process to measure impact on its budget(s).

A significant percentage of the Commonwealth's funding comes from federal sources. Offeror's must be able to provide detailed service information necessary to ensure the uninterrupted flow of federal funds.

On a monthly basis, the Offeror must present the Commonwealth with a single enterprise invoice and multiple agency invoices for chargeback purposes. The agency's invoices must include sufficient detail to validate and accurately allocate charges to funding sources based on actual usage.

The Offeror is required to capture and provide information related to monthly volumes of work, counts, and utilization of specific infrastructure areas. The Offeror and the Commonwealth will develop a set of detailed, equitable and repeatable chargeback procedures for each provided Service based on either actual monthly utilization or allocation methods depending on which is most appropriate. The chargeback procedures will include the ability to map to discrete programs and funding sources identified by agencies with this requirement.

The Offeror must integrate its Financial Management tool with the Commonwealth's Enterprise ITSM system which currently is BMC Remedy Billing module and processes; which may change during the term of the resulting contract. The Offeror must leverage any current chargeback procedures and implementation configuration to accelerate the implementation of the new system. The Offeror must expand the chargeback system to capture all related computing related charges associated with the Datacenter project.

Reference Documentation

N/A

	Requirements	Describe Compliance
1.	Provide a uniform rate structure which charges the same rates for the same/similar Services.	Offeror must provide detailed descriptions on the type of Services included in its overall solution. Cost information must not be provided in the technical submittal.
2.	Monthly invoicing for Services will be provided to the Commonwealth. Invoicing will identify Services rendered, pricing, and agency specific service usage. Transparency in billing will identify service cost per agency. The Commonwealth does not have a common system for charge backs. Some current services are not charged back, and some are done manually. The selected Offeror must connect to the Commonwealth's ITSM system. The Commonwealth does not require a full charge back system. The agency invoices should provide billing detail so the agency has full transparency into the services it consumed. Billing details shall include all services procured by agency general ledger (GL) code. A service may be allocated across multiple GL codes. Identify method for adjusting agency level billing due to failing to meet SLAs.	Offeror must describe its process or policies that will address this requirement. Offeror must provide at least one relevant example from a prior engagement, in which it was engaged, that is similar to the needs of the Commonwealth.

3.	Flexible pricing will be applied when Services are either increased or decreased.	Offeror must describe its process or policies that will address the flexible pricing requirements. Offeror must provide at least one relevant example from a prior engagement, in which it was engaged, that is similar to the needs of the Commonwealth.
4.	Interim Financial Management Procedures will be required as the Commonwealth transitions its current architecture to the Offeror's Services.	Offeror must describe its approach and procedure(s) for providing invoices, invoice verification and charge back to datacenter customers including but not limited to the following; service components, asset management, asset transfer, forecasting, etc.
5.	During the term of the Contract, provide cost effective approaches and suggestions to improve Services while maintaining or lowering the cost for Services. For example as the industry costs for server and storage capacity are reduced over time, it is expected that there will be a continual cost reduction in like Services within this contract.	Offeror must describe its process or policies that will address this requirement. Offeror must provide at least one relevant example from a prior engagement, in which it was engaged, that is similar to the needs of the Commonwealth.
6.	Integrate Financial Management with other service management processes, especially with SLA, Capacity and Configuration Management.	Offeror must describe how it will accomplish this.
Deliverables		
Deliverables are defined in **Schedule K – Key Program Deliverables**		
Offeror Response		

3.2.1.1.2 Governance & Policy Compliance

Major IT decisions related to this Contract will be reviewed and approved according to the Commonwealth's governance policy. These decisions are critical to the success of the Commonwealth. IT governance addresses compliance initiatives, and satisfies the need for greater accountability for decision-making.

Reference Documentation

Schedule B - Governance

	Requirements	Describe Compliance
1.	Major IT decisions will be made under the guidance of the Commonwealth governance organization.	Offeror must describe its overall compliance policy and enforcement measures. Offeror must provide at least one relevant example from a prior engagement, in which it was engaged, that is similar to the needs of the Commonwealth.
2.	Design and architecture decisions will be made with a high level of integrity and advance the interests of the Commonwealth. All designs must be approved by the Commonwealth.	Offeror must describe the overall design and architecture methodology. Offeror must provide at least one relevant example from a prior engagement, in which it was engaged, that is similar to the needs of the Commonwealth.
3.	All policies and procedures will be executed in a consistent manner to ensure the Services are completed as planned and consistent with specifications. Audits will be conducted on a yearly basis to verify and report on compliance with policies and procedures.	Offeror must describe its compliance and audit policy and enforcement measures. Offeror must provide at least one relevant example from a prior engagement, in which it was engaged, that is similar to the needs of the Commonwealth.

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

3.2.1.1.3 Subcontractor Management

The Offeror may provide some of its Services and offerings via subcontractors. The Offeror must be the prime provider of Commonwealth Services, and is responsible to contract with subcontractors, manage its subcontractors, and for Offeror's performance and the performance of its subcontractors throughout the term of the Contract.

Reference Documentation

N/A

	Requirements	Describe Compliance
1.	Obtain, manage, and be responsible for all Services or offerings provided by subcontractors. Subcontractors may change over the course of this contract. Offeror is required to notify the Commonwealth of the new subcontractor(s) and assure the Commonwealth that there will not be a conflict of interest, and that the new subcontractor meets or exceeds the qualifications of the replaced subcontractor. The Commonwealth must approve all subcontractors.	Offeror must describe / list all subcontractors that it will be utilize for this project. Describe process or policies that will address this requirement. Offeror must provide at least one relevant example from a prior engagement, in which it was engaged, that is similar to the needs of the Commonwealth.
2.	CJIS Security Policy requires fingerprint based background checks and executing a Management Control Agreement (MCA) and Security Addendum with the Pennsylvania State Police (additional information is provided in the PSP exhibit material).	Offeror must describe its process or policies that will address this requirement.

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

3.2.1.1.4 Business Partners Management

The Commonwealth has business partners such as banks and insurance companies that require connections to its hosted systems and applications. The Offeror must coordinate with the Commonwealth to support any Commonwealth – Business Partner agreements that require a committed connection to its hosted systems.

Reference Documentation

N/A

	Requirements	Describe Compliance
1.	The Offeror must provide coordination and support of Commonwealth – Business Partner agreements that require connections and Services to the Offeror's datacenter Services to ensure that any committed connections and service levels are maintained.	Offeror must describe its process or policies that will address this requirement.

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

3.2.1.1.5 Additional Planning Services

The Commonwealth may use different/additional methods for requesting technical information and support. Depending on the type of request those methods could include but not be limited to:

- Statement of Objectives (SOO)
- Work Order
- Service Request
- Request for Technical Analysis
  - Cost-Benefit Analysis
  - Conceptualization
  - High Level Estimate (HLE)
  - Technical Opinion(s)

Reference Documentation

N/A

Requirements		Describe Compliance
1.	Statement of Objectives - Perform requested additional Services across various functional areas, where the work requires funding either because of materials needed or because the activity requested is not part of the base contract.	Offeror must describe its ability and timeframes to support these additional service requests.
2.	Work Orders - Perform work across various functional areas, where the work is considered part of the base contract and where no additional funding is required.	Offeror must describe its ability and timeframes to support these additional service requests.
3.	A Service Request will be used to request work within one functional area, where the work is considered part of the base contract and where no additional funding is required.	Offeror must describe its ability and timeframes to support these additional service requests.
4.	Requests for Technical Analysis will be used to seek information regarding	Offeror must describe its ability and timeframes to support these additional

	potential technical solutions. The documents generated by the Offeror must provide the Commonwealth with direction regarding a specific technology and possibly the estimated cost to implement the solution. Four types of requests for technical analysis may be made by the Commonwealth. These requests are described below: • Cost-Benefit Analysis - A cost-benefit analysis is requested when the Commonwealth wants to know not only the implementation cost of a solution, but also the cost-benefit ratio for Commonwealth implementation of the solution. It may be used to analyze a single solution against the status quo, or compare the relative costs of multiple solutions. • Conceptualization - A conceptualization is requested when the Commonwealth has an objective, but is unsure about the possible technical means of fulfilling it. The Offeror must examine multiple paths for achieving the objective, and provide the technical benefits and consequences of the possible solutions presented. Costs are not considered in a conceptualization. • High Level Estimate (HLE or sometimes referred to as a rough order of magnitude ROM) - A HLE is requested when the Commonwealth has a clear technical direction and needs	service requests.

	rough estimates on the cost of implementing it. HLEs may be used to attach a cost estimate to a prior conceptualization or technical opinion produced by the Offeror. • Technical Opinion(s) - A technical opinion is requested when the Commonwealth has a specific technology or set of technologies it wants the Offeror to analyze for both technical merits and suitability for deployment in the Commonwealth environment. While product and operational costs provided in Offeror's literature may be considered in a technical opinion, the Offeror's deployment and operational costs will not be calculated or presented.	

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

3.2.1.1.6 Continual Service Improvement

The purpose of the Continual Service Improvement is to reduce risk, improve service quality, improve client satisfaction, and ensure service transparency through a continuous cycle of evaluation and improvement.

Reference Documentation

N/A

	Requirements	Describe Compliance
1.	Reduce service risks.	Related to the project management and contract management role, Offeror must describe its methods for eliminating or mitigating service risks.
2.	Improve service quality.	Offeror must describe its methods for addressing continuous service improvement processes.
3.	Improve client satisfaction.	Offeror must provide examples of previous Offeror initiatives aimed at continually improving client satisfaction.
4.	Ensure service transparency.	Offeror must describe its methods for ensuring service transparency and providing visibility into service execution.
5.	Customer Satisfaction Surveys – Survey of Service Desk satisfaction is a key component of providing best in class customer service. Receive completed surveys of Service Desk satisfaction from the Commonwealth and tabulating results from such surveys	Offeror must describe its approach to perform surveys of Service Desk satisfaction for a subset of the problems, questions, or requests that are resolved by, or coordinated by, the Service Desk. Offeror must describe its approach to creating and advertising a web site for day-to-day feedback from datacenter customers which is accessible through the Offeror's KMP. Offeror must describe its approach to performing a customer satisfaction survey on a quarterly basis.

6.	Improve/reduce costs	Offeror must identify its methods for addressing continuous service improvement targeted at minimizing or reducing costs of Services and operations.

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

3.2.1.2 Availability/SLA Management

The purpose of the System Availability and SLA function is to ensure that each service is delivered within, or exceeds, the agreed availability service level, and prescribed credits are received by the Commonwealth when the service level has not been achieved. Availability Management provides a point of focus and management for all availability related issues, ensuring that availability targets are established, measured, and achieved. The basic requirement is to balance the value and quality of Services with the costs of the Services. Availability and SLA management will be responsible for establishing and reviewing the SLA's to meet the Commonwealth's requirements. Offeror should review referenced exhibits for a list of SLAs and associated descriptions, tools and methodologies.

Availability/SLA Management ensures that datacenter service availability standards, as prescribed in appropriate datacenter SLAs, are achieved.

Reference Documentation

Schedule J.1 - Datacenter Service Level Management

Schedule J.2 - Datacenter Service Level Matrix

Schedule J.3 - Datacenter SLA Definitions

Requirements		Describe Compliance
1.	Establish a formal Availability and SLA Management service. This service will include representatives from the Offeror and the Commonwealth for reviewing and	Offeror must describe its methodology and approach to Availability Management and Service Level Management.

	approving the availability and SLA metrics. Offeror must publish the formal Availability and SLA Management plan based on a Service Catalog. Identify key Services and the associated level of availability or capacity as appropriate. Identify the Services that will be measured by an SLA. Define the basis the SLA service levels will be monitored and obtained. Obtain approval from the Commonwealth.	
2.	Identify Service Level Measurement Tools	Offeror must provide a list of those Service Level measurement and monitoring tools that it will use to measure and report Offeror's performance of the Services at a level of detail sufficient, as determined by the Commonwealth, to verify Offeror's compliance with those Service Levels described in **Schedule J.3 Datacenter SLA Definitions**. Offeror must review and update the required sections within Schedule J.3 Datacenter SLA Definitions. Offeror must complete the following sections in each of the Critical Service Levels and Key Measurements: • Collection Process – identify how the measurement data will be collected • Reporting Tools – identify any tools, automated or manual, that will be used • Raw Data Storage (Archives) – identify where data will be stored and accessible by the Commonwealth for further analysis. • Reporting Format/s – identify the proposed reporting format

3.	Integrate Availability Management with other service management processes, such as SLA, Capacity Management, Problem Management and Service Desk.	Offeror must describe how its proposed Availability Management process is integrated with other service management processes such as SLA, Capacity Management, Problem Management and Service Desk.
4.	Establish automated non-compliance indicators. Automatically e-mail the designated Commonwealth contact when SLA service parameters are not met. Create email notification groups by major service. Utilize this, or a similar process for outage notification.	Offeror must describe its process for managing Services performance.
5.	Investigate all instances of non-compliance. Notify the Commonwealth of an outage as defined in the CCPM. Complete a root cause analysis (RCA) for all major outages, and provide a detailed report to the Commonwealth and impacted user. Completion of the Incident report must occur within 2 days of the incident and the RCA within 10 days of the incident.	Offeror must describe its process for root cause analysis and for meeting the required SLAs. Offeror must include definitions of outage types and how it will make reports available to the Commonwealth.
6.	Identify integrated tools, methods, and activities to be used for reporting service and component availability. Ensure proactive measures to improve availability of Services are implemented whenever it is cost justified.	Offer must identify tools, methods, and activities it will use for reporting service and component availability. Offeror must describe its offerings in this area.

7.	Integrate Agency Availability Management processes with SLA Management. On a monthly basis, consolidate all system SLA availability reports into a management operations report, summarizing availability, outages, and SLA compliance by platforms.	Offeror must describe its offering in this area.
8.	Develop and maintain a Portal/Website for agencies to view operational status, planned maintenance, and component level outages.	Offeror must describe its Portal/Website to view operational status, planned maintenance and component level outages.
Deliverables		
Deliverables are defined in **Schedule K – Key Program Deliverables**		
Offeror Response		

3.2.1.3 Change & Release Management

Change & Release Management ensures that all changes within the datacenter environment are planned, executed, monitored, documented, and that the change produced the intended effect. The Offeror must establish the overall Change & Release Management function and manage the daily operations of the functions. This will ensure that all changes are processed in a uniform manner that required documentation, approvals, and notifications are completed before the change is implemented within each of the lower infrastructure environments and then moved into the production environment. Post implementation review and approval will require that all steps have been completed as documented, and within the time frame allotted. All change and release documentation must be maintained in a manner that will facilitate random compliance auditing. On a yearly basis, random selections of changes will be audited for compliance purposes.

Reference Documentation

Schedule H - Commonwealth Computing Process and Procedures Manual (CCPM)

	Requirements	Describe Compliance
1.	Establish a formal Change & Release Management function. This function will include representatives from the Offeror and Commonwealth to support the review and approval of all changes. Offeror must publish the formal Change & Release Management plan. Identify key elements and roles; Request for Change Form & Process, Change Manager, Change Advisory Board, Emergency Change Advisory Board, Notification process, Change review process. The documentation and process will follow industry best practices. Train appropriate Commonwealth staff on the process as requested by the Commonwealth. The Offeror's Change Management & Release management process must consider and integrate with the Commonwealth's individual change management policies and procedures,	Offeror must described its proposed process and provide a sample overview of its process and procedures. Offeror must describe the system tool it will use to support the Change & Release Management processes. Offeror must describe how it will integrate its Change & Release Management tool with the Commonwealth's Enterprise ITSM solution. Offeror must describe its process and procedure for the Commonwealth to perform random audits.

	for example from January to May of each year, Department of Revenue (DOR) maintains a "no update policy" to DOR servers that have any production Tax-Related Applications running on them.	
2.	Institute a Change Advisory Board (CAB) The CAB members shall ensure that the requested changes are thoroughly checked and assessed from both a technical and business perspective.	Offeror must describe its proposed approach to creating a CAB and describe how members should be selected. Offeror must describe its approach to handling changes at an agency level. Offeror must provide a sample CAB organization and meeting schedule.
3.	Test infrastructure related changes & releases before implementation. This includes Offeror managed hardware and any Offeror managed software. Offeror must file a Pre-Change Test Plan, as part of the Change & Release request process, including results before final approval to proceed. Offeror must create and maintain test environments where testing will be conducted and evaluated prior to implementing any change into production environments.	Offeror must described its proposed process and provide a sample overview of process and procedures.
4.	Establish scheduled maintenance periods, and communicate the scheduled outages. Create a notification process for maintenance, emergency, and unplanned outages. Offeror must establish regular maintenance periods for each computing platform. Maintenance periods must be coordinated per agency due to different peak business requirements. Create mechanism to notify clients of	Offeror must describe its process for managing maintenance periods and system outages, with examples. The Offeror must provide an approach to managing multiple agency specific maintenance periods with different peak periods.

	expected and unexpected outages.	
5.	Notify affected Commonwealth agencies before and after any changes. Provide Change & Release Notifications prior to implementation via a central web site and e-mail.	Offeror must describe its proposed process and procedure related to notifications. Offeror must describe any other change notifications capabilities available to the Commonwealth.
6.	Validate all changes after implementation. Complete a post change review to validate the success or failure of the change or release, and post the information within the change record. Take follow up action as appropriate.	Offeror must describe its proposed process and procedure.
7.	Prepare back out procedures for all changes. As part of the Change & Release process, file a back out plan as appropriate to remove the change and restore Services to the prior level.	Offeror must describe its proposed process and procedure related to back out procedures.
8.	Track all (successes / failures) changes and produce Change & Release management statistics. Create and deliver a monthly Change & Release Management Report to the Commonwealth, detailing changes, implementation status, and outage time periods as compared to planned outage schedules.	Offeror must describe its proposed process and procedure.
Deliverables		
Deliverables are defined in **Schedule K – Key Program Deliverables**		
Offeror Response		

3.2.1.4 Service Desk

As part of the Services, Offeror shall provide telephone support (e.g., a "Service desk") to the Commonwealth to assist the appropriate end users in determining, tracking and resolving questions regarding the Services. Offeror shall provide telephone support through such telephone support infrastructure maintained by the Offeror. This telephone service desk is to augment the required “online” Service Desk capabilities as set forth in the RFP.

The Service Desk will be the single point of contact for authorized Commonwealth users regarding incidents, which include events that cause or may cause an interruption or reduction of service, as well as requests for information, and requests for Services relating to all of the Services provided within the Offeror’s catalog of Services. The Offeror’s Service Desk must have processes for Service Delivery and Service Management that are ITIL-conformant. The Service Desk process includes Service Management processes: Incident Management, Problem Management, Change Management, Configuration Management and Service Request Management.

Currently most Commonwealth agencies provide a local Help Desk function to support staff’s desktops, local printing systems, applications, and the general public users it serves. The Offeror must develop a process and electronic connection to these agency Help Desks. The majority of the agency Help Desks utilize the Commonwealth’s Enterprise ITSM. A connection between the Commonwealth’s Enterprise ITSM and the Offeror’s Service Desk will be required to keep Help Desk tools synchronized.

In addition, the Offeror must provide an Internet accessible KMP as a central repository for processes and procedures, communications plans, and other relevant documentation to be shared with the Commonwealth. Knowledge Management will be a function shared by the Commonwealth along with the Offeror. This will allow the Commonwealth to combine data from all Commonwealth agencies and the Offeror, reorganize it, make it understandable, and present it to the Commonwealth.

The Offeror must coordinate with the Commonwealth to provide feedback on the effectiveness and accuracy of KMP content. In addition, the Offeror must notify the Commonwealth when incorrect information is identified, reference material becomes outdated, or when the content is rendered inaccurate. At the Commonwealth’s discretion, the Offeror may be required to develop content, as needed, including answers to frequently asked questions, reference/educational materials, and other documents to be added at the Commonwealth discretion.

The Offeror must create and keep current a CPPM that documents the processes, procedures and timelines used to meet the requirements of this contract. The CPPM must provide detailed process descriptions to support the computing needs of the Commonwealth utilizing best practices and be made available (via Offeror’s Portal) to all Commonwealth agencies throughout the term of the contract.

Reference Documentation

Exhibit K - OA Enterprise ITSM System and Volumetrics

Schedule H - Commonwealth Computing Procedures Manual (CCPM)

Requirements		Describe Compliance
1.	Provide an integrated Service Desk process with the other Service Management processes, including Incident Management, Problem Management, Change Management, Configuration Management and Service Request Management. The final Service Desk processes and procedures must consider current Commonwealth service management policies and procedures.	Offeror must describe its Service Desk solution offering (processes, procedures, staffing, and technologies). Offeror must provide a sample of its KMP from a previous or current engagement of Offeror.
2.	Provide a Service Desk with processes and tools for Service Delivery and Service Management that are ITIL-conformant.	
3.	Seamlessly integrate the Service Desk (including tools, technology and processes) with the Service/Help Desk(s) of other identified Agency Service Desks as required. The Offeror must coordinate the integration of the proposed Service Desk with the Commonwealth's Enterprise ITSM System and other agency Help Desks as required. Integration with other agency ITSM systems is not required.	
4.	Analyze incident trends, and recommend and implement actions, with Commonwealth's approval, to reduce incidents.	
5.	Conduct random surveys of authorized users of the Service Desk in accordance	

	with the Commonwealth each month.	
6.	Develop and document processes regarding interfaces, interaction, and responsibilities between Level 1 Support personnel, Level 2 Support personnel, and any other internal or external persons or entities that may either submit notice of an incident or receive notice of an incident.	
7.	Ensuring staffing levels and work allocation remains appropriate to handle incident volumes and incident response targets.	
8.	Provide trained service desk personnel.	
9.	Ensure that the Service Desk is available at all times (i.e. 24 hours a day, 365 days a year).	
10.	Manage all Incidents and/or Service Requests from authorized users relating to Contracted Services.	
11.	Provide weekly reports to the Commonwealth on Service Desk activities, performance, and adherence to established SLAs. Service Desk reporting must include at a minimum: • Key issues relating to Service Desk processes, improvements, script development. • Status as to Service Desk staffing, training, and authorization. • Integration activities and issues with other Service Desks belonging to the Commonwealth. • Trend analysis shall include (13) most recent months. If the Service	

	has been in place less than thirteen months then trend analysis shall include all months of Service. • Calculate metrics and provide monthly reports. • Number of Contacts, to include all interactions (Calls, phone calls, electronic, automated or otherwise). • Number of calls abandoned, average call duration, average time to answer, average time to abandon. • Number and percentage of Contacts resolved. • Number and percentage of Contacts passed to other Service Desks. • Other pertinent information regarding Service Desk operation and performance.	
12.	Enable a KMP accessible by all authorized users. Content for the KMP will be approved by the Commonwealth.	
13.	Offeror must record all incidents, problems, service requests, change requests, and configuration information in the software recording tool. All updates to the record, contacts with clients or vendors, and resolutions will be recorded in a real-time and consistent manner. This recording tool will house the KMP.	
14.	Monitor reporting system to ensure incidents and problems are being addressed to meet agreed SLAs.	
15.	Transition must include the transfer of system and application monitoring alerts with the ability to turn-off the problem	Offeror must describe its approach to ensure alerts are transitioned successfully.

	alert process during maintenance windows and other scheduled outages.	
16.	Interim Support Desk Procedures will be required as the Commonwealth transitions from its current support architecture to the Offeror's Service Desk.	Offeror must describe an interim approach and procedure(s) for providing Service Desk operation throughout the transition to the Offeror's fully managed service.
17.	Incident Management - The Offeror's Incident Management process shall encompass Incident Management processes deployed across all Service Components that are designed to: restore service as quickly as possible, minimize disruption to the Commonwealth, aim for highest levels of availability and service quality, completely transparent and auditable delivery of service, and promote the highest level for user satisfaction.	Offeror must describe its Incident Management Process and how it will be applied to the overall IT Service Management Program for the Commonwealth.
18.	Problem Management - The Offeror's Problem Management Process must minimize the adverse effect on the business of Incidents and Problems caused by errors in the IT infrastructure, Applications, systems and supporting components, and proactively prevent the occurrence of Incidents and Problems by identifying and eliminating causes of failure.	Offeror must describe its Problem Management Process and how it will be applied to the overall IT Service Management Program for the Commonwealth.
Deliverables		
Deliverables are defined in **Schedule K – Key Program Deliverables**		
Offeror Response		

3.2.1.5 Technical Architecture

The Technical Architecture function will oversee the ongoing design of the various computing platforms that will support the Commonwealth's existing computing topologies, as well as plan for the approaching consolidation of the Commonwealth datacenters. The intent is to design an infrastructure which will ultimately utilize multiple datacenters for processing, tiered DR Services, and on-demand Services in a secure environment. At the conclusion of the design, and after approval by the Commonwealth, the Offeror must document the environment via a Service Catalog.

Offeror must design the technical architecture of the computing systems based on current best practices, to support the evolving technologies and business needs of the Commonwealth. The volume of computing and storage will vary during the term of the contract due to applications development, testing, certification, the retirement of existing production environments, as well as cyclical processing demands such as the various tax seasons. The Offeror must be able to expand and contract service offerings based on Commonwealth needs in a timely and cost effective manner.

Reference Documentation

Exhibit A - Commonwealth Network Environment

Exhibit(s) B.1 through B.6 - Data PowerHouse (DPH) Exhibits

Exhibit(s) C.1 through C.13 - Department of Public Welfare (DPW) Exhibits

Exhibit(s) D.1 through D.15 - Enterprise Datacenter (EDC) Exhibits

Exhibit(s) E.1 through E.43 - Department of Labor & Industry (DLI) Exhibits

Exhibit(s) F.1 through F.4 - Department of Health (DOH) Exhibits

Exhibit(s) G.1 through G.16 - PA State Police (PSP) Exhibits

Exhibit(s) H.1 through H.8 - Department of Revenue (DOR) Exhibits

Exhibit(s) I.1 through I.13 - Commonwealth SAP Environment - Integrated Enterprise Services (IES) Exhibits

Exhibit L - Master Application Inventory

Exhibit(s) M.1 through M.7 - Department of Corrections (DOC) and Pennsylvania Board of Probation and Parole (PBPP) Exhibits

Exhibit(s) N.1 through N.2 - PennDOT Exhibits

	Requirements	Describe Compliance
1.	Create a Service Catalog. Define the Services and platforms to be offered.	Offeror must describe the catalog of Services it proposes.

	Provide a detailed list of Services, via a common Service Catalog to be provided to the Commonwealth. Utilize an industry standard software product to ensure the detailed service offering is recorded.	Offeror must provide a sample of a Catalog of Services that includes both Services and platforms that it proposes.
2.	Design and build the IT architecture required to support the Services. Design and build the IT technical architecture to support the Services selected by the Commonwealth. Provide the design to the Commonwealth for review and approval prior to execution. All designs must be approved by the Commonwealth.	Offeror must describe its overall service design process.
3.	Design platform and support lifecycles. Provide a technical support staff structure for the Services and platforms to be offered. Support will consider all skills needed to plan, operate and support each technology platform.	Offeror must describe its proposed technical architecture team. Resumes for proposed key personnel must be provided as described in **Schedule G - Staffing Plan and Key Positions**.
4.	Define Technical Support Services. Provide the skills of and the size of the support staff to plan, manage, and operate the various IT infrastructure platforms.	Offeror must describe its proposed technical architecture team. . Resumes for proposed key personnel must be provided as described in **Schedule G - Staffing Plan and Key Positions**.
5.	Interoperability Strive to design architectures with system components that facilitate system data accessibility.	Offeror must describe its methodology and approach to designing technical architecture
Deliverables		
Deliverables are defined in **Schedule K – Key Program Deliverables**		

Offeror Response

3.2.1.5.1 Technology Refresh

Technology refresh will be an ongoing activity required of the Offeror. The Offeror will prepare technology impact statements that address the key technologies planned for refresh or technologies identified to be of interest to the Commonwealth. These impact statements will provide a wide range of information, including the following matters applicable to the Offeror's environment:

- Technology trends
- IT Infrastructure Offeror releases and offerings
- IT Infrastructure Offeror retirement of older versions of products
- Proposed scheduling of Offeror releases into the datacenter environment
- Potential impact of the new releases on business applications in the datacenter infrastructure
- Potential impact of the new releases on deployment and operational processes
- Risk analyses with recommendations for mitigation of risks

The Commonwealth and the Offeror will review the impact statements. Based on these reviews, the Offeror must recommend a plan and schedule for technology refresh to the Commonwealth. Since the expected usable life of any hardware approved for the datacenter environment is about 36 months, the plan shall project an 18-month window into the future, and include resource estimates for each recommended refresh activity. Software refresh will depend on software releases and the Offeror must ensure operational compatibility with existing Commonwealth applications and/or functionality or must provide upgrade alternatives and options. The Offeror must obtain Commonwealth approvals prior to implementing technology upgrades that will affect Commonwealth operations.

Reference Documentation

N/A

Requirements		Describe Compliance
1.	Update Technical Architecture approach and project plan including; Service Catalog, IT Architecture, and Technical support	Offeror must document its Technical Architecture approach and project plan including; Service Catalog, IT Architecture, and Technical support
2.	Technology refresh approach - describe methodology for reviewing and refreshing technology on a scheduled basis.	Offeror must describe its methodology for reviewing and refreshing technology on a scheduled basis.
3.	Technical Architecture Staffing	Offeror must identify its technical

		architecture organization and staff.
Deliverables		
Deliverables are defined in **Schedule K – Key Program Deliverables**		
Offeror Response		

3.2.1.5.2 IT Service Continuity Architecture

The Offeror's IT Service Continuity Architecture will provide tiered DR capabilities and Services for applications that have been identified by the Commonwealth. The Offeror must provide a Service Continuity solution that includes DR computing, storage, networking systems and recovery processes and will be included in the overall Commonwealth architecture design. Only critical applications and associated equipment identified by the Commonwealth will be addressed with DR systems. Additional information regarding Tiered Service Delivery and Tiered DR can be found in referenced supporting exhibits.

The Commonwealth will lead the Business Continuity effort with assistance from the Offeror.

Reference Documentation

Schedule J.1 - Datacenter Service Level Management

Requirements		Describe Compliance
1.	DR Architecture and Plan will be documented by the Offeror and approved by the Commonwealth.	Offeror must describe its infrastructure and service offering for a DR and Business Continuity Plan.
2.	IT Service Continuity Architecture and Plan - Backup hardware and software will be obtained, configured and available per an agreed to Service Level to process the identified critical applications. Where applicable, data will be electronically replicated (including disk-2-disk) to the backup systems (off site) to insure a successful recovery. Wherever data	Offeror must describe the design of its Tiered DR plan in the design of the Commonwealth technical architecture. Offeror must provide at least one relevant example from a prior engagement, in which it was engaged, that is similar to the needs of the Commonwealth. Offeror must describe its process for modifying the scope/service level for DR

	replication is not viable, backup tape data will be utilized.	coverage.
3.	Recovery systems must be available via network access. Routing must be configured and tested during initial system architecture design. Include the network requirements of the DR plan in the design of the network architecture.	Offeror must describe the network requirements of its DR plan in its proposed design of the network architecture.
4.	Recovery documentation for each identified system/ application will be required. Information will include the targeted backup hardware, software, networking changes, data location, restoration and access process, execution authorization, and notification to service owner when an application has been restored to service. Offeror must create recovery documentation for each system / application identified as a critical system where DR is required.	Offeror must provide at least one relevant example from a prior engagement, in which it was engaged, that is similar to the tiered DR needs of the Commonwealth.
5.	A DR support plan must be created. The DR team must notify the Commonwealth when a recovery plan will be put into action, and must manage questions and issues that may arise after implementation. Create a DR team that will manage the execution of the DR plan from declaration to recovery when required.	Offeror must provide at least one relevant example from a prior engagement, in which it was engaged, that is similar to the DR needs of the Commonwealth.
6.	For critical systems identified as having a current tested DR Plan within the DPH, the Offeror will update the associated DR test plans for the new	Offeror must provide its approach to creating and testing DR Plans.

	target environment. Successful testing of each revised DR Plan is required prior to Commonwealth acceptance.	

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

3.2.1.6 Account Management

The Account Management function is responsible to provide each Commonwealth agency with oversight of the contracted Services and support required to satisfy the Commonwealth's computing needs. The Account Manager will provide direct interface with the Commonwealth agencies ensuring daily operations and needs are provided, and create monthly operational summaries reporting to both the agencies and the Commonwealth. This report will address all operational events and issues that occurred during the month that would have effected service level attainments, problems and incidents, and recommendations for changes needed to provide continuous, secure computing Services. Each Commonwealth agency will interact with its assigned Account Manager to discuss needs, issues, problems or costs.

Reference Documentation

Schedule G - Staffing Plan and Key Positions

Requirements		Describe Compliance
1.	Assign an Account Manager to each identified agency. The Account Manager will be responsible for all Services provided, represent the Commonwealth agency's needs, and be the advocate for the agency throughout the Offeror's organization. Based on the size and application complexity of the Commonwealth	Offeror must identify its account management structure, roles, and responsibilities. The Offeror must provide resumes and qualifications for each of its proposed Account Managers and other key positions.

	agency, the Offeror must assign additional account management resources. Account Managers shall understand agencies line of business and business trend analysis. Offeror must assign a minimum of 6 dedicated account managers.	
2.	Account Managers will meet with assigned agency contacts on a regular basis. It is anticipated that this will be at minimum weekly during the initial program start and through transition.	Offeror must describe its approach to meet this requirement.
3.	Meet with Commonwealth teams on a monthly basis. It is anticipated that this will be at minimum weekly during the initial program start and transition to monthly meetings with the Commonwealth teams to address problems and assure continuous service improvements.	Offeror must describe its approach to meet this requirement.
4.	Participate in agency-sponsored IT planning sessions on a quarterly basis. Offeror must schedule quarterly computing capacity reviews to ensure sufficient processing capacity, needs, and issues are being addressed. Suggest changes when necessary.	Offeror must describe its approach to meet this requirement.
5.	Advocate for agency interests. Offeror's Account Management team will advocate for the Commonwealth's interests. For example, intervene with Service Desk personnel to resolve a major problem; problem escalation process, support root cause analyses process. Another example, coordinate with agency and service providers to ensure timing of	Offeror must describe its approach to meet this requirement.

	technology refreshes have the least impact on the agency.	
6.	Monthly status reports - Ensure The Commonwealth is aware of operational status and project update information on a monthly basis. Create and deliver a monthly status report, summarizing operational metrics as defined in the CCPM, by service platform, including highlights and exceptions, and project status.	Offeror must describe approach and provide a representative sample report.
Deliverables		
Deliverables are defined in **Schedule K – Key Program Deliverables**		
Offeror Response		

3.2.1.7 Configuration Management

The Offeror's Configuration Management system must ensure complete and accurate recordkeeping relative to datacenter assets; hardware, operating system software, firmware, and network. The Offeror's Configuration Management Database (CMDB) system must be synchronized with the proposed datacenter Change and Release Management processes. Also included will be associations of infrastructure configuration items (CIs) and Agency application infrastructure to support application infrastructure related SLAs.

At the end of the contract the Offeror will be responsible to provide the Commonwealth with a final electronic copy of the CMDB.

The following list identifies but does not limit the roles and responsibilities that the Offeror must perform:

- Define and document Configuration Management standards and procedures per ITIL v3 standards.
- Establish an electronic interface to the Commonwealth's CMDB(s) to keep current both the Commonwealth's CMDB and the Offeror's CMDB.
- Establish process for tracking configuration changes
- Establish process interfaces to Incident and Problem Management, Change Management,

technical support, maintenance and asset management processes

- Establish appropriate authorization controls for modifying configuration items
- Establish configuration baselines as reference points for rebuilds, and providing ability to revert to stable configuration states
- Establish process for verifying the accuracy of configuration items, adherence to Configuration Management process, identify process deficiencies and recommend corrective actions

The Commonwealth will require online access to configuration related information and reports to satisfy application updates and audit requirements.

Reference Documentation

Schedule H - Commonwealth Computing Procedures Manual (CCPM)

Requirements		Describe Compliance
1.	Provide a documented process to track configuration changes accordingly to ITIL V3 framework	Offeror must describe how its Configuration Management System addresses the list of requirements described above. Offeror must provide a toolset description and an example of a configuration management system from a prior or current engagement of the Offeror.
2.	Per agency request, provide specific application related infrastructure component configuration information.	Offeror must describe how its configuration management systems can support this requirement.
3.	Provide current configuration reports at an agency level by datacenter component.	Offeror must describe its process to request configuration management reports. Offeror must provide a sample of a Configuration Management report used by Offeror on a current or previous engagement.
4.	Continuous review and updates to the Offeror's and Commonwealth's CMDB	Offeror must describe its approach to maintaining the accuracy of the CMDBs (Offeror & Commonwealth).
5.	CMDB that constitutes the common repository created by the Offeror to include, but not be limited to, location	Offeror must describe its approach to meet this requirement.

	information, service information, configuration information, application information, billing data, inventory data, and performance data. This data will be provided to the Commonwealth via electronic interface in a format approved by the Commonwealth.	
Deliverables		
Deliverables are defined in **Schedule K – Key Program Deliverables**		
Offeror Response		

3.2.1.8 3rd Party License Management

Currently the Commonwealth manages over 2,000 business applications that require numerous software platforms and products. The Offeror's 3rd Party License Management service must ensure accurate inventory and licensing compliance for all Offeror provided infrastructure software products. The Offeror will be solely responsible for the management of all infrastructure software products provided through this contract.

The Offeror must coordinate with the Commonwealth to ensure compatibility between Commonwealth provided applications related software, and the Offeror provided infrastructure software. The Offeror must provide a method for tracking and reporting on both Offeror provided and Commonwealth provided software that will reside on the managed infrastructure.

The Offeror must provide the ability to purchase the Third Party Software listed in Exhibit B.4 - DPH - Third Party Softwareand additional third party software if required to provide the contracted services. The Offeror shall be responsible for the licensing and maintenance and support for the Third Party Software. The Commonwealth at its sole discretion may procure third party software from appropriate contracts.

The Offeror must provide the ability to purchase maintenance and support for the Third Party Software listed in Exhibit B.10 - DPH – Hybrid Third Party Software. The Offeror shall be responsible for the maintenance and support for the Third Party Software. The Commonwealth at its sole discretion may procure third party software maintenance and support from appropriate contracts.

Reference Documentation

Exhibit B.3 - DPH - Commonwealth Software Asset Listing

Exhibit B.4 - DPH - Third Party Software

Exhibit B.10 - DPH – Hybrid Third Party Software

See each target datacenter exhibits for current applications supported.

Requirements		Describe Compliance
1.	Provide, as requested, current software license reports for in scope infrastructure. For example specific OS version and patch levels per service instance.	Offeror must describe its approach to providing 3rd party software inventory and tracking per agency related infrastructure.
2.	Improve service quality, efficiency, and effectiveness.	Offeror must describe its methods to address continuous service improvement process

		related to 3rd party software management.
3.	Improve/reduce cost of service.	Offeror must provide examples of 3rd Party Software Management initiatives it has implemented and which may be utilized to achieve reduced costs of Services and to meet or exceeded ROI (Return on Investment) analysis projections.
Deliverables		
Deliverables are defined in **Schedule K – Key Program Deliverables**		
Offeror Response		

3.2.2 Technical Services

3.2.2.1 Transition Management (New Customer and/or Services)

The Transition Management service ensures the systematic planning, management, execution, and monitoring of major changes to the datacenter environment(s). This Services offering is to support new customers and/or new Services (i.e. remote file servers, remote databases, etc.). This service offering includes the phased migration of Commonwealth applications to the Offeror's managed service excluding initial transition.

Information and tasks pertaining to the transition of the initial Targeted Datacenters and Agencies can be found in Section 3.3 – Transition Services.

Reference Documentation

N/A

Requirements		Describe Compliance
1.	Transition Management Office - Create a Transition Management Office and team that will be responsible for the migration projects of hardware and applications from the Commonwealth's locations to the new target datacenter environments.	Offeror must describe its transition management approach and its proposed transition team. Provide resumes for key members of the proposed transition team.
2.	Create a computing environment;	Offeror must discuss its approach to

	hardware, software, network systems, peripherals, and devices as required to migrate the Services from the Commonwealth.	migrating the Commonwealth's computing platforms (mainframe, mid-range and x86) and associated infrastructure to the Offeror's proposed solution.
3.	Provide recommendations for the repurpose, replacement, or retirement of existing Commonwealth hardware, software, network systems, and peripheral devices as required after system migrations have been completed.	Offeror must discuss its approach.
4.	Optimize Current Process and Procedures – Coordinate with Commonwealth customer to review and plan for a transition of processes and procedures.	Offeror must describe its overall plan for optimization of the existing processes, procedures, tools, etc. to provide more efficient and effective Services. The description must include approach, plan, and methodologies.
5.	Develop detailed plans to migrate Commonwealth applications, and associated infrastructure from Commonwealth datacenters to the Offeror's datacenters. On a monthly basis, Offeror must create a report to detail the transition projects on the plan, status, risks, and the forecasted transition date.	Offeror must discuss its approach to support the migration of Commonwealth applications to the proposed solution including communicating and reporting on the migration plan, risks and schedule.
6.	Coordinate with Commonwealth applications project teams to plan and execute the application and infrastructure migration plans.	Offeror must discuss its approach.
7.	Revise datacenter disaster recovery plans on the occasion of major changes to the datacenter hardware, software, or network portfolio.	Offeror must discuss its approach.
Continual Process Improvement		
8.	Reduce service risks.	Offeror must provide examples of previous

		Offeror initiatives aimed at eliminating or mitigating service risks.
9.□	Improve service quality.	Offeror must provide examples of previous Offeror initiatives aimed at improving service quality.
10.□	Improve client satisfaction.	Offeror must provide examples of previous Offeror initiatives aimed at continually improving client satisfaction.
11.□	Provide service transparency.	Offeror must provide examples of previous Offeror initiatives aimed at providing service transparency; in particular, visibility into the service execution process.
12.□	Ensure service sustainability.	Offeror must provide examples of previous Offeror initiatives aimed at ensuring service sustainability; in particular, efforts targeted at cost containment and cost reductions.
13.□	Improve/reduce cost of service	Offeror must provide examples of previous technology initiatives implemented by Offeror that achieved reduced costs of Services and that met or exceeded ROI (Return on Investment) analysis projections.
Deliverables		
Deliverables are defined in **Schedule K – Key Program Deliverables**		
Offeror Response		

3.2.2.2 Infrastructure Architecture

The Infrastructure Architecture service will define and manage the scope and design of the infrastructure architecture for the computing systems to support the evolving needs of the Commonwealth. This range of Services includes design of the mainframe, mid-range, x86 servers, (both physical and virtual), Local Area Network (LAN), storage, backup systems, and the DR systems. The design will also need to detail how the most current data will be restored to the targeted DR system.

Efforts are underway to re-write many of the Commonwealth business applications. For example, some of the mainframe applications are being migrated to newer server based systems. The Offeror must consider the planned retirement of some of the mainframe workload, and at the same time consider the offsetting growth in other server platform environments.

At the direction of the Commonwealth, the Offeror must transition Commonwealth based computing infrastructure to one of the datacenters. The Offeror must work with the Commonwealth agencies to understand the systems involved, and the timeframe of these migrations. Working with the Commonwealth agencies, the Offeror must provide the design, project management, hardware and technical support required to test and migrate these systems to the new production environment. At its discretion, each agency will provide the applications staff to support the migrations.

The Infrastructure Architecture service will review and recommend hardware, software, and the technical configurations required to build the requested infrastructure environments. Prior to migrating each of the current application workloads to the new target infrastructure, the Offeror must work with each Commonwealth agency to develop a mutually agreed to Acceptance Test Plan that includes the testing of application infrastructure performance characteristics.

Reference Documentation

Exhibit A - Commonwealth Network Environment

Exhibit(s) B.1 through B.6 - Data PowerHouse (DPH) Exhibits

Exhibit(s) C.1 through C.13 - Department of Public Welfare (DPW) Exhibits

Exhibit(s) D.1 through D.15 - Enterprise Datacenter (EDC) Exhibits

Exhibit(s) E.1 through E.43 - Department of Labor & Industry (DLI) Exhibits

Exhibit(s) F.1 through F.4 - Department of Health (DOH) Exhibits

Exhibit(s) G.1 through G.16 - PA State Police (PSP) Exhibits

Exhibit(s) H.1 through H.8 - Department of Revenue (DOR) Exhibits

Exhibit(s) I.1 through I.13 - Commonwealth SAP Environment - Integrated Enterprise Services (IES) Exhibits

Exhibit L - Master Application Inventory

Schedule J.1 - Datacenter Service Level Management

Exhibit(s) M.1 through M.7 - Department of Corrections (DOC) and Pennsylvania Board of Probation and Parole (PBPP) Exhibits

Exhibit(s) N.1 through N.2 - PennDOT Exhibits

Requirements		Describe Compliance
1.	Define the infrastructure technology Services to be offered. Provide a detailed list of Services and computer platforms to be provided to the Commonwealth.	Offeror must describe its ability to provide infrastructure technical Services across multiple computing platforms (mainframe, mid-range and x86). Include explanation of different service tiers (e.g. gold, silver and bronze).
2.	Design and build the IT infrastructure architecture to support the Services required by the Commonwealth. Design will provide as much interoperability and open standards as possible. All designs must be approved by the Commonwealth. Provide the design in a Visio format to the Commonwealth for review and approval prior to execution. This	Offeror must describe its methodology and approach to infrastructure architecture design Services. Offeror must describe the documentation requirements, timelines for both normal requests and emergency situations. Offeror must provide representative sample of infrastructure design documentation.

	diagram will be dated and maintained as Services are altered for the duration of the engagement.	
3.	Address CJIS and Criminal History Record Information Act (CHRIA) requirements for agency application infrastructure designs where required. Some agency application infrastructure designs (e.g. PSP) require additional security and encryption level requirements imposed by CJIS.	Offeror must provide examples of its experience in designing infrastructures that adhere to CJIS and CHRIA requirements.
4.	SAP Infrastructure Design The Offeror's proposed target infrastructure design for the Commonwealth's SAP environments must include a certified SAP sizing report prior to migration of the systems.	Offeror must provide examples of its experience in sizing and design of SAP infrastructures. All designs must be approved by the Commonwealth.
5.	Commonwealth Wide Area Net connectivity. Provide connectivity from the datacenter to the Commonwealth Network. Redundant network links are required.	Offeror must describe its capabilities to connect to and manage the requisite connections. Explain ongoing network support Services to manage these links including the ability to increase capacity as needed to support changes in the application infrastructure requirements.
6.	Develop Acceptance Test Plan. Prior to migrating each of the current application workloads to the new target infrastructure, the Offeror will work with each Commonwealth Agency to develop a mutually agreed to Acceptance Test Plan that includes the testing of application infrastructure performance characteristics.	Offeror must discuss its proposed approach to systems acceptance testing and include the approach to performance testing.

7.	Provide System Acceptance testing. The Offeror must conduct system acceptance testing, and provide the Commonwealth with written verification prior to declaring the system is fit for use. This acceptance test must include validation of infrastructure performance against system performance characteristics agreed to by both parties.	Offeror must discuss its proposed approach to systems acceptance testing.
8.	Ready for use certification	Offeror must provide the Commonwealth with written verification prior to declaring the Service is ready for use. The Service will not be considered ready for use until written acceptance is obtained from the Commonwealth.
9.	Support User Acceptance Testing.	Offeror must support the Commonwealth's user acceptance testing. The Commonwealth shall not be charged for Services until written acceptance is obtained from the Commonwealth.
10.	Provide Application Infrastructure environments. Provide non-production and production environments for each of the application computing platforms. The non-production environments will be used for testing new technologies and applications, updates and upgrades, prior to production implementations.	Offeror must describe its approach to the design and management of multiple application infrastructures. Identify proposed solution to individual or consolidated non-production environments for agencies.
11.	Design service lifecycle. Provide the infrastructure design for the Services and platforms to be offered. Provide ongoing evaluation and recommend new technologies to	Offeror must describe its approach to provide service lifecycle design for all Commonwealth computing platforms and associated infrastructures. Offeror must provide the Commonwealth and

	enhance, improve, and reduce the cost of Services.	its agencies the ability to request new technologies to be available.
12.	Define Technical Support functions.	Offeror must list Offeror's support staff levels required to plan, manage, and operate the IT infrastructure, based on the various service levels offered.
Continual Service Improvement		
13.	Reduce service risks.	Relative to the service in question, Offeror must provide examples of previous Offeror initiatives aimed at eliminating or mitigating service risks.
14.	Improve service quality.	Offeror must provide examples of previous Offeror initiatives aimed at improving service quality.
15.	Improve client satisfaction.	Offeror must provide examples of previous Offeror initiatives aimed at continually improving client satisfaction.
16.	Provide service transparency.	Offeror must provide examples of previous Offeror initiatives aimed at providing service transparency; in particular, visibility into the service execution process.
17.	Ensure service sustainability.	Offeror must provide examples of previous Offeror initiatives aimed at ensuring service sustainability; in particular, efforts targeted at cost containment and cost reductions.
18.	Improve/reduce cost of service	Offeror must provide examples of previous technology initiatives implemented by Offeror that achieved reduced costs of Services and that met or exceeded ROI (Return on Investment) analysis projections.
Deliverables		
Deliverables are defined in **Schedule K - Key Program Deliverables**		

Offeror Response

3.2.2.3 Capacity Management

The Capacity Management activity focuses on the planning and scheduling of the Commonwealth's infrastructure capacity and growth. Capacity planning includes consideration of data communications, networking, processing, storage, and other environmental variables. The Offeror must issue periodic reports showing usage, trends, capacity forecasts, and recommendations for upgrades.

Processor capacity planning focuses on estimating, measuring, and reporting on the central processing unit (CPU) and memory usage, including peak usage and average usage over time.

Forecasting of each agency's application-based processor and memory usage will be determined using projected transaction and user volumes supplied by the Commonwealth. The Offeror must track application-based processor and memory usage and report the usage and trends to the Commonwealth. The Offeror must make periodic recommendations for upgrading existing server capacity.

Data storage capacity planning focuses on estimating, measuring, and reporting on data storage used per application over time.

Forecasting of application-based data storage usage will be provided by the Commonwealth. The Offeror must track current data storage usages and report the usage and trends to the Commonwealth. The Offeror must make periodic recommendations for upgrading existing data storage capacity.

New application infrastructure capacity planning focuses on estimating, measuring, and reporting on network, server, and data storage usage over time per application. New processing requirements will be established during testing in test environments. The Offeror must track application-based infrastructure usage. The Offeror must make monthly recommendations for upgrading existing infrastructure capacity.

The following list identifies but does not limit the roles and responsibilities that the Offeror must perform:

- Establish comprehensive Capacity Management planning process
- Identify future business Commonwealth requirements that will alter capacity requirements
- Assess capacity impacts when adding, removing or modifying applications
- Capture trending information and forecast future agency infrastructure capacity requirements based on agency defined thresholds

- Recommend changes to capacity to improve service performance
- Assess impact/risk and any cost of capacity changes with agencies
- Maintain capacity levels to optimize use of existing IT resources and minimize agency costs
- Ensure adequate capacity exists within the IT environments

Reference Documentation

Schedule H - Commonwealth Computing Procedures Manual (CCPM)

	Requirements	Describe Compliance
1.	Working with each agency, develop the initial Capacity Management Plan based on an inventory and review of each of the agency applications and associated managed infrastructure. Develop the initial Capacity Management Plan and provide quarterly updates to the plan.	Offeror must discuss its approach to Capacity Management and provide a sample of a Capacity Management Plan.
2.	Meet with the Commonwealth and agency representatives on a monthly basis to assess the future datacenter resource requirements; processors, storage space, network (LAN & WAN), selected application transactions, and number of users, etc.	Offeror must discuss its approach to support the current and future needs of Commonwealth agencies. Offeror must provide a sample of a Capacity Management report that includes processor, storage, network and application metrics.
3.	Produce an annual datacenter Capacity Plan and Trend Analysis.	Offeror must discuss its approach to meet this requirement. Provide a sample Capacity Management Plan and Trend Analysis.
4.	Produce a monthly planned vs. actual resource usage report.	Offeror must discuss its approach. Provide a sample resource usage report.
5.	Recommend methods for reducing hardware “footprints”, e.g., replacing server storage with network attached storage and aggressive server virtualization.	Offeror must discuss its approach.

6.	Allow emergency or temporary orders for additional Services or capacity without a minimum service commitment.	Offeror must discuss its approach.
Continual Service Improvement		
7.	Reduce service risks.	Offeror must provide examples of previous Offeror initiatives aimed at eliminating or mitigating service risks.
8.	Improve service quality.	Offeror must provide examples of previous Offeror initiatives aimed at improving service quality.
9.	Improve client satisfaction.	Offeror must describe methods to continually improve client satisfaction.
10.	Provide service transparency.	Offeror must provide examples of previous Offeror initiatives aimed at providing service transparency; in particular, visibility into the service execution process.
11.	Ensure service sustainability.	Offeror must provide examples of previous Offeror initiatives aimed at ensuring service sustainability; in particular, efforts targeted at cost containment and cost reductions.
12.	Improve/reduce cost of service.	Offeror must provide examples of previous capacity initiatives implemented that achieved reduced costs of Services and that met or exceeded ROI (Return on Investment) analysis projections. If costs of Services increased due to increased required capabilities, so identify.
Deliverables		
Deliverables are defined in **Schedule K – Key Program Deliverables**		

Offeror Response

3.2.2.4 DR Planning & Testing

The DR Planning & Testing service ensures that the Offeror provides expert assistance in developing, documenting, deploying, and testing tiered datacenter recovery strategies that includes access for Commonwealth end users. This service will protect the identified applications processing at the datacenters, Commonwealth employees and constituents who utilize the application.

The Commonwealth will provide the Offeror with a list of agency applications that require a DR solution and related DR plan after contract is awarded. The Offeror is expected to provide DR Planning and Testing Services for agency applications that require DR Services. For Commonwealth agency applications that do not currently have DR plans, these Services will be provided in the event the Commonwealth elects to order DR services for these applications.

Reference Documentation

Exhibit B.5 - DPH - Agency Disaster Recovery Matrix

Schedule J.1 - Datacenter Service Level Management

Requirements		Describe Compliance
1.	Meet with the Commonwealth and agency representatives on an annual basis and upon request to assess its DR requirements. Post contract award, Offeror must document the Tiered DR plans in an online software program that will be available to Commonwealth and Offeror staff. The documented plans must be made available at the time each individual critical application is transitioned to the Offeror's managed Services.	Offeror must discuss its approach to providing a Tiered DR service offering to meet the needs of the agencies. Offeror must provide at least one relevant example from a prior engagement, in which it was engaged, that is similar to the DR needs of the Commonwealth. Offeror must discuss the DR capabilities that are included in its proposed Architecture.
2.	Review and update Disaster Recovery	Offeror must describe an approach to

	Plans (DRPs) - Offeror must review existing Disaster Recovery Plans (DRPs) to determine gaps in existing or future DR Services, within the first 120 days after the Effective Date. The Offeror must at least annually review and update the disaster recovery plans. Assist the Commonwealth in identifying dependencies/limitations to DR testing due to non-Offeror infrastructure.	perform a gap analysis of the existing Disaster Recovery Plans (DRPs). Offeror must include a description of the process it will use to track and resolve all identified gaps.
3.	Provide the Commonwealth and agency representatives with access to an online DR planning tool.	Offeror must discuss its approach to meet this requirement. Identify and describe the proposed online DR planning tool.
4.	Provide the Commonwealth and agency representatives with access to an automated emergency notification system. This would be invoked on the occasion of a disaster or other emergency.	Offeror must discuss its approach to meet this requirement. Identify and describe the proposed emergency notification system that could be used to invoke a DR event.
5.	Assist the Commonwealth and agency representatives as requested to review agency identified critical business applications and related IT applications and infrastructure.	Offeror must discuss its approach to meet this requirement.
6.	Assist the Commonwealth and agency representatives as requested in developing, documenting, deploying, and exercising its tiered disaster recovery plans.	Offeror must discuss its approach and optional service offering. Offeror must describe its approach to perform a successful recovery test within 6 months of transition to the Offeror's Managed Service.
7.	Assist the Commonwealth and agency representatives as requested in coordinating disaster recovery exercises.	Offeror must discuss its approach and optional service offering.

	Frequency of DR exercises will be at the discretion of the Commonwealth. The Offeror must every six (6) months test the operability of the disaster recovery plan then in effect.	
8.	Assist the Commonwealth and agency representatives as requested in developing, documenting, deploying, and exercising its continuity of operations (COOP) and continuity of government (COG) plans.	Offeror must discuss its approach.
9.	Assist the Commonwealth and agency representatives as requested in integrating its disaster recovery plans into its COOP and COG plans.	Offeror must discuss its approach.
10.	As requested by the Commonwealth, evaluate the efficiency of business partner disaster recovery and/or business continuity plans.	Offeror must discuss its approach.
11.	In concert with the Commonwealth and agency representatives, lead the recovery operations as requested in the event of a disaster or other major disruption.	Offeror must discuss its approach and optional service offerings.
12.	Conduct disaster recovery planning and activities in accordance with the Business Continuity Institute Good Practice Guideline or similar standard.	Offeror must identify the standard and describe its approach to meet this requirement.
13.	Ensure DR Planning & Testing Services are documented in the Service Catalog.	Offeror must provide a prototype of this section of the Service Catalog.
Continual Service Improvement		
14.	Reduce service risks.	Relative to the service in question, Offeror

		must provide examples of previous Offeror initiatives aimed at eliminating or mitigating service risks.
15.	Improve service quality.	Offeror must provide examples of previous Offeror initiatives aimed at improving service quality.
16.	Improve client satisfaction.	Offeror must describe methods to continually improve client satisfaction.
17.	Provide service transparency.	Offeror must provide examples of previous Offeror initiatives aimed at providing service transparency; in particular, visibility into the service execution process.
18.	Ensure service sustainability.	Offeror must provide examples of previous Offeror initiatives aimed at ensuring service sustainability; in particular, efforts targeted at cost containment and cost reductions.
19.	Validate business case for cost of the service.	Offeror will provide examples to validate the projected cost savings or cost avoidance projected versus the cost of using this service.
20.	Improve/reduce cost of service.	Offeror must provide examples of previous disaster recovery initiatives implemented that achieved reduced costs of Services and that met or exceeded ROI (Return on Investment) analysis projections. If costs of Services increased due to increased required capabilities, so identify.
Deliverables		
Deliverables are defined in **Schedule K – Key Program Deliverable**		
Offeror Response		

3.2.2.5 Security Management

The Security Management service must ensure the confidentiality, integrity and availability of Commonwealth information and infrastructure systems. All support and implementation activities must be conducted in accordance with, but not limited to, leading industry and Commonwealth standards, which include, but are not limited to, ISO 27001:2005 and ISO 27002:2005. The Offeror must support all related system audits at the Offeror's expense. The Offeror must maintain current security ISO 27001, ISO 9001 and ISO/IEC 20000 certifications.

The Offeror must comply with Commonwealth IT policies and directives as well as federal and Commonwealth laws, regulations and policies, including but not limited to the Criminal History Record Information Act (CHRIA), Health Insurance Portability and Accountability Act (HIPAA), Criminal Justice Information Services (CJIS) regulations, The United States Social Security Administration (SSA)regulations, IRS (Internal Revenue Service) Publications, Commonwealth Information Technology Bulletins (ITBs) and the Payment Card Industry (PCI) standards. The Offeror must work with each agency to understand and ensure compliance with all laws, regulations, and policies as they pertain to each individual agency.

Reference Documentation

Exhibit J.1 through J.3 - Commonwealth Security and Compliance Requirements

Exhibit G.6 - PSP - CJIS Security Policy

Exhibit G.9 - PSP – CCHRI

Exhibit G.7 - PSP - Summary of CJIS Requirements

Exhibit G.12 - PSP - CHRIA Handbook

Requirements		Describe Compliance
1.	Develop an annual Security Management Plan.	Offeror must describe its approach to Security Management and provide a sample of a Security Management Plan. Highlight how stated security objectives align with Commonwealth business goals, IT policies, and regulatory requirements.
2.	Deploy complement of network security systems. Implement at minimum: spam filtering, anti-virus, malware protection, firewall (web, application), intrusion prevention and detection,	Offeror must describe its proposed solution including the following: • Processes and Procedures • Tools / Applications • End User Reports o Standard

	web content filtering, virtual private network, and data loss prevention systems.	o Custom • Escalation Procedures Offeror must describe its prior experience relative to providing datacenter management and support of CJIS, CCHRI, HIPAA and PCI systems.
3.	Perform quarterly (at the Offeror's expense) Vulnerability Analyses (VA) and penetration testing to identify new or emerging information security threats. Perform penetration testing (at the Offeror's expense) and present the results of each VA on a quarterly basis. Should exposures be identified, plan and remediate the exposure in accordance with Commonwealth IT policy guidelines. Report results to the Commonwealth within the time set out in an applicable SLA. The above requirement will be for all systems/subsystems that the Offeror is responsible for including managed servers/virtual servers, network devices, security devices including , but not limited to, the following: • Performing web application firewall administration and securing web applications behind it. • Ensuring and maintaining PCI level 1 compliance. • Implementing DLP for the data center server assets to avoid a breach. • Implementing Database Firewall to secure database assets from breach.	Offeror must describe its capabilities and approach to performing vulnerability analysis and penetrating testing on a quarterly basis. Provide sample reports for each.

4.	Review network and other security logs for evidence of attacks. Utilize enterprise grade intrusion detection tool(s) to systematically identify, stop, and report security threats. Produce a monthly Security Log Analysis as part of the monlthy status reports as described in RFP section IV-5 Reports and Project Control.	Offeror must describe its solution and approach.
5.	Apply operating system and other security patches. Implement a Patch Management Program to ensure the timely application of security updates on all infrastructure platforms in accordance with Commonwealth IT policy guidelines. The Patch Management Program must adhere to the Change Management process that includes Commonwealth approvals.	Offeror must describe its proposed Patch Management program.
6.	Restrict physical access to all network systems and equipment with biometric or other second factor access control systems.	Offeror must describe solution and approach to meet this requirement.
7.	Restrict access to all data in the Commonwealth network infrastructure. Restrict and control all data access right, groups and special permissions based on the data security program designed by the Commonwealth security team and/or specified by the agencies. Access level changes and exceptions will be executed only when	Offeror must describe solution and approach to meet this requirement.

	approved paperwork is complete and approved. A file of all access changes will be maintained by the Offeror for audit purposes. Offeror must support Commonwealth initiated security audits.	
8.	Evaluate the security standing of network-connected subcontractors. Conduct information security audits of prominent subcontractors on an annual basis.	Offeror must describe solution and approach to meet this requirement.
Continual Service Improvement		
9.	Reduce service risks.	Relative to the service in question, Offeror must provide examples of previous Offeror initiatives aimed at eliminating or mitigating service risks.
10.	Improve service quality.	Offeror must provide examples of previous Offeror initiatives aimed at improving service quality.
11.	Improve client satisfaction.	Offeror must provide examples of previous Offeror initiatives aimed at continually improving client satisfaction.
12.	Provide service transparency.	Offeror must provide examples of previous Offeror initiatives aimed at providing service transparency; in particular, visibility into the service execution process.
13.	Ensure service sustainability.	Offeror must provide examples of previous Offeror initiatives aimed at ensuring service sustainability; in particular, efforts targeted at cost containment and cost reductions.
14.	Improve/reduce cost of service.	Offeror will provide examples of Security Management initiatives that have been implemented or can be utilized to achieve reduced costs of Services and to meet or

		exceeded ROI (Return on Investment) analysis projections.
Deliverables		
Deliverables are defined in **Schedule K – Key Program Deliverables**		
Offeror Response		

3.2.2.6 Performance Monitoring & Management

The Performance Monitoring & Management Service of the infrastructure components, databases, and applications provide the critical input for meeting service level commitments. Performance monitoring is a proactive method to identify and respond to system database, processor utilization, or environmental problems that may affect the Services, or might negatively affect Services in the near future. The selected performance monitoring tools will also provide one of the key inputs for calculating SLAs, and the associated monthly evaluation and reporting needs.

The Offeror must collect performance information and report on infrastructure and application performance status on a daily basis using performance management and monitoring tools.

All tracked performance information must be reported daily, including processing performance, network (LAN / WAN) performance, and storage performance data. The Offeror must determine trends in conjunction with the Commonwealth, and all trends will be reported to address, if necessary, any changes from an established baseline. Forecasts of future usage will be determined based on expected growth in application transaction volume and expected deployment of future applications.

The Offeror must provide a base level of performance monitoring for key infrastructure components such as server, storage, network, and security. Additional Performance Monitoring Services such as database and application monitoring will be offered to the Commonwealth as an additional level of service.

Agency applications may require additional application level monitoring provided and managed by the Commonwealth Agencies. The Offeror must allow additional Commonwealth based monitors to be installed and managed by individual Commonwealth Agencies.

Reference Documentation

Schedule J.3 - Datacenter SLA Definitions

Requirements		Describe Compliance
1.	Identify the performance monitor software tool(s) that will be used to monitor selected infrastructure Services. The selected infrastructure service will be presented to the Commonwealth for approval.	Offeror must describe its proposed performance management toolset.
2.	Create and maintain performance monitoring procedures for each	Offeror must describe its approach to monitoring performance across multiple

	platform to ensure each system is monitored in a consistent manner. All identified systems will be monitored under the parameters established in the CCPM.	platforms and environments including the following: • Process and Procedures • Tools / Applications • End User Reports o Standard o Custom • Escalation Procedures
3.	Performance information reporting - Collect and report on the performance data on a monthly basis. Offeror must utilize these reports to ensure SLA's are being achieved. A monthly report will be created to provide a review of how well the systems are performing. Also, provide daily reporting. Recommend system changes to correct over and under system utilization, as well as system upgrades as appropriate. These reports and recommendations will be shared with the Commonwealth. Daily performance reports summarizing incidents for the past 24-hours and immediate reports of incidents and routine status reports of incidents in progress for resolution such as a network or server outage that impacts Commonwealth Services. Examples of automated notifications include, but are not limited to, drive full (Warning, critical), unscheduled reboots, server instability, etc. and to be defined in the CCPM. Offeror must have to ability to provide performance information on a daily, weekly, and monthly basis.	Offeror must provide sample performance monitoring reports and approach to supporting daily, weekly and monthly reporting. Offeror must describe its approach to provide Commonwealth the ability to utilize Offeror's monitors (tools) as well as adding its own.

4.	Support the load testing of applications by providing additional targeted performance monitoring Services during the testing period. This service will be made available as an additional service. Provide load-testing performance monitoring as an add-on service.	Offeror must describe its monitoring capabilities and tools to support load-testing performance.
5.	Performance Monitoring training - Provide the Commonwealth with training on the use of performance management tools and reporting.	Offeror must describe its training approach to provide this training to Commonwealth users.
6.	Support for agency level monitors - agency applications may require additional application level monitoring to be provided and managed by the Commonwealth agencies. Support synthetic transactions in applications to create a “dashboard” view that applications are working properly. The Offeror must allow additional agency based monitors to be installed and managed by individual Commonwealth Agencies.	Offeror must describe its approach to meet these requirements.
Continual Service Improvement		
7.	Reduce service risks.	Relative to the service in question, Offeror must provide examples of previous Offeror initiatives aimed at eliminating or mitigating service risks.
8.	Improve service quality.	Offeror must provide examples of previous Offeror initiatives aimed at improving service quality.
9.	Improve client satisfaction.	Offeror must provide examples of previous

		Offeror initiatives aimed at continually improving client satisfaction.
10.	Provide service transparency.	Offeror must provide examples of previous Offeror initiatives aimed at providing service transparency; in particular, visibility into the service execution process.
11.	Ensure service sustainability.	Offeror must provide examples of previous Offeror initiatives aimed at ensuring service sustainability; in particular, efforts targeted at cost containment and cost reductions.
12.	Improve/reduce cost of service.	Offeror must provide examples of Performance Monitoring and Management initiatives that have been implemented or can be utilized to achieve reduced costs of Services and to meet or exceeded ROI (Return on Investment) analysis projections.
Deliverables		
Deliverables are defined in **Schedule K – Key Program Deliverables**		
Offeror Response		

3.2.3 Facilities Management

3.2.3.1 Facilities Architecture / Maintenance

The Facilities Architecture and Maintenance service will provide and staff a minimum of two fully operational datacenter facilities in a multi datacenter mode. This service will require the integration and alignment of the non-core Services, including those relating to the premises, required to operate and maintain a datacenter that will fully support the core objectives of this project.

These datacenters will be geographically dispersed to provide protection from regional disruptions such as weather, power or other emergencies. The process of locating and managing these physical environments will include defining the physical site requirements, selecting appropriate facilities, and designing effective processes for monitoring and maintaining environmental Services and managing physical access. Effective management of the physical environment reduces the possibility of service interruptions due to unauthorized access and damage to computing equipment and personnel. Please review Exhibit D.7 - EDC Facility Summary for information regarding the EDC facilities.

Facilities Management includes all aspects of providing and managing the physical environment. For example; power and power distribution, cooling and ventilation, fire detection and suppression, building security and access control, and environmental monitoring are all required. Listed below are the basic Services required, but not inclusive of all Services needed, to manage an enterprise class datacenters required by the Commonwealth.

Reference Documentation

Exhibit D.7 - EDC Facility Summary

	Requirements	Describe Compliance
1.	Safe and secure datacenter. Two layers of authentication and appropriate clearances will be required. Provide datacenter environments which are secured to ensure that only authorized personal have physical access to the buildings, systems and all levels of data. This includes data storage within networked storage devices, servers, tapes, diskettes, optical and paper formats.	Offeror must describe its proposed facilities security program.

	Comply with the security requirements of the Commonwealth. Immediately inform the Commonwealth of any vulnerability or weakness in the Services, and recommend a solution or mitigation. Offeror must assess the EDC facilities and provide a report to the Commonwealth as it pertains to required security upgrades.	
2.	Provide fully redundant environmental Services. To include, but not limited to, HVAC, UPS conditioned power and distribution, generator backup, automated transfer switch, fire suppression system. Offeror must integrate its Facilities Management process with Service Management processes, especially Change Management, Incident Management, Service Continuity Management and Availability Management. Offeror must confirm its ability to provide, manage, maintain and operate multiple Tier 3 equivalent facilities. Offeror must assess the EDC facilities and provide a report to the Commonwealth as it pertains to required HVAC and power upgrades.	Offeror must describe solution and approach to meet this requirement. Offeror must provide details and supporting documentation on its proposed facilities and tier rating.
3.	Staff the datacenters with appropriate operational and management levels of personnel 24/7/365. Critical engineering and management staff will be available to the Commonwealth Monday through Friday, between 8am – 5pm Eastern time excluding Commonwealth observed holidays. Access to operational staff	Offeror must describe its proposed facilities staffing approach, including its staffing approach related to the EDC.

	will be available 24/7/365. Video surveillance system will be utilized at all entry points and throughout the datacenter and tape storage areas. Datacenter Staff will be required to adhere to the Commonwealth requirements for background checks and security clearances. Offeror shall be required to monitor the status of staff and to take appropriate action for staff found to subsequently have violated prescribed legal or ethical standards as described in **Schedule G –Staffing Plan and Key Positions**. Such violations shall be immediately reported and appropriate actions taken. Commonwealth verification of the requirements will be necessary prior to staff working on Commonwealth related systems.	
4.	Procurement Planning - Provide program and processes to alter the datacenter environment and to refresh the environmental Services at end-of-life, and as additional Services are needed.	Offeror must describe its facilities management processes, including those related to the EDC.
5.	Physical Access to Facilities- Coordinate with the Commonwealth to provide for physical access and facilitate inspections by government authorities (including the Commonwealth) for auditing the conduct of government business. Offeror must assess the EDC facilities and provide a report to the Commonwealth as it pertains to required physical access to the EDC facility.	Offeror must describe its facilities access policies and procedures.
6.	SLA Reporting - Identify and create environmental service level objectives in	Offeror must describe how it monitors and

	the form of SLAs, and report on the service availability, problems, and corrective actions on a monthly basis. Offeror must assess the EDC facilities and provide a report to the Commonwealth as it pertains to monitoring, maintain and reporting on EDC SLAs.	manages facility availability.
7.	The facilities must be designed and operated with environmentally friendly equipment and techniques, and be SSAE 16 compliant. Offeror must assess the EDC facilities and provide a report to the Commonwealth as it pertains to monitoring, maintaining and reporting on EDC SLAs.	Offeror must list all compliance ratings achieved at the proposed datacenters. Offeror must provide copies of annual SSAE 16 audits for all datacenters used to service the Commonwealth (and its agencies) at the Offeror's expense.
8.	Offeror must schedule (at its expense) a SSAE 16 audit of the EDC datacenter no more than 12 months after the effective date of the contract.	Offeror must provide proof of a valid (updated) SSAE16 certification in the form of audit findings report prior to implementing any Commonwealth service in any other proposed datacenter.
Continual Service Improvement		
9.	Reduce service risks.	Offeror must provide methods to eliminate or mitigate service risks.
10.	Improve service quality.	On a quarterly basis, Offeror must recommend to the Commonwealth team any facility changes that would be appropriate to maintained or improve SLA commitments.
11.	Improve client satisfaction.	Offeror must provide examples of previous Offeror initiatives aimed at continually improving client satisfaction.

12.	Ensure service transparency.	Offeror must provide methods and practice to ensure service transparency, providing visibility into service execution.
13.	Improve/reduce cost of service.	Offeror must provide examples of Facilities Management initiatives that have been implemented or can be utilized to achieve reduced costs of Services and to meet or exceeded ROI (Return on Investment) analysis projections.

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

3.2.3.2 Site Operations

The Site Operation service will provide datacenter operations staff and management to operate and monitor the IT computing equipment and Services being provided. The staff will interface with Commonwealth staff to institute best practice datacenter Services. Datacenter operations include, but are not limited to, management of the computing platforms, storage, local area networking, security firewall, tape backup, and offsite tape rotation systems.

Reference Documentation

Exhibit – D.7 - EDC Facility Summary

Exhibit G.6 - PSP - CJIS Security Policy

Exhibit G.9 - PSP – CCHRI

Exhibit G.7 - PSP - Summary of CJIS Requirements

Requirements		Describe Compliance
1.	Monitor and operate the various computer systems, network, network and local disk storage and firewall security systems.	Offeror must describe its facilities site operations including monitoring and general upkeep of the facilities including the following:

	Provide datacenter operations staff to monitor the computer system platforms, associated disk systems, networking Services and firewall and security systems. Ensure proper equipment operations, timely batch jobs processing and appropriate response to any abnormal end and error conditions. The Offeror will support application specific operations as determined by the application owner. This includes executing the troubleshooting procedures required by the application owners as detailed within the CCPM. This may include operational activities and initial troubleshooting steps, contact and escalation lists (aka "Run Book"). This information will be maintained by the Offeror on an application by application basis and will be hosted within the Knowledge Management Portal. A daily operations batch schedule report will be created and used to log normal / abnormal conditions. Abnormal conditions will be investigated for problem determination and rerun. Any abnormal condition that cannot be corrected will be referred to technical support staff for resolution. Properly clean and maintain equipment to minimize problems and outages, at intervals established with the Commonwealth or in compliance with stated and written specifications. Offeror must assess the EDC facilities and provide a report to the Commonwealth as it pertains to monitoring, maintaining and operating	• Processes and Procedures • Tools / Applications • End User Reports o Standard o Custom • Escalation Procedures

	the installed infrastructure.	
2.	For the systems that utilize tape backup Services, Offeror must provide a structured tape management approach. For systems that utilize disk-2-disk backup approach Offeror must provide a structured disk-2-disk approach. Manage and maintain the tape backup system and Services. Rotate designated tapes to, and returned from approved offsite storage location. Maintain detailed audit log of tape movement. Some agency applications fall under additional CJIS and CCHRI security requirements for tape backups. Provide datacenter operations staff to manage and maintain the tape management system. Tapes will be rotated to, and returned from an approved offsite vaulting subcontractor. An automated software process will be utilized to report the completion status of backup processing, with electronic notification of failures sent to Offeror technical support, and identified Commonwealth staff for follow up and corrective action. Provide the facilities to Retrieve External Storage Media from on-site and off-site storage as requested by the Commonwealth or as required in an emergency. Wipe or erase the data and configuration information resident on the media prior to disposal or re-use, and in accordance with Commonwealth standards.	Offeror must describe its tape management approach and describe the process to work with the Commonwealth Agencies to provide a classification and categorize tapes per the type of data contained on the tapes. Offeror must describe its disk-2-disk backup approach. Offeror must assess the EDC tape backup facilities and provide a report to the Commonwealth as it pertains to manage and operated the installed tape backup systems and media operations.

	Dispose of retired media in an environmentally sound manner after purging any Commonwealth data using Commonwealth, and/or Federal guidelines/policies prior to disposing of media. Operate media libraries and library management systems as required to provide the Services. Maintain an existing inventory control system to properly manage External Storage Media in storage and prepare them for shipment to the contingency site.	
3.	Monitor physical access and security of the datacenter. Video surveillance is required. Staff the datacenter with appropriate level of staff and management 24/7/365. The Offeror must monitor physical access to the datacenter and respond to security incidents in a consistent and auditable manner. All breaches will be reported to the Commonwealth for review and follow up action as required. Monitoring of the video system for all entry points and throughout the datacenter and tape storage areas will be included in this responsibility. Offeror will be required to adhere to the Commonwealth requirements for background checks and security clearances. Commonwealth verification that the requirements have been met will be necessary prior to Offeror working on Commonwealth related systems.	Offeror must describe its physical access and security monitoring approach for proposed Offeror datacenters including staff roles, responsibilities and background check process. Offeror must assess the EDC current physical access and security plan and provide a report to the Commonwealth as it pertains to any required upgrades.

4.□	Manage and maintain equipment configuration inventory system. Provide staff to create and maintain a configuration record for all hardware and software components in the datacenter. This must be an accurate record of all software, computing, disk storage, tape, network, racking, cables, and environmental equipment.	Offeror must describe the proposed approach to managing the support of its datacenter technology.
5.□	Provide programs and processes to alter the operational environment, and to refresh the Services at asset end-of-life or implementation of new technology Services, as these Services are needed.	Offeror must describe solution and approach to meet this requirement.
6.□	Identify and create service objectives for the site operational Services in the form of SLAs, and report on the service availability, problems, and corrective actions on a monthly basis.	Offeror must describe how it monitors and manages facility operations to meet/exceed the agreed to availability service levels.
Continual Service Improvement		
7.□	Reduce service risks.	Offeror must provide methods to eliminate or mitigate service risks.
8.□	Improve service quality.	On a quarterly basis, Offeror must also recommend to the Commonwealth team any site operational changes that would be appropriate to maintained or improve SLA commitments.
9.□	Improve client satisfaction.	Offeror must provide examples of previous Offeror initiatives aimed at continually improving client satisfaction.
10.□	Ensure service transparency.	Offeror must provide methods and practices to ensure service transparency, providing visibility into service execution.

11.	Integrate Continuous Improvement Program processes into Availability Management and Service Level Management.	Offeror must describe offering in this area including the projected impacts/benefits.
12.	Improve/reduce cost of service.	Offeror must provide examples of Site Operations initiatives that have been implemented or can be utilized to achieve reduced costs of Services and to meet or exceeded ROI (Return on Investment) analysis projections.
Deliverables		
Deliverables are defined in **Schedule K – Key Program Deliverables**		
Offeror Response		

3.2.4 Managed Hosting Services

For all Managed Hosting Services, the Offeror must actively monitor the daily operations of the infrastructure used to provide the services. The Offeror must execute the troubleshooting procedures required by the application owners as detailed within the CCPM. This may include operational activities and initial troubleshooting steps, contact and escalation lists (aka "Run Book"). This information will be maintained by the Offeror on an application by application basis and will be hosted within the Knowledge Management Portal.

3.2.4.1 Windows Support

This service will provide hosting, operations and support Services for Microsoft Windows based servers (physical and virtual) located at the central datacenters. Offeror must support various hardware systems and various versions of the Microsoft operating systems, and support service software. The Offeror must provide support for both physical and virtual servers. Currently the Commonwealth utilizes virtualization technology from VMware and Microsoft's Hyper-V. See attached Exhibits for hardware and software details. The number and level of support staff members required to perform the below listed tasks will be determined by the Offeror, based on number of Commonwealth clients, hardware, software, and operating systems being serviced.

Listed below are the basic Services required, but not inclusive of all Services needed, to manage an enterprise class datacenter required by the Commonwealth. Offeror must include these Services within the base level of Services in this Offering. Change requests will be approved and authorized using the change management process.

Reference Documentation

Exhibit B.1 – DPH - Asset List

Exhibit B.2 - Commonwealth Owned DPH IT Assets

Exhibit C.1 – DPW - Room 105 and CAO Servers – Storage

Exhibit D.1 - EDC - Server Inventory

Exhibit D.2 - EDC - Switch Summary

Exhibit D.3 - EDC - Storage Summary

Exhibit D.5 – EDC - DOT Datacenter Inventory

Exhibit E.1 - DLI - Datacenter Inventory Template

Exhibit F.1 - DOH - Datacenter Inventory

Exhibit F.2 - DOH - DPH Asset List

Exhibit F.3 - DOH - DPH COPA Software Asset IBM

Exhibit F.4 – DOH – Physical Servers

Exhibit G.1 - PSP - Datacenter HW Inventory

Exhibit G.3 - PSP - DPH Asset List

Exhibit H.1 - DOR - Datacenter Inventory

Exhibit H.2 - DOR - DPH Asset List

Exhibit H.4 - DOR - SAP TRM System

Exhibit I.1 - IES - DPH COPA Owned IT Assets

Requirements		Describe Compliance
1.	Monitor local operations, troubleshoot and resolve operational issues. Actively monitor the daily operations of all MS Windows servers. Maintain a log for each server detailing hardware / software configuration and critical service operations. Document review of the system logs on a weekly basis to ensure critical system Services are processing without errors. Complete weekly server log indicating which logs were reviewed, date and	Offeror must describe its approach to supporting Windows based server environment including the following: • Processes and Procedures • Tools / Applications • End User Reports o Standard o Custom • Tiered Service/Support Levels • Escalation Procedures

	initial the log.	
2.	Monitor system backup processing on a daily basis. Review daily backup log for successful completion. Note failures, and correct the problems. Create problem record for any abnormal condition and any repairs that have been made, re-execute as appropriate. An automated software process will be utilized to report the completion status of backup processing, with electronic notification of failures sent to Offeror technical support, and identified Commonwealth staff for follow up and corrective action.	Offeror must describe its approach to performing an initial review and audit of the backup policies, procedures and reports, to ensure the accuracy of the backup schedules, retention periods, target directories, and recovery point objectives. Offeror must describe its approach to identify gaps and potential risks, and how those gaps and risks will be resolved. Offeror must describe how the authorized Commonwealth users will have online access to backup logs.
3.	Provide Microsoft Hyper-V and VMware trained staff holding manufacturer recognized certifications for hardware and software technical support. Post award; provide the Commonwealth a resume or CV for each operational staff member assigned to this engagement. A copy will be maintained on Offeror file including verified background clearances as required.	Offeror must submit a representative sample of staff resumes typically provided for these positions detailing their experience, education, and certifications.
4.	Provide cost effective operational and technical support for the Windows computing platform. Provide platform level operational and technical support for the computing platform. Provide Level 2 and Level 3 Support to the Service Desk and/or Commonwealth Users.	Offeror must describe its approach to providing and maintaining different tiered levels (i.e. Level 2 & Level 3 Technical Support) of support. Offeror must provide a representative sample of available tiered service support Services.

	Provide a tiered level of support Services (e.g. Gold, Silver, and Bronze). Provide technical advice and support to the Application Development and Maintenance (ADM) and Database Administration (DBA) staffs, as required. Post award; provide Commonwealth with a resume or CV for each operational staff member assigned to this engagement. A copy will be maintained on Offeror file.	
5.	Ensure network connectivity and consistent system response times. Utilize automated system management tool(s) to ensure real- time monitoring and notification of server availability and response times. Stop / Start times of servers will be a source of input for SLA measurements. Identify tool set(s).	Offeror must describe its real-time monitoring approach and its toolset for providing and maintaining network availability and performance. Offeror must identify tools it uses to support network availability and performance.
6.	Ensure server operating systems are maintained with the current patch level, based on the Services provided by the server. Analyze monthly service patches and determine which need to be applied, by server type. Create a change record, log the update in the server log, install based on server maintenance schedule and update the server configuration record. Notify impacted Commonwealth users immediately of any unscheduled service interruptions via email/web. The Offeror must be document normal	Offeror must describe its approach to patch management. Offeror must identify tools it uses to manage system patches. Offeror must describe its approach to testing and validating updates to the OS and 3rd Party software that it supports. Offeror must describe its approach to communicate unscheduled and scheduled outages, including escalation process.

	work hours and holiday schedules with each agency to determine the contact method and escalation process of each Commonwealth agency.	
7.□	Provide a review and analysis of system performance/capacity to determine if current performance/capacities are sufficient to support the needs of the stakeholders.	Offeror must perform an initial review and audit of the current usage, procedures and reports and provide an analysis of the current usage, processes and reports currently being supported. Offeror must document its review and audit findings and recommendations.
8.□	User Account Management - Provide certified operating system administration staff to create and maintain the registration of profiles, associated groups, and the security permissions required to service the approved client base of the operating systems.	Offeror must describe its approach to managing user accounts.
9.□	Procurement Planning Provide program and processes to refresh the hardware at asset end-of-life, and as upgrades are needed to meet anticipated growth in utilization.	Offeror must describe its programs and processes for procuring new or upgraded systems.
10.□	SLA Reporting Collect actual system availability, utilization and response time data. On a monthly basis, Offeror must create a Service Level Agreement report for the Commonwealth team.	Offeror must describe processes and toolsets it uses for monitoring and maintaining service levels. Offeror must provide a representative sample of an SLA report.
11.□	Installation of Windows updates/patches must be coordinated by Agency. For IES, windows version upgrades must be SAP certified. Coordinate at an agency level and account for any required patching as	Offeror must describe its programs and processes for applying system updates/patches.

	technology upgrades require.	
12.	The Offeror must provide Software License Management.	Offeror must describe solution and approach to meet this requirement.
Continual Service Improvement		
13.	Reduce service risks.	Offeror must provide methods to eliminate or mitigate service risks.
14.	Improve service quality.	On a quarterly basis, Offeror must also recommend to the Commonwealth team any system changes that would be appropriate to maintain or improve SLA commitments.
15.	Improve client satisfaction.	Offeror must provide examples of previous Offeror initiatives aimed at continually improving client satisfaction.
16.	Ensure service transparency.	Offeror must provide methods and practices to ensure service transparency, providing visibility into service execution.
17.	Improve/reduce cost of service.	Offeror must provide examples of Windows Support initiatives that have been implemented or can be utilized to achieve reduced costs of Services and to meet or exceeded ROI (Return on Investment) analysis projections.
Deliverables		
Deliverables are defined in **Schedule K – Key Program Deliverables**		
Offeror Response		

3.2.4.2 Storage Management

The Storage Management service will provide hosting and operational support Services for storage management systems. Storage management systems must be maintained at current support levels for optimal performance, recoverability, and secure operations. Systems will be located in the Offeror's datacenters. The Offeror must support the hardware and software components of these systems.

The proposed storage management service and solution must address adherence to multiple security and compliance requirements relating to the storage and management of multiple types of data assets (e.g. CHRIA law, criminal history).

Reference Documentation

Exhibit B.1 - DPH - Asset List

Exhibit B.2 - DPH - Commonwealth Owned DPH IT Assets

Exhibit C.1 - DPW - Room 105 and CAO Servers – Storage

Exhibit D.1 - EDC - Server Inventory

Exhibit D.2 - EDC - Switch Summary

Exhibit D.3 - EDC - Storage Summary

Exhibit D.5 - EDC - DOT Datacenter Inventory

Exhibit E.1 - DLI - Datacenter Inventory Template

Exhibit F.1 - DOH - Datacenter Inventory Template

Exhibit F.2 - DOH - DPH Asset List

Exhibit F.3 - DOH - DPH COPA Software Asset IBM

Exhibit F.4 – DOH – Physical Servers

Exhibit G.1 - PSP - Datacenter HW Inventory

Exhibit G.3 - PSP - DPH Asset List

Exhibit G.12 - PSP - CHRIA Handbook

Exhibit H.1 - DOR - Datacenter Inventory

Exhibit H.2 - DOR - DPH Asset List

Exhibit H.4 - DOR - SAP TRM System

Exhibit I.1 - IES - DPH COPA Owned IT Assets

Requirements		Describe Compliance
1.	Monitor local operations, troubleshoot and resolve operational issues. Monitor system backup processing on a daily basis. Actively monitor the daily operations of all storage units. Maintain a log for each storage unit. Complete weekly service logs indicating the frequency logs are reviewed, and the status of the daily backup process. Create problem records for any abnormal	Offeror must describe proposed storage management Services. Offeror must identify tools it uses to support data backups including the following: • Processes and Procedures • Tools / Applications • End User Reports o Standard o Custom • Tiered Service/Support Levels

	condition and any repairs that have been made.	• Escalation Procedures
2.	Provide appropriately trained staff that hold current manufacturer certifications for hardware and software technical support (where available). Staff will interact with vendor support Services as needed. Provide Commonwealth with a resume or CV for each operational staff member assigned to this engagement. A copy will be maintained on Offeror file including required background checks and clearances as required.	Offeror must submit a representative sample of staff resumes typically provided for these positions detailing their experience, education, and certifications.
3.	Provide platform level operational and technical support for the computing platform. Provide Level 2 and Level 3 Support to the Service Desk and/or Commonwealth Users. Provide a tiered level of support Services (e.g. Gold, Silver, Bronze)	Offeror must describe its approach to providing and maintaining different tiered levels of support. Offeror must provide a representative sample of available tiered service support Services.
4.	Monitor system backup processing on a daily basis. Review daily backup log for successful completion. Note failures, and correct the problem. Create problem record for any abnormal condition and any repairs that have been made. An automated software process will be utilized to report the completion status of backup processing, with electronic notification of failures sent to identified Commonwealth staff and Offeror technical support for follow	Offeror must describe its approach to perform an initial review and audit of the backup policies, procedures and reports, to ensure the accuracy of the backup schedules, retention periods, target directories, and recovery point objectives. Offeror must describe its approach to identifying gaps and potential risks, and how those gaps and risks will be resolved.

	up and corrective action.	
5.	Ensure network connectivity, and consistent system response times. Identify automated system management tool(s) to ensure storage system availability and expected response times. Stop / Start time records will be a source of input for SLA measurements. Identify tool set(s).	Offeror must describe its real-time monitoring approach and toolset to provide and maintain network availability and performance. Offeror must identify tools it uses to support network availability and performance.
6.	Ensure storage device operating systems are maintained with the current system patch level, including firmware upgrades. Analyze monthly service patches and determine which patches need to be applied. Create a change record, log the update in the storage system log, and install based on maintenance schedule. Notify impacted Commonwealth users immediately of any unscheduled service interruptions via email/web. The Offeror must document normal work hours and holiday schedules with each agency to determine the contact method and escalation process of each Commonwealth agency. Coordinate at an agency level and account for any required patching as technology upgrades require.	Offeror must describe its approach to patch management. Offeror must identify tools used to manage system patches. Offeror must describe its approach for testing and validating updates to the OS and 3rd Party software that it supports. Offeror must describe its approach to communicating unscheduled and scheduled outages, including escalation process.
7.	Utilize data storage conservation techniques such as data de-duplication or other industry standards, to reduce the overall footprint of the data.	Offeror must describe approach and toolset to meet this requirement. Offeror must describe data retention options/Services to store data for extended periods.

8.□	Propose options/solutions for self-provisioning or limited self-management of storage as a service.	Offeror must describe approach and toolset to meet this requirement.
Continual Service Improvement		
9.□	Reduce service risks.	Offeror must provide methods to eliminate or mitigate service risks.
10.□	Improve service quality.	On a quarterly basis, Offeror must also recommend to the Commonwealth team any system changes that would be appropriate to maintain or improve SLA commitments.
11.□	Improve client satisfaction.	Offeror must provide examples of previous Offeror initiatives aimed at continually improving client satisfaction.
12.□	Ensure service transparency.	Offeror must provide methods and practices to ensure service transparency, providing visibility into service execution.
13.□	Improve/reduce cost of service.	Offeror must provide examples of Storage Management initiatives that have been implemented or can be utilized to achieve reduced costs of Services and to meet or exceeded ROI (Return on Investment) analysis projections.
Deliverables		
Deliverables are defined in **Schedule K – Key Program Deliverables**		
Offeror Response		

3.2.4.3 ERP Hosting – SAP / Oracle

ERP Hosting – SAP service will provide hosting and operational support Services for two SAP-ERP systems that are currently located at the DPH. One system Services the General Accounting System application, and the other Services the Integrated Tax System application for the Department of Revenue. Each application has associated development and testing environments support on segregated equipment. Offeror must support various production and non-production versions of the applications and the associated hardware. The roles and the number of staff members required to perform the below listed tasks will be determined by the Offeror.

Due to the critical and complex nature of these SAP environments, the Commonwealth requires an experienced SAP hosting provider. The Offeror's proposed target infrastructure design for the Commonwealth's SAP environments must include a certified SAP sizing report prior to migration of the systems.

The ERP Hosting – Oracle service will provide hosting and operational support Services for the current Oracle Enterprise system utilized by the Pennsylvania Liquor Control Board (PLCB). The application has associated development and testing environments support on segregated equipment. Offeror must support various production and non-production versions of the applications and the associated hardware.

Reference Documentation

Exhibit H.4 - DOR - SAP TRM System

Exhibit I.1 - IES - DPH Commonwealth Owned IT Assets

Exhibit I.2 - IES - Application Inventory

Exhibit I.3 - IES - DPH Commonwealth Software Asset Unisys

Exhibit I.4 - IES - DPH September 2012 Measurement Report

Exhibit B.2 - Commonwealth Owned DPH IT Assets (see PLCB Oracle systems)

	Requirements	Describe Compliance
1.	Provide ERP Hosting Services for SAP and Oracle based applications.	Offeror must describe its approach to providing ERP Hosting Services for both SAP and Oracle ERP systems. Offeror must provide a minimum of 3 verifiable Customer References of customers that use its SAP Hosting Services. Offeror must provide a minimum of 3

		verifiable Customer References of customers that use its Oracle Hosting Services.
2.	Monitor local system operations, troubleshoot and resolve operational issues. Actively monitor the daily operations of all ERP systems. Maintain a log for each server detailing hardware / software configuration and critical service operations. Document review of the system logs on a weekly basis to ensure critical system Services are processing without errors. Complete weekly server log indicating which logs were reviewed, date and initial the log.	Offeror must describe its approach to monitoring and maintaining SAP and Oracle ERP systems including the following: • Processes and Procedures • Tools / Applications • End User Reports o Standard o Custom • Tiered Service/Support Levels • Escalation Procedures
3.	Monitor system backup processing on a daily basis. Review daily backup log for successful completion. Note failures, and correct the problem. Create problem record for any abnormal condition and any repairs that have been made. An automated software process will be utilized to report the completion status of backup processing, with electronic notification of failures sent to Offeror technical support, and identified Commonwealth staff for follow up and corrective action.	Offeror must describe its approach to perform an initial review and audit of the backup policies, procedures and reports, to ensure the accuracy of the backup schedules, retention periods, target directories, and recovery point objectives. Offeror must describe its approach to identify gaps and potential risks, and how those gaps and risks will be resolved.
4.	Provide IBM, SAP, and Oracle trained staff holding current manufacturer certifications for hardware and software technical support. Staff will interact with vendor support Services	Offeror must submit a representative sample of staff resumes typically provided for these positions detailing their experience, education, and certifications.

	when needed. Provide Commonwealth with a resume or CV for each operational staff member assigned to this engagement. A copy will be maintained on Offeror file including required background checks and clearances as required.	
5.	Provide cost effective operational and technical support for the computing platform. Provide Level 2 and Level 3 Support to the Service Desk and/or Commonwealth Users. Provide a tiered level of support Services (e.g. Gold, Silver, and Bronze).	Offeror must describe its approach to providing and maintaining different tiered levels of ERP (SAP & Oracle) support.
6.	Ensure network connectivity, and consistent system response times. Utilize automated system management tool(s) to ensure real-time monitoring and notification of server availability and response times. Stop / Start times of servers will be a source of input for SLA measurements. Identify tool set(s).	Offeror must describe its real-time monitoring approach and toolset to provide and maintain network availability and performance. Offeror must identify tools it uses to support network availability and performance.
7.	Ensure server operating systems are maintained with the current system patch level, based on the Services provided by the server. Analyze monthly service patches and determine which patches need to be applied, by server type. Create a change record, log the update in the server log, and install based on server maintenance schedule. Implement a Patch Management Program to ensure the timely application of updates on all	Offeror must describe its approach to patch management including analysis, communications, schedule (change records) and installation process. Offeror must describe its approach for testing and validating updates to the OS and 3rd Party software that it supports. Offeror must describe its approach to communicating unscheduled and scheduled outages, including its escalation process.

	infrastructure platforms in accordance with Commonwealth IT policy guidelines.	
8.	User Account Management Provide certified system administration staff to create and maintain the registration of profiles, associated groups, and the security permissions required to service the approved client base of the system and application.	Offeror must describe its administration/support approach and provide representative resumes.
9.	Procurement Planning Provide program and process to refresh the hardware at asset end-of-life, and when upgrades are needed to meet anticipated growth in utilization.	Offeror must describe its program and processes for upgrading systems.
10.	SLA Reporting Collect actual system availability, utilization and response time data. On a monthly basis, Offeror must create a SLA report for the Commonwealth and Vendor Management teams.	Offeror must describe its processes and toolset for monitoring and maintaining service levels. Offeror must provide a representative sample of its SLA reports for ERP hosting Services.
Continual Service Improvement		
11.	Reduce service risks.	Offeror must provide methods to eliminate or mitigate service risks.
12.	Improve service quality.	On a quarterly basis, Offeror must also recommend to the Commonwealth team any system changes that would be appropriate to maintain or improve SLA commitments.
13.	Improve client satisfaction.	Offeror must provide examples of previous Offeror initiatives aimed at continually improving client satisfaction.

14.	Ensure service transparency.	Offeror must provide methods and practices to ensure service transparency, providing visibility into service execution.
15.	Improve/reduce cost of service.	Offeror must provide examples of ERP Hosting initiatives that have been implemented or can be utilized to achieve reduced costs of Services and to meet or exceeded ROI (Return on Investment) analysis projections.
Deliverables		
Deliverables are defined in **Schedule K – Key Program Deliverables**		
Offeror Response		

3.2.4.4 UNIX Support – AIX / Linux

The Unix Support – AIX / Linux service will provide hosting and operational support Services for AIX and Linux server systems. The systems will be located in the Offeror's datacenters. Offeror must support various versions of the AIX and Linux operating systems. The number of staff members required to perform the operational tasks listed below will be determined by the Offeror.

Reference Documentation

Exhibit E.1 - DLI - Datacenter Inventory Template

Exhibit H.1 - DOR - Datacenter Inventory

Exhibit H.2 - DOR - DPH Asset List

Exhibit H.4 - DOR - SAP TRM System

Exhibit I.1 - IES - DPH Commonwealth Owned IT Assets

Exhibit I.2 - IES - Application Inventory

Exhibit I.3 - IES - DPH Commonwealth Software Asset Unisys

Exhibit B.2 - Commonwealth Owned DPH IT Assets (see PLCB Oracle systems)

Requirements		Describe Compliance

1.	Monitor local operations, troubleshoot and resolve operational issues.
	
	Actively monitor the daily operations of all AIX / Linux systems. Assume responsibility for all master and subordinate console functions. Issue operator commands to control all In-Scope platforms. Assume the responsibility for and perform all console operations. Monitor the performance of online interactive traffic and take appropriate action to resolve online-system-related incidents and/or problems, including escalating (as appropriate) the incident and/or problem to the proper Level 2 Support group. Monitor the transmission of files between the
		Offeror must describe its UNIX/Linux monitoring, operations and troubleshooting approach Commonwealth including the following:
		
		• Processes and Procedures
		• Tools / Applications
		• End User Reports
		  o Standard
		  o Custom
		• Support Levels
		• Escalation Procedures

	Commonwealth and any other parties as designated by Commonwealth. Provide operational support for data transmission (send/receive), consistent with commercial or agency standards. Manage, maintain, monitor, and control online and batch process, both scheduled and unscheduled (including on-request processing). Maintain a log for each server detailing hardware / software configuration and critical service operations. Review the system logs on a weekly basis to ensure critical system Services are processing without errors. Document review of the system logs on a weekly basis to ensure critical system Services are processing without errors. Complete weekly server log indicating which logs were reviewed, date and initial the log. Maintain and update the operational documentation for all operations procedures and Services.	
2.	Provide a review and analysis of UNIX system performance/capacity to determine if current performance/capacities are sufficient to support the needs of the UNIX stakeholders.	Offeror must perform an initial review and audit of the current UNIX usage, procedures and reports and provide an analysis of the current UNIX usage, processes and reports currently being supported. Offeror must document its review and audit findings and recommendations.
3.	Production Control and Scheduling (including batch processing) Describe the process of scheduling batch jobs within Commonwealth agency defined windows to achieve maximum performance as long as required batch completion times are met. A cross platform (e.g. Window,	Offeror must describe its approach to supporting the batch processing needs of the Commonwealth including the following: • Processes and Procedures • Tools / Applications • End User Reports 0 Standard 0 Custom

	Unix, and Mainframe) system will be required. Where practicable, provide for automated scheduling of batch work and processes including backups. Commonwealth agencies have a number of applications that require scheduling software / batch processing software (i.e. $Universe, SAP certified, etc.), this software is heavily integrated into many of these systems. Develop, maintain, and utilize an emergency contact list and escalation procedures to resolve abnormally ended jobs. Resolve abnormally ended jobs caused by conditions external to production programs. Repair abnormally ended jobs when possible and perform job restarts in accordance with the Service Management Manual. Check job outputs and print queues, and change job priorities. Notify Commonwealth agencies in accordance with the Offeror's proposed notification procedures in the event that applications do not execute properly.	• Tiered Service & Support Levels • Escalation Procedures Offeror must describe how it will operate and maintain current scheduling/batch software tools.
4.	Monitor system backup processing on a daily basis. Review daily backup logs for successful completion. Note failures, and correct the problem. Create problem record for any abnormal condition and any repairs that have been made. An automated software	Offeror must describe its approach to performing an initial review and audit of the backup policies, procedures and reports, to ensure the accuracy of the backup schedules, retention periods, target directories, and recovery point objectives. Offeror must describe its approach to identifying gaps and potential risks, and how those gaps and risks will be resolved.

	process will be utilized to report the completion status of backup processing, with electronic notification of failures sent to Offeror technical support, and identified Commonwealth staff for follow up and corrective action.	
5.	Provide AIX and Linux trained staff that hold current manufacturer certifications for hardware and software technical support. Provide technical advice and support to the Application Development and Maintenance (ADM) and Database Administration (DBA) staffs, as required. Post award; provide Commonwealth with a resume or CV for each operational staff member assigned to this engagement. A copy will be maintained on Offeror file.	Offeror must submit a representative sample of staff resumes typically provided for these positions detailing their experience, education, and certifications.
6.	Provide cost effective operational and technical support for the computing platform. Provide platform level operational and technical support for the computing platform. List the service levels for the various service tiers that can be provided. See Schedule J.1 Datacenter Service Level Management for the definitions of the expected options. Provide Level 2 and Level 3 Support to the Service Desk and/or Commonwealth Users.	Offeror must describe its approach to supporting the operational and technical support needs of the Commonwealth.
7.	Ensure network connectivity to COPANET, and consistent system response times.	Offeror must describe its real-time monitoring approach and toolset to provide and maintain network availability and

	Utilize automated system management tool(s) to ensure real-time monitoring and notification of server availability and response times. Stop / Start times of servers will be a source of input for SLA measurements.	performance. Offeror must identify tools it uses to support network availability and performance.
8.	Ensure server operating systems are maintained with the current system patch level, based on the Services provided by the server. Analyze monthly service patches and determine which patches need to be applied, by server type. Create a change record, log the update in the server log, and install based on server availability schedule. Change requests will be approved and authorized using the change management process. Notify the Commonwealth of any scheduled or unscheduled service interruptions. Implement a Patch Management Program to ensure the timely application of updates on all infrastructure platforms in accordance with Commonwealth IT policy guidelines.	Offeror must describe its approach to supporting the software patch needs of the Commonwealth. Offeror must describe its approach to testing and validating updates to the OS and 3rd Party software that it supports. Offeror must describe its approach to communicating unscheduled and scheduled outages, including escalation process.
9.	User Account Management Provide certified system administration staff to create and maintain the registration of profiles, associated groups, and the security permissions required to service the approved client base of the system and application.	Offeror must describe its approach to supporting the needs of the Commonwealth.
10.	Procurement Planning Provide program and processes to	Offeror must describe its approach to supporting the needs of the Commonwealth.

	refresh the hardware at asset end-of-life, and when upgrades are needed to meet anticipated growth in utilization.	
11.	SLA Reporting Collect actual system availability, utilization and response time data. On a monthly basis, create a Service Level Agreement report for the Commonwealth and Vendor Management teams.	Offeror must describe its approach to supporting the needs of the Commonwealth.
12.	The Offeror must provide Software License Management.	Offeror must describe solution and approach to meet this requirement.
Continual Process Improvement		
13.	Reduce service risks.	Offer to identify methods and approaches to eliminate or mitigate service risks.
14.	Improve service quality.	On a quarterly basis, Offeror must also recommend to the Commonwealth team any system changes that would be appropriate to maintain or improve SLA commitments.
15.	Improve client satisfaction.	Offeror must provide examples of previous Offeror initiatives aimed at continually improving client satisfaction.
16.	Ensure service transparency.	Offeror must identify methods and practice to ensure service transparency, providing visibility into service execution.
17.	Improve/reduce cost of service.	Offeror will provide examples of UNIX Support initiatives that have been implemented or can be utilized to achieve reduced costs of Services and to meet or exceeded ROI (Return on Investment) analysis projections.

Deliverables
Deliverables are defined in **Schedule K – Key Program Deliverables**
Offeror Response

3.2.4.5 Mainframe Services

The Mainframe Services will provide hosting and operational support Services for both IBM and Unisys mainframe systems. These mainframe systems run several Logical Partitions (LPAR's) and Integrated Facility for Linux (IFL) partitions. Offeror must support the mainframe operating systems and the management of the associated partitions. The number of support staff members required to perform the tasks listed below will be determined by the Offeror.

Listed below are the basic Services required to manage the Mainframe systems required by the Commonwealth. Offeror must include these Services in addition to the base level of Services in this Offering.

Reference Documentation

Exhibit B.1 DPH - Asset List

Exhibit B.3 DPH - Commonwealth Software Asset Listing

Exhibit B.4 - DPH - Third Party Software

Exhibit B.5 DPH - Agency Disaster Recovery Matrix

Exhibit B.6 - DPH - COPA NETWORK

	Requirements	**Describe Compliance**
1.	Provide Mainframe systems and operations (Unisys, IBM). Ability to purchase metered IBM & Unisys Million Instructions Per Second (MIPS). Monitor local operations, troubleshoot and resolve operational issues. Actively monitor the daily operations of all mainframe (current) systems.	Offeror must describe its approach to supporting the needs of the Commonwealth including the following: • Processes and Procedures • Tools / Applications • End User Reports o Standard o Custom • Tiered Service/Support Levels

	Assume responsibility for all master and subordinate console functions. Issue operator commands to control all In-Scope platforms throughout the organization. Provide all tools and apps that are currently being provided, for example MAPPER/APPMAP, browser based terminal emulation access, and middleware components (like OpenTI, IBM WBM & WMQ, etc.) that are critical to agency operations and application usage. Assume the responsibility for and perform all console operations. Monitor the performance of online interactive traffic and take appropriate action to resolve online-system-related incidents and/or problems, including escalating (as appropriate) the incident and/or problem to the proper Level 2 Support group. Monitor the transmission of files between the Commonwealth and any other parties as designated by the Commonwealth. Provide operational support for data transmission (send/receive), consistent with commercial or agency standards. Manage, maintain, monitor, and control online and batch process, both scheduled and unscheduled (including on-request processing). Maintain a log for each system detailing hardware / software configuration and critical service operations. Review the system logs on a weekly basis to ensure critical system Services are processing	• Escalation Procedures

	without errors. Maintain and update the operational documentation for all operations procedures and Services.	
2.	Provide a review and analysis of mainframe usage to determine if current usage is required to support the needs of the mainframe stakeholders. Offeror must perform an initial review and audit of the current mainframe usage, procedures and reports and provide an analysis of the current mainframe usage, processes and reports currently being supported. Offeror must document its review and audit findings and recommendations.	Offeror must describe solution and approach to meet this requirement.
3.	Production control and scheduling (including batch jobs) Provide a process of scheduling batch jobs within Commonwealth agency defined windows to achieve maximum performance as long as required batch completion times are met. Provide for automated scheduling of batch work and processes including backups. Provide the capability for agencies to schedule and monitor batch processing. Develop, maintain, and utilize an emergency contact list and escalation procedures to resolve abnormally ended jobs. Resolve abnormally ended jobs caused by conditions external to production	Offeror must describe solution and approach to meet this requirement.

	programs. Repair abnormally ended jobs when possible and perform job restarts in accordance with the Service Management Manual. Check job outputs and print queues, and change job priorities. Notify Commonwealth agency customers in accordance with the notification procedures in the event that applications and batch processing do not execute properly.	
4.	Batch Monitoring Actively monitor batch operations on all mainframe systems on a daily basis. Maintain a log for each batch system and review the system logs on a daily basis to ensure key batch Services are processing without errors. Document review of the system logs on a daily basis to ensure critical batch Services are processing without errors. Notify Commonwealth agencies in accordance with the notification procedures in the event that batch processing does not execute properly. Offeror must provide online monitoring of batch processing by the Commonwealth.	Offeror must describe its approach to supporting the needs of the Commonwealth. Offeror must describe its approach to allowing Commonwealth users to monitor the batch processing online.
5.	Monitor system backup processing on a daily basis. Process to review daily backup log for successful completion. Note any failures, initial and date the log, and correct the problem. Create problem	Offeror must describe its approach to performing an initial review and audit of the backup policies, procedures and reports, to ensure the accuracy of the backup schedules, retention periods, target directories, and recovery point objectives. Offeror must describe its approach to

	record for any abnormal condition and any repairs that have been made. Automated software process will be utilized to report the completion status of backup processing, with electronic notification of failures sent to Offeror technical support, and identified Commonwealth staff for follow up and corrective action.	identifying gaps and potential risks, and how those gaps and risks will be resolved.
6.	Provide cost effective, operational, and technical support for the computing platform. Provide platform level operational and technical support for computing platforms including Mainframe, Storage, AIX, LINUX, SAP, Oracle and Windows architects. Provide Level 2 and Level 3 Support to the Service Desk and/or Commonwealth Users. Provide technical advice and support to the Application Development and Maintenance (ADM) and Database Administration (DBA) staffs, as required. List the service levels for the various levels of service tiers that can be provided. See **Schedule J.1 Datacenter Service Level Management** for the definitions of the expected options.	Offeror must describe its approach to supporting the needs of the Commonwealth.
7.	Ensure network connectivity to COPANET, and consistent system response times. Utilize automated system management tool(s) to ensure real time monitoring and notification of system availability	Offeror must describe its real-time monitoring approach and toolset to provide and maintain network availability and performance. Offeror must identify tools it uses to support

	and response times. Stop / Start times of servers will be a source of input for SLA measurements	network availability and performance.
8.	Ensure operating systems are maintained with the current system patch level, based on the Services provided by the server. Analyze monthly service patches and determine which patches need to be applied. Create a change record, log the update in the system log, and install based on system availability schedule. Notify the Commonwealth of any scheduled or unscheduled service interruptions with consideration to Commonwealth scheduled holidays and standard workweek. Implement a Patch Management Program to ensure the timely application of updates on all infrastructure platforms in accordance with Commonwealth IT policy guidelines.	Offeror must describe its approach to supporting the needs of the Commonwealth. Offeror must describe its approach for testing and validating updates to the OS and 3rd Party software that it supports. Offeror must describe its approach to communicate unscheduled and scheduled outages, including escalation process.
9.	User Account Management Provide certified system administration staff to create and maintain the registration of profiles, associated groups, and the security permissions (including password management) required to service the approved client base of the system and application.	Offeror must describe its approach to supporting the needs of the Commonwealth.
10.	Procurement Planning Provide a program and process to refresh the hardware at asset end-of-life, and when upgrades are needed to	Offeror must describe its approach to supporting the needs of the Commonwealth.

	meet anticipated growth in utilization	
11.	SLA Reporting Collect actual system availability, utilization and response time data. Create a SLA report on a monthly basis, for the Commonwealth and Offeror.	Offeror must describe its approach to supporting the needs of the Commonwealth.
12.	The Offeror must provide Software License Management.	Offeror must describe solution and approach to meet this requirement.
13.	Coordinate at an agency level and account for any required patching as technology upgrades require.	Offeror must describe its approach to supporting the needs of the Commonwealth.
Continual Service Improvement		
14.	Reduce service risks. Methods to eliminate or mitigate service risks.	Offeror must describe its approach to supporting the needs of the Commonwealth
15.	Improve service quality. On a quarterly basis, make recommendations to the Commonwealth team any system changes that would be appropriate to maintain or improve SLA commitments.	Offeror must describe its approach to supporting the needs of the Commonwealth.
16.	Improve client satisfaction.	Offeror must provide examples of previous Offeror initiatives aimed at continually improving client satisfaction.
17.	Ensure service transparency. Methods and practice to ensure service transparency, providing visibility into service execution.	Offeror must describe its approach to supporting the needs of the Commonwealth.
18.	Improve/reduce cost of service.	Offeror must provide examples of Mainframe Support initiatives that have been implemented or can be utilized to achieve reduced costs of Services and to

		meet or exceeded ROI (Return on Investment) analysis projections.

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

3.2.4.6 Security & Firewall

The Security & Firewall service will provide hosting and operational support Services for security products and firewalls located at the datacenters. These security devices and Services protect the equipment and applications in the datacenters from malicious attempts to penetrate the computing environment with worms, phishing, Trojan horse malware, and unlawful data access. Offeror must install and maintain mainstream security hardware and software utilizing current industry best practices sufficient to protect the enterprise class datacenter environments with a significant volume of sensitive class data (e.g. HIPAA, CJIS, CHRIA, PCI, PII, etc.). The number of support staff members required to perform the tasks listed below will be determined by the Offeror.

Listed below are the basic Services required to manage the security & firewall systems required by the Commonwealth. Offeror must include these Services in addition to the base level of Services in this Offering.

Reference Documentation

Exhibit A - Commonwealth Network Environment

Exhibit J.1 through J.3 - Commonwealth Security and Compliance Requirement

Exhibit G.6 - PSP - CJIS Security Policy

Exhibit G.9 - PSP - CCHRI

Exhibit G.7 - PSP - Summary of CJIS Requirements

Exhibit G.12 - PSP - CHRIA Handbook

Requirements		Describe Compliance
1.	Monitor local security operations, troubleshoot and resolve operational issues.	Offeror must describe its approach to supporting the needs of the Commonwealth including the following:

	Actively (normal daily process) monitor the operations of all security, firewall systems and security zones. Maintain a log for each server/appliance/system and review the system logs on a daily basis to ensure key system Services are processing without errors. Provide the ability to import data to agency SIEM or enterprise SIEM tool for correlation and reporting purposes. Provide the ability for Commonwealth agencies to request security modifications (firewall changes) as documented in the CCPM. Document review of the system security logs on a weekly basis to ensure critical system Services are processing without errors. Complete weekly server log indicating which logs were reviewed, date and initial the log.	• Processes & Procedures • Tools / Applications • End User Reports o Standard o Custom • Tiered Service/Support Levels • Escalation Procedures Offeror must describe prior experience relative to providing datacenter management and support of CJIS, CCHRI, HIPAA and PCI compliant systems.
2.	Provide security training to Commonwealth personnel specific to the security Services being delivered. Provide the Commonwealth with a resume or CV for each operational staff member assigned to this engagement. Comply with agency background checks and clearances as defined in Appendix A - Terms and Conditions.	Offeror must describe its approach to supporting the needs of the Commonwealth. Offeror must submit a representative sample of staff resumes typically provided for these positions and describe the process to ensure compliance of background checks and clearances.
3.	Achieve cost effective 24/7 security operational coverage for this critical system. Provide dedicated security support staff onsite during scheduled business days, and automated log and notification	Offeror must describe its security operations coverage and how it will be applied.

	systems to alert security team of possible intrusion events in real time mode. Provide Level 2 and Level 3 Support to the Service Desk and/or Commonwealth Users. Security staff must be available to respond and evaluate the severity of the event 24/7/365.	
4.	Ensure network connectivity, and ensure consistent system response times. Utilize automated system management tool(s) to ensure real-time monitoring and notification of server availability and response times.	Offeror must describe its real-time monitoring approach and toolset to provide and maintain network availability and performance. Offeror must identify tools it uses to support network availability and performance.
5.	Ensure server/appliance operating systems are maintained with the current system patch level. Implement a Patch Management Program to ensure the timely application of security updates on all infrastructure platforms in accordance with Commonwealth IT policy guidelines. Ensure signature and threat analysis files are updated on a regular basis, and conform to industry best practices. Analyze monthly service patches and determine which patches need to be applied, by server type. Create a change record, log the update in the server log, and install based on server availability schedule. Notify the Commonwealth of any scheduled or unscheduled service interruptions.	Offeror must describe its approach to supporting the needs of the Commonwealth. Offeror must describe its approach for testing and validating updates to the OS and 3rd Party software that it supports. Offeror must describe its approach to communicating unscheduled and scheduled outages, including escalation process.

6.	Provide active security operations, corrective action, and reporting by utilizing Offeror software to monitor inbound and outbound traffic for malicious patterns and content, and take appropriate protective measures. The ability to utilize security management software to detect threats and analyze firewall logs, to proactively detect and protect from malicious events. Comply with agency specific security requirements. Comply with all agency and OA/OIT security policies and ITBs. On a quarterly schedule, run appropriate penetration testing, and report results to Commonwealth and Offeror. Create monthly report on events, incidents and corrective activities. Report that indicates systems not in compliance with security standards. Real time reporting of security breaches.	Offeror must describe its Security Operations Process and how it will be applied.
7.	SLA Reporting including but not limited to collecting actual system availability, utilization and response time data. Create a Service Level Agreement report for the Commonwealth and Offeror on a monthly basis.	Offeror must describe its approach to supporting the needs of the Commonwealth.
8.	Software License Management	Refer to 3rd Party Software Management service.

Continual Process Improvement		
9.	Reduce service risks.	Offer methods to eliminate or mitigate service risks.
10.	Improve service quality. Make recommendations to the Commonwealth team any system changes that would be appropriate to maintain or improve SLA commitments on a quarterly basis.	Offeror must describe its approach to supporting the needs of the Commonwealth.
11.	Improve client satisfaction.	Offeror must provide examples of previous Offeror initiatives aimed at continually improving client satisfaction.
12.	Ensure service transparency using documentation methods to ensure service transparency, by providing visibility into service execution.	Offeror must describe its approach to supporting the needs of the Commonwealth.
13.	Improve/reduce cost of service.	Offeror must provide examples of Security and Firewall Support initiatives that have been implemented or can be utilized to achieve reduced costs of Services and to meet or exceeded ROI (Return on Investment) analysis projections.
Deliverables		
Deliverables are defined in **Schedule K – Key Program Deliverables**		
Offeror Response		

3.2.4.7 Database Management Services

The Database Management Service will provide the Commonwealth with a "managed database" service offering. The service must include the database platform (Hardware/Software) and the ongoing database management administration Services. The Offeror must provide a multi-tiered level of service (e.g. Gold, Silver, and Bronze) across multiple database platforms. While the Commonwealth's application portfolio (over 2,000 applications) currently utilizes numerous database technologies, the majority of the applications that are utilizing database technologies are using Oracle, Microsoft SQL, IMS, Sybase, or DB2.

It is anticipated the Database Management Services will be an optional service that can be utilized by the Agencies beyond the basic infrastructure Services.

Reference Documentation

N/A

Requirements		Describe Compliance
1.	Design, manage, and administer database environments that support multiple business applications.	Offeror must describe proposed approach to designing and supporting enterprise level database platforms and Services that support multiple agency business applications.
2.	Provide Level 2 and Level 3 Support to the Service Desk and/or Commonwealth Users.	Offeror must describe its approach to supporting the needs of the Commonwealth including the following: • Processes & Procedures • Tiered Service/Support Levels • Tools / Applications • Escalation Procedures • End User Reports o Standard o Custom
3.	Monitor database backup and recovery processing on a daily basis. Review daily backup log for successful completion. Note any failures, initial and date the log, and correct the problem. Create problem	Offeror must describe its approach to perform an initial review and audit of the backup and recovery policies, procedures and reports, to ensure the accuracy of the backup schedules, retention periods, target directories, and recovery point objectives. Offeror must describe its approach to

	record for any abnormal condition and any repairs that have been made. Automated software process will be utilized to report the completion status of backup processing, with electronic notification of failures sent to Offeror technical support and identified Commonwealth staff for follow up and corrective action.	identifying gaps and potential risks, and how those gaps and risks will be resolved.
4.	Provide a multi-tiered level of service (e.g. Platinum, Gold, Silver, Bronze, and Basic) for Oracle, Sybase, Microsoft SQL, IMS or DB2 database platforms. Provide Level 2 and Level 3 Support to the Service Desk and/or Commonwealth Users.	Offeror must describe its approach to providing multi-tiered Services level.
5.	Utilize the proposed service management Services (e.g. Incident, Service Request, Change, Configuration) to manage database management Services with multiple agency customers.	Offeror must describe how its proposed database management Services will support multiple agency service requests.
6.	Provide a review and analysis of system performance/capacity to determine if current performance/capacities are sufficient to support the needs of the stakeholders.	Offeror must perform an initial review and audit of the current usage, procedures and reports and provide an analysis of the current usage, processes and reports currently being supported. Offeror must document its review and audit findings and recommendations.
7.	Monitor system backup processing on a daily basis. Review daily backup log for successful completion. Note failures, and correct the problem. Create problem record for any abnormal condition and any repairs that have	Offeror must describe it approach to performing an initial review and audit of the backup policies, procedures and reports, to ensure the accuracy of the backup schedules, retention periods, target directories, and recovery point objectives. Offeror must describe its approach to identifying gaps and potential risks, and how

	been made. An automated software process will be utilized to report the completion status of backup processing, with electronic notification of failures sent to Offeror technical support, and identified Commonwealth staff for follow up and corrective action.	those gaps and risks will be resolved.
Continual Process Improvement		
8.	Reduce service risks.	Offeror must provide methods to eliminate or mitigate service risks.
9.	Improve service quality.	On a quarterly basis, Offeror must also recommend to the Commonwealth team any system changes that would be appropriate to maintain or improve SLA commitments.
10.	Improve client satisfaction.	Offeror must provide examples of previous Offeror initiatives aimed at continually improving client satisfaction.
11.	Ensure service transparency.	Offeror must provide methods and practices to ensure service transparency, providing visibility into service execution.
12.	Improve/reduce cost of service.	Offeror must provide examples of Database Management Support initiatives that have been implemented or can be utilized to achieve reduced costs of Services and to meet or exceeded ROI (Return on Investment) analysis projections.
Deliverables		
Deliverables are defined in **Schedule K – Key Program Deliverables**		
Offeror Response		

3.2.4.8 Limited-Use Colocation Services

While the Commonwealth's goal is to move to a fully managed infrastructure Services model, it is anticipated that there will be a need for the Offeror to provide some limited co-location Services within its proposed datacenter Services solution. Some examples of where colocation Services may be required are:

- Support for existing systems in the EDC prior to transformation to a fully managed service.
- 3rd Party Vendor Equipment that requires co-location with the primary systems for performance and/or security reasons.

The Offeror must provide datacenter co-location Services with the following options:

- Co-location Service Option 1: Datacenter Only (Rackspace, power, network connectivity, basic infrastructure Services)
- Co-location Service Option 2: Datacenter with Managed Services Option (Bronze, Silver, Gold Tiers) – Technology owned maintained by 3rd Party or Commonwealth
- Co-location Service Option 3: Remote Hands Support

Currently there are 3 areas within the Commonwealth EDC that are supporting co-location Services. EDC facility summary is provided as **Exhibit D.7**. While many of these systems will be migrated to a fully managed service over time, the Offeror shall plan for co-location space in its Datacenter Architecture.

Reference Documentation

Exhibit D.1 through D.15 Series - Enterprise Datacenter (EDC) Exhibits

Requirements		Describe Compliance
1.	Provide colocation Services within each of the datacenters. One of those centers will be the Commonwealth EDC.	Offeror must describe how each of the datacenters will support its co-location offering within its proposed datacenter architecture.
2.	Provide Colocation Service Option 1: Datacenter Only (Rackspace, power, network connectivity, basic infrastructure Services)	Offeror must describe how it will support this colocation service option.

3.□	Provide Co-location Service Option 2: Datacenter with Managed Services Option (Bronze, Silver, Gold Tiers) – Technology owned maintained by 3rd Party or Commonwealth	Offeror must describe how it will support this co-location service option.
4.□	Provide Co-location Service Option 3: Remote Hands Support	Offeror must describe how it will support this co-location service option.
Continual Process Improvement		
5.□	Reduce service risks.	Offeror must provide methods to eliminate or mitigate service risks.
6.□	Improve service quality.	On a quarterly basis, Offeror must also recommend to the Commonwealth team any system changes that would be appropriate to maintain or improve SLA commitments.
7.□	Improve client satisfaction.	Offeror must provide examples of previous Offeror initiatives aimed at continually improving client satisfaction.
8.□	Ensure service transparency.	Offeror must provide methods and practices to ensure service transparency, providing visibility into service execution.
Deliverables		
Deliverables are defined in **Schedule K – Key Program Deliverables**		
Offeror Response		

3.2.5 Capacity on Demand Services

3.2.5.1 Server Capacity on Demand

The Server Capacity On Demand is an Infrastructure as a Service (IaaS) offering that ensures the ready availability of server and mainframe capacity to accommodate cyclical, and seasonal, processing requirements, sudden or unplanned production demands, and short-term application development needs. Server capacity may be physical or virtual as requested by the Commonwealth.

The Server Capacity On Demand would include support for the following system platforms:

- X86
  - Windows
  - Linux
- I Series
  - i5/OS
- P Series
  - Linux
  - AIX
- Mainframe
  - IBM
  - Unisys

Reference Documentation

N/A

	Requirements	Describe Compliance
1.	Provide a provisioning capability to support on-demand requests for server resource capacity. The Commonwealth will require access to additional capacity on demand for the following platforms: X86 • Windows • Linux IBM I Series • i5/OS IBM P Series	Offeror must describe its request and provisioning process for each of the anticipated platform systems. Offeror must describe its approach to supporting the needs of the Commonwealth including the following: • Infrastructure/Capacity • Tiered Service/Support Levels • Tools / Applications to manage and maintain capacity • End User Reports

	• Linux • AIX Mainframe • IBM • Unisys	o Standard o Custom Offeror must describe its experience operating and managing mixed computing environments such as the Commonwealth.
2.	Maintain an adequate inventory of Windows/Linux, mid-range, and Mainframe server capacity that will be sufficient to satisfy forecasted informal, ad hoc, and cyclical Commonwealth requests.	Offeror must describe its approach to supporting the needs of the Commonwealth.
3.	As a function of ongoing account management, meet with the Commonwealth/Agencies to assess future server requirements.	Offeror must describe its approach to supporting the needs of the Commonwealth.
4.	Encourage Commonwealth server conservation via server virtualization when appropriate.	Offeror must describe its approach to supporting the needs of the Commonwealth.
5.	Provide expedited service, when requested, to satisfy urgent requirements.	Offeror must describe its approach to supporting the needs of the Commonwealth.
6.	Provide a self-provisioning tool to be used by the agencies to order and configure servers.	Offeror must describe its approach to supporting the needs of the Commonwealth.
Continual Process Improvement		
7.	Reduce service risks.	Offeror must describe its approach and provide examples of previous Offeror initiatives aimed at eliminating or mitigating service risks.
8.	Improve service quality.	Offeror must describe its approach and provide examples of previous Offeror initiatives aimed at improving service quality.

9.	Improve client satisfaction.	Offeror must provide examples of previous Offeror initiatives aimed at continually improving client satisfaction.
10.	Provide service transparency.	Offeror must describe its approach and provide examples of previous Offeror initiatives aimed at providing service transparency; in particular, visibility into the service execution process.
11.	Ensure service sustainability.	Offeror must describe its approach and provide examples of previous Offeror initiatives aimed at ensuring service sustainability; in particular, efforts targeted at cost containment and cost reductions.
12.	Improve/reduce cost of service.	Offeror must provide examples of On-Demand Server initiatives that have been implemented or can be utilized to achieve reduced costs of Services and to meet or exceeded ROI (Return on Investment) analysis projections.
Deliverables		
Deliverables are defined in **Schedule K – Key Program Deliverables**		
Offeror Response		

3.2.5.2 Storage Capacity on Demand

The Storage Capacity On Demand service is an Infrastructure as a Service (IaaS) offering that ensures the ready availability of storage capacity to accommodate cyclical, or seasonal, storage requirements, sudden or unplanned production demands, short-term application development needs, and storage access for web enabled devices.

Reference Documentation

N/A

Requirements		Describe Compliance
1.	Maintain an adequate access to, or supply of storage area equipment, to satisfy forecasted informal, ad hoc, and cyclical Commonwealth requests.	Offeror must describe its approach to supporting the needs of the Commonwealth including the following: • Infrastructure/Capacity • Tiered Service/Support Levels • Tools / Applications to manage and maintain capacity • End User Reports o Standard o Custom
2.	Meet with the Commonwealth on a annual basis, or as requested, to assess future storage requirements.	Offeror must describe its approach to supporting the needs of the Commonwealth.
3.	Encourage data storage conservation via data de-duplication, compression, and other industry techniques.	Offeror must describe its approach to supporting the needs of the Commonwealth.
4.	Provide expedited data storage service to satisfy urgent requirements, as requested.	Offeror must describe its approach to supporting the needs of the Commonwealth.
5.	Provide online storage capabilities (Centralized Private Cloud Storage), which includes web service, browser, and mobile device accessibility, that are fully secure, (compliant with ISO 27000, NIST 800-53, and Secure	Offeror must describe its approach to supporting the needs of the Commonwealth.

	SDLC). This service must provide file-level encryption, multiple hierarchical permission levels, account level dynamic storage-sizing, and anti-virus capability.	
6.	Storage solution must include the capability to make quick copies of databases (SNAPS, Flash copies). Storage backup proposals must include disk-2-disk solutions.	Offeror must describe its approach to supporting the needs of the Commonwealth.
Continual Service Improvement		
7.	Reduce service risks.	Offeror must describe its approach and provide examples of previous Offeror initiatives aimed at eliminating or mitigating service risks.
8.	Improve service quality.	Offeror must describe its approach and provide examples of previous Offeror initiatives aimed at improving service quality.
9.	Improve client satisfaction.	Offeror must provide examples of previous Offeror initiatives aimed at continually improving client satisfaction.
10.	Provide service transparency.	Offeror must describe its approach and provide examples of previous Offeror initiatives aimed at providing service transparency; in particular, visibility into the service execution process.
11.	Ensure service sustainability.	Offeror must describe its approach and provide examples of previous Offeror initiatives aimed at ensuring service sustainability; in particular, efforts targeted at cost containment and cost reductions.
12.	Improve/reduce cost of service.	Offeror must provide examples of On-Demand Storage initiatives that have been implemented or can be utilized to achieve

		reduced costs of Services and to meet or exceeded ROI (Return on Investment) analysis projections.

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

3.2.5.3 DR Infrastructure on Demand

The DR Infrastructure On Demand service is an infrastructure as a service (IaaS) offering that ensures the ready availability of DR infrastructure; servers, storage systems, networking capabilities, etc. This infrastructure will enable Commonwealth datacenters to recover critical business applications and data in the event of a disaster.

Reference Documentation

N/A

	Requirements	Describe Compliance
1.	Maintain an adequate inventory of servers, storage systems, and networking capacity sufficient to satisfy forecasted informal, ad hoc, and cyclical Commonwealth requests.	Offeror must describe its approach to supporting the needs of the Commonwealth including the following: • Processes and procedures for developing and testing DR Plans • Capacity (servers, storage, etc.) • Tiered Service/Support Levels • Tools / Applications to manage and maintain capacity • End User Reports

		o Standard o Custom
2.	Meet with the Commonwealth on a annual basis and as requested to assess its future DR requirements.	Offeror must describe its approach to supporting the needs of the Commonwealth.
3.	Revise datacenter and disaster recovery plans, upon request of the Commonwealth.	Offeror must describe its approach to supporting the needs of the Commonwealth.
4.	Provide support for the Commonwealth with identifying and establishing DR or Continuity of Government (CoG) capabilities and plans.	Offeror must describe its approach to supporting the needs of the Commonwealth.
Continual Process Improvement		
5.	Reduce service risks.	Offeror must describe its process and provide examples of previous Offeror initiatives aimed at eliminating or mitigating service risks.
6.	Improve service quality.	Offeror must describe its process and provide examples of previous Offeror initiatives aimed at improving service quality.
7.	Improve client satisfaction.	Offeror must provide examples of previous Offeror initiatives aimed at continually improving client satisfaction.
8.	Provide service transparency, in particular, visibility into the service execution process.	Offeror must describe its process and provide examples of previous Offeror initiatives aimed at providing service transparency.
9.	Ensure service sustainability, in particular, efforts targeted at cost containment and cost reductions.	Offeror must describe its process and provide examples of previous Offeror initiatives aimed at ensuring service sustainability.

10.	Improve/reduce cost of service.	Offeror must provide examples of On-Demand Infrastructure initiatives that have been implemented or can be utilized to achieve reduced costs of Services and to meet or exceeded ROI (Return on Investment) analysis projections.

Deliverables

Deliverables are defined in **Schedule K – Key Program Deliverables**

Offeror Response

3.2.5.4 Additional Technical Services

The Commonwealth may require additional technical support beyond the standard service level based infrastructure Services. The availability and access to skilled resources would complement the standard hosting offerings. The Offeror is expected to provide these additional resources for both short and longer-term engagements.

Reference Documentation

N/A

	Requirements	Describe Compliance
1.	Provide access to skilled technology resources. Additional technology support Services categories include but are not limited to: • Infrastructure (mainframe, mid-range and x86) Architects/Engineers • Performance Specialists • Database Architects • Database Analysts • Security Architects	Offeror must describe its ability to support both short and long-term assignments for a variety of technology skill sets. Offeror must provide representative resumes within each skill category. Offeror must provide a rate card for each resource category in the Cost Matrix.

	• Security Analysts • Unix (AIX, Linux) Administrators • Windows Server Administrators • Mainframe Systems Programmers • Batch Administrators • Microsoft Product Specialists (e.g. Exchange, SharePoint) • 3rd Party Software Product Specialists • Basis and SAP Oracle support	
Deliverables		
Deliverables are defined in **Schedule K – Key Program Deliverables**		
Offeror Response		

3.3 Transition Services

3.3.1 Transition Services – Guiding Principals

At present, the Commonwealth's information technology Services are hosted at a variety of Commonwealth datacenters, including:

- Shared enterprise facilities - (EDC and DPH) and;
- Agency facilities, for example those managed and maintained by DPW, DOR, DOH, PSP and DLI.

The Commonwealth datacenter locations are identified in Exhibit S - Datacenter locations.

In an effort to reduce datacenter costs, simplify datacenter administration, and provide more robust and reliable information Services to the Commonwealth, the Commonwealth datacenter modernization initiative calls for the phased migration or transition of Commonwealth information Services to the newly-established Offeror managed multi datacenter environment.

The Guiding Principles associated with the transition to the new datacenter environment are:

- Transition approach must meet the milestone objectives as described in **Schedule D**.
  - Based on the Commonwealth's number of licenses, additional licenses may be needed for the transition of Services. The Offeror shall be responsible for any additional licenses needed for the transition of service.
  - The Commonwealth, at its sole discretion, may procure the software licenses through existing statewide contract.
- Initial transition approach of the Commonwealth's mainframe and SAP environments requires that the results be as close to the Commonwealth's current configuration as technically possible.
  - Any deviations from current environments must be approved by the Commonwealth.
- Customized approach developed to meet the needs of the Commonwealth
  - The selected Offeror's transition approach shall account for Commonwealth specific needs such as the Transition Considerations and Critical Configuration Considerations as described in Exhibits R and T.
  - The selected Offeror shall implement a discovery process during transition planning to acquire information required to develop a Detailed Transition Plan.
  - The selected Offeror shall include application level transformation models. Transformation models must take into account the initial transition approach that the Commonwealth's mainframe and SAP environments must be as close to the Commonwealth's current configuration as possible.

- Transformation project managers experienced in projects of similar size and complexity.
- Strong governance model, which includes:
  - Clearly defined roles and responsibilities
  - Jointly developed processes
  - Effective meetings and reporting framework to minimize resource requirements while achieving goals
  - Mechanisms in place to identify and address risks and issues
  - Compliance with applicable policies, standards, processes, and procedures
- Effective communication, which includes:
  - Consistent delivery of key messages through well-defined communication plans
  - Tailored communications to target audiences and stakeholders
  - Communications to meet the needs of the Commonwealth.
- Collaboration and teamwork, which includes:
  - Detailed upfront project planning and feedback
  - Agreement on status for reporting purposes
  - Plans scaled to address Commonwealth agency differences in size and complexity
  - Establishment and support for successful deliverable review process
  - Feedback on deliverables throughout the life of the project.

3.3.2 Transition Planning/Governance

The Offeror's Transition Program Management Office (TPMO) will contain a dedicated consolidation specific program team. The team will be responsible to jump-start the consolidation program by bringing respective stakeholders together for a series of transition workshops. The transition workshops will work to align the stakeholders, and produce the following deliverables:

- Overall transition approach and strategy for Server and Mainframe consolidation
- Transition and consolidation governance plan
- Transition risk assessment plan
- Consolidation cost/benefit analysis
- Consolidation stakeholder transition agreements
- Consolidation transition planning guidelines

The TPMO will provide program management Services to deliver architecture, transition plan integration, and organizational change management, as well as quality assurance, verification of testing, financial oversight, and operational readiness for the Mainframe and Server transition/consolidation program. The TPMO will exist under the overall Offeror's PMO office and will include a combination of resources dedicated to the effort full time, plus resources that participate in the program on an as needed basis. The program plan and architecture will be developed by the Offeror and approved by the Commonwealth. The Offeror must ensure processes and tools are implemented to support Transition change control, schedule, quality, communications, risk and issues management.

Proposed Transition Plan

The Commonwealth anticipates the following high-level sequence of transition activities. The Offeror must develop an initial transition plan and present with its proposal. At minimum, the Offeror's proposed Transition Plan must reference these activities and project timeframes.

Transition Activities

The high level transition milestones and deliverables are described in **Schedule D - Transition Milestones** and **Schedule K - Key Program Deliverables**.

Target Datacenter Transitions

The following table includes the target datacenter facilities that are to be initially transitioned by the Offeror. The target datacenter facilities are defined as the physical Commonwealth facilities that are selected to be transitioned to the Offeror's control and/or facilities. The Offeror must coordinate with each Commonwealth agency or datacenter representative to create a *Facility Specific Transition Plan* for each targeted facility. The Offeror must include target datacenter transitions in its proposed Transition Timeline to be included in its proposal. The Offeror must include a "pilot" transition approach to ensure successful transitions of Commonwealth applications and infrastructure. This approach will demonstrate to the agencies that Offeror's approach will be successful before moving forward with additional transition phases.

Offeror must establish a high-speed direct link (not via COPANet) with the current DPH location to enable "systems" connectivity that would facilitate the ability to effect smoother transition of data.

The selected Offeror shall not charge the Commonwealth for completion of a Transition Milestone. All transition costs must be included in the selected Offeror's unit prices for the Services.

	Target Datacenter Facilities		Transition Requirement Notes
	Group1 Transitions		
1	**DPH** (All Agency Mainframe – Unisys/IBM; IES SAP, and all other Agency hosted environments)		• The DPH operation and all of its supported agency application workloads must be successfully migrated out of the current facility to the Offeror's Datacenter. • Operations support will be assumed by the Offeror once the workloads are successfully moved to the new provider's datacenter environment. • Key Transition Milestone(s): o Refer to **Schedule D - Transition Milestones**
1	**EDC**		• Offeror must assume operations support of the EDC datacenter • Key Transition Milestone(s): o Refer to **Schedule D - Transition Milestones**
Group 2 Transition			
2	**DLI**		• The DLI datacenter operations and all of its supported application workloads must be successfully migrated out of the DLI facility to the Offeror's Datacenter. • Key Transition Milestone(s): o Refer to **Schedule D - Transition Milestones**
Group 3 Transitions			
3	**DPW** – Rm. 105, 106 (Lower Environments, PACSES)		• The DPW Rooms 105, 106 datacenter operation and all supported application workloads must be successfully migrated out of the current DPW facility to the Offeror's Datacenter architecture. • Key Transition Milestone(s): Refer to **Schedule D - Transition Milestones**
3	**DOR**		• The DOR datacenter operation and all of its supported application workloads must be successfully migrated out of the current DOR facility to the Offeror's Datacenter architecture.

	Target Datacenter Facilities		Transition Requirement Notes
			• Key Transition Milestone(s): o Refer to **Schedule D - Transition Milestones**
3	**DOH**		• The DOH datacenter operation and all of its supported application workloads must be successfully migrated out of the current DOH facility to the Offeror's Datacenter architecture. • Key Transition Milestone(s): o Refer to **Schedule D - Transition Milestones**
3	**PSP**		• The PSP datacenter operation (Headquarters) and all of its supported application workloads must be successfully migrated out of the current PSP facilities to the Offeror's Datacenter architecture. • Key Transition Milestone(s): o Refer to **Schedule D - Transition Milestones**

3.3.2.1 Transition Program Management

The TPMO function ensures the non-disruptive migration of Commonwealth information Services from current Commonwealth host locations, to the Offeror provided multi datacenter environments.

The Offeror must establish a TPMO and develop the requisite transition plans.

A transition approach and detailed transition plan for each of the Commonwealth's existing Datacenters must be developed by the Offeror and approved by the Commonwealth. The Commonwealth has over 2,000 business applications with over 50% designated mission critical. The Offeror must work with each agency to determine its application environment within each facility. The Offeror's target datacenter environment must be configured and tested prior to migration of the application.

Reference Documentation

Schedule D - Transition Milestones

Exhibit D.7 - EDC - Facility Summary

Exhibit A - Commonwealth Network Environment

Exhibit(s) B.1 through B.6 - Data PowerHouse (DPH) Exhibits

Exhibit(s) C.1 through C.13 - Department of Public Welfare (DPW) Exhibits

Exhibit(s) D.1 through D.15 - Enterprise Datacenter (EDC) Exhibits

Exhibit(s) E.1 through E.43 - Department of Labor & Industry (DLI) Exhibits

Exhibit(s) F.1 through F.4 - Department of Health (DOH) Exhibits

Exhibit(s) G.1 through G.16 - PA State Police (PSP) Exhibits

Exhibit(s) H.1 through H.8 - Department of Revenue (DOR) Exhibits

Exhibit(s) I.1 through I.13 - Commonwealth SAP Environment - Integrated Enterprise Services (IES) Exhibits

Exhibit L - Commonwealth Master Application Inventory

Exhibit(s) M.1 through M.7 Department of Corrections (DOC) and Pennsylvania Board of Probation and Parole (PBPP) Exhibits

Exhibit(s) N.1 through N.2 - PennDOT Exhibits

Requirements		Describe Compliance
1.	Establish a TPMO to manage all information service transition	Offeror must describe the proposed TPMO, and discuss the mission, goals and objectives, and the roles and responsibilities of the

	activities. The Office will be jointly administered by Offeror and Commonwealth staff. Provide a communication plan that will provide an information vehicle for all interested parties.	Offeror. Offeror must provide at least one sample where Offeror has successfully created an office similar to the required TPMO.
2.	Provide a functional organization chart for the TPMO, including an estimate of the type and number of full time Offeror resources that will be required to ensure the successful transition of Services from current multiple datacenters to the Offeror's datacenter Services.	Offeror must describe the TPMO structure including but not limited to the number of full time resources and the role of the TPMO in the transition.
3.	Analyze applications and design the required computing architecture to migrate Commonwealth datacenters to Offeror datacenter environments. Hardware, software, network, etc. Work with Commonwealth technical staff to ascertain the requirements to successfully migrate processing to Offeror datacenter environments	Offeror must describe solution and approach to meet this requirement. Offeror must provide at least one relevant example from a prior engagement, in which it was engaged, that is similar to the needs of the Commonwealth.
4.	Optimize Current Process and Procedures – Coordinate with Commonwealth agencies to review and plan for a transition of processes and procedures.	Offeror must describe its overall plan for optimization of the existing processes, procedures, tools, etc. to provide more efficient and effective Services. The description must include approach, plan, and methodologies.
5.	Revise datacenter DR plans on the occasion of major changes to the datacenter hardware, software, or network portfolio to reflect those major changes.	Offeror must describe solution and approach to meet this requirement.
6.	Establish an IT infrastructure that	Offeror must describe solution and approach

	meets all application processing requirements. The Offeror must confirm that the target IT infrastructure meets or exceeds current computing requirements. Work with Commonwealth technical staff to design and build the infrastructure required to support the applications being migrated to the Offeror multi datacenter environment.	to meet this requirement. Offeror must provide at least one relevant example from a prior engagement, in which it was engaged, that is similar to the needs of the Commonwealth.
7.	A multi-faceted Transition Strategy will be required: • Comprehensive; • Non-disruptive; and • Compliant with Commonwealth requirements. The Strategy will address the transition of: • Shared infrastructure elements, as appropriate; and • Specific information Services. • Disparate Agency application architectures and impacts to move to the new environment(s) The Strategy must also address the following: • Cost/Benefit for the Agency • Risks and Risk Mitigation Plan The migration order of the Commonwealth datacenters will be provided by the Commonwealth.	Offeror must describe the transition (interim and steady state strategies) and transition plans that it has employed during other similar size engagements.
8.	Identify mandatory requirements and critical success factors that will have a direct impact on developing a	Offeror must describe the 3-5 characteristics, conditions, or variables it believes will have a direct and critical impact on the effectiveness, efficiency, and viability of the

	successful transition plan	Offeror's solution. Offeror must describe its approach to mitigating risks and ensuring these critical factors are successfully addressed.
9.	Create a Transition Timeline that outlines the overall timeline starting at effective date and continues through delivering transition Services for each of the targeted datacenters.	Offeror must describe the overall timeline from the start of pre-Transition activities through the point at which the Offeror expects it will be delivering predictable, repeatable Managed Service Results that meet the requirements of the RFP. The schedule must include a description of the critical milestones related to Transition efforts for each targeted Commonwealth datacenter. Any critical milestones identified must be included in the Transition Project Plan.
10.	Create a generic Infrastructure Element Transition Plan that may be readily adapted to accommodate specific infrastructure element transitions. Create a prospective Infrastructure Element Transition Plan. Appropriate EDC, DPH and other Agency Datacenter hardware elements may be re-purposed wherever possible.	Offeror must describe a realistic Transition Project Plan to transition the Commonwealth's datacenters to the proposed architecture.
11.	The EDC Managed Services datacenter assets must be managed and maintained by the Offeror until they are transitioned to the Offeror's managed Services. The current maintenance contract for the EDC servers is scheduled to expire on June 30, 2014.	Offeror must describe its transition approach to address the transition of operations and management of the EDC infrastructure from the Commonwealth to the Offeror's support Services and how it intends to address the server maintenance expiration issue.
12.	Create, manage and execute an application / infrastructure migration	Offeror must describe solution and approach to meet this requirement. Offeror must

	plan. The Offeror has the primary responsibility for planning and executing the transition of infrastructure elements, with support of Commonwealth technical and business support staff. The Offeror must provide adequate tools and techniques for moving and migrating Commonwealth data to the new target storage environment. The Offeror must ensure that critical applications are not decoupled from key infrastructure components causing system latency.	provide at least one sample where it has successfully migrated application and hardware. Offeror must describe its proposed tools and techniques for moving and migrating Commonwealth data to the new target storage environment.
13.	Create a generic Information Service Transition Plan that may be readily adapted to accommodate specific information service transitions.	Offeror must outline a prospective Information Service Transition Plan to take over support of migrated Commonwealth systems and applications. Offeror must provide at least one sample where it has successfully completed application and hardware migrated.
14.	Meet with Commonwealth to produce and execute specific Information Service Transition Plans. Select cut over windows that minimize system unavailability and coordinate approval with the affected agency. Communicate to the Commonwealth cut over date and times. Setup a special call number and support staff to take calls concerning the migration, these Services must be made available to transitioned users until the transition is officially signed off as completed. .	Offeror must describe solution and approach to meet this requirement. Offeror must provide at least one relevant example from a prior engagement, in which it was engaged, that is similar to the needs of the Commonwealth.
15.	Work with Commonwealth to create testing, business acceptance and	Offeror must describe solution and approach to meet this requirement. Offeror must provide at least one relevant example from a

	fallback plans.	prior engagement, in which it was engaged, that is similar to the needs of the Commonwealth.
16.	Service Management Systems – Offeror must transition all agency system management platforms currently in place to the Offeror, consolidating all system management responsibilities. The Offeror must make available all system management platforms and tools that are currently supporting the Commonwealth infrastructure.	Offeror must describe solution and approach to meet this requirement.
17.	CMDB – Work with the Commonwealth to acquire asset information to support the asset management system and configuration management system.	Offeror must describe its approach to capturing, validating and storing all configuration information required to perform the Services within 120 days of the Effective Date of the Contract. In particular, the Offeror must address how it will identify and relate critical associations (e.g. Application to Server, Server Tier to Application, Application to Disaster Recovery Time Objective, software to server, etc.) for the enterprise. Offeror must describe its approach to transitioning the data and related processes from the existing CMDB or equivalent system/database to the Offeror's solution and how the Offeror must ensure accuracy of data across Service Management areas to ensure accurate and timely invoicing and chargeback to the Commonwealth.
18.	Chargeback – Work with the Commonwealth to interface with the Commonwealth's billing processing and validation ITSM system to provide a chargeback system for new and	Offeror must describe its transition approach to Chargeback Management. Offeror must describe its approach to assisting the Commonwealth in transitioning Commonwealth customers from the existing Chargeback system. The description must

	existing Services available on the Offeror's Service Catalog.	include an expected analysis of the current billing system environment, expected termination assistance, communications plans, strategy for testing and major milestones.
19.	Identify Options and Costs – List the appropriate different options that will satisfy the requirements of the transition scope. Communicate options with the Commonwealth and obtain approval on selected option(s) to proceed.	Offeror must describe proposed approach.
20.	Expand/reconfigure datacenter facilities to accommodate growth in Commonwealth information and information systems.	Offeror must discuss its approach; the expansion/reconfiguration plans must include the EDC.
21.	Produce weekly reports on the progress of the information service transition initiatives.	Offeror must describe its proposed approach to providing weekly transition progress reports.
Deliverables		
Deliverables are defined in **Schedule K – Key Program Deliverables**		
Offeror Response		

3.3.2.2 Security Transition Activities

To maintain continuity of Services, Offeror must provide training to Offeror's employees and subcontractors on security policies during initial phase of the Transition.

Reference Documentation

Schedule D - Transition Milestones

Exhibit D.7 - EDC Facility Summary

Exhibit A - Commonwealth Network Environment

Exhibit(s) B.1 through B.6 - Data PowerHouse (DPH) Exhibits

Exhibit(s) C.1 through C.13 - Department of Public Welfare (DPW) Exhibits

Exhibit(s) D.1 through D.15 - Enterprise Datacenter (EDC) Exhibits

Exhibit(s) E.1 through E.43 - Department of Labor & Industry (DLI) Exhibits

Exhibit(s) F.1 through F.4 - Department of Health (DOH) Exhibits

Exhibit(s) G.1 through G.16 - PA State Police (PSP) Exhibits

Exhibit(s) H.1 through H.8 - Department of Revenue (DOR) Exhibits

Exhibit(s) I.1 through I.13 - Commonwealth SAP Environment - Integrated Enterprise Services (IES) Exhibits

Exhibit L - Commonwealth Master Application Inventory

Exhibit(s) M.1 through M.7 Department of Corrections (DOC) and Pennsylvania Board of Probation and Parole (PBPP) Exhibits

Exhibit(s) N.1 through N.2 - PennDOT Exhibits

	Requirements	Describe Compliance
1.	Baseline Security Risk and Vulnerability Assessment Conduct a security risk assessment, which includes a penetration test on the In-Scope systems, an architecture review, and a vulnerability assessment. This assessment must result in a report with recommendations for meeting the Commonwealth's baseline security standard.	Offeror must describe its proposed approach to conducting a security risk assessment including penetration test, which must result in a report with recommendations.

2.	Security Training The Offeror's security team will meet with the Commonwealth's Security teams (OA & Agency) to participate in creating a comprehensive Security Program strategy. The Offeror and the Commonwealth Security teams will develop security awareness training content consisting of the Offeror's Security Plan documentation, Commonwealth OA and agency security policy guidelines. Security training will be mandatory for employees, contractors and subcontractors assigned to work on the Commonwealth's Datacenter project. Appropriate levels of training will be designated and tracked for compliance based on the specific area the employee will be working in. Both an individual's current training status and overall attainment of group training goals must be tracked and reported in the security clearance database. These levels will range from general security awareness that all employees will participate in to task-specific security and governance requirements targeted at operations, specialist, Commonwealth agency specific regulations, or working rules needed for compliance with Commonwealth or federal mandates unique to certain Commonwealth agencies and programs. This training will be delivered both during the new hire process, and on a regular schedule to be determined during Transition as new updates become necessary.	Offeror must describe its proposed approach to developing and implement a comprehensive Security Program.

3.	Initial Security Plan During the initial phase of the Transition the Offeror's security team will work with the Commonwealth's Security Team to create a Security Plan. Begin work on draft policy and procedure documents collectively known as the Security Plan during the start of the Transition Risk and Vulnerability Assessment, which will be completed one (1) month prior to Transition activities. Use best practice security standards (as outlined in the Requirements section of the RFP) along with past engagement experience to provide an outline that will address but will not be limited to the following: security strategy and technology roadmaps, security operations procedures, standard hardware and software security configurations, physical security policies and procedures, security incident management, private and protected data use standards, and audit procedures and reporting standards. This set of documents will be used as the foundation of the Offeror's master security plan for Datacenter operations which will be reviewed and updated on an annual basis.	Offeror must describe its proposed approach to performing the following: • Create a comprehensive Security Plan • Complete a Vulnerability Assessment (at the Offeror expense) • Document the agreed upon security strategy and roadmap • Document security procedures and standards • Document the security incident Management approach including o Standards o Processes o Reporting o Escalation
4.	On-boarding and off-boarding Conduct required background checks for its employees working on the Commonwealth Datacenter project. Where appropriate, use identity management tools to manage access to the systems requiring access by its	Offeror must describe its proposed approach to conducting required background checks for Offeror staff.

	employees. For systems where the Offeror is unable to use its identity management system, assign staff to manage the access. Train Offeror employees on his or her responsibilities within the contract. For logical and physical access to Commonwealth Co-location facilities and environments not managed by the Offeror, the Commonwealth's security access request process will be followed. For off-boarding, update security clearance database with the status of Offeror employee and concurrently update its identity management tool to ensure the access is revoked. Provide a monthly report describing personnel actions including but not limited to; new hires, terminations, any change in employee status/duties, etc.,	
5.	Complete DR Transition Activities Conduct knowledge transfer during the initial phase of the Transition, including review of Commonwealth DR plans and review of Third Party DR contracts. The Offeror must also update the DR plan contact information and any changes made in the first six (6) months of Transition.	Offeror must describe proposed approach to support the Tiered DR Services.
Deliverables		
Deliverables are defined in **Schedule K – Key Program Deliverables**		
Offeror Response		

Request for Proposal

RFP # 6100022698

Commonwealth of Pennsylvania

Office of Administration

Office for Information Technology

Data Center Computing Services

Schedule G

Staffing Plan and Key Positions

Table of Contents

PROJECT ORGANIZATION PLAN **3**
1. PROJECT ORGANIZATION CHART **3**
2. OFFEROR KEY PERSONNEL **3**
3. OFFEROR KEY PERSONNEL INSTRUCTIONS **5**
4. OFFEROR KEY PERSONNEL TABLE **6**
5. SUB-CONTRACTORS (IF APPLICABLE) INSTRUCTIONS **8**
6. SUB-CONTRACTOR KEY STAFF **9**
7. STAFF CONTINGENCY PLAN **11**
8. STAFF MANAGEMENT **11**
9. TRAINING POLICIES AND PROCEDURES **11**
10. STAFF RETENTION **11**

Project Organization Plan

Instructions: The Offeror must describe the integrated staffing organizational plan required to execute the proposed datacenter computing (architecture, build, transition and maintain) approach. This section includes details regarding the Offeror's team, proposed use of subcontractors, and the Offeror's expectations of Commonwealth resources.

The Offeror must provide a staffing plan detailing the number of personnel, level, role and responsibilities. The staffing plan must also detail the team reporting relationships and identify the approach to integration and communication between Offeror, Commonwealth, and Commonwealth designee. This plan must show proposed Offeror personnel by phase (architecture, build, transition and maintain), by personnel level, and by role for the entire project.

<Response>

1. Project Organization Chart

Instructions: Offerors must provide a proposed organization chart showing the Offeror staff including all sub-contractors. The organization chart must include all the key Offeror personnel for each phase of the project and a summary of each key member's high level responsibilities (see Key Positions section below).

<Response>

2. Offeror Key Personnel

This schedule lists the Key Personnel. For the purposes of this schedule and the Contract, the following Offeror roles/titles have the following responsibilities:

a) **Engagement Executive** - The Engagement Executive is responsible for overall accountability of the Commonwealth business relationship and the success of the project. Serves as the primary contact for the management of the contract and assist Commonwealth customers with all facets of services, including assisting in building strong customer teaming relationships and delivering the highest level of customer service and satisfaction.

b) **Program Manager (Offeror Project Manager)** - The Program Manager has overall responsibility for delivery of the Services to the Commonwealth and exercises day-to-day supervision of the Program Management Office (PMO). The PMO Manager will manage the overall relationship ensuring that the Offeror fulfills all of its obligations under the Contract by working with the Commonwealth Management Committee to establish, manage, and meet commitments, requirements, and expectations to ensure operational compliance with the Contract. The PMO Manager will have a detailed knowledge and understanding of the Service Levels structure and credits, billing formats, hierarchies and credits, and Services being provided to ensure that Offeror fulfills its obligations under the Contract, including all obligations relating to deliverables. There will be one PMO Manager 100% dedicated to the Commonwealth

for the Term. The PMO Manager will be located at the Offeror's Harrisburg, Pennsylvania location.

c) **PMO Transition Manager(s)** – The PMO Transition Manager provides technical expertise and leadership during the transition of the current state datacenter services to the steady state managed datacenter services (i.e. the Commonwealth's new datacenter structure and services to be provided by Offeror pursuant to the Contract), and provides continuing engineering support through the remainder of the Term. In conjunction with the Commonwealth, the PMO Transition Manager develops plan(s) (inclusive of a detailed schedule(s) for performing associated tasks) for Offeror's implementation and transition of the Commonwealth from its legacy providers, cooperating with the Commonwealth to obtain the Commonwealth's approval and acceptance of the Transition Plan, and identifying the Transition Plan roles, responsibilities, and performance contingencies.

There will be two (2) PMO Transition Managers 100% dedicated to the Commonwealth for the entire Ramp-up Period. After the Ramp-up Period, the number of Transition Managers is reduced to one for the Term. The Transition Managers will be located at the Offeror's Harrisburg, Pennsylvania location during transition period.

d) **Availability Manager** – The Availability Manager is responsible for the overall service level management program for all of the Datacenter Services delivered.

e) **Service Level Management Analyst** – The PMO Service Level Management Analyst will prepare and package mutually agreed to operational reports, SLA reports, maintains Operations Manual, and oversees the Governance performance reporting. The Service Level Management Analyst will be located at the Offeror's Harrisburg, Pennsylvania location.

f) **Sr. Enterprise Infrastructure Architect** – The Enterprise Infrastructure Architect is responsible for the overall technology management program for the Datacenter Services delivered. The Enterprise Architect will provide executive level technology oversight to the Program. The Enterprise Architect will provide leadership in the forecasting and outlook for new technologies and services to be added during the term of the Program. The Enterprise Architect must have deep understanding of infrastructure, application deployment, and web and software applications.

g) **Incident Management Manager** - The PMO Incident Manager will provide technical and operational escalations management and resolution by working with the help desk and Operations Centers to provide escalation oversight and back up support for Program Manager. The PMO Incident Manager will provide SLA review, compliance, and management; facilitate chronic issue management and resolution; and address operational and delivery issues and adherence to performance; assist with incidents, issues, and escalations; and provide root cause analysis and resolution.

h) **Change Manager and Change Analyst** – The Change Manager and Change Analyst will provide oversight and overall coordination of standard change management, process across products and services, and provide change management for future strategy and planning.

i) **Finance Manager and Finance Analyst** – The Finance Manager and Finance Analyst will provide billing support and facilitation of the consolidated billing process support for the one single invoice to the Commonwealth.

j) **Agency Account Managers** – Offeror will provide a minimum of five (5) dedicated Agency Account Managers responsible for understanding all of the services provided by Offeror and providing guidance to the agencies in understanding their datacenter business needs. Offeror must assign an Agency Account Manager to each agency that purchases services through the contract. Not all Agency Account Managers must be assigned to a single agency. Offerors shall identify the number of Agency Account Managers that will be assigned to this project as part of their proposal. Agency Account Managers will act as a liaison between Offeror and the agency; strengthen the strategic relationship between Offeror and the Commonwealth; maintain overall responsibility for sales, support, and operations; ensure that agreements are finalized and signed by all parties; provide periodic briefings to the Commonwealth on new services and technologies that may be of interest/use and provide the Commonwealth with pricing information on request. The Agency Account Managers will be located at the Offeror's Harrisburg, Pennsylvania location.

k) **Agency Infrastructure Architects (Service Area Leads) -** Offeror will provide a minimum of five (5) Infrastructure Architects responsible for the detailed design engineering of the Commonwealth's specific datacenter services designs and quotes and for coordinating Commonwealth related requests. There will be at least five (5) Infrastructure Architects dedicated to the Commonwealth for the Term.

l) **Security Manager** – Offeror will provide a Security Manager to oversee all aspects of the project to ensure compliance with all security standards and requirements.

3. Offeror Key Personnel Instructions

The Offeror must identify key personnel for the project including:

- Name
- Position in organization
- Proposed role on project
- Experience in the proposed role
- Qualifications for the proposed role
- Role in the last three projects
- Percentage of time the person is committed for the entire project (if not, start and end dates must be provided)

Note: The Offeror may submit additional key personnel in addition to those listed in Schedule G.

4. Offeror Key Personnel Table

Name	Title/Account Role	Experience in Proposed Role (Years)	Qualifications for Proposed Role	Primary work location	% Committed for Entire Project?
	Agency Account Managers				
	Agency Infrastructure Architects				
	Availability Manager				
	Change Analyst				
	Change Manager				
	Security Manager				
	Engagement Executive				
	Finance Analyst				
	Finance Manager				
	Incident/Problem Manager				
	PMO Transition				

	Managers				
	Program Manager				
	Service Level Management Analyst				
	Sr. Enterprise Infrastructure Architect				

5. Sub-Contractors (If Applicable) Instructions

The Offeror must identify the subcontractor's key staff for the project including:

- Name
- Proposed role on project
- Experience in the proposed role
- Qualifications for the proposed role
- Role in the last three projects
- Percentage of time the person is committed for the entire project (if not, start and end dates must be provided)

6. Sub-Contractor Key Staff

Name	Title/Account Role	Experience in Proposed Role (Years)	Qualifications for Proposed Role	Primary work location	% Committed for Entire Project?

Offeror acknowledges that certain of the Offeror employees are critical to the provision of the Services hereunder ("Key Positions"). With respect to Key Positions, the Parties agree as follows:

- Each individual in a Key Position shall be dedicated to the Commonwealth account in accordance with the requirements set out in this schedule;

- Before assigning an individual to a Key Position, whether as an initial assignment or as a replacement, Offeror shall:
  - Notify the Commonwealth of the proposed assignment;
  - Introduce the individual to appropriate representatives of the Commonwealth;
  - Provide the Commonwealth with a resume and any other information regarding the individual that may be reasonably requested by the Commonwealth;
  - Allow the Commonwealth to interview the individual; and
  - Obtain the Commonwealth's approval for such assignment, which approval will not be unreasonably withheld.
  - Offeror shall only assign an individual to a Key Position who is mutually agreed upon by the Commonwealth and Offeror; Offeror retains exclusive direction and control as to hiring, termination, and right to discipline or reward such individuals in connection with their employment.
- Offeror shall not replace or reassign individuals in Key Positions (except as a result of voluntary resignation, involuntary termination for cause, serious illness, disability or death) for the applicable time period set out in this Schedule following the date of his or her assignment to the Commonwealth account unless the Commonwealth consents in writing to such reassignment or replacement or such individual in such Key Position.
- If the Commonwealth decides that any individual in a Key Position should not continue in that position, then the Commonwealth may, in its sole discretion and upon notice to Offeror, require removal of such individual in the Key Position from the Offeror Personnel in accordance with the following:
  - Offeror shall, as soon as reasonably practicable, replace such individual in the Key Position with another person of suitable ability and qualifications in accordance with procedures set forth above; and
  - In the event that an individual in a Key Position is convicted of criminal conduct or is in breach of Offeror's obligations, Offeror shall immediately remove and replace such individual with another person of suitable ability and qualifications in accordance with the procedures set forth above.
  - Offeror must notify the Commonwealth Agency\Criminal Justice Sponsor immediately of becoming aware of any employee deemed not compliant with the PA CHRIA or FBI CJIS policies\regulations and the

Offeror will adhere to any guidance/requirements of those standards with regard to actions to take regarding the employee's physical/logical access and/or employment.

- Offeror shall not without the Commonwealth consent replace or reassign greater than twenty percent (20%) of individuals in Key Positions in any rolling six (6) month period.

7. Staff Contingency Plan

Instructions: The Offeror must provide a contingency plan that shows the ability to add more staff if needed to ensure meeting the Project's due date(s) and milestones as outlined in the Offerors proposal.

<Response>

8. Staff Management

Instructions: Describe internal standards, policies and procedures regarding hiring, professional development and human resource management.

<Response>

9. Training Policies and Procedures

Instructions: Describe Offeror's policies and processes for training and ongoing education of its personnel.

<Response>

10. Staff Retention

Instructions: Please describe Offeror's process and methodology for retaining Offeror personnel.

<Response>

Request for Proposal

RFP # 6100022698

Commonwealth of Pennsylvania

Office of Administration

Office for Information Technology

Data Center Computing Services

Schedule H

Commonwealth Computing Procedures Manual (CCPM)

Contents

1 PURPOSE 3
1.1 Organizational Overview 3
1.2 Transition and Support Activities and Responsibilities 4
1.3 IT Service Management Procedures 5
1.4 Financial Management Procedures 10
1.5 Contract Management Procedures 12
1.6 Relationship Management Procedures 14
1.7 Offeror Operational Procedures 16
1.8 The Commonwealth Customer Operations Manuals 18

Content	Description
1 PURPOSE	The Offeror should describe the purpose of the Commonwealth Computing Procedures Manual. This section should address who should use the Manual, how the Manual is organized, how the initial version and updates will be distributed, version control procedures for the Manual, when updates will occur, and procedures for authorizing and implementing updates. It is intended that the structure of the Manual will require that the individual compliance requirements and business rules of each participating Commonwealth Customer are separately identified where applicable for each section or component part of the Manual.
1.1 Organizational Overview	
1. Offeror Governance Organization	Include organization charts, description of functions performed, contact information.
2. Offeror Management and Delivery Organization	Include organization charts, description of functions performed, contact information.
3. Key Contacts - Offeror	A list of contacts that are key users of the Services and/or perform a liaison function in regard to the Services (by Commonwealth and Commonwealth Agencies, by location).

Content	Description
4. Key Contacts – Third Parties	A list of key Third Parties (maintenance providers, software providers, telecom carriers, etc).
1.2 Transition and Support Activities and Responsibilities	
1. Overall Management and Reporting Process	A description of Offeror management structure, reporting, and review process associated with Transition Services and Transformation Services.
2. Critical Deliverables and Milestones	A list of Critical Deliverables, milestones and timeline for the Transition Services and Transformation Services periods.
3. Interim Performance Management Procedures	A description of interim procedures to monitor and coordinate Service delivery, including Problem Management, Change Management, Service Level monitoring and reporting, physical and Logical Security, project management, work authorization, etc. A description of the responsibilities of both Parties.

Content	Description
4. Interim Financial Management Procedures	A description of interim procedures for invoicing, invoice verification, charge back to the Commonwealth Customers, determining Resource Unit volume by Service Component, asset management, asset transfers, forecasting, Commonwealth Customer support, etc. A description of the responsibilities of both Parties.
5. Interim Contract Management Procedures	A description of interim procedures for managing and administering the Agreement including proposed changes to the Agreement, interpretation procedures, issue-escalation process, and disputes. A description of the responsibilities of both Parties.
6. Other Transition and Support Procedures and Responsibilities	Any other pertinent procedures and responsibilities.
1.3 IT Service Management Procedures	
1. Service Desk	The facilities, associated technologies, and fully trained staff who respond to Calls, coordinate all Incident Management, Problem Management and Request Management activities, and act as a single point of contact for Authorized Users in regard to the Services.

Content	Description
2. Incident Management	The use of people, processes and technology with the primary goal to restore normal Service operations as quickly as possible and minimize the adverse impact on business operations, thus ensuring that the best achievable levels of service quality and availability are maintained.
3. Problem Management	The process, software, techniques and procedures that aid in identification, tracking, communication, and resolution of Problems arising in Customer's IT Environment, and resolving those Problems arising from or related to the Services. The goal of Problem Management is to minimize the adverse impact of Incidents and Problems on the business that are caused by errors within the IT infrastructure, and to prevent recurrence of Incidents related to these errors. In order to achieve this goal, Problem Management seeks to get to the root cause of Incidents and then initiate actions to improve or correct the situation.
4. Change Management	The processes relating to planning and performing all changes in IT environment pertaining to the Services, including changes to individual components and coordination of changes across all components. The Change Management processes will support and include checkpoints to determine any potential or required Change Control Procedures and includes a process of controlling changes to the infrastructure or any aspect of Services, in a controlled manner, enabling approved changes with minimum disruption.

<table>
<tr><th>Content</th><th>Description</th></tr>
<tr><td>5. Configuration Management</td><td>The process of identifying and defining CIs in a system, recording and reporting the status of CIs and RFCs, and verifying the completeness and correctness of the CIs.

The following data fields are required as a minimum for Asset/Configuration Management (any number of these may require that auditing be enabled.):

<table>
<tr><th>Physical Attributes</th><th>Logical Attributes</th></tr>
<tr><td>CI Name</td><td>System Role</td></tr>
<tr><td>Serial Number</td><td>Primary Capability</td></tr>
<tr><td>Commonwealth Asset Tag</td><td>Capability</td></tr>
<tr><td>Owner</td><td>Complexity</td></tr>
<tr><td>Ownership Type</td><td>Priority</td></tr>
<tr><td>Funding Source</td><td>Storage (currently TPC tool)</td></tr>
<tr><td>Purchase Date</td><td>24 x 7 Access</td></tr>
<tr><td>Life Cycle Dates</td><td>OS Billing Platform</td></tr>
<tr><td>Status</td><td>Operating System (OS)</td></tr>
<tr><td>Physical Location</td><td>OS Version</td></tr>
</table>
</td></tr>
</table>

Content	Description
6. Release Management	The process responsible for planning, scheduling and controlling the movement of Releases to Test and Live Environments. The primary objective of Release Management is to ensure that the integrity of the Live Environment is protected and that the correct Components are released. Release Management works closely with Configuration Management and Change Management.
7. Request Management and Fulfillment	The process responsible for managing the lifecycle of all Service Requests.
8. Availability Management	The process responsible for defining, analyzing, Planning, measuring and improving all aspects of the Availability of IT services. Availability Management is responsible for ensuring that all IT Infrastructure, Processes, tools, roles etc. are appropriate for the agreed Service Level targets for Availability.
9. Capacity Management	The process responsible for ensuring that the Capacity of IT Services and the IT Infrastructure are able to deliver agreed Service Level targets in a cost effective and timely manner. Capacity Management considers all Resources required to deliver the IT Service, and plans for short, medium and long term business requirements.

Content	Description
10. Service Level Management (SLM)	The process responsible for negotiating SLAs, and ensuring that these are met. SLM is responsible for ensuring that all IT Service Management Processes, OLAs, and Underpinning Contracts, are appropriate for the agreed Service Level targets. SLM monitors and reports on Service Levels, facilitates Service Delivery Failure actions with the appropriate Governance Committee and holds regular Commonwealth Customer reviews.
11. IT Service Continuity Management (ITSCM)	The process responsible for managing risks that could seriously impact IT Services. ITSCM ensures that the IT Offeror can Always provide minimum agreed Service Levels, by reducing the risk to an acceptable level and Planning for the recovery of IT Services. ITSCM should be designed to support Business Continuity Management.
12. IT Financial Management	The process responsible for managing the Budgeting, Accounting, Invoicing and Chargeback requirements).
13. Information Security Management	The process that ensures the confidentiality, integrity and Availability of an organization's Assets, information, data and IT Services. Information Security Management usually has a wider scope than the Offeror. It normally includes handling of paper, building access, phone calls etc., for the entire organization.

Content	Description
14. Project Management and Support	Project Management and Support will align projects to Commonwealth requirements and deliver projects from request through end-to-end solutioning including turnover to the Commonwealth Customers and validation that project requirements were met in terms of timing, quality, and cost.
15. Service Catalog	A database or structured Document with information about select Services, including those available for Deployment. The Service Catalog is the only part of the Service portfolio published to Commonwealth Customers, and is used to support the request and delivery of select Services. The Service Catalog may include information about Deliverables, prices, contact points, ordering and request processes.
1.4 Financial Management Procedures	
1. Invoicing	The Offeror should describe procedures for invoicing. The content should include procedures for calculating Resource Unit volumes for pricing (per Service Component, as applicable), invoicing of Projects, etc. The content should include procedures regarding disputed invoice amounts.

Content	Description
2. Chargeback	The Offeror should describe procedures for charge back of costs related to the Services and the overall Agreement to the Commonwealth Customers (to include responsibilities and support by both the Offeror and the Commonwealth).
3. Budgeting	The Offeror should describe how it would assist the Commonwealth with the annual budgeting cycle. Process should include estimation of Resource Unit volumes (by Service Component and Commonwealth Customer as appropriate), potential Projects, review cycle, etc. The content should include the responsibilities of Offeror, the Commonwealth, and Commonwealth Agencies.
4. Forecasting	The Offeror should describe procedures for forecasting cost versus budget.
5. Procurement	The Offeror should describe procedures for procurement Services (where Offeror performs procurement on behalf of the Commonwealth, as applicable). The content should include responsibilities and process for both the Commonwealth staff and Offeror.

Content	Description
6. Service Level Credits and Earnback	The Offeror should describe procedures for calculating Service Level Credits on invoices and Earnback calculations.
1.5 Contract Management Procedures	
1. Contract Change Control	The Offeror should describe procedures regarding changes to the Agreement, including changes to any Exhibit or Attachment. Content should include procedures to classify services as a New Service, and resulting process to change the Agreement (including pricing). Content should include notification period and process, authority levels, and escalation procedures for changes to the Agreement.
2. Reporting	The Offeror should describe procedures and activities regarding key standard Reports and requests for ad hoc reports from the Commonwealth and The Commonwealth Agencies.
3. New Service Levels	The Offeror should describe procedures for determining new Service Levels (based on continuous improvement and/or Commonwealth request).

Content	Description
4. Benchmarking	The Offeror should describe procedures for Benchmarking exercises, including determination and agreement of benchmark firm, sample peer group and process used for benchmark, payment for benchmark, review of results, and potential outcome. Content should include dispute resolution process.
5. Auditing	The Offeror should describe procedures for operational and/or financial audits (as required by the Commonwealth auditing and/or regulatory agencies). The Offeror should describe notification process and procedures to resolve audit findings.
6. Offeror Key Personnel and Subcontractors	The Offeror should describe procedures for Commonwealth approval regarding replacement or removal of Offeror Key Personnel and major Subcontractors to Offeror.
7. Dispute Resolution	The Offeror should describe procedures regarding formal dispute resolution process.

Content	Description
1.6 Relationship Management Procedures	
1. Customer Satisfaction Surveys	The Offeror should describe the process to be used for conducting customer satisfaction surveys. Content should include procedures regarding action items and attempts to resolve customer issues.
2. Commonwealth Agencies	The Offeror should describe procedures and responsibilities regarding the relationship between the Commonwealth, the Commonwealth Agencies and the Offeror. Content should include procedures regarding communication and coordination regarding work requests, Service delivery issues, budgeting and financial issues, etc.
3. Authorized Users	The Offeror should describe procedures and responsibilities regarding responding to Authorized Users (including listing of Authorized Users) problems, requests, and questions.

Content	Description
4. Third Party Vendors	Offeror to describe procedures for relationship regarding Third Party Vendors which may provide services, Equipment, and/or Software that are ancillary to (or support) the overall delivery of Services. Procedures and coordination with key Third Party Vendors should be documented.
5. Other Third Parties	The Offeror should describe procedures for any other contact or requests from other Third Parties in regard to the Agreement.

Content	Description
1.7 Offeror Operational Procedures	
1. Operating Level Agreements (OLA)	OLAs are internal "back-to-back" agreements that define how two different Service Component Providers will work together to support the delivery of defined IT Services to the Commonwealth and Commonwealth agencies. The OLAs will define how Service Component Providers will work together to meet the Service Requirements documented in SOWs and Service Level Requirements documented in formal SLAs for the DCS initiative. The OLAs are a set of operational processes that supplements the IT Service Management section of the Commonwealth Computing Procedures Manual providing the second level detail required for individual Service Components to interoperate. Simply stated, the OLA "bolts" multiple Service Components together operationally.
2. Operational Procedures (by Service Component, as applicable)	The Offeror should describe the activities that the Offeror proposes to undertake in order to provide the Services, including those directions, supervision, monitoring, staffing, reporting, Planning and oversight activities normally undertaken by the Offeror which shall be consistent with those Offeror activities used to provide services similar to the Services.

Content	Description
3. Service Responsibility Matrix (SRM)	A map of the Functional Service Areas which potentially overlap Offeror responsibility and Commonwealth responsibility required to deliver business solutions to the business units. A Service Responsibility Matrix will be developed for each such area to delineate which party is responsible for performing select service elements and/or providing assistance or input.

Content	Description
1.8 The Commonwealth Customer Operations Manuals	
1. Individual Commonwealth Customer Operations Manual	The Commonwealth Computing Procedures Manual will also contain specific sections dedicated to operational procedures for Services provided to individual The Commonwealth Customers (each a "**The Commonwealth Customer Operations Manual**"). Each The Commonwealth Customer Operations Manual will address unique operational requirements of the respective The Commonwealth Customer, including operational areas such as the following: • Runbooks • Data safeguarding, use and release restrictions • Data security policies • Disaster Recovery requirements • Notification levels and procedures (e.g. problems and initial Severity Level procedures)

Request for Proposal

RFP # 6100022698

Commonwealth of Pennsylvania

Office of Administration
Office for Information Technology

Datacenter Computing Services

Schedule I

Offeror Pricing Forms

Description of Exhibit and Instructions

This Schedule I - Offeror Pricing Forms sets forth the following:

Configuration Definitions

- This tab contains the descriptions of the defined configurations which are used on the Volumetrics and Catalog of Services tabs.
- No entry is required on this tab.

1. Volumetrics

- This tab includes the resource unit categories and target quantities that the Offeror's will use to determine their price.
- Offerors should not assume that these are a guaranteed minimum units over the contract period.
- No entry is required on this tab.

2. Total Charges

- Summary of all Services Charges.
- No entry is required on this tab

3. Technical Staff Rate Card

- Offerors should use this tab to provide their staffing rates for the optional support services
- Offeror should only input in highlighted (yellow) cells.
- This rate card will become part of the service catalog at the Effective Date of the contract.

4. Catalog of Services

- Offerors should use this tab to include their Catalog of Services with pricing.
  See "Configuration Definitions" Tab for detail on what is included in each service catalog item.
- Offeror should only input in highlighted (yellow) cells.
- Only provide costs within the highlighted (yellow) cells; no additional services will be accepted here.
- All costs for services must be included in the item cost in the catalog of services. No additional costs should be incurred by the Commonwealth for the services requested by this RFP.

5. Software

- Offerors should use this tab to include their pricing of the required Third Party Software and Hybrid Third Party Software.
- Offeror should only input in highlighted (yellow) cells.
- Only provide costs within the highlighted (yellow) cells; no additional software products will be accepted here.
- Offerors should price software titles listed or equivalent.
- Offerors must provide a catalog of monthly single unit prices as part of its proposal. a single unit could be a single MIP, a single core, a single user, a single server, etc. The configuration will be determined as part of transition planning.
- Offerors are required to provide all of the listed software within this table. The Commonwealth will assume if there is no price indicated for a particular requested software item; that item will be provided at no cost to the Commonwealth.

6. Termination Fees

- This tab identifies the Termination for Convenience Fees.
- No entry is required on this tab.

Additional Notes

a.) All input tabs (3, 4, 5) should be filled out completely.

b.) Total Charges (tab 2): Information is linked with input tabs and will calculate automatically.

c.) Any cost field left blank will indicate the item will be available to the Commonwealth at no cost.

d.) Formulas are imbedded in all tabs. Offeror must verify that all calculations, subtotal costs and grand total costs are accurate.

e.) Please contact the Issuing Officer with any questions or concerns.

f.) Payment for services under this contract are unit-based. The total units (volumetrics) listed are for informational purposes only and will not be binding on the Commonwealth

g.) All Transition costs must be included in the service prices as included in the Catalog of Services tab over years 1 thru 7. Any change to transition plans shall not alter the costs as included in Offeror's completed Schedule I - Offeror Pricing Form. No additional costs will be incurred by the Commonwealth for changes to Offeror's proposed Transition Plan.

h.) All DC architecture costs must be included in the service prices as included in the Catalog of Services tab over years 1 thru 7.

i.) All pricing must not include any assumptions of a minimum commitment for services from the Commonwealth.

j.) Offerors must include in the base unit pricing for all configurations the components and services required to meet the security requirements of the RFP for all compute services, to include but not limited to Schedule F Sections 3.2.4.6 and 3.2.2.5.

Configuration Definitions (**)

The below definitions and configurations are referenced throughout Schedule I - Offeror Pricing Forms.

(1) Fully Managed and (2) Managed Only

Servers and Storage Services (x86, p-Series, i-Series)

Servers and Storage services should include the server, disk and backup devices, as well as hardware supplies; software, including operating and data management systems; the facilities, including raised floor and office space; and facilities management.

Unit Prices should include all services costs associated with providing, managing, operating, and transitioning to each technology unit per the RFP requirements Schedule F COPA Datacenter Statement of Work;

3.1	Establish Datacenter Architecture
3.1.1	Multi Datacenter Environment (2+ Architecture)
3.1.2	Network and Security Architecture
3.1.3	Datacenter Architecture and Technology
3.2	Enable Common Service Portfolio
3.2.1	Program & Service Management
3.2.1.1	PMO & Contract Management
3.2.1.2	Availability/SLA Management
3.2.1.3	Change & Release Management
3.2.1.4	Service Desk
3.2.1.5	Technical Architecture
3.2.1.6	Account Management
3.2.1.7	Configuration Management
3.2.1.8	3rd Party License Management
3.2.2	Technical Services
3.2.2.1	Transition Management (New Customer and/or Services)
3.2.2.2	Infrastructure Architecture
3.2.2.3	Capacity Management
3.2.2.4	DR Planning & Testing
3.2.2.5	Security Management
3.2.2.6	Performance Monitoring & Management
3.2.3	Facilities Management
3.2.3.1	Facilities Architecture / Maintenance
3.2.3.2	Site Operations
3.2.4	Managed Hosting Services
3.2.4.1	Windows Support
3.2.4.2	Storage Management
3.2.4.3	ERP Hosting – SAP / Oracle
3.2.4.4	UNIX Support – AIX / Linux
3.2.4.6	Security & Firewall
3.3	Transition Services
3.3.1	Transition Services – Guiding Principals
3.3.2	Transition Planning/Governance
3.3.2.1	Transition Program Management
3.3.2.2	Security Transition Activities

Fully Managed Infrastructure is fully owned and managed by the Offeror

Managed Only Infrastructure is managed by the Service Provider but owned by the Commonwealth and/or a 3rd Party

(3) Limited Co-Lo

Limited Co-Lo is infrastructure that is located in the Service Provider managed datacenter(s). Either owned or managed by the Commonwealth; or 3rd Party.

Limited Co-Lo Services Unit Prices should include all services costs associated with providing, managing, and transitioning to each technology unit per the RFP requirements Schedule F COPA Datacenter Statement of Work Unit Prices should include all services costs associated with providing, managing, operation, and transitioning to each technology unit per the RFP requirements Schedule F COPA Datacenter Statement of Work;

3.1	Establish Datacenter Architecture
3.1.1	Multi Datacenter Environment (2+ Architecture)
3.1.2	Network and Security Architecture
3.1.3	Datacenter Architecture and Technology
3.2	Enable Common Service Portfolio
3.2.1	Program & Service Management
3.2.1.1	PMO & Contract Management
3.2.1.2	Availability/SLA Management
3.2.1.3	Change & Release Management
3.2.1.4	Service Desk
3.2.1.5	Technical Architecture

Configuration Definitions (**)

3.2.1.6 Account Management
3.2.1.7 Configuration Management
3.2.1.8 3rd Party License Management
3.2.2 Technical Services
3.2.2.1 Transition Management (New Customer and/or Services)
3.2.2.2 Infrastructure Architecture
3.2.2.3 Capacity Management
3.2.2.4 DR Planning & Testing
3.2.2.5 Security Management
3.2.2.6 Performance Monitoring & Management
3.2.3 Facilities Management
3.2.3.1 Facilities Architecture / Maintenance
3.2.3.2 Site Operations
3.2.4 Managed Hosting Services
3.2.4.8 Limited-Use Colocation Services
3.3 Transition Services
3.3.1 Transition Services – Guiding Principals
3.3.2 Transition Planning/Governance
3.3.2.1 Transition Program Management
3.3.2.2 Security Transition Activities

(4) Mainframe Services - Include both IBM and Unisys Mainframe services

Mainframe services should include the hardware for the mainframe processing units; disk and backup devices, as well as hardware supplies; software, including operating and data management systems; the facilities, including raised floor and office space; and facilities management in addition to the services described below.

Mainframe Services Unit Prices should include all services costs associated with providing, managing, operating, and transitioning to each technology unit per the RFP requirements Schedule F COPA Datacenter Statement of Work;

3.1 Establish Datacenter Architecture
3.1.1 Multi Datacenter Environment (2+ Architecture)
3.1.2 Network and Security Architecture
3.1.3 Datacenter Architecture and Technology
3.2 Enable Common Service Portfolio
3.2.1 Program & Service Management
3.2.1.1 PMO & Contract Management
3.2.1.2 Availability/SLA Management
3.2.1.3 Change & Release Management
3.2.1.4 Service Desk
3.2.1.5 Technical Architecture
3.2.1.6 Account Management
3.2.1.7 Configuration Management
3.2.1.8 3rd Party License Management
3.2.2 Technical Services
3.2.2.1 Transition Management (New Customer and/or Services)
3.2.2.2 Infrastructure Architecture
3.2.2.3 Capacity Management
3.2.2.4 DR Planning & Testing
3.2.2.5 Security Management
3.2.2.6 Performance Monitoring & Management
3.2.3 Facilities Management
3.2.3.1 Facilities Architecture / Maintenance
3.2.3.2 Site Operations
3.2.4 Managed Hosting Services
3.2.4.2 Storage Management
3.2.4.5 Mainframe Services
3.2.4.6 Security & Firewall
3.3 Transition Services
3.3.1 Transition Services – Guiding Principals
3.3.2 Transition Planning/Governance
3.3.2.1 Transition Program Management
3.3.2.2 Security Transition Activities

Offerors must also use exhibit B1 DPH Asset List for configuration requirements for mainframe services.

(5) On-Demand (IaaS) Services

On-Demand Unit Prices should include all services costs associated with providing, managing, operating, and transitioning to each technology unit per the RFP requirements Schedule F COPA Datacenter Statement of Work;

3.1 Establish Datacenter Architecture
3.1.1 Multi Datacenter Environment (2+ Architecture)
3.1.2 Network and Security Architecture
3.1.3 Datacenter Architecture and Technology
3.2 Enable Common Service Portfolio

Configuration Definitions (**)

3.2.1	Program & Service Management
3.2.1.1	PMO & Contract Management
3.2.1.2	Availability/SLA Management
3.2.1.3	Change & Release Management
3.2.1.4	Service Desk
3.2.1.5	Technical Architecture
3.2.1.6	Account Management
3.2.1.7	Configuration Management
3.2.1.8	3rd Party License Management
3.2.2	Technical Services
3.2.2.1	Transition Management (New Customer and/or Services)
3.2.2.2	Infrastructure Architecture
3.2.2.3	Capacity Management
3.2.2.4	DR Planning & Testing
3.2.2.5	Security Management
3.2.2.6	Performance Monitoring & Management
3.2.3	Facilities Management
3.2.3.1	Facilities Architecture / Maintenance
3.2.3.2	Site Operations
3.2.5	Capacity on Demand Services
3.2.5.1	Server Capacity on Demand
3.2.5.2	Storage Capacity on Demand
3.2.5.3	DR Infrastructure on Demand
3.2.5.4	Additional Technical Services
3.3	Transition Services
3.3.1	Transition Services – Guiding Principals
3.3.2	Transition Planning/Governance

Configurations (**)

Limited Co-Lo (Data Center Only Charge)

Limited Co-Lo Configurations	Minimum Specifications	Unit
Co-Lo Config - 1	1/4 Rack Configuration includes: 10U Cabinet Space; 5,000 GB Network Bandwidth; 100Mb/s Uplink; 6 IP Addresses; 5 -110V AC Circuits	Monthly Per Config
Co-Lo Config - 2	1/2 Rack Configuration includes: 21U Cabinet Space; 10,000 GB Network Bandwidth; 100Mb/s Uplink; 14 IP Addresses; 10 -110V AC Circuits	Monthly Per Config
Co-Lo Config - 3	Full Rack Configuration includes: 42U Cabinet Space; 20,000 GB Network Bandwidth; 100Mb/s Uplink; 30 IP Addresses; 20 -110V AC Circuits	Monthly Per Config

Server Configurations (Fully Managed)

x86 Server Configurations	Minimum Specifications	Unit
Windows pConfig - 1	2-way Quad-Core 2.0 GHz; 4 GB RAM; Mirrored 146 15K Hard Drives; Windows Server 2008 R2	Physical Server
Windows pConfig - 2	2-way Six-Core 2.4 GHz; 16 GB RAM; Mirrored 146 15K Hard Drives; Windows Server 2008 R2	Physical Server
Windows pConfig - 3	4-way Six-Core 2.0 GHz; 64 GB RAM; 500 GB SAN Attached Storage; Windows Server 2008 R2	Physical Server

Configuration Definitions (**)

Windows pConfig - 4	2-way Six-Core 2.4 GHz; 16 GB RAM; Mirrored 146 15K Hard Drives; Windows Server 2008 R2; Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Physical Server
Windows pConfig - 5	2-way Six-Core 2.4 GHz; 16 GB RAM; Mirrored 146 15K Hard Drives; Windows Server 2008 R2; Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Physical Server
Linux pConfig - 1	2-way Quad-Core 2.0 GHz; 4 GB RAM; Mirrored 146 15K Hard Drives; RedHat or SUSE	Physical Server
Linux pConfig - 2	2-way Six-Core 2.4 GHz; 16 GB RAM; Mirrored 146 15K Hard Drives; RedHat or SUSE	Physical Server
Linux pConfig - 3	4-way Six-Core 2.0 GHz; 64 GB RAM; 500 GB SAN Attached Storage; RedHat or SUSE	Physical Server
Linux pConfig - 4	2-way Six-Core 2.4 GHz; 16 GB RAM; Mirrored 146 15K Hard Drives; RedHat or SUSE; Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Physical Server
Linux pConfig - 5	2-way Six-Core 2.4 GHz; 16 GB RAM; Mirrored 146 15K Hard Drives; RedHat or SUSE; Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Physical Server
Windows vConfig - 1	2vCPU; 4 GB Ram; Windows Server 2008 R2; ~~Firewall/IDS; Site-Site VPN; VPN Client; VLAN~~	Virtual Server Instance
Windows vConfig - 2	4vCPU; 16 GB Ram; Windows Server 2008 R2;~~Firewall/IDS; Site-Site VPN; VPN Client; VLAN~~	Virtual Server Instance
Windows vConfig - 3	8vCPU; 64 GB Ram; Windows Server 2008 R2; ~~Firewall/IDS; Site-Site VPN; VPN Client; VLAN~~	Virtual Server Instance
Windows vConfig - 4	4vCPU; 16 GB Ram; Windows Server 2008 R2; ~~Firewall/IDS; Site-Site VPN; VPN Client; VLAN~~; Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Virtual Server Instance

Configuration Definitions (**)

Windows vConfig - 5	4vCPU; 16 GB Ram; Windows Server 2008 R2; ~~Firewall/IDS; Site-Site VPN; VPN Client; VLAN~~; Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Virtual Server Instance
Linux vConfig - 1	2vCPU; 4 GB Ram; RedHat or SUSE; ~~Firewall/IDS; Site-Site VPN; VPN Client; VLAN~~	Virtual Server Instance
Linux vConfig - 2	4vCPU; 16 GB Ram; RedHat or SUSE; ~~Firewall/IDS; Site-Site VPN; VPN Client; VLAN~~	Virtual Server Instance
Linux vConfig - 3	8vCPU; 64 GB Ram; RedHat or SUSE; ~~Firewall/IDS; Site-Site VPN; VPN Client; VLAN~~	Virtual Server Instance
Linux vConfig - 4	4vCPU; 16 GB Ram; RedHat or SUSE; ~~Firewall/IDS; Site-Site VPN; VPN Client; VLAN;~~ Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Virtual Server Instance
Linux vConfig - 5	4vCPU; 16 GB Ram; RedHat or SUSE; ~~Firewall/IDS; Site-Site VPN; VPN Client; VLAN;~~ Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Virtual Server Instance

P-Series Server Configurations		
AIX Config - 1	3.0GHz POWER7; 0.5 Cores; 6 GB RAM; AIX	LPAR
AIX Config - 2	3.0GHz POWER7; 1.0 Cores; 12 GB RAM; AIX	LPAR
AIX Config - 3	3.0GHz POWER7; 1.5 Cores; 18 GB RAM; AIX	LPAR
AIX Config - 4	3.0GHz POWER7; 1.0 Cores; 12 GB RAM; AIX; Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	LPAR
AIX Config - 5	3.0GHz POWER7; 1.0 Cores; 12 GB RAM; AIX; Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	LPAR

Mainframe Configurations (*)		
IBM Mainframe Configurations	**Minimum Specifications**	**Unit**
IBM Mainframe Config - 1	IBM System zEnterprise Processor z/OS	MIP
IBM Mainframe Config - 2	IBM System zEnterprise Processor Virtual Linux Prod IFL	MIP

Configuration Definitions (**)

IBM Mainframe Config - 3	IBM System zEnterprise Processor Virtual Linux Prod IFL; Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	MIP
IBM AS400 Config 1	IBM i Series / AS400	CPW
IBM AS400 Config 2	IBM i Series / AS400; Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	CPW
Unisys Mainframe Configurations	**Minimum Specifications**	**Unit**
Unisys Mainframe Config - 1	Unisys (Clearpath / Dorado)	MIP
Unisys Mainframe Config - 2	Unisys (Clearpath / Libra)	MIP
Unisys Mainframe Config - 3	Unisys (Clearpath / Dorado); Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	MIP
Unisys Mainframe Config - 4	Unisys (Clearpath / Libra) ; Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	MIP

On-Demand (IaaS) Configurations		
IaaS x86 Server Configurations	**Minimum Specifications**	**Unit (per month)**
IaaS Windows vConfig - 1	2vCPU; 4 GB Ram; Windows Server 2008 R2; ~~Firewall/IDS; Site-Site VPN; VPN Client; VLAN~~	Virtual Server Instance
IaaS Windows vConfig - 2	4vCPU; 16 GB Ram; Windows Server 2008 R2; ~~Firewall/IDS; Site-Site VPN; VPN Client; VLAN~~	Virtual Server Instance
IaaS Windows vConfig - 3	8vCPU; 64 GB Ram; Windows Server 2008 R2; ~~Firewall/IDS; Site-Site VPN; VPN Client; VLAN~~	Virtual Server Instance
IaaS Windows vConfig - 4	4vCPU; 16 GB Ram; Windows Server 2008 R2; ~~Firewall/IDS; Site-Site VPN; VPN Client; VLAN;~~ Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Virtual Server Instance
IaaS Windows vConfig - 5	4vCPU; 16 GB Ram; Windows Server 2008 R2; ~~Firewall/IDS; Site-Site VPN; VPN Client; VLAN;~~ Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Virtual Server Instance
IaaS Linux vConfig - 1	2vCPU; 4 GB Ram; RedHat or SUSE; ~~Firewall/IDS; Site-Site VPN; VPN Client; VLAN~~	Virtual Server Instance

Configuration Definitions (**)

IaaS Linux vConfig - 2	4vCPU; 16 GB Ram; RedHat or SUSE; ~~Firewall/IDS; Site-Site VPN; VPN Client; VLAN~~	Virtual Server Instance
IaaS Linux vConfig - 3	8vCPU; 64 GB Ram; RedHat or SUSE; ~~Firewall/IDS; Site-Site VPN; VPN Client; VLAN~~	Virtual Server Instance
IaaS Linux vConfig - 4	4vCPU; 16 GB Ram; RedHat or SUSE; ~~Firewall/IDS; Site-Site VPN; VPN Client; VLAN;~~ Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Virtual Server Instance
IaaS Linux vConfig - 5	4vCPU; 16 GB Ram; RedHat or SUSE; ~~Firewall/IDS; Site-Site VPN; VPN Client; VLAN;~~ Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Virtual Server Instance
IaaS Storage Configurations		
IaaS Storage Config - 1	SAN attached storage; Raid 5; 10K - 15K RPM discs	Monthly per GB
IaaS Storage Config - 2	SAN attached storage; Raid 10; 10K - 15K RPM discs	Monthly per GB
IaaS Storage Config - 3	Network Attached Storage	Monthly per GB

IaaS Backup Configurations		
IaaS Backup Config - 1	Remote Offsite backup per GB	Monthly per GB

Notes:
(*) Offerors must use exhibit B1 DPH Asset List for configuration requirements for mainframe services.

Baseline Units - Volumetrics

Note: The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all inclusive representation of every service desired by the Commonwealth.

Resource Description	Service Tier / Configuration (6)	Units	Year 1 Qty	Year 2 Qty	Year 3 Qty	Year 4 Qty	Year 5 Qty	Year 6 Qty	Year 7 Qty	Opt - Year 8 Qty	Opt - Year 9 Qty	Opt - Year 10 Qty
Server - Fully Managed (1)												
x86 (Windows, Linux) - Physical Servers												
	Platinum Tier											
	Windows pConfig - 1	Server	27	26	24	23	22	21	20	19	18	17
	Windows pConfig - 2	Server	23	22	21	20	19	18	17	16	15	14
	Windows pConfig - 3	Server	14	13	13	12	11	11	10	10	9	9
	Windows pConfig - 4	Server	2	2	2	2	2	2	1	1	1	1
	Windows pConfig - 5	Server	2	2	2	2	2	2	1	1	1	1
	Linux pConfig - 1	Server	12	11	11	10	10	9	9	8	8	8
	Linux pConfig - 2	Server	8	8	7	7	7	6	6	6	5	5
	Linux pConfig - 3	Server	6	6	5	5	5	5	4	4	4	4
	Linux pConfig - 4	Server	2	2	2	2	2	2	1	1	1	1
	Linux pConfig - 5	Server	2	2	2	2	2	2	1	1	1	1
sub-total x86 (Windows, Linux) - Physical Servers - Plantinum			**98**	**94**	**89**	**85**	**82**	**78**	**70**	**67**	**63**	**61**
	Gold Tier											
	Windows pConfig - 1	Server	245	233	221	210	200	190	180	171	163	154
	Windows pConfig - 2	Server	209	199	189	179	170	162	154	146	139	132
	Windows pConfig - 3	Server	122	116	110	105	99	94	90	85	81	77
	Windows pConfig - 4	Server	18	17	16	15	15	14	13	13	12	11
	Windows pConfig - 5	Server	18	17	16	15	15	14	13	13	12	11
	Linux pConfig - 1	Server	108	103	97	93	88	84	79	75	72	68
	Linux pConfig - 2	Server	72	68	65	62	59	56	53	50	48	45
	Linux pConfig - 3	Server	54	51	49	46	44	42	40	38	36	34
	Linux pConfig - 4	Server	18	17	16	15	15	14	13	13	12	11
	Linux pConfig - 5	Server	18	17	16	15	15	14	13	13	12	11
sub-total x86 (Windows, Linux) - Physical Servers - Gold			**882**	**838**	**795**	**755**	**720**	**684**	**648**	**617**	**587**	**554**
	Silver Tier											
	Windows pConfig - 1	Server	272	258	245	233	222	210	200	190	180	189
	Windows pConfig - 2	Server	236	224	213	202	192	183	173	165	157	164
	Windows pConfig - 3	Server	136	129	123	117	111	105	100	95	90	95
	Windows pConfig - 4	Server	18	17	16	15	15	14	13	13	12	13
	Windows pConfig - 5	Server	18	17	16	15	15	14	13	13	12	13
	Linux pConfig - 1	Server	120	114	108	103	98	93	88	84	80	84
	Linux pConfig - 2	Server	120	114	108	103	98	93	88	84	80	84
	Linux pConfig - 3	Server	24	23	22	21	20	19	18	17	16	17
	Linux pConfig - 4	Server	18	17	16	15	15	14	13	13	12	13
	Linux pConfig - 5	Server	18	17	16	15	15	14	13	13	12	13
sub-total x86 (Windows, Linux) - Physical Servers - Silver			**980**	**930**	**883**	**839**	**801**	**759**	**719**	**687**	**651**	**685**
	Bronze Tier											
	Windows pConfig - 1	Server	120	114	108	103	98	93	88	84	80	76
	Windows pConfig - 2	Server	120	114	108	103	98	93	88	84	80	76
	Windows pConfig - 3	Server	47	45	42	40	38	36	35	33	31	30
	Windows pConfig - 4	Server	8	8	7	7	7	6	6	6	5	5
	Windows pConfig - 5	Server	3	3	3	3	2	2	2	2	2	2
	Linux pConfig - 1	Server	75	71	68	64	61	58	55	52	50	47
	Linux pConfig - 2	Server	75	71	68	64	61	58	55	52	50	47

Baseline Units - Volumetrics

Note: The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all inclusive representation of every service desired by the Commonwealth.

Resource Description	Service Tier / Configuration (6)	Units	Year 1 Qty	Year 2 Qty	Year 3 Qty	Year 4 Qty	Year 5 Qty	Year 6 Qty	Year 7 Qty	Opt - Year 8 Qty	Opt - Year 9 Qty	Opt - Year 10 Qty
	Linux pConfig - 3	Server	20	19	18	17	16	15	15	14	13	13
	Linux pConfig - 4	Server	4	4	4	3	3	3	3	3	3	3
	Linux pConfig - 5	Server	2	2	2	2	2	2	1	1	1	1
sub-total x86 (Windows, Linux) - Physical Servers - Bronze			**474**	**451**	**428**	**406**	**386**	**366**	**348**	**331**	**315**	**300**
	Basic Tier											
	Windows pConfig - 1	Server	240	228	217	206	195	186	176	168	159	151
	Windows pConfig - 2	Server	240	228	217	206	195	186	176	168	159	151
	Windows pConfig - 3	Server	110	105	99	94	90	85	81	77	73	69
	Windows pConfig - 4	Server	17	16	15	15	14	13	12	12	11	11
	Windows pConfig - 5	Server	7	7	6	6	6	5	5	5	5	4
	Linux pConfig - 1	Server	95	90	86	81	77	74	70	66	63	60
	Linux pConfig - 2	Server	95	90	86	81	77	74	70	66	63	60
	Linux pConfig - 3	Server	8	8	7	7	7	6	6	6	5	5
	Linux pConfig - 4	Server	9	9	8	8	7	7	7	6	6	6
	Linux pConfig - 5	Server	5	5	5	4	4	4	4	3	3	3
sub-total x86 (Windows, Linux) - Physical Servers - Basic			**826**	**786**	**746**	**708**	**672**	**640**	**607**	**577**	**547**	**520**
Total - Fully Managed - x86 Physical - All Support Tiers (Window, Linux)			**3,260**	**3,099**	**2,941**	**2,793**	**2,661**	**2,527**	**2,392**	**2,279**	**2,163**	**2,120**
x86 (Windows, Linux) - Virtual Servers												
	Platinum Tier											
	Windows vConfig - 1	Instance	28	29	31	32	34	36	38	39	41	43
	Windows vConfig - 2	Instance	23	24	25	27	28	29	31	32	34	36
	Windows vConfig - 3	Instance	14	15	15	16	17	18	19	20	21	22
	Windows vConfig - 4	Instance	3	3	3	3	4	4	4	4	4	5
	Windows vConfig - 5	Instance	2	2	2	2	2	3	3	3	3	3
	Linux vConfig - 1	Instance	12	13	13	14	15	15	16	17	18	19
	Linux vConfig - 2	Instance	10	11	11	12	12	13	13	14	15	16
	Linux vConfig - 3	Instance	6	6	7	7	7	8	8	8	9	9
	Linux vConfig - 4	Instance	2	2	2	2	2	3	3	3	3	3
	Linux vConfig - 5	Instance	1	1	1	1	1	1	1	1	1	2
sub-total x86 (Windows, Linux) - Virtual Servers - Platinum			**101**	**106**	**110**	**116**	**122**	**130**	**136**	**141**	**149**	**158**
	Gold Tier											
	Windows vConfig - 1	Instance	244	256	269	282	297	311	327	343	360	379
	Windows vConfig - 2	Instance	204	214	225	236	248	260	273	287	301	316
	Windows vConfig - 3	Instance	122	128	135	141	148	156	163	172	180	189
	Windows vConfig - 4	Instance	24	25	26	28	29	31	32	34	35	37
	Windows vConfig - 5	Instance	16	17	18	19	19	20	21	23	24	25
	Linux vConfig - 1	Instance	108	113	119	125	131	138	145	152	160	168
	Linux vConfig - 2	Instance	85	89	94	98	103	108	114	120	126	132
	Linux vConfig - 3	Instance	54	57	60	63	66	69	72	76	80	84
	Linux vConfig - 4	Instance	13	14	14	15	16	17	17	18	19	20
	Linux vConfig - 5	Instance	9	9	10	10	11	11	12	13	13	14
sub-total x86 (Windows, Linux) - Virtual Servers - Gold			**879**	**922**	**970**	**1017**	**1068**	**1121**	**1176**	**1238**	**1298**	**1364**
	Silver Tier											
	Windows vConfig - 1	Instance	272	286	300	315	331	347	365	383	402	422
	Windows vConfig - 2	Instance	232	244	256	269	282	296	311	326	343	360

Baseline Units - Volumetrics

Note: The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all inclusive representation of every service desired by the Commonwealth.

Resource Description	Service Tier / Configuration (6)	Units	Year 1 Qty	Year 2 Qty	Year 3 Qty	Year 4 Qty	Year 5 Qty	Year 6 Qty	Year 7 Qty	Opt - Year 8 Qty	Opt - Year 9 Qty	Opt - Year 10 Qty
	Windows vConfig - 3	Instance	136	143	150	157	165	174	182	191	201	211
	Windows vConfig - 4	Instance	24	25	26	28	29	31	32	34	35	37
	Windows vConfig - 5	Instance	16	17	18	19	19	20	21	23	24	25
	Linux vConfig - 1	Instance	120	126	132	139	146	153	161	169	177	186
	Linux vConfig - 2	Instance	98	103	108	113	119	125	131	138	145	152
	Linux vConfig - 3	Instance	60	63	66	69	73	77	80	84	89	93
	Linux vConfig - 4	Instance	13	14	14	15	16	17	17	18	19	20
	Linux vConfig - 5	Instance	9	9	10	10	11	11	12	13	13	14
sub-total x86 (Windows, Linux) - Virtual Servers - Silver			**980**	**1030**	**1080**	**1134**	**1191**	**1251**	**1312**	**1379**	**1448**	**1520**
	Bronze Tier											
	Windows vConfig - 1	Instance	91	96	100	105	111	116	122	128	134	141
	Windows vConfig - 2	Instance	91	96	100	105	111	116	122	128	134	141
	Windows vConfig - 3	Instance	44	46	49	51	53	56	59	62	65	68
	Windows vConfig - 4	Instance	1	1	1	1	1	1	1	1	1	2
	Windows vConfig - 5	Instance	1	1	1	1	1	1	1	1	1	2
	Linux vConfig - 1	Instance	38	40	42	44	46	48	51	53	56	59
	Linux vConfig - 2	Instance	38	40	42	44	46	48	51	53	56	59
	Linux vConfig - 3	Instance	18	19	20	21	22	23	24	25	27	28
	Linux vConfig - 4	Instance	1	1	1	1	1	1	1	1	1	2
	Linux vConfig - 5	Instance	1	1	1	1	1	1	1	1	1	2
sub-total x86 (Windows, Linux) - Virtual Servers - Bronze			**324**	**341**	**357**	**374**	**393**	**411**	**433**	**453**	**476**	**504**
	Basic Tier											
	Windows vConfig - 1	Instance	181	190	200	210	220	231	243	255	267	281
	Windows vConfig - 2	Instance	181	190	200	210	220	231	243	255	267	281
	Windows vConfig - 3	Instance	90	95	99	104	109	115	121	127	133	140
	Windows vConfig - 4	Instance	1	1	1	1	1	1	1	1	1	2
	Windows vConfig - 5	Instance	1	1	1	1	1	1	1	1	1	2
	Linux vConfig - 1	Instance	80	84	88	93	97	102	107	113	118	124
	Linux vConfig - 2	Instance	80	84	88	93	97	102	107	113	118	124
	Linux vConfig - 3	Instance	40	42	44	46	49	51	54	56	59	62
	Linux vConfig - 4	Instance	1	1	1	1	1	1	1	1	1	2
	Linux vConfig - 5	Instance	1	1	1	1	1	1	1	1	1	2
sub-total x86 (Windows, Linux) - Virtual Servers - Basic			**656**	**689**	**723**	**760**	**796**	**836**	**879**	**923**	**966**	**1020**
Total - Fully Managed - x86 Virtual - All Support Tiers (Window, Linux)			**2,940**	**3,088**	**3,240**	**3,401**	**3,570**	**3,749**	**3,936**	**4,134**	**4,337**	**4,566**
UNIX (IBM P-Series, AIX)												
	Platinum Tier											
	AIX Config - 1	LPAR	36	38	40	42	44	46	48	51	53	56
	AIX Config - 2	LPAR	26	27	29	30	32	33	35	37	38	40
	AIX Config - 3	LPAR	18	19	20	21	22	23	24	25	27	28
	AIX Config - 4	LPAR	5	5	6	6	6	6	7	7	7	8
	AIX Config - 5	LPAR	5	5	6	6	6	6	7	7	7	8
sub-total P-Series (AIX) - Bronze			**90**	**94**	**101**	**105**	**110**	**114**	**121**	**127**	**132**	**140**
	Gold Tier											
	AIX Config - 1	LPAR	36	38	40	42	44	46	48	51	53	56
	AIX Config - 2	LPAR	26	27	29	30	32	33	35	37	38	40

Baseline Units - Volumetrics

Note: The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all inclusive representation of every service desired by the Commonwealth.

Resource Description	Service Tier / Configuration (6)	Units	Year 1 Qty	Year 2 Qty	Year 3 Qty	Year 4 Qty	Year 5 Qty	Year 6 Qty	Year 7 Qty	Opt - Year 8 Qty	Opt - Year 9 Qty	Opt - Year 10 Qty
	AIX Config - 3	LPAR	18	19	20	21	22	23	24	25	27	28
	AIX Config - 4	LPAR	5	5	6	6	6	6	7	7	7	8
	AIX Config - 5	LPAR	5	5	6	6	6	6	7	7	7	8
sub-total P-Series (AIX) - Gold			**90**	**94**	**101**	**105**	**110**	**114**	**121**	**127**	**132**	**140**
	Silver Tier											
	AIX Config - 1	LPAR	72	76	79	83	88	92	96	101	106	112
	AIX Config - 2	LPAR	52	55	57	60	63	66	70	73	77	81
	AIX Config - 3	LPAR	36	38	40	42	44	46	48	51	53	56
	AIX Config - 4	LPAR	10	11	11	12	12	13	13	14	15	16
	AIX Config - 5	LPAR	10	11	11	12	12	13	13	14	15	16
sub-total P-Series (AIX) - Silver			**180**	**191**	**198**	**209**	**219**	**230**	**240**	**253**	**266**	**281**
	Bronze Tier											
	AIX Config - 1	LPAR	24	25	26	28	29	31	32	34	35	37
	AIX Config - 2	LPAR	24	25	26	28	29	31	32	34	35	37
	AIX Config - 3	LPAR	8	8	9	9	10	10	11	11	12	12
	AIX Config - 4	LPAR	2	2	2	2	2	3	3	3	3	3
	AIX Config - 5	LPAR	2	2	2	2	2	3	3	3	3	3
sub-total P-Series (AIX) - Bronze			**60**	**62**	**65**	**69**	**72**	**78**	**81**	**85**	**88**	**92**
	Basic Tier											
	AIX Config - 1	LPAR	64	67	71	74	78	82	86	90	95	99
	AIX Config - 2	LPAR	64	67	71	74	78	82	86	90	95	99
	AIX Config - 3	LPAR	32	34	35	37	39	41	43	45	47	50
	AIX Config - 4	LPAR	10	11	11	12	12	13	13	14	15	16
	AIX Config - 5	LPAR	10	11	11	12	12	13	13	14	15	16
sub-total P-Series (AIX) - Basic			**180**	**190**	**199**	**209**	**219**	**231**	**241**	**253**	**267**	**280**
Total - Fully Managed - P-Series (AIX) - All Support Tiers (Window, Linux)			**600**	**631**	**664**	**697**	**730**	**767**	**804**	**845**	**885**	**933**
Server - Managed Only (2)												
x86 (Windows, Linux)												
	Platinum Tier	Server/Instance	100	60	36	22	50	50	50	50	50	50
	Gold Tier	Server/Instance	900	540	324	194	50	50	50	50	50	50
	Silver Tier	Server/Instance	1000	600	360	216	50	50	50	50	50	50
	Bronze Tier	Server/Instance	750	450	270	162	50	50	50	50	50	50
	Basic Tier	Server/Instance	1050	630	378	227	50	50	50	50	50	50
Total Managed Only- x86 - All Support Tiers (Window, Linux)			**3,800**	**2,280**	**1,368**	**821**	**250**	**250**	**250**	**250**	**250**	**250**
UNIX (IBM P-Series, AIX)												
	Platinum	LPAR	5	3	2	10	10	10	10	10	10	10
	Gold Tier	LPAR	15	9	5	10	10	10	10	10	10	10
	Silver Tier	LPAR	30	18	11	10	10	10	10	10	10	10
	Bronze Tier	LPAR	40	24	14	10	10	10	10	10	10	10
	Basic Tier	LPAR	30	18	11	10	10	10	10	10	10	10
Total Managed Only- P-Series - All Support Tiers (AIX)			**120**	**72**	**43**	**50**	**50**	**50**	**50**	**50**	**50**	**50**
Storage and Backup - Fully Managed (1)												

Baseline Units - Volumetrics

Note: The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all inclusive representation of every service desired by the Commonwealth.

Resource Description	Service Tier / Configuration (6)	Units	Year 1 Qty	Year 2 Qty	Year 3 Qty	Year 4 Qty	Year 5 Qty	Year 6 Qty	Year 7 Qty	Opt - Year 8 Qty	Opt - Year 9 Qty	Opt - Year 10 Qty
Enterprise Storage												
	* Dedicated - Config 1 - SAN Raid 5	GB	2300000	2530000	2783000	3061300	3367430	3704173	4074590	4482049	4930254	5423280
	* Dedicated - Config 2 - SAN Raid 10	GB	400000	440000	484000	532400	585640	644204	708624	779487	857436	943179
	Dedicated - Config 3 - Net Attached	GB	10000	11000	12100	13310	14641	16105	17716	19487	21436	23579
Total Enterprise Storage - Fully Managed			**2,710,000**	**2,981,000**	**3,279,100**	**3,607,010**	**3,967,711**	**4,364,482**	**4,800,930**	**5,281,023**	**5,809,126**	**6,390,038**
Tape and Backup												
	** Server Tape Stored	GB Stored	2700000	2970000	3267000	3593700	3953070	4348377	4783215	5261536	5787690	6366459
	** Offsite Tape Storage	Tapes	5000	5500	6050	6655	7321	8053	8858	9744	10718	11790
Total Tape and Backup - Fully Managed			**2,705,000**	**2,975,500**	**3,273,050**	**3,600,355**	**3,960,391**	**4,356,430**	**4,792,073**	**5,271,280**	**5,798,408**	**6,378,249**

Limited Co-Lo (Data Center Only Charge) (3)												
Server, Storage, Network, Security Equipment												
	Co-Lo Config - 1	Per Config	20	20	20	20	20	20	20	20	20	20
	Co-Lo Config - 2	Per Config	20	20	20	20	20	20	20	20	20	20
	Co-Lo Config - 3	Per Config	80	80	80	80	40	40	40	40	40	40
Total Limited Co-Lo (Data Center Only Charge)			**120**	**120**	**120**	**120**	**80**	**80**	**80**	**80**	**80**	**80**

Mainframe Services (4)												
IBM Services												
	*** IBM Mainframe Allocated DASD	GB	100000	100000	100000	100000	100000	100000	100000	100000	100000	100000
	IBM Tapes in Storage - VTS	GB	100000	100000	100000	100000	100000	100000	100000	100000	100000	100000
	IBM Offsite Tape Storage	Tape/Reel	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000
Total IBM Services			**201,000**	**201,000**	**201,000**	**201,000**	**201,000**	**201,000**	**201,000**	**201,000**	**201,000**	**201,000**
IBM Configurations												
	Platinum Tier											
	IBM Mainframe Config - 1	MIP	1705	1705	1705	1705	1705	1705	1705	1705	1705	1705
	IBM Mainframe Config - 2	MIP	141	141	141	141	141	141	141	141	141	141
	IBM Mainframe Config - 3	MIP	330	330	330	330	330	330	330	330	330	330
	IBM AS400 Config 1	CPW	364	364	364	364	364	364	364	364	364	364
	IBM AS400 Config 2	CPW	1460	1460	1460	1460	1460	1460	1460	1460	1460	1460
sub-total IBM Mainfram Services - Plantinum			**4000**	**4000**	**4000**	**4000**	**4000**	**4000**	**4000**	**4000**	**4000**	**4000**
	Gold Tier											
	IBM Mainframe Config - 1	MIP	213	213	213	213	213	213	213	213	213	213
	IBM Mainframe Config - 2	MIP	18	18	18	18	18	18	18	18	18	18
	IBM Mainframe Config - 3	MIP	41	41	41	41	41	41	41	41	41	41
	IBM AS400 Config 1	CPW	46	46	46	46	46	46	46	46	46	46
	IBM AS400 Config 2	CPW	182	182	182	182	182	182	182	182	182	182
sub-total IBM Mainfram Services - Gold			**500**	**500**	**500**	**500**	**500**	**500**	**500**	**500**	**500**	**500**
	Basic Tier											
	IBM Mainframe Config - 1	MIP	213	213	213	213	213	213	213	213	213	213
	IBM Mainframe Config - 2	MIP	18	18	18	18	18	18	18	18	18	18
	IBM Mainframe Config - 3	MIP	41	41	41	41	41	41	41	41	41	41
	IBM AS400 Config 1	CPW	46	46	46	46	46	46	46	46	46	46
	IBM AS400 Config 2	CPW	182	182	182	182	182	182	182	182	182	182
sub-total IBM Mainfram Services - Basic			**500**	**500**	**500**	**500**	**500**	**500**	**500**	**500**	**500**	**500**

Baseline Units - Volumetrics

Note: The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all inclusive representation of every service desired by the Commonwealth.

Resource Description	Service Tier / Configuration (6)	Units	Year 1 Qty	Year 2 Qty	Year 3 Qty	Year 4 Qty	Year 5 Qty	Year 6 Qty	Year 7 Qty	Opt - Year 8 Qty	Opt - Year 9 Qty	Opt - Year 10 Qty
Total - IBM Mainframe Services - All Support Tiers			**5,000**	**5,000**	**5,000**	**5,000**	**5,000**	**5,000**	**5,000**	**5,000**	**5,000**	**5,000**
Unisys Services												
	*** Unisys DASD	GB	100000	100000	100000	100000	100000	100000	100000	100000	100000	100000
	Unisys Tapes in Storage - VTS	GB	100000	100000	100000	100000	100000	100000	100000	100000	100000	100000
	Unisys Offsite Tape Storage	Tape/Reel	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000
Total Unisys Services			**201,000**	**201,000**	**201,000**	**201,000**	**201,000**	**201,000**	**201,000**	**201,000**	**201,000**	**201,000**
Unisys Configurations												
	Platinum Tier											
	Unisys Mainframe Config - 1	MIP	550	550	550	550	550	550	550	550	550	550
	Unisys Mainframe Config - 2	MIP	220	220	220	220	220	220	220	220	220	220
	Unisys Mainframe Config - 3	MIP	2882	2882	2882	2882	2882	2882	2882	2882	2882	2882
	Unisys Mainframe Config - 4	MIP	875	875	875	875	875	875	875	875	875	875
sub-total Unisys Mainfram Services - Plantinum			**4527**	**4527**	**4527**	**4527**	**4527**	**4527**	**4527**	**4527**	**4527**	**4527**
	Gold Tier											
	Unisys Mainframe Config - 1	MIP	44	44	44	44	44	44	44	44	44	44
	Unisys Mainframe Config - 2	MIP	27	27	27	27	27	27	27	27	27	27
	Unisys Mainframe Config - 3	MIP	176	176	176	176	176	176	176	176	176	176
	Unisys Mainframe Config - 4	MIP	110	110	110	110	110	110	110	110	110	110
sub-total Unisys Mainfram Services - Gold			**357**	**357**	**357**	**357**	**357**	**357**	**357**	**357**	**357**	**357**
	Basic Tier											
	Unisys Mainframe Config - 1	MIP	44	44	44	44	44	44	44	44	44	44
	Unisys Mainframe Config - 2	MIP	27	27	27	27	27	27	27	27	27	27
	Unisys Mainframe Config - 3	MIP	176	176	176	176	176	176	176	176	176	176
	Unisys Mainframe Config - 4	MIP	110	110	110	110	110	110	110	110	110	110
sub-total Unisys Mainfram Services - Basic			**357**	**357**	**357**	**357**	**357**	**357**	**357**	**357**	**357**	**357**
Total - Unisys Mainframe Services - All Support Tiers			**5,241**	**5,241**	**5,241**	**5,241**	**5,241**	**5,241**	**5,241**	**5,241**	**5,241**	**5,241**
On-Demand (IaaS) (5)												
IaaS Servers - x86 (Windows, Linux) - Virtual Servers												
	IaaS Windows vConfig - 1	Instance	40	48	58	69	84	100	120	143	172	188
	IaaS Windows vConfig - 2	Instance	40	48	58	69	84	100	120	143	172	188
	IaaS Windows vConfig - 3	Instance	40	48	58	69	84	100	120	143	172	188
	IaaS Windows vConfig - 4	Instance	15	18	21	25	30	36	44	54	65	72
	IaaS Windows vConfig - 5	Instance	15	18	21	25	30	36	44	54	65	72
	IaaS Linux vConfig - 1	Instance	20	24	29	34	42	50	60	72	86	94
	IaaS Linux vConfig - 2	Instance	20	24	29	34	42	50	60	72	86	94
	IaaS Linux vConfig - 3	Instance	20	24	29	34	42	50	60	72	86	94
	IaaS Linux vConfig - 4	Instance	7	9	11	13	15	18	23	27	32	36
	IaaS Linux vConfig - 5	Instance	7	9	11	13	15	18	23	27	32	36
Total IaaS Servers - x86 (Windows, Linux) - Virtual Servers			**224**	**270**	**325**	**385**	**468**	**558**	**674**	**807**	**968**	**1,062**
IaaS Storage On-Demand												
	IaaS Storage Config - 1	GB	1000	1200	1440	1728	2074	2488	2986	3583	4300	5160
	IaaS Storage Config - 2	GB	500	600	720	864	1037	1244	1493	1792	2150	2580
	IaaS Storage Config - 3	GB	50	50	50	50	50	50	50	50	50	50

Baseline Units - Volumetrics

Note: The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all inclusive representation of every service desired by the Commonwealth.

Resource Description	Service Tier / Configuration (6)	Units	Year 1 Qty	Year 2 Qty	Year 3 Qty	Year 4 Qty	Year 5 Qty	Year 6 Qty	Year 7 Qty	Opt - Year 8 Qty	Opt - Year 9 Qty	Opt - Year 10 Qty
Total IaaS Storage On-Demand			**1,550**	**1,850**	**2,210**	**2,642**	**3,161**	**3,782**	**4,529**	**5,425**	**6,500**	**7,790**
IaaS Backup On-Demand												
	IaaS Backup Config - 1	GB	2,000	2,400	2,880	3,456	4,147	4,977	5,972	7,166	8,600	10320
Total IaaS Backup On-Demand			**2,000**	**2,400**	**2,880**	**3,456**	**4,147**	**4,977**	**5,972**	**7,166**	**8,600**	**10,320**
Reserve Account												
		Mos Balance	1	1	1	1	1	1	1	1	1	1
Reserve Account			**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**

Notes:

For purposes of submitting a proposal, Offerors should assume that tapes are equivalent in capacity to LTO4 tapes.

* For purposes of submitting a proposal, Offerors should assume that the slower Tier1 RAID5 uses 10K drives and the Tier2 RAID10 uses 15K drives.

** The volume is expressed as native.

*** For purposes of evaluation DASD is expressed in Usable (not Raw)

Third Party Software

Third Party Software

Vendor	Product											
B & L	BL/LIB Tape Library Management System	License	1	1	1	1	1	1	1	1	1	1
B & L	BL/SCHED Scheduling & Monitoring System	License	1	1	1	1	1	1	1	1	1	1
BMC Software	BMC AppSight for Windows/.NET - Division Edition	License	1	1	1	1	1	1	1	1	1	1
BMC Software	BMC AppSight Named Users	License	50	50	50	50	50	50	50	50	50	50
BMC Software	BMC AppSight QA Users	License	20	20	20	20	20	20	20	20	20	20
BMC Software	CONTROL-M Enterprise Manager	License	1	1	1	1	1	1	1	1	1	1
BMC Software	CONTROL-M Full Admin User	License	5	5	5	5	5	5	5	5	5	5
BMC Software	CONTROL-M Tasks (100 Tasks per Unit)	License	6	6	6	6	6	6	6	6	6	6
BMC Software	Database Director (D2)	License	1	1	1	1	1	1	1	1	1	1
BMC Software	Eclipse iBuild	License	1	1	1	1	1	1	1	1	1	1
BMC Software	Eclipse iChange	License	1	1	1	1	1	1	1	1	1	1
BMC Software	Eclipse iCheck	License	1	1	1	1	1	1	1	1	1	1
BMC Software	Eclipse iCopy	License	1	1	1	1	1	1	1	1	1	1
BMC Software	Eclipse iExtract	License	1	1	1	1	1	1	1	1	1	1
BMC Software	Eclipse iLM	License	1	1	1	1	1	1	1	1	1	1
BMC Software	Eclipse iLoad	License	1	1	1	1	1	1	1	1	1	1
BMC Software	Eclipse iRecover	License	1	1	1	1	1	1	1	1	1	1
BMC Software	Eclipse iSurvey	License	1	1	1	1	1	1	1	1	1	1
BMC Software	Eclipse iUnload	License	1	1	1	1	1	1	1	1	1	1
BMC Software	Mission Control	License	1	1	1	1	1	1	1	1	1	1
Business Objects	Crystal Reports	License	4	4	4	4	4	4	4	4	4	4
Bytware Inc.	StandGuard Anti-Virus	License	1	1	1	1	1	1	1	1	1	1
Citrix	XenApp Advanced (User Counts)	License	100	100	100	100	100	100	100	100	100	100
Citrix	XenApp Enterprise (User Counts)	License	750	750	750	750	750	750	750	750	750	750
Computer Associates International, Inc.	CA-Explore for CICS	License	1	1	1	1	1	1	1	1	1	1

Baseline Units - Volumetrics

Note: The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all inclusive representation of every service desired by the Commonwealth.

Resource Description	Service Tier / Configuration (6)	Units	Year 1 Qty	Year 2 Qty	Year 3 Qty	Year 4 Qty	Year 5 Qty	Year 6 Qty	Year 7 Qty	Opt - Year 8 Qty	Opt - Year 9 Qty	Opt - Year 10 Qty
Computer Associates International, Inc.	SOA Security Manager	License	1	1	1	1	1	1	1	1	1	1
Computer Associates International, Inc.	SOA Security Manager Additional Secured Web Services	License	100	100	100	100	100	100	100	100	100	100
Computer Associates International, Inc.	SOA Security Manager Additional Users	License	50,000	50,000	50,000	50,000	50,000	50,000	50,000	50,000	50,000	50,000
Cor icon Technologies	Corticon Business Rules Server – Unlimited CPUs	License	1	1	1	1	1	1	1	1	1	1
Cor icon Technologies	Corticon Server – per Non-Production Server	License	2	2	2	2	2	2	2	2	2	2
Cor icon Technologies	Corticon Business Rules Modeling Studio – per Named User	License	12	12	12	12	12	12	12	12	12	12
CSI International	EPIC	License	1	1	1	1	1	1	1	1	1	1
CSI International	FAQS/PCS	License	1	1	1	1	1	1	1	1	1	1
CSI International	FAQS/ASO	License	1	1	1	1	1	1	1	1	1	1
EMC Corporation	PowerPath	License	83	83	83	83	83	83	83	83	83	83
EMC Corporation	PowerPath (per CPU)	License	252	252	252	252	252	252	252	252	252	252
EMC Corporation	Symmetrix® VMAX Fully Automated Storage Tiering for Virtual Pools (FAST VP)	License	1	1	1	1	1	1	1	1	1	1
EMC Corporation	Vsphere Enterprise Plus	License	24	24	24	24	24	24	24	24	24	24
Experian QAS	NameSearch - Production (Licensed per Server up to 8 CPU)	License	2	2	2	2	2	2	2	2	2	2
Experian QAS	NameSearch - Non-Production (Licensed per Server)	License	3	3	3	3	3	3	3	3	3	3
Formula Consultants, Inc.	Star 1100	License	3	3	3	3	3	3	3	3	3	3
GlobalScape	CuteFTP Pro 2.0	License	4	4	4	4	4	4	4	4	4	4
HELPSYS	Robot/Schedule	License	3	3	3	3	3	3	3	3	3	3
Idea Integration	XGEN	License	1	1	1	1	1	1	1	1	1	1
Informatica Corporation	SSA-Name 3	License	1	1	1	1	1	1	1	1	1	1
Infragistics	NetAdvantage for .NET	License	6	6	6	6	6	6	6	6	6	6
KMSYS Worldwide, Inc.	lQU Plus-1	License	2	2	2	2	2	2	2	2	2	2
Levi, Ray and Shoup	VPS/PCL	License	1	1	1	1	1	1	1	1	1	1
Levi, Ray and Shoup	VPS/TCP/IP	License	1	1	1	1	1	1	1	1	1	1
Levi, Ray and Shoup	VPS/DRS	License	1	1	1	1	1	1	1	1	1	1
Levi, Ray and Shoup	VPS	License	1	1	1	1	1	1	1	1	1	1
MacKinney Systems, Inc.	CICS Response Time Monitor	License	1	1	1	1	1	1	1	1	1	1
~~Marble Computer, Inc.~~	~~OS DCD III Data Correlation and Documentation System~~	~~License~~	0	0	0	0	0	0	0	0	0	0
Microsoft	BizTalk Adaptor for MQSeries	License	8	8	8	8	8	8	8	8	8	8
Microsoft	BizTalk Server Enterprise (Single Processor)	License	5	5	5	5	5	5	5	5	5	5
Microsoft	BizTalk Server Standard (Single Processor)	License	4	4	4	4	4	4	4	4	4	4
Microsoft	SQL Server CAL	License	10	10	10	10	10	10	10	10	10	10
Microsoft	SQL Server Enterprise (Single Processor)	License	10	10	10	10	10	10	10	10	10	10
Microsoft	SQL Server Enterprise	License	11	11	11	11	11	11	11	11	11	11
Microsoft	SQL Server Standard (Single Processor)	License	2	2	2	2	2	2	2	2	2	2
Microsoft	SQL Server Standard	License	8	8	8	8	8	8	8	8	8	8
Microsoft	SQL Server Standard per 2-Core	License	4	4	4	4	4	4	4	4	4	4
Microsoft	Visual Studio Foundation Server	License	1	1	1	1	1	1	1	1	1	1

Baseline Units - Volumetrics

Note: The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all inclusive representation of every service desired by the Commonwealth.

Resource Description	Service Tier / Configuration (6)	Units	Year 1 Qty	Year 2 Qty	Year 3 Qty	Year 4 Qty	Year 5 Qty	Year 6 Qty	Year 7 Qty	Opt - Year 8 Qty	Opt - Year 9 Qty	Opt - Year 10 Qty
Microsoft	Visual Studio Foundation Server CAL	License	6	6	6	6	6	6	6	6	6	6
Microsoft	Visual Studio Professional with MSDN	License	8	8	8	8	8	8	8	8	8	8
Microsoft	Windows Server Datacenter Edition (Single Processor)	License	284	284	284	284	284	284	284	284	284	284
Microsoft	Windows Server Enterprise Edition	License	318	318	318	318	318	318	318	318	318	318
Microsoft	Windows Server Standard Edition	License	221	221	221	221	221	221	221	221	221	221
Microsoft	Windows Terminal Service Client Access Licenses	License	100	100	100	100	100	100	100	100	100	100
Network Associates	McAfee Anti-Virus	License	420	420	420	420	420	420	420	420	420	420
Novell	Platespin Migrator	License	12	12	12	12	12	12	12	12	12	12
Novell	SuSE Linux	License	11	11	11	11	11	11	11	11	11	11
OpenText	Metastorm Integration Manager for CICS (MIM for CICS)	License	1	1	1	1	1	1	1	1	1	1
Oracle	Oracle Change Management Pack	License	10	10	10	10	10	10	10	10	10	10
Oracle	Oracle Database 10g Enterprise	License	3	3	3	3	3	3	3	3	3	3
Oracle	Oracle Database Enterprise Edition	License	18	18	18	18	18	18	18	18	18	18
Oracle	Oracle Diagnos ic Pack	License	13	13	13	13	13	13	13	13	13	13
Oracle	Oracle Enterprise Linux	License	3	3	3	3	3	3	3	3	3	3
Oracle	Oracle Exadata Storage Software	License	1	1	1	1	1	1	1	1	1	1
Oracle	Oracle Partitioning	License	8	8	8	8	8	8	8	8	8	8
Oracle	Oracle Tuning Pack	License	13	13	13	13	13	13	13	13	13	13
Oracle	Real Application Cluster - Processor Perpetual	License	4	4	4	4	4	4	4	4	4	4
Oracle	Spatial and Graph - Processor Perpetual	License	4	4	4	4	4	4	4	4	4	4
Pitney Bowes	Finalist (Doc Sense)	License	1	1	1	1	1	1	1	1	1	1
Pitney Bowes	CODE-1 Plus	License	1	1	1	1	1	1	1	1	1	1
Pitney Bowes	CODE-1 Plus (Test / Development)	License	1	1	1	1	1	1	1	1	1	1
Pitney Bowes	Online Window for Finalist	License	1	1	1	1	1	1	1	1	1	1
Quest	Central Performance Suite for SQL Server, Tier A	License	2	2	2	2	2	2	2	2	2	2
Quest	Central Performance Suite for SQL Server, Tier B	License	10	10	10	10	10	10	10	10	10	10
Quest	Foglight Database Management Suite for SQL Server	License	8	8	8	8	8	8	8	8	8	8
Quest	Foglight for SQL Server per CPU Socket	License	42	42	42	42	42	42	42	42	42	42
Quest	Foglight OS Management per CPU Socket	License	47	47	47	47	47	47	47	47	47	47
Quest	Foglight Server for FSM	License	2	2	2	2	2	2	2	2	2	2
RealVNC	VNC Enterprise Edition for Windows	License	15	15	15	15	15	15	15	15	15	15
Red Hat	Red Hat Enterprise Linux	License	3	3	3	3	3	3	3	3	3	3
~~Schema Systems Limited~~	~~Q Editor Plus One~~	~~License~~	0	0	0	0	0	0	0	0	0	0
Segus Inc.	OPC/Graph	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG20	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG40	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG60	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG80	License	1	1	1	1	1	1	1	1	1	1

Baseline Units - Volumetrics

Note: The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all inclusive representation of every service desired by the Commonwealth.

Resource Description	Service Tier / Configuration (6)	Units	Year 1 Qty	Year 2 Qty	Year 3 Qty	Year 4 Qty	Year 5 Qty	Year 6 Qty	Year 7 Qty	Opt - Year 8 Qty	Opt - Year 9 Qty	Opt - Year 10 Qty
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG130	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG20	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG40	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG60	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG80	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG130	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG140	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - MAPPER, SWG20	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - MAPPER, SWG40	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - MAPPER, SWG60	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - MAPPER, SWG80	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - MAPPER, SWG130	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG20	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG40	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG60	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG80	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG130	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG140	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - System Log, SWG20	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - System Log, SWG40	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - System Log, SWG60	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - System Log, SWG80	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - System Log, SWG130	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - System Log, SWG140	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG20	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG40	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG60	License	1	1	1	1	1	1	1	1	1	1

Baseline Units - Volumetrics

Note: The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all inclusive representation of every service desired by the Commonwealth.

Resource Description	Service Tier / Configuration (6)	Units	Year 1 Qty	Year 2 Qty	Year 3 Qty	Year 4 Qty	Year 5 Qty	Year 6 Qty	Year 7 Qty	Opt - Year 8 Qty	Opt - Year 9 Qty	Opt - Year 10 Qty
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG80	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG130	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG140	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Power Agent, SWG20	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Power Agent, SWG40	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Power Agent, SWG60	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Power Agent, SWG80	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Power Agent, SWG130	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Power Agent, SWG140	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Torch Capacity Manager Power Agent, SWG40	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Torch Capacity Manager Power Agent, SWG60	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Torch Capacity Manager Power Agent, SWG130	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Torch Capacity Manager Power Agent, SWG140	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Torch Interface Agent - I/O TRACE, SWG40	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Torch Interface Agent - I/O TRACE, SWG60	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Torch Interface Agent - I/O TRACE, SWG130	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Torch Interface Agent - LOG, SWG40	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Torch Interface Agent - LOG, SWG60	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Torch Interface Agent - LOG, SWG130	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Torch Interface Agent - LOG, SWG140	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Torch Interface Agent - MAPPER, SWG40	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Torch Interface Agent - MAPPER, SWG60	License	1	1	1	1	1	1	1	1	1	1
Sightline	OS 2200 Torch Interface Agent - MAPPER, SWG130	License	1	1	1	1	1	1	1	1	1	1
Sightline	Windows 2000 Interface Agent - Internet Informa ion Server	License	7	7	7	7	7	7	7	7	7	7
Sightline	Windows 2000 Interface Agent - .NET	License	7	7	7	7	7	7	7	7	7	7
Sightline	Windows 2000 Interface Agent - SQL Server	License	4	4	4	4	4	4	4	4	4	4
Sightline	Windows 2000 Power Agent Upto 32 CPU's	License	3	3	3	3	3	3	3	3	3	3
SMA	OpCon/xps EXEC LSAM, Group 3	License	1	1	1	1	1	1	1	1	1	1
SMA	OpCon/xps EXEC LSAM, Group 12	License	1	1	1	1	1	1	1	1	1	1
SMA	OpCon/xps EXEC LSAM Development, Group 2	License	1	1	1	1	1	1	1	1	1	1
SMA	OpCon/xps EXEC LSAM Development, Group 12	License	1	1	1	1	1	1	1	1	1	1

Baseline Units - Volumetrics

Note: The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all inclusive representation of every service desired by the Commonwealth.

Resource Description	Service Tier / Configuration (6)	Units	Year 1 Qty	Year 2 Qty	Year 3 Qty	Year 4 Qty	Year 5 Qty	Year 6 Qty	Year 7 Qty	Opt - Year 8 Qty	Opt - Year 9 Qty	Opt - Year 10 Qty
SMA	OpCon/xps Production SAM	License	1	1	1	1	1	1	1	1	1	1
SMA	OpCon/xps Starter Kit	License	1	1	1	1	1	1	1	1	1	1
SMA	OpCon/xps User Interface	License	17	17	17	17	17	17	17	17	17	17
Sybase	EAServer Deploy Advanced - Active	License	2	2	2	2	2	2	2	2	2	2
Sybase	EAServer Deploy Advanced - Passive	License	2	2	2	2	2	2	2	2	2	2
Symantec	Backup Exec System Recovery Server	License	83	83	83	83	83	83	83	83	83	83
Symantec	EndPoint Protection	License	3	3	3	3	3	3	3	3	3	3
Symantec	Ghost Solution Suite	License	25	25	25	25	25	25	25	25	25	25
Symantec	NetBackup Client Application and Database Pack, UNX, Tier 3	License	3	3	3	3	3	3	3	3	3	3
Symantec	NetBackup Client Application and Database Pack, UNX, Tier 4	License	2	2	2	2	2	2	2	2	2	2
Symantec	NetBackup Client Application and Database Pack, WIN, Tier 2	License	7	7	7	7	7	7	7	7	7	7
Symantec	NetBackup Client Application and Database Pack, WIN, Tier 3	License	20	20	20	20	20	20	20	20	20	20
Symantec	NetBackup Client Application and Database Pack, WIN, Tier 4	License	1	1	1	1	1	1	1	1	1	1
Symantec	NetBackup Enterprise Client, UNX, Tier 4	License	1	1	1	1	1	1	1	1	1	1
Symantec	NetBackup Enterprise Client, WIN, Tier 1	License	3	3	3	3	3	3	3	3	3	3
Symantec	NetBackup Enterprise Client, WIN, Tier 2	License	10	10	10	10	10	10	10	10	10	10
Symantec	NetBackup Enterprise Client, WIN, Tier 3	License	18	18	18	18	18	18	18	18	18	18
Symantec	NetBackup Enterprise Server, WIN, Tier 2	License	3	3	3	3	3	3	3	3	3	3
Symantec	NetBackup Enterprise Server, WIN, Tier 3	License	16	16	16	16	16	16	16	16	16	16
Symantec	NetBackup Library Based Tape Drive Option, XPLAT	License	51	51	51	51	51	51	51	51	51	51
Symantec	NetBackup Media Server Encryption Option (MSEO) WIN, Tier 2	License	1	1	1	1	1	1	1	1	1	1
Symantec	NetBackup Platform Base, XPLAT (per Terabyte)	License	65	65	65	65	65	65	65	65	65	65
Symantec	NetBackup Shared Storage Option, XPLAT	License	56	56	56	56	56	56	56	56	56	56
Symantec	NetBackup Standard Client, XPLAT	License	133	133	133	133	133	133	133	133	133	133
Symantec	NetBackup Vault Additional Drive Option, XPLAT	License	6	6	6	6	6	6	6	6	6	6
Symantec	NetBackup Vault Base Option, XPLAT (4 tape drives per license)	License	6	6	6	6	6	6	6	6	6	6
Symantec	Veritas NetBackup Enterprise Server License, Tier 3	License	1	1	1	1	1	1	1	1	1	1
Symantec	Veritas NetBackup Windows Client, Tier 4	License	2	2	2	2	2	2	2	2	2	2
Tone Software Corp.	Dynastep	License	1	1	1	1	1	1	1	1	1	1
Unicon Group Ltd.	LOUIS II LCOM Host Module	License	1	1	1	1	1	1	1	1	1	1
Unicon Group Ltd.	LOUIS II Extract & Reporting Module	License	1	1	1	1	1	1	1	1	1	1
Unicon Group Ltd.	LOUIS II DERIVE Option	License	2	2	2	2	2	2	2	2	2	2
Unicon Group Ltd.	LOUIS II DMS Interface	License	1	1	1	1	1	1	1	1	1	1
Unicon Group Ltd.	LOUIS II RDMS Interface	License	1	1	1	1	1	1	1	1	1	1
Unicon Group Ltd.	LOUIS II RELATE Option	License	2	2	2	2	2	2	2	2	2	2
VanDyke Technologies	VShell Workgroup Server	License	6	6	6	6	6	6	6	6	6	6
Veeam	nWorks ESX Monitoring for SCOM	License	32	32	32	32	32	32	32	32	32	32
Veeam	nWorks Management Pack for VMWare	License	62	62	62	62	62	62	62	62	62	62

Baseline Units - Volumetrics

Note: The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all inclusive representation of every service desired by the Commonwealth.

Resource Description	Service Tier / Configuration (6)	Units	Year 1 Qty	Year 2 Qty	Year 3 Qty	Year 4 Qty	Year 5 Qty	Year 6 Qty	Year 7 Qty	Opt - Year 8 Qty	Opt - Year 9 Qty	Opt - Year 10 Qty
VMware, Inc.	VMware vSphere 4 Enterprise Plus for 1 Processor	License	8	8	8	8	8	8	8	8	8	8
VMware, Inc.	VMware vSphere 5 Enterprise Plus for 1 Processor	License	16	16	16	16	16	16	16	16	16	16
~~Western American Data~~	~~Rlist~~	~~License~~	0	0	0	0	0	0	0	0	0	0
Winternals	Winternals Administrator's Pak	License	1	1	1	1	1	1	1	1	1	1
WinZip Computing	Winzip	License	59	59	59	59	59	59	59	59	59	59
XtremeSoft	AppMetrics	License	1	1	1	1	1	1	1	1	1	1
USPS	Correct Address	License	1	1	1	1	1	1	1	1	1	1
IBM	FileNet	License	1	1	1	1	1	1	1	1	1	1
Microsoft	SharePoint (with SA)	License	2	2	2	2	2	2	2	2	2	2
IBM	WebSphere MQ (Procesor Value Unit)	License	1	1	1	1	1	1	1	1	1	1
Xerox	XeroxDocuShare	License	1	1	1	1	1	1	1	1	1	1
Hybrid Third Party Software												
Vendor	**Product**											
Computer Associates International, Inc.	CA 90's Services (freeware)	License	3	3	3	3	3	3	3	3	3	3
Computer Associates International, Inc.	Vision Builder	License	1	1	1	1	1	1	1	1	1	1
Computer Associates International, Inc.	Easytrieve Plus	License	1	1	1	1	1	1	1	1	1	1
Computer Associates International, Inc.	Easytrieve Plus MVS	License	1	1	1	1	1	1	1	1	1	1
Computer Associates International, Inc.	Easytrieve Plus IMS	License	1	1	1	1	1	1	1	1	1	1
Computer Associates International, Inc.	Easytrieve Plus IMS Option MVS	License	1	1	1	1	1	1	1	1	1	1
Computer Associates International, Inc.	Easytrieve Plus DB2 OPT	License	1	1	1	1	1	1	1	1	1	1
Computer Associates International, Inc.	Easytrieve Plus DB2 Option MVS	License	1	1	1	1	1	1	1	1	1	1
Computer Associates International, Inc.	Endevor/MVS Automated Configura ion Mgr MVS	License	1	1	1	1	1	1	1	1	1	1
Computer Associates International, Inc.	Endevor/MVS External Security Int. MVS	License	1	1	1	1	1	1	1	1	1	1
Computer Associates International, Inc.	Endevor/MVS MVS	License	1	1	1	1	1	1	1	1	1	1
Computer Associates International, Inc.	Endevor/MVS Extended Processor	License	1	1	1	1	1	1	1	1	1	1
Computer Associates International, Inc.	CA-Librarian	License	1	1	1	1	1	1	1	1	1	1
Computer Associates International, Inc.	CA-META COBOL	License	1	1	1	1	1	1	1	1	1	1
Computer Associates International, Inc.	Panvalet	License	1	1	1	1	1	1	1	1	1	1
Computer Associates International, Inc.	Panvalet ISPF	License	1	1	1	1	1	1	1	1	1	1
Computer Associates International, Inc.	SORT (INCL DART)	License	1	1	1	1	1	1	1	1	1	1
Computer Associates International, Inc.	SRAM	License	1	1	1	1	1	1	1	1	1	1
dotJ Software Inc.	dotJ Custom Tag Library	License	1	1	1	1	1	1	1	1	1	1
Formula Consultants, Inc.	Star 1100	License	3	3	3	3	3	3	3	3	3	3
Idea Integration	XGEN	License	1	1	1	1	1	1	1	1	1	1
Informatica Corporation	Change DataMove for DB2 Source	License	1	1	1	1	1	1	1	1	1	1
Informatica Corporation	DataMove for DB2 Source	License	1	1	1	1	1	1	1	1	1	1
Informatica Corporation	Change DataMove	License	1	1	1	1	1	1	1	1	1	1
Informatica Corporation	DataMove for IMS Source	License	1	1	1	1	1	1	1	1	1	1
Informatica Corporation	Change DataMove for IMS Source	License	1	1	1	1	1	1	1	1	1	1
Informatica Corporation	DataMove	License	1	1	1	1	1	1	1	1	1	1
Informatica Corporation	Change DataMove DB2 Target	License	1	1	1	1	1	1	1	1	1	1
Informatica Corporation	DataMove DB2 Target	License	1	1	1	1	1	1	1	1	1	1
Informatica Corporation	Change DataMove/DataMove Target for UDB	License	1	1	1	1	1	1	1	1	1	1
Informatica Corporation	SSA - Name 3	License	1	1	1	1	1	1	1	1	1	1

Baseline Units - Volumetrics

Note: The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all inclusive representation of every service desired by the Commonwealth.

Resource Description	Service Tier / Configuration (6)	Units	Year 1 Qty	Year 2 Qty	Year 3 Qty	Year 4 Qty	Year 5 Qty	Year 6 Qty	Year 7 Qty	Opt - Year 8 Qty	Opt - Year 9 Qty	Opt - Year 10 Qty
KMSYS Worldwide, Inc.	IQU Plus-1	License	5	5	5	5	5	5	5	5	5	5
KMSYS Worldwide, Inc.	IQU Reorg Composer	License	1	1	1	1	1	1	1	1	1	1
KMSYS Worldwide, Inc.	QPLXSS	License	350	350	350	350	350	350	350	350	350	350
KMSYS Worldwide, Inc.	QPLXSV	License	1	1	1	1	1	1	1	1	1	1
KMSYS Worldwide, Inc.	QPLXV	License	1	1	1	1	1	1	1	1	1	1
~~Marble Computer Inc.~~	~~OS DCD III Data Correlation and Documentation System~~	~~License~~	0	0	0	0	0	0	0	0	0	0
Microsoft	SQL Server Enterprise	License	2	2	2	2	2	2	2	2	2	2
SAS Institute, Inc.	Base SAS	License	1	1	1	1	1	1	1	1	1	1
SAS Institute, Inc.	SAS/ACCESS Interface for IMS	License	1	1	1	1	1	1	1	1	1	1
SAS Institute, Inc.	SAS/ACCESS DB2	License	1	1	1	1	1	1	1	1	1	1
SAS Institute, Inc.	SAS/AF	License	1	1	1	1	1	1	1	1	1	1
SAS Institute, Inc.	SAS/FSP	License	1	1	1	1	1	1	1	1	1	1
SAS Institute, Inc.	SAS/GRAPH	License	1	1	1	1	1	1	1	1	1	1
SAS Institute, Inc.	SAS/SHARE	License	1	1	1	1	1	1	1	1	1	1
SAS Institute, Inc.	SAS/STAT	License	1	1	1	1	1	1	1	1	1	1
~~Schema Systems Limited~~	~~Q Editor Plus One~~	~~License~~	0	0	0	0	0	0	0	0	0	0
SMA	OpCon/xps EXEC LSAM, Group 3	License	1	1	1	1	1	1	1	1	1	1
SMA	OpCon/xps EXEC LSAM, Group 8	License	1	1	1	1	1	1	1	1	1	1
SMA	OpCon/xps EXEC LSAM, Group 14	License	1	1	1	1	1	1	1	1	1	1
SMA	OpCon/xps Microsoft LSAM	License	5	5	5	5	5	5	5	5	5	5
SMA	OpCon/xps User Interface	License	15	15	15	15	15	15	15	15	15	15
Sybase	EAServer Deploy Advanced - Active	License	2	2	2	2	2	2	2	2	2	2
Sybase	EAServer Deploy Advanced - Passive	License	2	2	2	2	2	2	2	2	2	2
TRILOGexport, Inc.	TriTune Automation Component (APC)	License	1	1	1	1	1	1	1	1	1	1
Unicon Group Ltd.	LOUIS II Database Gateway	License	2	2	2	2	2	2	2	2	2	2
Unicon Group Ltd.	LOUIS II DMS Interface	License	3	3	3	3	3	3	3	3	3	3
Unicon Group Ltd.	LOUIS II Extract & Reporting Module	License	1	1	1	1	1	1	1	1	1	1
Unicon Group Ltd.	LOUIS II LCOM Host Module	License	3	3	3	3	3	3	3	3	3	3
Unicon Group Ltd.	LOUIS II MAPPER Interface	License	1	1	1	1	1	1	1	1	1	1
Unicon Group Ltd.	LOUIS II RDMS Interface	License	3	3	3	3	3	3	3	3	3	3
Verisign	Secure Site Pro SSL	License	2	2	2	2	2	2	2	2	2	2
~~Western American Data~~	~~Rlist~~	~~License~~	0	0	0	0	0	0	0	0	0	0
WinZip	Self-Extractor 10-user license	License	2	2	2	2	2	2	2	2	2	2
Total Third Party Software			**54,383**	**54,383**	**54,383**	**54,383**	**54,383**	**54,383**	**54,383**	**54,383**	**54,383**	**54,383**

Baseline Units - Volumetrics

Note: The Commonwealth has established mult

Price per unit \ per month

Resource Description	Service Tier / Configuration (6)	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Server - Fully Managed (1)											
x86 (Windows, Linux) - Physical Servers											
	Platinum Tier										
	Windows pConfig - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows pConfig - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows pConfig - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows pConfig - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows pConfig - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux pConfig - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux pConfig - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux pConfig - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux pConfig - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux pConfig - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
sub-total x86 (Windows, Linux) - Physical Servers - Plantinum		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
	Gold Tier										
	Windows pConfig - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows pConfig - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows pConfig - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows pConfig - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows pConfig - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux pConfig - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux pConfig - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux pConfig - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux pConfig - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux pConfig - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
sub-total x86 (Windows, Linux) - Physical Servers - Gold		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
	Silver Tier										
	Windows pConfig - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows pConfig - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows pConfig - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows pConfig - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows pConfig - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux pConfig - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux pConfig - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux pConfig - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux pConfig - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux pConfig - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
sub-total x86 (Windows, Linux) - Physical Servers - Silver		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
	Bronze Tier										
	Windows pConfig - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows pConfig - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows pConfig - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows pConfig - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows pConfig - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux pConfig - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux pConfig - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -

Note: The Commonwealth has established mult

Baseline Units - Volumetrics

Price per unit \ per month

Resource Description	Service Tier / Configuration (6)	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
	Linux pConfig - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux pConfig - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux pConfig - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
sub-total x86 (Windows, Linux) - Physical Servers - Bronze		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
	Basic Tier										
	Windows pConfig - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows pConfig - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows pConfig - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows pConfig - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows pConfig - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux pConfig - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux pConfig - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux pConfig - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux pConfig - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux pConfig - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
sub-total x86 (Windows, Linux) - Physical Servers - Basic		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Total - Fully Managed - x86 Physical - All Support Tiers (Window, Linux)		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
x86 (Windows, Linux) - Virtual Servers											
	Platinum Tier										
	Windows vConfig - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows vConfig - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows vConfig - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows vConfig - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows vConfig - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux vConfig - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux vConfig - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux vConfig - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux vConfig - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux vConfig - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
sub-total x86 (Windows, Linux) - Virtual Servers - Platinum		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
	Gold Tier										
	Windows vConfig - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows vConfig - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows vConfig - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows vConfig - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows vConfig - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux vConfig - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux vConfig - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux vConfig - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux vConfig - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux vConfig - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
sub-total x86 (Windows, Linux) - Virtual Servers - Gold		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
	Silver Tier										
	Windows vConfig - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows vConfig - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -

Note: The Commonwealth has established mult

Baseline Units - Volumetrics

Price per unit \ per month

Resource Description	Service Tier / Configuration (6)	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
	Windows vConfig - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows vConfig - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows vConfig - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux vConfig - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux vConfig - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux vConfig - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux vConfig - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux vConfig - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
sub-total x86 (Windows, Linux) - Virtual Servers - Silver		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
	Bronze Tier										
	Windows vConfig - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows vConfig - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows vConfig - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows vConfig - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows vConfig - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux vConfig - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux vConfig - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux vConfig - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux vConfig - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux vConfig - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
sub-total x86 (Windows, Linux) - Virtual Servers - Bronze		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
	Basic Tier										
	Windows vConfig - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows vConfig - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows vConfig - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows vConfig - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows vConfig - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux vConfig - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux vConfig - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux vConfig - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux vConfig - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux vConfig - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
sub-total x86 (Windows, Linux) - Virtual Servers - Basic		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Total - Fully Managed - x86 Virtual - All Support Tiers (Window, Linux)		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
UNIX (IBM P-Series, AIX)											
	Platinum Tier										
	AIX Config - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	AIX Config - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	AIX Config - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	AIX Config - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	AIX Config - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
sub-total P-Series (AIX) - Bronze		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
	Gold Tier										
	AIX Config - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	AIX Config - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -

Baseline Units - Volumetrics

Note: The Commonwealth has established mult

Price per unit \ per month

Resource Description	Service Tier / Configuration (6)	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
	AIX Config - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	AIX Config - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	AIX Config - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
sub-total P-Series (AIX) - Gold		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
	Silver Tier										
	AIX Config - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	AIX Config - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	AIX Config - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	AIX Config - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	AIX Config - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
sub-total P-Series (AIX) - Silver		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
	Bronze Tier										
	AIX Config - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	AIX Config - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	AIX Config - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	AIX Config - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	AIX Config - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
sub-total P-Series (AIX) - Bronze		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
	Basic Tier										
	AIX Config - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	AIX Config - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	AIX Config - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	AIX Config - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	AIX Config - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
sub-total P-Series (AIX) - Basic		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Total - Fully Managed - P-Series (AIX) - All Support Tiers (Window, Linux)		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Server - Managed Only (2)											
x86 (Windows, Linux)											
	Platinum Tier	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Gold Tier	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Silver Tier	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Bronze Tier	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Basic Tier	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Total Managed Only- x86 - All Support Tiers (Window, Linux)		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
UNIX (IBM P-Series, AIX)											
	Platinum	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Gold Tier	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Silver Tier	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Bronze Tier	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Basic Tier	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Total Managed Only- P-Series - All Support Tiers (AIX)		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Storage and Backup - Fully Managed (1)											

Note: The Commonwealth has established mult

Baseline Units - Volumetrics

Price per unit \ per month

Resource Description	Service Tier / Configuration (6)	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Enterprise Storage											
	* Dedicated - Config 1 - SAN Raid 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	* Dedicated - Config 2 - SAN Raid 10	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Dedicated - Config 3 - Net Attached	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Total Enterprise Storage - Fully Managed		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Tape and Backup											
	** Server Tape Stored	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	** Offsite Tape Storage	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Total Tape and Backup - Fully Managed		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Limited Co-Lo (Data Center Only Charge) (3)											
Server, Storage, Network, Security Equipment											
	Co-Lo Config - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Co-Lo Config - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Co-Lo Config - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Total Limited Co-Lo (Data Center Only Charge)		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Mainframe Services (4)											
IBM Services											
	*** IBM Mainframe Allocated DASD	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IBM Tapes in Storage - VTS	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IBM Offsite Tape Storage	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Total IBM Services		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
IBM Configurations											
	Platinum Tier										
	IBM Mainframe Config - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IBM Mainframe Config - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IBM Mainframe Config - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IBM AS400 Config 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IBM AS400 Config 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
sub-total IBM Mainfram Services - Plantinum		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
	Gold Tier										
	IBM Mainframe Config - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IBM Mainframe Config - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IBM Mainframe Config - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IBM AS400 Config 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IBM AS400 Config 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
sub-total IBM Mainfram Services - Gold		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
	Basic Tier										
	IBM Mainframe Config - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IBM Mainframe Config - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IBM Mainframe Config - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IBM AS400 Config 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IBM AS400 Config 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
sub-total IBM Mainfram Services - Basic		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**

Note: The Commonwealth has established mult

Baseline Units - Volumetrics

Price per unit \ per month

Resource Description	Service Tier / Configuration (6)	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Total - IBM Mainframe Services - All Support Tiers		$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unisys Services											
	*** Unisys DASD	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Unisys Tapes in Storage - VTS	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Unisys Offsite Tape Storage	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Total Unisys Services		$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unisys Configurations											
	Platinum Tier										
	Unisys Mainframe Config - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Unisys Mainframe Config - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Unisys Mainframe Config - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Unisys Mainframe Config - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
sub-total Unisys Mainfram Services - Plantinum		$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Gold Tier										
	Unisys Mainframe Config - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Unisys Mainframe Config - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Unisys Mainframe Config - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Unisys Mainframe Config - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
sub-total Unisys Mainfram Services - Gold		$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Basic Tier										
	Unisys Mainframe Config - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Unisys Mainframe Config - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Unisys Mainframe Config - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Unisys Mainframe Config - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
sub-total Unisys Mainfram Services - Basic		$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Total - Unisys Mainframe Services - All Support Tiers		$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
On-Demand (IaaS) (5)											
IaaS Servers - x86 (Windows, Linux) - Virtual Servers											
	IaaS Windows vConfig - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IaaS Windows vConfig - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IaaS Windows vConfig - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IaaS Windows vConfig - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IaaS Windows vConfig - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IaaS Linux vConfig - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IaaS Linux vConfig - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IaaS Linux vConfig - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IaaS Linux vConfig - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IaaS Linux vConfig - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Total IaaS Servers - x86 (Windows, Linux) - Virtual Servers		$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Storage On-Demand											
	IaaS Storage Config - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IaaS Storage Config - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IaaS Storage Config - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -

Baseline Units - Volumetrics

Note: The Commonwealth has established mult

Price per unit \ per month

Resource Description	Service Tier / Configuration (6)	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Total IaaS Storage On-Demand		$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Backup On-Demand											
	IaaS Backup Config - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Total IaaS Backup On-Demand		$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Reserve Account											
		$ 84,000 00	$ 84,000 00	$ 84,000 00	$ 84,000 00	$ 84,000 00	$ 84,000 00	$ 84,000 00	$ 84,000 00	$ 84,000 00	$ 84,000 00
Reserve Account		**$ 84,000.00**	**$ 84,000.00**	**$ 84,000.00**	**$ 84,000.00**	**$ 84,000.00**	**$ 84,000.00**	**$ 84,000.00**	**$ 84,000.00**	**$ 84,000.00**	**$ 84,000.00**

Notes:

For purposes of submitting a proposal, Offerors should assume that tapes are equivalent in ca

* For purposes of submitting a proposal, Offerors should assume that the slower Tier1 RAID5

** The volume is expressed as native.

*** For purposes of evaluation DASD is expressed in Usable (not Raw)

Third Party Software

Third Party Software

Vendor	Product										
B & L	BL/LIB Tape Library Management System	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
B & L	BL/SCHED Scheduling & Monitoring System	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	BMC AppSight for Windows/.NET - Division Edition	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	BMC AppSight Named Users	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	BMC AppSight QA Users	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	CONTROL-M Enterprise Manager	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	CONTROL-M Full Admin User	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	CONTROL-M Tasks (100 Tasks per Unit)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Database Director (D2)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iBuild	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iChange	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iCheck	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iCopy	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iExtract	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iLM	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iLoad	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iRecover	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iSurvey	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iUnload	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Mission Control	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Business Objects	Crystal Reports	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Bytware Inc.	StandGuard Anti-Virus	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Citrix	XenApp Advanced (User Counts)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Citrix	XenApp Enterprise (User Counts)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	CA-Explore for CICS	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -

Note: The Commonwealth has established mult

Baseline Units - Volumetrics

Price per unit \ per month

Resource Description	Service Tier / Configuration (6)	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Computer Associates International, Inc.	SOA Security Manager	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	SOA Security Manager Additional Secured Web Services	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	SOA Security Manager Additional Users	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Cor icon Technologies	Corticon Business Rules Server – Unlimited CPUs	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Cor icon Technologies	Corticon Server – per Non-Production Server	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Cor icon Technologies	Corticon Business Rules Modeling Studio – per Named User	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
CSI International	EPIC	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
CSI International	FAQS/PCS	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
CSI International	FAQS/ASO	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
EMC Corporation	PowerPath	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
EMC Corporation	PowerPath (per CPU)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
EMC Corporation	Symmetrix® VMAX Fully Automated Storage Tiering for Virtual Pools (FAST VP)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
EMC Corporation	Vsphere Enterprise Plus	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Experian QAS	NameSearch - Production (Licensed per Server up to 8 CPU)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Experian QAS	NameSearch - Non-Production (Licensed per Server)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Formula Consultants, Inc.	Star 1100	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
GlobalScape	CuteFTP Pro 2.0	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
HELPSYS	Robot/Schedule	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Idea Integration	XGEN	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	SSA-Name 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Infragistics	NetAdvantage for .NET	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
KMSYS Worldwide, Inc.	lQU Plus-1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Levi, Ray and Shoup	VPS/PCL	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Levi, Ray and Shoup	VPS/TCP/IP	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Levi, Ray and Shoup	VPS/DRS	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Levi, Ray and Shoup	VPS	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
MacKinney Systems, Inc.	CICS Response Time Monitor	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
~~Marble Computer, Inc.~~	~~OS DCD III Data Correlation and Documentation System~~	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	BizTalk Adaptor for MQSeries	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	BizTalk Server Enterprise (Single Processor)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	BizTalk Server Standard (Single Processor)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	SQL Server CAL	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	SQL Server Enterprise (Single Processor)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	SQL Server Enterprise	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	SQL Server Standard (Single Processor)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	SQL Server Standard	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	SQL Server Standard per 2-Core	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	Visual Studio Foundation Server	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -

Baseline Units - Volumetrics

Note: The Commonwealth has established mult

Price per unit \ per month

Resource Description	Service Tier / Configuration (6)	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Microsoft	Visual Studio Foundation Server CAL	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	Visual Studio Professional with MSDN	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	Windows Server Datacenter Edition (Single Processor)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	Windows Server Enterprise Edition	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	Windows Server Standard Edition	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	Windows Terminal Service Client Access Licenses	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Network Associates	McAfee Anti-Virus	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Novell	Platespin Migrator	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Novell	SuSE Linux	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
OpenText	Metastorm Integration Manager for CICS (MIM for CICS)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Oracle	Oracle Change Management Pack	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Oracle	Oracle Database 10g Enterprise	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Oracle	Oracle Database Enterprise Edition	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Oracle	Oracle Diagnos ic Pack	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Oracle	Oracle Enterprise Linux	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Oracle	Oracle Exadata Storage Software	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Oracle	Oracle Partitioning	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Oracle	Oracle Tuning Pack	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Oracle	Real Application Cluster - Processor Perpetual	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Oracle	Spatial and Graph - Processor Perpetual	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Pitney Bowes	Finalist (Doc Sense)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Pitney Bowes	CODE-1 Plus	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Pitney Bowes	CODE-1 Plus (Test / Development)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Pitney Bowes	Online Window for Finalist	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Quest	Central Performance Suite for SQL Server, Tier A	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Quest	Central Performance Suite for SQL Server, Tier B	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Quest	Foglight Database Management Suite for SQL Server	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Quest	Foglight for SQL Server per CPU Socket	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Quest	Foglight OS Management per CPU Socket	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Quest	Foglight Server for FSM	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
RealVNC	VNC Enterprise Edition for Windows	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Red Hat	Red Hat Enterprise Linux	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
~~Schema Systems Limited~~	~~Q Editor Plus One~~	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Segus Inc.	OPC/Graph	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG20	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG40	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG60	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG80	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -

Baseline Units - Volumetrics

Note: The Commonwealth has established mult

Price per unit \ per month

Resource Description	Service Tier / Configuration (6)	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG130	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG20	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG40	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG60	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG80	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG130	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG140	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - MAPPER, SWG20	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - MAPPER, SWG40	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - MAPPER, SWG60	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - MAPPER, SWG80	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - MAPPER, SWG130	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG20	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG40	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG60	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG80	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG130	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG140	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - System Log, SWG20	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - System Log, SWG40	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - System Log, SWG60	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - System Log, SWG80	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - System Log, SWG130	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - System Log, SWG140	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG20	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG40	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG60	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -

Baseline Units - Volumetrics

Note: The Commonwealth has established mult

Price per unit \ per month

Resource Description	Service Tier / Configuration (6)	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG80	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG130	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG140	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Power Agent, SWG20	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Power Agent, SWG40	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Power Agent, SWG60	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Power Agent, SWG80	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Power Agent, SWG130	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Power Agent, SWG140	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Torch Capacity Manager Power Agent, SWG40	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Torch Capacity Manager Power Agent, SWG60	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Torch Capacity Manager Power Agent, SWG130	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Torch Capacity Manager Power Agent, SWG140	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Torch Interface Agent - I/O TRACE, SWG40	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Torch Interface Agent - I/O TRACE, SWG60	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Torch Interface Agent - I/O TRACE, SWG130	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Torch Interface Agent - LOG, SWG40	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Torch Interface Agent - LOG, SWG60	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Torch Interface Agent - LOG, SWG130	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Torch Interface Agent - LOG, SWG140	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Torch Interface Agent - MAPPER, SWG40	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Torch Interface Agent - MAPPER, SWG60	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Torch Interface Agent - MAPPER, SWG130	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	Windows 2000 Interface Agent - Internet Informa ion Server	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	Windows 2000 Interface Agent - .NET	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	Windows 2000 Interface Agent - SQL Server	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	Windows 2000 Power Agent Upto 32 CPU's	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SMA	OpCon/xps EXEC LSAM, Group 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SMA	OpCon/xps EXEC LSAM, Group 12	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SMA	OpCon/xps EXEC LSAM Development, Group 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SMA	OpCon/xps EXEC LSAM Development, Group 12	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -

Baseline Units - Volumetrics

Note: The Commonwealth has established mult

Price per unit \ per month

Resource Description	Service Tier / Configuration (6)	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
SMA	OpCon/xps Production SAM	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SMA	OpCon/xps Starter Kit	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SMA	OpCon/xps User Interface	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sybase	EAServer Deploy Advanced - Active	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sybase	EAServer Deploy Advanced - Passive	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	Backup Exec System Recovery Server	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	EndPoint Protection	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	Ghost Solution Suite	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Client Application and Database Pack, UNX, Tier 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Client Application and Database Pack, UNX, Tier 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Client Application and Database Pack, WIN, Tier 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Client Application and Database Pack, WIN, Tier 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Client Application and Database Pack, WIN, Tier 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Enterprise Client, UNX, Tier 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Enterprise Client, WIN, Tier 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Enterprise Client, WIN, Tier 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Enterprise Client, WIN, Tier 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Enterprise Server, WIN, Tier 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Enterprise Server, WIN, Tier 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Library Based Tape Drive Option, XPLAT	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Media Server Encryption Option (MSEO) WIN, Tier 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Platform Base, XPLAT (per Terabyte)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Shared Storage Option, XPLAT	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Standard Client, XPLAT	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Vault Additional Drive Option, XPLAT	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Vault Base Option, XPLAT (4 tape drives per license)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	Veritas NetBackup Enterprise Server License, Tier 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	Veritas NetBackup Windows Client, Tier 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Tone Software Corp.	Dynastep	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unicon Group Ltd.	LOUIS II LCOM Host Module	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unicon Group Ltd.	LOUIS II Extract & Reporting Module	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unicon Group Ltd.	LOUIS II DERIVE Option	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unicon Group Ltd.	LOUIS II DMS Interface	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unicon Group Ltd.	LOUIS II RDMS Interface	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unicon Group Ltd.	LOUIS II RELATE Option	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
VanDyke Technologies	VShell Workgroup Server	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Veeam	nWorks ESX Monitoring for SCOM	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Veeam	nWorks Management Pack for VMWare	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -

Baseline Units - Volumetrics

Note: The Commonwealth has established mult

Price per unit \ per month

Resource Description	Service Tier / Configuration (6)	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
VMware, Inc.	VMware vSphere 4 Enterprise Plus for 1 Processor	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
VMware, Inc.	VMware vSphere 5 Enterprise Plus for 1 Processor	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
~~Western American Data~~	~~Rlist~~	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Winternals	Winternals Administrator's Pak	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
WinZip Computing	Winzip	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
XtremeSoft	AppMetrics	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
USPS	Correct Address	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IBM	FileNet	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	SharePoint (with SA)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IBM	WebSphere MQ (Procesor Value Unit)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Xerox	XeroxDocuShare	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Hybrid Third Party Software											
Vendor	**Product**										
Computer Associates International, Inc.	CA 90's Services (freeware)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	Vision Builder	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	Easytrieve Plus	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	Easytrieve Plus MVS	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	Easytrieve Plus IMS	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	Easytrieve Plus IMS Option MVS	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	Easytrieve Plus DB2 OPT	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	Easytrieve Plus DB2 Option MVS	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	Endevor/MVS Automated Configura ion Mgr MVS	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	Endevor/MVS External Security Int. MVS	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	Endevor/MVS MVS	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	Endevor/MVS Extended Processor	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	CA-Librarian	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	CA-META COBOL	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	Panvalet	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	Panvalet ISPF	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	SORT (INCL DART)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	SRAM	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
dotJ Software Inc.	dotJ Custom Tag Library	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Formula Consultants, Inc.	Star 1100	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Idea Integration	XGEN	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	Change DataMove for DB2 Source	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	DataMove for DB2 Source	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	Change DataMove	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	DataMove for IMS Source	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	Change DataMove for IMS Source	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	DataMove	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	Change DataMove DB2 Target	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	DataMove DB2 Target	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	Change DataMove/DataMove Target for UDB	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	SSA - Name 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -

Baseline Units - Volumetrics

Note: The Commonwealth has established mult

Price per unit \ per month

Resource Description	Service Tier / Configuration (6)	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
KMSYS Worldwide, Inc.	IQU Plus-1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
KMSYS Worldwide, Inc.	IQU Reorg Composer	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
KMSYS Worldwide, Inc.	QPLXSS	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
KMSYS Worldwide, Inc.	QPLXSV	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
KMSYS Worldwide, Inc.	QPLXV	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
~~Marble Computer Inc.~~	~~OS DCD III Data Correlation and Documentation System~~	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	SQL Server Enterprise	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SAS Institute, Inc.	Base SAS	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SAS Institute, Inc.	SAS/ACCESS Interface for IMS	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SAS Institute, Inc.	SAS/ACCESS DB2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SAS Institute, Inc.	SAS/AF	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SAS Institute, Inc.	SAS/FSP	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SAS Institute, Inc.	SAS/GRAPH	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SAS Institute, Inc.	SAS/SHARE	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SAS Institute, Inc.	SAS/STAT	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
~~Schema Systems Limited~~	~~Q Editor Plus One~~	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SMA	OpCon/xps EXEC LSAM, Group 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SMA	OpCon/xps EXEC LSAM, Group 8	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SMA	OpCon/xps EXEC LSAM, Group 14	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SMA	OpCon/xps Microsoft LSAM	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SMA	OpCon/xps User Interface	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sybase	EAServer Deploy Advanced - Active	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sybase	EAServer Deploy Advanced - Passive	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
TRILOGexport, Inc.	TriTune Automation Component (APC)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unicon Group Ltd.	LOUIS II Database Gateway	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unicon Group Ltd.	LOUIS II DMS Interface	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unicon Group Ltd.	LOUIS II Extract & Reporting Module	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unicon Group Ltd.	LOUIS II LCOM Host Module	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unicon Group Ltd.	LOUIS II MAPPER Interface	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unicon Group Ltd.	LOUIS II RDMS Interface	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Verisign	Secure Site Pro SSL	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
~~Western American Data~~	~~Rlist~~	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
WinZip	Self-Extractor 10-user license	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Total Third Party Software		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**

Note: The Commonwealth has established mult

Baseline Units - Volumetrics

Resource Description	Service Tier / Configuration (6)	Annual Costs Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Server - Fully Managed (1)											
x86 (Windows, Linux) - Physical Servers											
	Platinum Tier										
	Windows pConfig - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows pConfig - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows pConfig - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows pConfig - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows pConfig - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux pConfig - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux pConfig - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux pConfig - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux pConfig - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux pConfig - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
sub-total x86 (Windows, Linux) - Physical Servers - Plantinum		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
	Gold Tier										
	Windows pConfig - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows pConfig - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows pConfig - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows pConfig - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows pConfig - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux pConfig - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux pConfig - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux pConfig - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux pConfig - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux pConfig - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
sub-total x86 (Windows, Linux) - Physical Servers - Gold		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
	Silver Tier										
	Windows pConfig - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows pConfig - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows pConfig - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows pConfig - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows pConfig - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux pConfig - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux pConfig - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux pConfig - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux pConfig - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux pConfig - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
sub-total x86 (Windows, Linux) - Physical Servers - Silver		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
	Bronze Tier										
	Windows pConfig - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows pConfig - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows pConfig - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows pConfig - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows pConfig - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux pConfig - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux pConfig - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -

Note: The Commonwealth has established mult

Baseline Units - Volumetrics

Resource Description	Service Tier / Configuration (6)	Annual Costs Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
	Linux pConfig - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux pConfig - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux pConfig - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
sub-total x86 (Windows, Linux) - Physical Servers - Bronze		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
	Basic Tier										
	Windows pConfig - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows pConfig - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows pConfig - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows pConfig - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows pConfig - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux pConfig - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux pConfig - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux pConfig - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux pConfig - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux pConfig - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
sub-total x86 (Windows, Linux) - Physical Servers - Basic		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Total - Fully Managed - x86 Physical - All Support Tiers (Window, Linux)		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
x86 (Windows, Linux) - Virtual Servers											
	Platinum Tier										
	Windows vConfig - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows vConfig - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows vConfig - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows vConfig - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows vConfig - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux vConfig - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux vConfig - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux vConfig - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux vConfig - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux vConfig - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
sub-total x86 (Windows, Linux) - Virtual Servers - Platinum		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
	Gold Tier										
	Windows vConfig - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows vConfig - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows vConfig - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows vConfig - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows vConfig - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux vConfig - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux vConfig - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux vConfig - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux vConfig - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux vConfig - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
sub-total x86 (Windows, Linux) - Virtual Servers - Gold		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
	Silver Tier										
	Windows vConfig - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows vConfig - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -

Note: The Commonwealth has established mult

Baseline Units - Volumetrics

Resource Description	Service Tier / Configuration (6)	Annual Costs Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
	Windows vConfig - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows vConfig - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows vConfig - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux vConfig - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux vConfig - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux vConfig - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux vConfig - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux vConfig - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
sub-total x86 (Windows, Linux) - Virtual Servers - Silver		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
	Bronze Tier										
	Windows vConfig - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows vConfig - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows vConfig - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows vConfig - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows vConfig - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux vConfig - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux vConfig - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux vConfig - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux vConfig - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux vConfig - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
sub-total x86 (Windows, Linux) - Virtual Servers - Bronze		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
	Basic Tier										
	Windows vConfig - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows vConfig - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows vConfig - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows vConfig - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows vConfig - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux vConfig - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux vConfig - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux vConfig - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux vConfig - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Linux vConfig - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
sub-total x86 (Windows, Linux) - Virtual Servers - Basic		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Total - Fully Managed - x86 Virtual - All Support Tiers (Window, Linux)		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
UNIX (IBM P-Series, AIX)											
	Platinum Tier										
	AIX Config - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	AIX Config - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	AIX Config - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	AIX Config - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	AIX Config - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
sub-total P-Series (AIX) - Bronze		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
	Gold Tier										
	AIX Config - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	AIX Config - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -

Note: The Commonwealth has established mult

Baseline Units - Volumetrics

Resource Description	Service Tier / Configuration (6)	Annual Costs Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
	AIX Config - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	AIX Config - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	AIX Config - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
sub-total P-Series (AIX) - Gold		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
	Silver Tier										
	AIX Config - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	AIX Config - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	AIX Config - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	AIX Config - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	AIX Config - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
sub-total P-Series (AIX) - Silver		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
	Bronze Tier										
	AIX Config - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	AIX Config - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	AIX Config - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	AIX Config - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	AIX Config - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
sub-total P-Series (AIX) - Bronze		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
	Basic Tier										
	AIX Config - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	AIX Config - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	AIX Config - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	AIX Config - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	AIX Config - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
sub-total P-Series (AIX) - Basic		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Total - Fully Managed - P-Series (AIX) - All Support Tiers (Window, Linux)		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Server - Managed Only (2)											
x86 (Windows, Linux)											
	Platinum Tier	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Gold Tier	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Silver Tier	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Bronze Tier	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Basic Tier	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Total Managed Only- x86 - All Support Tiers (Window, Linux)		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
UNIX (IBM P-Series, AIX)											
	Platinum	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Gold Tier	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Silver Tier	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Bronze Tier	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Basic Tier	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Total Managed Only- P-Series - All Support Tiers (AIX)		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Storage and Backup - Fully Managed (1)											

Note: The Commonwealth has established mult

Baseline Units - Volumetrics

Resource Description	Service Tier / Configuration (6)	Annual Costs Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Enterprise Storage											
	* Dedicated - Config 1 - SAN Raid 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	* Dedicated - Config 2 - SAN Raid 10	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Dedicated - Config 3 - Net Attached	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Total Enterprise Storage - Fully Managed		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Tape and Backup											
	** Server Tape Stored	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	** Offsite Tape Storage	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Total Tape and Backup - Fully Managed		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Limited Co-Lo (Data Center Only Charge) (3)											
Server, Storage, Network, Security Equipment											
	Co-Lo Config - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Co-Lo Config - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Co-Lo Config - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Total Limited Co-Lo (Data Center Only Charge)		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Mainframe Services (4)											
IBM Services											
	*** IBM Mainframe Allocated DASD	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IBM Tapes in Storage - VTS	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IBM Offsite Tape Storage	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Total IBM Services		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
IBM Configurations											
	Platinum Tier										
	IBM Mainframe Config - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IBM Mainframe Config - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IBM Mainframe Config - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IBM AS400 Config 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IBM AS400 Config 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
sub-total IBM Mainfram Services - Plantinum		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
	Gold Tier										
	IBM Mainframe Config - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IBM Mainframe Config - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IBM Mainframe Config - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IBM AS400 Config 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IBM AS400 Config 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
sub-total IBM Mainfram Services - Gold		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
	Basic Tier										
	IBM Mainframe Config - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IBM Mainframe Config - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IBM Mainframe Config - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IBM AS400 Config 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IBM AS400 Config 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
sub-total IBM Mainfram Services - Basic		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**

Note: The Commonwealth has established mult

Baseline Units - Volumetrics

Resource Description	Service Tier / Configuration (6)	Annual Costs Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Total - IBM Mainframe Services - All Support Tiers		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Unisys Services											
	*** Unisys DASD	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Unisys Tapes in Storage - VTS	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Unisys Offsite Tape Storage	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Total Unisys Services		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Unisys Configurations											
	Platinum Tier										
	Unisys Mainframe Config - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Unisys Mainframe Config - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Unisys Mainframe Config - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Unisys Mainframe Config - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
sub-total Unisys Mainfram Services - Plantinum		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
	Gold Tier										
	Unisys Mainframe Config - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Unisys Mainframe Config - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Unisys Mainframe Config - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Unisys Mainframe Config - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
sub-total Unisys Mainfram Services - Gold		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
	Basic Tier										
	Unisys Mainframe Config - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Unisys Mainframe Config - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Unisys Mainframe Config - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Unisys Mainframe Config - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
sub-total Unisys Mainfram Services - Basic		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Total - Unisys Mainframe Services - All Support Tiers		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
On-Demand (IaaS) (5)											
IaaS Servers - x86 (Windows, Linux) - Virtual Servers											
	IaaS Windows vConfig - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IaaS Windows vConfig - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IaaS Windows vConfig - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IaaS Windows vConfig - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IaaS Windows vConfig - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IaaS Linux vConfig - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IaaS Linux vConfig - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IaaS Linux vConfig - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IaaS Linux vConfig - 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IaaS Linux vConfig - 5	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Total IaaS Servers - x86 (Windows, Linux) - Virtual Servers		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
IaaS Storage On-Demand											
	IaaS Storage Config - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IaaS Storage Config - 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IaaS Storage Config - 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -

Note: The Commonwealth has established mult

Baseline Units - Volumetrics

Resource Description	Service Tier / Configuration (6)	Annual Costs Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Total IaaS Storage On-Demand		$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Backup On-Demand											
	IaaS Backup Config - 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Total IaaS Backup On-Demand		$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Reserve Account											
		$ 1,008,000 00	$ 1,008,000 00	$ 1,008,000 00	$ 1,008,000 00	$ 1,008,000 00	$ 1,008,000 00	$ 1,008,000 00	$ 1,008,000 00	$ 1,008,000 00	$ 1,008,000 00
Reserve Account		**$ 1,008,000.00**	**$ 1,008,000.00**	**$ 1,008,000.00**	**$ 1,008,000.00**	**$ 1,008,000.00**	**$ 1,008,000.00**	**$ 1,008,000.00**	**$ 1,008,000.00**	**$ 1,008,000.00**	**$ 1,008,000.00**

Notes:

For purposes of submitting a proposal, Offerors should assume that tapes are equivalent in ca

* For purposes of submitting a proposal, Offerors should assume that the slower Tier1 RAID5

** The volume is expressed as native.

*** For purposes of evaluation DASD is expressed in Usable (not Raw)

Third Party Software

Third Party Software

Vendor	Product										
B & L	BL/LIB Tape Library Management System	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
B & L	BL/SCHED Scheduling & Monitoring System	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	BMC AppSight for Windows/.NET - Division Edition	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	BMC AppSight Named Users	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	BMC AppSight QA Users	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	CONTROL-M Enterprise Manager	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	CONTROL-M Full Admin User	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	CONTROL-M Tasks (100 Tasks per Unit)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Database Director (D2)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iBuild	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iChange	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iCheck	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iCopy	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iExtract	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iLM	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iLoad	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iRecover	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iSurvey	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iUnload	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Mission Control	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Business Objects	Crystal Reports	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Bytware Inc.	StandGuard Anti-Virus	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Citrix	XenApp Advanced (User Counts)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Citrix	XenApp Enterprise (User Counts)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	CA-Explore for CICS	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -

Note: The Commonwealth has established mult

Baseline Units - Volumetrics

		Annual Costs									
Resource Description	**Service Tier / Configuration (6)**	**Year 1**	**Year 2**	**Year 3**	**Year 4**	**Year 5**	**Year 6**	**Year 7**	**Opt - Year 8**	**Opt - Year 9**	**Opt - Year 10**
Computer Associates International, Inc.	SOA Security Manager	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	SOA Security Manager Additional Secured Web Services	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	SOA Security Manager Additional Users	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Cor icon Technologies	Corticon Business Rules Server – Unlimited CPUs	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Cor icon Technologies	Corticon Server – per Non-Production Server	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Cor icon Technologies	Corticon Business Rules Modeling Studio – per Named User	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
CSI International	EPIC	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
CSI International	FAQS/PCS	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
CSI International	FAQS/ASO	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
EMC Corporation	PowerPath	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
EMC Corporation	PowerPath (per CPU)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
EMC Corporation	Symmetrix® VMAX Fully Automated Storage Tiering for Virtual Pools (FAST VP)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
EMC Corporation	Vsphere Enterprise Plus	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Experian QAS	NameSearch - Production (Licensed per Server up to 8 CPU)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Experian QAS	NameSearch - Non-Production (Licensed per Server)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Formula Consultants, Inc.	Star 1100	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
GlobalScape	CuteFTP Pro 2.0	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
HELPSYS	Robot/Schedule	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Idea Integration	XGEN	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	SSA-Name 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Infragistics	NetAdvantage for .NET	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
KMSYS Worldwide, Inc.	lQU Plus-1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Levi, Ray and Shoup	VPS/PCL	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Levi, Ray and Shoup	VPS/TCP/IP	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Levi, Ray and Shoup	VPS/DRS	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Levi, Ray and Shoup	VPS	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
MacKinney Systems, Inc.	CICS Response Time Monitor	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
~~Marble Computer, Inc.~~	~~OS DCD III Data Correlation and Documentation System~~	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	BizTalk Adaptor for MQSeries	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	BizTalk Server Enterprise (Single Processor)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	BizTalk Server Standard (Single Processor)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	SQL Server CAL	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	SQL Server Enterprise (Single Processor)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	SQL Server Enterprise	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	SQL Server Standard (Single Processor)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	SQL Server Standard	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	SQL Server Standard per 2-Core	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	Visual Studio Foundation Server	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -

Baseline Units - Volumetrics

Note: The Commonwealth has established mult

		Annual Costs									
Resource Description	**Service Tier / Configuration (6)**	**Year 1**	**Year 2**	**Year 3**	**Year 4**	**Year 5**	**Year 6**	**Year 7**	**Opt - Year 8**	**Opt - Year 9**	**Opt - Year 10**
Microsoft	Visual Studio Foundation Server CAL	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	Visual Studio Professional with MSDN	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	Windows Server Datacenter Edition (Single Processor)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	Windows Server Enterprise Edition	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	Windows Server Standard Edition	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	Windows Terminal Service Client Access Licenses	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Network Associates	McAfee Anti-Virus	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Novell	Platespin Migrator	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Novell	SuSE Linux	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
OpenText	Metastorm Integration Manager for CICS (MIM for CICS)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Oracle	Oracle Change Management Pack	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Oracle	Oracle Database 10g Enterprise	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Oracle	Oracle Database Enterprise Edition	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Oracle	Oracle Diagnos ic Pack	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Oracle	Oracle Enterprise Linux	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Oracle	Oracle Exadata Storage Software	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Oracle	Oracle Partitioning	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Oracle	Oracle Tuning Pack	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Oracle	Real Application Cluster - Processor Perpetual	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Oracle	Spatial and Graph - Processor Perpetual	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Pitney Bowes	Finalist (Doc Sense)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Pitney Bowes	CODE-1 Plus	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Pitney Bowes	CODE-1 Plus (Test / Development)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Pitney Bowes	Online Window for Finalist	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Quest	Central Performance Suite for SQL Server, Tier A	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Quest	Central Performance Suite for SQL Server, Tier B	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Quest	Foglight Database Management Suite for SQL Server	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Quest	Foglight for SQL Server per CPU Socket	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Quest	Foglight OS Management per CPU Socket	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Quest	Foglight Server for FSM	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
RealVNC	VNC Enterprise Edition for Windows	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Red Hat	Red Hat Enterprise Linux	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
~~Schema Systems Limited~~	~~Q Editor Plus One~~	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Segus Inc.	OPC/Graph	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG20	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG40	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG60	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG80	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -

Baseline Units - Volumetrics

Note: The Commonwealth has established mult

Resource Description	Service Tier / Configuration (6)	Annual Costs									
		Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG130	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG20	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG40	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG60	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG80	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG130	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG140	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - MAPPER, SWG20	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - MAPPER, SWG40	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - MAPPER, SWG60	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - MAPPER, SWG80	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - MAPPER, SWG130	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG20	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG40	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG60	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG80	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG130	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG140	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - System Log, SWG20	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - System Log, SWG40	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - System Log, SWG60	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - System Log, SWG80	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - System Log, SWG130	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - System Log, SWG140	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG20	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG40	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG60	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -

Baseline Units - Volumetrics

Note: The Commonwealth has established mult

Resource Description	Service Tier / Configuration (6)	Annual Costs									
		Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG80	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG130	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG140	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Power Agent, SWG20	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Power Agent, SWG40	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Power Agent, SWG60	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Power Agent, SWG80	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Power Agent, SWG130	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Power Agent, SWG140	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Torch Capacity Manager Power Agent, SWG40	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Torch Capacity Manager Power Agent, SWG60	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Torch Capacity Manager Power Agent, SWG130	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Torch Capacity Manager Power Agent, SWG140	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Torch Interface Agent - I/O TRACE, SWG40	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Torch Interface Agent - I/O TRACE, SWG60	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Torch Interface Agent - I/O TRACE, SWG130	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Torch Interface Agent - LOG, SWG40	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Torch Interface Agent - LOG, SWG60	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Torch Interface Agent - LOG, SWG130	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Torch Interface Agent - LOG, SWG140	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Torch Interface Agent - MAPPER, SWG40	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Torch Interface Agent - MAPPER, SWG60	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Torch Interface Agent - MAPPER, SWG130	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	Windows 2000 Interface Agent - Internet Informa ion Server	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	Windows 2000 Interface Agent - .NET	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	Windows 2000 Interface Agent - SQL Server	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	Windows 2000 Power Agent Upto 32 CPU's	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SMA	OpCon/xps EXEC LSAM, Group 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SMA	OpCon/xps EXEC LSAM, Group 12	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SMA	OpCon/xps EXEC LSAM Development, Group 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SMA	OpCon/xps EXEC LSAM Development, Group 12	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -

Note: The Commonwealth has established mult

Baseline Units - Volumetrics

		Annual Costs									
Resource Description	**Service Tier / Configuration (6)**	**Year 1**	**Year 2**	**Year 3**	**Year 4**	**Year 5**	**Year 6**	**Year 7**	**Opt - Year 8**	**Opt - Year 9**	**Opt - Year 10**
SMA	OpCon/xps Production SAM	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SMA	OpCon/xps Starter Kit	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SMA	OpCon/xps User Interface	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sybase	EAServer Deploy Advanced - Active	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sybase	EAServer Deploy Advanced - Passive	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	Backup Exec System Recovery Server	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	EndPoint Protection	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	Ghost Solution Suite	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Client Application and Database Pack, UNX, Tier 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Client Application and Database Pack, UNX, Tier 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Client Application and Database Pack, WIN, Tier 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Client Application and Database Pack, WIN, Tier 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Client Application and Database Pack, WIN, Tier 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Enterprise Client, UNX, Tier 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Enterprise Client, WIN, Tier 1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Enterprise Client, WIN, Tier 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Enterprise Client, WIN, Tier 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Enterprise Server, WIN, Tier 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Enterprise Server, WIN, Tier 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Library Based Tape Drive Option, XPLAT	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Media Server Encryption Option (MSEO) WIN, Tier 2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Platform Base, XPLAT (per Terabyte)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Shared Storage Option, XPLAT	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Standard Client, XPLAT	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Vault Additional Drive Option, XPLAT	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Vault Base Option, XPLAT (4 tape drives per license)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	Veritas NetBackup Enterprise Server License, Tier 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	Veritas NetBackup Windows Client, Tier 4	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Tone Software Corp.	Dynastep	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unicon Group Ltd.	LOUIS II LCOM Host Module	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unicon Group Ltd.	LOUIS II Extract & Reporting Module	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unicon Group Ltd.	LOUIS II DERIVE Option	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unicon Group Ltd.	LOUIS II DMS Interface	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unicon Group Ltd.	LOUIS II RDMS Interface	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unicon Group Ltd.	LOUIS II RELATE Option	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
VanDyke Technologies	VShell Workgroup Server	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Veeam	nWorks ESX Monitoring for SCOM	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Veeam	nWorks Management Pack for VMWare	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -

Note: The Commonwealth has established mult

Baseline Units - Volumetrics

		Annual Costs									
Resource Description	**Service Tier / Configuration (6)**	**Year 1**	**Year 2**	**Year 3**	**Year 4**	**Year 5**	**Year 6**	**Year 7**	**Opt - Year 8**	**Opt - Year 9**	**Opt - Year 10**
VMware, Inc.	VMware vSphere 4 Enterprise Plus for 1 Processor	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
VMware, Inc.	VMware vSphere 5 Enterprise Plus for 1 Processor	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
~~Western American Data~~	~~Rlist~~	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Winternals	Winternals Administrator's Pak	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
WinZip Computing	Winzip	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
XtremeSoft	AppMetrics	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
USPS	Correct Address	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IBM	FileNet	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	SharePoint (with SA)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IBM	WebSphere MQ (Procesor Value Unit)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Xerox	XeroxDocuShare	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Hybrid Third Party Software											
Vendor	**Product**										
Computer Associates International, Inc.	CA 90's Services (freeware)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	Vision Builder	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	Easytrieve Plus	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	Easytrieve Plus MVS	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	Easytrieve Plus IMS	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	Easytrieve Plus IMS Option MVS	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	Easytrieve Plus DB2 OPT	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	Easytrieve Plus DB2 Option MVS	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	Endevor/MVS Automated Configura ion Mgr MVS	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	Endevor/MVS External Security Int. MVS	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	Endevor/MVS MVS	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	Endevor/MVS Extended Processor	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	CA-Librarian	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	CA-META COBOL	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	Panvalet	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	Panvalet ISPF	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	SORT (INCL DART)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	SRAM	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
dotJ Software Inc.	dotJ Custom Tag Library	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Formula Consultants, Inc.	Star 1100	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Idea Integration	XGEN	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	Change DataMove for DB2 Source	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	DataMove for DB2 Source	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	Change DataMove	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	DataMove for IMS Source	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	Change DataMove for IMS Source	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	DataMove	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	Change DataMove DB2 Target	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	DataMove DB2 Target	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	Change DataMove/DataMove Target for UDB	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	SSA - Name 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -

Note: The Commonwealth has established mult

Baseline Units - Volumetrics

		Annual Costs									
Resource Description	**Service Tier / Configuration (6)**	**Year 1**	**Year 2**	**Year 3**	**Year 4**	**Year 5**	**Year 6**	**Year 7**	**Opt - Year 8**	**Opt - Year 9**	**Opt - Year 10**
KMSYS Worldwide, Inc.	IQU Plus-1	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
KMSYS Worldwide, Inc.	IQU Reorg Composer	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
KMSYS Worldwide, Inc.	QPLXSS	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
KMSYS Worldwide, Inc.	QPLXSV	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
KMSYS Worldwide, Inc.	QPLXV	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
~~Marble Computer Inc.~~	~~OS DCD III Data Correlation and Documentation System~~	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	SQL Server Enterprise	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SAS Institute, Inc.	Base SAS	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SAS Institute, Inc.	SAS/ACCESS Interface for IMS	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SAS Institute, Inc.	SAS/ACCESS DB2	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SAS Institute, Inc.	SAS/AF	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SAS Institute, Inc.	SAS/FSP	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SAS Institute, Inc.	SAS/GRAPH	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SAS Institute, Inc.	SAS/SHARE	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SAS Institute, Inc.	SAS/STAT	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
~~Schema Systems Limited~~	~~Q Editor Plus One~~	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SMA	OpCon/xps EXEC LSAM, Group 3	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SMA	OpCon/xps EXEC LSAM, Group 8	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SMA	OpCon/xps EXEC LSAM, Group 14	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SMA	OpCon/xps Microsoft LSAM	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SMA	OpCon/xps User Interface	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sybase	EAServer Deploy Advanced - Active	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sybase	EAServer Deploy Advanced - Passive	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
TRILOGexport, Inc.	TriTune Automation Component (APC)	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unicon Group Ltd.	LOUIS II Database Gateway	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unicon Group Ltd.	LOUIS II DMS Interface	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unicon Group Ltd.	LOUIS II Extract & Reporting Module	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unicon Group Ltd.	LOUIS II LCOM Host Module	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unicon Group Ltd.	LOUIS II MAPPER Interface	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unicon Group Ltd.	LOUIS II RDMS Interface	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Verisign	Secure Site Pro SSL	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
~~Western American Data~~	~~Rlist~~	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
WinZip	Self-Extractor 10-user license	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Total Third Party Software		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**

Total Charges

Description	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Total Base Term	Opt - Year 8	Opt - Year 9	Opt - Year 10	Total Renewal Years	Total Base Term + Renewal Years
Total Charges Summary													
Server - Fully Managed													
Total - Fully Managed - x86 Physical - All Support Tiers (Window, Linux)	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00
Total - Fully Managed - x86 Virtual - All Support Tiers (Window, Linux)	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00
Total - Fully Managed - P-Series (AIX) - All Support Tiers (Window, Linux)	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00
Server - Managed Only													
Total Managed Only- x86 - All Support Tiers (Window, Linux)	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00
Total Managed Only- P-Series - All Support Tiers (AIX)	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00
Storage and Backup - Fully Managed													
Total Enterprise Storage - Fully Managed	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00
Total Tape and Backup - Fully Managed	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00
Limited Co-Lo (Data Center Only Charge)													
Total Limited Co-Lo (Data Center Only Charge)	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00
Mainframe Services													
Total IBM Services	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00
Total - IBM Mainframe Services - All Support Tiers	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00
Total Unisys Services	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00
Total - Unisys Mainframe Services - All Support Tiers	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00
On-Demand (IaaS)													
Total IaaS Servers - x86 (Windows, Linux) - Virtual Servers	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00
Total IaaS Storage On-Demand	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00
Total IaaS Backup On-Demand	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00
Reserve Account													
Reserve Account	$1,008,000 00	$1,008,000 00	$1,008,000 00	$1,008,000 00	$1,008,000 00	$1,008,000 00	$1,008,000 00	$7,056,000 00	$1,008,000 00	$1,008,000 00	$1,008,000 00	$3,024,000 00	$10,080,000 00
Third Party Software													
Total Third Party Software	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00	$0 00
Yearly Total	**$1,008,000.00**	**$1,008,000.00**	**$1,008,000.00**	**$1,008,000.00**	**$1,008,000.00**	**$1,008,000.00**	**$1,008,000.00**	**$7,056,000.00**	**$1,008,000.00**	**$1,008,000.00**	**$1,008,000.00**	**$3,024,000.00**	**$10,080,000.00**

Services (Base Term)	**$7,056,000.00**
Grand Total Base Term	**$7,056,000.00**
Services (Renewal Years)	**$3,024,000.00**
Grand Total w/ Renewal Years	**$10,080,000.00**

Technical Staff Rate Card

Staff Hourly Rate (*)										
Resource Description	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Infrastructure (mainframe, mid-range and x86) Architects/Engineers										
Microsoft Product Specialists (e.g. Exchange, SharePoint)										
Basis and SAP Oracle support										
Performance Specialists										
Mainframe Systems Programmers										
Batch Administrators										
3rd Party Software Product Specialists										
System Administrator (Windows, AIX, Linux)										
System Administrator (Middleware support)										
Storage Administrator										
Data Backup Administrator										
Database Administrator										
Database Architects										
Database Analysts										
Project Management Support										
Network Administrator										
Facilities Administrator										
Security Administrator										
Security Architects										
Security Analysts										
Asset Management Administrator										
Quality Assurance Support										
Remedy Support Specialist										
IT Service Continuity Specialist										

(*) Rates are "Not to Exceed Rates" and can be negotiated per order.

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	Product Name	Unit	Qty per config	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
* Note: This data is sample data provided as an example. The data contained do not contain actual prices or product information.																			
* Sample Data ==>	Mainframe_Dorado_MIPS	Per MIP		ABC51323698	45687	1245	rv 5.0.1	FDCFG12599	XYZ123	$0.001	$0.001	$0.001	$0.001	$0.001	$0.001	$0.001	$0.001	$0.001	$0.001
* Sample Data ==>	VirtualServer_Windows2008_vCPU	Per VCPU		ABC51323699	45688	1246	rv 5.0.2	FDCFG12600	XYZ124	$0.002	$0.002	$0.002	$0.002	$0.002	$0.002	$0.002	$0.002	$0.002	$0.002
* Sample Data ==>	VirtualServer_Windows2008_vRAM	Per Gig		ABC51323700	45689	1247	rv 5.0.3	FDCFG12601	XYZ125	$0.003	$0.003	$0.003	$0.003	$0.003	$0.003	$0.003	$0.003	$0.003	$0.003
* Sample Data ==>	VirtualServer_Windows2008_Gig_Diskspace_Tier1	Per Gig		ABC51323701	45690	1248	rv 5.0.4	FDCFG12602	XYZ126	$0.004	$0.004	$0.004	$0.004	$0.004	$0.004	$0.004	$0.004	$0.004	$0.004
* Sample Data ==>	VirtualServer_Windows2008_Gig_Diskspace_Tier2	Per Gig		ABC51323702	45691	1249	rv 5.0.5	FDCFG12603	XYZ127	$0.005	$0.005	$0.005	$0.005	$0.005	$0.005	$0.005	$0.005	$0.005	$0.005
* Sample Data ==>	VirtualServer_Windows2008_IIS_Feature	Per Instance		ABC51323703	45692	1250	rv 5.0.6	FDCFG12604	XYZ128	$0.006	$0.006	$0.006	$0.006	$0.006	$0.006	$0.006	$0.006	$0.006	$0.006
* Sample Data ==>	VirtualServer_Windows2008_WebServer_Feature	Per Instance		ABC51323704	45693	1251	rv 5.0.7	FDCFG12605	XYZ129	$0.007	$0.007	$0.007	$0.007	$0.007	$0.007	$0.007	$0.007	$0.007	$0.007
* Sample Data ==>	Backup_Service_Disk	Per Server		ABC51323705	45694	1252	rv 5.0.8	FDCFG12606	XYZ130	$0.008	$0.008	$0.008	$0.008	$0.008	$0.008	$0.008	$0.008	$0.008	$0.008
* Sample Data ==>	SSL_Certificate	Per Cert		ABC51323706	45695	1253	rv 5.0.9	FDCFG12607	XYZ131	$0.009	$0.009	$0.009	$0.009	$0.009	$0.009	$0.009	$0.009	$0.009	$0.009
Server - Fully Managed (1)																			
x86 Server Configurations (Windows)																			
Windows pConfig - 1	2-way Quad-Core 2.0 GHz	Per Server								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 2 4 5	2-way Six-Core 2.4 GHz	Per Server								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 3	4-way Six-Core 2.0 GHz	Per Server								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 1 2 3 4 5	GB RAM	Per GB								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 1, 2, 4, 5	Mirrored 146 15K Hard Drives	Per Primary + Mirror drive								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 3	SAN Attached Storage	Per GB								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 1, 2, 3, 4, 5	Windows Server 2008 R2	Per License								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 4	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization Site s Local SAN Storage from hourly data synchronization	Per Service								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 5	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Service								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 1	Fully Managed (1) - Platinum Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 1	Fully Managed (1) - Gold Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 1	Fully Managed (1) - Silver Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 1	Fully Managed (1) - Bronze Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 1	Fully Managed (1) - Basic Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 2	Fully Managed (1) - Platinum Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 2	Fully Managed (1) - Gold Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 2	Fully Managed (1) - Silver Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 2	Fully Managed (1) - Bronze Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 2	Fully Managed (1) - Basic Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 3	Fully Managed (1) - Platinum Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 3	Fully Managed (1) - Gold Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 3	Fully Managed (1) - Silver Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 3	Fully Managed (1) - Bronze Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 3	Fully Managed (1) - Basic Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 4	Fully Managed (1) - Platinum Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 4	Fully Managed (1) - Gold Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 4	Fully Managed (1) - Silver Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 4	Fully Managed (1) - Bronze Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 4	Fully Managed (1) - Basic Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 5	Fully Managed (1) - Platinum Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 5	Fully Managed (1) - Gold Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 5	Fully Managed (1) - Silver Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 5	Fully Managed (1) - Bronze Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 5	Fully Managed (1) - Basic Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 1	2-way Quad-Core 2.0 GHz		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	GB RAM		4							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Mirrored 146 15K Hard Drives		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows Server 2008 R2		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	Product Name	Unit	Qty per config	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
	Sub-Total									$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 1	Fully Managed (1) - Platinum Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 1	Fully Managed (1) - Gold Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 1	Fully Managed (1) - Silver Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 1	Fully Managed (1) - Bronze Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 1	Fully Managed (1) - Basic Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 2	2-way Six-Core 2.4 GHz		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	GB RAM		16							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Mirrored 146 15K Hard Drives		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows Server 2008 R2		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Sub-Total									$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 2	Fully Managed (1) - Platinum Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 2	Fully Managed (1) - Gold Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 2	Fully Managed (1) - Silver Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 2	Fully Managed (1) - Bronze Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 2	Fully Managed (1) - Basic Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 3	4-way Six-Core 2.0 GHz		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	GB RAM		64							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	SAN Attached Storage		500							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows Server 2008 R2		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Sub-Total									$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 3	Fully Managed (1) - Platinum Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 3	Fully Managed (1) - Gold Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 3	Fully Managed (1) - Silver Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 3	Fully Managed (1) - Bronze Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 3	Fully Managed (1) - Basic Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 4	2-way Six-Core 2.4 GHz		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	GB RAM		16							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Mirrored 146 15K Hard Drives		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows Server 2008 R2		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization Site s Local SAN Storage from hourly data synchronization		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Sub-Total									$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 4	Fully Managed (1) - Platinum Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 4	Fully Managed (1) - Gold Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 4	Fully Managed (1) - Silver Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 4	Fully Managed (1) - Bronze Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 4	Fully Managed (1) - Basic Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 5	2-way Six-Core 2.4 GHz		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	GB RAM		16							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Mirrored 146 15K Hard Drives		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows Server 2008 R2		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from Backup off-site tape Backups		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Sub-Total									$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 5	Fully Managed (1) - Platinum Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 5	Fully Managed (1) - Gold Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 5	Fully Managed (1) - Silver Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 5	Fully Managed (1) - Bronze Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows pConfig - 5	Fully Managed (1) - Basic Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
x86 Server Configurations (Linux)																			
Linux pConfig - 1	2-way Quad-Core 2.0 GHz	Per Server								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 2, 4, 5	2-way Six-Core 2.4 GHz	Per Server								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 3	4-way Six-Core 2.0 GHz	Per Server								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 1	GB RAM	Per GB								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 1, 2, 4, 5	Mirrored 146 15K Hard Drives	Per Primary + Mirror drive								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 3	SAN Attached Storage	Per GB								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 1 2 3 4 5	RedHat or SUSE	Per License								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	Product Name	Unit	Qty per config	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Linux pConfig - 4	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Service								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 5	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Service								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 1	Fully Managed (1) - Platinum Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 1	Fully Managed (1) - Gold Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 1	Fully Managed (1) - Silver Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 1	Fully Managed (1) - Bronze Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 1	Fully Managed (1) - Basic Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 2	Fully Managed (1) - Platinum Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 2	Fully Managed (1) - Gold Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 2	Fully Managed (1) - Silver Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 2	Fully Managed (1) - Bronze Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 2	Fully Managed (1) - Basic Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 3	Fully Managed (1) - Platinum Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 3	Fully Managed (1) - Gold Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 3	Fully Managed (1) - Silver Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 3	Fully Managed (1) - Bronze Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 3	Fully Managed (1) - Basic Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 4	Fully Managed (1) - Platinum Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 4	Fully Managed (1) - Gold Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 4	Fully Managed (1) - Silver Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 4	Fully Managed (1) - Bronze Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 4	Fully Managed (1) - Basic Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 5	Fully Managed (1) - Platinum Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 5	Fully Managed (1) - Gold Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 5	Fully Managed (1) - Silver Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 5	Fully Managed (1) - Bronze Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 5	Fully Managed (1) - Basic Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 1	2-way Quad-Core 2.0 GHz		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	4 GB RAM		4							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Mirrored 146 15K Hard Drives		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	RedHat or SUSE		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Sub-Total									$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 1	Fully Managed (1) - Platinum Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 1	Fully Managed (1) - Gold Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 1	Fully Managed (1) - Silver Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 1	Fully Managed (1) - Bronze Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 1	Fully Managed (1) - Basic Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 2	2-way Six-Core 2.4 GHz		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	16 GB RAM		16							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Mirrored 146 15K Hard Drives		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	RedHat or SUSE		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Sub-Total									$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 2	Fully Managed (1) - Platinum Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 2	Fully Managed (1) - Gold Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 2	Fully Managed (1) - Silver Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 2	Fully Managed (1) - Bronze Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 2	Fully Managed (1) - Basic Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 3	4-way Six-Core 2.0 GHz		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	64 GB RAM		64							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	SAN Attached Storage		500							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	RedHat or SUSE		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Sub-Total									$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 3	Fully Managed (1) - Platinum Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 3	Fully Managed (1) - Gold Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 3	Fully Managed (1) - Silver Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 3	Fully Managed (1) - Bronze Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 3	Fully Managed (1) - Basic Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 4	2-way Six-Core 2.4 GHz		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	Product Name	Unit	Qty per config	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
	16 GB RAM		16							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Mirrored 146 15K Hard Drives		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	RedHat or SUSE		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Sub-Total									**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Linux pConfig - 4	Fully Managed (1) - Platinum Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 4	Fully Managed (1) - Gold Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 4	Fully Managed (1) - Silver Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 4	Fully Managed (1) - Bronze Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 4	Fully Managed (1) - Basic Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 5	2-way Six-Core 2.4 GHz		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	16 GB RAM		16							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Mirrored 146 15K Hard Drives		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	RedHat or SUSE		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Sub-Total									**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Linux pConfig - 5	Fully Managed (1) - Platinum Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 5	Fully Managed (1) - Gold Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 5	Fully Managed (1) - Silver Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 5	Fully Managed (1) - Bronze Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux pConfig - 5	Fully Managed (1) - Basic Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
x86 (Windows) - Virtual Servers																			
Windows vConfig - 1	2vCPU	Per Instance								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 2, 4, 5	4vCPU	Per Instance								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 3	8vCPU	Per Instance								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 1 2 3 4 5	GB Ram	Per GB								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 1, 2, 3, 4, 5	Windows Server 2008 R2	Per License								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
~~Windows vConfig - 1, 2, 3, 4, 5~~	~~Firewall/IDS~~	~~Per Config~~																	
~~Windows vConfig - 1 2 3 4 5~~	~~Site-Site VPN~~	~~Per Config~~																	
~~Windows vConfig - 1, 2, 3, 4, 5~~	~~VPN Client~~	~~Per Config~~																	
~~Windows vConfig - 1 2 3 4 5~~	~~VLAN~~	~~Per Config~~																	
Windows vConfig - 4	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 5	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 1	Fully Managed (1) - Platinum Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 1	Fully Managed (1) - Gold Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 1	Fully Managed (1) - Silver Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 1	Fully Managed (1) - Bronze Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 1	Fully Managed (1) - Basic Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 2	Fully Managed (1) - Platinum Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 2	Fully Managed (1) - Gold Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 2	Fully Managed (1) - Silver Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 2	Fully Managed (1) - Bronze Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 2	Fully Managed (1) - Basic Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 3	Fully Managed (1) - Platinum Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 3	Fully Managed (1) - Gold Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 3	Fully Managed (1) - Silver Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 3	Fully Managed (1) - Bronze Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 3	Fully Managed (1) - Basic Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 4	Fully Managed (1) - Platinum Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 4	Fully Managed (1) - Gold Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 4	Fully Managed (1) - Silver Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 4	Fully Managed (1) - Bronze Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 4	Fully Managed (1) - Basic Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 5	Fully Managed (1) - Platinum Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	Product Name	Unit	Qty per config	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Windows vConfig - 5	Fully Managed (1) - Gold Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 5	Fully Managed (1) - Silver Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 5	Fully Managed (1) - Bronze Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 5	Fully Managed (1) - Basic Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 1	2vCPU		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	GB Ram		4							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows Server 2008 R2		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	~~Firewall IDS~~		0																
	~~Site-Site VPN~~		0																
	~~VPN Client~~		0																
	~~VLAN~~		0																
	Sub-Total									**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Windows vConfig - 1	Fully Managed (1) - Platinum Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 1	Fully Managed (1) - Gold Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 1	Fully Managed (1) - Silver Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 1	Fully Managed (1) - Bronze Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 1	Fully Managed (1) - Basic Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 2	4vCPU		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	GB Ram		16							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows Server 2008 R2		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	~~Firewall/IDS~~		0																
	~~Site-Site VPN~~		0																
	~~VPN Client~~		0																
	~~VLAN~~		0																
	Sub-Total									**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Windows vConfig - 2	Fully Managed (1) - Platinum Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 2	Fully Managed (1) - Gold Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 2	Fully Managed (1) - Silver Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 2	Fully Managed (1) - Bronze Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 2	Fully Managed (1) - Basic Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 3	8vCPU		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	GB Ram		64							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows Server 2008 R2		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	~~Firewall IDS~~		0																
	~~Site-Site VPN~~		0																
	~~VPN Client~~		0																
	~~VLAN~~		0																
	Sub-Total									**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Windows vConfig - 3	Fully Managed (1) - Platinum Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 3	Fully Managed (1) - Gold Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 3	Fully Managed (1) - Silver Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 3	Fully Managed (1) - Bronze Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 3	Fully Managed (1) - Basic Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 4	4vCPU		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	GB Ram		16							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows Server 2008 R2		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	~~Firewall/IDS~~		0																
	~~Site-Site VPN~~		0																
	~~VPN Client~~		0																
	~~VLAN~~		0																
	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Sub-Total									**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Windows vConfig - 4	Fully Managed (1) - Platinum Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 4	Fully Managed (1) - Gold Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 4	Fully Managed (1) - Silver Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 4	Fully Managed (1) - Bronze Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 4	Fully Managed (1) - Basic Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 5	4vCPU		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	GB Ram		16							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows Server 2008 R2		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	Product Name	Unit	Qty per config	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
	~~Firewall IDS~~		0																
	~~Site-Site VPN~~		0																
	~~VPN Client~~		0																
	~~VLAN~~		0																
	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Sub-Total									**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Windows vConfig - 5	Fully Managed (1) - Platinum Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 5	Fully Managed (1) - Gold Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 5	Fully Managed (1) - Silver Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 5	Fully Managed (1) - Bronze Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Windows vConfig - 5	Fully Managed (1) - Basic Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
x86 (Linux) - Virtual Servers																			
Linux vConfig - 1	2vCPU	Per Instance								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 2, 4, 5	4vCPU	Per Instance								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 3	8vCPU	Per Instance								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 1, 2, 3, 4, 5	GB Ram	Per GB								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 1 2 3 4 5	RedHat or SUSE	Per License								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 1 2 3 4 5	~~Firewall IDS~~	~~Per Config~~																	
Linux vConfig - 1, 2, 3, 4, 5	~~Site-Site VPN~~	~~Per Config~~																	
Linux vConfig - 1 2 3 4 5	~~VPN Client~~	~~Per Config~~																	
Linux vConfig - 1, 2, 3, 4, 5	~~VLAN~~	~~Per Config~~																	
Linux vConfig - 4	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 5	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 1	Fully Managed (1) - Platinum Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 1	Fully Managed (1) - Gold Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 1	Fully Managed (1) - Silver Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 1	Fully Managed (1) - Bronze Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 1	Fully Managed (1) - Basic Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 2	Fully Managed (1) - Platinum Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 2	Fully Managed (1) - Gold Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 2	Fully Managed (1) - Silver Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 2	Fully Managed (1) - Bronze Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 2	Fully Managed (1) - Basic Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 3	Fully Managed (1) - Platinum Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 3	Fully Managed (1) - Gold Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 3	Fully Managed (1) - Silver Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 3	Fully Managed (1) - Bronze Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 3	Fully Managed (1) - Basic Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 4	Fully Managed (1) - Platinum Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 4	Fully Managed (1) - Gold Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 4	Fully Managed (1) - Silver Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 4	Fully Managed (1) - Bronze Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 4	Fully Managed (1) - Basic Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 5	Fully Managed (1) - Platinum Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 5	Fully Managed (1) - Gold Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 5	Fully Managed (1) - Silver Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 5	Fully Managed (1) - Bronze Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 5	Fully Managed (1) - Basic Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 1	2vCPU		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	GB Ram		4							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	RedHat or SUSE		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	~~Firewall IDS~~		0																
	~~Site-Site VPN~~		0																
	~~VPN Client~~		0																
	~~VLAN~~		0																
	Sub-Total									**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	**Product Name**	**Unit**	**Qty per config**	**Provider Part Number**	**Version Major**	**Version Minor**	**Version Build**	**Manufacturer ID**	**Equipment Code**	**Price per unit \ Per Month**									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Linux vConfig - 1	Fully Managed (1) - Platinum Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 1	Fully Managed (1) - Gold Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 1	Fully Managed (1) - Silver Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 1	Fully Managed (1) - Bronze Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 1	Fully Managed (1) - Basic Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 2	4vCPU		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	GB Ram		16							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	RedHat or SUSE		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	~~Firewall IDS~~		0																
	~~Site-Site VPN~~		0																
	~~VPN Client~~		0																
	~~VLAN~~		0																
	Sub-Total									**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Linux vConfig - 2	Fully Managed (1) - Platinum Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 2	Fully Managed (1) - Gold Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 2	Fully Managed (1) - Silver Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 2	Fully Managed (1) - Bronze Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 2	Fully Managed (1) - Basic Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 3	8vCPU		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	GB Ram		64							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	RedHat or SUSE		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	~~Firewall IDS~~		0																
	~~Site-Site VPN~~		0																
	~~VPN Client~~		0																
	~~VLAN~~		0																
	Sub-Total									**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Linux vConfig - 3	Fully Managed (1) - Platinum Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 3	Fully Managed (1) - Gold Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 3	Fully Managed (1) - Silver Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 3	Fully Managed (1) - Bronze Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 3	Fully Managed (1) - Basic Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 4	4vCPU		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	GB Ram		16							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	RedHat or SUSE		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	~~Firewall IDS~~		0																
	~~Site-Site VPN~~		0																
	~~VPN Client~~		0																
	~~VLAN~~		0																
	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Sub-Total									**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Linux vConfig - 4	Fully Managed (1) - Platinum Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 4	Fully Managed (1) - Gold Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 4	Fully Managed (1) - Silver Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 4	Fully Managed (1) - Bronze Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 4	Fully Managed (1) - Basic Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 5	4vCPU		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	GB Ram		16							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	RedHat or SUSE		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	~~Firewall IDS~~		0																
	~~Site-Site VPN~~		0																
	~~VPN Client~~		0																
	~~VLAN~~		0																
	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Sub-Total									**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Linux vConfig - 5	Fully Managed (1) - Platinum Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 5	Fully Managed (1) - Gold Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 5	Fully Managed (1) - Silver Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 5	Fully Managed (1) - Bronze Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Linux vConfig - 5	Fully Managed (1) - Basic Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	Product Name	Unit	Qty per config	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
P-Series Server Configurations																			
AIX Config - 1 2 3 4 5	3.0GHz POWER7	Per Server								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 1 2 3 4 5	Cores	Per .5 Core								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 1, 2, 3, 4, 5	GB RAM	Per GB								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 1 2 3 4 5	AIX	Per License								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 4	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 5	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 1	Fully Managed (1) - Platinum Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 1	Fully Managed (1) - Gold Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 1	Fully Managed (1) - Silver Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 1	Fully Managed (1) - Bronze Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 1	Fully Managed (1) - Basic Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 2	Fully Managed (1) - Platinum Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 2	Fully Managed (1) - Gold Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 2	Fully Managed (1) - Silver Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 2	Fully Managed (1) - Bronze Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 2	Fully Managed (1) - Basic Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 3	Fully Managed (1) - Platinum Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 3	Fully Managed (1) - Gold Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 3	Fully Managed (1) - Silver Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 3	Fully Managed (1) - Bronze Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 3	Fully Managed (1) - Basic Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 4	Fully Managed (1) - Platinum Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 4	Fully Managed (1) - Gold Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 4	Fully Managed (1) - Silver Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 4	Fully Managed (1) - Bronze Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 4	Fully Managed (1) - Basic Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 5	Fully Managed (1) - Platinum Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 5	Fully Managed (1) - Gold Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 5	Fully Managed (1) - Silver Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 5	Fully Managed (1) - Bronze Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 5	Fully Managed (1) - Basic Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 1	3.0GHz POWER7		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	0.5 Cores (1 X 0.5 Cores)		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	6 GB RAM		6							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	AIX		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Sub-Total									$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 1	Fully Managed (1) - Platinum Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 1	Fully Managed (1) - Gold Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 1	Fully Managed (1) - Silver Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 1	Fully Managed (1) - Bronze Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 1	Fully Managed (1) - Basic Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 2	3.0GHz POWER7		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	1.0 Cores (2 X 0.5 Cores)		2							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	12 GB RAM		12							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	AIX		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Sub-Total									$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 2	Fully Managed (1) - Platinum Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 2	Fully Managed (1) - Gold Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 2	Fully Managed (1) - Silver Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 2	Fully Managed (1) - Bronze Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 2	Fully Managed (1) - Basic Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 3	3.0GHz POWER7		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	1.5 Cores (3 X 0.5 Cores)		3							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	18 GB RAM		18							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	AIX		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Sub-Total									$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 3	Fully Managed (1) - Platinum Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	Product Name	Unit	Qty per config	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
AIX Config - 3	Fully Managed (1) - Gold Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 3	Fully Managed (1) - Silver Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 3	Fully Managed (1) - Bronze Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 3	Fully Managed (1) - Basic Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 4	3.0GHz POWER7		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	1.0 Cores (2 X 0.5 Cores)		2							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	12 GB RAM		12							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	AIX		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Sub-Total									$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 4	Fully Managed (1) - Platinum Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 4	Fully Managed (1) - Gold Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 4	Fully Managed (1) - Silver Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 4	Fully Managed (1) - Bronze Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 4	Fully Managed (1) - Basic Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 5	3.0GHz POWER7		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	1.0 Cores (2 X 0.5 Cores)		2							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	12 GB RAM		12							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	AIX		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Sub-Total									$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 5	Fully Managed (1) - Platinum Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 5	Fully Managed (1) - Gold Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 5	Fully Managed (1) - Silver Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 5	Fully Managed (1) - Bronze Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 5	Fully Managed (1) - Basic Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
AIX Config - 5	**Total**									$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Server - Managed Only (2)																			
Server - Managed Only x86 (Windows, Linux)																			
	Platinum Tier	Server/Instance								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Gold Tier	Server/Instance								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Silver Tier	Server/Instance								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Bronze Tier	Server/Instance								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Basic Tier	Server/Instance								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Server - Managed Only UNIX (IBM P-Series, AIX)																			
	Platinum	LPAR								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Gold Tier	LPAR								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Silver Tier	LPAR								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Bronze Tier	LPAR								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Basic Tier	LPAR								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Storage and Backup - Fully Managed (1)																			
Enterprise Storage																			
	* Dedicated - Config 1 - SAN Raid 5	GB								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	* Dedicated - Config 2 - SAN Raid 10	GB								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Dedicated - Config 3 - Net Attached	GB								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Tape and Backup																			
	** Server Tape Stored	GB Stored								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	** Offsite Tape Storage	Tapes								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Limited Co-Lo (Data Center Only Charge) (3)																			
Limited Co-Lo Configurations																			
Co-Lo Config - 1	1/4 Rack Configuration includes 10U Cabinet	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Co-Lo Config - 2	1/2 Rack Configuration includes 21U Cabinet	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Co-Lo Config - 3	Full Rack Configuration includes 42U Cabinet	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Co-Lo Config - 1 2 3	Network Bandwidth	Per GB								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Co-Lo Config - 1, 2, 3	100Mb/s Uplink	Each								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Co-Lo Config - 1 2 3	IP Addresses	Each								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Co-Lo Config - 1	110V AC Circuits	Per Circuit								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	Product Name	Unit	Qty per config	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Co-Lo Config - 1	1/4 Rack Configuration includes 10U Cabinet		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	GB Network Bandwidth		5000							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	100Mb/s Uplink		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IP Addresses		6							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	110V AC Circuits		5							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Co-Lo Config - 1	**Total**									$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Co-Lo Config - 2	1/2 Rack Configuration includes 21U Cabinet Space		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	10 000 GB Network Bandwidth		10000							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	100Mb/s Uplink		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IP Addresses		14							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	110V AC Circuits		10							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Co-Lo Config - 2	**Total**									$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Co-Lo Config - 3	Full Rack Configuration includes 42U Cabinet		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	GB Network Bandwidth		20000							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	100Mb/s Uplink		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IP Addresses		30							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	110V AC Circuits		20							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Co-Lo Config - 3	**Total**									$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Mainframe Services (4)																			
IBM Mainframe																			
	*** IBM Mainframe Allocated DASD	GB								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IBM Tapes in Storage - VTS	GB								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	IBM Offsite Tape Storage	Tape/Reel								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IBM Mainframe Configurations																			
IBM Mainframe Config - 1	IBM System zEnterprise Processor z/OS	Per MIP								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IBM Mainframe Config - 2	IBM System zEnterprise Processor Virtual Linux Prod IFL	Per MIP								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IBM Mainframe Config - 3	IBM System zEnterprise Processor Virtual Linux Prod IFLw/ Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per MIP								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IBM AS400 Config 1	IBM i Series / AS400	Per CPW								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IBM AS400 Config 2	IBM i Series / AS400 w/ Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per CPW								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IBM Mainframe Config - 1	Mainframe Services (4) - Platinum Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IBM Mainframe Config - 1	Mainframe Services (4) - Gold Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IBM Mainframe Config - 1	Mainframe Services (4) - Basic Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IBM Mainframe Config - 2	Mainframe Services (4) - Platinum Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IBM Mainframe Config - 2	Mainframe Services (4) - Gold Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IBM Mainframe Config - 2	Mainframe Services (4) - Basic Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IBM Mainframe Config - 3	Mainframe Services (4) - Platinum Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IBM Mainframe Config - 3	Mainframe Services (4) - Gold Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IBM Mainframe Config - 3	Mainframe Services (4) - Basic Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IBM AS400 Config 1	Mainframe Services (4) - Platinum Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IBM AS400 Config 1	Mainframe Services (4) - Gold Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IBM AS400 Config 1	Mainframe Services (4) - Basic Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IBM AS400 Config 2	Mainframe Services (4) - Platinum Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IBM AS400 Config 2	Mainframe Services (4) - Gold Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IBM AS400 Config 2	Mainframe Services (4) - Basic Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IBM Mainframe Config - 1	IBM System zEnterprise Processor z/OS		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Sub-Total									$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IBM Mainframe Config - 1	Mainframe Services (4) - Platinum Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IBM Mainframe Config - 1	Mainframe Services (4) - Gold Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IBM Mainframe Config - 1	Mainframe Services (4) - Basic Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IBM Mainframe Config - 2	IBM System zEnterprise Processor Virtual Linux Prod IFL		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	Product Name	Unit	Qty per config	Provider Part Number	Version Major	Version Minor	Version Build	Manufacturer ID	Equipment Code	Price per unit \ Per Month									
Description / Use >	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
	Sub-Total									$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IBM Mainframe Config - 2	Mainframe Services (4) - Platinum Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IBM Mainframe Config - 2	Mainframe Services (4) - Gold Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IBM Mainframe Config - 2	Mainframe Services (4) - Basic Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IBM Mainframe Config - 3	IBM System zEnterprise Processor Virtual Linux Prod IFL w/ Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Sub-Total									$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IBM Mainframe Config - 3	Mainframe Services (4) - Platinum Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IBM Mainframe Config - 3	Mainframe Services (4) - Gold Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IBM Mainframe Config - 3	Mainframe Services (4) - Basic Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IBM AS400 Config 1	IBM i Series / AS400		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Sub-Total									$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IBM AS400 Config 1	Mainframe Services (4) - Platinum Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IBM AS400 Config 1	Mainframe Services (4) - Gold Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IBM AS400 Config 1	Mainframe Services (4) - Basic Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IBM AS400 Config 2	IBM i Series / AS400 w/ Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Sub-Total									$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IBM AS400 Config 2	Mainframe Services (4) - Platinum Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IBM AS400 Config 2	Mainframe Services (4) - Gold Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IBM AS400 Config 2	Mainframe Services (4) - Basic Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unisys Mainframe																			
	*** Unisys DASD	GB								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Unisys Tapes in Storage - VTS	GB								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Unisys Offsite Tape Storage	Tape/Reel								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unisys Mainframe Configurations																			
Unisys Mainframe Config - 1	Unisys (Clearpath / Dorado)	Per MIP								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unisys Mainframe Config - 2	Unisys (Clearpath / Libra)	Per MIP								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unisys Mainframe Config - 3	Unisys (Clearpath / Dorado) w/ Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per MIP								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unisys Mainframe Config - 4	Unisys (Clearpath / Libra) w/ Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per MIP								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unisys Mainframe Config - 1	Mainframe Services (4) - Platinum Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unisys Mainframe Config - 1	Mainframe Services (4) - Gold Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unisys Mainframe Config - 1	Mainframe Services (4) - Basic Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unisys Mainframe Config - 2	Mainframe Services (4) - Platinum Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unisys Mainframe Config - 2	Mainframe Services (4) - Gold Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unisys Mainframe Config - 2	Mainframe Services (4) - Basic Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unisys Mainframe Config - 3	Mainframe Services (4) - Platinum Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unisys Mainframe Config - 3	Mainframe Services (4) - Gold Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unisys Mainframe Config - 3	Mainframe Services (4) - Basic Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unisys Mainframe Config - 4	Mainframe Services (4) - Platinum Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unisys Mainframe Config - 4	Mainframe Services (4) - Gold Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unisys Mainframe Config - 4	Mainframe Services (4) - Basic Tier	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unisys Mainframe Config - 1	Unisys (Clearpath / Dorado)		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Sub-Total									$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unisys Mainframe Config - 1	Mainframe Services (4) - Platinum Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unisys Mainframe Config - 1	Mainframe Services (4) - Gold Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unisys Mainframe Config - 1	Mainframe Services (4) - Basic Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unisys Mainframe Config - 2	Unisys (Clearpath / Libra)		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	**Product Name**	**Unit**	**Qty per config**	**Provider Part Number**	**Version Major**	**Version Minor**	**Version Build**	**Manufacturer ID**	**Equipment Code**	**Price per unit \ Per Month**									
Description / Use *>*	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
	Sub-Total									$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unisys Mainframe Config - 2	Mainframe Services (4) - Platinum Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unisys Mainframe Config - 2	Mainframe Services (4) - Gold Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unisys Mainframe Config - 2	Mainframe Services (4) - Basic Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unisys Mainframe Config - 3	Unisys (Clearpath / Dorado) w/ Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Sub-Total									$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unisys Mainframe Config - 3	Mainframe Services (4) - Platinum Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unisys Mainframe Config - 3	Mainframe Services (4) - Gold Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unisys Mainframe Config - 3	Mainframe Services (4) - Basic Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unisys Mainframe Config - 4	Unisys (Clearpath / Libra) w/ Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Sub-Total									$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unisys Mainframe Config - 4	Mainframe Services (4) - Platinum Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unisys Mainframe Config - 4	Mainframe Services (4) - Gold Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unisys Mainframe Config - 4	Mainframe Services (4) - Basic Tier		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS x86 Server Configurations (Windows)																			
IaaS Windows vConfig - 1	2vCPU	Per Server								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Windows vConfig - 2, 4, 5	4vCPU	Per Server								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Windows vConfig - 3	8vCPU	Per Server								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Windows vConfig - 1, 2, 3, 4, 5	GB Ram	Per GB								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Windows vConfig - 1, 2, 3, 4, 5	Windows Server 2008 R2	Per License								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Windows vConfig - 1 2 3 4 5	~~Firewall IDS~~	~~Per Config~~																	
IaaS Windows vConfig - 1, 2, 3, 4, 5	~~Site-Site VPN~~	~~Per Config~~																	
IaaS Windows vConfig - 1 2 3 4 5	~~VPN Client~~	~~Per Config~~																	
IaaS Windows vConfig - 1 2 3 4 5	~~VLAN~~	~~Per Config~~																	
IaaS Windows vConfig - 4	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Windows vConfig - 5	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Windows vConfig - 1	2vCPU		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	GB Ram		4							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows Server 2008 R2		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	~~Firewall IDS~~		0																
	~~Site-Site VPN~~		0																
	~~VPN Client~~		0																
	~~VLAN~~		0																
IaaS Windows vConfig - 1	Total									$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Windows vConfig - 2	4vCPU		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	GB Ram		16							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows Server 2008 R2		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	~~Firewall IDS~~		0																
	~~Site-Site VPN~~		0																
	~~VPN Client~~		0																
	~~VLAN~~		0																
IaaS Windows vConfig - 2	Total									$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Windows vConfig - 3	8vCPU		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	GB Ram		64							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows Server 2008 R2		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	~~Firewall IDS~~		0																
	~~Site-Site VPN~~		0																
	~~VPN Client~~		0																
	~~VLAN~~		0																
IaaS Windows vConfig - 3	Total									$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	**Product Name**	**Unit**	**Qty per config**	**Provider Part Number**	**Version Major**	**Version Minor**	**Version Build**	**Manufacturer ID**	**Equipment Code**	**Price per unit \ Per Month**									
Description / Use *>*	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
IaaS Windows vConfig - 4	4vCPU		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	GB Ram		16							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows Server 2008 R2		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	~~Firewall IDS~~		0																
	~~Site-Site VPN~~		0																
	~~VPN Client~~		0																
	~~VLAN~~		0																
	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Windows vConfig - 4	Total									$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Windows vConfig - 5	4vCPU		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	GB Ram		16							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Windows Server 2008 R2		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	~~Firewall/IDS~~		0																
	~~Site-Site VPN~~		0																
	~~VPN Client~~		0																
	~~VLAN~~		0																
	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Windows vConfig - 5	Total									$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS x86 Server Configurations (Linux)																			
IaaS Linux vConfig - 1	2vCPU	Per Server								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Linux vConfig - 2, 4, 5	4vCPU	Per Server								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Linux vConfig - 3	8vCPU	Per Server								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Linux vConfig - 1, 2, 3, 4, 5	GB Ram	Per GB								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Linux vConfig - 1 2 3 4 5	RedHat or SUSE	Per License								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Linux vConfig - 1 2 3 4 5	~~Firewall IDS~~	~~Per Config~~																	
IaaS Linux vConfig - 1, 2, 3, 4, 5	~~Site-Site VPN~~	~~Per Config~~																	
IaaS Linux vConfig - 1 2 3 4 5	~~VPN Client~~	~~Per Config~~																	
IaaS Linux vConfig - 1, 2, 3, 4, 5	~~VLAN~~	~~Per Config~~																	
IaaS Linux vConfig - 4	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Linux vConfig - 5	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups	Per Config								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Linux vConfig - 1	2vCPU		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	4 GB Ram		4							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	RedHat or SUSE		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	~~Firewall IDS~~		0																
	~~Site-Site VPN~~		0																
	~~VPN Client~~		0																
	~~VLAN~~		0																
IaaS Linux vConfig - 1	Total									$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Linux vConfig - 2	4vCPU		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	16 GB Ram		16							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	RedHat or SUSE		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	~~Firewall IDS~~		0																
	~~Site-Site VPN~~		0																
	~~VPN Client~~		0																
	~~VLAN~~		0																
IaaS Linux vConfig - 2	Total									$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Linux vConfig - 3	8vCPU		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	64 GB Ram		64							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	RedHat or SUSE		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	~~Firewall IDS~~		0																
	~~Site-Site VPN~~		0																
	~~VPN Client~~		0																
	~~VLAN~~		0																

Catalog of Services

(a) Offeror should only input in highlighted (yellow) cells.

(b) Pricing for individuals config items should only include the price for the identified unit.

(c) Pricing for the managed tiers (ex. "Fully Managed (1) - Platinum Tier") should only include cost for the management of the identified configuration.

Field Name ==>	**Product Name**	**Unit**	**Qty per config**	**Provider Part Number**	**Version Major**	**Version Minor**	**Version Build**	**Manufacturer ID**	**Equipment Code**	**Price per unit \ Per Month**									
Description / Use *>*	*Unique Identifier*	*Unit*	*Qty per config*	*Provider's Part Number for Reference to Provider's catalog*	*High Level Version Number*	*Lower Level Version Number*	*Build Identifier if needed*	*Relevent Manufacture Part Number if needed*	*Provider's Equipment Code if needed*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
IaaS Linux vConfig - 3	Total									$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Linux vConfig - 4	4vCPU		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	16 GB Ram		16							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	RedHat or SUSE		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	~~Firewall/IDS~~		0																
	~~Site-Site VPN~~		0																
	~~VPN Client~~		0																
	~~VLAN~~		0																
	Disaster Recovery Server with a Restoral Interval of 24 hours via Backup Restoral from Backup Site's Local SAN Storage from hourly data synchronization		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Linux vConfig - 4	Total									$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Linux vConfig - 5	4vCPU		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	16 GB Ram		16							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	RedHat or SUSE		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	~~Firewall IDS~~		0																
	~~Site-Site VPN~~		0																
	~~VPN Client~~		0																
	~~VLAN~~		0																
	Disaster Recovery Server with a Restoral Interval of 72 hours via Backup Restoral from off-site tape Backups		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Linux vConfig - 5	Total									$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Storage Configurations																			
IaaS Storage Config - 1, 2	SAN attached storage	Per GB								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Storage Config - 3	Network Attached Storage	Per GB								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Storage Config - 1	Raid 5	Per GB								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Storage Config - 2	Raid 10	Per GB								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Storage Config - 1 2	10K - 15K RPM discs	Per GB								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Storage Config - 1	SAN attached storage		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Raid 5		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	10K - 15K RPM discs		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Storage Config - 1	Total									$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Storage Config - 2	SAN attached storage		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	Raid 10		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
	10K - 15K RPM discs		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Storage Config - 2	Total									$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Storage Config - 3	Network Attached Storage		1							$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Storage Config - 3	Total									$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IaaS Backup Configurations																			
IaaS Backup Config - 1	Remote Offsite backup per GB	Per GB								$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Reserve Account																			
	Reserve Account - Enterprise Datacenter									$84,000.00	$84,000.00	$84,000.00	$84,000.00	$84,000.00	$84,000.00	$84,000.00	$84,000.00	$84,000.00	$84,000.00

Software

Field Name ==>	Product Name		Unit	Price per unit \ Per Month									
Description / Use ==>	*Unique Identifier*		*Unit*	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
Vendor	**Product**	**Title if equivalency is priced**											
Third Party Software													
B & L	BL/LIB Tape Library Management System		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
B & L	BL/SCHED Scheduling & Monitoring System		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	BMC AppSight for Windows/.NET - Division Edition		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	BMC AppSight Named Users		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	BMC AppSight QA Users		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	CONTROL-M Enterprise Manager		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	CONTROL-M Full Admin User		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	CONTROL-M Tasks (100 Tasks per Unit)		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Database Director (D2)		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iBuild		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iChange		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iCheck		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iCopy		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iExtract		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iLM		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iLoad		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iRecover		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iSurvey		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Eclipse iUnload		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
BMC Software	Mission Control		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Business Objects	Crystal Reports		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Bytware Inc.	StandGuard Anti-Virus		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Citrix	XenApp Advanced (User Counts)		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Citrix	XenApp Enterprise (User Counts)		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	CA-Explore for CICS		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	SOA Security Manager		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	SOA Security Manager Additional Secured Web Services		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	SOA Security Manager Additional Users		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Corticon Technologies	Corticon Business Rules Server – Unlimited CPUs		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Corticon Technologies	Corticon Server – per Non-Production Server		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Corticon Technologies	Corticon Business Rules Modeling Studio – per Named User		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
CSI International	EPIC		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
CSI International	FAQS/PCS		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
CSI International	FAQS/ASO		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
EMC Corporation	PowerPath		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
EMC Corporation	PowerPath (per CPU)		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
EMC Corporation	Symmetrix® VMAX Fully Automated Storage Tiering for Virtual Pools (FAST VP)		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
EMC Corporation	Vsphere Enterprise Plus		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Experian QAS	NameSearch - Production (Licensed per Server up to 8 CPU)		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Experian QAS	NameSearch - Non-Production (Licensed per Server)		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Formula Consultants, Inc.	Star 1100		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
GlobalScape	CuteFTP Pro 2.0		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
HELPSYS	Robot/Schedule		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Idea Integration	XGEN		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	SSA-Name 3		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Infragistics	NetAdvantage for .NET		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
KMSYS Worldwide, Inc.	IQU Plus-1		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Levi, Ray and Shoup	VPS/PCL		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Levi, Ray and Shoup	VPS/TCP/IP		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Levi, Ray and Shoup	VPS/DRS		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Levi, Ray and Shoup	VPS		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
MacKinney Systems, Inc.	CICS Response Time Monitor		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
~~Marble Computer, Inc.~~	~~OS DCD III Data Correlation and Documentation System~~	INTENTIONALLY OMITTED	License										
Microsoft	BizTalk Adaptor for MQSeries		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	BizTalk Server Enterprise (Single Processor)		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	BizTalk Server Standard (Single Processor)		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	SQL Server CAL		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	SQL Server Enterprise (Single Processor)		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	SQL Server Enterprise		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -

Microsoft	SQL Server Standard (Single Processor)		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	SQL Server Standard		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	SQL Server Standard per 2-Core		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	Visual Studio Foundation Server		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	Visual Studio Foundation Server CAL		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	Visual Studio Professional with MSDN		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	Windows Server Datacenter Edition (Single Processor)		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	Windows Server Enterprise Edition		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	Windows Server Standard Edition		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	Windows Terminal Service Client Access Licenses		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Network Associates	McAfee Anti-Virus		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Novell	Platespin Migrator		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Novell	SuSE Linux		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
OpenText	Metastorm Integration Manager for CICS (MIM for CICS)		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Oracle	Oracle Change Management Pack		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Oracle	Oracle Database 10g Enterprise		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Oracle	Oracle Database Enterprise Edition		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Oracle	Oracle Diagnostic Pack		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Oracle	Oracle Enterprise Linux		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Oracle	Oracle Exadata Storage Software		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Oracle	Oracle Partitioning		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Oracle	Oracle Tuning Pack		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Oracle	Real Application Cluster - Processor Perpetual		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Oracle	Spatial and Graph - Processor Perpetual		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Pitney Bowes	Finalist (Doc Sense)		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Pitney Bowes	CODE-1 Plus		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Pitney Bowes	CODE-1 Plus (Test / Development)		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Pitney Bowes	Online Window for Finalist		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Quest	Central Performance Suite for SQL Server, Tier A		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Quest	Central Performance Suite for SQL Server, Tier B		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Quest	Foglight Database Management Suite for SQL Server		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Quest	Foglight for SQL Server per CPU Socket		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Quest	Foglight OS Management per CPU Socket		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Quest	Foglight Server for FSM		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
RealVNC	VNC Enterprise Edition for Windows		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Red Hat	Red Hat Enterprise Linux		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
~~Schema Systems Limited~~	~~Q Editor Plus One~~	INTENTIONALLY OMITTED	License										
Segus Inc.	OPC/Graph		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG20		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG40		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG60		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG80		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - CMS/Telcon, SWG130		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG20		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG40		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG60		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG80		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG130		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - KONS/TIP Memory, SWG140		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - MAPPER, SWG20		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - MAPPER, SWG40		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - MAPPER, SWG60		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - MAPPER, SWG80		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - MAPPER, SWG130		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG20		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG40		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -

Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG60		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG80		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG130		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - MCB/Step Control, SWG140		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - System Log, SWG20		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - System Log, SWG40		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - System Log, SWG60		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - System Log, SWG80		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - System Log, SWG130		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - System Log, SWG140		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG20		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG40		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG60		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG80		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG130		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Interface Agent - UDS/DMS, SWG140		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Power Agent, SWG20		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Power Agent, SWG40		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Power Agent, SWG60		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Power Agent, SWG80		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Power Agent, SWG130		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Power Agent, SWG140		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Torch Capacity Manager Power Agent, SWG40		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Torch Capacity Manager Power Agent, SWG60		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Torch Capacity Manager Power Agent, SWG130		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Torch Capacity Manager Power Agent, SWG140		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Torch Interface Agent - I/O TRACE, SWG40		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Torch Interface Agent - I/O TRACE, SWG60		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Torch Interface Agent - I/O TRACE, SWG130		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Torch Interface Agent - LOG, SWG40		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Torch Interface Agent - LOG, SWG60		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Torch Interface Agent - LOG, SWG130		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Torch Interface Agent - LOG, SWG140		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Torch Interface Agent - MAPPER, SWG40		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Torch Interface Agent - MAPPER, SWG60		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	OS 2200 Torch Interface Agent - MAPPER, SWG130		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	Windows 2000 Interface Agent - Internet Information Server		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	Windows 2000 Interface Agent - .NET		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	Windows 2000 Interface Agent - SQL Server		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sightline	Windows 2000 Power Agent Upto 32 CPU's		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SMA	OpCon/xps EXEC LSAM, Group 3		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SMA	OpCon/xps EXEC LSAM, Group 12		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SMA	OpCon/xps EXEC LSAM Development, Group 2		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SMA	OpCon/xps EXEC LSAM Development, Group 12		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SMA	OpCon/xps Production SAM		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SMA	OpCon/xps Starter Kit		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SMA	OpCon/xps User Interface		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sybase	EAServer Deploy Advanced - Active		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sybase	EAServer Deploy Advanced - Passive		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	Backup Exec System Recovery Server		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -

Symantec	EndPoint Protection		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	Ghost Solution Suite		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Client Application and Database Pack, UNX, Tier 3		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Client Application and Database Pack, UNX, Tier 4		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Client Application and Database Pack, WIN, Tier 2		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Client Application and Database Pack, WIN, Tier 3		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Client Application and Database Pack, WIN, Tier 4		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Enterprise Client, UNX, Tier 4		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Enterprise Client, WIN, Tier 1		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Enterprise Client, WIN, Tier 2		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Enterprise Client, WIN, Tier 3		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Enterprise Server, WIN, Tier 2		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Enterprise Server, WIN, Tier 3		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Library Based Tape Drive Option, XPLAT		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Media Server Encryption Option (MSEO) WIN, Tier 2		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Platform Base, XPLAT (per Terabyte)		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Shared Storage Option, XPLAT		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Standard Client, XPLAT		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Vault Additional Drive Option, XPLAT		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	NetBackup Vault Base Option, XPLAT (4 tape drives per license)		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	Veritas NetBackup Enterprise Server License, Tier 3		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Symantec	Veritas NetBackup Windows Client, Tier 4		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Tone Software Corp.	Dynastep		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unicon Group Ltd.	LOUIS II LCOM Host Module		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unicon Group Ltd.	LOUIS II Extract & Reporting Module		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unicon Group Ltd.	LOUIS II DERIVE Option		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unicon Group Ltd.	LOUIS II DMS Interface		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unicon Group Ltd.	LOUIS II RDMS Interface		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unicon Group Ltd.	LOUIS II RELATE Option		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
VanDyke Technologies	VShell Workgroup Server		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Veeam	nWorks ESX Monitoring for SCOM		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Veeam	nWorks Management Pack for VMWare		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
VMware, Inc.	VMware vSphere 4 Enterprise Plus for 1 Processor		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
VMware, Inc.	VMware vSphere 5 Enterprise Plus for 1 Processor		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
~~Western American Data~~	~~Rlist~~	INTENTIONALLY OMITTED	License										
Winternals	Winternals Administrator's Pak		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
WinZip Computing	Winzip		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
XtremeSoft	AppMetrics		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
USPS	Correct Address		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IBM	FileNet		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Microsoft	SharePoint (with SA)		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
IBM	WebSphere MQ (Procesor Value Unit)		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Xerox	XeroxDocuShare		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Hybrid Third Party Software													
Vendor	**Product**												
Computer Associates International, Inc.	CA 90's Services (freeware)		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	Vision Builder		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	Easytrieve Plus		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	Easytrieve Plus MVS		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	Easytrieve Plus IMS		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	Easytrieve Plus IMS Option MVS		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	Easytrieve Plus DB2 OPT		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	Easytrieve Plus DB2 Option MVS		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	Endevor/MVS Automated Configuration Mgr MVS		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	Endevor/MVS External Security Int. MVS		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	Endevor/MVS MVS		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	Endevor/MVS Extended Processor		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	CA-Librarian		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	CA-META COBOL		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	Panvalet		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	Panvalet ISPF		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	SORT (INCL DART)		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Computer Associates International, Inc.	SRAM		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -

dotJ Software Inc.	dotJ Custom Tag Library		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Formula Consultants, Inc.	Star 1100		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Idea Integration	XGEN		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	Change DataMove for DB2 Source		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	DataMove for DB2 Source		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	Change DataMove		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	DataMove for IMS Source		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	Change DataMove for IMS Source		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	DataMove		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	Change DataMove DB2 Target		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	DataMove DB2 Target		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	Change DataMove/DataMove Target for UDB		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Informatica Corporation	SSA - Name 3		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
KMSYS Worldwide, Inc.	IQU Plus-1		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
KMSYS Worldwide, Inc.	IQU Reorg Composer		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
KMSYS Worldwide, Inc.	QPLXSS		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
KMSYS Worldwide, Inc.	QPLXSV		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
KMSYS Worldwide, Inc.	QPLXV		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
~~Marble Computer Inc.~~	~~OS DCD III Data Correlation and Documentation System~~	INTENTIONALLY OMITTED	License										
Microsoft	SQL Server Enterprise		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SAS Institute, Inc.	Base SAS		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SAS Institute, Inc.	SAS/ACCESS Interface for IMS		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SAS Institute, Inc.	SAS/ACCESS DB2		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SAS Institute, Inc.	SAS/AF		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SAS Institute, Inc.	SAS/FSP		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SAS Institute, Inc.	SAS/GRAPH		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SAS Institute, Inc.	SAS/SHARE		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SAS Institute, Inc.	SAS/STAT		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
~~Schema Systems Limited~~	~~Q Editor Plus One~~	INTENTIONALLY OMITTED	License										
SMA	OpCon/xps EXEC LSAM, Group 3		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SMA	OpCon/xps EXEC LSAM, Group 8		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SMA	OpCon/xps EXEC LSAM, Group 14		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SMA	OpCon/xps Microsoft LSAM		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SMA	OpCon/xps User Interface		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sybase	EAServer Deploy Advanced - Active		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Sybase	EAServer Deploy Advanced - Passive		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
TRILOGexport, Inc.	TriTune Automation Component (APC)		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unicon Group Ltd.	LOUIS II Database Gateway		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unicon Group Ltd.	LOUIS II DMS Interface		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unicon Group Ltd.	LOUIS II Extract & Reporting Module		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unicon Group Ltd.	LOUIS II LCOM Host Module		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unicon Group Ltd.	LOUIS II MAPPER Interface		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Unicon Group Ltd.	LOUIS II RDMS Interface		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Verisign	Secure Site Pro SSL		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
~~Western American Data~~	~~Rlist~~	INTENTIONALLY OMITTED	License										
WinZip	Self-Extractor 10-user license		License	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -

Termination for Convenience Fees

	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Opt - Year 8	Opt - Year 9	Opt - Year 10
(A) Termination Fee Base	$30,000,000 00	$75,000,000 00	$30,000,000 00							
(B) Value of Services Performed*	(Services Performed)	(Services Performed)	(Services Performed)							
(C) Actual Termination for Convenience Fees	C =A-B	C =A-B	C =A-B							

No Termination for Convenience Fees are available after Year 3.

Termination for Conveinence Fees are not cumulative.

(*) The value of all Services performed by the Contractor consistent with the terms of the Contract prior to the effective date of termination

Request for Proposal

RFP # 6100022698

Commonwealth of Pennsylvania
Office of Administration
Office for Information Technology
Data Center Computing Services

Schedule J.1

Datacenter Service Level Management

Table of Contents

1 GENERAL 3
2 SERVICE LEVEL MEASUREMENT DESCRIPTIONS 3
3 REPORTING 4
4 NOTICE REQUIREMENTS FOR ADDITIONS, DELETIONS & MODIFICATIONS 4
5 SERVICE-LEVEL CREDITS 5
6 EARNBACK 6
7 ADDITIONS, MODIFICATIONS, AND DELETIONS OF SERVICE LEVELS 7
8 SERVICE DELIVERY FAILURE 8
9 COMMENCEMENT OF OBLIGATIONS 9
10 COOPERATION 10
11 IMPROVEMENT PLAN FOR KEY MEASUREMENTS 10
12 MEASURING TOOLS 10
13 TIMES 11
14 SINGLE INCIDENT/MULTIPLE DEFAULTS 11
15 EXCLUSIONS 11
16 PERCENTAGE OBJECTIVES 11

1 General

The Commonwealth has adopted the ITIL framework and has established Service Level Management to maintain and improve IT Service quality, through a constant cycle of agreeing, monitoring, measuring, and reporting upon IT Service achievements and the instigation of actions to eradicate poor service.

The Service Level Performance Measures and their targets that are described in this Schedule J.1 Datacenter Service Level Management have been specifically designed to support the Service Level Agreements set forth in Schedule J.2.

The methodology set out in this Schedule J.1 supports the Service Level Management cycle of agreeing, monitoring, measuring, reporting and improving the delivery of the services to the Commonwealth.

As of the Effective Date (or as otherwise specified in this Schedule J.1), the Offeror will perform the Services to which Service Levels apply, so that the Service Level Performance will, in each month of the Term, meet or exceed, the Service Levels.

New Service Levels (Critical Measurements, Key Measurements) may be added or substituted by the Commonwealth as specified in this Schedule J.1 during the Term. For example, such additions or substitutions may occur in conjunction with changes to the environment and the introduction of new Equipment or Software to support a new or additional catalog service. However, where such Equipment or Software or such means of Service delivery is a replacement or upgrade of existing technology to support an existing catalog service, there shall be a presumption of equivalent or improved performance.

The achievement of the Service Levels by the Offeror may require the coordinated, collaborative effort of the Offeror with other third party contractors. The Offeror shall provide a single point of contact for the prompt resolution of all Service Level Defaults and all failures to provide high quality Services to the Commonwealth, regardless of whether the reason for such Service Level Defaults, or failure to provide high quality Services to the Commonwealth, was caused by the Offeror.

2 Service Level Measurement Descriptions

2.1 Application Infrastructure Availability

The Service Level for "Applications Infrastructure Availability" measures the percentage of time an Application is Available and not in a Degraded Condition as defined in **Schedule A - Defined Terms**. This measurement is by application, not by server instance. Availability is defined by whether the application residing on any of the associated server instances is available to users. Server Instances and related configuration items (CIs) supporting Applications are identified in the CMDB.

2.2 Measuring Incident and Problem Resolution

The Service Level for "Incident and Problem Resolution" measures the percentage of Incident events with resolution times (commonly known as "Mean-Time-To-Restore" – MTTR) within the limits specified within the appropriate Commonwealth Compute Procedures Manual based on the Incident Priority/Severity. These incidents are either user reports or monitoring system generated events indicating a service issue.

2.3 Measuring Other Service Management and Service Delivery

The Service Level for "Other Service Management and Service Delivery" measure the percentage of Requests, Projects, Backups, Recoveries, Renewals and Proposals that are delivered within the limits specified within the appropriate Commonwealth Compute Procedures Manual based on the request.

3 Reporting

Unless otherwise specified in this Schedule J.1, each Service Level (Critical Measurement, Key Measurement), Critical Deliverable, Recurring Deliverable, and Transition Milestone shall be measured and reported on a monthly basis. The format, layout and content of such monthly report shall be as directed by the Commonwealth. The Offeror's monthly performance reports are due by the 5th Business day of each month and shall include a set of soft-copy reports such that the Commonwealth is able to verify the Offeror's performance and compliance with the Service Level (Critical Measurement, Key Measurement), Critical Deliverable (until all Critical Deliverables are received and approved by the Commonwealth), Recurring Deliverable, and Transition Milestone.

The Offeror shall provide detailed supporting information for each report to the Commonwealth in a format suitable for use on a personal computer. The data and detailed supporting information shall include the methodology used by Offeror to calculate the service level performance based on the data measured and reported by the measurement tool such that the Commonwealth is able to reproduce the calculations made by Offeror and validate the results reported in the monthly Service Level Performance reports. All detailed supporting information shall be the Commonwealth's Confidential Information, and the Commonwealth may access such information online and in real-time, where feasible, at any time during the Term. In addition, Offeror shall provide the Commonwealth with direct, unaltered access to review and audit all raw data collection related to Service Levels.

The Offeror will create, maintain, and provide to the Commonwealth detailed procedure documentation of its Service Level measurement process used to collect Service Level data and calculate Service Level attainment. The process documentation must include quality assurance reviews and verification procedures. The measurement process must be automated to the extent possible, and any manual data collection steps must be clearly documented, verified and auditable. All methods, codes and automated programs must be documented and provided to the Commonwealth for validation and approval. The Offeror must ensure it tests and validates the accuracy and currency of the documentation and measurement process on a quarterly basis.

4 Notice Requirements for Additions, Deletions & Modifications

The Commonwealth will send notice to the Offeror at least ninety (90) days prior to the date that additions or deletions to Performance Categories, or additions or deletions to Service Levels

(which include the movement of Critical Measurements to Key Measurements and Key Measurements to Critical Measurements), or modifications to Service-Level Pool Percentage Allocation for any Critical Measurements or additions or deletions to Recurring Deliverables are to be effective. The Commonwealth may send only one such notice (which notice may contain multiple changes) each calendar quarter. Movement of Critical Measurements to Key Measurements and Key Measurements to Critical Measurements does not constitute creation of new service levels.

5 Service-Level Credits

In the event of a Service Level Default, the Offeror shall provide the Commonwealth credits as defined below:

5.1 Schedule J.2 and Schedule J.3 set forth the information required to calculate whether the Service Level has met a Service Level Default level and how the Service Level is calculated and reported. For each Service Level Default, the Offeror shall provide credits to the Commonwealth, subject to Section 6 below, a Service Level Credit that will be computed in accordance with the following formula:

Service Level Credit = 100% of the effected month's invoicing for the service that experienced a Service Level Default to a maximum credit not to exceed the At-Risk Amount as defined in **Schedule A - Defined Terms**.

For example, assume that the Offeror fails to meet a Critical Measurement Service Level, the Offeror's Monthly Invoice Amount for the month in which the Service-Level Default occurred was $100,000. The credit would be $100,000.

If the event occurs where the total monthly credit amount exceeds the At-Risk-Amount, each Service Level Default will be calculated based on the percentage of the total credit Amount and applied to the At-Risk-Amount. An Example is if the At-Risk Amount is $100,000 and there are three Service Level Defaults (#1 = $50,000, #2=30,000 and #3=$80,000 for a total of $160,000) then the credit for Defaults would be calculated as follows:

Default 1		Default 2		Default 3		Total Credits Due
$50,000	+	$30,000	+	$80,000	=	$160,000

Default 1		Total Credits Due		Default 1Proration
$50,000	/	$160,000	=	31.25%

At-Risk Amount		Default 1 Proration		Credit Due for Default 1
$100,000	X	31.25%	=	$31,250

If more than one Service-Level Default has occurred in a single month, the sum of the corresponding Service-Level Credits shall be credited to the Commonwealth.

5.2 In no event shall the amount of Service-Level Credits credited to the Commonwealth with respect to all Service-Level Defaults occurring in a single month exceed, in total, the At-Risk Amount.

5.3 The Offeror shall notify the Commonwealth in writing if the Commonwealth becomes entitled to a Service-Level Credit, which notice shall be included in the standard monthly reporting for Critical Measurements and Key Measurements as described in Section 3 above. The monthly reports shall also describe any failure to meet Key Measurements for the month.

5.4 The total amount of Service-Level Credits that the Offeror will be obligated to pay to the Commonwealth, with respect to Service-Level Defaults occurring each month, shall be credited on the invoice that contains charges for the month during which the Service-Level Default(s) giving rise to such credit(s) occurred. For example, the amount of Service-Level Credits payable with respect to Service-Level Defaults occurring in August shall be set forth in the invoice for the August Monthly Invoice Amount issued in September.

5.5 The Offeror acknowledges and agrees that the Service-Level Credits shall not be deemed or construed to be liquidated damages or a sole and exclusive remedy or in derogation of any other rights and remedies the Commonwealth has hereunder or under the Contract.

6 Earnback

The Offeror shall have Earnback opportunities with respect to Service-Level Credits as follows:

6.1 The Service Level must be identified as Earnback Eligible per Schedule J.2 with a "Y" in the column titled "Earnback Eligible"

6.2 Within fifteen (15) days after the first anniversary of the month in which any Service Level Default occurs, the Offeror shall provide a report to the Commonwealth that will include, with respect to each Critical Measurement for which there was a Service-Level Default, the following:

6.2.1 Statistics on the Offeror's average monthly performance during the preceding twelve (12) months

6.2.2 The amount of Service Level Credit imposed for Service Level Default

6.2.3 The total amount of Service Level Credits imposed for Service Level Defaults

6.3 If the Offeror fails to meet the "Earnback Minimum" objective, Service Level Credits will be calculated and applied on the next Billing Cycle.

6.3.1 Earn-back WILL NOT be available to the Offeror if it fails to meet the "Earnback Minimum" objective (Credit applied on the next Billing Cycle).

6.4 If the Offeror fails to meet the "Required" objective, Service Level Credits will be calculated and applied in twelve (12) months if an Earnback is not earned or immediately upon failure of a "Required" objective.

6.4.1 Earn-back WILL be available to the Offeror if they fail to meet the "Required" objective. If the Offeror meets the "Required" objective for the following (consecutive) 12 months, the Offeror will not be required to issue the credit.

6.4.2 If, during a rolling 12-Month Review Period, the Commonwealth deletes the Critical Measurement (including demotion of a Critical Measurement to a Key Measurement) that corresponds to the Service Level Default giving rise to such 12-Month Review Period, Offeror shall continue to track its performance for such former Critical Measurement and shall be entitled to an Earnback if and to the extent, and at the time, it would have otherwise been entitled to such Earnback in accordance with the procedures described in Section 6.4.1 above had the Critical Measurement not been so deleted or demoted to a Key Measurement during such 12-Month Review Period.

6.5 If the Contract is terminated for default all service credits are due upon notice of termination.

7 Additions, Modifications, and Deletions of Service Levels

The Commonwealth may add, modify or delete Critical Measurements or Key Measurements as described below by sending written notice in accordance with Section 4 above.

7.1 Additions

The Commonwealth may add Service Levels in accordance with this Section 7.1 and by providing written notice in accordance with Section 4. Service Level commitments associated with added Service Levels will be computed as follows:

7.1.1 Where at least nine (9) consecutive months of verifiable service measurements exist for a particular Service that is being provided by the Offeror, the Parties agree that the Service Level shall be defined as the average of such service measurements for the Nine-Month Measurement Window , or

7.1.2 Where no measurements exist for a particular Service that is being provided by the Offeror, the Parties shall attempt in good faith to agree on a Service Level commitment using industry standard measures or third party advisory services (for example, Gartner Group, Yankee Group, etc.), or

7.1.3 Where less than nine (9) months or no measurements exist for a particular Service that is being provided by the Offeror, and the Parties fail to agree on a Required Service Level and an Earnback Minimum Service Level commitment using industry-standard measures as described in Item 2 of Section 7.1 of this Schedule, the Parties shall do the following:

7.1.3.1 The Offeror shall begin providing monthly measurements within ninety (90) days after the Offeror's receipt of the Commonwealth's written request and subject to agreement on such measurements in accordance with the Change Control Procedures.

7.1.3.2 After nine (9) or more actual Service Level attainments have been measured (or should have been measured per Section 7.1.3.1 of this Schedule J.1 and if

not so measured; constructed as described in Section 7.1.3.2.1 of this Schedule J.1), the Commonwealth may at any time in writing request that Section 7.1.1 above be used to establish the Service Level commitments:

7.1.3.2.1 If the Offeror is responsible for measuring actual service-level attainments for nine (9) consecutive months and fails to provide one (1) or more measurements during the Six-Month Measurement Window such that nine (9) consecutive measurements are not available, the missing measurement(s) shall be constructed according to the following:

(i) if one measurement is missing, the missing measurement shall be constructed by using the highest of the eight (8) actual measurements, or

(ii) if two (2) or more measurements are missing, the first missing measurement shall be constructed by using the highest of the actual measurements and adding to that measurement twenty percent (20%) of the difference between that measurement and one hundred percent (100%) and each of the remaining missing measurements shall be constructed by using the highest of the actual measurements and adding to that measurement thirty-five percent (35%) of the difference between that measurement and one hundred percent (100%).

For example, if there were four measurements for a particular Service, and the highest of the four measurements were 95%, then the measurements for the missing two months would be deemed to be 96.00% (representing 95.00% plus (20% of 5%)) and 96.75% (representing 95.00% plus 35% of 5%)), respectively.

7.1.3.2.2 If the Offeror has provided twenty-four (24) actual service-level attainment measurements for any particular Service provided by the Offeror, and the Commonwealth has not used Item 1 of Section 7.1 of this Schedule to establish Service Level commitments, then continued provision of actual service-level attainment measurements shall be subject to the Parties' mutual agreement in accordance with the Change Control Procedures.

7.2 Deletions

The Commonwealth may delete Critical Measurements or Key Measurements by sending written notice in accordance with Section 4 herein.

8 Service Delivery Failure

If either (i) three (3) Service Level Defaults occur in any six (6) month period, or (ii) the Problem Management Process, as defined in the Commonwealth Computing Procedures Manual (CCPM), has identified a Major recurring Problem not directly reflected in SLA performance and there is no formal Chronic Service Issue project underway to address such Problem (each a "Service Delivery Failure" or “SDF”) , then within thirty (30) days of the occurrence of such Service Delivery

Failure, Offeror will provide the Commonwealth with a written plan (the "SD (Service Delivery) Service Improvement Plan") for improving the Offeror's performance to address the Service Delivery Failure, which plan will include a specific implementation timetable. The SD Service Improvement Plan will be subject to the Commonwealth's approval. Within 30 days of the Commonwealth's approval, or such other timeframe agreed to by the Commonwealth, Offeror will implement the SD Service Improvement Plan, which will include making timely and appropriate investments in people, processes and technology. In addition, the Offeror will demonstrate to the Commonwealth's reasonable satisfaction, that the changes implemented by Offeror have been made in normal operational processes to sustain compliant performance results in the future.

If Offeror fails to implement the SD Service Improvement Plan in the specified timetable, or if after the implementation of the SD Service Improvement Plan performance has not consistently improved, Offeror will be liable for a Service Level Credit in an amount equal to 10 percent (10%) of the then-current monthly invoice (the "SDF Credit"). The SDF Credit will be applied to the monthly invoice until such time as Offeror has demonstrated, for three (3) consecutive months, effective Service delivery, as evidenced by satisfying the criteria specified in the Problem Management RCA process related to the Service and/or no reoccurrence of the Service Level Defaults which triggered the applicable Service Delivery Failure. The SDF Credit will not be subject to Earnback. Under no circumstances shall the imposition of the SDF Credit described above or the Commonwealth's exercise of any other rights hereunder be construed as the Commonwealth's sole or exclusive remedy for any failures described hereunder. SDF Credits are not to be considered a part of the At-Risk Amount calculation in relation or Service Levels and are a separate commitment from the Offeror indicating the Offeror’s commitment to delivering service.

Further, the Offeror will work with the Commonwealth to define and document a repeatable Chronic Service Issue Resolution process in the Problem Management section of the Service Management Manual to be effective on the Effective Date. At a minimum, the process should address:

8.1 Establishment of a project team to drive and manage the process improvement

8.2 Approach to development of an Improvement Plan which will include milestones, resources and dependencies

8.3 Approach to Program Management of Plan implementation including integration of improvements/changes into daily operational processes

8.4 Implementation of Progress Reporting within the Offerors management structure, the Commonwealth and the Commonwealth Customers

8.5 Closure process to transition solution into normal operations including alignment of processes defined in the Service Management Manual

9 Commencement of Obligations

The obligations set forth herein shall commence on the first full month of service delivery in accordance with provisions set forth in Section 7.1 above.

10 Cooperation

The achievement of the Service Levels by the Offeror may require the coordinated, collaborative effort of the Offeror with other Third Parties. The Offeror will provide a single point of contact for the prompt resolution of all Service-Level Defaults and all failures to provide high quality Services to the Commonwealth, regardless of whether the reason for such Service-Level Defaults, or failure to provide high-quality Services to the Commonwealth, was caused by the Offeror.

11 Improvement Plan for Key Measurements

If the Offeror fails to satisfy any Key Measurement for three (3) months in any rolling six (6) month period, the Offeror shall provide the Commonwealth with a written plan for improving the Offeror's performance to satisfy the Key Measurement within thirty (30) days of the third (3rd) failure to meet the Service Level for the Key Measurement. At Offeror's sole cost and expense, the Offeror shall promptly implement such plan. If Offeror fails to implement the plan in the specified timetable, or if after ninety (90) days after any such implementation of the plan, the Key Measurement has not consistently improved, then the Commonwealth may at its option declare that such failure will constitute a Service Delivery Failure and Offeror will comply with the requirements of Section 8 above.

12 Measuring Tools

As of the Effective Date, the measuring tools and methodologies set forth in Schedule J.3 Datacenter SLA Definitions represent acceptable measuring tools and methodologies for the Critical Measurements and Key Measurements designated.

If there are any Critical Measurement Service Levels for which the measuring tools and methodologies have not been agreed upon by the Commonwealth and the Offeror and for which measuring tools are not included in Schedule J.3, and the Offeror fails to propose a measuring tool for such Critical Measurement that is acceptable to the Commonwealth prior to the date upon which the Offeror shall be responsible for Service Level performance and Service-Level Credits due for Service-Level Default, such failure shall be deemed a Service-Level Default for the Critical Measurement until the Offeror proposes and implements such acceptable measuring tool. The Commonwealth will not unreasonably withhold approval for the Offeror's recommendation for an alternate tool.

Tools for new Critical Measurement Service Levels will be implemented according to the Change Control Procedures. Upon the Commonwealth's written notice approving a proposed alternate or new measurement tool, such tool shall be deemed automatically incorporated into Schedule J.3 as of the date for completion of implementation set forth in the Commonwealth's notification without requirement for an additional written amendment of this Agreement.

If, after the Effective Date or the implementation of tools for new Critical Measurements, the Offeror desires to use a different measuring tool for a Critical Measurement, the Offeror shall provide written notice to the Commonwealth, in which event the Parties will reasonably adjust the measurements as necessary to account for any increased or decreased sensitivity in the new measuring tools; provided that, if the Parties cannot agree on the required adjustment, the Offeror will continue to use the measuring tool that had been initially agreed to by the Parties.

It is not anticipated that changes in the measuring tools will drive changes in Service Levels; rather, the need to collect and accurately reflect the performance data should drive the development or change in performance monitoring tools. Offeror will configure all measuring tools to create an auditable record of each user access to the tool and any actions taken with respect to the data measured by or residing within the tool. All proposed measuring tools must include functionality enabling such creation of an auditable record for all accesses to the tool.

13 Times

Unless otherwise set forth herein, all references in this Schedule to times shall refer to definition as described in **Schedule A – Defined Terms**.

14 Single Incident/Multiple Defaults

If a single incident results in the failure of the Offeror to meet more than one Service Level, the Offeror shall issue Service Level Credits for every failure not to exceed the At-Risk Amount.

An example would be if a network component experienced a failure that denies access to ten subscribed services. The CMDB would identify in impacted service and Service Level Credits would be due on all ten services.

15 Exclusions

For purposes of calculating Actual Uptime and Availability, the Scheduled Uptime and Downtime shall not include any period of Downtime that is the result of scheduled time required to perform system maintenance (for example, preventive maintenance, system upgrades, etc.), provided that such time has been mutually agreed between the Parties and is scheduled so as to minimize the impact to the Commonwealth's business. The Offeror shall maintain Availability during such periods to the extent reasonably practicable.

16 Percentage Objectives

Both parties understand that certain Service Levels may not be measured against an objective of one hundred percent (100%), for example, Time (days, hours, etc.), defects, etc. where zero (0) hours/days and zero percent (0%), respectively, are the appropriate objectives. The calculations described in this Section will be modified when appropriate to reflect these objectives. For example, if the Service Level involved defects in lines of code where zero percent (0%) is the objective, lowest would be changed to highest in Item 1 of Section 7.1 herein, highest would be changed to lowest in Item 3.2.1 of Section 7.1 herein and one hundred percent (100%) would be changed to zero percent (0%) in Item 3 of Section 7.1.

Request for Proposal

RFP # 6100022698

Commonwealth of Pennsylvania
Office of Administration
Office for Information Technology

Data Center Computing Services

Schedule J.2

Datacenter Service Level Matrix

Description of Exhibit

This Schedule J.2 (Service Level Matrix) sets forth the following:

1. For Critical Measurements (CMs)

- the numeric measurements for Minimum Service Levels and Expected Service Levels;
- the timing regarding the commencement of obligations for each Critical Service Level
- a cross-reference to Schedule J.3 Datacenter SLA Definitions where the qualitative description of the Performance Category and the associated Critical Service Level can be found

2. For Key Measurements (KMs)

- the numeric measurements for Minimum Service Levels and Expected Service Levels;

Service Level Matrix

Ref [a]	Service Level Categories	Required	Earnback Minimum	Earnback Eligible	Measurement Window	SLA Class[b]	Default Remedy Type[c]
SL01	Application Infrastructure Availability Platinum	99.999%	99.999%	N	Monthly	CM	Monthly Invoice Amount for Impacted Service
SL02	Application Infrastructure Availability - Gold	99.990%	99.990%	N	Monthly	CM	Monthly Invoice Amount for Impacted Service
SL03	Application Infrastructure Availability - Silver	99.900%	99.400%	Y	Monthly	CM	Monthly Invoice Amount for Impacted Service
SL04	Application Infrastructure Availability -Bronze	99.400%	99.200%	Y	Monthly	CM	Monthly Invoice Amount for Impacted Service
SL05	Application Infrastructure Availability -Basic	98.500%	98.500%	N	Monthly	CM	Monthly Invoice Amount for Impacted Service
SL06	Resolution Time - Severity Level 1 Incidents	97.500%	96.000%	Y	Monthly	CM	Monthly Invoice Amount for Impacted Service
SL07	Resolution Time - Severity Level 2	97.500%	96.000%	Y	Monthly	CM	Monthly Invoice Amount for Impacted Service
SL08	Resolution Time - Severity Level 3/4	97.500%	96.000%	Y	Monthly	CM	Monthly Invoice Amount for Impacted Service
SL09	Solution Request Fulfillment	95.000%	90.000%	Y	Monthly	CM	Monthly Invoice Amount for Impacted Service
SL10	Standard Service Request Fulfillment	95.000%	90.000%	Y	Monthly	CM	Monthly Invoice Amount for Impacted Service
SL11	Completion of Project/Solution Phase	95.000%	90.000%	Y	Monthly	CM	Monthly Invoice Amount for Impacted Service
SL12	Solution and Procurement Proposals Delivered	95.000%	90.000%	Y	Monthly	CM	Monthly Invoice Amount for Impacted Service
SL13	CMDB Content Accuracy and Timeliness	98.000%	95.000%	Y	Monthly	CM	$10,000.00 Credit on Invoice
SL14	Software License Renewal Timeliness	99.900%	99.500%	Y	Monthly	CM	$5,000.00 Credit on Invoice
SL15	Successful Backups	97.000%	96.000%	Y	Monthly	CM	Monthly Invoice Amount for Impacted Service
SL16	Successful Recoveries	99.000%	98.000%	Y	Monthly	CM	Monthly Invoice Amount for Impacted Service
SL17	Security Incident Notification Timeliness	100.000%	100.000%	N	Monthly	CM	$5,000.00 Credit on Invoice
SL18	Security Update Timeliness	100.000%	100.000%	N	Monthly	CM	$5,000.00 Credit on Invoice

Ref [a]	Service Level Categories	Required	Earnback Minimum	Earnback Eligible	Measurement Window	SLA Class[b]	Default Remedy Type[c]
SL19	Incident Management Communication – for Severity 1 Incidents	95.000%	90.000%	Y	Monthly	KM	Monthly Invoice Amount for Impacted Service
SL20	Root Cause Analysis Delivery	98.000%	96.000%	Y	Monthly	KM	Monthly Invoice Amount for Impacted Service
SL21	Chronic Problems	1.000%	2.000%	Y	Monthly	KM	Monthly Invoice Amount for Impacted Service
SL22	High Risk Security Patch Updates Timeliness	99.999%	99.900%	Y	Monthly	KM	$50,000.00 Credit on Invoice
SL23	Change Management Effectiveness	96.800%	93.750%	Y	Monthly	KM	$5,000.00 Credit on Invoice
SL24	Service Desk – Call Answer Time	< 27 Sec	< 30 Sec	Y	Monthly	KM	Monthly Invoice Amount for Impacted Service
SL25	Service Desk – Abandon Rate	3.000%	4.000%	Y	Monthly	KM	Monthly Invoice Amount for Impacted Service
SL26	Incident Ticket Quality	97.000%	95.000%	Y	Monthly	KM	$5,000.00 Credit on Invoice
SL27	Service Desk – Customer Satisfaction	4.2	3.9	Y	Monthly	KM	Monthly Invoice Amount for Impacted Service
SL28	Batch Scheduling Launched on Time	1.00	0.99	Y	Monthly	KM	Monthly Invoice Amount for Impacted Service
SL29	Batch Processing Completed Successfully	99.900%	99.500%	Y	Monthly	KM	Monthly Invoice Amount for Impacted Service
SL30	Reports Delivered On Time	10.00	5.00	Y	Monthly	KM	$10,000.00 Credit on Invoice
SL31	Off-Site Media Management	95.000%	90.000%	Y	Monthly	KM	Monthly Invoice Amount for Impacted Service

Notes:

(a) Ref- See Schedule J.3 Datacenter SLA Definitions for detailed description of the Service Level metrics.

(b) SLA Class as defined in Schedule J.1.

-- SLA Class "CM" means "Critical Measurement"

-- SLA Class "KM" means "Key Measurement"

(c) Amount listed for Key Measurements to be used in the event the Key Measurement becomes a Critical Measurement through the Change Management Process. While the Service Level remains a Key Measurement no Default Remedies are due.

Request for Proposal

RFP # 6100022698

Commonwealth of Pennsylvania
Office of Administration
Office for Information Technology
Data Center Computing Services

Schedule J.3

Datacenter SLA Definitions

CONTENTS

1. OFFEROR GUIDELINES....4

1.1. Offeror Instructions....4

1.2. Service Level Class Definitions....4

2. SERVICE LEVEL DETAILS....4

SL01 Application Infrastructure Availability – Platinum....5

SL02 Application Infrastructure Availability – Gold....6

SL03 Application Infrastructure Availability – Silver....7

SL04 Application Infrastructure Availability – Bronze....8

SL05 Application Infrastructure Availability – Basic....9

SL06 Resolution Time - Severity Level 1 Incidents....10

SL07 Resolution Time - Severity Level 2....12

SL08 Resolution Time - Severity Level 3/4....14

SL09 Solution Request Fulfillment....16

SL10 Standard Service Request Fulfillment....17

SL11 Completion of Project/Solution Phase....18

SL12 Solution and Procurement Proposals Delivered....19

SL13 CMDB Content Accuracy and Timeliness....20

SL14 Software License Renewal Timeliness....22

SL15 Successful Backups....24

SL16 Successful Recoveries....25

SL17 Security Incident Notification Timeliness....26

SL18 Security Update Timeliness....27

SL19 Incident Management Communication – for Severity 1 Incidents....28

SL20 Root Cause Analysis Delivery....30

SL21 Chronic Problems....32

SL22 High Risk Security Patch Updates....34

SL23 Change Management Effectiveness....35

SL24 Service Desk – Call Answer Time....37

SL25 Service Desk – Abandon Rate....38
SL26 Incident Ticket Quality....39
SL27 Service Desk – Customer Satisfaction....41
SL28 Batch Scheduling Launched on Time....42
SL29 Batch Processing Completed Successfully....43
SL30 Reports Delivered On Time....44
SL31 Off-Site Media Management....45
SLXX Name (Template)....46

3. NOTES....47

4. ADDITIONAL DEFINITIONS....47

1. Offeror Guidelines

This Schedule contains specific service level requirements that the Offeror must meet in order to perform the requested Services. The Offeror must respond to the requirements contained in this Schedule according to the instructions provided below.

1.1. Offeror Instructions

- The Offeror's response to the RFP should reflect and comply with the information contained in this Schedule.
- The Offeror will complete the following sections in each of the Critical Measurements and Key Measurements:
  - Collection Process – identify how the measurement data will be collected
  - Reporting Tools – identify any tools, automated or manual, that will be used
  - Raw Data Storage (Archives) – identify where data will be stored and accessible by the Commonwealth for further analysis
  - Reporting Format/s – identify the proposed reporting format

1.2. Service Level Class Definitions

There are two classes of Service Level performance metrics used, Critical Measurements (CMs) and Key Measurements (KMs).

- **Critical Measurements (CMs)** are performance measurements defined for the most important service areas. CMs will have associated fees, e.g. Performance Credits, payable by the Offeror to Commonwealth for missed CMs according to the terms of the negotiated contract.

- **Key Measurements (KMs)** are performance target measurements for non-critical service areas. KMs are not eligible for Performance Credits. Key Measures cover less critical service deliverables, sub processes or interim activities that are related to CM performance, and are reflective of overall effective and efficient service performance management. Based on periodic contractual SLA reviews, adjustments may be negotiable and KMs may be promoted to CMs.

Service Level measurement and reporting normally begins immediately following the Service Commencement Date. However, to allow for stabilization where appropriate, application of Performance Credits may be reduced or waived for some period of time (to be negotiated) after the Service Commencement Date.

2. Service Level Details

The following pages describe each Service Level, its calculation, and other details relevant to the Service Level.

SL01 Application Infrastructure Availability – Platinum

Service Level Reference	Description
Application Infrastructure Availability– Platinum	
Service Category	Availability
Metric Description	This Service Level measures the percentage of time the Applications are Available during the applicable Measurement Window. This measurement is by application, not by server instance. Availability is defined by whether the application residing on any of the associated server instances is available to users. Targeted Applications will be determined by the Commonwealth based on the critical nature of the Agency Application.
Metric Inclusions	Server Instances and related CIs supporting Targeted Applications are identified in the CMDB. Scheduled hours of operations and maintenance windows for each infrastructure element related to the Targeted Applications will be maintained in the Commonwealth Computing Procedures Manual.
Metric Exclusions	• All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** The Service Level calculation for "Targeted Applications Infrastructure Availability" is the sum of Actual Uptime for the individual Applications divided by the sum of expected, scheduled Uptime for the Applications, with the result expressed as a percentage. • = 1 – ((Sum of Minutes the Application is not Available) / ((1440 Minutes Per Day) X (Calendar Days In Month))) expressed as a percentage
Collection Process	*[Offeror to Complete]*
Reporting Tools / Data Source(s)	*[Offeror to Complete]*
Data Storage (Archives)	*[Offeror to Complete]*
Reporting Format/s	*[Offeror to Complete]*
Service Level Reporting Window	Monthly

SL02 Application Infrastructure Availability – Gold

Service Level Reference	Description
Application Infrastructure Availability – Gold	
Service Category	Availability
Metric Description	This Service Level measures the percentage of time the Applications are Available during the applicable Measurement Window. This measurement is by application, not by server instance. Availability is defined by whether the application residing on any of the associated server instances is available to users. Targeted Applications will be determined by the Commonwealth based on the critical nature of the Agency Application.
Metric Inclusions	Server Instances and related CIs supporting Targeted Applications are identified in the CMDB. Scheduled hours of operations and maintenance windows for each infrastructure element related to the Targeted Applications will be maintained in the Commonwealth Computing Procedures Manual.
Metric Exclusions	• All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** The Service Level calculation for "Targeted Applications Infrastructure Availability" is the sum of Actual Uptime for the individual Applications divided by the sum of expected, scheduled Uptime for the Applications, with the result expressed as a percentage. • = 1 – ((Sum of Minutes the Application is not Available) / ((1440 Minutes Per Day) X (Calendar Days In Month))) expressed as a percentage
Collection Process	*[Offeror to Complete]*
Reporting Tools / Data Source(s)	*[Offeror to Complete]*
Data Storage (Archives)	*[Offeror to Complete]*
Reporting Format/s	*[Offeror to Complete]*
Service Level Reporting Window	Monthly

SL03 Application Infrastructure Availability – Silver

Service Level Reference	Description
Application Infrastructure Availability– Silver	
Service Category	Availability
Metric Description	This Service Level measures the percentage of time the Applications are Available during the applicable Measurement Window. This measurement is by application, not by server instance. Availability is defined by whether the application residing on any of the associated server instances is available to users. Targeted Applications will be determined by the Commonwealth based on the critical nature of the Agency Application.
Metric Inclusions	Server Instances and related CIs supporting Targeted Applications are identified in the CMDB. Scheduled hours of operations and maintenance windows for each infrastructure element related to the Targeted Applications will be maintained in the Commonwealth Computing Procedures Manual.
Metric Exclusions	• All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** The Service Level calculation for "Targeted Applications Infrastructure Availability" is the sum of Actual Uptime for the individual Applications divided by the sum of expected, scheduled Uptime for the Applications, with the result expressed as a percentage. • = 1 – ((Sum of Minutes the Application is not Available) / ((1440 Minutes Per Day) X (Calendar Days In Month))) expressed as a percentage
Collection Process	*[Offeror to Complete]*
Reporting Tools / Data Source(s)	*[Offeror to Complete]*
Data Storage (Archives)	*[Offeror to Complete]*
Reporting Format/s	*[Offeror to Complete]*
Service Level Reporting Window	Monthly

SL04 Application Infrastructure Availability – Bronze

Service Level Reference	Description
Application Infrastructure Availability– Bronze	
Service Category	Availability
Metric Description	This Service Level measures the percentage of time the Applications are Available during the applicable Measurement Window. This measurement is by application, not by server instance. Availability is defined by whether the application residing on any of the associated server instances is available to users. Targeted Applications will be determined by the Commonwealth based on the critical nature of the Agency Application.
Metric Inclusions	Server Instances and related CIs supporting Targeted Applications are identified in the CMDB. Scheduled hours of operations and maintenance windows for each infrastructure element related to the Targeted Applications will be maintained in the Commonwealth Computing Procedures Manual.
Metric Exclusions	• All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** The Service Level calculation for "Targeted Applications Infrastructure Availability" is the sum of Actual Uptime for the individual Applications divided by the sum of expected, scheduled Uptime for the Applications, with the result expressed as a percentage. • = 1 – ((Sum of Minutes the Application is not Available) / ((1440 Minutes Per Day) X (Calendar Days In Month))) expressed as a percentage
Collection Process	*[Offeror to Complete]*
Reporting Tools / Data Source(s)	*[Offeror to Complete]*
Data Storage (Archives)	*[Offeror to Complete]*
Reporting Format/s	*[Offeror to Complete]*
Service Level Reporting Window	Monthly

SL05 Application Infrastructure Availability – Basic

Service Level Reference	Description
Application Infrastructure Availability - Basic	
Service Category	Availability
Metric Description	This Service Level measures the percentage of time the Applications are Available during the applicable Measurement Window. This measurement is by application, not by server instance. Availability is defined by whether the application residing on any of the associated server instances is available to users. Targeted Applications will be determined by the Commonwealth based on the critical nature of the Agency Application.
Metric Inclusions	Server Instances and related CIs supporting Targeted Applications are identified in the CMDB. Scheduled hours of operations and maintenance windows for each infrastructure element related to the Targeted Applications will be maintained in the Commonwealth Computing Procedures Manual.
Metric Exclusions	• All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** The Service Level calculation for "Targeted Applications Infrastructure Availability" is the sum of Actual Uptime for the individual Applications divided by the sum of expected, scheduled Uptime for the Applications, with the result expressed as a percentage. • = 1 – ((Sum of Minutes the Application is not Available) / ((1440 Minutes Per Day) X (Calendar Days In Month))) expressed as a percentage
Collection Process	*[Offeror to Complete]*
Reporting Tools / Data Source(s)	*[Offeror to Complete]*
Data Storage (Archives)	*[Offeror to Complete]*
Reporting Format/s	*[Offeror to Complete]*
Service Level Reporting Window	Monthly

SL06 Resolution Time - Severity Level 1 Incidents

Service Level Reference	Description
Resolution Time - Severity Level 1 Incidents	
Service Category	Incident and Problem Resolution
Metric Description	This Service Level measures the percentage of time Offeror resolves Severity Level 1 events within the applicable time period. Also known as "Mean Time To Resolve" (MTTR) for Severity Level 1 Incidents.
Metric Inclusions	Includes all Applications Infrastructure components as defined by the CMDB and Severity Level 1 events that are assigned to the appropriate Service Level. The time limits for the resolution of each are as listed below. Time frame for resolution shall be based on the Tier designation for the highest mainframe, server or instance associated with the respective incident. For incidents not associated with a specific Mainframe, Server, or Instance, the resolution timeframe shall be measured as a Silver Tier. Platinum < 90 minutes Gold < 120 minutes Silver < 180 minutes Bronze < 240 Minutes
Metric Exclusions	• All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** The Service Level calculation for "Resolution Time – Severity Level 1" is the total number of Incidents that are or become Severity Level 1 that are Resolved within the relevant Resolution Time specified, divided by the total number of Incidents that are or become Severity Level 1 during the applicable Measurement Window, with the result expressed as a percentage. • = (Number of Severity Level 1 Incidents Resolved within Limit) / (Total Number of Severity Level 1 Incidents) expressed as a percentage
Collection Process	*[Offeror to Complete]*
Reporting Tools / Data Source(s)	*[Offeror to Complete]*

Data Storage (Archives)	*[Offeror to Complete]*
Reporting Format/s	*[Offeror to Complete]*
Service Level Reporting Window	Monthly

SL07 Resolution Time - Severity Level 2

Service Level Reference	Description
Resolution Time - Severity Level 2	
Service Category	Incident and Problem Resolution
Metric Description	This Service Level measures the percentage of time Offeror resolves Problems within the applicable time periods. Also known as "Mean Time To Resolve" (MTTR) for Severity Level 2 Incidents.
Metric Inclusions	Includes all Mainframes, Servers, and Instances associated with Targeted Applications and other Severity Level 2 events not associated with Servers or Instances. The time limits for the resolution of each mainframe, server or instance are as listed below. Time frame for resolution shall be based on the Tier designation for the highest mainframe, server or instance associated with the respective incident. For incidents not associated with a Mainframe, Server, or Instance, resolution shall be measured as Silver Tier (< 360 minutes). Platinum < 90 minutes Gold < 180 minutes Silver < 360 minutes Bronze < 960 Minutes
Metric Exclusions	• All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** The Service Level calculation for "Resolution Time – Severity Level 2" is the total number of Incidents that are or become Severity Level 2 that are Resolved within the relevant Resolution Time specified, divided by the total number of Incidents that are or become Severity Level 2 during the applicable Measurement Window, with the result expressed as a percentage. • = (Number of Severity Level 2 Incidents Resolved within Limit) / (Total Number of Severity Level 2 Incidents) expressed as a percentage
Collection Process	*[Offeror to Complete]*
Reporting Tools / Data Source(s)	*[Offeror to Complete]*
Data Storage (Archives)	*[Offeror to Complete]*

Reporting Format/s	*[Offeror to Complete]*
Service Level Reporting Window	Monthly

SL08 Resolution Time - Severity Level 3/4

Service Level Reference	Description
Resolution Time - Severity Level 3/4	
Service Category	Incident and Problem Resolution
Metric Description	This Service Level measures the percentage of time Offeror resolves Incidents within the applicable time periods. Also known as "Mean Time To Resolve" (MTTR) for Severity Level 3 and Severity Level 4 Incidents.
Metric Inclusions	Severity Level 3 - For all Severity Level 3 Incidents , the incident shall be resolved within 3,780 Business Minutes (i.e. 63 hours) Severity Level 4 - For all Severity Level 4 Incidents, the incident shall be resolved within 4,860 Business Minutes (i.e. 81 hours or 9 business days) Total Business Minutes shall be measured during only those minutes between 8:00 AM and 5:00 PM inclusive, Monday through Friday inclusive (1 Business day = 9 Business hours = 540 Business minutes); (1 Business Week = 2,700 minutes)
Metric Exclusions	• All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	8:00AM – 5:00 PM
Days of Measurement	Monday through Friday
Calculation	• **Summary:** The Service Level calculation for "Resolution Time – Severity Level 3/4" is the total number of Incidents that are or become Severity Level 3 or 4 that are Resolved within the relevant Resolution Time specified, divided by the total number of Incidents that are or become Severity Level 3 or 4 during the applicable Measurement Window, with the result expressed as a percentage. • = ((Number of Severity Level 3 Incidents Resolved within Limit) +(Number of Severity Level 4 Incidents Resolved within Limit)) / ((Total Number of Severity Level 3 Incidents) + (Total Number of Severity Level 4 Incidents)) expressed as a percentage
Collection Process	*[Offeror to Complete]*
Reporting Tools / Data Source(s)	*[Offeror to Complete]*
Data Storage (Archives)	*[Offeror to Complete]*
Reporting Format/s	*[Offeror to Complete]*

Service Level Reporting Window	Monthly

SL09 Solution Request Fulfillment

Service Level Reference	Description
Solution Request Fulfillment	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the percentage of time Offeror successfully implements a Solution Request within the timeframe committed to the requester as measured in the applicable Measurement Window. All phases of the Solution implementation process from the Commonwealth Customer approval of the Solution Proposal through implementation and the Commonwealth Customer acceptance into production are included in this measure.
Metric Inclusions	For purposes of calculating this Service Level, only those requests which require a solution proposal that has been accepted by the State will be included in the calculation. Solution Requests without a production date established by the time the order is received will be counted as a "missed" expectation.
Metric Exclusions	None
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is the total number of projects that are successfully completed during the applicable Measurement Window on are before the due date specified in the applicable Solution Proposal and/or a subsequent project plan, divided by the total number of projects that should have been completed during the applicable Measurement Window, with the result expressed as a percentage. • = (Number of Solution Requests Completed within Limit) / (Total Number of Solution Requests) expressed as a percentage
Collection Process	*[Offeror to Complete]*
Reporting Tools / Data Source(s)	*[Offeror to Complete]*
Data Storage (Archives)	*[Offeror to Complete]*
Reporting Format/s	*[Offeror to Complete]*
Service Level Reporting Window	Monthly

SL10 Standard Service Request Fulfillment

Service Level Reference	Description
Standard Service Request Fulfillment	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the percentage of time Offeror successfully completes Standard Service Requests that do not require a purchase or a solution proposal to be approved by the State. Specific target timeframes are either established in the CCPM or a specific commitment date outside of the standard timeframe may be established at the State's discretion. Examples of these types of requests are provision of ID access, upgrade to a new OS version, run a special batch job, etc.
Metric Inclusions	Included as Standard Service Requests shall be an agreed upon set of service requests as specified in the Commonwealth Computing Procedures Manual.
Metric Exclusions	• Elapsed time waiting for the Commonwealth or a Commonwealth Customer's required approval or hold shall be excluded. • All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is the total number of Standard Service Requests successfully completed by Offeror during the applicable Measurement Window and within the required timeframes specified in Commonwealth Compute Procedure Manual (CCPM) or other agreed to date, divided by the number of Standard Service Requests that should have been completed by Offeror during the applicable Measurement Window, with the result expressed as a percentage. • = (Number of Standard Requests Completed within Limit) / (Total Number of Standard Requests) expressed as a percentage
Collection Process	*[Offeror to Complete]*
Reporting Tools / Data Source(s)	*[Offeror to Complete]*
Data Storage (Archives)	*[Offeror to Complete]*
Reporting Format/s	*[Offeror to Complete]*
Service Level Reporting Window	Monthly

SL11 Completion of Project/Solution Phase

Service Level Reference	Description
Completion of Project/Solution Phase	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the percentage of time Offeror successfully completes a phase (e.g. procurement, floor prep, network prep, physical install, turn-up and test, production) milestone no later than the committed timeframe. All phases of the Solution implementation process following the Commonwealth Customer approval of the Solution Proposal through implementation and the Commonwealth Customer acceptance into production are included in this measure.
Metric Inclusions	For purposes of calculating this Service Level, only those requests which require a solution proposal or project plan that has been accepted by the State and a production date established will be included in the calculation. If a milestone is missed, the rescheduled milestone will also be included in the measurement
Metric Exclusions	All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is the total number of Project or Solution Requests successfully completed by Offeror during the applicable Measurement Window and within the required timeframes specified in Commonwealth Compute Procedure Manual (CCPM) or other agreed to date, divided by the number of Project and Solution Requests that should have been completed by Offeror during the applicable Measurement Window, with the result expressed as a percentage • = (Number of Project/Solution Requests Completed within Limit) / (Total Number of Project/Solution Requests) expressed as a percentage
Collection Process	*[Offeror to Complete]*
Reporting Tools / Data Source(s)	*[Offeror to Complete]*
Data Storage (Archives)	*[Offeror to Complete]*
Reporting Format/s	*[Offeror to Complete]*
Service Level Reporting Window	Monthly

SL12 Solution and Procurement Proposals Delivered

Service Level Reference	Description
Solution and Procurement Proposals Delivered	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the percentage of time Offeror provides a viable proposal to the State, in response to a solution or procurement request, within the timeframe established in the Commonwealth Computing Procedures Manual for commodity and standard requests or a jointly agreed to commitment date for custom requests.
Metric Inclusions	Each proposal submitted to the State will be considered a measurable event. If there are multiple proposals for one request due to requirements changes then subsequent iterations will be counted as another event. Each will count as an event and an opportunity to succeed or fail.
Metric Exclusions	• All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is the total number of viable proposals submitted to the State during the applicable Measurement Window on or before the due date determined from the Commonwealth Computing Procedures Manual for Standard and Commodity Requests or jointly agreed for custom requests, divided by the total number of proposals that should have been submitted during the applicable Measurement Window, with the result expressed as a percentage. • = (Number of Solution and Procurement Proposal Requests Completed within interval) / (Total Number of Solution and Procurement Proposal Requests) expressed as a percentage
Collection Process	*[Offeror to Complete]*
Reporting Tools / Data Source(s)	*[Offeror to Complete]*
Data Storage (Archives)	*[Offeror to Complete]*
Reporting Format/s	*[Offeror to Complete]*
Service Level Reporting Window	Monthly

SL13 CMDB Content Accuracy and Timeliness

Service Level Reference	Description
CMDB Content Accuracy and Timeliness	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the percentage of an audited statistically valid sample of Inventory Records (as defined below) during the Measurement Window that is determined to be Accurate (as defined below) by such audits.
Metric Inclusions	The audited sample for this Service Level must contain a number of randomly selected CMDB Inventory Records that is reasonably acceptable to the Commonwealth. The random selection shall be a statistically significant stratified random sampling representing all Commonwealth Customers each month. **Definitions for purposes of this Service Level:** "Accurate" means all Critical Inventory Attributes are correctly and completely populated in the CMDB Inventory of Record. "Critical Inventory Attributes" means those database fields in an Inventory Record that are essential for Offeror's successful delivery of Service and necessary for CoPA's successful performance of retained responsibilities, including architecture, IT planning, and reconciliation of invoices. Critical Inventory Attributes that shall be audited are set out in Commonwealth Computing Procedures Manual and may be modified over time in accordance with the Commonwealth Computing Procedures Manual. "CMDB Inventory of Record" means the inventory of CIs, including all Equipment and Software, to be created and maintained by Offeror in accordance with the CCPM. "Inventory Record" means the record for a single item of Equipment or Software in the Inventory of Record, including all of the Critical Inventory Attributes for that item.
Metric Exclusions	• All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is the total number of CMDB Inventory Records that are audited during the applicable Measurement Window and that are Accurate, divided by the total number of Inventory Records that are audited during the applicable Measurement Window, with the result expressed as a percentage.

	• = ((Number of Valid Records Found) / (Total Number of Records Audited)) expressed as a percentage
Collection Process	*[Offeror to Complete]*
Reporting Tools / Data Source(s)	*[Offeror to Complete]*
Data Storage (Archives)	*[Offeror to Complete]*
Reporting Format/s	*[Offeror to Complete]*
Service Level Reporting Window	Monthly

SL14 Software License Renewal Timeliness

Service Level Reference	Description
Software License Renewal Timeliness	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the timeliness of all license and maintenance renewals for software managed by Offeror.
Metric Inclusions	This SLA includes the renewal of software licenses included in the Agreement and hardware maintenance agreements included in Hardware Service Charges (HSC) to a the Commonwealth Customer (e.g. renewal of SSL certificates, Application Utility software, custom solution hardware (covered by a maintenance agreement) charged to the Commonwealth Customer through the HSC).
Metric Exclusions	• Renewals for software or maintenance purchased outside of this contract by the Commonwealth or the Commonwealth Customers and not included in Offeror's charges to the Commonwealth are excluded. • All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	This Service Level measures the timeliness of all license and maintenance renewals for software managed by Offeror.
Days of Measurement	N/A
Calculation	• **Summary:** Renewals are routinely expected to be installed ten (10) or more Business Days prior to the renewal due date for the item or service. (Renewal due date is the date when the current license or maintenance contract expires.) The Service Level calculation for "Software License Renewal Timeliness" is a percentage derived from the total number of all renewals processed divided by the total number due for the month that were renewed before the renewal expiration date without disruption in service. • = ((Successful Software Renewals implemented within Time Frame) / (Total Software License Renewals Completed)) expressed as a percentage
Collection Process	*[Offeror to Complete]*
Reporting Tools / Data Source(s)	*[Offeror to Complete]*
Data Storage (Archives)	*[Offeror to Complete]*
Reporting Format/s	*[Offeror to Complete]*
Service Level Reporting Window	Monthly

SL15 Successful Backups

Service Level Reference	Description
Successful Backups	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the percentage of time Offeror completes backup jobs successfully during the applicable Measurement Window in accordance with the relevant criteria specified in the Commonwealth Computing Procedures Manual.
Metric Inclusions	Backup jobs include all registered backup clients (including but not limited to all file systems, databases, application files, operating systems, applications and respective data).
Metric Exclusions	• If there is an appropriate tool available and in use that captures open files, then the backup of open files are included as part of the backup. If there is not an appropriate tool available and in use for the capture of open files, then open files are skipped and not counted against this Service Level. Any batch jobs related to infrastructure backups, or other functionality exclusively for Offeror would be excluded. • All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level is the sum of the number of times Offeror completes backup jobs successfully and complete on time during the applicable Measurement Window divided by the of the sum of the number of times Offeror began or should have begun backup jobs within the applicable measurement window, with the result expressed as a percentage. • = ((Number of Successful Backups) / (Total Number of Backups Attempted)) expressed as a percentage
Collection Process	*[Offeror to Complete]*
Reporting Tools / Data Source(s)	*[Offeror to Complete]*
Data Storage (Archives)	*[Offeror to Complete]*
Reporting Format/s	*[Offeror to Complete]*
Service Level Reporting Window	Monthly

SL16 Successful Recoveries

Service Level Reference	Description
Successful Recoveries	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the percentage of time Offeror completes data recoveries successfully and on time during the applicable Measurement Window in accordance with the relevant criteria specified in the Commonwealth Computing Procedures Manual.
Metric Inclusions	Recoveries include all registered recovery clients (including but not limited to all file systems, databases, application files, operating systems, applications and respective data).
Metric Exclusions	• Any batch jobs related to infrastructure recoveries, or other functionality exclusive for the Offeror would be excluded. • All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is the total number of data recovery jobs that are completed successfully and on time in accordance with the relevant criteria set forth in the Commonwealth Computing Procedures Manual during the applicable Measurement Window, divided by the total number of data recovery jobs that were attempted or scheduled to be completed during the applicable Measurement Window, with the result expressed as a percentage. • = ((Number of Successful Recoveries) / (Total Number of Recoveries Attempted)) expressed as a percentage
Collection Process	*[Offeror to Complete]*
Reporting Tools / Data Source(s)	*[Offeror to Complete]*
Data Storage (Archives)	*[Offeror to Complete]*
Reporting Format/s	*[Offeror to Complete]*
Service Level Reporting Window	Monthly

SL17 Security Incident Notification Timeliness

Service Level Reference	Description
Security Incident Notification Timeliness	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the percentage of time Offeror completes identifying and notifying CoPA of detected security incidents in accordance with ITB-SEC024.
Metric Inclusions	Time required receiving and analyzing reactive and/or proactive incidents from any and all managed sources including, but not limited to, firewalls, intrusion detection/prevention devices, VPN appliances, switches, routers, and all other equipment over which Commonwealth traffic traverses. Time required contacting CoPA and reporting the incident in accordance with ITB-SEC024.
Metric Exclusions	• All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is the total number of Security Incidents reported in accordance with ITB SEC-024 using the procedure set forth in the Commonwealth Computing Procedures Manual, divided by the total number of detected security incidents, with the result expressed as a percentage. • = [(number of incidents reported in accordance with ITB SEC-024) / number of detected incidents)] expressed as a percentage
Collection Process	*[Offeror to Complete]*
Reporting Tools / Data Source(s)	*[Offeror to Complete]*
Data Storage (Archives)	*[Offeror to Complete]*
Reporting Format/s	*[Offeror to Complete]*
Service Level Reporting Window	Monthly

SL18 Security Update Timeliness

Service Level Reference	Description
Security Update Timeliness	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the percentage of time Offeror completes Security Updates successfully and on time during the applicable Measurement Window in accordance with the relevant criteria specified in the Commonwealth Computing Procedures Manual.
Metric Inclusions	Security Updates include all updates and changes designated as a Security Update at the time or request/order. These updates includes, but are not limited to, Security Patches, Firewall configuration changes, Proxy updates and changes, and Identity Management Changes.
Metric Exclusions	• Any batch jobs related to infrastructure recoveries, or other functionality exclusive for the Offeror would be excluded. • All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is the total number of Security update requests that are completed successfully and on time in accordance with the relevant criteria set forth in the Commonwealth Computing Procedures Manual during the applicable Measurement Window, divided by the total number of Security update requests that were requested to be completed during the applicable Measurement Window, with the result expressed as a percentage. • = ((Number of Security Updates) / (Total Number of Requested Security Updates)) expressed as a percentage
Collection Process	*[Offeror to Complete]*
Reporting Tools / Data Source(s)	*[Offeror to Complete]*
Data Storage (Archives)	*[Offeror to Complete]*
Reporting Format/s	*[Offeror to Complete]*
Service Level Reporting Window	Monthly

SL19 Incident Management Communication – for Severity 1 Incidents

Service Level Reference	Description
Incident Management Communication – for Severity 1 Incidents	
Service Category	Incident & Problem Resolution
Metric Description	This Service Level measures the percentage of time the Offeror provides the notices to the applicable Authorized Users within the following timeframes with respect to Incidents that are or become Severity 1 Incidents and that are not Resolved in less than one (1) hour from the Start Time for such Incident. • First notice: Within one hour of incident ticket creation • Subsequent notices: every 30 minutes A "notice" is defined as : • Verbal communication to Authorized User, as documented in the ticket • Bridge call including Authorized User, as documented in the ticket • Email to Authorized User, as documented in the ticket Such notices shall not be deemed to have been provided unless (a) the Authorized User that reported the Incident has been contacted by the Offeror and such notice of status has been provided or (b) Offeror has left a voice mail (or if not possible because the Authorized User does not have a voice mail box, sent an email or attempted some other reasonable means of communication) for the Authorized User.
Metric Inclusions	Includes all Priority 1 Incidents
Metric Exclusions	• Priority 2, 3 and 4 Incidents • Duplicate Incident Reports for the incident • All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is the total number of Incidents that are or become Severity 1 Incidents, that have Start Times during the applicable Measurement Window, that have actual Resolution Times of greater than one (1) hour and for which Offeror provided the applicable Authorized User the required notice(s) within the required timeframe(s) as set forth in this Section, divided by the total number of Incidents that are or become Severity 1 Incidents, that have Start Times during the applicable Measurement Window and that have actual Resolution Times of

	greater than one (1) hour, with the result expressed as a percentage. • = ((Number of Incidents with Communications within Established Intervals) / (Total Number of Severity 1 Incidents)) expressed as a percentage
Collection Process	*[Offeror to Complete]*
Reporting Tools / Data Source(s)	*[Offeror to Complete]*
Data Storage (Archives)	*[Offeror to Complete]*
Reporting Format/s	*[Offeror to Complete]*
Service Level Reporting Window	Monthly

SL20 Root Cause Analysis Delivery

Service Level Reference	Description
Root Cause Analysis Delivery	
Service Category	Incident & Problem Resolution
Metric Description	This Service Level measures the percentage of time Offeror reports the results of a Formal Root Cause Analyses for Service Restoral Incidents within the timeframes below during the Measurement Window: • RCA's due within ten (10) Business Days from the request of the RCA.
Metric Inclusions	An Authorized User may request a Formal RCA for incidents that require more in-depth analysis than required with the "normal" Root Cause Analysis process. The Formal RCA is documented and tracked within the Problem Management process, and upon completion, is presented by the Offeror Problem Management Team to the affected the Commonwealth Customer and the Commonwealth for review and approval. Offeror shall perform a "Formal" Root Cause Analysis with respect to any Service Restoral Incident, if requested by the Commonwealth, and that has a Start Time during the applicable Measurement Window.
Metric Exclusions	• Those Service Restoral Incidents for which the Commonwealth or the Commonwealth's Customer does not request a "Formal" Root Cause Analysis. • Duplicate Requests • All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is the total number of written Formal Root Cause Analyses that are delivered to the Commonwealth within the timeframes specified in this Section during the applicable Measurement Window, divided by the total number of written Formal Root Cause Analyses that should have been delivered to the Commonwealth during the applicable Measurement Window, with the result expressed as a percentage. • = ((Number of Formal Root Cause Analyses Delivered within Established Interval) / (Total Number of Formal Root Cause Analyses Due)) expressed as a percentage
Collection Process	*[Offeror to Complete]*

Reporting Tools / Data Source(s)	*[Offeror to Complete]*
Data Storage (Archives)	*[Offeror to Complete]*
Reporting Format/s	*[Offeror to Complete]*
Service Level Reporting Window	Monthly

SL21 Chronic Problems

Service Level Reference	Description
Chronic Problems	
Service Category	Incident & Problem Resolution
Metric Description	A "Chronic Problem" means a problem which meets any of the following criteria: 1. The existence two or more incidents with the same root cause for the same software, service, process, or hardware for which Offeror, the Commonwealth, or the Commonwealth Customer, have designated as a problem requiring a Root Cause Analysis with a Corrective Action Plan. 2. The existence of three or more service failures or outages for the same software, service, process, or hardware within the same month for any two (2) months within any rolling six (6) months. 3. The existence of three (3) or more service failures or outages for the same software, service, process, or hardware within any rolling six (6) month period for which no root cause has been determined. Multiple Incidents that are opened contemporaneously for the same software, service, process, or hardware due to the same root cause shall be deemed to be a single incident for purposes of this Service Level.
Metric Inclusions	All incidents and Problem Investigation reports for all services covered by any service level metric.
Metric Exclusions	• Problems which have a published Root Cause Analysis with an associated action plan approved by the Commonwealth Customers and which has all agreed corrective actions on schedule (not exceeding their completion dates) and have had no reoccurrences of the same failure may be excluded at the Offeror's request and the Commonwealth's approval. • All items defined in Note 2 at the bottom of this Schedule J.3 • Duplicate Incident Reports for the same Incident
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** Offeror's performance shall be measured by determining the total number of Problem that are or become Chronic Problem during the applicable Measurement Window. • ((the number of Chronic Problems) / (the total number of problems)) expressed as a percentage
Collection Process	*[Offeror to Complete]*

Reporting Tools / Data Source(s)	*[Offeror to Complete]*
Data Storage (Archives)	*[Offeror to Complete]*
Reporting Format/s	*[Offeror to Complete]*
Service Level Reporting Window	Monthly

SL22 High Risk Security Patch Updates

Service Level Reference	Description
High Risk Security Patch Updates	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the timeliness in which high-risk security patches are applied. All high risk security patches must be applied within five (5) Business Days from the date the software vendor or applicable industry guiding entity provides notice to the Offeror or other date as agreed to by the Commonwealth or the Commonwealth Customer.
Metric Inclusions	Includes those security patches for which the vendor or applicable industry guiding entity indicates is "high" risk.
Metric Exclusions	• Excludes low and medium risk patches • All items defined in Note 2 at the bottom of this Schedule J.J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is the total number of high risk security patches released five (5) Business Days prior to the beginning and end of the measurement window that were installed within five (5) Business Days divided by the total number of high risk security patches released five (5) Business Days prior to the beginning and end of the measurement window, with the result expressed as a percentage. • = ((Number of High Risk Intrusion Protection Updates Installed within Established Interval) / (Total Number of High Risk Intrusion Protection Updates Installed)) expressed as a percentage
Collection Process	*[Offeror to Complete]*
Reporting Tools / Data Source(s)	*[Offeror to Complete]*
Data Storage (Archives)	*[Offeror to Complete]*
Reporting Format/s	*[Offeror to Complete]*
Service Level Reporting Window	Monthly

SL23 Change Management Effectiveness

Service Level Reference	Description
Change Management Effectiveness	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the percentage of time Offeror successfully implements Changes to the Services.
Metric Inclusions	Changes are not successfully implemented if they: (i) do not comply with the Change Management procedures (including the Change Control Process), (ii) do not comply with the Change Management procedures detailed within the Commonwealth Computing Procedures Manual, (iii) cause Severity 1 Incidents or Severity 2 Incidents, within 168 hours of implementing the change, (iv) exceeds the reserved implementation or maintenance window as approved within the ITSM Change Request, or (v) are backed out.
Metric Exclusions	• Severity Level 1 and Severity Level 2 incidents that occur during the implementation window for the change and are resolved before the Implementation or Maintenance window ends. • All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is the number of changes that are successfully implemented by Offeror during the applicable Measurement Window, divided by the number of changes that should have been implemented by Offeror during the applicable Measurement Window, with the result expressed as a percentage. • = ((Number of Successful Change Management Requests) / (Total Number of Change Management Requests Scheduled during the period)) expressed as a percentage
Collection Process	*[Offeror to Complete]*
Reporting Tools / Data Source(s)	*[Offeror to Complete]*
Data Storage (Archives)	*[Offeror to Complete]*

Reporting Format/s	*[Offeror to Complete]*
Service Level Reporting Window	Monthly

SL24 Service Desk – Call Answer Time

Service Level Reference	Description
Service Desk – Call Answer Time	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the elapsed time an Authorized User is placed on hold after leaving the Interactive Voice Response or Automatic Call Distribution System to the time the phone call is answered by a live support technician.
Metric Inclusions	All phone calls to the Service Desk shall be included in the calculation of this Service Level with no exceptions for phone calls to the Service Desk during any period of Downtime.
Metric Exclusions	• All items defined in Note 2 at the bottom of this Schedule J.3 • Excludes the time a caller is listening to a Menu of choices before being routed to a helpdesk agent.
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is the total number of seconds, for all phone calls to the Service Desk during the applicable Measurement Window, between the time the phone caller first selects a menu option on the IVR or Automatic Call Distribution System for assistance by a live support technician to the time the phone call is verbally answered by a live support technician ready to start working on the phone call, divided by the total number of all phone calls to the Service Desk during the applicable Measurement Window. • = (Average Time a Call takes to be answered by Service Desk Agent) expressed in seconds
Collection Process	*[Offeror to Complete]*
Reporting Tools / Data Source(s)	*[Offeror to Complete]*
Data Storage (Archives)	*[Offeror to Complete]*
Reporting Format/s	*[Offeror to Complete]*
Service Level Reporting Window	Monthly

SL25 Service Desk – Abandon Rate

Service Level Reference	Description
Service Desk – Abandon Rate	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the percentage of phone calls to the Service Desk that are abandoned by the Authorized User after the Authorized User selected a service option and prior to a live support technician answering the phone call.
Metric Inclusions	All phone calls to the Service Desk shall be included in the calculation of this Service Level with no exceptions for phone calls to the Service Desk during any period of Downtime.
Metric Exclusions	• Calls disconnected prior to an automated voice response system completing the Menu of choices for callers are not counted as abandoned. • All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is the total number of phone calls to the Service Desk during the applicable Measurement Window that are abandoned by the Authorized User (prior to an automated voice response system answers), divided by the total number of phone calls to the Service Desk during the applicable Measurement Window, with the result expressed as a percentage. • = ((Number Of Abandoned Telephone Calls) / (Total Number Of Telephone Calls)) expressed as a percentage
Collection Process	*[Offeror to Complete]*
Reporting Tools / Data Source(s)	*[Offeror to Complete]*
Data Storage (Archives)	*[Offeror to Complete]*
Reporting Format/s	*[Offeror to Complete]*
Service Level Reporting Window	Monthly

SL26 Incident Ticket Quality

Service Level Reference	Description
Incident Ticket Quality	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the quality and timeliness of the Offeror's incident management and communication of incident management activities (as defined in the Commonwealth Computing Procedures Manual Commonwealth Computing Procedures Manual). Offeror must update the incident tickets at a minimum on the following frequencies:
Metric Inclusions	Includes a statistically valid random sample of Service Restorals and Service Requests closed during the Measurement Window, all priorities.
Metric Exclusions	• Excludes Change Requests (CRQ), Solution Requests (REQ), and Problem Management (PBI) • All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is the number of sampled tickets in the Measurement Window which meet the defined quality and communication frequency criteria divided by the total number of sampled tickets in the Measurement Window, with the result expressed as a percentage. • ((Number of service restorals and requests that met the interval) / (the total number of service restorals and requests)) expressed as a percentage
Collection Process	*[Offeror to Complete]*
Reporting Tools / Data Source(s)	*[Offeror to Complete]*
Data Storage (Archives)	*[Offeror to Complete]*
Reporting Format/s	*[Offeror to Complete]*

Service Restorals	**Service Requests**
P1: every 15 minutes	P1: Daily
P2: 30 minutes	P2: Weekly
P3: daily	P3: every 2 weeks
P4: weekly	P4: Monthly

Service Level Reporting Window	Monthly

SL27 Service Desk – Customer Satisfaction

Service Level Reference	Description
Service Desk – Customer Satisfaction	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the average scores of the customer satisfaction surveys taken on a random statistical sample of customers that had a service contact with the Offeror during the measurement period. The surveys will be conducted in accordance with the Commonwealth Computing Procedures Manual.
Metric Inclusions	Survey responses shall be on a five (5) point scale (with five (5) being the most satisfied) or shall reflect such other satisfaction criteria established pursuant to the survey design process.
Metric Exclusions	• All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** At the Commencement Date, This Service Level calculation is the sum of all scores for each response (question answered) for the Point of Service surveys that are returned during the applicable Measurement Window, divided by the total number of responses for all Point of Service surveys that are returned during the applicable Measurement Window. • = (Average Score of Surveys)
Collection Process	*[Offeror to Complete]*
Reporting Tools / Data Source(s)	*[Offeror to Complete]*
Data Storage (Archives)	*[Offeror to Complete]*
Reporting Format/s	*[Offeror to Complete]*
Service Level Reporting Window	Monthly

SL28 Batch Scheduling Launched on Time

Service Level Reference	Description
Batch Scheduling Launched on Time	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the percentage of time Offeror starts the Batch job schedules defined in the standard scheduling tool or manually scheduled at the established start time associated with such schedules specified in the Commonwealth Computing Procedures Manual.
Metric Inclusions	Scheduled Batch jobs include normally scheduled and recurring production jobs, as well as production jobs that are run on an as-needed basis.
Metric Exclusions	• Any batch jobs related to infrastructure backups, or other functionality exclusive for Offeror would be excluded. • All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is the total number of Batch job schedules defined in the standard scheduling tool that are started during the applicable Measurement Window at the established start time associated with such schedules as set forth in the Commonwealth Computing Procedures Manual, divided by the total number of Batch job schedules that should have been started during the applicable Measurement Window, with the result expressed as a percentage. • = (Number Of Batches Launched On Time) / (Total Number Of Batches Scheduled) expressed as a percentage
Collection Process	*[Offeror to Complete]*
Reporting Tools / Data Source(s)	*[Offeror to Complete]*
Data Storage (Archives)	*[Offeror to Complete]*
Reporting Format/s	*[Offeror to Complete]*
Service Level Reporting Window	Monthly

SL29 Batch Processing Completed Successfully

Service Level Reference	Description
Batch Processing Completed Successfully	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the percentage of time Offeror completes Batch jobs successfully and on time during the applicable Measurement Window in accordance with the relevant specifications located in the Commonwealth Computing Procedures Manual.
Metric Inclusions	Batch jobs include normally scheduled and recurring production jobs, as well as production jobs that are run on an as-needed basis. To be considered Successful the Batch must complete within the schedule window for that particular Batch Job.
Metric Exclusions	• Any batch jobs related to infrastructure backups, or other functionality exclusive for Offeror would be excluded. • All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is the total number of Batch jobs that are completed successfully and on time in accordance with the relevant criteria set forth in the Online CCPM repository during the applicable Measurement Window, divided by the total number of Batch jobs that should have been completed during the applicable Measurement Window, with the result expressed as a percentage. • = ((Number Of Successful Batches) / (Total Number Of Batches Scheduled)) expressed as a percentage
Collection Process	*[Offeror to Complete]*
Reporting Tools / Data Source(s)	*[Offeror to Complete]*
Data Storage (Archives)	*[Offeror to Complete]*
Reporting Format/s	*[Offeror to Complete]*
Service Level Reporting Window	Monthly

SL30 Reports Delivered On Time

Service Level Reference	Description
Reports Delivered On Time	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level for Reports delivered on time as outlined in Schedule K - Reports measures the percentage of time Offeror delivers the Reports on time in accordance with the requirements. Each Report provided with respect to a Critical Service Level or Key Measurement shall be deemed an individual Report for the purposes of calculating this Service Level.
Metric Inclusions	Schedules as set forth in the Commonwealth Computing Procedures Manual.
Metric Exclusions	• Any reports identified as Critical Monthly Reports in the Commonwealth Computing Procedures Manual and measured in Critical Service Levels. • All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	24x7
Days of Measurement	365
Calculation	• **Summary:** This Service Level calculation is a count of the total number of Reports that were not successfully delivered (i.e. on time and in compliance with content and format requirements) during the applicable Measurement Window. • = ((Number Of Reports Delivered On Time) / (Total Number Of Reports Scheduled To Be Delivered)) expressed as a percentage
Collection Process	*[Offeror to Complete]*
Reporting Tools / Data Source(s)	*[Offeror to Complete]*
Data Storage (Archives)	*[Offeror to Complete]*
Reporting Format/s	*[Offeror to Complete]*
Service Level Reporting Window	Monthly

SL31 Off-Site Media Management

Service Level Reference	Description
Off-Site Media Management	
Service Category	Other Service Management and Delivery
Metric Description	This Service Level measures the accuracy of the Offeror's management of off-site media, specifically the physical location and electronic tracking accuracy of off-site media. The measure is intended to sample one-twelfth of the universe of off-site media such that each the Commonwealth Customer's complete environment is sampled at least once per year.
Metric Inclusions	All media for which Offeror receives an off-site storage resource unit charge.
Metric Exclusions	• Virtual tapes and tapes retained in the Consolidated Data Centers or Non-Consolidated Service Locations. • All items defined in Note 2 at the bottom of this Schedule J.3
Hours of Measurement	N/A
Days of Measurement	N/A
Calculation	• **Summary:** This Service Level calculation is based on a statistically valid random sample representing one-twelfth of the universe of off-site media and is the sum of the number of times a tape is either physically in the correct location or electronically listed in the correct location divided by the total number of tapes in the random sample, with the result expressed as a percentage. • = ((Number Of Correct Audits) / (Total Number Of Audits))expressed as a percentage
Collection Process	*[Offeror to Complete]*
Reporting Tools / Data Source(s)	*[Offeror to Complete]*
Data Storage (Archives)	*[Offeror to Complete]*
Reporting Format/s	*[Offeror to Complete]*
Service Level Reporting Window	Monthly

SLXX Name (Template)

Service Level Reference	Description
SLA Name (Template)	
Service Category	
Metric Description	
Metric Inclusions	
Metric Exclusions	
Hours of Measurement	
Days of Measurement	
Calculation	
Collection Process	
Reporting Tools / Data Source(s)	
Data Storage (Archives)	
Reporting Format/s	
Service Level Reporting Window	

3. Notes

Note 1: Offeror's failure to achieve any Service Level will not constitute a Service Level Default or accrue toward a Service Level Termination Event to the extent such failure is directly attributable to any Force Majeure events as (as defined in Paragraph 65 of the Contract.

Note 2: Offeror's failure to achieve any Service Level will not constitute a Service Level Default or accrue toward a Service Level Termination Event to the extent such failure is directly attributable to any of the following:

(i) the failure or unavailability of equipment or other resources for which the Commonwealth is operationally and managerially responsible pursuant to the Contract,

(ii) changes made to the environment by the Commonwealth that were not communicated in accordance with the Change Control Procedure or other method agreed upon by the Parties, and

(iii) scheduled and approved maintenance windows.

4. Additional Definitions

1. "Accurate" means all Inventory Attributes are correctly and completely populated in the CMDB Inventory of Record.
2. "Bronze" is defined as a level of service that has a specific Availability value or Response time interval requirement.
3. "CMDB Inventory of Record" means the inventory of CIs, including all Equipment and Software, to be created and maintained by Offeror in accordance with the CCPM.
4. "Commonwealth Computing Procedures Manual" means the established procedural manual related to services offered within this procurement.
5. "Configuration Management Database" (CMDB) is defined as the complete database of all Hardware and software items that make up a service.
6. "Customer Request Date" means the customer requested due date (CRDD) in the Offeror's service management platform (SMP).
7. "Emergency Downtime" means downtime agreed by the Parties to enable maintenance and break fix
   i. necessary to address Service issues stemming from Force Majeure causes or
   ii. Otherwise agreed by the Commonwealth pursuant to the Emergency provisions of the Change Control Procedures.
8. "Gold" is defined as a level of service that has a specific Availability value or Response time interval requirement.
9. "Hold Time" or "Customer Time" is defined as a period of time when Offeror is prevented from progressing the investigation or repair of an incident (outage or degradation) due to Commonwealth required decisions or actions. Examples of this include, but are not limited to:

i. Not providing physical access to a facility pursuant to the Contract so that equipment can be tested or replaced

ii. Not releasing a Application or Server for testing

iii. Not providing accurate or complete information when opening an incident resulting in a Offeror inability to progress the resolution of the logged incident

iv. Not responding with necessary additional information upon request to enable the effective investigation or repair of a logged Service ID

v. related incident

vi. Commonwealth requested delays in the installation of required patches and/or upgrades

vii. Failure of user authentication services, unique end-user VPN client software issues, or other components managed by the Commonwealth. In every case in which Offeror intends to place an incident or ticket on Hold Time or Customer Time, Offeror will make the appropriate prior notification to the Commonwealth. Valid Hold Time and Customer Time is excluded as outage time in calculations of Service Level Availability and Time to Restore.

10. "Inventory Attributes" means those database fields in an Inventory Record that are essential for Offeror's successful delivery of Service and necessary for The Commonwealth's successful performance of retained responsibilities, including architecture, IT planning, and reconciliation of invoices. Inventory Attributes that shall be audited are set out in Commonwealth Computing Procedures Manual and may be modified over time in accordance with the Commonwealth Computing Procedures Manual.

11. "Inventory Record" means the record for a single item of Equipment or Software in the Inventory of Record, including all of the Inventory Attributes for that item.

12. "Major Degradation of Service" means a Service that tests as fully operational but is degraded below user expectations across a significant segment of the user population as determined by the Commonwealth.

13. "Non-Excluded Outage Minutes" is defined as a Minutes that are not considered Customer Time, Hold Time, Scheduled Downtime as defined within this Schedule J.3

14. "Resolution" is defined as removing a fault or degradation from the Commonwealth operational environment. Resolution is followed by notification to the Commonwealth and either performing further joint testing or receiving an approval to place the affected Service or Service ID back in operation.

15. "Response" or "Respond" is defined as Offeror taking and logging meaningful action to progress the testing and restoration of any Service ID, or, as the case may be, Security Services, that has an active Incident ticket opened in the Incident Management System as defined by the Incident and Problem Management Process which is part of the Process and Procedures Manual.

Examples of meaningful response actions include the following, all pursuant to the Policies and Procedures Manual:

- Calling the Commonwealth to obtain additional information to help progress the testing and restoration of the logged incident
- Requesting access to a facility
- Requesting release of a Service ID for testing

- Requesting contact information required to progress the incident management process
- Escalating the incident to technical support for additional testing and analysis

16. "Scheduled Availability" means 24/7/365, unless otherwise specified in a Service Level, minus Scheduled Downtime, Customer Time, Hold Time, and Emergency Downtime.

17. "Scheduled Downtime" means downtime expected and agreed by the Parties, expressed monthly, for which the underlying systems were taken off- line for routine or scheduled maintenance during the Measurement Window.

18. "Service ID" means the unique identifier assigned to a service by Offeror.

19. "Service Level Availability" shall mean the actual availability of access and all functionality of the Services described in a Service Level expressed as percentage of the Scheduled Availability for such Services.

20. "Severity Level" means a priority setting assigned to an incident or change that represents the impact the event has on service for the customer. This level is set by the person reporting the incident or requesting the change and may be adjusted by authorized personnel at the Commonwealth.

21. "Silver" is defined as a level of service that has a specific Availability value or Response time interval requirement.

22. "Standard Service Interval" means the corresponding period of time in the Standard Service Intervals in the Policy and Procedures Manual, including procedures regarding accuracy, completeness and changes to previously accepted orders. As of the Execution Date, the Standard Service Intervals are set forth in the document provided by the Offeror to the Commonwealth labeled [***to be completed by Offeror***].

23. For purposes of This Service Level Matrix, a "day" means a 24 hours period from the trigger for the measurement. For example, if a ticket is logged at 9:15am on Tuesday the 14th, a "day" ends at 9:15am on Wednesday day the 15th.

Request for Proposal

RFP # 6100022698

Commonwealth of Pennsylvania
Office of Administration
Office for Information Technology
Data Center Computing Services

Schedule K

Key Program Deliverables

Table of Contents

INTRODUCTION –PROGRAM DELIVERABLES 3
KEY PROGRAM DELIVERABLES 3
D-01 Datacenter Architecture Plan and Roadmap 3
D-02 Commonwealth Computing Procedures Manual (CCPM) 5
D-03 Technology Architecture and Refresh Approach 15
D-04 IT Service Continuity Architecture and Plan 17
D-05 Transition Management Plan 18
D-06 Agency Level DR Plan(s) 19
D-07 Security Management Plan 20
D-08 Facilities Management Plan 22
D-09 Security Risk and Vulnerability Assessment Report 23
D-10 Gap Analysis Report 23
D-11 Contract Management Plan 24
DELIVERABLE ACCEPTANCE CRITERIA MATRIX 25
EXAMPLE - DELIVERABLE ACCEPTANCE MATRIX 27

Introduction –Program Deliverables

This Schedule sets forth certain obligations of Offeror regarding Program Deliverables. The Offeror must deliver to the Commonwealth any Key Program Deliverables as described below, in format and content acceptable to the Commonwealth.

As specified below, Offeror shall provide each Key Program Deliverable on or before the date specified in this Schedule. The Key Program Deliverable Acceptance Criteria and the Commonwealth Sign-off Matrix will be developed prior to the Effective Date and will be in the format referenced below in this document.

Key Program Deliverables

D-01 Datacenter Architecture Plan and Roadmap

The Datacenter Architecture Plan and Roadmap will include the Offeror's proposed Datacenter Architecture that will be utilized to support the Project. The Datacenter Architecture Plan and Roadmap should include at minimum sections that support the following:

- 2+ Datacenter Architecture (with EDC) - describes the overall Datacenter Architecture used in the delivery of the Offeror's Enterprise Datacenter Services. This should include details on datacenter specifications, location, physical security, and capacity. The architecture will show how the Commonwealth's Enterprise Data Center (EDC) will be incorporated into the Offeror's overall datacenter capacity.

- Datacenter Network Architecture - describes the required network connectivity between each of the datacenters. Included are connection requirements to the Commonwealth's network COPANET. The Offeror will also describe its Internet connection to the proposed Datacenter(s).

- Datacenter Security Architecture - describes the security architecture used to ensure the confidentiality, integrity and availability of Commonwealth information and infrastructure systems. The Security Architecture will describe the security technology components such as firewalls, intrusion detection devices, virus detection, etc. that will be utilized in the Offerors solution. Datacenter Security implementation activities must be conducted in accordance with, but not limited to, leading industry and Commonwealth standards such as ISO 27001:2005 and ISO 27002:2005.

- Datacenter Technology Environment - describes the Datacenter technology used in the delivery of the Offeror's Enterprise Datacenter Services. A summary of the planned allocation of platforms within each of the proposed datacenters should be included. Note: more detailed technology specifications shall be provided in the *D-03 Technology Architecture and Refresh Approach* deliverable.

- Datacenter Implementation Roadmap – presents the detailed implementation plan for the enablement of the overall Datacenter Architecture. The Datacenter Implementation Roadmap shall Reference roles and responsibilities, as well as critical dates and timelines.

EDC Assessment		
D-01.01	Effective Date + 45 days	Offeror must assess the EDC facilities and provide a report to the Commonwealth as it pertains to: • Required security upgrades • Required HVAC and power upgrades • Required physical access to the EDC facility • Monitoring, maintain and reporting on EDC SLAs • Monitoring, maintaining and operating the installed infrastructure
Multi Datacenter Environment (2+ Architecture)		
D-01.02	Effective Date + 60 days – with quarterly updates	*Datacenter Architecture Plan and Roadmap* Datacenter Architecture Plan and Roadmap includes: • 2+ datacenter architecture (with/plus EDC) • Datacenter Network Architecture • Datacenter Security Architecture • Datacenter Technology Environment • Datacenter Implementation Roadmap Offeror must publish quarterly updates to the Datacenter Architecture Plan and Roadmap to include proposed updates to the technical architecture and implementation plan
Network and Security Architecture		
D-01.03	Effective Date + 60 days – with quarterly updates	*Datacenter Architecture Plan and Roadmap – Network and Security Architecture* The Network and Security Architecture - describes the network and security architecture to support the 2+ datacenter architecture.
Datacenter Architecture and Technology		
D-01.04	Effective Date +60 days– with quarterly updates	*Datacenter Architecture Plan and Roadmap* – Datacenter Technology The Datacenter Technology describes the technology used in the delivery of the Offeror's Enterprise Datacenter Services.
D-01.05	Effective Date +90 days – with quarterly updates	*Datacenter Architecture Plan and Roadmap* – Datacenter Technology Roadmap The Datacenter Technology Roadmap will identify specific, short-term steps and schedules for project of changes with estimated timings and cost impact to Commonwealth datacenter customers.

D-01.06	Effective Date + 180 days	*Datacenter Architecture Plan and Roadmap – Configuration Item Reconciliation* *The Configuration Item Reconciliation is the validation and update of the CMDB of record with the Offeror's configuration information including the EDC assets and CI's.*
Limited-Use Colocation Services		
D-01.07	Effective Date + 30 days	*Datacenter Architecture Plan and Roadmap*

D-02 Commonwealth Computing Procedures Manual (CCPM)

Offeror will develop documentation in accordance with the requirements in **Schedule H** - **Commonwealth Computing Procedures Manual (CCPM)**. This comprehensive services management manual will include, but not be limited to, the following sections as described in **Schedule H**:

- Organizational Overview
- Transition and Support Activities and Responsibilities
- IT Service Management Procedures
- Financial Management Procedures
- Contract Management Procedures
- Relationship Management Procedures
- Offeror Operational Procedures
- Commonwealth Customer Operations Manuals

Additional Planning Services		
D-02.01	Effective Date + 14 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide the initial version of the Commonwealth Computing Procedures Manual (CCPM) (see Schedule H CCPM Commonwealth Computing Procedures Manual) that includes Offeror's overall program and service management processes and procedures. The comprehensive manual includes the following sections: • Organizational Overview • Transition and Support Activities and Responsibilities • IT Service Management Procedures • Financial Management Procedures • Contract Management Procedures • Relationship Management Procedures • Offeror Operational Procedures • The Commonwealth Customer Operations Manuals PMO & Contract Management will focus on the bolded sections of the CCPM.

D-02.02	As needed during transition	After review and approval from the Commonwealth, Offeror must provide ongoing updates to the CCPM during the startup and transition phase
D-02.03	Yearly or as required	Offeror must provide CCPM updates as required as new services are added and yearly after the transition phase.
Availability/SLA Management		
D-02.04	Effective Date + 30 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must document the Availability and SLA Management approach and providing updates to the CCPM.
D-02.05	Effective Date +45 days	*Commonwealth Computing Procedures Manual (CCPM)* After review and approval from the Commonwealth, Offeror must review the Availability and SLA Management approach and project plan with Commonwealth stakeholders.
D-02.06	Monthly	*Commonwealth Computing Procedures Manual (CCPM)* SLA Achievement Report, detailing system availability, SLA attainment, and reason for outages.
D-02.07	As Needed	*Commonwealth Computing Procedures Manual (CCPM)* Root Cause Analysis (RCA) report for all major outages within SLA (e.g. hours/days of outage).
D-02.08	As requested	*Commonwealth Computing Procedures Manual (CCPM)* Ad hoc – Availability and SLA Reports
Change & Release Management		
D-02.09	Effective Date + 30 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must document the Change and Release Management approach and project plan updating appropriate sections to the CCPM.
D-02.10	Effective Date +45 days	*Commonwealth Computing Procedures Manual (CCPM)* After review and approval from the Commonwealth, Offeror must review the Change and Release Management approach and project plan with Commonwealth stakeholders.
D-02.11	Weekly	*Commonwealth Computing Procedures Manual (CCPM)* Weekly Change Management Meeting with the Change Advisory Board
D-02.12	Monthly	*Commonwealth Computing Procedures Manual (CCPM)* Monthly Change & Release Management summary report containing the number of changes, by platform, by Commonwealth organization, and status.

D-02.13	Yearly	*Commonwealth Computing Procedures Manual (CCPM)* On a yearly basis, randomly select completed Changes & Releases for detail auditing to determine compliance to policies. Create a summary report of the finding and make recommendations for improvements where appropriate.
D-02.14	Per Change Event	*Commonwealth Computing Procedures Manual (CCPM)* Complete Change Control & Release Management process for each change event adhering to the letter and spirit of the policy and process. Maintain a complete copy of the change / release for possible future audit.
Service Desk		
D-02.15	Effective Date + 30 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must document the Service Desk approach, organization, schedule and project plan.
D-02.16	Effective Date +45 days	*Commonwealth Computing Procedures Manual (CCPM)* After review and approval from the Commonwealth, Offeror must review the Service Desk approach and project plan with Commonwealth stakeholders
D-02.17	Effective Date + 60 days	*Knowledge Management Portal (KMP)* Offeror must provide a Knowledge/Service Management portal that describes the Offeror's contract information, pricing schedules, service offerings and operating procedures (operational, service delivery processes, SLAs, service ordering, etc.)
D-02.18	Effective Date +60 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide Commonwealth Computing Procedures Manual (CCPM) including but not limited to the following: Datacenter Operations, Change Management, Service Desk Operations, Security Management, Backup Management, Disaster Recovery, Performance Management, Asset Management, Service Level Management and Configuration Management. The Offeror must make the CCPM available on the Offeror's Knowledge/Service portal. See Schedule H Commonwealth Computing Procedures Manual (CCPM) for additional detail.
D-02.19	Effective Date +180 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must describe the process to keep separate and current specific sections of the CCPM dedicated to the operations of individual Commonwealth customers.
D-02.20	Effective Date +90 days	Knowledge Management Portal Offeror must provide Knowledge/Service portal training to authorized Commonwealth stakeholders

D-02.21	Weekly	*Commonwealth Computing Procedures Manual (CCPM)* Weekly summary report containing the type of incidents and problems being reported to the Service Desk. Identify measures being taken to reduce or eliminate stated incidents and problems.
D-02.22	Monthly	*Commonwealth Computing Procedures Manual (CCPM)* Monthly summary report containing the type of incidents and problems being reported to the Service Desk. Identify measures being taken to reduce or eliminate stated incidents and problems.
Account Management		
D-02.23	Effective Date + 30 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must document their Account Management approach and project plan.
D-02.24	Effective Date +45 days	*Commonwealth Computing Procedures Manual (CCPM)* After review and approval from the Commonwealth, Offeror must review the Account Management approach and project plan with Commonwealth stakeholders
D-02.25	Monthly	Monthly summary report containing the operational availability report on all systems in service, events and issues that occurred during the month. Report shall contain operational metrics by service platform, highlights and exceptions, and project status updates.
Configuration Management		
D-02.26	Effective Date + 30 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must document their Configuration Management approach, tool(s) and project plan.
D-02.27	Effective Date +45 days	*Commonwealth Computing Procedures Manual (CCPM)* After review and approval from the Commonwealth, Offeror must review the Configuration Management approach, tool(s) and project plan with Commonwealth stakeholders
D-02.28	As Requested	Offeror must provide Agency / Commonwealth level Configuration Management Reports
3rd Party License Management		
D-02.29	Effective Date + 30 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must document their 3rd Party License Management approach, tool(s) and project plan.
D-02.30	Effective Date +45 days	*Commonwealth Computing Procedures Manual (CCPM)* After review and approval from the Commonwealth, Offeror must review the 3rd Party License Management approach, tool(s) and project plan with Commonwealth stakeholders

D-02.31	Per request	Offeror must provide Software License Reports
Capacity Management		
D-02.32	Effective Date + 30 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must document their Capacity Management approach, tool(s) and project plan.
D-02.33	Effective Date +45 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must review the Capacity Management approach, tool(s) and project plan with Commonwealth stakeholders
D-02.34	Effective Date + 240 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must present the baseline Capacity Management Plan
D-02.35	Monthly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must issue periodic reports showing usage, trends, capacity forecasts, and recommendations for upgrades.
D-02.36	Annual	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide technology usage report (i.e. MIPS, vcpu, storage, etc.) by stakeholder and overall usage by the Commonwealth. The report must show monthly technology growth patterns by stakeholder.
Windows Support		
D-02.37	Effective Date + 30 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must present their roadmap and project plan to address the Windows Operations and Management including but not limited to the following; windows servers, backups, network connectivity, technical support, staffing, etc.
D-02.38	Effective Date + 45 days	*Commonwealth Computing Procedures Manual (CCPM)* After review and approval from the Commonwealth, Offeror must present plan to address the assessment recommendations identified in the Windows Operations and Management project plan.
D-02.39	Effective Date +60 days	*Commonwealth Computing Procedures Manual (CCPM)* Present a report describing the methodology the Offeror will follow to perform a Windows backups audit finding and recommendation to the Commonwealth Stakeholders, the audit report will include findings, recommendations, project plan and cost estimates.
D-02.40	Monthly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide SLA report(s). Provide a report detailing system availability, SLA attainment, reason for outages, and recommendations for improvements.

D-02.41	Quarterly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide Continuous Improvement Report. Provide a report detailing system availability and SLA attainment. Recommend system and cost improvements as appropriate.
Storage Management		
D-02.42	Effective Date + 30 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must present their roadmap and project plan to address Storage Management including but not limited to the following; data storage, backups, network connectivity, technical support, staffing, etc.
D-02.43	Effective Date + 45 days	*Commonwealth Computing Procedures Manual (CCPM)* After review and approval from the Commonwealth, Offeror must present plan to address the assessment recommendations identified in the Storage Management project plan.
D-02.44	Effective Date +60 days	*Commonwealth Computing Procedures Manual (CCPM)* Present a report describing the methodology the Offeror will follow to perform a system backups audit finding and recommendation to the Commonwealth Stakeholders, the audit report will include findings, recommendations, project plan and cost estimates.
D-02.45	Monthly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide SLA report(s). Provide a report detailing system availability, SLA attainment, reason for outages, and recommendations for improvements.
D-02.46	Quarterly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide Continuous Improvement report(s). Provide a report detailing system availability and SLA attainment. Recommend system and cost improvements as appropriate.
ERP Hosting – SAP / Oracle		
D-02.47	Effective Date + 30 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must present their roadmap and project plan to address ERP Hosting including but not limited to the following; data storage, backups, network connectivity, technical support, staffing, etc.
D-02.48	Effective Date + 45 days	*Commonwealth Computing Procedures Manual (CCPM)* After review and approval from the Commonwealth, Offeror must present plan to address the assessment recommendations identified in the ERP Hosting project plan.

D-02.49	Effective Date +60 days	*Commonwealth Computing Procedures Manual (CCPM)* Present a report describing the methodology the Offeror will follow to perform a system backup audit finding and recommendation to the Commonwealth Stakeholders, the audit report will include findings, recommendations, project plan and cost estimates.
D-02.50	Monthly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide SLA report(s). Provide a report detailing system availability, SLA attainment, reason for outages, and recommendations for improvements.
D-02.51	Quarterly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide Continuous Improvement report(s). Provide a report detailing system availability and SLA attainment. Recommend system and cost improvements as appropriate.
UNIX Support – AIX / Linux		
D-02.52	Effective Date + 30 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must present their roadmap and project plan to address UNIX Support including but not limited to the following; data storage, backups, network connectivity, technical support, staffing, etc.
D-02.53	Effective Date + 45 days	*Commonwealth Computing Procedures Manual (CCPM)* After review and approval from the Commonwealth, Offeror must present plan to address the assessment recommendations identified in the UNIX Support project plan.
D-02.54	Effective Date +60 days	*Commonwealth Computing Procedures Manual (CCPM)* Present UNIX audit finding and recommendation to the Commonwealth Stakeholders, the report will include findings, recommendations, project plan and cost estimates.
D-02.55	Monthly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide SLA report(s). Provide a report detailing system availability, SLA attainment, reason for outages, and recommendations for improvements.
D-02.56	Quarterly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide Continuous Improvement report(s). Provide a report detailing system availability and SLA attainment. Recommend system and cost improvements as appropriate.

Mainframe Services		
D-02.57	Effective Date + 30 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must present their roadmap and project plan to address Mainframe Support (IBM & Unisys) including but not limited to the following; data storage, backups, network connectivity, technical support, staffing, etc.
D-02.58	Effective Date + 45 days	*Commonwealth Computing Procedures Manual (CCPM)* After review and approval from the Commonwealth, Offeror must present project plan to address the assessment recommendations identified in the Mainframe Support (IBM & Unisys) plan.
D-02.59	Effective Date +60 days	*Commonwealth Computing Procedures Manual (CCPM)* Present mainframe audit finding and recommendation to the Commonwealth Stakeholders, the report will include findings, recommendations, project plan and cost estimates.
D-02.60	Monthly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide SLA report(s). Provide a report detailing system availability, SLA attainment, reason for outages, and recommendations for improvements.
D-02.61	Quarterly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide Continuous Improvement report(s). Provide a report detailing system availability and SLA attainment. Recommend system and cost improvements as appropriate.
Database Management Services		
D-02.62	Effective Date + 30 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must document their Database Management approach, tool(s) and project plan.
D-02.63	Effective Date +45 days	*Commonwealth Computing Procedures Manual (CCPM)* After review and approval from the Commonwealth, Offeror must review the Database Management approach, tool(s) and project plan with Commonwealth stakeholders
D-02.64	Effective Date +60 days	*Commonwealth Computing Procedures Manual (CCPM)* Present backup audit finding and recommendation to the Commonwealth Stakeholders, the report will include findings, recommendations, project plan and cost estimates.
D-02.65	Effective Date	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide Database Management Service Architecture document (Oracle, Sybase, and MS SQL).

D-02.66	Monthly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide Database Management Service Usage Reports
Server Capacity on Demand		
D-02.67	Effective Date + 30 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must document their Server Capacity on Demand approach, tool(s) and project plan.
D-02.68	Effective Date +45 days	*Commonwealth Computing Procedures Manual (CCPM)* After review and approval from the Commonwealth, Offeror must review the Server Capacity on Demand approach, tool(s) and project plan with Commonwealth stakeholders
D-02.69	Quarterly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must host a quarterly meeting with the Commonwealth to review current server utilization on all managed server platforms and locations, and forecast future quarter's server processing requirements. Recommendations to increase capacities will be made, when approved by the Commonwealth; the additional equipment will be scheduled for deployment.
Storage Capacity on Demand		
D-02.70	Effective Date + 30 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must document their Storage Capacity on Demand approach, tool(s) and project plan.
D-02.71	Effective Date +45 days	*Commonwealth Computing Procedures Manual (CCPM)* After review and approval from the Commonwealth, Offeror must review the Storage Capacity on Demand approach, tool(s) and project plan with Commonwealth stakeholders
D-02.72	Quarterly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must host a quarterly meeting with the Commonwealth to review current SAN storage utilization on all managed SAN platforms and locations, and forecast future quarter's SAN storage requirements. Recommendations to increase capacities will be made, when approved by the Commonwealth; the additional equipment will be scheduled for deployment.
DR Infrastructure on Demand		
D-02.73	Quarterly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must host a quarterly meeting with the Commonwealth to review current disaster recovery service and capabilities, and forecast future quarter's disaster recovery requirements. Recommendations to increase capacities will be made, when approved by the Commonwealth, the additional equipment and services will be scheduled for deployment.

Additional Technical Services		
D-02.74	Monthly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide a monthly report on technical support services usage by Commonwealth datacenter customer.
Limited-Use Colocation Services		
D-02.75	Effective Date + 30 days	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must document their approach, tool(s) and project plan for supporting Limited-Use Colocation Services.
D-02.76	Effective Date +45 days	*Commonwealth Computing Procedures Manual (CCPM)* After review and approval from the Commonwealth, Offeror must review the Limited-Use Colocation Services approach, tool(s) and project plan with Commonwealth stakeholders
D-02.77	Effective Date +60 days	*Commonwealth Computing Procedures Manual (CCPM)* Present backup audit finding and recommendation to the Commonwealth Stakeholders, the report will include findings, recommendations, project plan and cost estimates.
D-02.78	Monthly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide Limited-Use Colocation Services Usage Reports
Performance Monitoring & Management		
D-02.79	Monthly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide monthly summary report containing the performance level achieved for each system being monitored. This report will be reviewed with the Commonwealth and plans will be made to address system utilization as appropriate.
D-02.80	Daily	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide daily reports containing the performance level achieved for each system being monitored. Daily reports summarizing incidents for the past 24-hours and immediate reports of incidents and routine status reports of incidents in progress for resolution such as a network or server outage that impacts a facility and our business. These reports will be reviewed with the Commonwealth and plans will be made to address system utilization as appropriate.

Transition Program Management		
D-02.81	Effective Date + 60 days	*Commonwealth Computing Procedures Manual (CCPM)* Establish Interim Contract Management Procedures during the transition of datacenter services. Offeror must describe an interim procedure to monitor and manage service delivery including but not limited to the following; Problem Management, Change Management, Service Level monitoring and reporting, physical and logical security, project management, etc. while the service is transitioned from the Commonwealth to the Offeror.
D-02.82	Weekly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide Transition Status reports, including any schedule variance that cannot be remediated will trigger the escalation procedures outlined in the Transition Plan/Agreement, which will be developed during Transition.
Security & Firewall		
D-02.83	Quarterly	*Commonwealth Computing Procedures Manual (CCPM)* Offeror must provide Continuous Improvement report. Provide a report detailing system availability and SLA attainment. Recommend system and cost improvements as appropriate.

D-03 Technology Architecture and Refresh Approach

The Technology Architecture and Refresh Approach will include the Offeror's proposed the Technology that will be utilized to support the architecture and delivery of services across all platform and services. The Technology Architecture and Refresh Approach should include at minimum sections that support the following:

- Datacenter Technology - describes the technology used in the delivery of the Offeror's Enterprise Datacenter Services. The technology descriptions should include hardware, software that will be included in the overall solution delivery. The technology should also include a complete list of those Service Level measurement and monitoring tools that will be used to measure and report Offeror's performance of the Services at a level of detail sufficient, as determined by the Commonwealth, to verify Offeror's compliance with those Service Levels described in **Schedule J.1 Datacenter Service Level Management** as of the Effective Date.

- Datacenter Technology Roadmap - will identify specific, short and long term steps and schedules for planned and proposed future changes with estimated timings and cost impact to Commonwealth datacenter customers. This should be the basis for generation of technology roadmaps which will include schedules, dependencies and requirements for introduction of new technology changes as well as acquisition, support, and retirement of current software/hardware.

- Configuration Item Reconciliation - is the validation and update of the CMDB of record with the Offerors configuration information including the EDC assets and Configuration Items (CI's).

Technology Refresh		
D-03.01	Effective Date + 30 days	*Technology Architecture and Refresh Approach* Offeror must document the following Technical Architecture approach and project plan including; Service Catalog, IT Architecture, and Technical support
D-03.02	Effective Date +45 days	*Technology Architecture and Refresh Approach* After review and approval from the Commonwealth, Offeror must review the Technical Architecture approach and project plan with Commonwealth stakeholders
D-03.03	Effective Date + 60 days	Offeror must identify the technical architecture organization and staff.
Infrastructure Architecture		
D-03.04	Effective Date + 45 days	*Technology Architecture and Refresh Approach* Offeror must document the approach and project plan for the computing infrastructure architecture and review with Commonwealth Stakeholders
D-03.05	Effective Date + 45 days	*Technology Architecture and Refresh Approach* After review and approval from the Commonwealth, Offeror must document the approach and project plan for the network architecture to connect Offeror's datacenter(s), review with Commonwealth Stakeholders
D-03.06	As requested by Commonwealth Stakeholders	*Technology Architecture and Refresh Approach* Offeror must describe the process to request a review new technologies evaluations by Commonwealth datacenter customers.
D-03.07	Per request – prior to a new application infrastructure service	*Technology Architecture and Refresh Approach* Offeror must provide Infrastructure Architecture Design Reports
Performance Monitoring & Management		
D-03.08	Effective Date + 30 days	*Technology Architecture and Refresh Approach* Offeror must document their Performance Monitoring and Management approach, tool(s) and project plan.
D-03.09	Effective Date +45 days	*Technology Architecture and Refresh Approach* After review and approval from the Commonwealth, Offeror must review the Performance Monitoring and Management approach, tool(s) and project plan with Commonwealth stakeholders

D-04 IT Service Continuity Architecture and Plan

The IT Service Continuity Architecture and Plan will include the Offeror's proposed Disaster Recovery (DR) solution architecture. The DR solution architecture will describe how the Offeror will deliver multiple tiers of disaster recovery services. The IT Service Continuity Architecture and Plan will also describe the Offeror's approach to reviewing the Commonwealth's current DR Plans and the updating of those plans in coordination with the Commonwealth.

IT Service Continuity Architecture		
D-04.01	Effective Date + 30 days	*IT Service Continuity Architecture and Plan* Offeror must describe their methodology for reviewing and refreshing technology on a scheduled basis.
D-04.02	Effective Date + 30 days	*IT Service Continuity Architecture and Plan* Offeror must provide an IT Service Continuity Architecture and Plan to Implement DR solution
D-04.03	30 days prior to transition of each critical application	*IT Service Continuity Architecture and Plan* Offeror must describe their approach to providing Develop/Update Agency Application DR and Business Recovery Plan(s)
D-04.04	Depending on DR Tier Solution • Current DR • Tier 0 • Tier 1 • Tier 2 • Tier 3 • Tier 4	*IT Service Continuity Architecture and Plan* Offeror must develop a plan to transition agencies to Tiered DR Solution • Currently have DR (DPH) – at time of transition • Tier 0 – Transition + 90 days • Tier 1 – Transition + 60 days • Tier 2 – Transition + 30 days • Tier 3 – at time of transition • Tier 4 – at time of transition
DR Planning & Testing		
D-04.05	Effective Date + 30 days	*IT Service Continuity Architecture and Plan* Offeror must document their Tiered Disaster Recovery approach, tool(s) and project plan.
D-04.06	Effective Date +45 days	*IT Service Continuity Architecture and Plan* After review and approval from the Commonwealth, Offeror must review their Tiered Disaster Recovery approach, tool(s) and project plan with Commonwealth stakeholders

D-04.07	Monthly	*IT Service Continuity Architecture and Plan* Offeror must provide report(s) describing schedule of stakeholder participation in DR solution

D-05 Transition Management Plan

The Transition Management Plan will provide a detailed overview of the Offeror's transition management approach, process and procedures. The Transition Management Plan will describe the enablement of the Transition Project Management Office (TPMO) and also provide a detailed implementation schedule of transition activities and milestones. The Transition Management Plan should include at minimum sections that support the following:

- Transition Management Approach
- Transition Project Management Office (TPMO) Organization and Responsibilities
- Transition Management Communications Plan
- Transition Schedule

Transition Management (New Customer and/or Services)		
D-05.01	Effective Date + 60 days	*Transition Management Plan* Offeror must create a Transition Roadmap with major milestones and present it to the Commonwealth for review
D-05.02	Effective Date + 90 days	*Transition Management Plan* After review and approval from the Commonwealth, Offeror must create a Detailed Transition Project Plan with major milestones and present it to the Commonwealth for review
D-05.03	Weekly	*Transition Management Plan* Offeror must create a report for the Commonwealth detailing the transition projects on the plan, status, schedule, risks, and the forecasted transition date.
Transition Program Management		
D-05.04	Effective Date + 60 days	*Transition Management Plan* Offeror must present their approach to transition Commonwealth computing assets. The approach must include a roadmap and project plan to successfully transition Commonwealth computing assets using the schedule identified in the RFP
D-05.05	Effective Date + 90 days	*Transition Management Plan* Present and review the transition roadmap and plan to Commonwealth stakeholders.

D-05.06	Effective Date + 60 days	*Transition Management Plan* Establish Interim Contract Management Procedures during the transition of datacenter services. Offeror must describe an interim procedure to monitor and manage service delivery including but not limited to the following; Problem Management, Change Management, Service Level monitoring and reporting, physical and logical security, project management, etc. while the service is transitioned from the Commonwealth to the Offeror.
D-05.07	Effective Date + 60 days	*Transition Management Plan* EDC / Legacy Datacenter Infrastructure Maintenance Strategy – Offeror must document their strategy as it related to providing a solution to the infrastructure maintenance expiration issue at the EDC and any other datacenter that has the same or similar issue.
D-05.08	Effective Date + 60 days	*Transition Management Plan* Offeror must provide the procedure to standup their Transition Management Office
D-05.09	Weekly during transition	*Transition Management Plan* Offeror must provide Transition Status reports, including any schedule variance that cannot be remediated will trigger the escalation procedures outlined in the Transition Plan/Agreement, which will be developed during Transition.
Security Transition Activities		
D-05.10	Effective Date + 60 days	*Transition Management Plan* Offeror must provide their Security Transition Plan
D-05.11	Weekly updates during transition	*Transition Management Plan* Offeror must provide their Security Transition Status Report(s)

D-06 Agency Level DR Plan(s)

The Offeror is required to assist the Commonwealth Agencies with updates to or development of their current DR Plans (DRPs). These Agency Level DR Plans will reflect the Offeror's DR approach and solution for DR testing. The following describes the Offeror's responsibilities regarding the updating of Agency Level DRPs:

- Within six (6) months after the Effective Date, Offeror shall complete the update all existing Agency-specific Disaster Recovery Plans and technical recovery guides to reflect all changes implemented to the Services infrastructure prior to or during the performance of Transition Services.
- For Applications lacking tested Disaster Recovery Plans, Offeror shall work with Commonwealth Agencies to complete a gap analysis of the current Disaster Recovery

Plans and technical recovery guides compared to the requested recovery time objective, as specified in **Schedule J.1 Datacenter Service Level Management**, and update the Disaster Recovery Plans with the results within forty-eight (48) months after the Effective Date.

- For Agencies without a Disaster Recovery Plan, the Offeror shall work with Agencies to develop a basic Disaster Recovery Plan and technical recovery guides within eighteen (18) months after the Effective Date.

DR Planning & Testing		
D-06.01	Monthly	*Agency Level DR Plan* Offeror must provide report(s) describing the schedule of DR test being performed by stakeholders
D-06.02	Monthly	*Agency Level DR Plan* Offeror must provide report(s) describing the results of stakeholder DR test
D-06.03	As requested– Per Agency Critical Application	*Agency Level DR Plan* Offeror must provide DR Test Plans as required

D-07 Security Management Plan

The Security Management Plan will address the overall security management for the planned facility security implementation for the EDC, the Offeror Facilities, software and equipment deployment specifically for data and online security, annual security assessments and other standard security concepts for ensuring the safety, security and confidentiality of Commonwealth Data.

The Security Management Plan shall include a complete description of the personnel security management program. It shall comply with background check requirements specified in the Terms and Conditions and shall provide a methodology for ongoing evaluation and reporting of any change in status of Offeror personnel that would negatively impact their ability to continue to meet Commonwealth or Agency security requirements.

Security Management		
D-07.01	Effective Date + 30 days	*Security Management Plan* Offeror must document their Security Management approach, tool(s) and project plan.
D-07.02	Effective Date +45 days	*Security Management Plan* After review and approval from the Commonwealth, Offeror must review their Security Management approach, tool(s) and project plan with Commonwealth stakeholders.

D-07.03	Quarterly	*Security Management Plan* Offeror must provide the Commonwealth with a report containing the detailed results of the Vulnerability Analyses testing. Include any remediation activities that are required.
D-07.04	Monthly	*Security Management Plan* Offeror must provide the Commonwealth with the detailed monthly Security Log Analysis report. Include any remediation activities that are required.
D-07.05	Ongoing	*Security Management Plan* Offeror must maintain a hardcopy file of all security access changes. The copy will contain the date, time, file changes, access rights applied and the name of the security officer completing the access request.
Security & Firewall		
D-07.06	Effective Date + 30 days	*Security Management Plan* Offeror must document their Security and Firewall approach, tool(s) and project plan.
D-07.07	Effective Date +45 days	*Security Management Plan* After review and approval from the Commonwealth, Offeror must review the Security and Firewall approach, tool(s) and project plan with Commonwealth stakeholders
D-07.08	Monthly	*Security Management Plan* Threat Assessment and Analysis Report. Provide a monthly report detailing the threat assessments, volume and major types of malware detected, volume of SPAM rejected, corrective actions, and recommendations that would improvement security of Commonwealth systems.
D-07.09	Monthly	*Security Management Plan* Offeror must provide SLA reports. Provide a report detailing system availability, SLA attainment, reason for outages, and recommendations for improvements, security incident notification, and security change request intervals and results.
D-07.10	Monthly	*Security Training and On-boarding Status Report* Offeror must provide a monthly Security Training and On-boarding Status Report detailing security training, changes to project personnel, and background check status and results.

D-08 Facilities Management Plan

The Facilities Management Plan will address management for both the EDC facility and the proposed Offeror's facility(s). The Facilities Management Plan should describe the Offeror's plan for providing and managing the physical environment. For example; power and power distribution, cooling and ventilation, fire detection and suppression, building security and access control, and environmental monitoring. Provide an approach for yearly review and self-verification that the datacenters will be managed, maintained and operated at the equivalent of Uptime Institute of Tier 3 rating. The plan should also address how the Offeror will support SSAE-16 compliance audits.

Facilities Architecture / Maintenance		
D-08.01	Effective Date + 60 days	*Facilities Management Plan* Offeror must present their assessment of the EDC and any required facility changes/modification required to upgrade the facility to meet service level objectives. The assessment must include a roadmap and project plan to make any required facility modifications.
D-08.02	On the July 31st following the Commonwealth's acceptance of Milestone M-14	*Facilities Management Plan* Present results of the SSAE 16 audit of the EDC. The audit period is to cover the period from Transition completion through the following June 30th
D-08.03	Monthly	*Facilities Management Plan* Offeror must provide monthly Facilities SLA Report, detailing environmental equipment availability, SLA attainment, and reason for outages.
D-08.04	Quarterly	*Facilities Management Plan* Offeror must provide quarterly Facility service improvement report. Report changes and improvements to the facility or the maintenance of the facilities.
D-08.05	Annual	*Facilities Management Plan* Offeror must provide annual SSAE 16 audit reports for each datacenter facility being used to support the Commonwealth. The Audit Report for the EDC must be provided on the anniversary of the Audit Report described in Deliverable D-08.02.
Site Operations		
D-08.06	Effective Date + 60 days	*Facilities Management Plan* Offeror must present their assessment of the EDC monitoring and staffing changes/modification required to upgrade the facility to meet Commonwealth service level objectives. The assessment must include a roadmap and project plan to make any required monitoring and staffing modifications.

D-08.07	Effective Date + 90 days	*Facilities Management Plan* Present plan to address the assessment recommendations identified in the EDC monitoring, project plan and staffing report.
D-08.08	Daily, Monthly	*Facilities Management Plan* Offeror must provide daily and monthly SLA report(s), detailing environmental equipment availability, SLA attainment, and reason for outages.
D-08.09	Quarterly	*Facilities Management Plan* Offeror must provide quarterly site operations improvement report. Identify changes or improvements to the site operations that would assist the Offeror in meeting the agreed facility SLAs.

D-09 Security Risk and Vulnerability Assessment Report

The Offeror will execute a Baseline Security Risk and Vulnerability Assessment. The assessment report must include a roadmap and project plan to make any required security modifications prior to final transition of services.

Security Transition Activities		
D-09.01	Effective Date + 60 days	*Security Risk and Vulnerability Assessment Report* Offeror must execute a Baseline Security Risk and Vulnerability Assessment. The assessment must include a roadmap and project plan to make any required security modifications.
D-09.02	Effective Date + 90 days	*Security Risk and Vulnerability Assessment Report* Present results of the Security Risk and Vulnerability assessment along with a Roadmap and Project Plan to address the recommendation identified in the assessment.

D-10 Gap Analysis Report

The Offeror will execute a Data Center Gap Analysis. The analysis report must identify gaps in the current data centers and the Offeror's recommendations and corrective approach.

Gap Analysis Activities		
D-10.01	Effective Date + 120 days	*Gap Analysis Report* Offeror must execute a Data Center Gap Analysis. The analysis must include gaps identified and a roadmap and project plan to institute any recommendations and corrective actions.

D-10.02	Effective Date + 150 days	*Gap Analysis Report* Present results of the Data Center Gap Analysis along with a Roadmap and Project Plan to address the recommendations identified in the analysis.

D-11 Contract Management Plan

The Contract Management Plan will address management for the overall contract. The Contract Management Plan should describe the Offeror's plan to ensure it is adhering to the terms and conditions of the contract and providing the services/products that meet the requirements of the project. The Contract Management Plan must identify the activities to be performed or initiated to manage, track, amend, and close the contract. The Contract Management Plan must include but is not limited to: participants roles and responsibilities, task accomplishment plan, status reports, deliverable management, contact performance management, risk management, and contract closeout.

Contract Management Plan		
D-11.01	Effective Date + 45 days	*Contract Management Plan* Offeror must document its Contract Management approach, tool(s) and project plan.
D-11.02	Effective Date + 60 days	*Contract Management Plan* After review and approval from the Commonwealth, Offeror must review its Contract Management approach, tool(s) and project plan with Commonwealth stakeholders.

Deliverable Acceptance Criteria Matrix

This section is provided for the Offeror to understand the process the Commonwealth will use for acceptance of Deliverables/Milestones that are committed to in the RFP. The Matrix provided below is an example of the template that will be used to capture Deliverables/Milestones and other information related to the acceptance process.

It is critical to the success of the Data Center Computing Services project that the deliverable acceptance process is thorough and that any deficiencies are addressed as early as possible to minimize impacts to the Services. Designated Commonwealth working teams will be reviewing the Deliverables/Milestones throughout the phases of development. The Offeror will solicit input from the Commonwealth team members as the items are developed with the goal of understanding expectations in advance so as to obtain acceptance upon delivery. Feedback and suggestions received from the Commonwealth must be incorporated into the Deliverables/Milestones. The Commonwealth will identify the individuals authorized to provide formal Acceptance Approval / Nonconformance notification to the Offeror for the Deliverables/Milestones. The deliverable acceptance process will comply with the following guidelines and be formally documented in the Commonwealth Computing Procedures Manual (CCPM).

1. The Offeror will give written notice to the Commonwealth that a Deliverable / Milestone is complete.
2. A walk-through review of the Deliverable and/or Milestone will be scheduled by the Offeror seven (7) days following the issuance of the written notice to the Commonwealth. The purpose of the walk-through is to provide a forum for discussion and review of the Transition Deliverable / Milestone with the approver/s. If additional review, physical inspection, on-line access or backup information is required, the Commonwealth will notify the Offeror at this time.
3. The Commonwealth will provide the Offeror with notice that the Deliverable / Milestone is Accepted or notice of Noncompliance no later than seven (7) days after the walk-through, fourteen (14) days after notice of completion.
4. If the Commonwealth does not provide notice to the Offeror of their Acceptance or Nonconformance within fourteen (14) days of notice of completion, the Offeror will give the Commonwealth written notice that the request was not received and the Acceptance Review Period will be extended an additional seven (7) days.
5. The Enterprise Datacenter Services Transition Management Committee will review all Deliverable / Milestones which have not received written notice of Acceptance or Noncompliance within fourteen (14) days after notice of completion. The Enterprise Datacenter Services Transition Management Committee's goal is to determine and document the Commonwealth and Offeror actions necessary to complete the review minimizing any potential delays to the project and addressing any substantive issues.
6. For any Deliverables / Milestones which are found to be Noncompliant, the Offeror will address the nonconformity (and any other problems of which it has knowledge) and redeliver the item to the Commonwealth using the process outlined above.

The status of each Deliverable and any associated issues will be managed through a monthly deliverables review meeting between the Commonwealth and the Offeror. The objective of the meeting is to review the status of all deliverables, communicate deliverable owners and

deliverable recipients for upcoming deliverables, review rejected deliverables and remediation plans for those deliverables.

Example - Deliverable Acceptance Matrix

Reference #	Deliverable / Milestone Name	Due Date	Acceptance Criteria	Monthly Credit
D-01	Datacenter Architecture Plan and Roadmap		•	
D-02	Commonwealth Computing Procedures Manual (CCPM)		•	
D-03	Technology Architecture and Refresh Approach		•	
D-04	IT Service Continuity Architecture and Plan		•	
D-05	Transition Management Plan		•	
D-06	Agency Level DR Plan(s)		•	
D-07	Security Management Plan		•	
D-08	Facilities Management Plan		•	
D-09	Security Risk and Vulnerability Assessment Report		•	
D-10	Gap Analysis Report		•	
D-11	Contract Management Plan			

Request for Proposal

RFP # 6100022698

Commonwealth of Pennsylvania

Office of Administration

Office for Information Technology

Data Center Computing Services

SCHEDULE L

APPROVED SUBCONTRACTORS

(Offeror to provide a list of Offeror's subcontractors within the Schedule)

Request for Proposal

RFP # 6100022698

Commonwealth of Pennsylvania

Office of Administration

Office for Information Technology

Data Center Computing Services

SCHEDULE M

DETAILED TRANSITION PLAN

(Offeror to provide Offeror's Detailed Transition Plan within the Schedule)

Request for Proposal

RFP # 6100022698

Commonwealth of Pennsylvania
Office of Administration
Office for Information Technology
Data Center Computing Services

Confidential Exhibits to RFP
Pages Removed for Confidentiality

pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Date:	December 5, 2012
Subject:	Data Center Computing Services Addendum
Solicitation Number:	6100022698
Solicitation Due Date	March 8, 2013
Addendum Number:	1

To All Offerors:
The Commonwealth of Pennsylvania defines a solicitation "Addendum" as an addition to or amendment of the original terms, conditions, specification, or instruction of a procurement solicitation (e.g. Invitation for Bids, Request for Quotes and Request for Proposals).

The following changes have been made to the solicitation identified above:

1. In reference to Part I-8 (Enterprise Data Center (EDC) Tour) of the RFP, the Commonwealth requests Offerors register for the EDC tour prior to 2:00 PM EST on Tuesday, December 11, 2012.

2. The heading on Appendix C (Project References) was changed from "Appendix E" to "Appendix C." See updated Appendix C posted December 5, 2012.

For electronic solicitations responses via the PASupplierPortal:

- Attach this addendum to your solicitation response.
- To attach the Addendum, download the Addendum and save to your computer. Move to "My Notes", use the "Browse" button to find the document you just saved and press "Add" to upload the document.
- Review the Attributes section of our solicitation response to ensure you have responded, ad required, to any question relevant to solicitation addenda issues subsequent to the initial advertisement of the solicitation opportunity,

For Solicitation where a "hard copy" (vs. electronic) response if requested:

- If you are already submitted a response to the original solicitation, you may either submit a new response, or return this Addendum with a statement=n that your original response remain fir, by the due date to the following address:

Except as amended by this Addendum, the terms, conditions, specification, and instruction of the solicitation and any previous solicitation addenda, remain as originally written.

Very truly yours,

Name: Sheryl Kimport
Title: Commodity Specialist
Phone: 717.346.2670
Email: skimport@pa.gov

pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Date:	December 17, 2012
Subject:	Data Center Computing Services Addendum
Solicitation Number:	6100022698
Solicitation Due Date	March 8, 2013
Addendum Number:	2

To All Offerors:
The Commonwealth of Pennsylvania defines a solicitation "Addendum" as an addition to or amendment of the original terms, conditions, specification, or instruction of a procurement solicitation (e.g. Invitation for Bids, Request for Quotes and Request for Proposals).

The following changes have been made to the solicitation identified above:

1. A list of visitors that attended the Enterprise Data Center (EDC) tours on December 12th & 13th, 2012 has been posted.

2. A handout provided at the tours detailing information about the EDC facility has been posted.

For electronic solicitations responses via the PASupplierPortal:

- Attach this addendum to your solicitation response.
- To attach the Addendum, download the Addendum and save to your computer. Move to "My Notes", use the "Browse" button to find the document you just saved and press "Add" to upload the document.
- Review the Attributes section of our solicitation response to ensure you have responded, ad required, to any question relevant to solicitation addenda issues subsequent to the initial advertisement of the solicitation opportunity,

For Solicitation where a "hard copy" (vs. electronic) response if requested:

- If you are already submitted a response to the original solicitation, you may either submit a new response, or return this Addendum with a statement=n that your original response remain fir, by the due date to the following address:

Except as amended by this Addendum, the terms, conditions, specification, and instruction of the solicitation and any previous solicitation addenda, remain as originally written.

Very truly yours,

Name: Sheryl Kimport
Title: Commodity Specialist
Phone: 717.346.2670
Email: skimport@pa.gov

pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Date:	January 9, 2013
Subject:	Data Center Computing Services Addendum
Solicitation Number:	6100022698
Solicitation Due Date	March 8, 2013
Addendum Number:	3

To All Offerors:
The Commonwealth of Pennsylvania defines a solicitation "Addendum" as an addition to or amendment of the original terms, conditions, specification, or instruction of a procurement solicitation (e.g. Invitation for Bids, Request for Quotes and Request for Proposals).

The following changes have been made to the solicitation identified above:

1. The Commonwealth received approximately 650 questions during the first round of Q&A. Due to the large volume, the Commonwealth will post answers to the questions in parts. A document labeled "Questions and Answers Round 1 Part "1 has been posted to the emarketplace website. Additional questions and answers will be posted as the answers are finalized. Please continue to monitor the emarketplace website.

For electronic solicitations responses via the PASupplierPortal:

- Attach this addendum to your solicitation response.
- To attach the Addendum, download the Addendum and save to your computer. Move to "My Notes", use the "Browse" button to find the document you just saved and press "Add" to upload the document.
- Review the Attributes section of our solicitation response to ensure you have responded, ad required, to any question relevant to solicitation addenda issues subsequent to the initial advertisement of the solicitation opportunity,

For Solicitation where a "hard copy" (vs. electronic) response if requested:

- If you are already submitted a response to the original solicitation, you may either submit a new response, or return this Addendum with a statement=n that your original response remain fir, by the due date to the following address:

Except as amended by this Addendum, the terms, conditions, specification, and instruction of the solicitation and any previous solicitation addenda, remain as originally written.

Very truly yours,

Name: Sheryl Kimport
Title: Commodity Specialist
Phone: 717.346.2670
Email: skimport@pa.gov

pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Date:	January 11, 2013
Subject:	Data Center Computing Services Addendum
Solicitation Number:	6100022698
Solicitation Due Date	March 8, 2013
Addendum Number:	4

To All Offerors:
The Commonwealth of Pennsylvania defines a solicitation "Addendum" as an addition to or amendment of the original terms, conditions, specification, or instruction of a procurement solicitation (e.g. Invitation for Bids, Request for Quotes and Request for Proposals).

The following changes have been made to the solicitation identified above:

1. Additional Round 1 questions and answers have been posted to the emarketplace website. This document is labeled as "Questions and Answers Round 1 Part 2". Please continue to monitor the emarketplace website.

2. A revised Schedule F – COPA DATACENTER STATEMENT OF WORK has been posted to the emarketplace website. The following changes have been made to Schedule F:
   1) Added Exchange as a Service as Section 3.2.5.5.
   2) Modified Transition Planning/Governance Section 3.3.2.

3. A revised Schedule I – OFFEROR PRICING FORMS has been posted to the emarketplace website. The following changes have been made to Schedule I:
   1) Modified Offeror Pricing Forms, Tab 3-Transition Charges.

For electronic solicitations responses via the PASupplierPortal:

- Attach this addendum to your solicitation response.
- To attach the Addendum, download the Addendum and save to your computer. Move to "My Notes", use the "Browse" button to find the document you just saved and press "Add" to upload the document.
- Review the Attributes section of our solicitation response to ensure you have responded, ad required, to any question relevant to solicitation addenda issues subsequent to the initial advertisement of the solicitation opportunity,

For Solicitation where a "hard copy" (vs. electronic) response if requested:

- If you are already submitted a response to the original solicitation, you may either submit a new response, or return this Addendum with a statement=n that your original response remain fir, by the due date to the following address:

Except as amended by this Addendum, the terms, conditions, specification, and instruction of the solicitation and any previous solicitation addenda, remain as originally written.

Very truly yours,

Name: Sheryl Kimport
Title: Commodity Specialist
Phone: 717.346.2670
Email: skimport@pa.gov

pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Date:	January 17, 2013
Subject:	Data Center Computing Services RFP Addendum
Solicitation Number:	6100022698
Solicitation Due Date	March 8, 2013
Addendum Number:	5

To All Offerors:

The Commonwealth of Pennsylvania defines a solicitation "Addendum" as an addition to or amendment of the original terms, conditions, specification, or instruction of a procurement solicitation (e.g. Invitation for Bids, Request for Quotes and Request for Proposals).

This addendum is intended to inform suppliers of the following:

1. Two sections of the RFP relating to the Small Diverse Business Program have been modified. Part I-13 (Small Diverse Business Information) and Part II-9 (Small Diverse Business Participation Submittal) have been replaced with new language.

   A revised version of the RFP has been posted to the emarketplace website. This new version of the RFP, dated January 17, 2013, replaces the previously posted RFP document.

2. The pre-proposal conference attendance list has been posted to the emarketplace website.

3. Copies of the business cards collected at the pre-proposal conference have been posted to the emarketplace website.

4. The pre-proposal conference presentation has been posted to the emarketplace website.

For electronic solicitations responses via the PASupplierPortal:

- Attach this addendum to your solicitation response.
- To attach the Addendum, download the Addendum and save to your computer. Move to "My Notes", use the "Browse" button to find the document you just saved and press "Add" to upload the document.
- Review the Attributes section of our solicitation response to ensure you have responded, ad required, to any question relevant to solicitation addenda issues subsequent to the initial advertisement of the solicitation opportunity,

For Solicitation where a "hard copy" (vs. electronic) response if requested:

- If you are already submitted a response to the original solicitation, you may either submit a new response, or return this Addendum with a statement=n that your original response remain fir, by the due date to the following address:

Except as amended by this Addendum, the terms, conditions, specification, and instruction of the solicitation and any previous solicitation addenda, remain as originally written.

Very truly yours,

Name: Sheryl Kimport
Title: Commodity Specialist
Phone: 717.346.2670
Email: skimport@pa.gov

Pre-proposal Conference for:

Commonwealth Data Center
Computing Services
RFP 6100022698

pennsylvania
OFFICE OF ADMINISTRATION

A

- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible] A [illegible]

[illegible]

pennsylvania
OFFICE OF ADMINISTRATION

[illegible]

- [illegible]
  - [illegible]
  - [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]

pennsylvania
OFFICE OF ADMINISTRATION

□ □□□□□□□□□

□ □□□□□□□□

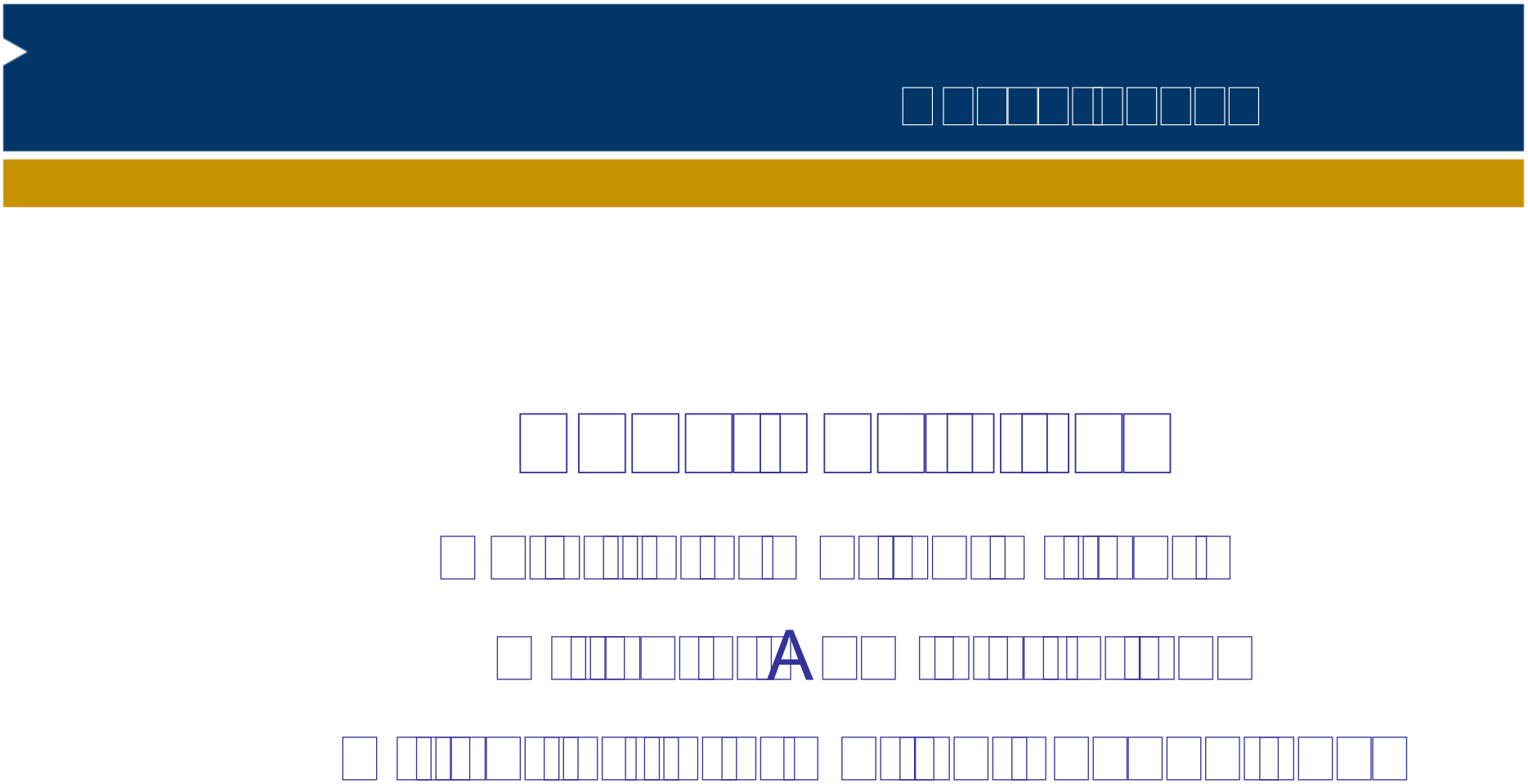
□ □□□□□□□□□

This pre-proposal conference has three purposes:

pennsylvania
OFFICE OF ADMINISTRATION

Agency Representatives:

- **Office for Information Technology:**
  - [illegible]
  - [illegible]
  - [illegible]A [illegible]
  - [illegible]
- **Bureau Of Small Business Opportunities**
  - [illegible]



pennsylvania
OFFICE OF ADMINISTRATION

[illegible]

- [illegible]
  - [illegible]
  - [illegible]
  -

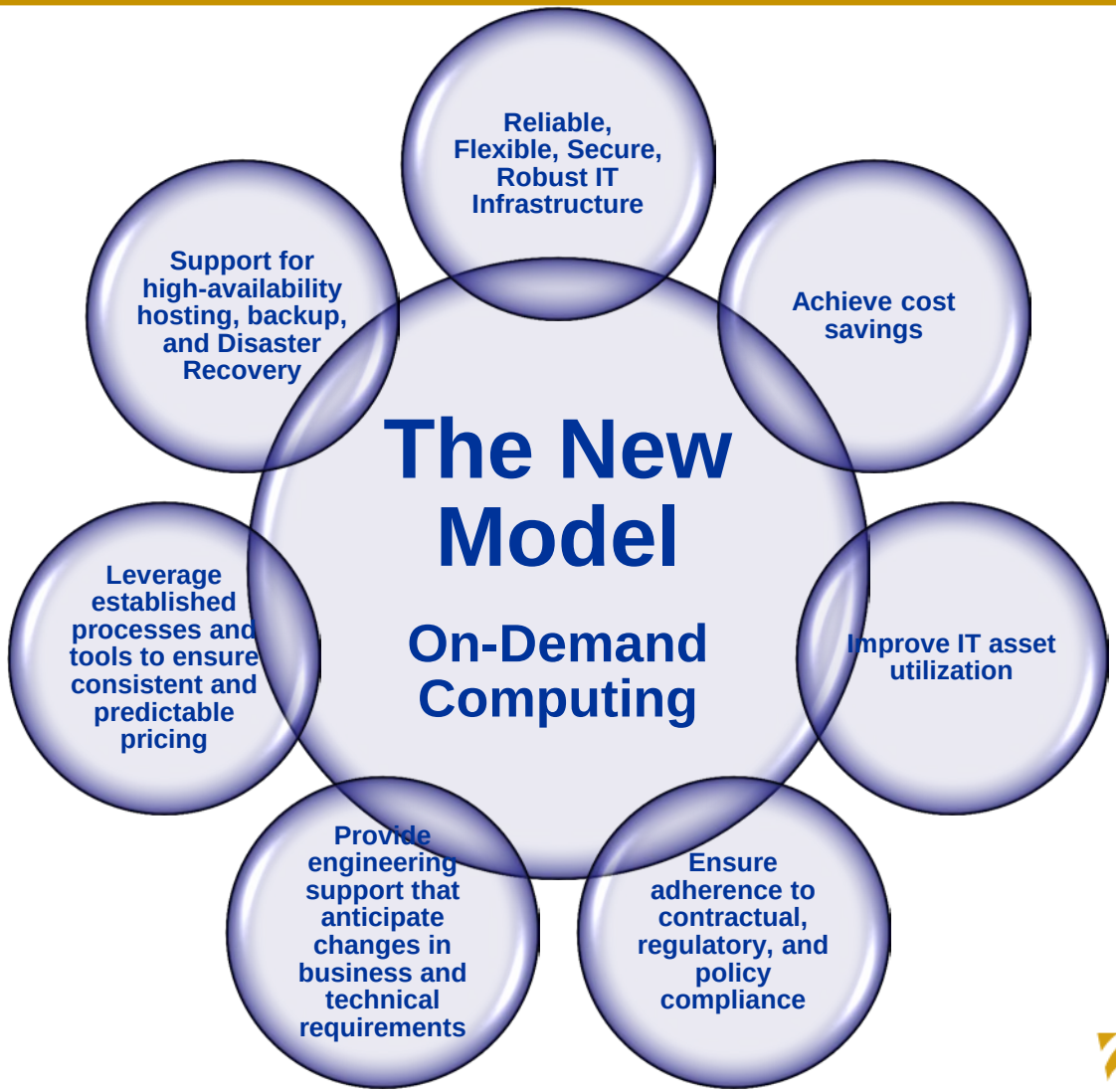
[illegible]

- [illegible]
- [illegible]
  - [illegible]
    - [illegible]
  - [illegible]
    - [illegible]
- [illegible]

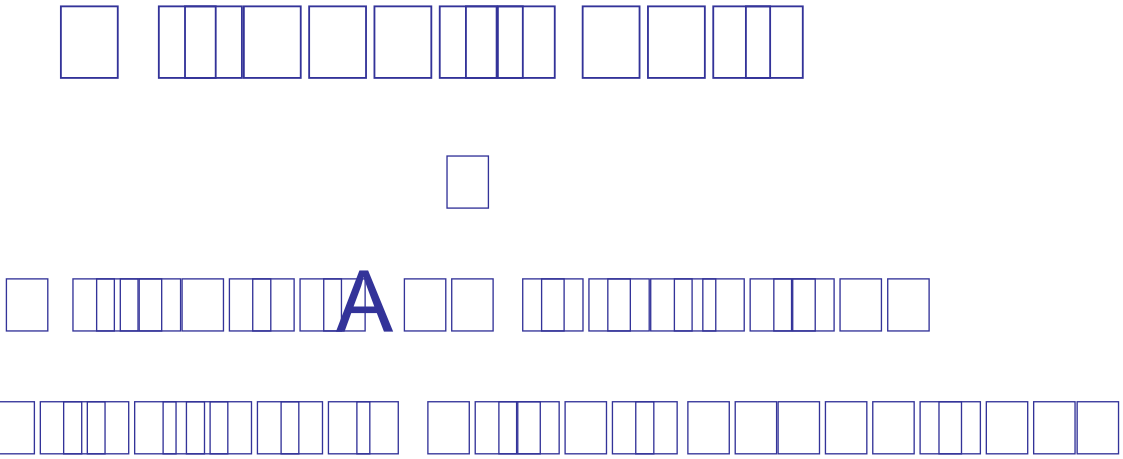
pennsylvania
OFFICE OF ADMINISTRATION

[illegible]

- [illegible]
- [illegible]

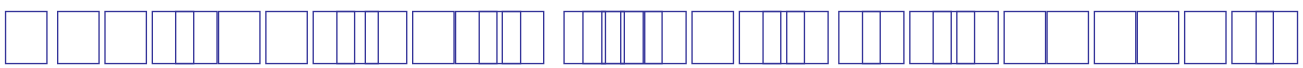


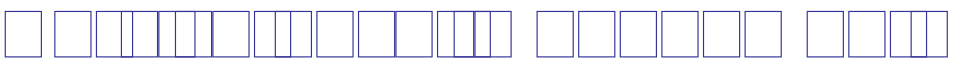
pennsylvania
OFFICE OF ADMINISTRATION

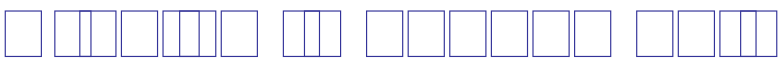


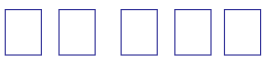
pennsylvania
OFFICE OF ADMINISTRATION

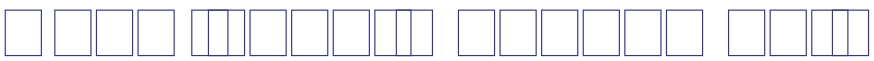
- [illegible]
  - [illegible]
  - [illegible]
  - [illegible]
  - [illegible]
  - [illegible]
  - [illegible]
  - [illegible]
- [illegible]











pennsylvania
OFFICE OF ADMINISTRATION

PMO & Service Management

- Project / Contract Management
- Availability / SLA Management
- Change & Release Management
- Service Desk
- Technical Architecture
- Account Management
- Configuration Management
- 3rd Party License Management

Technical Services

- Transition Management
- Infrastructure Architecture
- Capacity Management
- DR Planning & Testing
- Security Management
- Performance Management & Monitoring

Facilities Management

- Facilities Management
- Site Operations

Managed Hosting Services

- Windows Support
- Storage Management
- ERP Hosting SAP/Oracle
- Unix Support AIX/Linux
- Mainframe Services IBM/Unisys
- Security & Firewall
- Database Services

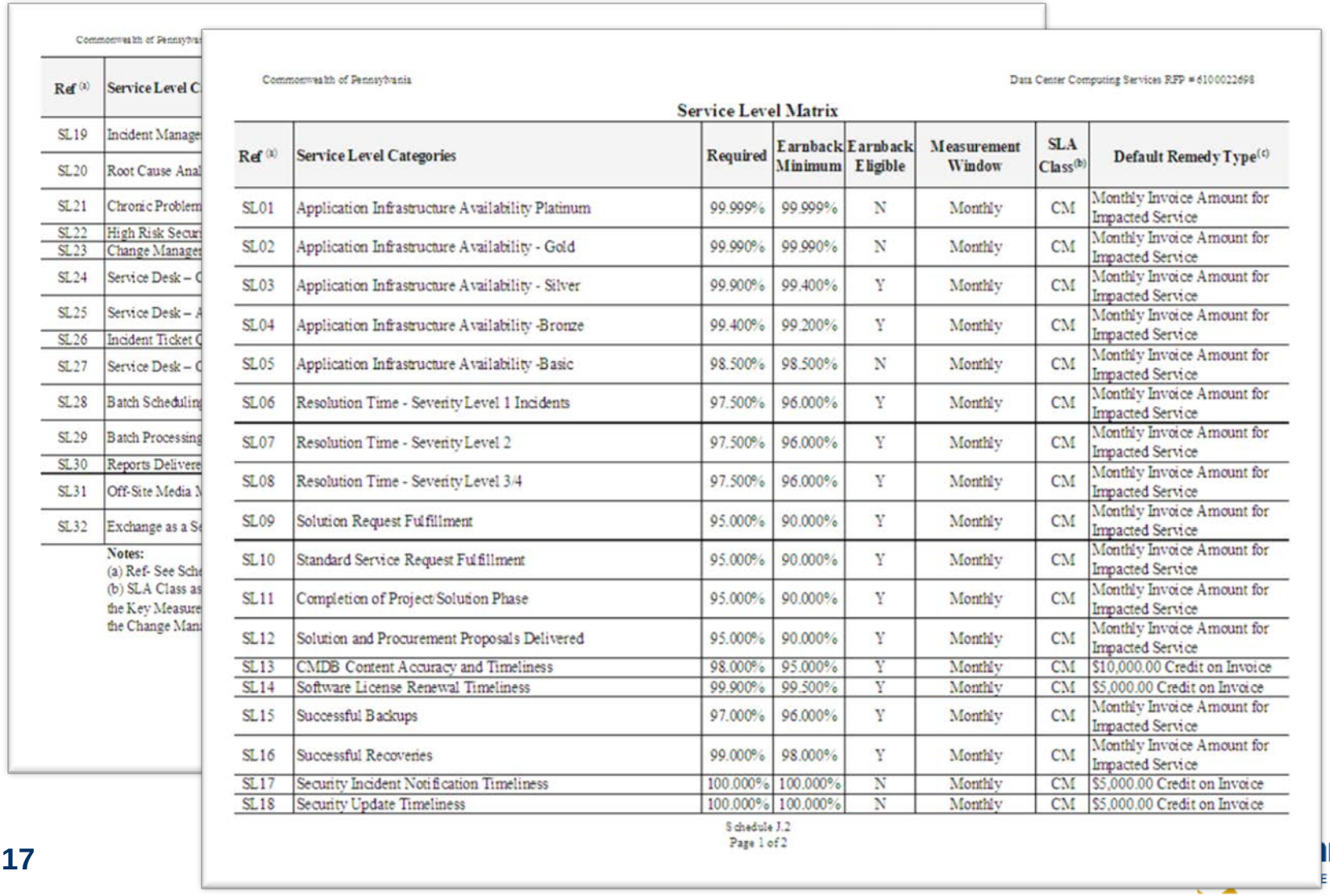
Capacity On Demand and Additional Services

- Server Capacity On Demand
- Storage Capacity On Demand
- DR Infrastructure Services
- Additional Technical Services
- Exchange as a Service

[illegible]

- [illegible]
  - [illegible]
  - [illegible]
  - [illegible]
  - [illegible]
  - [illegible]
  - [illegible]
  - [illegible]
  - [illegible]

pennsylvania
OFFICE OF ADMINISTRATION



Commonwealth of Pennsylvania

Data Center Computing Services RFP # 6100022698

Service Level Matrix

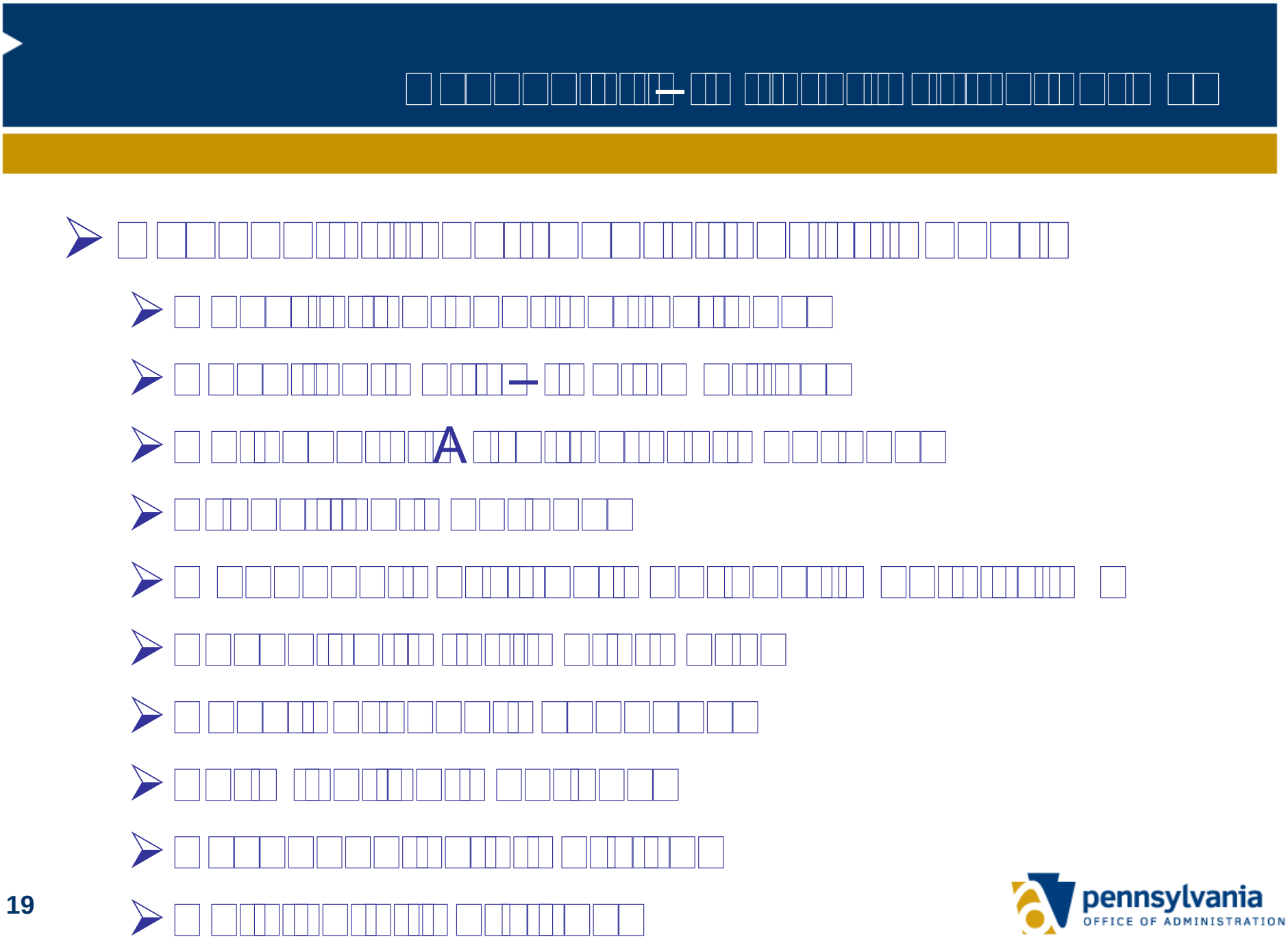
Ref [a]	Service Level Categories	Required	Earnback Minimum	Earnback Eligible	Measurement Window	SLA Class [b]	Default Remedy Type [c]
SL01	Application Infrastructure Availability Platinum	99.999%	99.999%	N	Monthly	CM	Monthly Invoice Amount for Impacted Service
SL02	Application Infrastructure Availability - Gold	99.990%	99.990%	N	Monthly	CM	Monthly Invoice Amount for Impacted Service
SL03	Application Infrastructure Availability - Silver	99.900%	99.400%	Y	Monthly	CM	Monthly Invoice Amount for Impacted Service
SL04	Application Infrastructure Availability -Bronze	99.400%	99.200%	Y	Monthly	CM	Monthly Invoice Amount for Impacted Service
SL05	Application Infrastructure Availability -Basic	98.500%	98.500%	N	Monthly	CM	Monthly Invoice Amount for Impacted Service
SL06	Resolution Time - Severity Level 1 Incidents	97.500%	96.000%	Y	Monthly	CM	Monthly Invoice Amount for Impacted Service
SL07	Resolution Time - Severity Level 2	97.500%	96.000%	Y	Monthly	CM	Monthly Invoice Amount for Impacted Service
SL08	Resolution Time - Severity Level 3/4	97.500%	96.000%	Y	Monthly	CM	Monthly Invoice Amount for Impacted Service
SL09	Solution Request Fulfillment	95.000%	90.000%	Y	Monthly	CM	Monthly Invoice Amount for Impacted Service
SL10	Standard Service Request Fulfillment	95.000%	90.000%	Y	Monthly	CM	Monthly Invoice Amount for Impacted Service
SL11	Completion of Project Solution Phase	95.000%	90.000%	Y	Monthly	CM	Monthly Invoice Amount for Impacted Service
SL12	Solution and Procurement Proposals Delivered	95.000%	90.000%	Y	Monthly	CM	Monthly Invoice Amount for Impacted Service
SL13	CMDB Content Accuracy and Timeliness	98.000%	95.000%	Y	Monthly	CM	$10,000.00 Credit on Invoice
SL14	Software License Renewal Timeliness	99.900%	99.500%	Y	Monthly	CM	$5,000.00 Credit on Invoice
SL15	Successful Backups	97.000%	96.000%	Y	Monthly	CM	Monthly Invoice Amount for Impacted Service
SL16	Successful Recoveries	99.000%	98.000%	Y	Monthly	CM	Monthly Invoice Amount for Impacted Service
SL17	Security Incident Notification Timeliness	100.000%	100.000%	N	Monthly	CM	$5,000.00 Credit on Invoice
SL18	Security Update Timeliness	100.000%	100.000%	N	Monthly	CM	$5,000.00 Credit on Invoice

Schedule J.2
Page 1 of 2

[illegible]

- [illegible]
  - [illegible]
  - [illegible]
- [illegible]
  - [illegible]
  - [illegible]
- [illegible]
  - [illegible]
  - [illegible]

pennsylvania
OFFICE OF ADMINISTRATION



[illegible]

- [illegible]

- [illegible]

pennsylvania
OFFICE OF ADMINISTRATION

[illegible]

- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]

pennsylvania
OFFICE OF ADMINISTRATION

Bureau Of Small Business Opportunities (BSBO)

[illegible]

[illegible]

- [illegible]
- [illegible]

pennsylvania
OFFICE OF ADMINISTRATION

[illegible]

- [illegible]
  - [illegible]
  - [illegible]
  - [illegible]
  - [illegible]
  - [illegible]

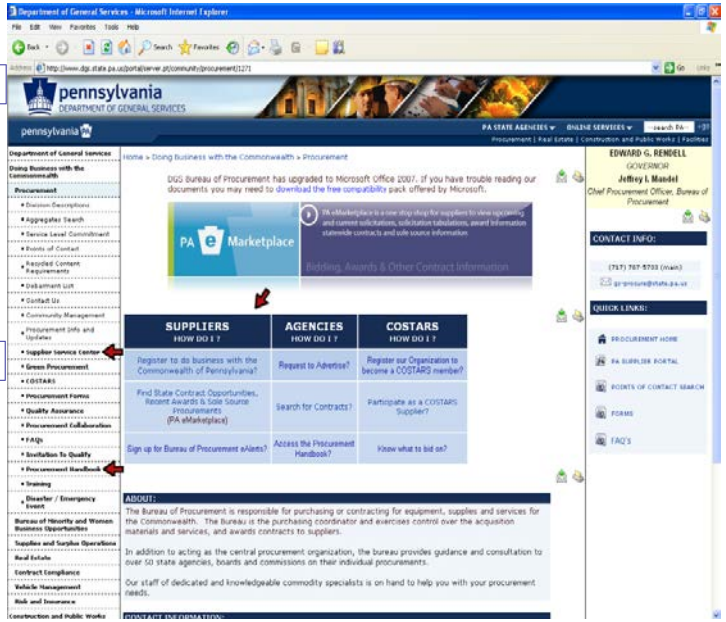
pennsylvania
OFFICE OF ADMINISTRATION

Contact Information

[illegible]

pennsylvania
OFFICE OF ADMINISTRATION

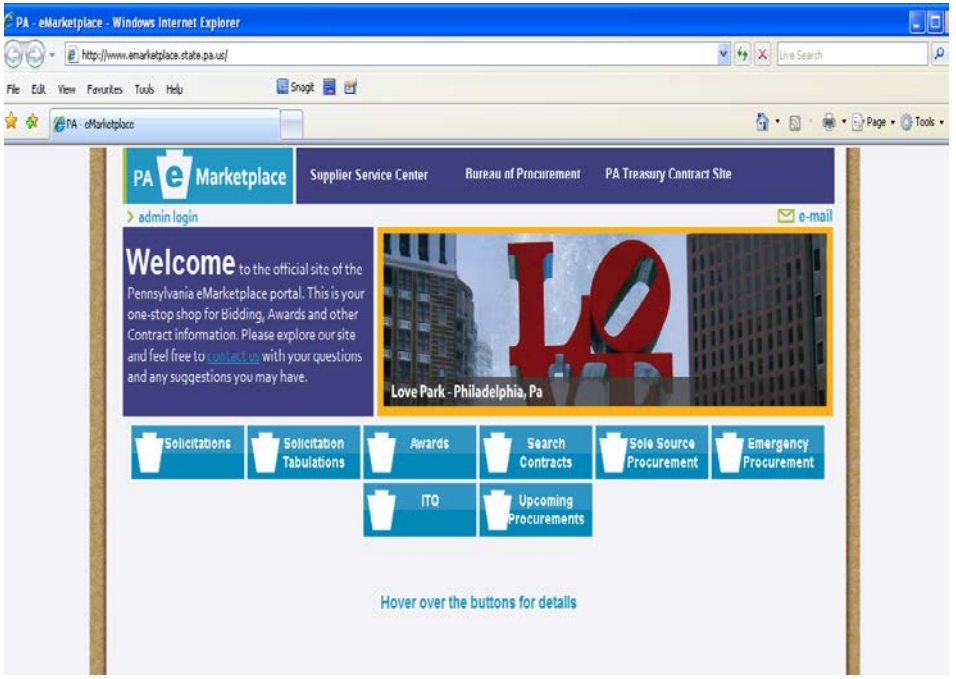
Your Gateway to All Procurement Information



pennsylvania
OFFICE OF ADMINISTRATION

Your Gateway to Contract Information

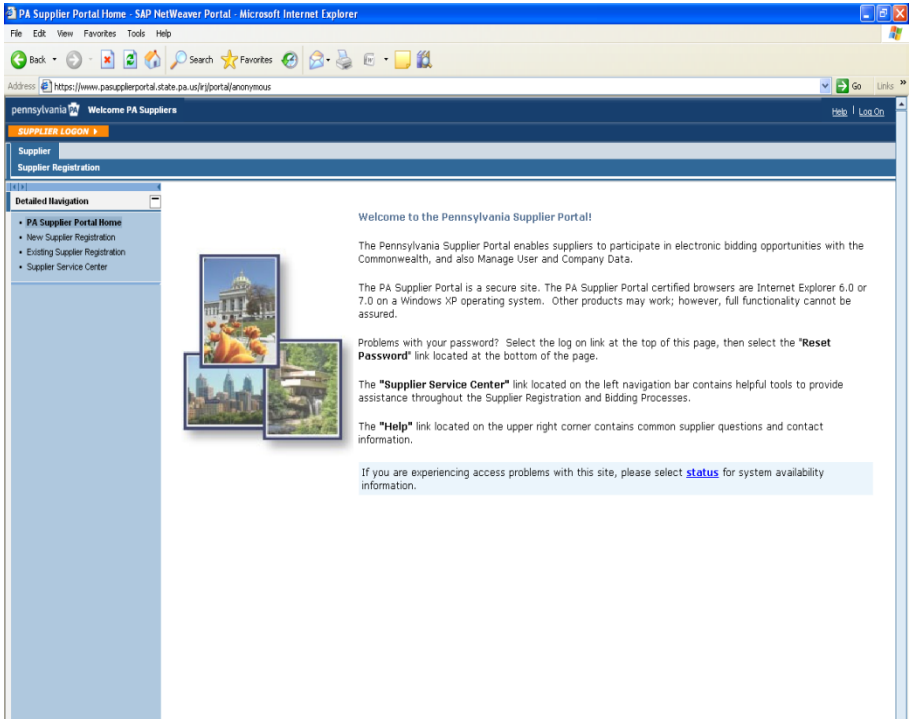
- Solicitations
- Tabulations
- Awards
- Contracts
- Sole Source
- Upcoming Procurements
- Links:
  - Supplier Service Center
  - Treasury Contracts



pennsylvania
OFFICE OF ADMINISTRATION

Your Gateway to Procurement

- New Supplier Registration
- Manage company data
- Link:
  - Supplier Service Center



pennsylvania
OFFICE OF ADMINISTRATION

[illegible]

- [illegible]
  - [illegible]
  - [illegible]
  - [illegible]
- [illegible]
  - [illegible]14[illegible]
  - [illegible]1[illegible]
  - [illegible]2[illegible]
  - [illegible]2[illegible]

pennsylvania
OFFICE OF ADMINISTRATION

[illegible]

- [illegible]

To be responsive, a proposal must be:

- [illegible]
- [illegible]
- [illegible]
  - [illegible]
- [illegible]
  - [illegible]

[illegible]

[illegible]

pennsylvania
OFFICE OF ADMINISTRATION

- [illegible]
  - [illegible]
  - [illegible]
  -

ADDRESS PROPOSAL PROPERLY

[illegible]

- [illegible]
- [illegible]
- [illegible]
- A[illegible]

pennsylvania
OFFICE OF ADMINISTRATION

[illegible]

[illegible] **March 8, 2013, by 1:00 PM EST** [illegible]

Sheryl Kimport, Bureau of IT Procurement
c/o Commonwealth Mail Processing Center
2 Technology Park (rear)
Attn: IT Procurement 506 Finance
Harrisburg, PA 17110

Note: [illegible]

- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]

pennsylvania
OFFICE OF ADMINISTRATION

[illegible]

[illegible]	[illegible]	[illegible]
[illegible] (http://www.emarketplace.state.pa.us) [illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible] *(rear)* [illegible] **Note:** [illegible]	[illegible]	[illegible]

pennsylvania
OFFICE OF ADMINISTRATION

A

- A

  - *Questions Submittal Form* A

  - A

- **All Q&A will become official when posted to DGS e-marketplace website.**

pennsylvania
OFFICE OF ADMINISTRATION

Suppliers requesting a CD copy of the confidential Exhibits for this RFP must contact Sheryl Kimport (Issuing Officer).

Sheryl will be available after the meeting.

Thank you for attending today's pre-proposal conference.

pennsylvania
OFFICE OF ADMINISTRATION

pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Date:	January 29, 2013
Subject:	Data Center Computing Services RFP Addendum
Solicitation Number:	6100022698
Solicitation Due Date	April 12, 2013
Addendum Number:	6

To All Offerors:

The Commonwealth of Pennsylvania defines a solicitation "Addendum" as an addition to or amendment of the original terms, conditions, specification, or instruction of a procurement solicitation (e.g. Invitation for Bids, Request for Quotes and Request for Proposals).

This addendum is intended to inform suppliers of the following change:

1. Due to the high volume of questions received for this RFP and the several requests from the vendor community to extend the due date for responses to this RFP, the Commonwealth has updated the Calendar of Event section of the RFP. Please note the updates/additions below:

Activity	Responsibility	Date
Enterprise Data Center (EDC) Tour and Exhibit Distribution	Issuing Office/Potential Offerors	12/12/12 and 12/13/12
Deadline to submit initial questions via email to RA-OITPurchases@state.pa.us.	Potential Offerors	12/21/12 by 1:00 PM EST
Pre-proposal Conference—Location. Forum 500 Walnut St. Harrisburg, PA 17101	Issuing Office/Potential Offerors	1/17/13 @ 9:00 AM EST
Deadline to submit second round questions via email to RA-OITPurchases@state.pa.us	Potential Offerors	2/1/13 by 1:00 PM EST
Answers to initial questions and second round questions posted to the DGS website (http://www.emarketplace.state.pa.us).	Issuing Office	2/15/13
Deadline to submit final questions via email to RA-OITPurchases@state.pa.us	Potential Offerors	2/22/13 by 1:00 PM EST
Answers to final questions posted to the DGS website (http://www.emarketplace.state.pa.us).	Issuing Office	3/6/13

Activity	Responsibility	Date
Please monitor website for all communications regarding the RFP.	Potential Offerors	Ongoing
Sealed proposal must be received by the Issuing Office at Bureau of IT Procurement c/o Commonwealth Mail Processing Center 2 Technology Park (rear) Attn: IT Procurement 506 Finance Harrisburg PA 17110 Attn: Sheryl Kimport Proposals must be time and date stamped by the facility receiving the proposals. Proposals may only be hand-delivered between 6:00 a.m. and 2:45 p.m., Monday through Friday, excluding Commonwealth holidays.	Offerors	4/12/13 by 1PM EST

For electronic solicitations responses via the PASupplierPortal:

- Attach this addendum to your solicitation response.
- To attach the Addendum, download the Addendum and save to your computer. Move to "My Notes", use the "Browse" button to find the document you just saved and press "Add" to upload the document.
- Review the Attributes section of our solicitation response to ensure you have responded, ad required, to any question relevant to solicitation addenda issues subsequent to the initial advertisement of the solicitation opportunity,

For Solicitation where a "hard copy" (vs. electronic) response if requested:

- If you are already submitted a response to the original solicitation, you may either submit a new response, or return this Addendum with a statement=n that your original response remain fir, by the due date to the following address:

Except as amended by this Addendum, the terms, conditions, specification, and instruction of the solicitation and any previous solicitation addenda, remain as originally written.

Very truly yours,

Name: Sheryl Kimport
Title: Commodity Specialist
Phone: 717.346.2670
Email: skimport@pa.gov

pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Date:	February 8, 2013
Subject:	Data Center Computing Services RFP Addendum
Solicitation Number:	6100022698
Solicitation Due Date	April 12, 2013
Addendum Number:	7

To All Offerors:

The Commonwealth of Pennsylvania defines a solicitation "Addendum" as an addition to or amendment of the original terms, conditions, specification, or instruction of a procurement solicitation (e.g. Invitation for Bids, Request for Quotes and Request for Proposals).

This addendum is intended to inform suppliers of the following change:

1. Additional Round 1 questions and answers have been posted to the emarketplace website. This document is labeled as "6100022698 Questions and Answers - Round 1 Part 3". Please continue to monitor the emarketplace website.

2. A revised Schedule A – DEFINED TERMS 2.8.13 has been posted to the emarketplace website. The following addition has been made to Schedule A:
   1) Definition of "Run Book"

3. A revised Schedule F – COPA DATACENTER STATEMENT OF WORK 2.8.13 has been posted to the emarketplace website. The following sections of Schedule F have been revised:
   1) 3.2.3.2 Site Operations
   2) 3.2.4 Managed Hosting Services

4. A revised Schedule G – STAFFING PLAN AND KEY POSITIONS 2.8.13 has been posted to the emarketplace website. The following section of Schedule G has been revised:
   1) Section 4. Offeror Key Personnel Table

5. A revised Schedule K – KEY PROGRAM DELIVERABLES 2.8.13 has been posted to the emarketplace website. The following sections of Schedule K have been revised:
   1) D – 02.39
   2) D – 02.44
   3) D – 02.49

For electronic solicitations responses via the PASupplierPortal:

- Attach this addendum to your solicitation response.
- To attach the Addendum, download the Addendum and save to your computer. Move to "My Notes", use the "Browse" button to find the document you just saved and press "Add" to upload the document.

- Review the Attributes section of our solicitation response to ensure you have responded, ad required, to any question relevant to solicitation addenda issues subsequent to the initial advertisement of the solicitation opportunity,

For Solicitation where a "hard copy" (vs. electronic) response if requested:

- If you are already submitted a response to the original solicitation, you may either submit a new response, or return this Addendum with a statement=n that your original response remain fir, by the due date to the following address:

Except as amended by this Addendum, the terms, conditions, specification, and instruction of the solicitation and any previous solicitation addenda, remain as originally written.

Very truly yours,

Name: Sheryl Kimport
Title: Commodity Specialist
Phone: 717.346.2670
Email: skimport@pa.gov

pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Date:	February 15, 2013
Subject:	Data Center Computing Services RFP Addendum
Solicitation Number:	6100022698
Solicitation Due Date	April 12, 2013
Addendum Number:	8

To All Offerors:

The Commonwealth of Pennsylvania defines a solicitation "Addendum" as an addition to or amendment of the original terms, conditions, specification, or instruction of a procurement solicitation (e.g. Invitation for Bids, Request for Quotes and Request for Proposals).

This addendum is intended to inform suppliers of the following change:

1. Additional Round 1 questions and answers have been posted to the emarketplace website. This document is labeled as "6100022698 Questions and Answers - Round 1 Part 4". Please continue to monitor the emarketplace website.

2. Due to the large volume, the Commonwealth will post answers to the questions from Round 2 at a later date. Please continue to monitor the emarketplace website.

3. The Commonwealth has posted a revised RFP document titled 6100022698 – Request for Proposal (Revised 2.15.13). Revisions were made to the Calendar of Events (Second Round Responses Date) and Table of Contents (Added reference to Exhibit D.8 and Exhibit O).

For electronic solicitations responses via the PASupplierPortal:

- Attach this addendum to your solicitation response.
- To attach the Addendum, download the Addendum and save to your computer. Move to "My Notes", use the "Browse" button to find the document you just saved and press "Add" to upload the document.
- Review the Attributes section of our solicitation response to ensure you have responded, ad required, to any question relevant to solicitation addenda issues subsequent to the initial advertisement of the solicitation opportunity,

For Solicitation where a "hard copy" (vs. electronic) response if requested:

- If you are already submitted a response to the original solicitation, you may either submit a new response, or return this Addendum with a statement=n that your original response remain fir, by the due date to the following address:

Except as amended by this Addendum, the terms, conditions, specification, and instruction of the solicitation and any previous solicitation addenda, remain as originally written.

Very truly yours,

Name: Sheryl Kimport
Title: Commodity Specialist
Phone: 717.346.2670
Email: skimport@pa.gov

pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Date:	February 22, 2013
Subject:	Data Center Computing Services RFP Addendum
Solicitation Number:	6100022698
Solicitation Due Date	April 12, 2013
Addendum Number:	9

To All Offerors:

The Commonwealth of Pennsylvania defines a solicitation "Addendum" as an addition to or amendment of the original terms, conditions, specification, or instruction of a procurement solicitation (e.g. Invitation for Bids, Request for Quotes and Request for Proposals).

This addendum is intended to inform suppliers of the following change:

1. Additional Round 1 questions and answers have been posted to the emarketplace website. This document is labeled as "6100022698 Questions and Answers - Round 1 Part 5."

2. Please continue to monitor the emarketplace website for additional Question and Answer postings.

3. The Commonwealth has posted a revised RFP document titled 6100022698 – Request for Proposal (Revised 2.22.13). Revisions were made to the Table of Contents (Added Exhibits B.7 and B.8 and D.8 through D.12). . These are confidential documents. To receive a copy, please contact Sheryl Kimport, the Issuing Officer.

4. Revised versions of the following documents have been posted to the emarketplace website. Revisions were made based on information provided as part of as "6100022698 Questions and Answers - Round 1 Part 5":
   - 6100022698 - Schedule D - Transition Milestones 2.22.13
   - 6100022698 - Schedule F - Datacenter Statement of Work 2.22.13
   - 6100022698 - Schedule G - Staffing Plan and Key Positions 2.22.13
   - 6100022698 - Schedule J.2 - Datacenter Service Level Matrix 2.22.13
   - 6100022698 - Schedule J.3 - Datacenter SLA Definitions 2.22.13

For electronic solicitations responses via the PASupplierPortal:

- Attach this addendum to your solicitation response.
- To attach the Addendum, download the Addendum and save to your computer. Move to "My Notes", use the "Browse" button to find the document you just saved and press "Add" to upload the document.
- Review the Attributes section of our solicitation response to ensure you have responded, ad required, to any question relevant to solicitation addenda issues subsequent to the initial advertisement of the solicitation opportunity,

For Solicitation where a "hard copy" (vs. electronic) response if requested:

- If you are already submitted a response to the original solicitation, you may either submit a new response, or return this Addendum with a statement=n that your original response remain fir, by the due date to the following address:

Except as amended by this Addendum, the terms, conditions, specification, and instruction of the solicitation and any previous solicitation addenda, remain as originally written.

Very truly yours,

Name: Sheryl Kimport
Title: Commodity Specialist
Phone: 717.346.2670
Email: skimport@pa.gov

pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Date:	February 27, 2013
Subject:	Data Center Computing Services RFP Addendum
Solicitation Number:	6100022698
Solicitation Due Date	June 19, 2013
Addendum Number:	10

To All Offerors:

The Commonwealth of Pennsylvania defines a solicitation "Addendum" as an addition to or amendment of the original terms, conditions, specification, or instruction of a procurement solicitation (e.g. Invitation for Bids, Request for Quotes and Request for Proposals).

This addendum is intended to inform suppliers of the following change:

1. The Commonwealth has updated the Calendar of Event section of the RFP. Please note the updates/additions below:

Activity	Responsibility	Date
Enterprise Data Center (EDC) Tour and Exhibit Distribution	Issuing Office/Potential Offerors	12/12/12 and 12/13/12
Deadline to submit initial questions via email to RA-OITPurchases@state.pa.us.	Potential Offerors	12/21/12 by 1:00 PM EST
Pre-proposal Conference—Location. Forum 500 Walnut St. Harrisburg, PA 17101	Issuing Office/Potential Offerors	1/17/13 @ 9:00 AM EST
Deadline to submit second round questions via email to RA-OITPurchases@state.pa.us	Potential Offerors	2/1/13 by 1:00 PM EST
Answers to second round of questions posted to the DGS website (http://www.emarketplace.state.pa.us).	Issuing Office	TBD
Deadline to submit third round questions via email to RA-OITPurchases@state.pa.us	Potential Offerors	2/22/13 by 1:00 PM EST
Answers to third round of questions posted to the DGS website (http://www.emarketplace.state.pa.us).	Issuing Office	TBD

Activity	Responsibility	Date
Post updated RFP documents including Schedules, Exhibits and answers to all questions received.	Issuing Office	4/17/13
Deadline to submit final questions via email to RA-OITPurchases@state.pa.us	Potential Offerors	4/26/13 by 12:00 PM EST
Answers to final questions posted to the DGS website **(**http://www.emarketplace.state.pa.us **)**.	Issuing Office	5/14/13
Please monitor website for all communications regarding the RFP.	Potential Offerors	Ongoing
Sealed proposal must be received by the Issuing Office at Bureau of IT Procurement c/o Commonwealth Mail Processing Center 2 Technology Park (rear) Attn: IT Procurement 506 Finance Harrisburg PA 17110 Attn: Sheryl Kimport Proposals must be time and date stamped by the facility receiving the proposals. Proposals may only be hand-delivered between 6:00 a.m. and 2:45 p.m., Monday through Friday, excluding Commonwealth holidays.	Offerors	6/19/13 by 1:00 PM EST

For electronic solicitations responses via the PASupplierPortal:

- Attach this addendum to your solicitation response.
- To attach the Addendum, download the Addendum and save to your computer. Move to "My Notes", use the "Browse" button to find the document you just saved and press "Add" to upload the document.
- Review the Attributes section of our solicitation response to ensure you have responded, ad required, to any question relevant to solicitation addenda issues subsequent to the initial advertisement of the solicitation opportunity,

For Solicitation where a "hard copy" (vs. electronic) response if requested:

- If you are already submitted a response to the original solicitation, you may either submit a new response, or return this Addendum with a statement=n that your original response remain fir, by the due date to the following address:

Except as amended by this Addendum, the terms, conditions, specification, and instruction of the solicitation and any previous solicitation addenda, remain as originally written.

Very truly yours,

Name: Sheryl Kimport
Title: Commodity Specialist
Phone: 717.346.2670
Email: skimport@pa.gov

pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Date:	March 1, 2013
Subject:	Data Center Computing Services RFP Addendum
Solicitation Number:	6100022698
Solicitation Due Date	June 19, 2013
Addendum Number:	11

To All Offerors:

The Commonwealth of Pennsylvania defines a solicitation "Addendum" as an addition to or amendment of the original terms, conditions, specification, or instruction of a procurement solicitation (e.g. Invitation for Bids, Request for Quotes and Request for Proposals).

This addendum is intended to inform suppliers of the following change:

1. Additional Round 1 questions and answers have been posted to the emarketplace website. This document is labeled as "6100022698 Questions and Answers - Round 1 Part 6."

2. A revised 6100022698 - Schedule J.3 - Datacenter SLA Definitions 3 1 13 has been posted to the emarketplace website.

   1) Updated formula for SL20

3. The Commonwealth received 117 questions during the second round of Q&A. Due to the large volume, the Commonwealth will post answers to the questions in parts. A document labeled "6100022698 Questions and Answers - Round 2 Part 1" has been posted to the emarketplace website.

4. Please continue to monitor the emarketplace website for additional Question and Answer postings.

For electronic solicitations responses via the PASupplierPortal:

- Attach this addendum to your solicitation response.
- To attach the Addendum, download the Addendum and save to your computer. Move to "My Notes", use the "Browse" button to find the document you just saved and press "Add" to upload the document.
- Review the Attributes section of our solicitation response to ensure you have responded, ad required, to any question relevant to solicitation addenda issues subsequent to the initial advertisement of the solicitation opportunity,

For Solicitation where a "hard copy" (vs. electronic) response if requested:

- If you are already submitted a response to the original solicitation, you may either submit a new response, or return this Addendum with a statement=n that your original response remain fir, by the due date to the following address:

Except as amended by this Addendum, the terms, conditions, specification, and instruction of the solicitation and any previous solicitation addenda, remain as originally written.

Very truly yours,

Name: Sheryl Kimport
Title: Commodity Specialist
Phone: 717.346.2670
Email: skimport@pa.gov

pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Date:	March 8, 2013
Subject:	Data Center Computing Services RFP Addendum
Solicitation Number:	6100022698
Solicitation Due Date	June 19, 2013
Addendum Number:	12

To All Offerors:

The Commonwealth of Pennsylvania defines a solicitation "Addendum" as an addition to or amendment of the original terms, conditions, specification, or instruction of a procurement solicitation (e.g. Invitation for Bids, Request for Quotes and Request for Proposals).

This addendum is intended to inform suppliers of the following change:

1. Additional Round 1 questions and answers have been posted to the emarketplace website. This document is labeled as "6100022698 Questions and Answers - Round 1 Part 7."

2. Please continue to monitor the emarketplace website for additional Question and Answer postings.

For electronic solicitations responses via the PASupplierPortal:

- Attach this addendum to your solicitation response.
- To attach the Addendum, download the Addendum and save to your computer. Move to "My Notes", use the "Browse" button to find the document you just saved and press "Add" to upload the document.
- Review the Attributes section of our solicitation response to ensure you have responded, ad required, to any question relevant to solicitation addenda issues subsequent to the initial advertisement of the solicitation opportunity,

For Solicitation where a "hard copy" (vs. electronic) response if requested:

- If you are already submitted a response to the original solicitation, you may either submit a new response, or return this Addendum with a statement=n that your original response remain fir, by the due date to the following address:

Except as amended by this Addendum, the terms, conditions, specification, and instruction of the solicitation and any previous solicitation addenda, remain as originally written.

Very truly yours,

Name: Sheryl Kimport
Title: Commodity Specialist
Phone: 717.346.2670
Email: skimport@pa.gov

pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Date:	March 29, 2013
Subject:	Data Center Computing Services RFP Addendum
Solicitation Number:	6100022698
Solicitation Due Date	June 19, 2013
Addendum Number:	13

To All Offerors:

The Commonwealth of Pennsylvania defines a solicitation "Addendum" as an addition to or amendment of the original terms, conditions, specification, or instruction of a procurement solicitation (e.g. Invitation for Bids, Request for Quotes and Request for Proposals).

This addendum is intended to inform suppliers of the following change:

1. Additional questions and answers have been posted to the emarketplace website. This document is labeled as "6100022698 Questions and Answers -Additional Answers."

   Please note this will be the final posting of questions and answers prior to the posting of the updated RFP documents on April 17th. Any questions that have not been answered thus far will be posted on April 17th.

For electronic solicitations responses via the PASupplierPortal:

- Attach this addendum to your solicitation response.
- To attach the Addendum, download the Addendum and save to your computer. Move to "My Notes", use the "Browse" button to find the document you just saved and press "Add" to upload the document.
- Review the Attributes section of our solicitation response to ensure you have responded, ad required, to any question relevant to solicitation addenda issues subsequent to the initial advertisement of the solicitation opportunity,

For Solicitation where a "hard copy" (vs. electronic) response if requested:

- If you are already submitted a response to the original solicitation, you may either submit a new response, or return this Addendum with a statement=n that your original response remain fir, by the due date to the following address:

Except as amended by this Addendum, the terms, conditions, specification, and instruction of the solicitation and any previous solicitation addenda, remain as originally written.

Very truly yours,

Name: Sheryl Kimport
Title: Commodity Specialist
Phone: 717.346.2670
Email: skimport@pa.gov

pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Date:	April 3, 2013
Subject:	Data Center Computing Services RFP Addendum
Solicitation Number:	6100022698
Solicitation Due Date	June 19, 2013
Addendum Number:	14

To All Offerors:

The Commonwealth of Pennsylvania defines a solicitation "Addendum" as an addition to or amendment of the original terms, conditions, specification, or instruction of a procurement solicitation (e.g. Invitation for Bids, Request for Quotes and Request for Proposals).

This addendum is intended to request additional information:

The Issuing Office received the following questions regarding the Small Disadvantaged Business (SDB) program and corresponding sections of the RFP and has not yet provided answers. To ensure the questions are addressed accurately and completely, please clarify the questions and provide additional detail to fully state all concerns about the requirements of the SDB Program specific to this RFP. **Please provide this information and any additional questions about the SDB Program no later than 4:00pm on Friday, April 5, 2013.**

Q The Commonwealth's response to question #45 (Round 1, Part 3), stated: "The 60% requirement stated in Part III-4 applies to all prime contractors. No SDB points will be awarded to an Offeror unless the company serving as the prime contractor directly performs at least 60% of the total contract value."

"Total Contract Value" implies the inclusion of labor, facilities, hardware, software, telecommunications, office space, etc. Could the Commonwealth please confirm that the aforementioned components should be included in total contract value?

Request for Offeror Clarification: If it is assumed, for purposes of evaluation only, that the total set out in the Offeror's cost submittal is the Total Contract Value, please explain why these items would not normally be included in the Total Contract Value. Also, please provide a complete list of items that the Offeror would not consider to be part of the Total Contract value.

Q Related to question #45 (Round 1, Part 3), the Commonwealth has made no commitment to a baseline volume. As such, legally, there is no financial commitment associated with this contract. In this case the Total Contract Value = $0. Given this, it would be impossible to calculate the percentage of work performed (i.e. the 60% requirement) of total contract value, because the denominator is 0. In such an event, no vendor would qualify for any of the Small Diverse Business Participation points. Is our interpretation correct?

Request for Offeror Clarification: If it is assumed that, for purposes of evaluation only, that the total set out in the Offeror's cost submittal is the Total Contract Value. What information, other than baseline commitments, is required to allow an Offeror to determine the percentage of work to be performed?

Q Section II-9, subsection B, item 1, of the RFP on page 21 states "Offerors must include a numerical percentage which represents the total percentage of the work (as a percentage of the total cost in the Cost Submittal) to be performed by the Offeror and not by subcontractors and suppliers." As this relates to the 60% requirement in RFP section III-4, item C.1 on page 24 of the RFP, can the Commonwealth provide guidance on how to meet the 60% requirement given the amount of facilities, hardware, software, telecommunications, office space, etc. that would have to be included in the denominator of this calculation?

Request for Offeror Clarification: If it is assumed that, for purposes of evaluation only, that the total set out in the Offeror's cost submittal is the Total Contract Value, with the exception of committed baselines, what other information would be required to determine the 60%.

Q The answer to this question (#29 in Round 1, Part 3) restated the requirement to provide a "numerical percentage"; however, the answer did not address how a "dollar amount of each subcontract commitment to a Small Diverse Business" (as called for in the RFP Part II-9, B, 2, page 21) can be provided since the Commonwealth is not committing to a minimum participation. In other words, given that the Commonwealth is unwilling to provide any level of financial commitment or any level of committed participation, please clarify how the "dollar amount" requirement should be calculated.

Request for Offeror Clarification: If it is assumed that, for purposes of evaluation only, that the total set out in the Offeror's cost submittal would be equivalent to the Total Contract Value, with the exception of committed baselines, what other information would be required to calculate the dollar amount for each commitment?

For electronic solicitations responses via the PASupplierPortal:

- Attach this addendum to your solicitation response.
- To attach the Addendum, download the Addendum and save to your computer. Move to "My Notes", use the "Browse" button to find the document you just saved and press "Add" to upload the document.
- Review the Attributes section of our solicitation response to ensure you have responded, ad required, to any question relevant to solicitation addenda issues subsequent to the initial advertisement of the solicitation opportunity,

For Solicitation where a "hard copy" (vs. electronic) response if requested:

- If you are already submitted a response to the original solicitation, you may either submit a new response, or return this Addendum with a statement=n that your original response remain fir, by the due date to the following address:

Except as amended by this Addendum, the terms, conditions, specification, and instruction of the solicitation and any previous solicitation addenda, remain as originally written.

Very truly yours,

Name: Sheryl Kimport

Title: Commodity Specialist
Phone: 717.346.2670
Email: skimport@pa.gov

pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Date:	April 17, 2013
Subject:	Data Center Computing Services RFP Addendum
Solicitation Number:	6100022698
Solicitation Due Date	June 19, 2013
Addendum Number:	15

To All Offerors:

The Commonwealth of Pennsylvania defines a solicitation "Addendum" as an addition to or amendment of the original terms, conditions, specification, or instruction of a procurement solicitation (e.g. Invitation for Bids, Request for Quotes and Request for Proposals).

This addendum is intended to inform suppliers of the following change:

1. The document titled "6100022698 - Master Questions and Answers (4.16.13)" replaces all previously posted Question and Answer documents. This document contains responses to all questions received for this RFP as of April 17, 2013. The Commonwealth has provided revised answers to some previous responses. The revised answers can be found in the "New and Revised Answers" section of this document.

2. Revised versions of the following documents are made part of this RFP:
   - 6100022698 - Request for Proposal (4.17.13)
   - 6100022698 - Appendix A - Terms and Conditions (4.16.13)
   - 6100022698 - Schedule A - Defined Terms (4.16.13)
   - 6100022698 - Schedule C - Services Catalog (4.16.13)
   - 6100022698 - Schedule D - Transition Milestones (4.16.13)
   - 6100022698 - Schedule F - Datacenter Statement of Work (4.16.13)
   - 6100022698 - Schedule G - Staffing Plan and Key Positions (4.16.13)
   - 6100022698 - Schedule I - Offeror Pricing Forms (4.16.13)
   - 6100022698 - Schedule J.3 - Datacenter SLA Definitions (4.16.13)
   - 6100022698 - Schedule K - Key Program Deliverables (4.16.13)
   - 6100022698 - Exhibit D.1 - EDC - Server Inventory
   - 6100022698 - Exhibit J.2 - ITB SEC022
   - 6100022698 - Exhibit K - OA Enterprise ITSM System and Volumetric
   - 6100022698 - Exhibit O – 2012 Agency No Maintenance Periods

3. The following new documents are added to the RFP:
   - 6100022698 - Appendix J - SDB Letter of Intent
   - 6100022698 - Exhibit B.4 - DPH - Third Party Software - Contractor provided
   - 6100022698 - Exhibit B.9 - DPH - Recovery Time Objectives
   - 6100022698 - Exhibit B.10 - DPH - Third Party Software - Commonwealth Licensed Contractor Maintained and Managed
   - 6100022698 - Exhibit C.12 - DPW - Environments_v25_Updated_03-20-2013

- 6100022698 - Exhibit C.13 - DPW - Products on Mainframes
- 6100022698 - Exhibit D.13 - EDC - Business Partner Circuits
- 6100022698 - Exhibit D.14 - EDC - Hardware Warranty Information
- 6100022698 - Exhibit D.15 - EDC - Electrical System Testing Results
- 6100022698 - Exhibit E.42 - DLI - BOIS Software List
- 6100022698 - Exhibit E.43 - DLI - UC Software
- 6100022698 - Exhibit F.4 - DOH - Physical Servers
- 6100022698 - Exhibit G.6 - PSP - CJIS Security Policy
- 6100022698 - Exhibit I.14 - IES - IES Anticipated SLA Service Levels
- 6100022698 - Exhibit J.4 – Security Agent Standard Tools
- 6100022698 - Exhibit N.1 - PennDOT - Enterprise Network Connectivity Diagram
- 6100022698 - Exhibit N.2 - PennDOT - Monitoring
- 6100022698 - Exhibit P - Enterprise Internet Bandwidth Utilization
- 6100022698 - Exhibit Q - Mailbox Restore Policy
- 6100022698 - Exhibit R - Transition Considerations
- 6100022698 - Exhibit S - Datacenter Locations
- 6100022698 - Exhibit T - Critical Configuration Considerations
- 6100022698 - Exhibit U - COPANET Locations
- 6100022698 - Exhibit V - SCSC - Power 520 System I

Note: All Schedules and Appendices have been made available on the emarketplace website. All exhibits are confidential documents. To receive a copy, please contact Sheryl Kimport, the Issuing Officer.

For electronic solicitations responses via the PASupplierPortal:

- Attach this addendum to your solicitation response.
- To attach the Addendum, download the Addendum and save to your computer. Move to "My Notes", use the "Browse" button to find the document you just saved and press "Add" to upload the document.
- Review the Attributes section of our solicitation response to ensure you have responded, ad required, to any question relevant to solicitation addenda issues subsequent to the initial advertisement of the solicitation opportunity,

For Solicitation where a "hard copy" (vs. electronic) response if requested:

- If you are already submitted a response to the original solicitation, you may either submit a new response, or return this Addendum with a statement=n that your original response remain fir, by the due date to the following address:

Except as amended by this Addendum, the terms, conditions, specification, and instruction of the solicitation and any previous solicitation addenda, remain as originally written.

Very truly yours,

Name: Sheryl Kimport
Title: Commodity Specialist
Phone: 717.346.2670
Email: skimport@pa.gov

pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Date:	May 14, 2013
Subject:	Data Center Computing Services RFP Addendum
Solicitation Number:	6100022698
Solicitation Due Date	June 19, 2013
Addendum Number:	16

To All Offerors:

The Commonwealth of Pennsylvania defines a solicitation "Addendum" as an addition to or amendment of the original terms, conditions, specification, or instruction of a procurement solicitation (e.g. Invitation for Bids, Request for Quotes and Request for Proposals).

This addendum is intended to inform suppliers of the following change:

1. 1. The document titled "6100022698 - Master Questions and Answers (5.14.13)" replaces all previously posted Question and Answer documents. This document contains responses to all questions received for this RFP as of May 14, 2013.

2. Revised versions of the following documents are made part of this RFP:
   - 6100022698 - Request for Proposal (5.14.13)
   - 6100022698 - Appendix A - Terms and Conditions (5.14.13)
   - 6100022698 - Schedule A - Defined Terms (5.14.13)
   - 6100022698 - Schedule F - Datacenter Statement of Work (5.14.13)
   - 6100022698 - Schedule I - Offeror Pricing Forms (5.14.13)
   - 6100022698 - Schedule J.2 – Datacenter Service Level Matrix (5.14.13)
   - 6100022698 - Schedule J.3 - Datacenter SLA Definitions (5.14.13)
   - 6100022698 - Schedule K - Key Program Deliverables (5.14.13).
   - 6100022698 - Exhibit B.4 – DPH – Third Party Software (5.14.13)
   - 6100022698 - Exhibit B.10 – DPH – Hybrid Third Party Software (5.14.13)

Note: All Schedules and Appendices have been made available on the emarketplace website. All exhibits are confidential documents. To receive a copy, please contact Sheryl Kimport, the Issuing Officer.

For electronic solicitations responses via the PASupplierPortal:

- Attach this addendum to your solicitation response.
- To attach the Addendum, download the Addendum and save to your computer. Move to "My Notes", use the "Browse" button to find the document you just saved and press "Add" to upload the document.
- Review the Attributes section of our solicitation response to ensure you have responded, ad required, to any question relevant to solicitation addenda issues subsequent to the initial advertisement of the solicitation opportunity,

For Solicitation where a "hard copy" (vs. electronic) response if requested:

- If you are already submitted a response to the original solicitation, you may either submit a new response, or return this Addendum with a statement=n that your original response remain fir, by the due date to the following address:

Except as amended by this Addendum, the terms, conditions, specification, and instruction of the solicitation and any previous solicitation addenda, remain as originally written.

Very truly yours,

Name: Sheryl Kimport
Title: Commodity Specialist
Phone: 717.346.2670
Email: skimport@pa.gov

pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Date:	May 24, 2013
Subject:	Data Center Computing Services RFP Addendum
Solicitation Number:	6100022698
Solicitation Due Date	June 19, 2013
Addendum Number:	17

To All Offerors:

The Commonwealth of Pennsylvania defines a solicitation "Addendum" as an addition to or amendment of the original terms, conditions, specification, or instruction of a procurement solicitation (e.g. Invitation for Bids, Request for Quotes and Request for Proposals).

This addendum is intended to inform suppliers of the following change:

Revised versions of the following documents are made part of this RFP:

1. 6100022698 - Request for Proposals (5.24.13)
   - The Issuing Officer has been changed to:

     Janis Brown
     506 Finance Building
     Harrisburg, PA 17120
     RA-OITPurchases@pa.gov

2. 6100022698 - Appendix A - Terms and Conditions (5.24.13)
   - Section 45 (Insurance) has been revised.

Note: All Schedules and Appendices have been made available on the emarketplace website

For electronic solicitations responses via the PASupplierPortal:

- Attach this addendum to your solicitation response.
- To attach the Addendum, download the Addendum and save to your computer. Move to "My Notes", use the "Browse" button to find the document you just saved and press "Add" to upload the document.
- Review the Attributes section of our solicitation response to ensure you have responded, ad required, to any question relevant to solicitation addenda issues subsequent to the initial advertisement of the solicitation opportunity,

For Solicitation where a "hard copy" (vs. electronic) response if requested:

- If you are already submitted a response to the original solicitation, you may either submit a new response, or return this Addendum with a statement that your original response remains firm, by the due date to the following address:

Bureau of IT Procurement
c/o Commonwealth Mail Processing Center
2 Technology Park (rear)
Attn: IT Procurement 506 Finance
Harrisburg PA 17110
Attn: Janis Brown

Except as amended by this Addendum, the terms, conditions, specification, and instruction of the solicitation and any previous solicitation addenda, remain as originally written.

Very truly yours,

Name: Sheryl Kimport
Title: Commodity Specialist
Phone: 717.346.2670
Email: skimport@pa.gov

Previously Answered Questions (Note: answers with strikethrough have been revised. The revised answers can be found in the "New and Revised Answers" section of this document.)

Addendum 3 - Round 1, Part 1

	Doc	Sec	Pg	Question	Answer
1.	Appendix A	N/A	N/A	As the Commonwealth has required financial background info for the Offerors, and likely they will be publically traded companies. As a result, they will be subject to Sarbanes-Oxley. In this light, it is required that firms have the ability to identity all liabilities to shareholders and the SEC. The RFP identifies unlimited liability in several areas not limited to security breaches. This provides unreasonable expectations as all liabilities are expected to be quantified. Will the Commonwealth please consider limiting all liability as it pertains to this contract?	Objections to the terms and conditions set forth in Appendix A may be made according to Part II-8 of the RFP.
2.	Appendix A	2(f)(1) & Sec. 5(a)	Pages 2 and 4	Appendix A, Sec. 2(f)(1) of the contract states that no handwritten signatures will be required in order for the Contract or Purchase Order to be legally enforceable, whereas Sec. 5(a) suggests that the contract will include a signature page. If signature pages are not required, will the Commonwealth please clarify how the parties will evidence their intent to enter into a binding contract?	The contract will include a signature page. The selected Offeror will be required to sign the contract in ink. All Commonwealth officials will sign the contract electronically.
3.	Appendix A	1.B	1	Commonwealth states "Further, the Commonwealth reserves the right to extend this Contract or any part of this Contract up to three (3) months, or as necessary to prevent a lapse in Contract coverage". As currently written the Commonwealth reserves this right in perpetuity. Is that the intent?	The term of the contract will be for 7-years and may be extended by the Commonwealth for up to three additional years. The referenced provision allows the Commonwealth to extend the contract for a period of time to avoid a lapse in contract coverage. Objections to the terms and conditions set forth in Appendix A may be made according to Part II-8 of the RFP.
4.	Appendix A	1(a) Contract Term	1	Is the estimated 18-30 month transition period included in the 7-year base contract? Or does the 7-year term begin after transition is complete (18-30 month transition plus 7-years)?	The transition period is included within the 7-year term.
5.	Appendix A	1(b)	1	In the phrase "any part of this contract", what constitutes a part i.e. a single system, a single agency, etc.?	This phrase refers to any Service or portion of a Service included in the contract. Objections to the terms and conditions set forth in Appendix A may be made according to Part II-8 of the RFP.
6.	Appendix A	2	2	How will the Purchase Order process be used and how does it differ from the Change Control procedures?	The RFP references two types of change control procedures. Section 27 (Change Control) of Appendix A sets out the procedures that will be used to modify the contract. The RFP also references ITIL change control procedures that may be used to modify the configuration of an infrastructure component of a Service. Other than a purchase order serving as a notice to proceed, the Commonwealth does not anticipate issuing Purchase Orders during the term of this contract.

Addendum 3 - Round 1, Part 1					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
7.□	Appendix A	2(a)	Page 2	Appendix A, Sec. 2(a): The contract states that the Commonwealth may issue one or more Purchase Orders against the Contract. Will one purchase order be issued in connection with the base term of the agreement?	Other than a purchase order serving as a notice to proceed, the Commonwealth does not anticipate issuing Purchase Orders during the term of this contract.
8.□	Appendix A	2(a)	2	How do purchase orders align to the "Change Control Procedures" process defined in section 27?	Other than a purchase order serving as a notice to proceed, the Commonwealth does not anticipate issuing Purchase Orders during the term of this contract.
9.□	Appendix A	2 (g)	2	Please provide an estimate on the quantity of purchase orders over a monthly period where you expect that payment would be made using the Commonwealth Procurement Visa Card.	The Commonwealth expects this to occur very infrequently. Less than 5 times per year.
10.□	Appendix A	6 (b) (2) (ii)	5	Please provide examples of incidental services, functions or responsibilities not specifically described in the contract.	The provision speaks for itself. Objections to the terms and conditions set forth in Appendix A may be made according to Part II-8 of the RFP.
11.□	Appendix A	6.(j)	7	Please also confirm that this includes all proprietary software not found in Section 8, but listed throughout the exhibits.	"Contractor Licenses and Permits" includes software licenses for the proprietary software listed throughout the RFP.
12.□	Appendix A	6.(j)	7	Please clarify that the use of the words "Contractor Licenses and Permits" also includes software licenses.	"Contractor Licenses and Permits" includes software licenses.
13.□	Appendix A	7(a)(1) Equipment	8	"All replacements and upgrades shall be addressed through the Change Control Procedure." Does this mean any hardware refresh should be excluded from RFP solution and pricing?	All replacements, upgrades and hardware refreshes must be included within the proposal and pricing.
14.□	Appendix A	6 (i)	6	Who will manage Internet ingress points?	Initially, all internet ingress to the Commonwealth's Applications and Data is to be delivered to the Offeror's datacenters via the Commonwealth's private data network (COPANET). However, as a future option, the Commonwealth may desire to have direct access between the users and the datacenter.
15.□	Appendix A	6(g)	10	Does DC adjacency FROR extend to virtual conditions like a shared mainframe?	Please clarify the question so that the Commonwealth may respond. What is meant by adjacency?
16.□	Appendix A	6 (c)	5	In a scenario where the Commonwealth decides to "in source or re-procure any or all of the services", what is the process for termination of such services?	Refer to Section 32 (Termination) of Appendix A.
17.□	Appendix A	6 (g)	6	Please be aware that in many cases Service Providers cannot provide client names that may share environments due to security and contractual related issues. As a result, please explain in what circumstance the Commonwealth would not approve a third-party proposed to share the data processing environment.	Section 6(g) of Appendix A provides detail on this topic. Objections to the terms and conditions set forth in Appendix A may be made according to Part II-8 of the RFP.

Addendum 3 - Round 1, Part 1					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
18.	Appendix A	6 (i)	6	Is the Commonwealth requesting that the Contractor provide remote access to the hosted services or provide remote access as a service to enable Commonwealth personnel access to their internal networks (hosted or offices)?	The Commonwealth is requiring the ability for secure remote access to hosted systems for operational and administration purposes for designated personnel. The Commonwealth currently has VPN services hosted by Verizon as part of its Telecom Contract.
19.	Appendix A	6 (d)	5	With respect to a decrease in services, what is the committed baseline of services?	There is no committed baseline.
20.	Appendix A	6 (g)	6	From the point of request for approval, how long will it take the Commonwealth to provide approval?	This question is related to the approval of a new datacenter facility and duration is variable based on many factors. Some of the factors include (but are not limited to) a review of the SSA16 audit reviews, Security policies and architecture, networking policies and architecture, and subcontractor approvals.
21.	Appendix A	6 (k)	7	Has the Commonwealth had audits to determine where exposures and current non-compliance with regulations exists? Could results be shared with vendors?	Yes. No.
22.	Appendix A	7.(a)	8	This section states that the "Contractor shall maintain, replace and upgrade the Contractor Machines at its sole cost and expense." Does this include all technology refreshes? There is a requirement to replace "Commonwealth Machine" at its respective end of life. Will this replacement be at the Commonwealth expense? Does this requirement to replace a system at the "end of life" also apply to the "Contractor Machines" and at the service provider's expense?	Yes, this includes all technology refreshes. No, the Commonwealth will not purchase new machines. The Commonwealth is procuring computing services and will no longer be purchasing equipment. The Commonwealth is procuring computing services. The contractor will be required to purchase machines to provide the Services required by the contract.
23.	Appendix A	7.a.1	8	There does not appear to be a definition in either Appendix A or Schedule A for "Commonwealth Machine". Please define.	A "Commonwealth Machine" is a piece of equipment that is owned or leased by the Commonwealth.
24.	Appendix A	9 (a)	10	Will Offeror have any responsibility for logical access (LDAP, Exchange, Active Directory, etc.)?	~~Exchange as a Service is included within the scope of the RFP but the other services such as LDAP and Active Directory will remain under the Commonwealth's control. However, the selected Offeror must provide the equipment to operate these services.~~
25.	Appendix A	9 (b)	10	The RFP states that the contractor cannot store data outside of the United States. Is it permissible for staff outside of the United States to access Commonwealth data stored in the US?	No, unless approved by the Commonwealth.

Addendum 3 - Round 1, Part 1					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
26.	Appendix A	9 (a)	9	As indicated, the Commonwealth will retain administration of logical and data access security. Does this mean that the Commonwealth retains ID administration on all systems or will just manage the process and expect the Contractor to provide the ID administration service on all supported environments?	The Commonwealth has implemented IBM's Tivoli Identity Manager, SiteMinder and CA Identity Minder to manage the users and applications within some systems**.** However, some agencies require the Offeror to manage the System level IDs based on the application owner's needs.
27.	Appendix A	9 (d)	10	Requirements in section 9 (d) are in conflict with requirements in section 42 (d). Assuming that direction in 9 (d) prevails, can you please elaborate on the term "appropriately authenticated", and provide information regarding encryption tools the Commonwealth would use to read the encrypted data?	The requirements of Section 9(d) are more specific than those in Section 42(d) and must be followed. The Commonwealth will determine the appropriate encryption method.
28.	Appendix A	9. (a)	10	Please confirm that the Commonwealth will "retain administration of logical and data access security".	This depends on the service being acquired from the agency.
29.	Appendix A	10 (c)	12	In an "enterprise-wide" survey, will the survey include all end-users of Commonwealth systems?	No, the survey will include only the application owners and key management.
30.	Appendix A	13 (b) (3)	17	How does cost and expenses defined in this section differ from costs and expenses referenced in section 13 (d)?	Section 13 (d) details that funds from the "Reserve Account" are intended for capital improvements or major repairs to the EDC. These projects support or improve the property or facility and will remain after this contract has terminated. Section 13(b) addresses expenses for all maintenance, security and upkeep of the property under the contractor's control.
31.	Appendix A	12 (d)	15	Certain types of requirements can have an impact to the solution including requirements for physical separation and caged environments. Please provide Agency specific security requirements.	Agency specific security requirements are set forth in the RFP, including but not limited to the CJIS and CHIRA documentation.
32.	Appendix A	13(a)(1)	16	Will the Commonwealth consider an offer to buy the existing data center and lease it back to the Commonwealth as an integral part of a response to the RFP?	No.
33.	Appendix A	13 (a) (1)	16	Is it a requirement that the vendor upgrade the Enterprise Data Center to a tier 3 equivalence?	No.
34.	Appendix A	12		Given that Section 12 requires Commonwealth approval for any Services performed from or at locations outside the continental United States, and that no Commonwealth approval has yet been provided, should a Contractor assume that all Services must be performed with US-based labor?	Yes, all Services must be performed with US based labor unless approved by the Commonwealth. Offerors must submit proposals in accordance with the RFP requirements including Appendix A. Objections to the terms and conditions set forth in Appendix A may be made according to Part II-8 of the RFP. Appendix D
35.	Appendix A	12(b)	14	Why is the Commonwealth not requiring the data centers to be located within the Commonwealth of Pennsylvania, thereby securing the jobs and tax revenue for the Commonwealth?	The Commonwealth requires a minimum of one datacenter be located within the Commonwealth of PA – the Enterprise Data Center. To receive the best possible pricing, the Commonwealth is providing the option for Offerors to use their existing datacenters if they choose.

Addendum 3 - Round 1, Part 1					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
36.	Appendix A	12 (d)	15	Commonwealth references DOD 5200.28-STD. This regulation has been superseded by DODI 8500.01 - is this acceptable to reference 8500.01 instead?	The most current standard applies.
37.	Appendix A	12 (d3)	16	Will agencies be required to perform data classifications and communicate that information in order for the Offeror to know what compliance and audit standards they must meet?	Yes – the Commonwealth expects the Offeror to determine this during transition planning in cooperation with the application/data owner.
38.	Appendix A	14 (a) (2)	19	Non-disruptive transitions are technically possible, but extremely costly. Will the Commonwealth consider some degree of downtime associated with transition that minimally impacts the business in order to contain costs?	Yes, the Commonwealth will consider a minimal amount of downtime during transition on a case-by-case basis.
39.	Appendix A	13.b.1	17	Will Offeror be responsible for paying for rent, utilities, etc for the EDC facility?	Refer to Section 13 (Conditions of Contractor's Occupancy of Commonwealth Provided Real Property) of Appendix A.
40.	Appendix A	15 Disaster Recovery and Business Continuity	23	Appendix A requires a DR plan every six months. Could you please reconcile this with the Schedule F requirements as requested in the next question (#3)?	Appendix A states: "Jointly with the Commonwealth, Contractor shall at least annually review and update the disaster recovery plan." It does not require a DR plan every six months. It does, however require that the plan be tested every six months. Frequency of DR exercises will be at the discretion of the Commonwealth.
41.	Appendix A	17 (c)	25	This section refers to the role of Contractor Services Location Manager; however, this position is not defined in schedule G Staffing Plan and Key Positions. Is this a key role?	No.
42.	Appendix A	20	29	Can you please clarify when the monthly invoices are due to the Commonwealth? Within the RFP documents, the invoicing section states the 15th of the month that is being invoiced. However within the SL credits section, there is reference that the invoice is provided to Commonwealth the month following (invoice in September for August monthly Services).	Invoices are due no later than the 15th of the month following the service provided. As described in the example, the invoice will be delivered no later than September 15th for services provided during August.
43.	Appendix A	23.c,d	Page 31	Please clarify the difference between the 2 clauses other than the addition of "liquidated" in line 4 of 23.c?	Please clarify the question. Objections to the terms and conditions set forth in Appendix A may be made according to Part II-8 of the RFP.
44.	Appendix A	33.d.ii	48	If the Service Provider has employment contracts in place with its employees, compliance with this section may not be possible. Given this, has the Commonwealth negotiated these terms with other vendors to reflect existing employment contracts?	Objections to the terms and conditions set forth in Appendix A may be made according to Part II-8 of the RFP.
45.	Appendix A	43a	67	Is there a requirement for encryption of all data?	Not all data - only data which requires encryption by IT policy, law, or other requirement of RFP.
46.	Appendix A	43 (a)	67	Does the phrase "appropriate encryption technologies" infer that a data classification exercise will take place in advance of actually enabling encryption?	Yes – the Commonwealth expects the Offeror to determine this during transition planning in cooperation with the application/data owner.

Addendum 3 - Round 1, Part 1					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
47.	Appendix A	45(a),(1)	68-69	This section states that "Approved Subcontractors" must provide insurance as described in this section. Please confirm that this requirement also applies to all "Small Disadvantaged Businesses" that will all be listed as "Approved Subcontractors".	Confirmed. The insurance requirements apply to all subcontractors, including Small Diverse Businesses.
48.	Appendix A Contract Terms and Conditions	1(b) Contract Term	1	Document states that the three option years pricing is "to be negotiated but consistent with and no less favorable than the pricing in force at the date of the renewal". Does this mean no price required now for the option years? Language implies pricing will be provided later at end of base contract.	Offerors must provide prices for the option years as part of their proposals. Refer to Schedule I (Offeror Pricing Forms).
49.	Appendix A Exhibit D.7	13(b)	16-18	What are the DR configurations and locations for machines in the EDC?	There are no DR configurations within the EDC. However, there are DR facilities in Selinsgrove, Wyomissing, and Scranton that will be decommissioned with the full implementation of this RFP and resulting agreement.
50.	Appendix A Exhibit D.7	13(b)	16-18	Is the EDC capable of supporting water-cooled machines?	Yes, the EDC is capable of supporting water-cooled machines but is not configured to do so at this time.
51.	Appendix A Schedule F	12(a) 2.3.1 3.1.1(3)	14 8 14	Under what conditions can the Offerors make use of the existing Data Powerhouse facility for any class of services? Can it be combined with the EDC to be considered a single facility for purposes of separation?	Offerors cannot make use of the existing Data Power House facility.
52.	Asset list	Exhibit B.1	1	Reviewing the Exhibit B.1 Asset list – multiple agencies are listed – is this an all-inclusive list? Will OA's assets be a part of the data center migration?	Exhibit B.1 is only a list of DPH assets. No assets on that exhibit will be transferred only the applications will be migrated
53.	Defined Terms	Schedule A	All	There are terms in the RFP, Schedules and Appendices that have capitalized words; however, they are not included in the Schedule A Defined Terms. When do you expect these capitalized words to be defined?	Please provide specific references to the undefined terms.
54.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			What is the warranty of the roof and are the warranties conditions being maintained?	15 Years, Yes

Addendum 3 - Round 1, Part 1					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
55.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			What is the open elevation of the access floor (height between the concrete slab and the bottom of the access panels?	2 feet
56.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Electrical			What is the make, year of manufacture, type of fuel system, and emissions tier level of the generator?	2000kw, 3516C Diesel engine, CAT SR4B 2009, Tier 2
57.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			What is the electrical demand for each UPS by month for the last 12 months?	**2012** / **UPS A KVA** / **UPS B KVA** Jan 286 199 Feb 285 200 March 286 206 April 292 206 May 297 217 June 299 220 July 299 222 Aug 305 228 Sept 313 233 Oct 319 239 Nov 331 253 Dec 335 256
58.	EDC tour	Tour handout		HVAC … 325 tons listed in tour handout; 275 listed in RFP materials. Which is correct?	325 tons

Addendum 3 - Round 1, Part 1					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
59.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			What is the capacity of the CRAC equipment located in the UPS room (tons or Watts)?	60 tons
60.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			What is the weight limit of the access panels for the access flooring?	800 lbs. per tile
61.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			What type of battery monitoring system is installed?	Batteries are PM monthly, monitored only with UPS alerts through BMS
62.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			Can access to the building / parking lot be restricted?	Building access is controlled with a card access security system. In addition there is fingerprint (biometric) access to selected areas of the EDC. Parking lot is a shared Commonwealth lot for four Commonwealth buildings. The Offeror must provide more details before the Commonwealth can comment on specific restrictions to the building and parking lot.
63.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			What changes / modifications have been made to the Fire Control / Decoction System	Cheetah xi Addressable Fire Suppression Control System installed 2006

Addendum 3 - Round 1, Part 1					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
64.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			Could the Commonwealth provide the actual tons installed for each area of the data center	Computer Room 1, 225 tons Computer Room 2, 100 tons
65.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			What is the method for fuel spill containment at the facility?	Double-walled underbelly fuel tanks
66.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			What is the capacity of the fuel storage system?	Each of the two generators is equipped with a 6000 gal. underbelly tank
67.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			Could the Commonwealth describe the electrical distribution of the power from the UPS to the PDUs / RPPs?	Even numbered PDUs align to UPSB Odd numbered PDUs align to UPSA RDC 1 powered by PDUs 4 & 10 RDC 2 powered by PDUs 11 & 12 RDC 3 powered by PDUs 13 & 14 Each PDU has a Static Switch.
68.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			For the ASCO transfer switch in the warehouse space; what equipment feeds it and what equipment does it support?	Fed from two main bus panels; supports the entire building excluding the computer room

Addendum 3 - Round 1, Part 1					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
69.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			What types of smoke detection devices are installed?	Fike thermal, photoelectric, ionization
70.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Mechanical			What is type of heat exchange system used?	Freon direct expansion; all Liebert equipment
71.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			What is the source of fresh water for the site?	Harrisburg Water Authority
72.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			Is there an air contamination monitoring system installed?	Yes, in the Battery Room
73.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Fire System			Where in the facility are the Halon storage tanks?	In the mechanical room in the warehouse.

Addendum 3 - Round 1, Part 1					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
74.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			What is the age of the building roof?	Installed June 2010.
75.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			What type of leak detection is provided?	Local to each CRAC
76.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			Describe how the electrical system is distributed to the mechanical systems (CRAC units / condenser units)?	Main distribution panel feeds subpanels feeds condenser units; Main distribution panel feeds CRAC
77.	EDC tour	Tour		Is electrical/mechanical maintenance and project work done by union labor?	Maintenance, no Project, yes
78.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			What remote monitoring or access (control) is in operation for the electrical system?	Monitored through the BMS, Johnson Control System
79.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			Are the CRAC units controlled by the BMS system or is monitoring only provided?	Monitoring only but cycles on through BMS if power interruption detected

Addendum 3 - Round 1, Part 1					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
80.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			Is there a regular maintenance schedule for cleaning under the access floor? If yes, what is the schedule?	No
81.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			For the UPS power: is there a diagram of the power distribution at the device (IT equipment) level? Can this diagram be provided for review?	No
82.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			Is the leak detection system connected to the BMS system?	No
83.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			Are there any overhead water, drain or condensate pipes or sprinkler heads located in the data centers or UPS room?	No
84.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			Is there a wet / pre-action Sprinkler system installed? If yes, which one and in what areas?	No
85.	EDC tour	Tour		Have there been any site failures (power, cooling, infrastructure) since new electrical building was completed and brought on-line?	No

Addendum 3 - Round 1, Part 1					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
86.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			Does an electrical single line drawing exist for the facility showing the utility and electrical distribution of the site? If yes, can the Commonwealth provide a copy?	No single line drawing exists.
87.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			Has the water been tested for hardness, minerals, turbidity, etc? Can the report be provided for review?	No testing has been conducted. No report exists.
88.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			What is the method of fresh air make-up for the data centers? What is the percentage of air exchange for fresh air?	None
89.	EDC tour			You indicated that the new electrical building was added in 2009. During that process was the site ever evaluated against the UTI Tiering criteria? If so, did an independent EE/ME firm do the evaluation? If so, what is the name of the firm and their address?	None of the EDC facilities were evaluated against UTI criteria.
90.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			How is the water treated before use on the site?	Not known.
91.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			What is the fire rating of the data center space (1 hr, 2 hr, 3 hr or none)?	Not known.

Addendum 3 - Round 1, Part 1					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
92.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			Is there a drawing of the building mechanical systems, including the fresh air make-up equipment? Can the drawing be provided for review?	The Commonwealth has as-built prints only. This document is confidential. To receive a copy, please contact Sheryl Kimport, Issuing Officer.
93.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			What year was the Halon system installed?	Original to EDC, approximately 21 years
94.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			How is condensate water removed from the data center?	Pumped into drain system to sanitary sewer
95.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			What is the operating demand loads in the generators during operational (loaded) testing?	Quarterly Load bank tested approximately 1000 kw.

Addendum 3 - Round 1, Part 1					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
96.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			What is the demand load for each of the metered PDU's?	Racks not equipped with metered PDUs. Approximate output kva for computer room PDUs: PDU1 47 kva PDU2 39 kva PDU3 44 kva PDU4 52 kva PDU5 29 kva PDU6 46 kva PDU7 46 kva PDU8 36 kva PDU9 42 kva PDU10 17 kva PDU11 98 kva PDU12 51 kva PDU13 39 kva PDU14 43 kva
97.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			Does the access floor height change in any off data center spaces?	Raised floor exists only in data center.
98.	EDC tour	tour		How long are CCTV security tapes kept on-site and off-site?	Recorder kept on site approximately 4 months

Addendum 3 - Round 1, Part 1					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
99.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			What is the monthly electrical demand loads for the facility by utility feed and by month?	Secondary Utility Feed shows no usage last year. Primary Utility Feed **Billing Month** / **Usage (kwh)** / **Max Demand (kw)** Nov-12 747,750 1,182 Oct-12 867,000 1,137 Sep-12 818,250 1,250 Aug-12 745,500 1,190 Jul-12 771,750 1,197 Jun-12 810,000 1,187 May-12 707,250 1,146 Apr-12 717,000 1,135 Mar-12 689,250 1,100 Feb-12 750,000 1,079 Jan-12 689,250 1,083 Dec-11 708,000 1,091 Nov-11 759,000 1,060
100.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			Is the fuel storage system shared or separate?	Separate
101.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			What is the method for humidity control in the data center?	Set individually by CRAC units

Addendum 3 - Round 1, Part 1					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
102.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			For the two Emerson static switch PDUs located in the warehouse, where are these devices fed from and what devices / equipment do they feed?	St Sw 13 & StSw 14 feed PDUs 13 & 14 respectively. Both static switches are fed redundantly from Switchboard #1A (UPS B) and Switchboard #2 (UPS A)
103.	EDC tour	Tour		Can the Commonwealth provide a copy of the most recent data center audit or assessment? (e.g., SAS 70, SSAE 16)	The EDC is the only in scope Datacenter for this procurement and no SSAE 16 Audit has been completed. Therefore there is no audit to provide.
104.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			Is a drawing available documenting the electrical distribution to the mechanical systems available? Can it be provided for review?	The only prints available are the prints used to construct the facility in 1992. There has been no update made. These documents are confidential. To receive a copy, please contact Sheryl Kimport, Issuing Officer.
105.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			Is there a drawing showing the redundant utility feed installations? Can this drawing be provided for review?	The only prints available are the prints used to construct the facility in 1992. There has been no update made. These documents are confidential. To receive a copy, please contact Sheryl Kimport, Issuing Officer.
106.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			In the perimeter "proposed" expansion areas, what is the construction of the flooring (i.e. slab on grade? some access floor, etc.?	There are no perimeter “proposed” expansion areas identified in Exhibit D.7
107.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			What is the structural weight loading for the concrete slabs in these areas?	There are no perimeter “proposed” expansion areas identified in Exhibit D.7
108.	EDC tour	tour		Are the CCTV video feeds monitored 7x24x365 by eyes on? Does that occur within the building?	This information is considered confidential. The selected Offeror is to provide security to the EDC as part of the contract.

Addendum 3 - Round 1, Part 1					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
109.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			What is the warranty on the C& D batteries (years remaining)?	Unsure of warranty. Approximately 17 years remaining on 20 year service life batteries
110.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			Is there a vapor barrier integrated into the data center walls? Ceiling? Concrete flooring?	Walls-no; Ceiling-no; Floor-6 mil
111.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			Is the building floor slab sealed?	Yes
112.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			Is the fire control / monitoring system connected to a central station and BMS?	Yes to a central station and Capital Police
113.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			Is there attic stock available of ceiling tiles for use in the data center? If yes, how many panels?	Yes, unknown count.

Addendum 3 - Round 1, Part 1					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
114.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			Is there an attic stock of access floor panels (uncut) available for use / replacement in the data center? If yes, how many panels?	Yes, approximately 80 tiles
115.	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			Is there a warranty/ service agreement in place for the mechanical systems? Has it been in continuous service since the initial equipment installation?	Yes. Yes.
116.	Exhibit B.1			Is zVM - zVSE included in the scope as depicted in Exhibit B1 Mainframes - IBM?	Yes
117.	Exhibit B.1			Do the MIPS for zLinux environment in the pricing matrix map to Exhibit B1 Mainframes - IBM?	Yes, Line #'s 21 - 96
118.	Exhibit B.2 DPH - Commonwealth Owned DPH IT A V1 Exhibit B.5 DPT - DPH Agency Disaster Recovery V1 Exhibit D.1 EDC - Server Inventory V1 Exhibit D.5 EDC - DOT Datacenter Inventory V1 Exhibit G.1 PSP - Datacenter HW Inventory V1			For the Mid-Range and x86 servers, can the Commonwealth please provide the processor type and speed for the exhibits?	All available Commonwealth info is contained in exhibits.
119.	Exhibit B.5 DPH Agency Disaster Recovery	"DPH BCP Agencies" Tab	Page1,Line # 3-12	For the dedicated DR equipment located at SunGard in Philadelphia, please identify who will own these machines at the end of the current contract?	The Commonwealth does not know who currently has title to the equipment at SunGard. The Commonwealth does not have title to any equipment at SunGard.

Addendum 3 - Round 1, Part 1					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
120.□	Exhibit D.1	MS and MSL	Virtual=TRUE	There are some virtual machines with high memory (16GB+). Does the Commonwealth have an expectation of the maximum amount of CPU and Memory permitted for an On Demand Server Service (Cloud)? For example, max=16GB, or Max=64GB? 8vCPU? Please provide expected min/max configuration for cloud virtualization.	The Commonwealth has no expectations related to the maximum amount of CPU and Memory permitted for an On Demand Server Service (Cloud).
121.□	Exhibit d.x edc	EDC Facility Summary		What is the diesel fuel storage capacity of the generators … belly tanks local to each gen? Is there shared fuel storage between the tanks? Is the fuel polished?	6000 gallons. No shared storage. Yes
122.□	Exhibit d.x edc	EDC Facility Summary		What is the age of the UPS, electrical switch gear, gens, and battery bank?	All were installed in 2010.
123.□	Exhibit d.x edc	EDC Facility Summary		redundant HVAC cooling … 275 tons. Does this imply that you are 2N or N+1 in cooling capacity? IS each CRAC isolatable so that it can be taken offline?	N+1 for maintenance Each CRAC is isolatable
124.□	Exhibit d.x edc	EDC Facility Summary		Are the valves in the cooling system concurrently maintainable without the need to diminish service to the critical load? Does the redundancy extend to the piping systems?	No, maintenance to valves requires condenser shutdown which reduces cooling capacity. No.
125.□	Exhibit d.x edc			Is there a specific location set aside for contractor installed electrical distribution panel and meters?	No, Offeror will be required to work with Commonwealth building manager.
126.□	Exhibit d.x edc	EDC Facility Summary		Is the BMS physically monitored 24x7x365 locally within the building? If remote … where does this occur?	This information is considered confidential. The selected Offeror is to provide security to the EDC as part of the contract.
127.□	Exhibit d.x edc	EDC Facility Summary		How many diesel vendors are under contract? What is the delivery SLA and priority vs. their other clients? What are the distances from the fuel depot to EDC for each contractor?	Varies with number listed on state contract. EDC has agreement with one vendor to deliver within 5 hours after notification of any emergency. Current vendor is less than 20 miles
128.□	Exhibit d.x edc	EDC Facility Summary		How often are the gens tested? Does this test include running the critical load off the gens?	Weekly. Test does not include running critical load off gen. Load bank tested quarterly.
129.□	Exhibit d.x edc	EDC Facility Summary		Is it standard that all components of the critical load (servers, switches, storage units, etc.) have dual power supplies?	Yes.
130.□	Exhibit d.x edc	EDC Facility Summary		If the above is affirmative, does each power supply run back to independent PDUs (in rack and on RF) and independent UPS/Gens also? We'd like to confirm that redundant implies a 2N power train all the way thru the electrical system.	Yes, redundant implies a 2N power train all the way thru the electrical system.

Addendum 3 - Round 1, Part 1					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
131.	Exhibit d.x edc	EDC Facility Summary		Do the generators service the critical and essential systems? Do they service any other systems in the building (emergency lighting, building water pumping, etc.)	Yes. The entire building is serviced by the generators.
132.	Exhibit G.5			The architecture shows PSP having its own Private Cloud. Please comment on this, and moving forward if the PSP requires separate infrastructure from the general COPA infrastructure. Are other technologies (such as POD separation) acceptable if the PSP can be wall and separated? Are there any other Agencies that require such special handling regarding technical architecture (Private vs. Public, vs. Hybrid). Or, was it just a matter of expediency of history that PSP maintained its own Private Cloud?	PSP requires a design that is compliant with the FBI's CJIS Security Policy. The diagrams included with the Summary of CJIS Requirements are shown as examples of how data at rest and in transit needs to be protected. Yes, there are additional agencies that require "special handling" as defined with the RFP.
133.	Exhibit J.1,	Maturity Level	Page 8	"The Provider is obliged to obtain a Statement on Auditing Standards No. 70 (SAS 70) II certification for the Services provided under this Agreement." SAS 70 certification has been replaced with SSAE 16. Is the Commonwealth looking for SAS 70 II or SSAE 16?	SSAE 16.
134	Exhibit L - Schedule F -	3.3.2.2	152	Does the Commonwealth expect the Offeror to perform Baseline Security Risk and Vulnerability Assessment on all or just a sub-set of applications in-scope (as detailed in Exhibit L) for the Security Transition Services described in Schedule F? Please provide the list of applications that are in scope for the security assessment.	~~The Offeror must perform Baseline Security Risk and Vulnerability Assessments on infrastructure only.~~ ~~Security at OS level is performed by the Commonwealth. Commonwealth~~
135.	exhibit n	Penndot		What form of network redundancy standards are built into the servers?	Redundancy is dependent on business requirements. IES ERP network within the DPH is fully redundant.
136.	General	All	All	Other than the "On-Demand" optional services for Database support and application load testing, please confirm that there are no other application services (like application design, application development, application performance, and or application maintenance) within the scope of this RFP.	Items within the scope of this procurement is limited to managed infrastructure services, database management/design services, Software as a Service, and technical personnel that are related to the other services.
137.	General			Will the Commonwealth provide a financial base case of current spending?	No – the Commonwealth will not provide the current budget or spend on the services included within this procurement.
138.	General	General	General	Please clarify if the Commonwealth will own the Data Powerhouse assets at the end of the Unisys contract or if Unisys will own the assets.	The assets will not be transferred to the new contractor. Most Data Powerhouse equipment is provided as a service. The Commonwealth has title (or lease) to very little of the equipment within the Data Powerhouse.
139.	General	All	All	Who is responsible for debugging and troubleshooting 3rd party software products (including Microsoft O/S products) and Commonwealth application software, the Commonwealth or the Service Provider? If it is the Service Provider, who is financially responsible for this same work?	The Commonwealth is procuring managed services within this RFP. Therefore, the Offeror is responsible for the Hardware, network, and Operating System for all services. Troubleshooting of all Offeror provided infrastructure is the responsibilities of the Offeror (including O/S in all cases). However, software and applications provided by the Commonwealth are the Commonwealth's responsibility to troubleshoot.

Addendum 3 - Round 1, Part 1					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
140.	General	General	General	Please confirm who will be responsible for directory services (AD, LDAP and NDS, etc.)?	The Commonwealth is responsible for the listed services.
141.	General	N/A	N/A	Is there a lab environment existing today to test applications before deployment?	There is no specific lab environment. Each agency / application may have a "Lab" established for their use.
142.	General	General	N/A	Is it permissible for Bidders to submit documents not available in Microsoft Office format in Adobe PDF format only (e.g., audited financial statements, insurance documentation, etc.)?	Yes.
143.	General Information	Exhibit B.1	1	What special consideration, if any, is being given to how geospatial services, content, data and applications are managed as a part of the project?	The Commonwealth hosts these services within the infrastructure listed. The data and applications are managed by the Commonwealth and are not within the scope of this procurement.
144.	Request for Proposal			Who is allowed to use co-location services? Exactly what services are to be provided to those co-locating?	Any Commonwealth agency is allowed to use co-location services. There is existing infrastructure owned by the Commonwealth that may remain in co-location until the infrastructure is to be refreshed. The Commonwealth owned infrastructure is required to be retired and the applications/software utilizing that infrastructure it to be moved to a managed service. The Commonwealth has a need to provide co-location services to 3rd parties as part of the services provided to/from the Commonwealth. This service will remain within the co-location service. The Commonwealth is to provide no new infrastructure into co-location services. Specific services are detailed within the RFP and include physical separation and security, cabinet space, network, cooling, and electrical power.
145.	Request for Proposal			For local Commonwealth access, will co-location facilities need to be located in the Harrisburg, PA area or can they be available anywhere in the continental USA?	Co-location can be located in other datacenters as long as the security of those datacenters meets the Commonwealth's security policies.
146.	Request for Proposal	N/A	N/A	Please confirm that the Commonwealth is looking for a prime service provider to provide all the requested services and that it is unacceptable to submit a partial response or a partial response that selectively picks favorable services and/or resource unit pricing.	Confirmed. It is unacceptable to submit a partial response.
147.	Request for Proposal	Part III III-4	24-25	Will the respondents be required to guarantee their PUE performance claims with a guarantor acceptable to the Commonwealth?	No.

Addendum 3 - Round 1, Part 1					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
148.	Request for Proposal	Part III III-4	24-25	Will those respondents providing an energy performance guarantee have their financial offering adjusted to reflect the real costs of better or poorer energy performance?	No.
149.	Request for Proposal	Part I I-23	7	If substantial savings can be offered by the respondent with a full 10 year commitment from the Commonwealth in lieu of the 7 year commitment with an option to extend to 10 years specified in the RFP, would the Commonwealth be able to accept a 10 year commitment as an alternative offering?	No.
150.	Request for Proposal			Does the Service Provider have any responsibility for hiring displaced Commonwealth staff as a result of this RFP?	No. There is no requirement for the Offeror to hire displaced Commonwealth staff.
151.	Request for Proposal			What if the Commonwealth is unable, for any reason, to fully execute a contract by July 1, 2013? That allows less than 18 months for due diligence and for a vendor to successfully complete the EDC and DPH transitions. Will the Milestone Due Dates and Milestone Credits reflected in Schedule D be adjusted?	Objections to the terms and conditions set forth in Appendix A may be made according to Part II-8 of the RFP.
152.	Request for Proposal			What if through the due diligence process there are changes to scope or mission? Will the Commonwealth allow re-pricing at that time to recognize these changes and adjust the timelines associated with Schedule D?	Refer to Section 27 (Change Control) of Appendix A.
153.	Request for Proposal			Given the size of penalties for missed transition dates, who mediates disputes where delays are caused by the Commonwealth?	Refer to Section 34 (Contract Controversies) of Appendix A.
154.	Request for Proposal	Part III III-4	24-25	Will the Commonwealth add to the selection criteria favorable consideration for locating the data centers in areas which the Commonwealth has identified as economically distressed and in which the Commonwealth has invested millions of tax dollars? If so, how heavily will this be weighted?	The Commonwealth does not disclose detailed evaluation criteria. Offerors should propose their best solution for the Commonwealth to evaluate.
155.	Request for Proposal	Part III III-4	24-25	Will the Commonwealth add to the selection criteria favorable consideration for locating the data centers in facilities in areas which the Commonwealth has invested millions of tax dollars in those specific facilities, thereby securing a return on their investment and securing employment in those facilities in areas they have identified as economically distressed and in which they have invested? If so, how heavily will this be weighted?	The Commonwealth does not disclose detailed evaluation criteria. Offerors should propose their best solution for the Commonwealth to evaluate.
156.	Request for Proposal	Part III III-4	24-25	Will weight be given in the evaluation for energy performance guarantees? If so, how will this be evaluated?	The Commonwealth does not disclose detailed evaluation criteria. Offerors should propose their best solution for the Commonwealth to evaluate.

Addendum 3 - Round 1, Part 1					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
157.	Request for Proposal	Part I I-23	7	The current timing of the transition of services subsequent to the signing of the contract does not allow for the construction of new, highly efficient data centers in which to house the equipment for the provided services. Knowing that the infrastructure and energy costs in a data center account for 60% or more of the overall expense in a data center, and knowing that locating in older, less efficient data centers will ultimately cost the Commonwealth millions of additional dollars in operating expense (as much as $2,300,000 per year or more, for a total of over $16,000,000 over the 7 year life of the contract), will the Commonwealth allow for additional time in the transition of services to enable the successful vendor to build and commission a state of the art facility within the Commonwealth to house the equipment and realize millions of dollars in annual savings to the Commonwealth? If not, why not?	No. Proposals must meet the requirements of the RFP. An Offeror may propose to utilize a new facility at the start of the contract or at a later time during the term of the contract as long as all of the contract requirements are met.

Addendum 4 – Round 1, Part 2					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
1.	Request for Proposal			Can a Service Provider use or hire redundant or excess Commonwealth staff as part of their proposal? To lower overall costs, can a Service Provider make assumptions around work that the Service Provider would assume to be the responsibility of the Commonwealth?	At this juncture the Commonwealth cannot assess the level of impact this procurement may have on existing Commonwealth IT staff. Should an impact ultimately be realized, he Commonwealth expects the Offeror to invite those impacted to apply for job opportunities, grant them interviews and provide them due consideration. No. Offerors should ask questions prior to the proposal due date to eliminate the need to make assumptions.
2.	Request for Proposal			Can a vendor use any of the existing Commonwealth data centers (beyond the EDC) to host some of the applications within scope, especially if there is a financial benefit to the Commonwealth to do so? If allowed, what sites would be available?	No. The only existing location to remain as a hosting site for applications is the EDC. All others will be repurposed.
3.	Request for Proposal			Given the Commonwealth will be providing the fiber link between the vendor data center and their network are SLAs waived if the link has any performance issues that impact categories of SLAs mandated in the RFP?	The Offeror is to provide the data link between the Commonwealth and the Offeror's datacenters. The SLAs apply.

Addendum 4 – Round 1, Part 2					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
4.	Request for Proposal			If a vendor's data center or cloud offering is shared with other non-Commonwealth clients, what physical changes will be required to the facility, if any, to separate the Commonwealth's computing assets from those of other clients? If needed to facilitate an existing public cloud offering, is the Commonwealth willing to sign the public cloud Offerors terms and conditions?	The requirements have been provided within the RFP, including the CJIS, CHRIA, and ITB references. No. See Part II-8 of the RFP.
5.	Request for Proposal Schedule I Offeror Pricing Forms	I-5 Type of Contract Descriptions and Instructions		RFP states: "It is proposed that if the Issuing Office enters into a contract as a result of this RFP, it will be a firm, fixed price contract containing the Contract Terms and Conditions as shown in Appendix A." However, Schedule I states on Descriptions and Instructions tab: "e.) Payment for services under this contract are unit-based. The total units (volume metrics) listed are for informational purposes only and will not be binding on the Commonwealth." Could the Commonwealth clarify whether this will eventually be a fixed annual price committed contract? Are unit rates and volume metrics non-binding only for this first round of the RFP? Will all (or a portion) of the final contract be unit rate based with committed volumes?	The unit prices entered by Offerors on Schedule I will become fixed prices. The total units (volume metrics) in Schedule I are not fixed and are for evaluation purposes only and will not be binding on the Commonwealth. The Commonwealth intends to pay a fixed cost per unit with the units being determined on a consumption-based model.
6.	Request for Proposal			Should the fiber connection be delayed or any other required act by the Commonwealth, what impact does that have on the December 31, 2014 deadline including the $50M penalty?	These would be handled on a case-by-case basis. If the delay is solely caused by the Commonwealth, the Offeror will not be responsible for failing to meet a Milestone. The Fiber Connection is the responsibility of the Offeror to deliver to the Commonwealth within the Milestone due date.
7.	Request for Proposal	I-5	1	The request for a firm fixed price contract appears to conflict with the problem statements goal to provide services on a consumption-based model. Please clarify.	The unit prices entered by Offerors on Schedule I will become fixed prices. The total units (volume metrics) in Schedule I are not fixed and are for evaluation purposes only and will not be binding on the Commonwealth. The Commonwealth intends to pay a fixed cost per unit with the units being determined on a consumption-based model.
8.	Request for Proposal	I-30, B	13	For the requested COSTARS form, please provide direction for how to note that a bidder has already paid (or will continue to pay) the COSTARS Administrative Fees.	The COSTARS administrative fee is paid on a per contract basis. To participate in the COSTARS program, the Offeror must pay the administrative fee for each contract.
9.	Request for Proposal	II-6	19	In the absence of visibility into Commonwealth staffing numbers by role, please provide the number of Commonwealth personnel to be trained?	Offerors must describe their training approach and methodologies. The number of staff to be trained will be dependent on the proposed methods.

Addendum 4 – Round 1, Part 2					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
10.	Request for Proposal	II-8	20	It appears there is conflict between the first and last paragraphs of this section. The first provides an opportunity for the Offeror to identify which of the T&C's in Appendix A they would like to negotiate and which they would like to add to the standard T&C's, whereas the last paragraph states that any proposal that is conditioned on the negotiation of the T&C's (Appendix A) will be rejected. Can you please clarify?	There is no conflict between the paragraphs. An Offeror may identify which, if any, of the terms and conditions contained in Appendix A it would like to negotiate and what additional terms and conditions the Offeror would like to add to the contract terms and conditions. The Commonwealth may, in its sole discretion, accept or reject any of the requested changes. Regardless of any objections set out in its proposal, the Offeror must submit its proposal, including the cost proposal, on the basis of the terms and conditions set out in Appendix A. The Issuing Office will reject any proposal that is conditioned on the negotiation of the terms and conditions set out in Appendix A.
11.	Request for Proposal	Sec. II-8	Page 20	RFP Sec. II-8 states that "The Offeror will identify which, if any, of the terms and conditions (contained in Appendix A) it would like to negotiate and what additional terms and conditions the Offeror would like to add to the standard contract terms and conditions… The Offeror shall not request changes to the other provisions of the RFP, nor shall the Offeror request to completely substitute its own terms and conditions for Appendix A." Given that Appendix A incorporates numerous Schedules of a contractual nature (examples: Schedule D – Transition Milestones; Schedules J1-J3 – Service Level Management), would the Commonwealth please confirm that vendors are authorized to request changes in connection with the Schedules as well?	Offerors may request changes to the Schedules attached to Appendix A in accordance with Part II-8 of the RFP. The Issuing Office will, however, reject any proposal that is conditioned on the negotiation of the terms and conditions set out in Appendix A and its Schedules.
12.	Request for Proposal	II-10 II-8	22 20	It is stated here that "Offerors should not include any assumptions in their cost submittals." Can assumptions be included according to section Part II-8 Objections and Additions to Contract Terms and Conditions of this same document?	No. Offerors should ask questions prior to the proposal due date to eliminate the need to make assumptions. Part II-8 refers to objections and additions to Appendix A.
13.	Request for Proposal	III-4	24	The RFP provides the lists of scoring criteria that will be used to evaluate and award technical proposal points. The Commonwealth has not listed the Service Provider's proposed Work Plan as a section to be scored in their criteria. Is this an oversight?	The Offeror's proposed Work Plan will be evaluated as part of the criteria listed in the RFP.
14.	Request for Proposal	IV-1	29	Is there an actual requirement to replace "the existing DPH" datacenter or can it be used as part of the proposed solution?	The existing DPH may not be used as part of a proposed solution.
15.	Request for Proposal	I-12	Page 33	Since the Commonwealth requires that Vendors submit their response in Microsoft Word format, is it acceptable to include unsigned versions of the documents/forms on the CD copies?	Signed MSWord documents are preferred. If unsigned MSWord documents are submitted, the Offeror must also submit signed PDF versions.
16.	Request for Proposal	1-12 and II	Pages 3 and 17	RFP states: "Offerors shall submit two (2) complete and exact copies of the entire proposal (Technical, Cost and SDB submittals, along with all requested documents) on CD-ROM or Flash drive…" and "three separately sealed submittals." Should Offerors seal 2 requested CD-ROMs or Flash Drives in a separate package as well? Or should Offerors include 2 electronic copies of each submittal sealed with the corresponding hard copies?	Offers should submit the two (2) complete exact copies of their entire proposal on CD-ROM or Flash Drive in a separately sealed package.

Addendum 4 – Round 1, Part 2					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
17.	Request for Proposal Part 1/ Appendix A/	I-23/ Appendix A/Schedule D	1 -1(d)/pg 1	The intro to Schedule D - Transition Milestones, implies billing would occur after milestone completion. However, no transition can begin until the Effective date. RFP I-23 states "the Contract will commence on the Effective Date and will end in seven (7) years." Where is there a transition period if it isn't prior to Effective date? Is it expected that transition and steady state start at the same time?	The transition period cannot start before the Effective Date of the contract. No, it is not expected that transition and steady state start at the same time. The Commonwealth anticipates the transition period will occur before steady state and be part of the seven year contract term.
18.	Request for Proposal Parts I-IVIV	III-4	Page 24	For the Technical evaluation criteria, what is the Commonwealth's established value(s) for each of the five (5) evaluation factors listed: 1. Proposed Facilities 2. Offeror Qualification 3. Personnel Qualifications 4. Soundness of Approach 5. Understanding the Problem What is the value for each of the evaluation factors? Please define the percentage of points for each category?	The Commonwealth does not disclose the value of each evaluation factor.
19.	Schedule	3.2.1.7	57	Is there a master list of CI's and their associated definitions that the state requires to be populated into the CMDB?	No.
20.	Schedule D	All M		In the event a critical Milestone is missed due to a non Offeror delay (State or Agency induced), there could be additional cost incurred by the Offeror as well as missed Milestone penalties and a potential impact to the Transition plan. What would be the proper remediation process between the Commonwealth and the Offeror?	Refer to Section 27 (Change Control) and Section 34 (Contract Controversies) of Appendix A.
21.	Schedule D	M-4	2	Does the Transition Milestone of Due Diligence shown in Schedule D imply that there will be a procedure for adjusting the price of the contract following any discovery?	No.
22.	Schedule F Schedule I			Is the Fully Managed price expected to include hardware refresh?	Yes.
23.	Schedule F			Is there a firm limit placed on the amount of Co-location services to be provided? What is to stop the agencies from using only Co-location?	1. Yes, per Commonwealth policy, co-location is to be used only for 3rd party equipment. 2. Commonwealth policy will dictate the amount and use of Limited Co-Lo Services.

Addendum 4 – Round 1, Part 2					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
24.	Schedule F			No middleware support requirements are set forth in the SOW. There is no middleware within the scope of this RFP?	The Commonwealth does not consider the management of middleware different than application management. The Commonwealth requires middleware support to be part of the service catalog offerings.
25.	Schedule F Schedule I			The SOW requires Capacity on Demand Services for I Series, P Series and Mainframe (IBM and Unisys), yet there are no Volumetrics in Schedule I. Are these services still required?	Yes. The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. Actual volumes will vary.
26.	Schedule F Schedule I			There appear to be differences in server support definitions between the SOW and Schedule I. Schedule I sets forth Fully Managed, Managed Only and Limited Co-Lo. The SOW describes Managed Hosting Services for specific scenarios, such as Windows Support, and Co-location Service Options 1, 2 and 3. Could the Commonwealth please reconcile the two schedules?	The Commonwealth is procuring “Fully Managed”, “Managed Only”, and “Limited Co-Lo” for many scenarios and several technologies. Schedule F (SOW) defines the technologies and scenarios. Schedule I (Offeror Pricing Forms) includes a sample of possible scenarios and will be used for the cost evaluation.
27.	Schedule F Schedule K			What is the contract start date mentioned in the SOW? Is it the same as the Effective Date set forth in Schedule K?	The Effective Date is defined in Appendix A, Paragraph 1. All references to Effective Date and Contract Start Date have that meaning.
28.	Schedule F			Will affected employees of the Commonwealth be made available to the Offeror for hiring? If displaced, does the incumbent supplier have an obligation to make affected employees available for hiring?	At this juncture the Commonwealth cannot assess the level of impact this procurement may have on existing Commonwealth IT staff. Should an impact ultimately be realized, there is no requirement for the Offeror to hire displaced Commonwealth staff. The Commonwealth does expect the Offeror to invite those impacted to apply for job opportunities, grant them interviews and provide them due consideration. (Please note this answer replaces the answer provided for question 150 of Round 1 Part 1 posting.) The Commonwealth has no knowledge of any restrictions on employees of the incumbent contractor that may be displaced.

Addendum 4 – Round 1, Part 2					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
29.	Schedule F	1, Offeror Guidelines	Page 4	Several sections in Schedule F contain tables/matrices with a placeholder for Offeror's response in the last row/cell. a. For ease review and evaluation, is it permissible that Offerors provide their response to each requirement immediately following the requirement? b. To accommodate and ease the use of graphics and tables in Offerors response, are Offerors allowed to provide their response not within a table cell, but outside of the table, as long as the RFP table or table row precede the response?	a. Yes B. Yes, the Offeror must provide the requirement reference number as part of their response.
30.	Schedule F	Requirements #4	14	The Request for Proposal requires the data center proposed to have 99.99% availability over the 6 months prior to December 2011. The award and transition will occur in approximately June of 2013. This creates a platform that is a minimum of 2 years old. This requirement eliminates the opportunity to transition to efficient infrastructure. Will the Commonwealth eliminate this time requirement in order to avail itself of newer, more efficient infrastructure?	The Commonwealth adjusts this requirement to: The Request for Proposal requires the data center proposed to have 99.99% availability over the 6 months prior to December 2012. The Commonwealth is procuring managed computing services not a datacenter. Therefore the Commonwealth is not dictating the age or efficiency of the Offeror's infrastructure as long as the Commonwealth's service requirement and SLA's are met.
31.	Schedule F	#6	14	The schedule states, "Each Data Center will have the capability to provide DR for the other, for the identified critical applications." What level of capability must be included at each data center?	The level of capability will be determined by application and ordered with the desired DR service capability. For each application with DR, there must be another Datacenter with the infrastructure to support the DR service.
32.	Schedule F	3.2.1.1.1	27	Does the Commonwealth have a current Chargeback backup implementation? If so, what is the product?	Currently the Commonwealth uses several chargeback processes. The intent of this procurement is to centralize these into a single product. The current methods use the Microsoft Excel, paper, and the Commonwealth's ESMS system.
33.	Schedule F	3.2.1.1.1	Page 27	How many agencies require chargeback invoices?	All Commonwealth agencies using the services must receive an invoice.

Addendum 4 – Round 1, Part 2					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
34.□	Schedule F	3.2.1.1.1	Page 27	Please describe the level of granularity required for chargeback capability.	Each invoice item must provide the following: •□ Agency name •□ Service Name •□ Service Identifier (i.e. Product number) •□ Unit Price •□ Quantity •□ GL Account Number (7 digits) •□ Department Number (4 alphanumeric characters) •□ Reporting Level (4 digits) •□ Sub-account number (4 digits) •□ SAP Fund number (10 digits) •□ Cost Center number (10 Digits) •□ Percent Allocation (percentage) *(the percent allocation is used if an invoice item is paid across differing Cost Centers.)*
35.□	Schedule F	3.2.1.5.1	52	An estimated 36 month usable life is defined to support a technology refresh. Many data center technologies, such as Storage and Network hardware, have a longer typical life cycle than 36 months. Should the Offeror limit all components to the 36 months or manufacturer's service life?	The Offeror should use its best judgment on the service life of its infrastructure. The Commonwealth is purchasing services that have associated SLA's and the selected Offeror must provide the services within those SLAs.
36.□	Schedule F	3.2.1.5.1 Requirement 1	52	What is the frequency in which the service catalog is required to be refreshed? (i.e. annually, semi-annually, etc?)	The Service Catalog (the total list of services being offered to the Commonwealth) should always remain current and should be refreshed with every change.
37.□	Schedule F	2.3.1	8	In the event a Commonwealth agency doesn't receive Offeror DR services, does their application still need to be replicated between datacenters? Page reference: "The Offeror is expected to implement a multi DR solution to limit the impact of any disruptive event at any datacenter location. This requirement is targeted for all systems that are currently covered by a DR solution."	No.

Addendum 4 – Round 1, Part 2					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
38.	Schedule F	2.3.1	8	Will the Commonwealth allow multiple connections to the Internet including those at EDC? Will the EDC connections to the Internet be decommissioned?	Yes, multiple connections are desired. No the current internet connection will not be disconnected.
39.	Schedule F -	3.3.2.2 & 3.2.2.5 & 3.2.1.1.2 & 3.2.3.1	152-153, 76-78, 30 & 87	We understand that the Commonwealth has EMC-RSA Archer tool licenses managing security compliance information. Can the Offeror leverage the Commonwealth's RSA Archer licenses and existing infrastructure to help track, monitor and maintain the datacenter security compliance?	Commonwealth does have the EMC-RSA Archer tool licenses; however, the vendor must have its own instance that has the ability to connect to or feed into the enterprise system, as needed.
40.	Schedule F	3.2.4.1	94	Currently, EDC provides application support in Managed Services. Are these services in scope of Offeror's responsibility?	Yes.
41.	Schedule F	3.2.4.1	94	Is the Offeror expected to provide hardware load balancing capabilities for the web applications?	Yes.
42.	Schedule F	3.2.1.1.2-2	30	As this relates to Transition, will design approval be needed for each of the 2000+ applications that need to be migrated to a new datacenter? How long will the Commonwealth need to provide such approval?	Yes, design approval is required. The time needed to approve these designs will be based on the complexity of the transition. The approval timeframes will be established as part of the Transition Plan.
43.	Schedule F	3.2.1.1.2	30	In many cases, the Commonwealth RFPs for application development projects request proposers to specify computing infrastructure requirements. How will the Commonwealth insure that future procurements for development services align to the datacenter architecture requested in this RFP?	This is an internal Commonwealth management issue and will be resolved internally.
44.	Schedule F	3.2.1.2	39	Bullet number five states that an incident report must be completed within two days of the incident and the RCA within five days of the incident. What if the incident remains unresolved after two days? Would it be acceptable to submit an incident report within two days of the incident resolution, and the RCA within five days of incident resolution?	The referenced reports must be delivered within the stated interval, and for those that are not resolved, the report must contain an action plan that is to be followed until the situation is resolved to the Commonwealth's satisfaction.
45.	Schedule F	3.2.1.2	39	What is the definition of a "major outage"?	Each service may have a unique definition but the Commonwealth views a major outage in general, as an outage where all or a substantial portion of a service is not functionally usable.
46.	Schedule F	3.2.2.2	64	Does the Commonwealth currently have a way to measure established performance baselines of its applications prior to transition?	The Commonwealth is determining these measurements at this time and will provide the measurements to the selected Offeror as part of transition planning.
47.	Schedule F	3.2.2.2-6	66	As it relates Acceptance Test Plans – Is the Commonwealth developing and benchmarking existing applications for comparison purposes and to insure that such testing works in the current environment?	The Commonwealth is determining these measurements at this time and will be provided to the selected Offeror as part of transition planning.
48.	Schedule F	3.1.2	16	Please confirm that the Offeror can procure telecomm circuits from their vendor of choice if it provides the greatest economical value to the Commonwealth.	Confirmed. T he Offeror can procure telecom services from a company of the Offeror's choice.

Addendum 4 – Round 1, Part 2					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
49.	Schedule F	3.1.2	17	Does the provisioning of private carrier network connections between datacenters satisfy the requirement for "secure connections" Is there a requirement to encrypt all network traffic between datacenters even if data is traversing over private WAN connections?	Yes. A private carrier network connection does satisfy the requirement for a secure connection. No. Not all data must be encrypted. The Offeror must follow the policies and requirements set forth by the Commonwealth relating to data security.
50.	Schedule F	3.3.2.2	153-154	Are your requirements for a security plan met by NIST 800-18's requirements for a system security plan with addendums for Commonwealth additional requirements; along with security activities defined as part of the overall project plan we develop?	Yes.
51.	Schedule F	3.3.2.2	152-153	Are your specific training requirements met by NIST SPs 800-16 and 800-50?	Yes.
52.	Schedule F	3.3.2.2	152	Requirement 1 references a penetration test. Do you conduct the penetration test in a hard or soft manner using non-operational data?	Both as appropriate.
53.	Schedule F	3.3.2 Transition Planning / Governance	142-145	Which agencies can the Offeror transition before Month 30, so that all agencies don't have to be transitioned in parallel? Are there any limitations to transitioning any agencies before Month 30?	The Commonwealth requires all transitions to be completed no later than the end of Month 30. There is no requirement that all transitions occur during Month 30. Offeror is to provide a proposed transition schedule to meet the requirement.
54.	Schedule F	3.3.2	144	While it is clear that DPH operations support will be assumed by the Offeror once the workloads are successfully moved to the new provider's data center environment, it is unclear within the agency data centers at what point that the Offeror should plan to provide operational support for the agency data centers. Should the Offeror provide support starting on day one of the contract in the agency data centers or at a time when the systems are transition to the new data center?	The Agencies will maintain operational support of their datacenters until the applications are transitioned to the Offeror's datacenters.
55.	Schedule F	3.2.1.3	42	(4) Refer: "Establish scheduled maintenance periods, and communicate the scheduled outages. Create a notification process for maintenance, emergency, and unplanned outages. " Confirm that the Offeror must comply with Enterprise Scheduled Maintenance Windows per ITB-NET015 (Enterprise Network Maintenance Scheduling) for maintenances affecting multiple agencies.	The selected Offeror must comply with Enterprise scheduled Maintenance Windows per ITB-NET015. The selected Offeror will be required to comply with all ITBs must be followed.
56.	Schedule F	2.3.3	9	What are the requirements for facilities management at the five (5) COPA datacenters? Should vendors assume that DGS/Commonwealth continues to provide support until transition is completed?	Yes, the Commonwealth will continue to maintain and manage the Commonwealth datacenters until the transitions are completed. With the exception of the EDC, the Offeror will have no responsibilities for those datacenters.
57.	Schedule F	3.2.1.4 Service Desk	44	In paragraph 4 it states that Offeror must provide electronic connection to all of the Agency Help Desks. Please provide a table showing agencies that are not connected to the Enterprise system, which also shows what help desk systems these Agencies use.	The Offeror is only responsible to connect to the OA's Enterprise Remedy.

Addendum 4 – Round 1, Part 2					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
58.	Schedule F	3.2.1.4	44	Who will be entitled to contact the Service Desk?	All Commonwealth Helpdesks, all Commonwealth Application Owners, and all Commonwealth IT Management (both OA and the Agencies) are entitled to contract the Offeror's Service Desk. Commonwealth End Users are not to contract the Offeror's helpdesk.
59.	Schedule F	3.2.1.4	45	In requirement #3 on page 45 please provide clarification: It is stated again that integration with the Enterprise Remedy system and other Agency Help Desks as required. But the last sentence states that integration with other agency ITSM systems is NOT required. Please clarify. If it is required, this section describes a requirement to develop a process and electronic connection to "these agency Help Desks". Other than the agencies using the Commonwealth's Enterprise Remedy System, please provide a list of all other agencies that have a requirement for an electronic connection and please provide the details on the type and brand of help desk software being used by those agencies.	The Commonwealth has several implementation of BMC's Remedy system. The Offeror will interface only with the Enterprise Remedy managed by the Office of Administration. All other Commonwealth Remedy instances will interface with the Enterprise Remedy to escalate incidents and requests to the Offeror.
60.	Schedule F	2.3.4	10	For PII have you conducted a Privacy Threshold Analysis (PTA) or Privacy Impact Assessment (PIA) and is it acceptable to follow Federal guidelines such as FISMA to address this?	1) No. 2) Yes.
61.	Schedule F	2.3.4(2)	11	To what categories of service do DBFW services apply?	DBFW services apply to databases that are considered high risk by the Commonwealth's application owners and CISO.
62.	Schedule F	3.2.4.4	112	Item number three references the Service Management Manual. Is this the same as the Commonwealth Computing Procedures Manual?	Yes. "Service Management Manual" should read "Commonwealth Computing Procedure Manual."
63.	Schedule F	3.2.4	94	Currently, the Commonwealth has Hyper-v for this section in Managed Hosting. Is it a requirement for Managed Hosting to support Hyper-V, or can the Offeror move the application to a different Hypervisor? Throughout this RFP, it is implied the Offeror has discretion on the Architecture. Is Hyper-V a requirement for MH and/or Public/Private Cloud?	Hyper-V is not a requirement for MH and/or Public/Private Cloud. The services provided by the Offeror must be able, however, to support the applications that currently operate on Hyper-V.
64.	Schedule F Exhibit J.2	(All), 3.2.4&5	(All), 133	Regarding IaaS and Managed Hosting, there is no mention of certification requirements, nor specific references in Exhibit J. How import are the following certification for the cloud provider (please rank Critical, Important, Optional: SSAE 16 Audited for SOC1, SOC2, SOC3, PCI Compliant Level 1 Service Provider underlying infrastructure and facilities, and IS0 27001,Information Security Management Systems Certification and Safe Harbor)	Offerors must meet the certification requirements set forth in the RFP.

Addendum 4 – Round 1, Part 2					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
65.□	Schedule F	3.2.2.5 Security Management	76	For the penetration testing, how many IP addresses are in scope? What types of penetration testing (social engineering, wireless assessment, application, etc.) does the Commonwealth seek? For vulnerability analyses, is that considered the same as vulnerability scanning by the Commonwealth?	All of the Commonwealth's IP addresses are in scope. All types. No.
66.□	Schedule F	3.2.2.5	76	Item 1 references a security management plan. Are your requirements for this met by NIST 800-18's requirements for a system security plan with addendums for Commonwealth additional requirements; along with security activities defined as part of the overall project plan we develop?	Yes.
67.□	Schedule F	3.2.2.5-6	78	What form of second factor access control exists today in the EDC?	Client certificates/tokens.
68.□	Schedule F -	3.3.2.2 & 3.2.2.5	152 & 77	We understand that the Commonwealth has licenses for security vulnerability assessment (both application and infrastructure) and secure code review tools. A. Can the Offeror leverage the Commonwealth licenses for security vulnerability assessment and secure code review tools? B. If yes, please provide the list of their licensed security tools for: a. Application security vulnerability testing. b. Infrastructure security vulnerability testing. c. Secure code review.	a.□ No b.□ N/A
69.□	Schedule F	3.2.5 Capacity on Demand Services	133-141	a.□ Does CoPA have difficulty managing peaks and valleys in demand and workload in their test / dev environments? b.□ Is MS Exchange as a service considered in or out of scope? c.□ Can GR resources be utilized for back office functions in our delivery model? d.□ Is CoPA willing to relinquish architectural control in a capacity on demand environment? e.□ Is the target for Image Activation in a capacity on demand environment under 24 hours? f.□ Is CoPA willing to sign up for a minimum baseline? g.□ Is CoPA flexible to change its standardized service request process? h.□ Is CoPA comfortable with the Agencies documenting requirements, but the Offeror defining the technology and service solution against those requirements to optimize across the Data Center? i.□ Is CoPA willing to relinquish control over outage windows and when/ how images are patched for their capacity on demand?	a.□ Yes. ~~b.□ In scope.~~ c.□ Please define "GR resources." d.□ No. The Offeror must propose an architecture and the Commonwealth then will approve or disapprove before implementation. e.□ Yes, the Commonwealth is, however, always looking for the ability to deliver services in a shorter interval. f.□ No. g.□ Yes. h.□ No. The Offeror must propose an architecture and the Commonwealth then will approve or disapprove before implementation. i.□ No
70.□	Schedule F	3.2.1.1.6	36	This section refers to performing a customer satisfaction survey on a quarterly basis. How does the survey differ from the annual survey discussed in appendix A section 10 (c)?	Section 3.2.1.1.6 of Schedule F is specific to the Service Desk and the Offeror must perform quarterly quality surveys of the Service Desk. Appendix A section 10 (c) refers to the entire scope of Service provided by the Offeror.

Addendum 4 – Round 1, Part 2					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
71.	Schedule F	3.2.1.6	56	Item number one indicates that the Offeror must assign a minimum of six dedicated account managers. Key Personnel noted in schedule G that five agency account managers are required. Which is correct?	Five are required as a minimum, but the Offeror may provide as many as are needed.
72.	Schedule F	3.2.2.6 Requirement 6	82	Where an agency will have additional agency-based monitoring tools, will the agency/Commonwealth and vendor mutually agree on a joint responsibility matrix prior to the service addition?	Monitoring tools does not mean that the Commonwealth will manage (and troubleshoot) any infrastructure under the Offeror's control. It only means that the Commonwealth wants visibility into that infrastructure. With that in mind, a responsibility matrix should be developed.
73.	Schedule F	3.2.4.6	123	Item 2 references security training. Are your specific requirements met by NIST SPs 800-16 and 800-50?	Yes.
74.	Schedule F	3.2.4.8	131	Should it be assumed that Co-location Service Option 1 will only be used by current customers of the EDC, and that availability of these services will terminate after all work is migrated to the managed service offering?	No. The Commonwealth expects to have requirements for co-location into the foreseeable future.
75.	Schedule F	2.1, 2.3	6,7	Section 2.1 indicates "*The Offeror must utilize the EDC as one of its datacenters and propose a minimum of one additional datacenter to meet the 2+ architecture requirement"* yet in Section 2.3, it indicates that *Target Datacenter 2: Architecture* indicates the EDC only needs to be included as operations support. One could interpret these two statements as conflicting. Does the EDC need to be included as part of the overarching technology and data center strategy, or is it only required to do ongoing maintenance of the facility and is optional to be included in the new technology direction?	The selected Offeror must assume operational support of the EDC as part of transition and may use the EDC as it sees fit (within the terms of the RFP) to provide services to the Commonwealth.
76.	Schedule F	2.1	5	Will the Commonwealth be establishing a corresponding architectural oversight team or process?	Yes.
77.	Schedule F	2.1	6	*"Applications hosted in the Offeror's datacenters must meet Quality of Service (QoS) requirements as determined by the Commonwealth agency application owners. "* What are the current QoS Requirements of the Agencies? How can the Commonwealth ensure unreasonable demands are not an Offeror's responsibility?	1) QoS requirements are set on a per application/service basis. 2) The Offeror must include within the transition plan a task to determine a baseline for each application. The governance process will be available to address "unreasonable" demands. Also, refer to Section 27 (Change Control) and Section 34 (Contract Controversies) of Appendix A.
78.	Schedule F	2.1	6	How will the Commonwealth ensure agency compliance with the contracted services and associated schedules? (rationalize)	This is an internal Commonwealth management issue and will be resolved internally.
79.	Schedule F	2.1	6	Please provide a copy of the Quality of Services (QoS) requirements as determined by the Commonwealth application owners.	QOS requirements are set on a per application/service basis. The Offeror must include within the Transition plan a task to determine a baseline for each application.

Addendum 4 – Round 1, Part 2					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
80.	Schedule F	2.2	7	Section 2.2 indicates that the Commonwealth has a set of Service Levels proposed? We are unable to locate specific current SLAs that the Commonwealth has today as a baseline, or is requiring as a minimum from the Offeror. Can the Commonwealth elaborate on its baseline requirement?	Schedules J.1, J.2 and J.3 detail the Service Levels required by the Commonwealth.
81.	Schedule F	2.3	7	Do we know what the current levels of service are at all the data centers that are in scope (outside of DPH & EDC)?	No.
82.	Schedule F	3.1	12	Does the Commonwealth have established criteria defined to evaluate new technology offerings? Is it anticipated that new technology offerings will be determined on an enterprise basis instead of an agency basis?	1) The Commonwealth does not have a formalized methodology to evaluate new technology offering. 2) All new technology offerings provided through this procurement will be available to all agencies, even if initially requested by a single agency.
83.	Schedule F	3.1	12	If a study indicates that currently installed capacity is underutilized, will the Commonwealth accept less capacity to reduce costs especially if a physical asset has reached end of service life and will be replaced?	Yes – the Commonwealth wishes to only pay for the service capacity needed and have the ability to increase or decrease as needed.
84.	Schedule F	3.1	13	As far as using outside datacenters to provide additional capacity on demand, other than secure connectivity, are there any other requirements needed for approval?	Yes. The new datacenter must meet all of the requirements of the RFP. If the datacenter Services will be provided by a subcontractor to the Prime, the subcontractor must be approved by the Commonwealth.
85.	Schedule F	3.2	22	The Commonwealth's RFP is heavily guided by ITIL. Please comment on the importance (High, Medium, Low) of the Offeror's datacenter operations (Production and DR) to have their datacenter's services delivery model based on ITIL V3 guidance, and importance of having a majority of ITIL-certified staff.	The Commonwealth does not provide detailed evaluation criteria. The Commonwealth desires all datacenter service delivery models to be based on ITIL V3.
86.	Schedule F	3.3 Transition Services		Are there hardcoded IP addresses within the applications? And if can you provide the list of applications by agency / equipment with hardcoded IP addresses?	There are certain applications that are configured with "hardcoded" IP addresses. This level of detail is considered part of the information that will be provided during transition.
87.	Schedule F	3.3 Transition Services		What provision has OA/OIT made to ensure the cooperation of the agencies with the Offeror during Transition?	These issues will be resolved internally within the Commonwealth.
88.	Schedule F	3.3 Transition Services	141-155	Is there a list of application interactions between agencies that can be provided to the bidders?	No. The Offeror should determine this as a task during Transition Planning.
89.	Schedule F	3.3 Transition Services	141-155	Is there a list of application interactions within agencies that can be provided to the bidders?	No. The Offeror should determine this as a task during Transition Planning.
90.	Schedule F	3.3	Pages 141-152	Where in the proposal should the Offeror provide the draft transition plan?	Schedule M.

Addendum 4 – Round 1, Part 2					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
91.	Schedule H	1.5.1	12	Please provide a definition for Authority Levels for changes to the Agreement.	The Commonwealth is requesting Offerors to describe their change control process. The Commonwealth will work with the selected Offeror to define authority levels within the Commonwealth for change requests.
92.	Schedule H	1.1.3	3	Please provide a list to validate agencies by location.	All agency headquarters are located within the city of Harrisburg, PA. All Commonwealth datacenters within scope of this procurement are within metro Harrisburg, PA, with the exception of the three Disaster Recovery Sites that will be consolidated into this procurement.
93.	Schedule I			Are the DASD requirements Raw or Usable?	The Offeror must be capable of providing both options.
94.	Schedule I	N/A	N/A	As the Commonwealth may be aware, GAAP accounting principles guide many organizations. Similarly, the Commonwealth is driven by budget. The lack of committed baselines could and likely will be interpreted by some as no contractually obligated revenue. As this contract is responsible for infrastructure support for several of the most critical applications in the Commonwealth, it is unrealistic to think of a situation where there would be no baselines required. It is requested that the Commonwealth provide committed baselines as it is expecting significant capital investment by the Offerors.	The Commonwealth will not provide a minimum commitment for this procurement.
95.	Schedule I			The Base Units - Volumetrics sets forth no quantity of physical systems for support of AIX. How is that to be handled?	The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all inclusive representation of every service desired by the Commonwealth. Offerors must respond to Schedule I as presented.
96.	Schedule J	5.1	5	Can you please confirm that each Critical and Key Measurement Service Level will be assigned a percentage whereby if a specific Critical Measurement is missed during a month, then the respective percentage assigned to this Critical Measurement will be used to multiply against the total At Risk amount to determine the amount of the credit due to Commonwealth?	That is not correct. The credit due the Commonwealth for a Service Level Default is defined in Schedule J.2 and is either based on the invoice amount for the impacted service or a fixed amount. The total amount of credits is not to exceed the "At Risk Amount."
97.	Schedule J.1	15	11	How do we manage to SLAs when in a test sequence? Do they still apply or are they held pending the completion of the test run?	If the duration of the Test sequence is defined within an approved infrastructure change request, the SLA's would not apply.
98.	Schedule J.1	5.1	5	A Service Level Credit is defined as 100% of the affected month's invoicing for the service that experienced a Service Level Default. According to the Commonwealth's requirements for invoicing, there is no requirement to break down the invoice by specific service being measured by a Service Level Agreement. Without that level of detail, how can the Service Provider determine the amount of the Service Level Credit?	Invoicing must be detailed by the service provided. This level of detail will be used for SLA Credit calculations.

Addendum 4 – Round 1, Part 2					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
99.	Schedule J.2	SL22	High Risk Security Patch Updates Timeliness	What is considered a high risk?	Each patch is evaluated by the Commonwealth's security teams and assigned a risk level. The patches are then deployed according to the assigned risk level. Please refer to Commonwealth ITB on Desktop and Server Software Patching Policy ITB-SYM006.
100.	Schedule J.2			Will each agency have its own SLAs or will the SLAs be calculated as a whole for the entire contract?	Each individual order item will have a SLA. SLAs must be tracked on an individual orderable item not the contract as a whole.
101.	Schedule J.2	N/A	1-2	Key Measurements (KM's) are target measurements for non-critical service areas and are not eligible for Performance Credits. If so, why does Schedule J2 list Default Remedy Types for all listed KM's?	The credits defined for Key Measurements are established because the SLA change methodology allows the Commonwealth to convert a Key Measurement into a Critical Measurement. The credit is to provide the Offeror with the expected credit should this occur.
102.	Schedule J.2	SL1-8	Various Application Infrastructure Availability	Could the Commonwealth provide application architecture documentation, so the bidder can assess the capability of the applications to meet the desired Service Levels?	No, Commonwealth service levels are not defined by application.
103.	Schedule J.3			The Service Level references Note 2, however, there is no Note 2 at bottom of the document. Will the Commonwealth please clarify?	~~There should not be a reference to Note 2.~~
104.	Schedule J.3	Metric Exclusion for each SLA		There are multiple references to Note 2, which cannot be found in the document.	~~There should not be a reference to Note 2.~~
105.	Schedule J.3	2	5	"Metric Exclusions" states that "all items defined in Note 2 at the bottom of this Schedule J.3." We cannot find Note 2 in this Schedule?	~~There should not be a reference to Note 2.~~
106.	Schedule K	D.02-54	12	Is the request for a backup audit for UNIX systems similar to D-02.39	Yes, one is for windows and one is for Unix
107.	Schedule K	D-02.59	12	Is the request for a backup audit for Mainframe systems similar to D-02.39	Yes, one is for windows and one is for mainframes.
108.	Schedule K	D-01.04, D-01.05, D-01.06	5-6	Should the reference to "Start Up" read "Effective Date"? If not, please define "Start Up".	Yes, "Start Up" should read "Effective Date."
109.	Section F Exhibit G.7	2.1 Application Narrative	5 2	Please comment on the importance (High, Medium, Low) for data center compliance in Production and Disaster Recovery: Facility Clearance Levels (FCL) at "Top Secret" (especially in relation to the PSP CJIS requirement); NIST 800-53rev3 controls at the "Moderate Impact" level for FISMA compliance; NIST 800-37 and NIST 800-53 at a Moderate level; DIACAP audit at the "MAC III" level.	Offerors must meet all of the requirements set forth in the RFP. The Commonwealth does not provide detailed evaluation criteria.

Addendum 4 – Round 1, Part 2					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
110.	Transition Milestones	Schedule D	1	Will consortiums have the ability to leverage multiple data centers to satisfy the Commonwealth business requirements? i.e. if a company specializes in line of business such as Esri GIS and offers data center capabilities focused on that suite of products and platform can that be included as part of a consortium bid to support GIS services, software, hardware, and platform requirements.	Yes, the Offeror and its consortium of subcontractors are encouraged to leverage their combined infrastructure options to provide the best service at the best price to the Commonwealth.

Addendum 7 – Round 1, Part 3					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
1	Schedule F	3.1	12	Please explain the use of the words “like for like” or increased computing capabilities. Please confirm that the Commonwealth is expecting to acquire “like for like” configurations for hardware, software and all technology defined in all of the exhibits. Also please explain how these configurations will be priced and reflected in the Cost tab under “Volumetrics” that appear not to be consistent with the requirements reflected in the exhibits.	"Like-for-like" in this RFP is intended to convey that the services provided by the Offeror must perform at the same level as those being performed today with the Commonwealth's current infrastructure. In some cases, this will require an exact duplication of the infrastructure in place today and in some cases new and more robust architectures will be required The Offeror must determine which configurations require "like-for-like" during transition planning. The configurations and Volumetrics are hypothetical and will be used for cost evaluation only. The pricing will be based on the service catalog provided by the Offeror in Schedule C.
2	Schedule F	3.2.1.5.2	53	Which exhibits provide details regarding Tiered DDR as only Schedule J.1 is referenced.	“DDR” is a typographical error. “DDR” should read “DR” in this section. DR services should be orderable catalog items based on the technology and configuration being offered.
3	Schedule F	3.2.2.2	64	What is the Commonwealth’s definition of “At the direction” and “At its discretion”? During the Transition, Commonwealth participation, especially application support resources will be critical to the program’s success.	”At the direction” indicates that the Offeror must receive Commonwealth approval before transitioning an application. The Commonwealth will assign staff to transition activities per the application owner's “discretion.”
4	Schedule F	3.2.1.4	44	What is the expectation on behalf of the Commonwealth regarding agencies that are not using the Commonwealth's Enterprise Remedy System (ERS)?	Agencies that do not participate in the Commonwealth’s Enterprise Remedy must have the availability to contact the service provider via telephone. Also, the Offeror must accept telephone calls from the Commonwealth for the reporting of incidents in the event the Commonwealth's Remedy system is not available for the caller. When this occurs, the selected Offeror must create an incident ticket that will be updated and sent to the Commonwealth’s Enterprise Remedy for tracking, escalation, SLA, and reporting purposes.

Addendum 7 – Round 1, Part 3					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
5	Schedule H	1.1.3	3	Please provide a list to validate agencies by location.	All agency headquarters and datacenters are located within 12 miles of Harrisburg, PA. Please note, however, the Commonwealth has over 3,200 locations that agency personnel occupy.
6	Schedule J.3	1.3.10	9	Please provide the Targeted Applications to be measured via Service Level Agreements. This was not contained in Schedule J.3	All applications will have a Service Level. The Commonwealth will select the service level category (Platinum, Gold, Silver, etc.).
7	Appendix A	17,(b)	25	Key Positions. This section states that all Key Employees shall be dedicated to the Commonwealth account on a full-time basis. This requirement is in conflict with the requirements specified in Schedule G. Please clarify?	All key employees must be dedicated to the Commonwealth account on a full time basis. Complete Schedule G accordingly.
8	Schedule F	3.2.5	133	In a cloud IaaS solution, particularly for Server Capacity, but in general, how important is available APIs to the Commonwealth? Can you rate as Critical, Important, or Optional?	All of the RFP requirements are important to the Commonwealth. The Commonwealth does not disclose detailed evaluation criteria.
9	Request for Proposal			If a vendor's data center or cloud offering is shared with other non-Commonwealth clients, can any of the computer hardware, storage devices or other IT infrastructure be shared with a non-Commonwealth client in order to help reduce costs?	As part of the Transition Process, this will be determined on an application by application basis.
10	Schedule H	1.2.3	4	To ensure that interim procedures align to current, please provide a current Joint Responsibility Matrix (JRM) of Performance Management Procedures on file.	Because the Commonwealth does not operate a majority of the datacenters jointly with a contractor, a Joint Responsibility Matrix is not available to provide.
11	Schedule H	1.2.4	5	To ensure that interim procedures align to current, please provide a current Joint Responsibility Matrix (JRM) for Financial Management Procedures.	Because the Commonwealth does not operate a majority of the datacenters jointly with a contractor, a Joint Responsibility Matrix is not available to provide.
12	Schedule H	1.2.5	5	To ensure that interim procedures align to current, please provide a current Joint Responsibility Matrix (JRM) of Contract Management Procedures.	Because the Commonwealth does not operate a majority of the datacenters jointly with a contractor, a Joint Responsibility Matrix is not available to provide.

Addendum 7 – Round 1, Part 3					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
13	General	All	All	What application performance requirements are included in the bid? In other words, other than the requirement to provide "like for like" infrastructure based on the exhibits are there any other performance requirements like benchmarks, etc.? If performance issues are introduced during the migrations of the existing data centers, who will be financially responsible to resolve those issues?	Before migration, the contractor shall work with agencies as part of transition planning to benchmark the applications and the new infrastructure. The Offeror must provide the infrastructure performance desired by the Commonwealth.
14	Schedule F	3.2.1.4	44	What does the acronym CPPM mean in below reference from respective page? It's not identified in Scheduled A (Defined terms). "The Offeror must create and keep current a CPPM that documents the processes, procedures and timelines used to meet the requirements of this contract. The CPPM must provide detailed process descriptions to support the computing needs of the Commonwealth utilizing best practices and be made available (via Offeror's Portal) to all Commonwealth agencies throughout the term of the contract."	CPPM was an incorrect reference. It should be listed as CCPM (Commonwealth Compute Procedure Manual - Schedule H).
15	Schedule F	3.2.5.5		What constitutes "current" software? N, N-1, N-2…?	Current software in this RFP means the software is currently supported by the publisher.
16	Schedule F	2.1	6	High Availability (HA) in the data center design is mentioned multiple times, along with DR. Yet HA is as much of an application design issue as it is a data center/network issue. Are any of the applications today designed for HA and is there a program in place within the Commonwealth to design critical applications for HA? If so, please provide the list of the application programs that are HA enabled?	Currently the Commonwealth has no applications designed for High Availability across multiple datacenters. The Commonwealth desires the infrastructure to readily support HA across datacenters, thus allowing future development for this capability.
17	Schedule F	3.2.1.1.1	27	The requirement for chargeback procedures state that those procedures "will include the ability to map to discrete programs and funding sources identified by agencies with this requirement". Please provide a list of requirements for both a list of those agencies and a list of the discrete programs.	Each invoice item will need to be assigned a specific General Ledger account code for chargeback purposes. This account code will provide the detail required by the Commonwealth.

Addendum 7 – Round 1, Part 3					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
18	Schedule J.3	SL01-SL05	5 thru 9	Hours and Days of Measurement for the five levels of service, basic through platinum, are indicated as 7 x 24 x 365. If all service levels required the same of availability is there a need for five service levels or should the hours of availability vary based on the service level being provided?	Each of the five service levels (SL01-SL05) are the same with the exception of the uptime requirement. Please refer to Schedule J.2 for those requirements.
19	Schedule F	3.2.2.4	72	For costing purposes, how many Commonwealth users should Offerors assume will require access to the online DR planning tool?	For purposes of submitting a proposal, Offerors should plan on 10 users requiring access to the DR planning tool. The actual number of users may vary during the contract term.
20	Schedule F	3.1.3 #5		What tiers of DR are required and how are they defined?	For this requirement, the Offeror should provide its approach to establishing tiers that will support the Commonwealth's DR requirements.
21	Schedule J.1	7.1.1	7	If new service levels are determined by the average of previous measurements, would the SLA for a service that has 100% availability for the previous 9 months be established at 100%?	In this specific case, the Service Level would be determined by the Commonwealth and, at the Commonwealth's sole discretion, may be set at 100%.
22	Schedule F	3.2.1.1 #4	24	Does this mean that SLAs beyond those in Schedule J will be created for the contract?	It is possible that SLAs beyond those in Schedule J will be created for the contract.
23	Appendix A	6 (f) Services	6	Does this include maintenance of existing equipment and disposal? If Offeror is responsible for disposal, what are the requirements?	Maintenance of all equipment will be the responsibility of the contractor. Disposal of Commonwealth owned equipment will be the responsibility of the Commonwealth. Disposal of contractor owned equipment will be the responsibility of the contractor.
24	Appendix A	6 (g)	6	If the vendor is proposing a shared facility, will the Commonwealth require a list of current tenants to be used in its evaluation criteria for this proposal? If so, please be aware that in any cases specific client names cannot be shared.	No – the Commonwealth does not require a list of current tenants as part of Offerors' proposals. The Commonwealth reserves the right to request this information during a later stage of the procurement process or during the term of the contract.
25	Schedule K	D-03	16	"Datacenter Technology Roadmap" requires estimated timings and "cost impact to Commonwealth". This implies that the Commonwealth is financially responsible for all technology refreshes. Is that correct?	No, that is not correct. This is a services based procurement and technology refreshes will be the responsibility of the selected Offeror.
26	Schedule F	3.1.2	18	Does the Commonwealth have a list of future application and database requirements that vendors should consider in responding to the requirement for an infrastructure environment that will meet all future data center requirements?	No, the Commonwealth does not have a list of future application and database requirements.

Addendum 7 – Round 1, Part 3					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
27	Appendix A	12(b)	14	Will the Commonwealth amend this Request for Proposal to include a requirement that the facilities be located within the Commonwealth of Pennsylvania?	No.
28	Schedule F	Section 2.1 Section 3.2.3(3)	6 85	Would the Commonwealth accept a lower tier rating for some service classes or categories (e.g. providing co-location from a tier 2 facility.)? If so, what are the minimum tiers for those service levels or categories?	No. The Offeror must provide all datacenter services from a Tier 3 equivalent datacenter
29	Appendix A	79	93	The Commonwealth has stated its requirement for fees to increase or decrease dependent on the volume consumed or variation in scope. Without a committed minimum participation or a long-range forecast of the variability of Commonwealth needs, how can a vendor commit to a fixed and ongoing financial participation to a small diverse business that may be providing these services?	~~Offerors must include a numerical percentage which represents the total percentage of the Total Base Term in the Cost Submittal that the Offeror commits to paying to Small Diverse Businesses (SDBs) as subcontractors. Per section IV of the RFP, the selected contractor's commitments to Small Diverse Businesses made at the time of proposal submittal or contract negotiation shall, to the extent so provided in the commitment, be maintained throughout the term of the contract and through any renewal or extension of the contract~~
30	Schedule F	3.3	141	"Initial transition approach of the Commonwealth's mainframe and SAP environments requires that the results be as close to the Commonwealth's current configurations as technically possible". Since the configurations described in the exhibits are not reflected in Schedule I, (Pricing Forms) is the Commonwealth financially responsible for paying for any gaps to ensure that these configurations meet or exceed current configurations?	~~Offerors must provide a catalog of services, including pricing, that includes sufficient detail to allow the Commonwealth to order the desired configuration(s) required to satisfy the need of the application owner. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all-inclusive representation of every service desired by the Commonwealth.~~
31	Schedule F	3.2.1.8	60	Will Offeror be financially responsible for any Commonwealth-provided software?	Please clarify the question and provide additional detail.
32	Schedule J.3	SL01-SL05		What is the experience or logs for the applications' availability?	Please clarify the question and provide additional detail.

Addendum 7 – Round 1, Part 3					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
33	Appendix D Domestic Workforce Utilization Certification	N/A	2	There are different types of Cloud resources that a Provider could recommend. One type is an "unmanaged" environment. In such an environment: 1) those who administer the base resources do not have root access to the virtual machines; 2) once an instance is provisioned, it becomes the sole responsibility of the Cloud consumer or the provider acting on his/her behalf. In the envisioned scenario, administrators of the base resources could be located in countries outside the U.S. and not part of WTO Government Procurement Agreement. Provisioned instances would be managed only by U.S. resources of the Provider. Would this scenario warrant Maximum Consideration by the Commonwealth? Or would a smaller score be awarded?	Please clarify the question and provide additional detail.
34	Schedule F	3.2.1.8	60	Will Offeror be granted permission to use any available Commonwealth ELAs?	Please define ELA and provide more detail concerning the permission being sought.
35	Appendix A	13 (b) (1)	17	Please define requirements for facility upkeep. For example does this include snow removal, janitorial services, etc.?	Please refer to Exhibit D.7 for those details.
36	Schedule F	3.2.3	85	Requirement 1 appears to be for a report only detailing the facility upgrades needed. Once the facility upgrade report is reviewed and approved by the Commonwealth, who is financially responsible for the costs of the facility upgrades? Will the capital improvement fund mentioned on page 18 of Appendix A be used to fund HVAC and power upgrades at the EDC?	Requirement 1 requires a report be provided. It does not require any changes to the building or datacenter. The Capital Improvement fund defined within Appendix A is available to fund certain building projects as detailed in Appendix A. This process requires the contractor to gain approval from the Commonwealth to use the Capital Improvements funds for a project. If approval is denied, the improvement will be the financial responsibility of the contractor.
37	Schedule G	4	6	Should the position of Sales Manager identified in the table be defined in the section 2 or is this not a required position?	Sales Manager is not a position that is considered "Key" for purposes of Schedule G.
38	Schedule F	2.3.3	10	The services framework graphic notes "Exchange as a Service" as a capacity on-demand/additional service offering. This offering is not described anywhere else in schedule F. Please provide requirements and expectations around this service.	~~Schedule F has been amended and reissued to include requirements.~~

Addendum 7 – Round 1, Part 3					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
39	Schedule I	Tab 3	N/A	Month 26 is missing. Please provide a revised version of the price volume template with this month included in the detail and relevant calculations.	Schedule I has been amended and reissued.
40	Schedule J.3	SL01-SL05		The calculations do not align with the definition of availability since the period of comparison is not the available time; instead the formula suggests that all applications are available 24x7 with no downtime for maintenance. Please clarify.	Scheduled and approved downtime will be deducted from the formula. The ITIL Infrastructure Change Management Procedures must be defined and followed.
41	Schedule	3.2.1.5.1	52	The pricing sheet has no place to enter the cost of the technical refresh. Is it the intention of the Commonwealth to include the technical refresh in the monthly RU? Or is Technical refresh to be considered a Project completed on a time and material basis?	Since the selected Offeror is providing a service, any refreshes are the responsibility of the Offeror and should be part of the rate that is being charged for the service.
42	Schedule F	3.1.3	18	What are the responsibilities of the Offerors for remediating or addressing application latency issues that arise by relocations from the current sites? Please provide a list of applications and a description of the latency problem to which each may be subject.	Some of the applications currently communicate through a shared core switch to minimize latency. The Offeror must provide the same level of network optimization, or better, as exists today. The Offeror must assist the Commonwealth with remediation of issues through analysis of network traffic and server performance. The Commonwealth currently is not experiencing any latency issues and is unable to anticipate which applications might experience latency issue post transition.
43	Schedule G	4	7	Should the position of Sales Support Technical Engineer be defined in section 2 or is this not a required position?	The "Sales Support Technical Engineer" position has been removed from Schedule G. Schedule G has been reissued.
44	Schedule I	1.Volumemetrics	Lines 216-217	Having tape capacity of about 1 times disk space does not conform to industry standards of having tape capacity of about 15 times disk space. Is this what the Commonwealth wants?	The 1 times disk space is the minimum acceptable by the Commonwealth. The Offeror must provide sufficient tape capacity to service the Commonwealth and meet the SLAs.

Addendum 7 – Round 1, Part 3					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
45	Request for Proposal	III-4,C.1	25	Section C describes "Small Diverse Business (SDB) Participation". Section C.1 states that a business submitting a proposal as a prime contractor must perform "60% of the total contract value" to receive points for this criterion under "any" priority ranking. Does the 60% requirement stated in this section only apply to SDB that are priming this opportunity or does the 60% requirement apply to all primes contractors? If this statement applies to all prime contractors, please confirm that no SDB points will be awarded unless the prime contractor directly performs at least 60% of the total contract value of opportunity.	~~The 60% requirement stated in Part III-4 applies to all prime contractors. No SDB points will be awarded to an Offeror unless the company serving as the prime contractor directly performs at least 60% of the total contract value.~~
46	Schedule F Schedule I			The Baseline Units - Volumetics shown in Schedule I do not increase as would be expected upon completion of Transition at Month 30. Why is that?	The Commonwealth cannot accurately estimate changes to the Volumetrics until a transition plan is finalized. The Volumetrics in Schedule I are estimates and will be used for costing evaluation only.
47	Schedule F	3.2.1.1.5	33	Please provide expectations around volumes expected by Additional Planning Services request type.	The Commonwealth cannot estimate volumes for this requirement.
48	Schedule F	3.3.2.1	149	Requirement # 12, states that "the Offeror must ensure that critical applications are not decoupled from key infrastructure components causing system latency." Please provide all agency application dependencies as well as any multi-agency application requirements to avoid system latency issues.	The Commonwealth considers this a transition activity for the selected Offeror to determine during transition planning.
49	Schedule F	3.2.2.5	76	Please provide details regarding the current status of agency compliance with all laws, regulations, and policies as they pertain to each agency.	The Commonwealth continually reviews it compliance against laws and Commonwealth policies.
50	Appendix A	15 (b)	24	What is the Commonwealth's current disaster recovery planning methodology software?	The Commonwealth currently does not have DR software. This requirement exists to ensure the offeror will support any future DR software selected by the Commonwealth.
51	Appendix A	7 (a)	8	Does the Commonwealth define currency as N or N-1?	The Commonwealth defines currency in this reference as the a level of hardware or software that has not been discontinued by the manufactured.

Addendum 7 – Round 1, Part 3					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
52	Schedule F	3.2.5.2		To what systems will this storage be attached? What are the anticipated volumes? What storage in current exhibits will be provided via this mechanism?	The Commonwealth desires the ability to attach any system that is compatible with the storage solution proposed. The storage solution is to be determined by the Offeror. The Commonwealth has not determined the anticipated volumes. No storage in current exhibits will be provided via this mechanism. The Commonwealth currently does not have this capability.
53	Schedule F	3.3 Transition Services	141-155	a. What does the Offeror have to demonstrate that a thorough latency strategy has been executed? What is the expectation relative to Application Discovery? Would CoPA entertain a low end validation tool to confirm manual data on application discovery and dependency mapping? Are there any assumptions CoPA has relative to the methods of migrations (lift/shift, PTV) etc?	The Commonwealth does not have a "latency strategy" documented at this time. The Commonwealth is willing to consider a "low end validation tool" to assist with discovery. However, the "tool" must be approved by the Commonwealth before implementation. The Commonwealth has no assumptions relative to methods of migration, but anticipates multiple methods of migrations to occur.
54	Appendix A	11 (b) (3)	13	Will the Commonwealth provide a gap analysis indicating where noncompliance with federal and state mandated policies exists within the infrastructure vendor is expected to support, or will the vendor be able to assess this during the due diligence period and adjust price accordingly?	The Commonwealth does not have an all-encompassing gap analysis indicating if any "noncompliance" exists. This analysis may occur during the transition planning period; however, the selected Offeror will not have an opportunity to adjust pricing.
55	Schedule F	3.2.1.1.3	Page 45	What is the average count of changes per month, for data center activity?	The Commonwealth does not have an exact count of changes per month. Between all seven in scope datacenters there are between 500 and 1,000 changes every month. Please note that these changes may vary from rather small, such as applying an operating system patch or opening a firewall port, to very large installations of several racks of servers or application updates.
56	Schedule F	2.3	7	Has a set of "available specialized services" been defined? Is it expected that "specialized services" will be built on a demand basis?	The Commonwealth does not understand the intent of this question and the meaning of "built on a demand basis." Please clarify.
57	Schedule K	Multiple	Multiple	In the second column within the tables, several requirements focused on regular reports switch from Effective Date + Number of Days to a reference of Weekly, Monthly, Quarterly. Is the Commonwealth's intension that the Offeror provides the procedure to produce the reports within the CCPM on the identified cycle or have the CCPM updated with requested reports on the identified cycle?	The Commonwealth expects the deliverables to be accomplished per the schedules set forth in Schedule K. If the requirement states that a deliverable must be performed monthly, then the Offeror must produce the deliverable every month. The same applies to the other intervals. The only one-time deliverables listed within Schedule K are those with a date or a single interval such as "Effective Date + 30 Days."

Addendum 7 – Round 1, Part 3					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
58	Schedule F	3.2	22	Are all Commonwealth service management processes been aligned with ITIL v3? If not, which processes are aligned at this time?	The Commonwealth has fully aligned Change Management with ITIL v3. Implementation of the other ITIL processes are in progress at this time.
59	Request for Proposal			What ITIL transformation within the Commonwealth agencies needs to be supported or engaged by the Offeror?	The Commonwealth has implemented ITIL Change Management and is using a modified ITIL Incident Management process today. The Offeror must support Incident Management, Change Management, Problem Management, CMDB, Service Level Management for all services provided within this contract. However, the Offeror is not responsible for implementing ITIL within the Commonwealth, only supporting the processes defined by the Commonwealth.
60	Schedule F	2.3.5	12	With regards to Transition Services, what are the perceived/known limitations on behalf of the Commonwealth to support the Transition Service? The Offeror must provide an estimate of any required Commonwealth resources, including the skills needed and the duration required for each of the resources required in order for the Offeror to implement its solution. Please explain the statement that "Commonwealth expects to provide limited resources." What are the Commonwealth expectations in terms of man-time commitments and direct involvement with regard to application migration schedule development, application upgrades to support new hardware and operating systems required under requirements section (3.2.1.5.1 - Technology Refresh), applications testing, architectural design and approvals?	The Commonwealth has limited staff available for the transitions related to this procurement. The referenced statement is intended to set the expectation that the Commonwealth will assist the contractor with the Transition Services, but has limited resources available. Thus, the Offeror is to provide an estimate of the Commonwealth resources it believes would be helpful.
61	Appendix A Exhibit D.7	13(b)	16-18	Has the Commonwealth evaluated or have an assessment of the EDC's tier rating? What is that assessment?	The Commonwealth has not had a formal Tier Rating assessment.
62	Request for Proposal			Does the Commonwealth intend to hire a vendor to assist them with oversight of this project? If so, what will be their role and when do you expect to have them under contract?	The Commonwealth is considering an IV&V vendor but at this time has not determined if one will be engaged. Therefore, no determination of scope and role has been defined at this time.

Addendum 7 – Round 1, Part 3					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
63	Schedule I Schedule J.2 Schedule J.3			Does the Commonwealth expect the bidder to improve the infrastructure configurations from those shown in Schedule I to meet the Service Levels? The documented configurations lack the high availability components to meet the higher order Service Levels.	The Commonwealth is procuring computing services. The selected Offeror must configure its infrastructure to meet to the SLAs.
64	Request for Proposal			Who (Commonwealth or vendor) is responsible to make any application changes caused by moving applications to a different data center site or issues related to re-hosting applications onto refreshed hardware? For example, applications using hard coded IP addresses, application recompilations, etc.	The Commonwealth is responsible for application changes.
65	Schedule F	3.1.3, Requirement 5	20	Will the Commonwealth accept a DR tier that leverages lower level application environments that are used on a daily basis that will act as a DR platform when required as a cost savings consideration? For clarity, this translates to the unavailability of test environments to the agency during each DR testing and during an actual recovery.	The Commonwealth recognizes this as an option for DR services. This will be determined on an application-by-application basis.
66	Schedule F	3.2.5.3		Provide clarity on how the Commonwealth expects to procure this. (E.g. Subscription, duplicate of infra, etc.) Does this apply only to CoD or other service categories?	The Commonwealth will procure DR Infrastructure On Demand in the same method used to procure all other services within this procurement. The Commonwealth will place an order with the contractor and the contractor will deliver the service.
67	Schedule J.3	SL20	30	Verification that Formal RCAs are only required when requested by Authorized User. Who will be designated as Authorized Users?	The Commonwealth will determine the authorized user list as part of transition.
68	Schedule F	3.2.2.2	67	What does the Commonwealth consider to be reasonable timeframe to receive written acceptance regarding ready for use and user acceptance testing? At what level will such approvals be required i.e. system, application, agency, etc.?	~~The Commonwealth will not unreasonably withhold or delay the acceptance or rejection of the Offeror's written notice regarding "ready for use". The range may vary but will generally fall within two (2) days to two (2) weeks based on many factors such as required Commonwealth verifications, Commonwealth personnel availability, complexity of the new environment, etc.~~
69	Schedule J.1	2	3	Who is responsible for interruptions to the "application Infrastructure" caused by the Commonwealth applications or staff?	The Commonwealth would be responsible if the interruption was determined to be solely due to the actions of the Commonwealth. Otherwise, the contractor would be responsible.

Addendum 7 – Round 1, Part 3					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
70	Schedule F	3.2.1.1.4	32	Is there a requirement to have dual connections for Commonwealth business partners to access to Commonwealth systems? Please provide a list of business partners and associated volumes such as number of users connecting, duration of connections, size of data transfers, and other relevant information.	The Commonwealth's Business Partners (BP) provide the physical circuits to the Commonwealth's BP network into the Commonwealth's Co-Location space within the EDC and DPH. The Business Partner determines the number, size and redundancy of the individual BP connections. The Offeror must support these connections by providing Security, Access, and Network Connections to the Commonwealth Network, Floor/Cabinet Space, Cooling, and Power. The Commonwealth or the Business Partner is financially responsible for these circuits. Currently there are 3.5 cabinets within the Co-Lo space in the EDC dedicated to the Business Partners containing 65 Business Partner connections to support within the EDC. The DPH has 1 data circuit (to HP) for Business Partner connections. The following is the current list of BP circuits within the EDC and may be different at the time of transition: Xerox/EBT – 2 Data Circuits, 1 Analog Circuit; FDCS/PNC Bank – 2 Data Circuits; Telvent/TrafficLand – 1 MPLS Ethernet Data Circuit; DTCC – 1 Data Circuit, 1 Analog Circuit; ITG (formerly MacGregor (MFN)) – 1 Data Circuit; Thomson Reuters/BT – 4 Data Circuits ; SGI – 1 Data Circuit ; PNC Bank – 1 Data Circuit, 1 Analog Circuit; GTECH/Central Control System – 1 Data Circuit; DST/Gateway – 1 Data Circuit, 1 Analog Circuit; Highmark – 1 Data Circuit; L-1 Identity Solutions (formerly IBT, Identix) – 1 Data Circuit; OMAP/APS – 1 Data Circuit, 1 Analog Circuit; UHC/Verizon Business – 1 Data Circuit, 1 Analog Circuit; DOLNet/BLS – 1 Data Circuit, 1 Analog Circuit; Xerox/UI-ICON – 1 Data Circuit; IBM Remote Management – 2 Data Circuits, 1 Analog Circuit; AAMVA – 2 Data Circuits, 2 Analog Circuits; Assurant – 1 Data Circuit; AT&T Messenger Services Network – 3 Data Circuits; IRS – 1 Data Circuit, 1 Analog Circuit; TitleNGo (PA Messenger Solutions) (JEBTech/Gatekeeper) – 2 Data Circuits; Verizon Business/Emissions Service – 2 Data Circuits; Xerox (formerly ACS)/Customer Call Center – 2 Data Circuits; Bloomberg – 8 Data Circuits; Financial Control Systems – 1 Data Circuit; BNY Mellon – 2 Data Circuits, 1 Analog Circuit; Trustmark Insurance/CoreSource – 1 Data Circuit, 1 Analog Circuit; Vitech – 1 MPLS Data Circuit; FMS/TOP – 1 Data Circuit; IO/Enterprise Networks – 2 Analog Circuits

Addendum 7 – Round 1, Part 3					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
71	Schedule F	3.2.1.7	57	As it relates to Configuration Management: What is the Commonwealth's current CMDB? What is meant by an electronic interface? Is an electronic copy/extract considered sufficient or must this be a transaction by transaction interface? What product / database is the Commonwealth using for its CMDB?	The Commonwealth's current CMDB is the BMC Remedy CMDB hosted within the Enterprise Remedy System. The data is housed within a Microsoft SQL Database located within the EDC. The Offeror is to provide updates to the CMDB directly from the Offeror's ITSM system on a regular basis.
72	Schedule F	3.2.1.7	57	Please provide more information regarding the Commonwealth's existing CMDB. Are all CIs under the scope of this contract currently documented in the Commonwealth CMDB? Has the CMDB recently been audited for accuracy?	The Commonwealth's CMDB is not complete. The Commonwealth's CMDD has not been audited.
73	Schedule F	3.2.1.4-11	46	As it relates to reporting on "Key issues relating to Service Desk processes, improvements, script development." What is the expectation regarding script development? Is this related to monitoring scripts, data collection scripts, or incident/problem resolution scripts?	The contractor must provide and continually improve the incident/problem scripts used by the helpdesk agents when a Commonwealth representative contacts the Services Desk.
74	Schedule F	3.1.3	18	This section states "The Offeror must address in its design how it will create a target environment that will minimize application latency concerns". If latency issues are introduced as part of the existing data center migrations to new facilities, who is financially responsible for resolving such issues, the Service Provider or the Commonwealth?	The contractor must provide the infrastructure to support the Commonwealth's applications. Application changes are not always possible. Therefore, it is the Offerors responsibility to resolve the issue.
75	Schedule F	3.2.1.5	50	Can the Commonwealth indicate the process that will be used to gain stakeholder approval from agency personnel in terms of format and duration for approval?	The contractor will submit a proposed architecture with anticipated costs to the respective application owner and OA-OIT. Then the application owner and OA-OIT will review, discuss, modify and approve or deny the architecture. The duration of this process is dependent on many factors including but not limited to the complexity of the proposed architecture and the availability of Commonwealth resources. Therefore, a set duration is not available.
76	Schedule F	3.2.2.4	72	Based on the statement in this section "The Commonwealth will provide the Offeror with a list of agency applications that require a DR solution and related DR plan after contract is awarded . " Are we to consider the data provided in Exhibit B.5 to be complete?	The data provided within Exhibit B.5 is the list of current DR solutions provided at this time. Additional applications may require DR. The selected Offeror must provide DR to any application that the Commonwealth orders with DR.

Addendum 7 – Round 1, Part 3					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
77	Schedule F	2.3.4 Data Protection	11-Oct	DLI is shown as Group 2 Transition and the other agencies (DPW, DOR, DOH and PSP) are shown as Group 3 Transition. Both groups are due to be completed within 30 months of contract start. What is the difference between the transition groups?	The datacenter for the Department of Labor and Industry has special power considerations, as a result, the Commonwealth wants to track the transition separately from the other transitions.
78	Appendix A Schedule F	12(d)(2) 3.2.5.3	15 138	Does the Commonwealth anticipate designating any dev/test/pre-production systems as DR recovery targets for any primary systems? If so, are applicable SLAs waived for these DR target systems in their principal role as dev/test/preproduction until the End of the disaster?	The DR configuration described in this question is one possible solution. Whether it could be implemented would be based on the requirements of the application owner. No, there are no provisions within the RFP for SLA waivers in this situation. The Offeror must support the subscribed to SLA for the "dev/test/pre-production" system.
79	Schedule F	3.1.1, Multi Datacenter Environment (2+ Architecture)	Pages 13 and 14	The requirement in the matrix starts with number 3. Are requirements 1 and 2 missing or is this matrix numbered incorrectly? Would the Commonwealth please clarify?	The matrix is numbered incorrectly. Numbers 1 and 2 are not used, which means that the matrix begins with number 3. There is no information missing.
80	Schedule D	M4, M9	2, 4	Both the Due Diligence and the ITSM System Integration milestones must be completed in 180 days. M4 includes as a bullet point “completion of data gathering on B2B interface to Enterprise Remedy, within the 180 day, and M9 requires that completion and acceptance of Integration between Enterprise Remedy and the Offeror’s ITSM system within the 180 days. Shouldn’t M9 allow for the data gathering to be completed first, and thus the timeframe for M9 be greater than 180 day?	The Milestones set out in Schedule D may be satisfied at any time prior to the Milestone Due Dates.
81	Schedule D	M4, M5	2, 4	Both the Due Diligence and the Detailed Transition Plan milestones must be completed in 180 days. M5 has a direct dependency on the completion and acceptance of the Due Diligence deliverable. Shouldn’t M5 allow for the data gathering to be completed first, and thus the timeframe for M5 be greater than 180 days?	The Milestones set out in Schedule D may be satisfied at any time prior to the Milestone Due Dates.

Addendum 7 – Round 1, Part 3					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
82	Schedule D	M4-M5-M9	2 and 3	It appears the delivery of the ITSM and Transition Project plans are due at the completion of the Due Diligence period all three are within 180 days of contract execution. Is this accurate or an oversight?	The Milestones set out in Schedule D may be satisfied at any time prior to the Milestone due dates.
83	Schedule D		2	Upon completion of due diligence, will the vendor have the option to modify other transition milestone deliverables that are due at the same time or prior to the completion of due diligence in accordance with results gathered during that process?	The Milestones set out in Schedule D may be satisfied at any time prior to the Milestone due dates. Refer to Section 27 (Change Control) of Appendix A regarding modifications to the milestone due dates.
84	Schedule F	3.2.1.4	44	What content does the Commonwealth envision including for agency use in the KMP and what responsibility will Offeror have regarding this content?	The Offeror must provide this portal. The information content will include but is not limited to: run-book type information for each application, service level and other management reports, configuration information that is relevant to the services provided, contact and escalation lists, process and procedure manual , project plans, and other information related to the contract and services. The Offeror will provide the portal and provide multiple levels of security for access to the information stored within. Also, the Offeror must provide the information related to the managed services provided as defined by the application owners and the Commonwealth's program office. There is to be multiple levels of access as determined by the Commonwealth.
85	Schedule F	3.2.1.8.3	60	Does the Commonwealth expect the Offeror to track application software licensing or infrastructure related software only?	The Offeror must track only the software licensing for the infrastructure included within this procurement.
86	Schedule F	3.2.1.5	50	What is the definition of industry standard software to contain the service catalog?	The Offeror must use a software package that is generally available for any US company to purchase and implement. A custom designed and written application is not acceptable.
87	Schedule F	3.2.2.4 DR Planning & Testing	72-75	From item #8: “At a minimum, the Offeror shall support annual and semi-annual DR exercises.” So, which is it?	The Offeror should plan that some applications will require an annual exercise and some will require semi-annual. Frequency of DR exercises will be at the discretion of the Commonwealth.
88	Schedule K	D-02.39	9	Is the expectation that the Offeror provide the procedures to produce the audit report or present the report as the Offeror will not have full responsibility for systems at 60 days past effective date.	The Offeror will provide the methodology to produce the audit report within the "Effective Date +60 Days" requirement. This is also the same for Deliverables D-02.39, D-02.44, and D-02.49. Schedule K has been revised and reissued.

Addendum 7 – Round 1, Part 3					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
89	Schedule F	3.2.1.4	44	As it relates to the "Offeror must provide an Internet accessible KMP as a central repository for processes and procedures, communications plans, and other relevant documentation to be shared with the Commonwealth" What level of security will be required for this internet facing Knowledge Management Portal? Will two factor authentications be the standard?	The portal must be capable, at a minimum, of being secured at the folder level by user. Secure information must be able to be limited to a few authorized people where other information should be available to full list of authorized users at the Commonwealth. The Commonwealth will establish an authorizing process as part of transition.
90	Appendix A	22c	32	Can you please elaborate on the Commonwealth's requirement that the Commonwealth will pay monthly invoice only if Commonwealth accepts our services with WRITTEN notice? How will this action be performed?	The process will be determined with the selected Offeror as part of CCPM creation. The Commonwealth anticipates that the invoice would be submitted as an order online via Remedy and if the service is accepted by the Commonwealth, an acknowledgement will be forwarded via Remedy to the contractor.
91	Schedule F	2.3.5	12	How does this activity impact out of scope facilities such as Selinsgrove and the Reading PA DR location? How will schedule conflicts be handled?	The referenced locations will be vacated once the Services under the contract have been fully transitioned. As a result, there should not be any schedule conflicts.
92	Schedule F	3.2.5 Capacity on Demand Services	133-141	Regarding the Capacity on Demand Services, are they subject to all the requirements described elsewhere in the SOW? For example, do all the Security Management requirements apply to systems in the Cloud. Typically, the Cloud is used for quick implementation and cost effective support of systems with a lesser set of requirements, such as development and test machines.	The requirements specified within the RFP apply to all services, including Capacity on Demand Services.
93	Appendix A	14 (a)	19	Does the responsibility for all costs associated with transition also include covering the costs for Commonwealth application support resources during the relocation phases?	The selected Offeror will not be responsible for modifying an application. The selected Offeror, will, however, responsible to provide the infrastructure that is required for the application to operate at the performance levels maintained before transition to the Offeror's services.
94	Schedule I	Tab 1	N/A	Will the Offeror add a new item to the services catalog and the SLA matrix every time a new configuration is used/requested?	The Service Catalog should be unit based to allow for agencies to order configuration changes without adding items to the Catalog. If a new service needs to be added then the Catalog, service descriptions and SLAs may need to be altered.
95	Schedule J.3	SL01-SL05		Do the applications have architectures that permit this type of SLA to be measured? What is the nature of the measurement that will suitably capture "availability"? Is that measurement identical for all applications?	The SLA is on the services provided by the Offeror. The CMDB must identify all infrastructure components used to provide that service and must be identified on an application basis. Therefore, the SLA is on the sum of the infrastructure components.

Addendum 7 – Round 1, Part 3					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
96	Schedule F	3.2.3.2	89	Requirement 1 states a need to not just monitor batch but also appears to require problem determination for "abnormal conditions" and rerun. This section also states that any abnormal condition that cannot be corrected will be referred to "technical support staff for resolution". Is the technical support staff reference in this section the Commonwealth application technical support staff responsible for the application batch jobs or the Service Provider's technical staff?	The technical staff responsible for investigating and resolving the "abnormal conditions" would be based on the results of initial troubleshooting and triage. The contractor is responsible to perform the initial triage and determine if the issue is potentially caused by an area managed by the contractor. If so, then the contractor is responsible to resolve the issue. If the troubleshooting determines it is an application issue, the contractor must contact the assigned application point of contact and assign the incident to the Commonwealth. The contractor must support the application support team in continued troubleshooting and resolution while maintaining a running log of events within the ITSM system.
97	Schedule F	2.1	5	When providing the multiple environments, does the Commonwealth require physical separation or will logical segregation and physical separation, where required by regulations and statutes be acceptable?	The type of separation required for each environment will be determined by IT policy or requirements of the application owner. This will be determined during transition planning on an application by application basis.
98	Exhibit G.12 , PSP - CHRIA Handbook			This document is missing the charts	There are no charts in Exhibit G.12 and the version provided is the current version issued by the Pennsylvania Office of Attorney General.
99	Request for Proposal			Are any of the cells in the cost matrix being weighted with greater value as part of the overall cost evaluation?	There are no minimum consumption parameters included in the contract. The volumes provided in Schedule I will be used to evaluate the cost portion of the RFP and are not a minimum commitment nor an all-inclusive list of services desired by the Commonwealth.
100	Request for Proposal	I-5	1	If Type of Contract is consumption-based model, then are there minimum consumption parameters that will be included in the contract?	There are no minimum consumption parameters included in the contract. The volumes provided in Schedule I will be used to evaluate the cost portion of the RFP and are not a minimum commitment nor an all-inclusive list of services desired by the Commonwealth.
101	Schedule F	2.3.2	8	Regarding the migration to IPv6, is there any federal or state deadline set for specific agencies to be migrated to IPv6?	There is no federal or state deadline for specific agencies to be migrated to IPv6 at this time.
102	Schedule J.2	SL29	Batch Processing	Will documentation be provided that gives specific details regarding the batch environment? There is nothing listed in the expected Exhibits related to batch.	This information will be provided as part of Transition planning.

Addendum 7 – Round 1, Part 3					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
103	Schedule F	2.1	6	*"The cost for those Services must remain less than the cost the Commonwealth would have incurred for providing the same infrastructure itself."* How is this calculated by the Commonwealth? Does the commonwealth have costs per service already defined, and does it include Power, Networking, Maintenance, Hardware replacement, Security, etc.?	This requirement is intended to encourage Offerors to be aggressive in providing low cost / high quality services to the Commonwealth. The Commonwealth will not provide the current budget or spend on services requested within this RFP.
104	Schedule F	2.2.1	6	Commonwealth states "The cost for those Services must remain less than the cost the Commonwealth would have incurred for providing the same infrastructure itself." To meet this requirement, please provide the current cost baseline cost that the Commonwealth will use to measure against and the make-up up of the current cost baseline.	This requirement is intended to encourage Offerors to be aggressive in providing low cost / high quality services to the Commonwealth. The Commonwealth will not provide the current budget or spend on services requested within this RFP.
105	Schedule J.1	8	8	Please elaborate on the (3) Service Level Defaults in (6) month period. Is this referring to (3) repeated occurrences of the same default or (3) defaults across the enterprise in total?	This section is referring to (3) repeated occurrences of the same default.
106	Schedule J.3	SL01-SL05		Which applications are expected to run at the various SLAs today and will be in the various levels coming/wanted?	This will be determined as part of the transition planning and will be on an application-by-application basis.
107	Schedule F	3.1.3	19	In requirement 3, is there a relationship between the storage approach types (Basic, Committed and Dedicated) and the Storage Tiers in Schedule I (Pricing)? If so, what is the breakdown of the volumes in Schedule I to the storage approach types?	This will be determined as part of the Transition Planning and will be on an application-by-application basis.
108	Schedule K	Through-out		How are Commonwealth induced or required delays to be accommodated within these deliverable due dates? For example, several deliverables listed require approval and review before a follow-on deliverable can be completed (e.g. D-02.04 and D-02.05 or D-02.09 and D-02.10).	Unless otherwise set forth in the CPPM, the Commonwealth will review deliverables according to the timeframes set forth in Section 22 (Inspection and Acceptance) of Appendix A.

Addendum 7 – Round 1, Part 3					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
109	Schedule F	3.1	12	Is the Offeror expected to reuse any Commonwealth owned hardware and software? Are there any restrictions on the reuse of Commonwealth owned hardware e.g. hardware owned by a specific agency can only be used by the owning agency?	With the application owner's approval, consolidation may be possible.
110	Schedule J.1	15	11	Do SLAs apply during a declared disaster?	Yes
111	Schedule G	4	6	There are inconsistencies noted between the requirements and the Offeror key personnel table entries. Is the Account Executive actually the Engagement Executive?	Yes, "Account Executive" and "Engagement Executive" refer to the same position. Schedule G has been reissued.
112	Request for Proposal			Can any agency that is currently included in scope of this RFP decide not to participate once bids are submitted?	Yes, an agency may choose not to participate.
113	Schedule F	2.1	7	Will agencies be able to request deviations from standard services processes used for all agencies?	Yes, however, standard processes must be developed to encompass all reasonable needs of the agencies; thus few exceptions should be required.
114	Schedule F	2.3.1	8	With regards to supporting multiple security and network zones to support specific agency requirements, other than logical VLAN separation, is there an expectation on behalf of the Commonwealth that multiple physical networks be created?	Yes, in some cases. Multiple physical networks must be created if required by law, IT policy, or an RFP requirement.
115	Exhibit K		12	Please verify – the Data Power House ACD Call volumes shown in the table are not included in the DPH line item volumes in the Table on page 11.	Yes, the ACD Call volumes are included in the Incident volumes. Not every ACD call is an Incident creation event. The call volumes provided in Exhibit K include opening an Incident, requesting and providing updates to open Incidents, and conversations on delivery of capabilities, and general questions. Incidents may, however, be requested by the Commonwealth in other means which may include email, meetings, escalations. The incumbent may also create an Incident from the incumbents' monitoring system results or through direct reports. Therefore, the number of calls do not have a direct correlation to the number of Incidents.
116	Exhibit d.x edc	EDC Facility Summary		Are there multiple data feeds into the building with diverse entry points and meet me locations?	Yes, there are multiple diverse data feeds, entry points and meet me location at the EDC.

Addendum 7 – Round 1, Part 3					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
117	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			Are there existing service / warranty agreements for the generator, transfer switches, batteries, UPS switch gear and PDU/ RPPS? What is the length of warranty or service for these devices	Yes, there is a current service agreement in place for the refaced power components. Current service agreements through 6/31/13.
118	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			Is there an existing service agreement for the fire protection system? Has it been in continuous effect since installation? With the same service supplier?	Yes, there is an existing service agreement. Yes, an agreement has been in continuous effect since installation. No, there has been more than one service supplier.
119	Schedule J.3	All	All	This section refers to Severity Levels. Should it be referring to Priority Levels?	Yes.
120	Schedule F	3.2.4.7	128	Does the scope of the Database Management optional service include both physical and logical database administration?	Yes.
121	Schedule F	3.2.5.3	138	Are DR services expected to be limited to the same class of service as the primary system's class of service (fully-managed, managed only, etc.)?	Yes.
122	Schedule F	3.2.5	133-139	Will any critical applications be hosted in or permitted in the Capacity-On-Demand environment?	Yes. Critical applications will be permitted in the Capacity on Demand environment.

Addendum 7 – Round 1, Part 3					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
123	Schedule F	3.1.2 Network and Security Architecture	17	Are HIDS required in the environment and if so which servers requires this support?	Yes. The Offeror must provide HIDS per the individual agency's requirements.
124	Schedule F	3.2.1.1.1	27	Does the request to integrate the financial management tool with the Commonwealth's Remedy Billing module constitute part of the expected invoicing process?	Yes. The selected Offeror must integrate its invoicing system into the Commonwealth's enterprise remedy system.
125	Request for Proposal			Should the fiber connection be delayed or any other required act by the Commonwealth, what impact does that have on the December 31, 2014 deadline including the $50M penalty?	The following is a revised answer to Round 1 Part 2 Question 6. The fiber connection is the responsibility of the Offeror. The selected Offeror must meet the transition milestones.
127	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			Is there attic stock available of ceiling tiles for use in the data center? If yes, how many panels?	The following is a revised answer to Round 1 Part 1 Question 113. Yes, 13 panels.

Addendum 8 - Round 1, Part 4					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
1	Schedule J.3	SL12	19	What is the Commonwealth's definition for "viable proposal"? What measures constitute "viability"?	A "viable proposal" for this SLA is a technically sound and complete proposal that includes enough details for the Commonwealth to place an order with the contractor. The proposal must be able to be provided from the then current Catalog of Services (Schedule C).

Addendum 8 - Round 1, Part 4					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
2	Appendix A	32j	51	Can you please define Proprietary Communications Network?	A communications network that is not commercially available to the Commonwealth from multiple providers.
3	Schedule J.3			What constitutes a complete request or acceptance?	A completed request is a request that has been completed by the contractor and has been turned over to the Commonwealth for validation. An accepted request is a request that has been accepted by the Commonwealth.
4	Schedule F	3.2.2.1	61	What type of peripherals does the Commonwealth currently use and expect to be moved as part of the Transition. Who manages these peripherals today?	All known hardware including peripherals is included in the existing Exhibits. Any additional peripherals will be discovered during the Transition planning stage of this procurement. These peripherals are currently managed by the Commonwealth.
5	Schedule F	3.2.5	133	In a cloud IaaS solution, particularly for Server Capacity, but in general, how important is portal access to the environment to the Commonwealth? Can you rate as Critical, Important, or Optional?	All of the RFP requirements are important to the Commonwealth. The Commonwealth does not disclose detailed evaluation criteria.
6	Appendix A	14 (c) (ii)	21	Can you please elaborate on system degradation? Does the Commonwealth have a way to collect baseline measurements and have tolerances been defined to determine if system performance is degraded?	Baseline measurements will be established during the transition phase. A service is degraded if it fails to meet the minimum baselines.
7	Exhibit K		11	Do the Incident Volumes in the table include Requests? Please provide a breakdown of call mix / call types.	Both requests and incidents are included in the table. The Commonwealth does not currently have a breakdown of the information requested and, therefore, is not available to provide it.
8	Appendix A Exhibit D.7	13(b)	16-18	Please describe any cooling challenges/hotspots, if any.	Computer Room 1 may become warm if a unit is down for an extended period of time. The area of warmth is generally limited to the area of the unit which is down. No other issues are known.
9	Schedule F	2.1	6	What HA (High Availability) application DR solutions exist today? Can the Commonwealth describe the technology and requirements around this requirement? For example: Active-Active replication requirements between data centers? What are the DR (Disaster Recovery) objectives for such HA solutions (RTO – Recovery Time Objective and RPO – Recovery Point Objective)?	Currently the Commonwealth has no applications designed for High Availability across multiple datacenters. The Commonwealth desires the infrastructure to readily support HA across datacenters, thus allowing future development of this capability. DR objectives are set on an application by application level and will be based on the needs of the application owner.
10	Appendix A Exhibit D.7	13(b)	16-18	Which equipment in the EDC is powered by dual power connections?	Dual power connections are the standard in the EDC. Very few components have a single power supply.
11	Exhibit K		11	Please provide an ACD analysis that shows hourly call arrival patterns for a representative week Sun-Sat.	See 6100022698 - Exhibit K - OA Enterprise Remedy and Volumetrics has been re-issued to provide this level of detail. This is a confidential document. To receive a copy, please contact Sheryl Kimport, the Issuing Officer.
12	Schedule F COPA	3.2.5.1 Server Capacity on Demand	134	Requirement #5 in this Section describes the desire for expedited service. How is expedited service defined?	Expedited service is the deployment of a service in an interval shorter than the standard interval identified in the service catalog. These should occur rarely, however, there may be times that this is required due to a failure of another service/equipment or a requirement set upon the Commonwealth that is outside the Commonwealth's control, such as one set by Federal or Commonwealth law.

Addendum 8 - Round 1, Part 4					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
13	Schedule J.3	SL29	43	Do job failures include those where an application failure occurs and is the cause? How are such jobs to be counted for purposes of this SLA?	Failures that are caused solely by an action or inaction of the Commonwealth would be excluded, including any failures related to software / application that is not the responsibility of the Offeror. The type of failures described here would be listed within the SLA Report but excluded from the calculations.
14	Schedule I	1. Volumetrics	N/A	Line 192-193 Tape Stored. Please clarify if volume is expressed as native or compressed (ratio) and if encrypted.	For Line 192-193 Tape Stored, the volume is expressed as native.
15	Schedule F	3.2.1.8	60	Reference: "The Offeror's 3rd Party License Management service must ensure accurate inventory and licensing compliance for all Offeror provided infrastructure software products." Please provide license compliance report for all existing infrastructure software that will need to be supported by Offeror. (Or optionally, can Offeror assume all existing infrastructure software listed in RFP exhibits have full support till Dec 2014?)	For purposes of submitting a proposal, Offerors may assume that all 3rd party software utilized within the DPH has full support through 12/31/2014.
16	Schedule D			Given the transition services and transition timeline to transition the EDC & DPH by 12/31/2014 and the other data centers within 30 months from contract execution, and given the financial credits for not achieving those milestones, is the Commonwealth going to commit to a contract start date to provide visibility into a transition timeline?	For purposes of submitting a proposal, Offerors should assume an approximate contract start date of December 2013. The actual start date may vary and will depend on a number of factors including the length of contract negotiations and the Commonwealth contract execution process.
17	Request for Proposal (General)	N/A	N/A	In order to provide accurate costing and schedules, please state the presumed start date of the contract.	For purposes of submitting a proposal, Offerors should assume an approximate contract start date of December 2013. The actual start date may vary and will depend on a number of factors including the length of contract negotiations and the Commonwealth contract execution process.
18	Schedule F	3.2.5.5		What is the contract start date for cost/price purposes? July 1, 2013?	For purposes of submitting a proposal, Offerors should assume an approximate contract start date of December 2013. The actual start date may vary and will depend on a number of factors including the length of contract negotiations and the Commonwealth contract execution process.
19	EDC tour	Tour handout		What is the % of servers hosted vs the % of servers managed lite vs the % of servers managed full?	Fully managed = 28%, Managed lite (up to O/S) = 58%, Hosted (Co-location) = 14%
20	Request for Proposal			How are agency schedule needs accommodated in the instance where those needs will delay or cause the delay in deliverables and milestones?	Identifying specific agency scheduling needs will be part of the transition planning. The Commonwealth does not have enterprise-wide "No Maintenance" periods. Each "No Maintenance" period is requested and scheduled by the individual agency. The Commonwealth does have several regularly scheduled "No Maintenance" periods every year. Please refer to ITB-NET015 which describes the process for requesting a "No Maintenance" period and the Commonwealth's approved Enterprise Maintenance Windows. See Exhibit O - 2012 Agency NMRs for the No Maintenance periods that occurred during 2012. This is a confidential document. To receive a copy, please contact Sheryl Kimport, the Issuing Officer.

Addendum 8 - Round 1, Part 4					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
21	Exhibit d x edc	EDC Facility Summary		Are the available power/cooling density (watts/sq') the same in both rooms? What are your documented power/cooling densities?	It is not known whether the available power/cooling density is the same in both rooms. The cooling densities are not documented.
22	Exhibit B.1 DPH - Asset List			Can the Commonwealth provide more detail regarding the processors and peripherals listed in Exhibit B1? Specifically-- For the mainframe processors (2817 and 2098): amount of processor storage (memory), number and type of specialty engines (IFL, zIIP, zAAP, etc.) and number and type of other adapters, such as FICON, ESCON, OSA, etc. For DASD: amount of processor memory, number and type channel adapters, number of drive sets, function authorization (OEL, PTC, PAV, etc). Tape: detailed configuration information for the 35xx and 39xx.	Mainframes: The 2817 and 2098 processors currently have a combined quantity of: 144 GB Processor Storage (memory) + 24GB HSA; 8 - SAP; 5 - IFL; 1 - zIIP FICON - 88; ESCON - 172; OSA - 42 DASD: The combined quantity of DASD owned and operated by IBM: DASD 128 GB Processor Memory (32) - 4GB FICON/FCP Adapters (14) - 146GB 15K Drive Sets (2) - 300GB 15K Drive Sets Function Authorization includes: OEL, PTC, PAV, HyperPAV, FICON Attachment *** DMX3 **** Processor Memory: 256GB Type of Adaptors (Mainframe Only): Fiber Channel Adaptors (2Gb) Number Adaptors (Mainframe Only): 32 Number of Drive Sets: 14 Raid Type: Raid5 3+1 *** VMAX *** Processor Memory: 64GB Type of Adaptors (Mainframe Only): Fiber Channel Adaptors (8Gb) Number Adaptors (Mainframe Only): 4 Number of Drive Sets: Thin Provisioning Raid Type: Raid6 6+2 *** DMX4 *** Processor Memory: 48GB Type of Adaptors (Mainframe Only): Frame Number Adaptors (Mainframe Only): 8 Number of Drive Sets: No Dedicated Raid Sets Raid Type: Raid5 7+1 TAPE: Information about the configurations about Tape hardware is provided in Exhibit B.1 of this RFP.
23	Schedule F	2.1	5	Commonwealth references their Systems Development Lifecycle (SDCL). Have you published your SDLC so we can view your development methodologies and lifecycle approach?	No, the Commonwealth has not published a standard Systems Development Lifecycle. The Commonwealth does not have a standardized SDLC. Each application may have its own SDLC.

Addendum 8 - Round 1, Part 4					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
24	Schedule D	M-4	2	Upon completion of due diligence, will the vendor have the option to modify other transition milestone deliverables that are due at the same time or prior to the completion of due diligence in accordance with results gathered during that process?	No, the Offeror may not modify milestones. The Offeror must follow the program deliverables set out in Schedule K - Key Program Deliverables. The milestones set out in Schedule D are in support of the outcomes required in Schedule K.
25	Schedule F	3.2.4.3	105	Should a Production Control Management requirement, such as 3.2.4.4 requirement 3, be included in ERP Hosting – SAP / Oracle?	No. A Production Control Management requirement, such as 3.2.4.4 requirement 3, should not be included in ERP Hosting - SAP/Oracle.
26	General	All	All	Will the Commonwealth consider a proposal that would include application redesign and redeployment of Agency applications to eliminate certain platforms like Unisys and IBM mainframes?	No. Application development services are outside the scope of this procurement.
27	Request for Proposal			Once due diligence is complete (starting in 2013) and the size of the fiber connection needed to connect between the vendor data center(s) and the Commonwealth's network is determined, will the Commonwealth assume full responsibility for acquiring the fiber connection (s), coordinating installation, the cost of installation and the monthly cost of the needed fiber to connect?	No. The Selected Offeror must provide the fiber connections to the Commonwealth at its cost.
28	Schedule F	3.1.3	18	This Section, first sentence states ", utilizing existing and/or underutilized technologies where appropriate," What method will be used to identify and acquire those assets if desired by the Offeror?	Offerors must propose a methodology to identify existing and/or underutilized technologies. Offerors will not "acquire" Commonwealth assets but may use certain hardware and software components with Commonwealth approval.
29	Schedule F	3.2.2.6	80	This section states that "Additional Performance Monitoring Services such as database and application monitoring will be offered to the Commonwealth as an additional level of service". Please define the use of the words "an additional level of service" and who will be financially responsible for any level of application monitoring.	Performance monitoring services should be offered to meet the specific needs of the agency and/or application. These may be built in to the level of service cost or may be offered ala carte.

Addendum 8 - Round 1, Part 4					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
30	Schedule F	3.2.4.8		Of the machines in the various locations, how do they split down by service category? What SLAs/response times are required for the Capacity-On-Demand environment? What network connectivity is required What location is expected for the Capacity-On-Demand environment? What transition milestones are expected/required for the Capacity-On-Demand environment?	Please clarify the first question. The Offeror must provide Capacity-On-Demand according to Service Levels SL01 through SL31, as defined in Schedules J.1, J.2, and J.3. Network connectivity is the responsibility of the Offeror. The Commonwealth has as no preference or requirement on which datacenters provide Capacity-On-Demand services. The selected Offeror must meet the milestones for Capacity-On-Demand as described in Schedule K.
31	Exhibit B.4 DPH - Third Party Software Asset	All	All	Please provide the current cost, licensing arrangement, cost metric (CPU, Core, PVU, etc.), and transfer or assignment cost that currently exist for each application?	Please clarify the question and provide additional detail.
32	Schedule J.3	SL14-SL15		Which software and in what service categories are covered? How will we learn about the software that we cannot otherwise discover plus the terms of that lease?	Please clarify the question and provide additional detail.
33	Schedule F Statement of Work	Schedule F	60	Will the Commonwealth include an evaluation of enterprise licensing agreements for applications that will be consolidated in the new data center?	Please clarify the question and provide additional detail.
34	Schedule J.3	SL16	25	Please provide elaboration on the "relevant criteria" specified in the Commonwealth Computing Procedures Manual.	Relevant Criteria means the information that specifically pertains to the data recovery functions contained within the CCPM.
35	Schedule F	3.2.1.8	60	Will Offeror-provided not commercially provided software need to be transferable to the Commonwealth at the expiration of the agreement?	Requirements related to ownership and transferability of software are set out in Appendix A to the RFP. Section II-8 of the RFP provides that, the Offeror may identify which, if any, of the terms and conditions (contained in Appendix A) it would like to negotiate.

Addendum 8 - Round 1, Part 4					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
36	Schedule F	3	12	This Task section states that the Commonwealth has provided detailed information on the current environments in the exhibits. It also states that the Offeror shall utilize the exhibits as the baseline requirements (in terms of services, quantities and bandwidth) for developing its proposal. Be aware that the "Volumetrics", reflected in Schedule I, do not reflect the current services, quantities, or the bandwidths that are reflected in the exhibits. Please explain this inconsistency. If the "Volumetrics" are only to be used for cost evaluation, how will the Commonwealth actual pay for the configurations reflected in the exhibits and being requested in this requirement?	~~Schedule I will be used to evaluate pricing. The Offeror is to provide catalog of services within the Catalog of Services tab of Schedule I, including rates that are consistent with the rates proposed throughout Schedule I. This service catalog will be used to determine the cost of each service provided to the Commonwealth. The invoice must reflect the items and rates listed in the catalog with quantities purchased.~~
37	Schedule F	3.3.2	143	This section states that "The selected Offeror shall not charge the Commonwealth for any Services currently Provided by the DPH or EDC until all of the Services provided by the DPH and EDC (Group 1) have been successfully transitioned." Can any fees be charged, such as transitions fees or any other fees, prior to transitioning all of the DPH and EDC services? Can any fees be charged to the Commonwealth prior to the expiration date of the existing contract scheduled for December 31, 2014?	~~Section 3.3.2. (Transition Planning/Governance) of Schedule F was revised by Addendum #4. The revised section states the following:~~ ~~The selected Offeror shall not charge the Commonwealth for any Services currently provided by the EDC until all of the Services provided by the EDC have been successfully transitioned.~~ ~~The selected Offeror shall not charge the Commonwealth for any Services currently provided by the DPH until all of the Services provided by the DPH have been successfully transitioned.~~ ~~The selected Offeror shall not charge the Commonwealth for any Services currently provided by an Agency's datacenter (example: DLI, DPW, DOR, DOH, PSP) until all of the Services provided by that datacenter have been successfully transitioned.~~ ~~The selected Offeror may charge the Commonwealth for new services after the contract effective date, excluding services that must be transitioned as described above.~~
38	Schedule H	1.4.3	11	Please provide the current process used for vendors to assist the Commonwealth for their budget cycle. Please elaborate on the budgeting process and your expectations for vendor participation.	See 3.2.1.1.5 for some examples of methods that could be used. The Offeror should, however, describe how it would assist the Commonwealth with the annual budgeting cycle. The offeror should describe its approach to assisting the Commonwealth through planning and forecasting.
39	Schedule F	3.1.1.9	15	Please provide further definition around segregation requirements for non-Commonwealth workloads and agency segregation. e.g. separate room / cage / raised floor in a shared datacenter.	See NIST 800-53 sections on physical security and physical security sections in CJIS policy http://www fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view
40	Schedule F	3.1.2	6	What is the Commonwealth's minimum FIPS 140-2 certification level?	See page 52 of CJIS policy

Addendum 8 - Round 1, Part 4					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
41	Request for Proposal	I-12	Page 3	Should Vendors also submit these forms/documents in PDF version to allow for signed versions to be included?	Signed MSWord documents are preferred. If unsigned MSWord documents are submitted, the Offeror must also submit signed PDF versions.
42	Schedule A , Defined Terms	N/A	Page 6	Schedule A – Defined Terms. In this section it does not specify what the "At-Risk Amount" will be on the contract. Should the Offeror assume an amount in its proposal, or will the definitive amount be negotiated by the parties following award?	The "At-Risk Amount" is 15% of the total monthly enterprise invoice submitted to the Commonwealth by the contractor each month.
43	Appendix A Exhibit D.7	13(b)	16-18	How much utility power is available to the EDC? What types of power are available for equipment in the EDC (e.g. 110VAC, 220VAC, 440VAC)?	The building is served by an underground 2000 kVA transformer at 277-480 volts. Equipment powered from the PDUs is 110VAC or 208VAC.
44	Schedule F	3.2.4	97	Requirement number 4 states "Provide technical advice and support to the Application Development and Maintenance (ADM) and Database Administration (DBA) staff, as required." Who is financially responsible for providing the advice and support in the above stated requirement? If it is the Service Provider, please define "as required" so that support can be properly scoped the included in our price. Does the scope of this RFP include application maintenance and database support?	The Commonwealth considers the referenced services to be a consulting level engagement that would be billable to the Commonwealth according to rate card in Schedule I. The selected Offeror must receive approval from the Commonwealth for all engagements utilizing the rate card.
45	Schedule F	3.2.4.5		How does the Commonwealth envision responsibilities for production control breaking down between the Commonwealth and the Offeror?	Please clarify the question and provide additional detail.
46	Schedule D	M13 thru M19	5 and 6	Are there or will there be any active in flight projects that may impede the Offeror's ability to execute their transition plan of record effectively? If so can the Commonwealth identify any major projects at the State or Agency level?	The Commonwealth has many active in flight projects. The impact of these projects on Offerors' proposed transition plans cannot be determined by the Commonwealth.
47	General Strategy Question			Does the Commonwealth intend to issue any additional RFP's for complementary services (e.g. Service Desk, Managed Print, Independent Validation and Verification, Desktop or Field Services) that would leverage or rely on the ITSM activities (Incident, Problem, Change, Configuration, Compliance, Capacity, SLA and Asset Management) in scope within this RFP?	The Commonwealth has no plans to release an RFP for complementary services at this time.

Addendum 8 - Round 1, Part 4					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
48	Schedule F	2.3.2	8, 9	Noting the two exceptions (Commonwealth Mainframe & SAP environments) are there any other legacy environments that will need to be transformed prior to the implementation of IPV6? What is the expectation on behalf of the Commonwealth that the O/S and applications be converted or reconfigured to IPV6 as part of the initial transition?	The Commonwealth is not ready for IPv6 at this time. Implementation of IPv6 will be a future project. The Offeror is to provide IPv4 throughout the infrastructure provided to the Commonwealth.
49	Exhibit K		11	Please provide a ticket dump for the past 6-12 months that shows ticket details.	The Commonwealth issues an average of 2,000 tickets per month. Please provide detail on the exact information requested.
50	Schedule F	2.3	7	What is meant by the word "enhanced" in the statement "enhanced disaster recovery capabilities…"?	The Commonwealth views “enhanced” as a DR service not currently used by the Commonwealth. An example of an enhanced DR service is the ability to have High Availability between geographically diverse datacenters. Offerors may propose other DR capabilities in response to this RFP.
51	Request for Proposal			Specifically what technical resources from the Commonwealth (OA and agencies) will assist with the transition? Will they be available as needed by the vendor? If not, do the penalties for missing transition dates still apply?	The Commonwealth will not identify specific technical resources at this time. The Offeror must provide an estimate of any required Commonwealth resources, including the skills needed and the duration required for each of the resources required in order for the Offeror to implement its solution. The Commonwealth expects to provide limited resources. The selected Offeror must meet the contract milestones.
52	Exhibit B.1 PSP Tab			For the two PSP partitions, can you verify the quantity, type and speed of disk interfaces?	~~The current configuration is:~~ ~~PSP Production: 6 9840C drives~~ ~~4 36 track drives (5236)~~ ~~PSP Development: 6 9840C drives~~ ~~4 36 track drives (5236)~~ ~~The Commonwealth requires the selected offeror to provide the services set forth in the RFP according to the contract terms and conditions. This existing infrastructure may not be sufficient for the long term. Offerors must determine the quantity, type, speed, etc. of the equipment required to provide the services throughout the term of the contract.~~
53	Exhibit B.1 PSP Tab			For the two PSP partitions, can you verify the quantity and type of tape drives required?	~~The current configuration is:~~ ~~* PSP Production: 4 Fibre PCI Cards SIOP Interfaces speed 2 Gb~~ ~~* PSP Development: 4 Fibre PCI Cards SIOP Interfaces speed 2 Gb~~ ~~The Commonwealth requires the selected offeror to provide the services set forth in the RFP according to the contract terms and conditions. This existing infrastructure may not be sufficient for the long term. Offerors must determine the quantity, type, speed, etc. of the equipment required to provide the services throughout the term of the contract.~~

Addendum 8 - Round 1, Part 4					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
54	Exhibit B.1 Dedicated DR Tab			For the three Dorado DR partitions, can you verify the quantity and type of tape drives required?	The current quantity and type of tape drive are: System A: 8 – 9840C drives 4 – 5236 drives System F: 8 – 9840C drives 2 – 5236 drives PSP: 4 – 9840C drives 2 – 5236 drives The Commonwealth requires the selected offeror to provide the services set forth in the RFP according to the contract terms and conditions. This existing infrastructure may not be sufficient for the long term. Offerors must determine the quantity, type, speed, etc. of the equipment required to provide the services throughout the term of the contract.
55	Exhibit B.1 DPW Tab			For the four Dorado partitions (Systems A, C, D, F), can you verify the quantity and type of tape drives required for each partition?	The current quantity and type of tape drive are: System A: 8 – 9840C drives 4 – 5236 drives System F: 8 – 9840C drives 2 – 5236 drives PSP: 4 – 9840C drives 2 – 5236 drives The Commonwealth requires the selected offeror to provide the services set forth in the RFP according to the contract terms and conditions. This existing infrastructure may not be sufficient for the long term. Offerors must determine the quantity, type, speed, etc. of the equipment required to provide the services throughout the term of the contract.
56	Schedule D,	M-13, M-14	Page 5	The dates for these milestones are given as calendar dates instead of elapsed time from contract execution. Please provide a defined number of days after the start of the contract before the penalty is considered invoked.	The dates are definite calendar dates. The date that the event must occur is not dependent upon the contract execution date.

Addendum 8 - Round 1, Part 4					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
57	Schedule F	3.2.5	134	Requirement number 2 uses the word "adequate inventory". Can this requirement for "Capacity on Demand Services" be made available in a "Public" cloud and shared with other users or is it needed in a "Private" cloud and will only be available to the Commonwealth? If a "Public" cloud is acceptable, please be aware that some of the "Mainframe server" platforms may not be readily available anywhere in a public cloud. If in a "Private" cloud only, please provide your requirements regarding your use of the word "adequate" to allow the Service Providers to meet this requirement.	The decision to use a public versus a private cloud would be a risk based decision taking in to account, at a minimum, agency, data classification, risk-level, and data value.
58	Exhibit d x edc	Exhibit D1 vs D4		3022 images (679 physical servers) ; 7936 images … why the difference in the values?	The difference is because D1 is a server inventory and D4 is an application inventory. Some servers host more than one application.
59	Exhibit B.1 DPW Tab			For the four Dorado partitions (Systems A, C, D, F), can you verify the quantity, type and speed of disk interfaces required for each partition?	The following are the current configurations: System A: 10 – Fibre PCI Cards, SIOP Interfaces – speed 2 Gb System C: 6 – Fibre PCI Cards, SIOP Interfaces –speed 2 Gb System D: 4 - Fibre PCI Cards, SIOP Interfaces –speed 2 Gb System F: 6 – Fibre PCI Cards, SIOP Interfaces –speed 2 Gb The Commonwealth requires the selected offeror to provide the services set forth in the RFP according to the contract terms and conditions. This existing infrastructure may not be sufficient for the long term. Offerors must determine the quantity, type, speed, etc. of the equipment required to provide the services throughout the term of the contract.
60	Exhibit B.1 Dedicated DR Tab			For the three Dorado DR partitions, can you verify the quantity, type and speed of disk interfaces?	The following are the current quantity, type and speed of the referenced disk interfaces: System A: 2 – Fibre PCI Cards, SIOP Interfaces – speed 2 Gb System F: 2 - Fibre PCI Cards, SIOP Interfaces – speed 2 Gb System PSP: 2 – Fibre PCI Cards, SIOP Interfaces –speed 2 Gb The Commonwealth requires the selected offeror to provide the services set forth in the RFP according to the contract terms and conditions. This existing infrastructure may not be sufficient for the long term. Offerors must determine the quantity, type, speed, etc. of the equipment required to provide the services throughout the term of the contract.

Addendum 8 - Round 1, Part 4					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
61	Exhibit B.1 Game Tab			For each of the game machines, please provide the Mip requirements and number of users, and verify the disk and tape requirements.	The following is the current information and this meets the requirements for this infrastructure: Game Production: 40 MIPS, users no limit 2 fiber PCI connections to 200 GB of disk storage 3 LTO-3 tape drives Game Test: 30 MIPS, users no limit 200 GB of internal disk storage No tape drives attached The Commonwealth requires the selected offeror to provide the services set forth in the RFP according to the contract terms and conditions. This existing infrastructure may not be sufficient for the long term. Offerors must determine the quantity, type, speed, etc. of the equipment required to provide the services throughout the term of the contract.
62	Exhibit B.1			For all Dorado and Libra systems, can you identify any required I/O throughput requirements, Request Existence Time requirements, or redundancy requirements?	The I/O throughput is application dependent based on a number of contributing variables including but not limited to the speed of the network, processors, host bus adapter speeds and other connected peripheral devices.
63	Exhibit I.1 IES - DPH COPA Owned IT Assets V1 Exhibit B.2 DPH - Commonwealth Owned DPH IT A V1	IES IES		Exhibit L1, worksheet “IES” and Exhibit B2, worksheet “IES” appear to be the same. Should the contents of both worksheets be included in the inventory?	The information provided by the Commonwealth within the referenced Exhibits must be addressed as part of an Offeror's proposal. Both exhibits (L.1 and B.2) contain the same information. They were included to provide the same information from two different points of view. L.1 is the information from the DPH point of view of Commonwealth owned assets and B.2 is from the application point of view of the infrastructure.
64	Exhibits M x DOC and Exhibits G x PSP Exhibit D.1 EDC - Server Inventory V1			It appears there is duplication in inventory between the exhibits from DOT, EDC and DOC. Which inventory or record/exhibit should be used?	The information provided by the Commonwealth within the referenced Exhibits must be addressed as part of an Offeror's proposal. The data was provided to give the Offerors points of view from several directions, such as from the agency view, from the application view, and from the datacenter view. Exhibit L = all CoPA Applications, including IES Exhibit I.2 = extract of IES Applications from L.1 Exhibit B.2 = List of physical and virtual servers and other hardware housing the I.2 applications Exhibits I.8, I.9, I.10, I.11 = list of hardware components from which B.2 systems are built.

Addendum 8 - Round 1, Part 4					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
65	Exhibit I.1 IES - DPH COPA Owned IT Assets V1 Exhibit B.2 DPH - Commonwealth Owned DPH IT A V1 Exhibit 1.8 IES - IES Technical Refresh Exhibit I.9 IES - IES Technical Refresh Exhibit I.10 IES - IES Technical Refresh Exhibit I.11 IES - IES Technical Refresh	IES IES		Should the proposal include the contents of Exhibits I.8, I.9, I.10, I.11 in addition to the inventory listed in Exhibit LI and Exhibit B2?	The information provided by the Commonwealth within the referenced Exhibits must be addressed as part of an Offeror's proposal. The data was provided to give the Offerors points of view from several directions, such as from the agency view, from the application view, and from the datacenter view. Exhibit L = all CoPA Applications, including IES Exhibit I.2 = extract of IES Applications from L.1 Exhibit B.2 = List of physical and virtual servers and other hardware housing the I.2 applications Exhibits I.8, I.9, I.10, I.11 = list of hardware components from which B.2 systems are built.
66	Schedule I	1.Volumetrics		Are the Base Units - Volumetrics for “Fully Managed” and “Managed Only” separate and stand alone? For example, there are Fully Managed Silver P-Series (AIX) LPARs = 180. There are Managed Only Silver P-Series (AIX) LPARs = 30. Are these two volumes separate for a total of 210 LPARs, or are the 30 LPARs included in the 180? It looks like they are separate and distinct, because they add up separately into the grand totals in the Schedule I pricing file. Could the Commonwealth clarify/confirm?	The information referenced is separate and stand alone; meaning the "Fully Managed" count does not include the "Managed Only" count.
67	Exhibit B.1 Dedicated DR Tab			For the equipment identified as “L1400”, can you identify the equipment type, usage, and quantity?	The L1400 consists of two (2) StorageTek L700 units. 1 - L1400 20 – 9840C tape drives 2 – LTO-3 tape drives It is used by both the Dorado and Libra mainframes located at DR.

Addendum 8 - Round 1, Part 4					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
68	Schedule J.2	SL21	4	Please provide definition around information contained in the columns titled Required and Earnback Minimum and how they relate to the SLM process.	The Offeror must provide the "Required" level of service to avoid a Service Level Default. Please refer to Schedule J.1 Section 6 for details on the Earnback methodology and process.
69	Schedule F	2.3.4	10	Please provide a list of confidential data and related applications, where they reside and their volumes. If not available, will the Commonwealth permit the incorporation of this information into line items in the service catalog and price sheets at a later time?	The Offeror should assume that all information hosted for the Commonwealth is confidential data. The service catalog should include various levels of security services for the Commonwealth to select.
70	Schedule F	3.1.2	17	Current Commonwealth ITB states that Proxy Servers must be hosted in the EDC. Relative to the requirement to propose a solution that minimizes application latency, will this ITB change and will Offerors be allowed to located the Proxy Servers anywhere they are needed?	The Offerors must follow the ITBs. The Commonwealth may consider revising this policy in the future.
71	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			What is the oldest HVAC device in operation in the data center today (i.e. CRAC, Condenser, air exchange)?	The oldest units are CRAC units installed in 1993.
72	Appendix A Exhibit D.7	13(b)	16-18	Please provide single line drawings for the electrical power systems including generators, UPS, and PDUs.	The previously provided single line electrical drawing included generators and UPS units.
73	Appendix A Exhibit D.7	13(b)	16-18	What is the floor loading capacity of the raised floor in the EDC? What is its height?	The raised floor loading capacity is 800 lbs per tile. The height of the raised floor is 2 feet .
74	Schedule I	Top	2	At the top of page 2, there is a reference to “This Exhibit B.5”. Is that correct?	~~The reference is incorrect. The correct reference is to "Schedule I.1."~~

Addendum 8 - Round 1, Part 4					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
75	Schedule F	3.2.1.7-3	58	What is considered a datacenter component as it relates to current configuration reports?	The requirement asks the Offeror to describe it process to request a report, and provide a sample of a report used on another account as part the Offeror's proposal. The Commonwealth expects a report that provides the required details to understand the information that is relevant to the component. As an example, a report for a server may contain the following information: - Server Name - applications on the server - Quantity and Speed of the network connections - Memory - Disk Space - OS - Patches - Storage type and size - Datacenter - Etc.
76	Schedule F	3.2.4	133	Is there an expected timeframe from the time the Contract starts to when Capacity on Demand services are available to the Agencies?	The selected Offeror must meet the milestones for Capacity-On-Demand as described in Schedule K.
77	Schedule D	M-14	5	What is the Offeror responsible to run in the EDC during Transition? What costs?	The selected Offeror will be responsible for services provided by the EDC once the services have been transitioned and accepted by the Commonwealth. The selected Offeror shall not charge the Commonwealth for any services currently provided by the EDC until all of the services provided by the EDC have been successfully transitioned.
78	Schedule F	3.1	12	Is the Offeror expected to reuse any Commonwealth owned hardware and software? Are there any restrictions on the reuse of Commonwealth owned hardware e.g. hardware owned by a specific agency can only be used by the owning agency?	There are restrictions on reuse of certain Commonwealth hardware and software components. The Offeror must receive prior approval from the Commonwealth before reusing any component. For purposes of submitting a proposal, Offerors should assume that no hardware or software components are available for reuse.
79	Inventory Exhibits			Could the Commonwealth provide the number of SAN ports and speed required by server?	This information, where available, was included in the Exhibits. The selected Offeror may receive additional detail from specific agencies as part of the transition planning process.
80	Inventory Exhibits			Could the Commonwealth provide the number of network ports and speed required by server?	This information, where available, was included in the Exhibits. The selected Offeror may receive additional detail from specific agencies as part of the transition planning process.
81	Request for Proposal			The RFP specifically states that any proposal must be less costly than the current as-is model. What is the current total cost of the as-is model the vendor must bid below? Does the current as-is model include any cost savings associated with reduced Commonwealth labor?	This requirement is intended to encourage Offerors to be aggressive in providing low cost / high quality services to the Commonwealth. The Commonwealth will not provide the current budget or spend on services requested within this RFP.

Addendum 8 - Round 1, Part 4					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
82	Schedule F	3.2.3	85	The contract in Appendix A has very large financial penalties associated with not compiling with the Commonwealth's security policies. Will the Service Provider be able to lock down the EDC floor space (hopefully not shared) to just those employees that are under the direct control of the Service Provider and all associated background checks have been obtained?	To a large extent, the Selected Offeror will have the ability to lock down the EDC floor space managed by the Offeror. The Commonwealth, however, requires that selected Commonwealth employees have access to this floor space. In addition, Commonwealth employees maintaining equipment in the colocation spaces will require physical access to this floor space.
83	Schedule I Offeror Pricing Form	Description and Instructions	Row 51	The Commonwealth indicates that this will be a unit-based contract. Does the Commonwealth plan to issue a pricing exhibit to explain how this will work? If not, what is the methodology that will be used to determine pricing variability? To ensure optimal pricing will the Commonwealth commit to minimum volume levels or an equitable adjustment for volumes below a certain threshold?	Unit based pricing is the concept of providing a catalog of services that provides a "unit" (of quantity one) monthly pricing that the Commonwealth can select from and order a quantity. This catalog must have the individual (unit) price components required to deliver a complete managed service. This includes, but is not limited to, units of servers, network ports, DR, SLA, storage type, Tier and quantity. The Offeror must provide unit pricing in such a way as to account for the variability's mentioned within the question. No, the Commonwealth will not commit to minimum or "Tiered" commitment levels for this procurement.
84	Schedule F	3.2.1.3	42	Pre-change test plans (bullet 3) - stipulates a test environment for any change that is being moved into production. Does this include firmware upgrades, storage changes, etc.? If that is the case, additional cost to maintain additional identical hardware platforms to test such changes would drive cost up. Please clarify.	Unless otherwise approved by the Commonwealth, the Offeror must provide a separate test environment for those changes that impact multiple environments (Dev, Test, Prod) of the same application. This includes SANs, Tape Silos, Firewalls, and other such infrastructure components. If the component supports only one environment (Dev, Test, Prod) for an application, then Offeror is not required to have separate infrastructure. All changes must follow the implementation plan approved by the Commonwealth.
85	Schedule F	3.2.4.7	128	Do optional database services include the requirement to support Unisys mainframe databases (DMS, RDMS)?	Yes, support of Unisys mainframe databases is included in these services.
86	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			Does an electrical single line drawing exist for the facility showing the utility and electrical distribution of the site? If yes, can the Commonwealth provide a copy?	Yes. Please see Exhibit D.8 - Single Line Electrical Drawing. This is a confidential document. To receive a copy, please contact Sheryl Kimport, the Issuing Officer.

Addendum 9 – Round 1, Part 5					
	Doc	**Sec**	**Pg**	**Question**	**Answer**

Addendum 9 – Round 1, Part 5					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
1	Request for Proposal			The Commonwealth is requiring consumptive-based pricing and also has not established a minimum or maximum purchase. 1) A vendor will require significant capital outlay to satisfy the requirements of the RFP. Without a commitment by the Commonwealth to purchase any level of services, this negatively impacts a vendor's ability to raise capital and also meet accounting reporting requirements mandated by the federal government. Would the Commonwealth be willing to establish a minimum purchase commitment for the 7 year contract? 2) Given agencies have a fixed budget each year for data center services, what happens when they consume in excess of their budgets? Will the vendor be impacted in any way or will the Commonwealth find the funds elsewhere?	1) No. 2) The Commonwealth is required to fund agency needs. If the funding does not meet the needs of an agency the Commonwealth will, at that time, decide the appropriate course of actions (either reduce services to reduce the costs or find the funding).
2	Schedule F	3.2.1.1.1	27	Can you please elaborate on what detailed service information will be required to ensure Commonwealth has uninterrupted flow of federal funds?	The agency invoices must include sufficient detail so the agency has full transparency into the services they consumed. This will allow the agency to apply its own cost allocation models for claiming federal funding. The Commonwealth will provide information regarding federal funding requirements during transition planning.
3	Schedule J.3	SL26	39	Please define P1, P2, P3 and P4.	"P" represents the Priority set on the incident. "P1" represents the highest priority. These are determined by the critically of the infrastructure and may be set by the reporting person.
4	Exhibit B.3 and B.4	All Tabs	All Pages	For Exhibits 3 and 4, Software is listed by Agency and by quantity, please provide a list of the Unisys mainframe software for each machine and each partition.	A new exhibit has been added to the RFP. Please see 6100022698 - Exhibit B.8 - Unisys Software - Dorado Libra contains the current software for the referenced Mainframes. This is a confidential document. To receive a copy, please contact Sheryl Kimport, the Issuing Officer.
5	Exhibit All			The Unisys billable software that runs on the mainframes (Dorado & Libra) does not seem to be identified in the software inventories. Can you verify?	A new exhibit has been added to the RFP. Please see 6100022698 - Exhibit B.8 - Unisys Software - Dorado Libra contains the current software for the referenced Mainframes. This is a confidential document. To receive a copy, please contact Sheryl Kimport, the Issuing Officer.

Addendum 9 – Round 1, Part 5					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
6	Exhibit B.3 Exhibit B.4 DPH -	UC – IBM, BOIS – IBM, DOC – IBM, DOT – IBM, REVENUE – IBM Oper.and Financial Resp.		These exhibits don't appear to provide a complete inventory (considering product inventory or version/release information of individual products) of the various software products. Will this data be updated by the Commonwealth? Additional, could the Commonwealth note if a software support agreement is currently in place with the vendor?	A new exhibit has been added to the RFP. Please see 6100022698 - Exhibit B.8 - Unisys Software - Dorado Libra contains the current software for the referenced Mainframes. This is a confidential document. To receive a copy, please contact Sheryl Kimport, the Issuing Officer.
7	Schedule F	3.1.3	18	Commonwealth States "The Offeror must address in its design how it will create a target environment that will minimize application latency concerns." If application latency issues are identified through the due diligence process and application remediation is needed will the Commonwealth take responsibility for that remediation? If that remediation causes delays in transition timeline, please provide relief to the Service Provider from committed timeline dates and credits? Regards to application performance and the potential for application/network latency, is the Commonwealth expecting application performance that will be the same as prior to the movement to a new data center model? If yes what baseline performance metrics will be used?	a) The selected Offeror must provide the infrastructure necessary to avoid latency issues. At its discretion, the Commonwealth will review the options for remediation and if it is viable for the Commonwealth to resolve the latency via a change in the application, the Commonwealth will make the change at the Commonwealth's expense. b) Transition Timelines are set out in the RFP and any changes to those dates will be addressed via the procedures set out in Appendix A (Terms and Conditions). c) The Offeror must provide infrastructure so that application performance remains the same or is improved. d) Baseline metrics are determined on an application by application basis and will be determined during transition planning.
8	Schedule F Statement of Work	Schedule F	23	How is the current geospatial enterprise environment going to be managed? Is a GIS managed services approach being considered?	a) GIS projects will be managed in the same manner as other Commonwealth projects. b) The scope of this procurement does not include outsourcing of GIS-specific services.

Addendum 9 – Round 1, Part 5					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
9	Appendix A	11 (b) (2)	13	Certification specified in this section are those held by individuals rather than the organization. What is the Commonwealth's requirement for quantity of professionals holding those certifications?	~~At a minimum, the Chief Information Security Officer (CISO) provided by the Offeror must maintain current security certifications as stated in referenced section of Appendix A. The Commonwealth has not defined the number of individuals that must hold the referenced certifications. Offerors should propose their best solutions.~~
10	Schedule J.2	SL05	3	Please confirm that there is no earn back eligibility for SL05 Application Infrastructure Availability - Basic, while there is earn back eligibility for silver and bronze levels.	Correct, there is no earn back eligibility for SL05 Application Infrastructure Availability - Basic. Silver (SL03) and Bronze (SL04) are earn back eligible.
11	Appendix A Exhibit D.7	13(b)	16-18	Will the Commonwealth make detailed EDC engineering and architectural drawings and descriptions available to Offerors? When? In what form? What will be included?	Details about the EDC facility have been provided in Exhibits D.8 through D.12. The Commonwealth will provide additional engineering and architectural drawings to the selected Offeror during transition planning. These are confidential documents. To receive a copy, please contact Sheryl Kimport, the Issuing Officer.
12	Request for Proposal			If a vendor's data center or cloud offering is shared with other non-Commonwealth clients, do all workers in the facility need the required Commonwealth security clearances or only those specifically employed to perform the Commonwealth's work?	For purposes of submitting a proposal, Offerors should assume all workers in the facility require Commonwealth security clearances. The Commonwealth, at its sole discretion, may grant exceptions.
13	Schedule F Statement of Work	Schedule F	7	How will other Commonwealth State Agency GIS project based solutions going to be managed?	GIS projects will be managed in the same manner as other Commonwealth projects.
14	Schedule J.3	SL22	34	Please define "high risk".	In the referenced section of Schedule J.3, "High risk" is a patch assigned the "Critical" Severity Rating per ITB-SYM006, which defines the Commonwealth's patching policy.
15	Appendix A	21 (b)	29	Please provide detailed information about the Commonwealth's Invoice Processing System and its invoices so that compatibility with this system can be determined.	Invoices will be processed through the Commonwealth's Remedy ITSM system's Billing Module. The current version of the Commonwealth's Enterprise Remedy is 7.6.04. The selected Offeror must remain compatible with the appropriate version of the Commonwealth's ITSM system for the duration of the contract. The billing interface currently is via an XML file transfer and processing.
16	Schedule F	2.3.4	10	What are your encryption requirements for data at rest and data in motion - e.g. FIPS 140-2?	ITBs SEC020 (Data at Rest) and SEC031 (Data in Motion) define the Commonwealth's policies on data at rest and data in motion. Agencies may have additional requirements, such as FIPS 140-2. The selected Offeror will identify additional requirements during transition for individual services and comply with those requirements.

Addendum 9 – Round 1, Part 5

	Doc	Sec	Pg	Question	Answer
17	Request for Proposal	All Exhibits		The exhibits do not provide the necessary system level software and hardware details required for the IBM/Unisys mainframes to propose a “like for like” configuration as required. Please provide the level of detail that is missing.	New exhibits have been added to the RFP. Please see "Exhibit B.8 - Unisys Software - Dorado Libra" contains the current software for the referenced Mainframes and "Exhibit B.7 - IBM MF SW Inventory v3" for additional details. Also please see the following Table SYSTEM/PARTITION HSHA HSHC HSHF HSHD IP's …… 8 4 4 4 MIPS……..…….. 1750 400 850 50 Memory (GW……..…. 4 3 2 2 CIOP (network IOP)…..…. 3 1 1 1 Ethernet PCI (dual)…..….. 12 2 2 2 SIOP (data IOP)……..…….. 3 2 2 1 FIBRE PC ICard (dual)..…. 12 5 10 5 SCSI PCI (dual)……..…. 9 5 2 5 This is a confidential document. To receive a copy, please contact Sheryl Kimport, the Issuing Officer.
18	Schedule J.3	SL16	25	Should the formula read “= ((Number of Successful Recoveries) / (Total Number of Scheduled Recoveries Attempted)) expressed as a percentage”?	No. The Offeror must report on all Recoveries attempted not just those "Scheduled".
19	Schedule F	3.2.4.6 Security and Firewall	Page 126, #6	How deep will penetration testing go on a system?	Penetration testing must be as deep as is required to ensure an acceptable security posture. Levels of penetration testing must be discussed/approved by application owners.
20	Exhibit B.1			Can the Commonwealth provide more detail regarding the IBM software running on the IBM mainframes?	Please see 6100022698 - Exhibit B.7 - IBM MF SW Inventory v3 for additional details. This is a confidential document. To receive a copy, please contact Sheryl Kimport, the Issuing Officer.
21	Schedule J			Where SLA performance depends upon Commonwealth participation, how is a delay in such participation in the performance to be considered for SLA calculation purposes? An example may be where Commonwealth participation in a project is key to meeting the schedule with a consequence for SLA 11.	Please see the definition #9 (Hold Time or Customer Time) within Schedule J.3 “Additional Definitions" section at the bottom of the schedule.
22	Schedule K	D-04 Service Continuity Architecture and Plan	18	What are the definitions of the DR Tiers (Tier 0, 1, 2, 3 and 4) mentioned in Schedule K on page 18?	Schedule F Section 3.1.3 Datacenter Architecture Requirement #5 states "Offeror must describe its tiered approach to the Disaster Recovery needs of the Commonwealth." The Offeror is to define the DR Tiers. Schedule K, item D-04, "IT Service Continuity Architecture and Plan" requires that the Offeror develop a plan to transition to the appropriate tier.

Addendum 9 – Round 1, Part 5					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
23	Schedule F	3.2.1.5.2 para #1	53	Please provide the description for DR tiers referenced as being in supporting documentation.	Schedule F Section 3.1.3 Datacenter Architecture Requirement #5 states "Offeror must describe its tiered approach to the Disaster Recovery needs of the Commonwealth." The Offeror is to define the DR Tiers. Schedule K, item D-04, "IT Service Continuity Architecture and Plan" requires that the Offeror develop a plan to transition to the appropriate tier.
24	Schedule J.1			What section describes the Tiered Service Delivery and DDR requirements to support Schedule F 3.2.1.5.2 on Page 53?	Schedule F Section 3.1.3 Datacenter Architecture Requirement #5 states "Offeror must describe its tiered approach to the Disaster Recovery needs of the Commonwealth." The Offeror is to define the DR Tiers. Schedule K, item D-04, "IT Service Continuity Architecture and Plan" requires that the Offeror develop a plan to transition to the appropriate tier.
25	Request for Proposal	PART III III-4	24-25	If the Commonwealth will not amend the Request for Proposal to include a requirement that the facilities be located within the Commonwealth of Pennsylvania then will the Commonwealth assess the cost of the lost tax revenue and lost jobs against the financial offering of the respondents who would locate outside the Commonwealth?	Schedule I defines the information that will be used to evaluate Offerors' cost submittals.
26	Schedule J.2	All	Default Remedy Type column heading	There is a (c) noted but no reference is provided to what this means. Please provide definition on item (c).	Schedule J.2 has been updated. The definition of (c) was hidden in the prior version. The definition of (c) is "Amount listed for Key Measurements to be used in the event the Key Measurement becomes a Critical Measurement through the Change Management Process. While the Service Level remains a Key Measurement no Default Remedies are due."
27	Schedule F	3.2.4.6	Page 125, Item 7	SLA reporting on server performance and availability should be addressed in section 3.2.4.4 page 115, Item 11. Please clarify that the SLAs that should be addressed in section 3.2.4.6 Item 7 should be SLs 17 and 18.	Security Infrastructure is a critical component of the Infrastructure procured by the Commonwealth. The availability of all infrastructure is included in the configuration of the application centric infrastructure and therefore this infrastructure is subject to the requirements in SL01 through SL23, SL30 and SL31.

Addendum 9 – Round 1, Part 5					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
28	Schedule I			Will the "Catalog of Services" cost sheet be used to acquire all necessary hardware and software components not included in a services provider's submitted price for a base Resource Unit? If yes, how will the Commonwealth evaluate the total cost for mainframe and AIX configurations that need to meet or exceed the performance of the current configurations on an apples-to-apples basis?	The "Catalog of Services" will be used for the Commonwealth to acquire all services from the Offeror . The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all-inclusive representation of every service desired by the Commonwealth.
29	Schedule D	M-11	4	Operational Readiness dependency listed as None under Dependency of Commonwealth. Shouldn't there be a dependency based on the acceptance component?	The "Dependency on Commonwealth" has been modified in the updated version of Schedule D.
30	Schedule J	5.1	5	Can you please elaborate on what is defined as At Risk Amount? It is unclear if it represents the total monthly Services Invoice from the Offeror.	The "At-Risk Amount" is 15% of the total monthly enterprise invoice submitted to the Commonwealth by the contractor each month.
31	Schedule F	3.2.4.7	128	Please provide a baseline of databases that need to be supported, including server platform, database vendor, database major and minor version and number of database instances.	The baseline of databases that needs to be supported are defined in the referenced section of the RFP. Additional detail will be discovered during the transition planning.
32	Schedule F	3.2.5.3	138	Please confirm that the Commonwealth is really looking for "DR Infrastructure on Demand" that implies that it will only be paid for in the event of a disaster versus paying for typical DR services. If correct, please provide your specific requirements for your use of the words "adequate inventory "as used in requirement number 1.	The Commonwealth is not looking for DR infrastructure on Demand as described within the question. The Commonwealth requires DR services to be available for any application as part of the ordered service package. On demand in this requirement indicates that the Commonwealth will change the DR requirements from time to time with or without a minimum duration.
33	Schedule J.3	SL28	42	What is the direct impact to an agency if batch processing is not started on time, but completes on time? If there is no impact in this scenario, measurement of the service level may be superfluous.	The Commonwealth requirements include both SL28 and SL29 in order to ensure that business needs are being met.
34	Appendix A Exhibit D.7	13(b)	16-18	Please provide EDC electric utility bills for the past two years.	The Commonwealth's current billing for electric utility usage is not broken out to define usage specifically for the EDC.
35	Schedule F	3.2.1.1.2	30	To better manage the costs required, please provide an indication on how governance will be applied to ensure agency compliance with enterprise direction.	The Commonwealth's Governance process is defined in Schedule B. The Commonwealth will provide a contract administrator to serve as primary contact with the selected Offeror to resolve governance-related issues.

Addendum 9 – Round 1, Part 5					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
36	Schedule F	3.3.2.1	150	Under number 16, the Offeror must make available all system management platforms and tools that are currently supporting the Commonwealth infrastructure. Can a list of the tools required be provided?	The following are application monitoring tools known to currently be in use by the Commonwealth : MS SCOM, MS SCCM, Paessler (External URL Testing), CiscoWorks, NIMS, syslog, Vmware vCenter, Idera SQL DM, Oracle OEM, Big Brother, EMC Data Protection Advisor, JC Metasys, IBM TPC, Tivoli ITCAM, SightLine, Wiley, SAP Solutions Manager, IBM Director, Nagius. For purposes of submitting a proposal Offerors shall assume none of the Commonwealth monitoring tools may be leveraged.
37	Schedule F	3.1.3.4	20	What tools and processes exist today for application monitoring that can or must be leveraged by the Offeror?	The following are application monitoring tools known to currently be in use by the Commonwealth : MS SCOM, MS SCCM, Paessler (External URL Testing), CiscoWorks, NIMS, syslog, Vmware vCenter, Idera SQL DM, Oracle OEM, Big Brother, EMC Data Protection Advisor, JC Metasys, IBM TPC, Tivoli ITCAM, SightLine, Wiley, SAP Solutions Manager, IBM Director, Nagius. For purposes of submitting a proposal Offerors shall assume none of the Commonwealth monitoring tools may be leveraged.

Addendum 9 – Round 1, Part 5					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
38	Schedule J	5.1	5	Please provide several specific examples of SLA defaults and how the default credit would be calculated, when the credit would appear on the invoice, when and if the credit could be earned back.	The following are to be used as examples only and represent a limited number of possible scenarios. The application of SLAS in the contract resulting from this RFP may vary from these examples. Assumptions used in these Scenarios: - 30 Day Month | SL03 used in all scenarios (99.900% Required & 99.400% Earnback) - Commonwealth pays $10,000 per month for the infrastructure supporting application Scenario # 1 - NO other SLA defaults have occurred within last 12 months - 2 network outages = 45 minutes + 1 server outage = 20 minutes - Total outage Minutes of 65 minutes - Availability at 99.850% (meets "Earnback Minimum" but not "Required") - Earnback eligible (Offeror must provide a report and track SLA Earnbacks) - Invoice shows $10,000 due from the Commonwealth Scenario # 2 - ONE other SLA defaults have occurred within last 12 months - 2 network outages = 45 minutes + 1 server outage = 20 minutes - Total outage Minutes of 65 minutes - Availability at 99.850% (meets "Earnback Minimum" but not "Required") - Earnback eligible (Offeror must provide a report and track SLA Earnbacks) - Invoice shows $10,000 due from the Commonwealth for current charges and $10,000 credit for previous SLA default (Earnback Credit rescinded) Scenario # 3 - 2 network outages = 45 minutes + 3 server outage = 220 minutes - Total outage Minutes of 265 minutes - NO pending Earnback for this Application - Availability at 99.378% (does not meet "Earnback Minimum" or "Required") - NOT Earnback eligible - Invoice shows $10,000 due from the Commonwealth for current charges and $10,000 credit for SLA default Scenario # 4 - 2 network outages = 45 minutes + 3 server outage = 220 minutes - Total outage Minutes of 265 minutes - Pending Earnback for this Application - Availability at 99.378% (does not meet "Earnback Minimum" or "Required") - NOT Earnback eligible - Invoice shows $10,000 due from the Commonwealth for current charges and $10,000 credit for SLA default plus $10,000 credit for failing to meet the Earnback from pending Earnback Eligible SLA default.

Addendum 9 – Round 1, Part 5					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
39	Exhibit B.1 DPH – Asset List	"GAME" Tab	Page 1,Line # 5, Line #14	For the two Unisys Libra 400 machines, please confirm (or clarify) that the Operating Systems are Windows Server (and that MCP in not used).	The Libra 400 machines operate on Windows Server 2003 R2 X64 SP2/MCP 13. MCP13 is used.
40	Schedule F	3.2.4.8	131	"Limited-Use Co-location Services." Although this section states that the Commonwealth's goal is to move to a fully managed infrastructure services model, it does not place a timeframe or amount of "Limited-Use Co-location services needed. Please provide the requirements for the amount of co-location floor space needed and the length of time that floor will be needed.	The maximum space needed to accommodate EDC Co-Location space is 3,800 sq. ft. In addition, cooling and power requirements for approximately 500 servers and storage arrays must be provided. The length of time that space, cooling and power requirements will be needed will be dictated by the business and technical lifecycle of the co-located applications and associated infrastructure.
41	Schedule I Offeror Pricing Forms	4.Managed Services (Only) 10. Catalog of Services		How do unit rates for catalog services tab #10 differ from unit rates to be provided in Managed Services tab #4?	~~The Offeror is to fill Tab #4 (Managed Services Only) with the total cost of the combined catalog items to meet the configuration defined within the Tab.~~ ~~The Offeror is to fill Tab #10 (Catalog of Services) with the individual price point / configuration items that are being offered to the Commonwealth.~~
42	Schedule I	1.Volumetrics		Does the Commonwealth need separate volume metrics for database support services or disaster recovery? Or should these services be allocated across all pricing rates?	~~The Offeror is to provide Database support services within Tab 6 (Technical Staff Rate Card) only. DR services are specified within the scenarios defined within Tab 1 (Volumetrics). Therefore, the Offeror should not allocate these services across all pricing rates. Information provided by the Offeror in Schedule I is intended for cost evaluation purposes only.~~
43	Schedule F	2.3.4	11	With regard to item 2: DBFW: What is the Commonwealth's expectation with regard to the Offeror's responsibility to Discover new databases and database objects in scope for security and compliance projects and automatically apply appropriate protection and audit policies? No, not automatically enabled on case by case basis How will the Commonwealth contribute to this effort?	The Offeror must discover and report on new databases and objects that are in scope for security and compliance projects. The Offeror should report the discoveries to the Commonwealth and take appropriate action once directed to do so by the Commonwealth.
44	Schedule J.3 Schedule F	SL20 3.2.1.2 #5	30 39	This SLA describes a Formal RCA as due in 10 days. Schedule F, section 3.2.1.2 #5 on page 39, requires an RCA within 5 days. Are these addressing the same requirement? If so, which applies?	The Offeror must provide the RCA within ten (10) Business Days from the request of the RCA. The requirement specific to delivery of the RCA report has been modified in the updated version of Schedule F.

Addendum 9 – Round 1, Part 5					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
45	EDC tour	Tour		What percent of the raised floor is open and available for additional load?	The percentage of raised floor that is open and available for additional load changes weekly based on virtualization efforts.
46	Schedule J.3	SL23	35	The calculation may incorrectly count a Change Management Request in the denominator when it may actually be scheduled in a later period. Should the formula read "=((Number of Successful Change Management Requests) / (Total Number of Change Management Requests Scheduled)) expressed as a percentage"?	The referenced formula has been modified in the updated version of Schedule J.3.
47	Schedule J.3	SL30	44	The calculation appears to incorrectly counting total reports in the denominator when some part of the total reports may actually be scheduled for delivery in a subsequent measurement period. Should the formula read "= ((Number Of Reports Delivered On Time) / (Total Number Of Reports Scheduled To Be Delivered)) expressed as a percentage"?	The referenced formula has been modified in the updated version of Schedule J.3.
48	Schedule F	3.2.1.2	38	In requirement 2, a reference to requiring Raw Data Storage (Archives) from the Service Level Management tools is required. Is there a required minimum amount of time (one month, 3 months, one year) that the archive must be online or retained to support this capability to allow Commonwealth access to the raw data?	The selected Offeror is responsible for storing raw data used to generate SLA reports for the duration of the contract plus 3 years. The selected Offeror must make that raw data available to the Commonwealth via the Offeror hosted Knowledge Management Portal for no-less than the most recent 13 months. Data older than the most recent 13 months must be provided on request in a format prescribed by the Commonwealth within 5 business days.
49	Schedule F	3.3	141	Who has the financial responsibility for 3rd party software related to the "additional licenses needed for the transition of service" as defined in this section?	The selected Offeror is responsible for the additional third-party licenses required for transition.
50	Schedule F	3.2.4.1	94	Is the Offeror expected to provide SSL hardware offloading capabilities for the web applications?	The selected Offeror must provide SSL hardware offloading capabilities for web applications. It may provide this capability with any solution that utilizes industry best practices.
51	Schedule F	3.2.3	85	When will the Service Provider be responsible for any SLAs penalties for facility failures related to the EDC facility?	The selected offeror will become responsible for the SLAs for the services provided from the EDC upon completion of the EDC transition.
52	Exhibit B.1	Mainframes - IBM	Lines 14-96	This exhibit shows the current zLinux images running for DOT. This shows fewer machines than the Schedule I Base Units -Volumetrics of 100. Could the Commonwealth please reconcile?	There are currently 93 zLinux images running for DOT. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all-inclusive representation of every service desired by the Commonwealth.

Addendum 9 – Round 1, Part 5					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
53	Schedule J.3	SL01 - SL05	9-Jan	Please list the server hardware or infrastructure characteristics that drive each of the five levels of servers and which supports the application availability SLAs. Ex.: Platinum = SAN Attached, dual HBA, dual network connections, clustered servers in an active/active configuration.	When the Commonwealth orders a service, it will work with the selected Offeror to identify the hardware or infrastructure required to support the requested SLA.
54	Schedule F	2.3.4 Data Protection	11-Oct	Is Offeror monitoring and/or reporting of confidential data usage expected for both Offeror and Commonwealth staff?	Yes, the selected Offeror will monitor and/or report on confidential data usage for both Offeror and Commonwealth staff.
55	Schedule J.3	SL22	34	Some vendors utilize Critical rather than High-Risk to denote patch risk. Are the 2 terms synonymous?	Yes. Please refer to ITB-SYM006 for the Commonwealth's patching policy. For this SLA, "high risk" is a patch assigned the "Critical" Severity Rating per the ITB.
56	Schedule F	3.1.2	18	Item 7 references CJIS data. CJIS requires encryption of user encryption keys as well as data. Whose responsibility is it to ensure such levels of security typically involving HSMs?	The requirement of the signed CJIS Security Addendum allows the responsibility to reside with a vendor on behalf of PSP. The final decision on responsibility will depend upon the proposed solution and will be discussed in more detail during the agency transition planning.

Addendum 11 – Round 1, Part 6					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
1	Schedule F	3.2.3.1	85	· Please comment on the importance (High, Medium, Low) of the following requirement of certification at the datacenters: Microsoft Gold Certified Partner, Hosting & App Services HP SP Signature Certified, Hosting Services SAS 70 Type II Certified Cisco Powered Network PCI DSS	The Commonwealth does not provide detailed evaluation criteria.

Addendum 11 – Round 1, Part 6					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
2	Security Management	3.2.2.5	76	Q1. Please define the scope of the offeror's responsibilities for the below requirement. The Offeror must support all related system audits at the Offeror's expense". "The Security Management service must ensure the confidentiality, integrity and availability of Commonwealth information and infrastructure systems. All support and implementation activities must be conducted in accordance with, but not limited to, leading industry and Commonwealth standards, which included, but are not limited to, ISO 27001:2005 and ISO 27002:2005. The Offeror must support all related system audits at the Offeror's expense". Q2. Please comment as to whether offeror is to provide assessment services regarding the security posture of each agency in order to determine its level of compliance with all pertinent laws, regulations, and policies in the current state, transition state, and final [end] state architectures…… The Offeror must work with each agency to understand and ensure compliance with all laws, regulations, and policies as it pertain to each individual agency.	Q1: The selected Offeror must provide resources, documentation, physical tours, policies, etc. to provide whatever is required for system audits at the Offerors expense. Q2: Yes, the selected Offerer must provide assessment services under agency guidance.
3	Asset Schedules	All	All	Please provide the ages of the assets or should the Offeror make a simplifying assumption such as 20 percent of the assets to be refreshed each year?	~~For the purposes of submitting a proposal Offerors should assume 20% of the assets to be refreshed each year.~~
4	Schedule F	3.2.2.4	Page 72	How many Disaster Recovery plans does the Commonwealth have in place today?	The Commonwealth has multiple disaster recovery plans in place today, utilizing multiple DR sites with varying levels of DR capabilities. Current disaster recovery needs are determined at an application level and agency DR requirements will be determined during the transition phase of the procurement. The Commonwealth's disaster recovery needs will be based on the services procured through the catalog of services.
5	Schedule F	2.3.4 Data Protection	10	Regarding encryption, where is the data that needs to be encrypted located? What platforms are involved? For data in motion is encryption required in the server and on the wire ("end-to-end")?	The Commonwealth expects the selected Offeror to determine this during transition planning in cooperation with the application/data owner.
6	Schedule F	2.3.4 Data Protection	11-Oct	What are the tools in place today for DLP and DBFW?	The current DLP solution is Cisco Ironport, which is used to monitor outbound email only. Email DLP is only in place in a limited fashion with only some small groups using DLP rules. Ironport is also used to encrypt data upon designation by the sender. There are no current DBFW tools in place.
7	Schedule F Schedule I			For those services requested in the SOW without a corresponding Baseline Units - Volumetric in Schedule I, does the Commonwealth expect those prices to be included in the Service Catalog? Without a baseline, how will the Commonwealth ensure a level evaluation between bidders? Examples of such services include: DR Planning and Testing, ERP Hosting, Security & Firewall and Database Management Services.	~~1. Yes, provide a price for all services in the catalog.~~ ~~2. The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all-inclusive representation of every service desired by the Commonwealth.~~
8	Schedule I	1.Volume metrics	Lines 216-218	The storage metrics seem inconsistent compared to today's actual allocations. Are these as desired by the Commonwealth?	The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all-inclusive representation of every service desired by the Commonwealth. Offerors must respond to Schedule I as presented.

Addendum 11 – Round 1, Part 6					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
9	Schedule F	3.1 Establish Datacenter Architecture	12	If a recompile is required is it still considered a like-for-like platform?	No
10	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			Are there any areas on the property that is restricted for locating any equipment?	Please clarify the question and provide more details or examples.
11	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			Could the Commonwealth describe the operation of the electrical system in the event of a power outage, generator failure and UPS failure?	This information is provided in Exhibit D.12 - Electrical failure sequence. This is a confidential document. To receive a copy, please contact Sheryl Kimport, the Issuing Officer.
12	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			Is there a drawing showing the locations of the PDU's/ RPP's in the data center? Can the drawing be provided for review?	Details about the EDC facility have been provided in Exhibits D.8 through D.12. This is a confidential document. To receive a copy, please contact Sheryl Kimport, the Issuing Officer.
13	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			Is there a drawing indicating the location of each CRAC unit in the data centers? Can it be provided for review?	Yes, the document exists and can be provided for review; however, it is confidential. To receive a copy, please contact Sheryl Kimport, Issuing Officer.

Addendum 11 – Round 1, Part 6					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
14	Schedule F	3.2.2.5 Security Management	76-79	a. Does CoPA have the in house skills (certified) to harvest SIEM benefits? Is a predictive monthly cost a requirement of the security environment? Does CoPA require an over SOC, single pane of glass approach? In other words, is there a method in place to map security requirements, CoPA regulatory requirements and SLA management across the contract? Does CoPA require 24x7 support? Does CoPA expect the Offeror to apply business analytics? In other word, is it expected ha intelligence to feed the ESM implementation? Who will be responsible to manage the tuning and operation of SourceFire IDS?	The Commonwealth has the in-house skills to harvest SIEM benefits. Offerors shall include security costs in the infrastructure costs. A separate charge for security is not allowed. The Commonwealth does not require an over SOC, single pane of glass approach. The Commonwealth requires 24x7 support. The Commonwealth requires the selected Offeror to apply security analytics. The selected Offeror will be responsible to manage the tuning and operation of SourceFire IDS.
15	Schedule F	3.2.1.1.1 Financial Management	27-29	i. To what extent does CoPA require a working solution for chargeback to allow States to comply with federal regulatory requirements for equality of charging for state and federal programs and justify their methodology: by not using this, are we not introducing undo risk of penalties into our bid? For example, are any of the below requirements of CoPA for Chargeback? Optimize resources by reviewing standard “Top 10” consumption reports Understand the cost details that went into the bill Understand what organization is using the most resources View invoice data online and drill down for detail information Allows client to manage chargeback system Apply price uplift to agency charges Apply additional agency or State/Company specific charges to bill Include charges for non-Offeror services for a single view of charges	The Commonwealth is not asking for a full charge back system. The agency invoices should provide billing detail so the agency has full transparency into the services they consumed. Billing details shall include all services procured by agency general ledger (GL) code. A service may be allocated across multiple GL codes. And this will suffice for equality of charging for state and federal programs. Schedule F has been revised to reflect the requirements.
16	Schedule F	3.3 Transition Services	141-155	Could the Commonwealth provide freeze periods for each agency when workloads cannot be migrated?	See Exhibit O - 2012 Agency NMRs for the No Maintenance periods that occurred during 2012. The Commonwealth cannot guarantee that the periods listed in Exhibit O will be identical during transition. This is a confidential document. To receive a copy, please contact Sheryl Kimport, the Issuing Officer.
17	exhibit n	Penndot		Is there a non-application management network for things like backup, monitoring, patching, SA access? If so, is this also a standard across the data center?	No, there is no non-application management network for things like backup, monitoring, patching, SA access, etc.
18	EDC tour	Tour handout		What is the disposition of all material in the warehouse at initiation of this contract?	The Commonwealth will relocate the material within the warehouse if requested by the selected Offeror.
19	Schedule F Statement of Work	Schedule F	23	How is the current geospatial enterprise environment going to be managed? Is a GIS managed services approach being considered?	This is an updated response to Question #8 from Round 1 Part 5. a) GIS projects will be managed in the same manner as other Commonwealth projects. The Offeror will be required to provide web servers and database infrastructure for GIS services procured through this contract. b) The scope of this procurement does not include outsourcing of GIS-specific services.

Addendum 11 – Round 1, Part 6					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
20	Request for Proposal			We understand that the Commonwealth expects the Offeror to implement a Database Firewall to help monitor privileged user and application user access. Has the Commonwealth determined the privileged user and application user groups that need to be monitored? Please provide the number of user groups that have to be monitored using DBFW to help the Offeror estimate the effort to implement?	No, the Commonwealth has not made this determination. This will be determined during transition planning.
21	Appendix A	9 (e)	11	How does the Commonwealth intend to disclose specific classification of its data to vendors to enable vendor to provide a solution which protects data based on its classification?	Data classifications are determined at agency and application level and will be determined during the transition phase of the contract.
22	Appendix A Exhibit D.7	13(b)	16-18	Please provide detailed descriptions of the EDC's mechanical/HVAC/CRAC/CRAH systems. What is the facility PUE?	Details about the EDC facility have been provided in Exhibits D.8 through D.12. This is a confidential document. To receive a copy, please contact Sheryl Kimport, the Issuing Officer.
23	Appendix A	44 (a)	68	Knowing that the PATCH background check specified in ITB-SEC009 will not report out of state infractions, will the PATCH system be the only requirement necessary for the required background checks?	No. Additional background checks must be performed to meet all requirements of the RFP, including CJIS and CHRIA requirements.
24	Schedule F	2.1	5	It states “Offeror must create and maintain test environments”; Is it mandatory for each application to have a Development, Integration, SAT/UAT, Training, Load Testing, Pre-Production and Production environments (i.e. as stated section 2.1, pg. 5) or will applications have a variable subset of these environments? What part of the volumetrics include these test environments? Which Service Tiers include these test environments?	Each application owner determines the types and counts of environments. The Offeror must be prepared to support all requested environments as ordered. The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. The Volumetrics in Schedule I will be used to evaluate Offerors’ cost proposals and are not a minimum commitment or an all-inclusive representation of every service desired by the Commonwealth. The test environment may reside in any “tier” based on the need of the application owner.
25	Schedule F	2.1	6	What is the Commonwealth expectation regarding the transformation of dedicated infrastructure to Capacity on Demand (CoD)? (rationalize)	This procurement is to provide the capability of CoD to the application owners. The application owners will determine the possibility and timeline for transformation to CoD.
26	Schedule F	3.1	13	Please define “critical Commonwealth processing”. This applies to the requirement for “each datacenter must be capable of supporting critical Commonwealth processing in the event the other datacenter goes offline”. In addition, does this requirement apply to all “critical Commonwealth processing” including those that run on IBM and Unisys Mainframes that will now require multiple platforms for those environments?	• Critical Commonwealth processing is any application determined by the Commonwealth, in its sole discretion, to be critical. For those applications with a DR subscription, the DR location must be within a geographically disperse datacenter as required by the RFP. • Yes. The platform is independent of the requirement. If DR is subscribed to for the application, then the required infrastructure must be provided by the Offeror
27	Schedule F	3.1.2, Requirement 4	17	What constitutes a "Commonwealth authorized user?" Does this include "exterior" applications that traverse the internet to gain access to Commonwealth servers and applications?	A "Commonwealth authorized user" is any user connecting to a Commonwealth resource. This does include "exterior" applications that traverse the internet to gain access to Commonwealth servers and applications
28	Schedule F	3.1.3	20	What are the specific requirements for monthly reporting of "efficiency"?	This requirement now reads "Offeror must describe its overall strategy to provide real-time scheduled system performance, operations, monitoring and capacity reporting for the entire datacenter architecture." Section 3.1.3 requirement #4 has been revised to reflect this change.

Addendum 11 – Round 1, Part 6					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
29	Schedule F	3.2.1.1.1	27	Please provide a summary of the BMC billing module (e.g., what software product) and billing format.	Invoices will be processed through the Commonwealth's Remedy ITSM system's Billing Module. The current version of the Commonwealth's Enterprise Remedy is 7.6.04. The selected Offeror must remain compatible with the appropriate version of the Commonwealth's ITSM system for the duration of the contract. The billing interface currently is via an XML file transfer and processing.
30	Schedule F	3.2.1.3	41	What are individual Agency business related change restrictions or freezes based upon the example in requirement 1?	See Exhibit O - 2012 Agency NMRs for the No Maintenance periods that occurred during 2012. The Commonwealth cannot guarantee that the periods listed in Exhibit O will be identical during transition. This is a confidential document. To receive a copy, please contact Sheryl Kimport, the Issuing Officer.
31	Schedule F	3.2.2.2 para. #3	64	To what degree may an agency delay or refuse reasonable plans and efforts to migrate their applications?	This is an internal Commonwealth management issue and will be resolved internally.
32	Schedule F	3.2.2.2-3	66	As it relates to CJIS and CHRIA requirements? Please provide all the required security and encryption requirements expected. Is the Commonwealth meeting all expected security requirements today? Are there application limitations that make meeting such CJIS requirements difficult or impossible?	1. The Commonwealth provided these details in Exhibit J.1 (Security Compliance Guidelines), Exhibit G.12 (PSP - CHRIA Handbook), Exhibit G.6 (PSP - CJIS Security Policy v5-1_07132012), and Exhibit G.7 (PSP - Summary of CJIS Requirements). This is a confidential document. To receive a copy, please contact Sheryl Kimport, the Issuing Officer. 2. Yes. The Commonwealth is meeting these requirements today. 3. No. The Commonwealth is meeting these requirements today.
33	Appendix A Schedule F	9(a), 12(d)(3), 38(c), 78(b)(1) 3.2.2.2 #3 3.2.2.5 para. 2	10, 16, 58, 93 76 66	Does the Commonwealth expect that services will be provided while meeting all potential/possible applicable regulations simultaneously? When regulations are in conflict (e.g. CJIS separation requirements) how is the applicable regulation to be determined? Which regulations apply to which part of the volumetrics provided in the Pricing Schedule? Please provide counts and the applicable segregation and separation requirements for the volumetrics.	1. Yes. 2. The agency responsible for interpreting the regulation determines how conflicts are resolved. In general, the more stringent requirement would apply. 3. The volumetric are not compiled by regulation. 4. The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all-inclusive representation of every service desired by the Commonwealth.
34	Schedule F	3.2.2.5 #3	77	How deeply and widely does the Commonwealth want quarterly penetration testing? Subset, all, targeted?	Penetration testing must be as deep as is required to ensure an acceptable security posture. Levels of penetration testing must be discussed/approved by application owners.
35	Schedule F	3.2.4.1	93	Should a Production Control Management requirement, such as 3.2.4.4 requirement 3 be included in Windows Support?	Yes. Requirement #3 in section 3.2.4.4 states the requirement applies across platforms (eg, Windows, Unix, and Mainframe).
36	Schedule F	3.2.4.1	94	Is the management or support of DNS or WINS within scope of Offeror's responsibility?	Yes, the management and support of DNS and WINS will be the responsibility of the selected Offeror.
37	Schedule F	3.2.4.1	94	Is the management or support of Public Key Infrastructure (PKI) within scope of Offeror's responsibility?	Yes, the management and support of Public Key Infrastructure (PKI) will be the responsibility of the selected Offeror.
38	Schedule F	3.2.4.1	94	Is the Offeror expected to procure, install or support SSL certificates from VeriSign or Entrust?	The Offeror must provide SSL certificates, including installation and support, as part of its Service offering through the Service Catalog.

Addendum 11 – Round 1, Part 6					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
39	Schedule F	3.2.4.4	110	Is the expectation to have the Contractor provide full management of the Batch service based upon Agency requirements or enable the Agency to use the batch software directly to schedule the batch activities?	This will be determined at an application level and both may be required based on the agency needs.
40	Schedule F	3.2.4.5	117	Provide all tools and apps currently being provided; the examples provided are not found in the exhibits identified.	The following are application monitoring tools known to currently be in use by the Commonwealth : MS SCOM, MS SCCM, Paessler (External URL Testing), CiscoWorks, NIMS, syslog, Vmware vCenter, Idera SQL DM, Oracle OEM, Big Brother, EMC Data Protection Advisor, JC Metasys, IBM TPC, Tivoli ITCAM, SightLine, Wiley, SAP Solutions Manager, IBM Director, Nagius. For purposes of submitting a proposal Offerors should assume none of the Commonwealth monitoring tools may be leveraged.
41	Schedule F	3.2.4.5	120	Requirement number 6 states “as required”. Please define as required and who will be financially responsible for providing this technical advice and support.	The selected Offeror will be responsible for providing this technical advice and support at its cost. Detailed engineering specification and assistance is considered a consulting type engagement and therefore would be chargeable to the Commonwealth from the Rate Card.
42	Schedule F	3.2.4.7	129	(4) Refer: "Provide a multi-tiered level of service (e.g. Platinum, Gold, Silver, Bronze, and Basic) for Oracle, Sybase, Microsoft SQL, IMS or DB2 database platforms." Sybase and IMS are not “current” database standard per ITB STD-INF001A. Confirm that Sybase and IMS support is required.	Sybase and IMS support is required.
43	Schedule F	3.2.4.8	131	Refer: “Currently there are to 3 areas within the Commonwealth EDC that are supporting co-location Services. EDC facility summary is provided as Exhibit D.7. While many of these systems will be migrated to a fully managed service over time, the Offeror shall plan for co-location space in its Datacenter Architecture.” Provide more details regarding the 3 areas supporting co-location services – specifically, floor space, weight, power and cooling requirements required.	Maximum space needed to accommodate EDC Co-Location space is 3,800 sq. ft. Cooling and power requirements for approximately 500 servers and storage arrays is currently in place. Additional information on the EDC environment will be determined during transition.
44	Exhibit L - Schedule F -	3.3.2.2	152	Has the Commonwealth categorized the risk levels for the applications described in Exhibit L? This will help estimate the effort required for performing the Baseline Security Risk and Vulnerability Assessment.	No, the Commonwealth has no comprehensive list of application security risk or vulnerability assessment.
45	Schedule J.3	SL20	30	The description speaks to Formal Root Cause Analysis while the calculation does not. In addition, the calculation may incorrectly include a Formal Root Cause Analysis in the total when that analysis may be due in a subsequent period. Should the formula read “= ((Number of Formal Root Cause Analysis’s Delivered within Established Interval) / (Total Number of Formal Root Cause Analysis’ Due)) expressed as a percentage”?	Schedule J.3 SL20 has been revised. The formula reads “= ((Number of Formal Root Cause Analyses Delivered within Established Interval) / (Total Number of Formal Root Cause Analyses Due)) expressed as a percentage”.
46	Schedule J.3	SL23	35	If a change is backed out due to a resulting Severity 1 or Severity 2 problem, is the change ignored for purpose of the SLA calculation?	No. Backed-out Changes due to a failure relating to the change is not considered a successful change and will not be ignored for SLA purposes.
47	Schedule J.3	SL28, SL29	42, 43	How are batch jobs that are run “as needed” to be counted for purposes of these measurements? Are they to be included in the calculation’s denominator as “scheduled”?	All batch jobs that are run "as needed" will be run at a "scheduled" time. These jobs must be included in the calculation, including the denominator as "scheduled."

Addendum 11 – Round 1, Part 6					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
48	Exhibit K		11, 12	What are the historical and expected incident handle times at the Service Desk?	This procurement includes consolidating several datacenters and each datacenter has a separate support organization. Therefore there is no consolidated historical data available. The Commonwealth is purchasing managed services as part of this procurement and incident handle times impact the availability of a service. The SLA's determine the availability requirement of the service. Therefore, differing levels of SLA availability (Platinum, Gold, Silver, Bronze and Basic) should include differing incident handle times. Each Offeror must establish "incident handle-times" to meet the SLAs for the service provided to the Commonwealth.

Addendum 11 – Round 2, Part 1					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
1	Schedule I -- Offeror Pricing Forms	Volumetrics		Is it appropriate for vendors to assume that the tapes specified in Schedule I in the Volumetrics tab are equivalent in capacity to LTO4 tapes and that vendors can propose new technology but pricing equivalent to LTO4 tapes?	For purposes of submitting a proposal, Offerors should assume the tapes are equivalent in capacity to LTO4 tapes. The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. These scenarios are for evaluation purposes only. Actual volumes will vary.
2	Schedule I – Offeror Pricing Forms	Volumetrics		Given the storage tier definition in Schedule I that indicates 10K and 15K drives in both "Tier1 Raid5" and "Tier2 Raid10", should vendors assume that the slower Tier1 RAID5 uses 10K drives and the Tier2 RAID10 uses 15K drives?	For purposes of submitting a proposal, Offerors should assume that the slower Tier1 RAID5 uses 10K drives and the Tier2 RAID10 uses 15K drives. The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. These scenarios are for evaluation purposes only. Actual volumes will vary.
3	Exhibit K	Datacenter Related Volumetrics	11,12	Of the monthly volumes listed on pages 11 &12, what percentage of these volumes are Service Requests? If zero, please provide the expected monthly Service Request Volumes that are in scope by type (i.e. ID Admin, PW Resets, etc).	The volumetric provided in Exhibit K do not differentiate between incidents and service requests. The Commonwealth is unable to provide expected monthly service request volumes.
4	Exhibit K	Datacenter Related Volumetrics	11	Of the monthly volumes listed on page 11, what percentage should the Offeror expect to receive during Prime Hours? Off-hours? Weekends?	For purposes of submitting a proposal Offerors should assume 95% are received during Prime Hours and 5% are received during off hours and/or weekends.

Addendum 11 – Round 2, Part 1					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
5	Schedule I	TAB 1 Volumetrics		For proper financial analysis of this RFP will the Commonwealth be providing the appropriate configurations in Schedule I to support the specified SLA levels mandated (Platinum, Gold, Silver, Bronze, and Basic)?	The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. Actual volumes will vary.
6	Schedule J.3	Section 2.Service Level Details		For "Managed Only" RUs where the Commonwealth has provided Commonwealth-owned infrastructure, please confirm that availability measurements will exclude issues related to Commonwealth provided assets. If Commonwealth owned asset issues are not excluded, please confirm that the Commonwealth will reconfigure hardware and/or purchase the necessary maintenance agreements to meet the various SLA tier requirements defined under "Managed Only" volumetric in TAB 4.	Availability measurements will not exclude issues related to Commonwealth provided assets. The selected Offeror must reconfigure hardware and/or purchase the necessary maintenance agreements to meet the various SLA tier requirements.
7	Schedule F	3.2.3.2	89	The Commonwealth requires the offeror to provide a structured disk-2-disk backup approach for systems that currently utilize this approach. Since there appear to be only options to provide pricing for tape, where in Schedule I should the offeror place pricing for their disk-2-disk backup approach?	~~Pricing should be provided in Schedule I, Tab 10 (Catalog of Services).~~
8	Schedule F – CoPA Datacenter Statement of Work	3.3 Transition Services	141 - 155	Is an extended, holiday weekend (3 days) considered an acceptable outage window? If not, could the Commonwealth please define an acceptable outage window?	An extended holiday weekend (3 days) is not necessarily an acceptable outage window. Acceptable outage windows will depend on the agency involved and the resources being transitioned. As indicated on Page 143 of Schedule F, "The Offeror must coordinate with each Commonwealth agency or datacenter representative to create a Facility Specific Transition Plan for each targeted facility".
9	Schedule F – CoPA Datacenter Statement of Work	3.3 Transition Services	141 - 155	Does the Commonwealth have limitations or implementation guidelines regarding DB stacking, such as multiple databases/schemas running under a single OS image and a single DB software instance?	There are no specific guidelines, but there could be restrictions in this area based on agency requirements including state or federal policy requirements for data separation. These requirements would be documented as part of the discovery process and factored into agency transition planning.

Addendum 12 – Round 1, Part 7					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
1	Request for Proposal	II-10	Page 22	What is the proposed mechanism for resolving discrepancies that result from unanswered questions, incomplete answers to questions, or discrepancies discovered during due diligence?	The governance process will be available to address these types of issues.
2	Schedule F –	3.2.4.3 ERP Hosting-SAP/Oracle	Page 105	a. If technical support of Oracle Applications software is in Offeror's scope of work then: What is the current version of Oracle Applications that has been implemented at PLCB? What Oracle modules have they implemented at PLCB? Requirement 2 (on Page 106 of section 3.2.4.3) mentions "Monitor local system operations, troubleshoot and resolve operational issues" in Schedule F. Is this monitoring restricted to the servers on which we host Oracle Applications or does this also include monitoring the Oracle Applications as well e.g. monitor system alerts, workflow alerts etc.? Requirement 7 (on Page 107 of section 3.2.4.3) mentions "Ensure server operating systems are maintained with current patch level". Is the Offeror required to patch the Oracle Application software as well? How big is the user base that needs to be supported for Oracle Applications? Please confirm that the Offeror will not be responsible for the following functions as these are not mentioned in the RFP: Maintaining application configurations for Oracle Modules that have been implemented Understand and maintain any current customizations made to base Oracle Applications Understand integration of Oracle Applications to any 3rd party systems and maintaining these 3rd party systems	a. The Commonwealth requires the selected Offeror to support PLCB's infrastructure for its Oracle ERP application. PLCB does not require application level support for this environment, so the version of Oracle in place at PLCB and the Oracle Modules in place at PLCB are not relevant to this procurement. b. Monitoring system operations in relation to this requirement is restricted to the servers on which Oracle Apps are hosted. c. The Offeror is not required to patch the Oracle Application software for the PLCB. d. The size of the PLCB's user base for the Oracle Application is 4,000 users. e. The Offeror is not required to maintain the Oracle Module configurations and is not required to understand and maintain the current customization made to the base Oracle Applications.
3	Schedule I	1. Volumetrics	N/A	Lines 195 – 202: Please provide a list of device models or actual devices that would be included in this category, and confirm that the level of support required for these devices is as described in Schedule F, Section 3.2.4.8, Limited-Use Colocation Services.	The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. Actual volumes will vary.
4	Exhibit J.1,	Maturity Level	Page 8	"The Provider is obliged to obtain a Statement on Auditing Standards No. 70 (SAS 70) II certification for the Services provided under this Agreement." When is the SAS 70 II certification due?	The requirement should refer to SSAE 16, not SAS 70. The selected Offeror must provide copies of initial and annual SSAE 16 audits pursuant to Schedule K, Section D-08, "Facilities Management Plan" for each datacenter used to service the Commonwealth at the Offeror's expense.
5	Schedule I	1. Volumetrics	N/A	Line 187-189 list GB volumes. Please provide volume allocation by Server Configuration and by Application.	The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. Actual volumes will vary.

Addendum 12 – Round 1, Part 7					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
6	Schedule I	1. Volumetrics	N/A	Line 192 list GB Stored. Please provide the daily data percent change to be backed up.	The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. Actual volumes will vary.
7	Schedule F	3.1.3 Datacenter Architecture and Technology	18-21	a. Have policies been documented, and data rationalized to the extent that we can identify Tier 3 and Tier 4 use cases (high latency) which can be moved to cheaper storage media? Is there a desire to lower the BAU base case price by implementing a pay as you go "target" storage environment for Tier ¾ which would not require capacity on the floor in the two production data centers? Does CoPA have a requirement to access their archives (search select for data) and to what extent? Does the capacity on demand solution we have in mind have encryption both at rest and in transit? Can you please quantify the filenet workload which can be moved off archivable content to save money?	a. The Commonwealth does not have documented policies or data rationalized sufficiently to identify Tier 3 and Tier 4 use cases. b. No. The Commonwealth is on a fixed budget and at this time the Commonwealth will subscribe to the amount of storage desired. c. Yes. This requirement is application dependent and is to be determining during transition. d. Please clarify this question. e. No. The Commonwealth has not quantified the filenet workload that could be moved off of archivable content.
8	Schedule F	3.3 Transition Services	141-155	Could the Commonwealth provide the acceptable outage windows for each application?	The Commonwealth is unable to provide an acceptable outage window for each application. ITB NET0015 references the methodology used to request periods of time where maintenance of Infrastructure is not to occur. Acceptable outage windows are determined on a case by case basis based on the application. Commonwealth does have several applications that are considered public safety and an acceptable outage window is less than 2 hours. However, most of the applications have out window tolerances of six to eight hours.
9	Services Catalog	Schedule C	2	Services Catalog is blank. Can you please provide a catalog of services that are relevant to this project, including GIS services?	~~This was intentionally left blank for the Offerors to provide the proposed catalog for Commonwealth review and evaluation. Schedule I tab 10. Catalog of Services has been revised to include a sample Catalog of Services. GIS projects will be managed in the same manner as other Commonwealth projects. The scope of this procurement does not include outsourcing of GIS specific services8.~~
10	General	All	All	If a Service Provider's attempt to provide a "like for like" infrastructure solution based on the exhibits is completely undersized from a capacity point of view, who will have the financial responsible to correct the deficiency, the Service Provider or the Commonwealth?	Exhibits are a point in time snapshot and are subject to change. The Commonwealth will order computing services from the Service Catalog on a subscription basis; therefore the service provided by the Contractor must meet the Commonwealth's needs as ordered.

Addendum 12 – Round 1, Part 7					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
11	Schedule F	2.3.1	8	Please provide a comprehensive list of agency requirements for multiple security and network zones?	The Commonwealth has seven (7) datacenters and each has several security zones. This information will be documented as part of the Discovery process during transition.
12	Schedule F	3.1	12	How will the Commonwealth govern requests for specific vendor technology by participating agencies especially if request are not consistent with a cost effective architecture?	The Offeror is to provide a Catalog of services from which the Commonwealth will order from. If an agency requests a service not in the Catalog, the Contract Change Process will govern requests for additional services.
13	Schedule F	3.1.1	14	Will vendor be able to consolidate workload from the EDC and agency server farm to another location?	Yes, with the application owner's approval. The Offeror must utilize the EDC as one of its datacenters and propose a minimum of one additional datacenter to meet the 2+ architecture requirement. It is the Offeror's option to utilize the EDC as one of its primary datacenters within its proposed solution.
14	Schedule F	3.1.1 para #1	13	Please define "integrated, qualified facilities".	The referenced requirement states "All Datacenters will be managed and maintained by the Offeror, including the Commonwealth's EDC and may be either a standalone facility, or integrated into existing qualified facilities." A qualified facility is any facility which meets the requirements of this RFP and is listed in Schedule E - Datacenter Locations.
15	Schedule F	3.1.3	21	Will the vendor have access to the Commonwealth's Remedy based CMDB? Does the Commonwealth's CMDB currently contain accurate inventory of all Commonwealth assets and relationships?	The intent is to share data between the Commonwealth's Enterprise Remedy's CMDB and the winning Offeror's CMDB for full visibility of the commonwealth's infrastructure for Incident, Problem, Change and Billing management. Currently, the CMDB contains only a partial inventory of the Commonwealth's assets but there is an ongoing project to improve the accuracy and to include assets not yet in the CMDB. It is not anticipated that the Commonwealth's Enterprise Remedy CMDB projects will be completed before the transition for this procurement begins.
16	Schedule F	3.2.1.1	24	Does the Commonwealth have specific requirements for interim contract management procedures which are expected to be different from final contract management procedures?	Yes, Offerors must describe interim procedures to monitor and manage service delivery while the service are being transitioned from the Commonwealth to the selected Offeror (conforming to Commonwealth policies and procedures) including but not limited to the following: Problem Management, Change Management, Service Level monitoring and reporting, physical and logical security, project management, etc.
17	Schedule F	3.2.1.1.1	27	What is the network connectivity today that connects the various state agencies back to the Federal Gov't?	It is a combination of direct links over telecommunications circuits provided by the Federal Government or over the internet.

Addendum 12 – Round 1, Part 7					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
18	Schedule F	3.2.4.3	108	(8) Refer: "User Account Management: Provide certified system administration staff to create and maintain the registration of profiles, associated groups, and the security permissions required to service the approved client base of the system and application." Confirm that Offeror is expected to support user account management within ERP application. Confirm that Offeror is expected to support user account management within applications running on Linux/AIX systems.	No, the Offeror is not expected to support user account management within ERP applications. No, the Offeror is not expected to support user account management within applications running on Linux/AIX systems
19	Schedule F	3.3.2.1	150	Is it expected that the existing service management data (e.g., incidents, change requests) will be transitioned to the Offeror's service management platform? What exact data should be transitioned to the Offeror's service management platform?	There is no expectation that this data will be transitioned to the selected Offeror's platform at this time, but if later desired, the Commonwealth will provide that information as part of transition.
20	Schedule J.1	5	5 & 6	How is the Service Level Default identified? Please provide an example.	A Service level default is defined as not meeting or exceeding the defined service level "Minimum" or "Target" as defined within Schedule J.3.
21	Schedule J.3	SL01-SL05		What is considered "available"?	Available means the system is fully functioning and not degraded.

Addendum 13 – Additional Answers					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
1	Exhibit B.1			Specific to PennDOT, is the intent to continue using the Tivoli Monitoring Environment on zLinux in the environment? If so, can the specifics of that monitoring environment be provided?	~~Yes, the intent is to continue using the Tivoli Monitoring Environment on zLinux. Please see Exhibit B.7 – IBM MF SW Inventory v3 and Exhibit N.1 – PennDOT Monitoring for additional details. These are confidential documents. To receive a copy, please contact Sheryl Kimport, the Issuing Officer.~~
2	Request for Proposal	Calendar of Events	ix and x	Can you describe the high level milestones/events after March 8th for the RFP process? (downselect process, award date and timeframe, etc)	The RFP Part III contains information on evaluation and selection. Additional information on the procurement process can be found at the DGS website. The proposal submission date has been extended. Please refer to Addendum 6 for additional information.

Addendum 13 – Additional Answers					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
3	Schedule F	3.2.1.1.1	28	Please provide specific Financial Management requirements regarding asset transfer and forecasting.	For purposes of submitting proposals Offerors should assume there will be no asset transfers. The Commonwealth foresees no asset transfers at this time related to this procurement. Forecasting should include anticipated demand for the services provided within the procurement and the associated costs. The Commonwealth requires the selected Offeror to perform the tasks and provide the deliverables detailed within this section of Schedule F.
4	Schedule F	3.2.1.1.4	32	Please provide more details around the quantity and nature of its business partner agreement connectivity support requirements expected from the Offeror.	The Commonwealth's Business Partners (BP) provide the physical circuits to the Commonwealth's BP network into the Commonwealth's co-location space within the EDC and DPH. The BP determines the number, size and redundancy of the individual BP connections. The Offeror must support these connections by providing security, access, network connections to the Commonwealth, network, floor/cabinet space, cooling, and power. Currently there are 3.5 cabinets within the Co-Lo space in the EDC dedicated to the BP containing 65 BP connections to support within the EDC. The DPH has 1 BP connection. Exhibit D.13 - EDC Business Partner Circuits contains the current list of BP circuits within the EDC and may be different at the time of transition. This is a confidential document. To receive a copy, please contact Sheryl Kimport, the Issuing Officer.
5	Schedule F	3.2.1.1.5	34-35	Pertaining to the noted requests (i.e. Cost-Benefit Analysis, Conceptualization, High Level Estimate and Technical Opinion(s)), should cost for such requests be reflected in the service catalog?	The selected Offeror will be responsible for providing cost-benefit analysis, conceptualization, high level estimates and technical opinion(s) at its cost and as part of the general provision of services. These services should not be included as standalone items in the Service Catalog. The Commonwealth considers detailed engineering specification and assistance services to be a consulting level engagement that would be billable to the Commonwealth according to the rate card in Schedule I. The selected Offeror must receive approval from the Commonwealth for all engagements utilizing the rate card.

Addendum 13 – Additional Answers					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
6	Schedule F	3.2.4.4	113	Requirement number 5 states “as required”. Please define as required and who will be financially responsible for providing this technical advice and support.	“As required” in reference to this requirement means the selected Offeror will be responsible for providing the referenced technical advice and support at its cost and as part of the general provision of services. The Commonwealth considers detailed engineering specification and assistance services to be a consulting level engagement that would be billable to the Commonwealth according to the rate card in Schedule I. The selected Offeror must receive approval from the Commonwealth for all engagements utilizing the rate card.
7	Schedule F	3.2.5	134	Item #5 states “Provide expedited service,…” please define “expedited”.	An expedited service is a deployment of an existing catalog service in an interval shorter than the standard interval. These should occur rarely, however, there may be times that this is required due to a failure of another service/equipment or a requirement set upon the Commonwealth that is outside the Commonwealth’s control, such as one set by Federal or state law.
8	Schedule F	3.3.2.1	151	What is COPA's current Chargeback System and what existing services are being charged back?	The Commonwealth does not have a common system for charge backs. Some current services are not charged back, and some are done manually. All services provided by the incumbent contractor are charged back using the Commonwealth custom ESMS system. The selected Offeror must connect to the Commonwealth’s ITSM system, which is currently BMC Remedy. The Commonwealth does not require a full charge back system. The agency invoices should provide billing detail so the agency has full transparency into the services it consumed. Billing details shall include all services procured by agency general ledger (GL) code. A service may be allocated across multiple GL codes.
9	Schedule J.1	1	3	Please provide clarification on how changes to an environment or introduction of new software would allow changes to service levels. These changes would require testing to verify environment can support new service levels.	Agencies will subscribe to Service Levels. Changes to the environment or software under the control of the selected Offeror will not change the SLA. If the Commonwealth requests a change that impacts or may impact an SLA, the Offeror must notify the Commonwealth that the SLA will no-longer be supportable and provide options to the Commonwealth for resolution before implementing the new environment or new software.
10	Schedule J.1	2.1	3	How is the complete infrastructure for an application determined for SLA purposes? How are application infrastructure components not under Offeror's control excluded from the Application Infrastructure Availability SLA?	The CMDB must include enough detailed information to allow the Commonwealth and selected Offeror to make the necessary determination. The CMDB must include all infrastructure details including components not under the Offeror’s control. Application infrastructure components not under Offeror's control will be excluded from the Application Infrastructure Availability SLA.

Addendum 13 – Additional Answers					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
11	Schedule J.1	2.1	3	The definition of "Degraded Condition" is very subjective in the absence of concrete measurements and data collection. How does the Commonwealth currently measure application degradation?	Currently the Commonwealth does not have a single standard definition for Degraded Condition. For purposes of this RFP, Schedule A - Defined Terms defines degraded condition as "A Service that tests as fully operational but is degraded below user expectations across a significant segment of the user population as determined by the Commonwealth."
12	Schedule J.3	2	5 thru 9	Per definitions SL-1 - SL-5 Application Infrastructure Availability, measurement is by application, not by server instance, however, the Offeror is not responsible for the Application. What provisions in your SLA definitions/requirements take into account infrastructure availability and application downtime due to application failure, Commonwealth activities, or Commonwealth suppliers outside the scope of this contract? Will there be 2000 Application Infrastructure Availability SLAs? What applications monitoring tools and processes exists today regarding the monitoring of availability for the 2000+ applications in scope?	The selected Offeror must provide the relationship of Infrastructure to Application within the CMDB. SL01 – SL05 take into consideration every infrastructure component for the application as related to the SLA ordered. The Offeror is responsible for the services ordered. Therefore, the selected Offeror will be responsible to make sure all of the associated services are working as designed and ordered. There will be an Application Infrastructure Availability SLA for each application. The following are known tools: MS SCOM, MS SCCM, Paessler (External URL Testing), CiscoWorks, NIMS, syslog, Vmware vCenter, Idera SQL DM, Oracle OEM, Big Brother, EMC Data Protection Advisor, JC Metasys, IBM TPC. Tivoli ITCAM. SightLine.Wiley. SAP Solutions Manager. IBM Director. Nagius. Please refer to Section 3.2.3.2 Site Operations of Schedule F; specifically requirement 1 and Section 3.2.4 for additional information.
13	Schedule K	D-02.77	14	"backup audit finding". Typically in co-location services the Service Provider is not responsible for backups. Please explain the need for this audit, and please provide the requirements for backing up co-location space if needed.	The Commonwealth EDC currently provides backup services for co-location. The selected Offeror must provide backup services as ordered. An audit is necessary for co-location services if backup service is ordered.
14	Schedule J.1-3 SLA and Schedule I			How will development and test environments be selected from the RUs? How will SLAs apply to development and test environments?	Development and test environments will be ordered from the Service Catalog and identified as application test or application development. SLAs will apply based on the SLA ordered by the application owner.
15	Schedule F – CoPA Datacenter Statement of Work	3.2.4.8	131	What services, equipment or access beyond rack space will be required in support of co-location services?	Services required to support co-location include rack space, power, network connectivity and SAN connectivity within a datacenter that meets the requirements of the RFP and is included in Schedule E - Datacenter Locations. It also includes access to the server rack for agency IT staff.

Addendum 13 – Additional Answers					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
16	Exhibit K	Datacenter Related Volumetrics	12	Are Prime Hours 0600-1800 Monday – Friday, or 7 days per week?	For purposes of submitting a proposal Offerors should assume prime hours are 0600-1800 Eastern time (Standard or Daylight Savings time, as applicable) Monday - Friday.
17	Schedule F - COPA Datacenter Statement of Work	3.2.4.1	94	We understand that the Commonwealth is considering leveraging the services of NIC for some application hosting. How does this impact the servers and services included in scope for this RFP?	The services referenced which fall under the Self-Funded EGovernment Services (44000010625) Contract held by Pennsylvania Interactive LLC may reduce the amount of infrastructure that will need to be transitioned from the EDC.
18	Schedule F – CoPA Datacenter Statement of Work	3.3 Transition Services	141 - 155	Could the Commonwealth please provide the number of landscapes per SAP application?	DOR has 5 landscapes: sandbox, development, QA, training, and production. IES's SAP ERP ECC system has 6 landscapes: sandbox, development, quality control, production support, production, and training. The other SAP applications have 5 or less depending on the SAP component and business need.

Addendum 13 – Additional Answers					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
19	Exhibit B.1 DPH Asset List Exhibit B.2 DPH Common Wealth Owned DPH IT Exhibit H.1 DOR Data Center Inventory Exhibit H.2 DOR DPH Asset List Exhibit I.9 IES Technical Refresh DP Exhibit I.1 IES DPH COPA Owned IT Assets Exhibit E.1 DLI Data Center Inventory Template			What failover technologies are deployed (active-active, active passive) and where?	Windows: All Vmware ESX are active-active in the same datacenter. AIX HACMP: PC1 CI/DB & prddb01/02 are active-active in the same datacenter and other clusters are active-passive See Exhibit I.14 IES Anticipated SLA service levels. This is a confidential document. To receive a copy, please contact Sheryl Kimport, the Issuing Officer.

Addendum 13 – Additional Answers					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
20	General Question			Regarding Commonwealth of Pennsylvania Data Center Computing Services RFP 6100022698 and the current sealed proposal submission date of Friday March 8, 2013 at 1:00pm eastern standard time, we formally requests from the Commonwealth of Pennsylvania, Office of Administration, Office for Information Technology, a 60 day extension to Wednesday May 8, 2013 at 1:00pm eastern standard time for submitting our sealed proposal response. We request this extension in order to provide the Commonwealth of Pennsylvania with the highest quality proposal response that meets all the objectives and requirements specified in RFP 6100022698 . A significant number of answers to questions asked by bidders in round one are still outstanding, having not yet been posted by the Commonwealth of Pennsylvania. In addition, the answers to questions from round two are not schedule to be posted by the Commonwealth of Pennsylvania until February 15, 2013. Answers to all questions are vital to us, in order to provide the highest quality proposal response to the Commonwealth of Pennsylvania. With the current schedule, time is of the essence given the current submission date.	The proposal submission date has been extended. Please refer to Addendum 6 for additional information.
21	Schedule A, Defined Terms	General Question	General Question	Which data centers utilize Internet service provided locally versus leveraged service from one location? What is the bandwidth and average utilization for Internet access at each location, which will need to be accommodated at the target data center?	All datacenters are connected to COPANET. The current internet connections are connected to COPANET. See Exhibit P – Enterprise Internet Bandwidth utilization. This is a confidential document. To receive a copy, please contact Sheryl Kimport, the Issuing Officer.

Addendum 13 – Additional Answers					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
22	Schedule A, Defined Terms and Schedule I , Offeror Pricing Forms	General Question	General Question	How many licensed Site to Site VPN tunnels will terminate in the EDC or Target Data Centers?	This is dependent upon the architecture provided.
23	Exhibit G.7, PSP – Summary of CJIS Requirements	General Question	General Question	Would the Commonwealth please describe the remote access systems which may be leveraged, the capacity, and how many users will require access into the EDC and Target Data Centers for PSP?	All remote access by technical staff supporting CJIS infrastructure and systems must be compliant with the CJIS Security Requirement. The Pennsylvania State Police maintains its own remote access infrastructure which is utilized for all remote access to PSP components residing in remote data centers for its technical staff and vendors supporting IT solutions. PSP's solution is a cluster of Juniper SSL VPN appliances which are maintained by the PSP Network Security Unit. Less than one hundred PSP users require access to the Data Centers.
24	Schedule A, Defined Terms	General Question	General Question	If the offeror expected to provide Internet Service at the EDC, what are the bandwidth requirements?	Internet service is already in place in the EDC. Expansion of Internet service, if required, shall be provided by the selected Offeror. See Exhibit P – Enterprise Internet Bandwidth Utilization. This is a confidential document. To receive a copy, please contact Sheryl Kimport, the Issuing Officer.
25	Schedule A, Defined Terms	General Question	General Question	What types of access and connectivity options are available to the offeror for CopaNet and at what locations?	The Commonwealth requires the selected Offeror to have at least two diverse connections to COPANET. One being EDC and the other determined during the discovery process in transition planning.
26	Schedule F, Statement of Work	3.2.3.2	88	As part of the security requirement, does all backup media need to be encrypted other than the listed CJIS and CCHRI requirements?	For purposes of submitting a proposal Offerors should assume all backup media must be encrypted.
27	Schedule F, Statement of Work	3.2.3.2	88	Would the Commonwealth please provide the current offsite storage vendor for the Commonwealth's tape/media handing?	Adaptive Data Storage, New Jersey
28	Schedule F	3.2.3.2	88	Is there any historical data that is retrieved on a regular basis? If so, would the Commonwealth please provide the typical age of the data along with the backup software and type of media?	Yes, there is historical data that is retrieved on a regular basis and is stored on primary server/storage. Typical/default retention policy for backups: Daily = 30 days Weekly = 30 days Monthly = 1 year Yearly = 7 years

Addendum 13 – Additional Answers

	Doc	Sec	Pg	Question	Answer
29	Revised Schedule F, Statement of Work	3.2.4.4 3.2.4.4	95 #1 110 #1	For servers hosted at the EDC facility, would the Commonwealth please provide the following information: • Location of the staff providing server console monitoring operations. • What systems management toolset is in place to perform server monitoring and console monitoring operations? • Who performs the console monitoring operation services? • What other duties do the console monitoring operations staff performs at the EDC facility?	The location of primary support/monitoring staff for server console monitoring operations is EDC. EDC systems management tools: MS SCOM, MS SCCM, Paessler (External URL Testing), CiscoWorks, NIMS, syslog, Vmware vCenter, Idera SQL DM, Oracle OEM, Big Brother, EMC Data Protection Advisor, JC Metasys, IBM TPC EDC console monitoring operations are performed by onsite operations staff at the EDC. Other duties include reporting, troubleshooting, patching, deployment assistance, etc.
30	Schedule A, Defined Terms	General Question	General Question	Please confirm that the offeror will not manage any network assets, belonging to the Commonwealth, outside the EDC.	The Commonwealth confirms that the Offeror will not manage any network assets, belonging to the Commonwealth, outside the EDC.
31	General Question	N/A	N/A	Would the Commonwealth list any tools or automations in place to update site content and how it avoids the manual process of updates?	Please clarify the question. The Commonwealth needs more specifics on what the Questioner means by "site content." Does "site content" refer to websites, Content Management Systems, or something else?
32	Schedule I, Offeror Pricing Forms	General	N/A	In the event Optional Services (use of Technical Rate Card) requires travel in order to perform the required services, how would the Commonwealth prefer these costs to be recovered? Is it reasonable to assume that the preferred approach would be to rebill travel expenses if and when required? If this is not acceptable to the Commonwealth, please provide the preferred approach.	~~In regard to Optional Services (use of Technical Rate Card), travel costs will be paid in accordance with Commonwealth Management Directive 230.10.~~.

Addendum 13 – Additional Answers					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
33	Schedule G, Staffing Plan and Key Positions	Sections 2 & 4	3-4	Section 2 of Schedule G has text describing positions and Section 4 has a table of positions. The 2 sections do not match. The table does not have 4 of the positions listed in the text (Availability Manager, Sr. Enterprise Infrastructure Architect, Incident Management Manager and Chief Information Security Officer) and it has 2 positions (Sales Manager and Sales Support Technical Engineers) that are not listed in the text. Can you clarify which Key Personnel are required in the proposal response?	The Commonwealth has amended Schedule G as part of Addendum 7. Please see the revised Schedule G. Also, Offerors may add additional "Key Personnel" to Schedule G outside of the required list if additional positions are critical to the proposed solution.
34	Schedule F, Statement of Work	3.2.4.1	94	What currently provided EDC application support in Managed Services is in scope of offeror's responsibility? See Q&A Round1, Part 2, #40. What agencies are the services provided for? What services are provided, for how many applications, of what level of complexity?	All of the applications in Managed Services are in scope. Agency application lists are provided in Exhibit D.4. Which applications will be provided by the selected Offeror, and their complexity, will be determined during the discovery process in transition planning.
35				In reference to Datacenter Computing Services RFP # 6100022698, we respectfully requests from the Commonwealth of Pennsylvania Office of Administration, Office for Information Technology, a 60 day extension to Wednesday May 8, 2013 at 1:00pm eastern standard time for submitting our sealed proposal response. Additionally, we respectfully request that OA IT consider providing their position on the extension request to the vendor community ASAP for planning purposes considering the considerable investment necessary to complete a high quality proposal response.	The proposal submission date has been extended. Please refer to Addendum 6 for additional information.
36	Schedule F – COPA Datacenter Statement of Work	3.2.5.5	142	Please confirm that the Commonwealth will be responsible for maintaining Desktop OS and Office versions at the required levels.	The Commonwealth will be responsible for maintaining Desktop OS and Office versions at the required levels.

Addendum 13 – Additional Answers					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
37	RFP			In reference to Datacenter Computing Services RFP # 6100022698, we respectfully request from the Commonwealth of Pennsylvania Office of Administration, Office for Information Technology, at a minimum a 90 day extension to Friday July 12, 2013 at 1:00pm eastern standard time for submitting our sealed proposal response. Additionally, we respectfully request that OA IT consider providing their position on the extension request to the vendor community as soon as possible for planning purposes considering the considerable investment necessary to complete a high quality proposal response. We are excited about the opportunity to respond to the Commonwealth's RFP for Data Center Computing Services. Our team is assembled and working through providing the State a response that addresses all facets of the RFP requirements and subsequent Q & A's. Our request for the 90 day extension is based on the following: • Finally, we recognize the Commonwealth's desire for competition which will provide the best outcome for a mutual partnership with the winning vendor/Commonwealth. With the 90 day extension the Commonwealth has our commitment that we will submit a Prime bid for the RFP with a very compelling solution, efficient pricing model and mutually beneficial small business plan. • A significant number of answers to questions asked by bidders in Round 1 are still outstanding, having not yet been posted by the Commonwealth. The questions asked pertain to items that are critical to providing a compliant, responsive and top quality proposal solution that provides maximum benefit to the Commonwealth. • Answers from Round 2 Questions are still pending. Additional questions s will most likely arise from feedback on outstanding Round 1 and Round 2 answers. Finally, we still will have to draft and submit Round 3 questions to the Commonwealth.	The proposal submission date has been extended. Please refer to Addendum 6 for additional information.

Addendum 13 – Additional Answers					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
38	Questions and Answers – Round 1 Part 3 Questions and Answers – Round 1 Part 1	28 33		Answers to these two questions appear to contradict each other. Please indicate whether the EDC must be upgraded to Uptime Institute Tier 3 equivalence in order to be used for any services. If it does not, what are the limits upon its use as a lessor facility?	The EDC does not have to be upgraded to Uptime Institute Tier 3 equivalence in order to be used for any services. Existing services provided by the EDC may remain in the EDC as long as the facility continues to meet the requirements for those services as set forth in the RFP. New applications may be added to the EDC with Commonwealth approval.
39	Questions and Answers – Round 1 Part 3	30		What represents “desired configurations”? (e.g. those represented on Schedule I “Managed Services”)	The desired configuration is the configuration as ordered by the application owner.
40	Questions and Answers – Round 1 Part 3	74 93		The answers to these questions appear to be in conflict in a requirement on the Offeror for making sure that required application changes ultimately fall on the Offeror even when the infrastructure meets the SLA requirements. Please clarify the answers. Does the Offeror have any responsibility for applications when an application modification is the means to resolving the issue?	The selected Offeror will not be responsible for modifying an application. The selected Offeror must provide the infrastructure required for the application to operate at the performance levels maintained prior to transition to the Offeror's services.
41	Questions and Answers – Round 1 Part 3	95		An arithmetic sum of availability measurements would result in availabilities higher than 100%. Please clarify on what is meant by “sum” of the infrastructure components and provide an example.	The service level calculation is " = 1 – ((Sum of Minutes the Application is not Available) / ((1440 Minutes Per Day) X (Calendar Days In Month))) expressed as a percentage". This calculation is based on the Sum of minutes the application is not available, not based on individual components.
42	General Question			The Appendix-F, Non-Disclosure Agreement HPES has signed limits our ability to share the confidential exhibits provided to HPES. We want to ensure we limit the administrative burden put on the Commonwealth. We would like to share the additional confidential exhibits with some of our Teaming Partners. Could you please provide us guidance on how we should proceed in providing certain Teaming Partners the confidential exhibits?	The confidential exhibits may be shared with teaming partners once the teaming partners have signed Appendix-F, Non-Disclosure Agreement. The teaming partners may email a scanned image of the signed Non-Disclosure Agreement to Sheryl Kimport, the Issuing Officer, at RA-OITPurchases@state.pa.us.

Addendum 15 – New and Revised Answers

Revised Answers

Revision for all previously posted answers
Revision: All references to the Commonwealth's Remedy system should reference the Commonwealth's ITSM system (currently Remedy).

Revised (original answers posted as Addendum 8 - Round 1, Part 4)

	Doc	Sec	Pg	Question	Answer
52	Exhibit B.1 PSP Tab			For the two PSP partitions, can you verify the quantity, type and speed of disk interfaces?	~~The current configuration is:~~ ~~PSP Production: 6 9840C drives~~ ~~4 36 track drives (5236)~~ ~~PSP Development: 6 9840C drives~~ ~~4 36 track drives (5236)~~ ~~The Commonwealth requires the selected offeror to provide the services set forth in the RFP according to the contract terms and conditions. This existing infrastructure may not be sufficient for the long term. Offerors must determine the quantity, type, speed, etc. of the equipment required to provide the services throughout the term of the contract.~~ **Revised Answer:** The current configuration is: * PSP Production: 4 – Fibre PCI Cards SIOP Interfaces – speed 2 Gb * PSP Development: 4 – Fibre PCI Cards SIOP Interfaces – speed 2 Gb The Commonwealth requires the selected offeror to provide the services set forth in the RFP according to the contract terms and conditions. This existing infrastructure may not be sufficient for the long term. Offerors must determine the quantity, type, speed, etc. of the equipment required to provide the services throughout the term of the contract.
53	Exhibit B.1 PSP Tab			For the two PSP partitions, can you verify the quantity and type of tape drives required?	~~The current configuration is:~~ ~~* PSP Production: 4 Fibre PCI Cards SIOP Interfaces speed 2 Gb~~ ~~* PSP Development: 4 Fibre PCI Cards SIOP Interfaces speed 2 Gb~~ ~~The Commonwealth requires the selected offeror to provide the services set forth in the RFP according to the contract terms and conditions. This existing~~

					~~infrastructure may not be sufficient for the long term. Offerors must determine the quantity, type, speed, etc. of the equipment required to provide the services throughout the term of the contract.~~ **Revised Answer:** The current configuration is: PSP Production: 6 – 9840C drives 4 – 36 track drives (5236) PSP Development: 6 – 9840C drives 4 – 36 track drives (5236) The Commonwealth requires the selected offeror to provide the services set forth in the RFP according to the contract terms and conditions. This existing infrastructure may not be sufficient for the long term. Offerors must determine the quantity, type, speed, etc. of the equipment required to provide the services throughout the term of the contract.

Revised (original answer posted as Addendum 13 – Additional Answers)

	Doc	Sec	Pg	Question	Answer
32	Schedule I, Offeror Pricing Forms	General	N/A	In the event Optional Services (use of Technical Rate Card) requires travel in order to perform the required services, how would the Commonwealth prefer these costs to be recovered? Is it reasonable to assume that the preferred approach would be to rebill travel expenses if and when required? If this is not acceptable to the Commonwealth, please provide the preferred approach.	~~In regard to Optional Services (use of Technical Rate Card), travel costs will be paid in accordance with Commonwealth Management Directive 230.10..~~ **Revised Answer:** The rates provided in the Technical Rate Card in Schedule I - Offeror Pricing Forms, should include all travel costs. The Commonwealth will not pay any travel costs in addition to the rates provided.

Revised (original answer posted as Addendum 3 - Round 1, Part 1)

	Doc	Sec	Pg	Question	Answer
134	Exhibit L - Schedule F -	3.3.2.2	152	Does the Commonwealth expect the Offeror to perform Baseline Security Risk and Vulnerability Assessment on all or just a sub-set of applications in-scope (as detailed in Exhibit L) for the Security Transition Services described in Schedule F? Please provide the list of applications that are in scope for the security assessment.	~~The Offeror must perform Baseline Security Risk and Vulnerability Assessments on infrastructure only.~~ ~~Security at OS level is performed by the Commonwealth. Commonwealth~~ **Revised Answer:** The selected Offeror must perform Baseline Security Risk and Vulnerability Assessments.

					The selected Offeror is required to perform host/network/OS level scanning and quarterly PCI scanning. OA is responsible for Web application scanning.

Revised answer (original answers posted as Addendum 4 - Round 1, Part 2)

	Doc	Sec	Pg	Question	Answer
103	Schedule J.3			The Service Level references Note 2, however, there is no Note 2 at bottom of the document. Will the Commonwealth please clarify?	~~There should not be a reference to Note 2.~~ **Revised Answer:** Schedule J.3 has been revised. The following exclusions have been identified in Note 2. Offeror's failure to achieve any Service Level will not constitute a Service Level Default or accrue toward a Service Level Termination Event to the extent such failure is directly attributable to any of the following: (i) the failure or unavailability of equipment or other resources for which the Commonwealth is operationally and managerially responsible pursuant to the Contract, (ii) changes made to the environment by the Commonwealth that were not communicated in accordance with the Change Control Procedure or other method agreed upon by the Parties, and (iii) scheduled and approved maintenance windows.
104	Schedule J.3	Metric Exclusion for each SLA		There are multiple references to Note 2, which cannot be found in the document.	~~There should not be a reference to Note 2.~~ **Revised Answer:** Schedule J.3 has been revised. The following exclusions have been identified in Note 2. Offeror's failure to achieve any Service Level will not constitute a Service Level Default or accrue toward a Service Level Termination Event to the extent such failure is directly attributable to any of the following: (i) the failure or unavailability of equipment or other resources for which the Commonwealth is operationally and managerially responsible pursuant to the Contract, (ii) changes made to the environment by the Commonwealth that were not communicated in accordance with the Change Control Procedure or other method agreed upon by the Parties, and (iii) scheduled and approved maintenance windows.

105	Schedule J.3	2	5	"Metric Exclusions" states that "all items defined in Note 2 at the bottom of this Schedule J.3." We cannot find Note 2 in this Schedule?	~~There should not be a reference to Note 2.~~ **Revised Answer:** Schedule J.3 has been revised. The following exclusions have been identified in Note 2. Offeror's failure to achieve any Service Level will not constitute a Service Level Default or accrue toward a Service Level Termination Event to the extent such failure is directly attributable to any of the following: (i) the failure or unavailability of equipment or other resources for which the Commonwealth is operationally and managerially responsible pursuant to the Contract, (ii) changes made to the environment by the Commonwealth that were not communicated in accordance with the Change Control Procedure or other method agreed upon by the Parties, and (iii) scheduled and approved maintenance windows.

Revised (original answers posted as Addendum 13 - Additional Answers)

	Doc	Sec	Pg	Question	Answer
1	Exhibit B.1			Specific to PennDOT, is the intent to continue using the Tivoli Monitoring Environment on zLinux in the environment? If so, can the specifics of that monitoring environment be provided?	~~Yes, the intent is to continue using the Tivoli Monitoring Environment on zLinux. Please see Exhibit B.7 - IBM MF SW Inventory v3 and Exhibit N.1 - PennDOT Monitoring for additional details. These are confidential documents. To receive a copy, please contact Sheryl Kimport, the Issuing Officer.~~ **Revised Answer:** Yes, the intent is to continue using the Tivoli Monitoring Environment on zLinux. Please see Exhibit B.7 - IBM MF SW Inventory v3 and Exhibit N.2 - PennDOT Monitoring for additional details. These are confidential documents. To receive a copy, please contact Sheryl Kimport, the Issuing Officer.

Revised (original answers posted as Addendum 7 - Round 1, Part 3)

	Doc	Sec	Pg	Question	Answer
45	Request for Proposal	III-4,C.1	25	Section C describes "Small Diverse Business (SDB) Participation". Section C.1 states that a business submitting a proposal as a prime contractor must perform "60% of the total contract value" to receive points for this criterion under "any" priority ranking. Does the 60% requirement stated in this section only apply to SDB that are priming this opportunity or does the 60% requirement apply to all primes contractors? If this statement applies to all prime contractors, please confirm that no SDB points will be awarded unless the prime contractor directly performs at least 60% of the total contract value of opportunity.	~~The 60% requirement stated in Part III-4 applies to all prime contractors. No SDB points will be awarded to an Offeror unless the company serving as the prime contractor directly performs at least 60% of the total contract value.~~ **Revised Answer:** The 60% requirement in Part III-4 has been deleted and Part II-9 of the RFP has been revised.
29	Appendix A	79	93	The Commonwealth has stated its requirement for fees to increase or decrease dependent on the volume consumed or variation in scope. Without a committed minimum participation or a long-range forecast of the variability of Commonwealth needs, how can a vendor commit to a fixed and ongoing financial participation to a small diverse business that may be providing these services?	~~Offerors must include a numerical percentage which represents the total percentage of the Total Base Term in the Cost Submittal that the Offeror commits to paying to Small Diverse Businesses (SDBs) as subcontractors. Per section IV of the RFP, the selected contractor's commitments to Small Diverse Businesses made at the time of proposal submittal or contract negotiation shall, to the extent so provided in the commitment, be maintained throughout the term of the contract and through any renewal or extension of the contract~~ **Revised Answer:** Part II-9 of the RFP has been revised.

New Answers

	Doc	Sec	Pg	Question	Answer
1	Schedule F	3.2.4.3	Page 105	Please clarify the intent of the ERP Hosting requirement. Does the requirement include SAP Basis support and technical application support for the Oracle Application software, or does the Commonwealth intend to retain technical application support for these items? If technical application support is to be included, is it the Commonwealth's intent to treat ERP Hosting as an optional service?	Schedule F Section 3.2.5.4 Additional Technical Services has been revised to include Basis and SAP Oracle support resources. ERP infrastructure hosting is a required service of this RFP.
2	Schedule F Schedule K	3.3 Transition Services		What assistance can be expected from the incumbent supplier during Transition? Who funds such assistance?	Under its contract the incumbent contractor is required to provide transition assistance. The selected Offeror will not be responsible to fund such assistance.
3	Schedule F Schedule I Offeror Pricing Forms Schedule J.1			There appear to be differences in storage support definitions between the SOW and Schedule I. The SOW sets forth Basic, Committed and Dedicated in section 3.1.3 on p. 20. Schedule I mentions Tier 1, 2 and 3 are associated with service levels and indicates these are defined in Schedule J.1, but they are not. However, Config 1, 2 and 3 is defined in Schedule I. Could the Commonwealth please reconcile?	~~For purposes of submitting proposals Offerors should assume the Configurations listed in Schedule I Offeror Pricing Forms are Dedicated. Schedule I has been revised to remove the "Tier" references from Enterprise Storage. Offerors should also include pricing in Schedule I Catalog of Services for Basic and Committed.~~
4	EDC tour Exhibit D.7 EDC Facility Summary and Requirements Facilities - Architecture			Are regularly scheduled full function / failure / back-up tests of the electrical systems performed? If yes, can test results be provided for review?	Yes. The results are provided in Exhibit D.15 - EDC Electrical System Testing Results. This document is confidential and to receive a copy, please contacts Sheryl Kimport Issuing Officer of IT Procurement.
5	Schedule F	3.1.3 Datacenter Architecture and Technology	18-21	a. Is the expectation that the Offeror will provide an out-of-region solution, so CoPA will not be affected by a regional disaster? b. Concerning the Disaster Recovery Exhibit, does CoPA have documented RPOs and RTOs for its critical applications? c. Can CoPA provide a list of applications with documented dependencies? d. This list, if it exists, was it gathered manually or through the application of automation? e. Can CoPA elaborate on their requirements for the "tiers of service" they expect, the volumes of applications they apply to, and the associated RTO / RPO's? f. Is the Offeror expected to document an overall	a. The purpose of a 2+ datacenter configuration and requiring a minimum of 50 miles between datacenters is intended to mitigate the impact of a regional disaster. b. See Exhibit B.9 – DPH – Recovery Time Objectives for a list of RTOs for applications in the DPH. The Commonwealth does not have RPO documentation. This information will be documented as part of the discovery process in transition planning. Exhibit B.9 – DPH – Recovery Time Objectives is a confidential document. To receive a copy, please contact Sheryl Kimport, the Issuing Officer. c. Application dependencies will be documented as part of the discovery process in transition planning. d. See answer to c.

				resiliency strategy and design as a part of due diligence so that each tier of service has been adequately designed into the data center architecture? g. Is the Offeror expected to document an overall resiliency strategy and design as a part of due diligence so that each tier of service has been adequately defined? h. Is the Offeror responsible to develop effective disaster recovery, business continuity and crisis plans as well as conduct testing during due diligence for the critical applications?	e. Section 3.1.3 of schedule F refers to "Multi-Tiered Storage Management". It is defined in section 3.1.3 as: • Basic – based on Pay-As-You-Go allocation model with no upfront resource allocation and resources are reserved on demand per workload. (shared, multitenant) • Committed – based on Allocation Pool allocation model which gives a minimal initial commitment of resources plus the ability to burst above that minimum if additional capacity is needed – usually a percentage of resources reserved for agency with over-allocation. (shared, multitenant) • Dedicated – based on Reservation Pool allocation model – 100% of resources are reservation–guaranteed. (dedicated, single tenant) The Commonwealth cannot provide the volume of applications these tiers apply to. The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all inclusive representation of every service desired by the Commonwealth. See answer to b. for RTO/RPOs. Any additional information needed will be documented as part of the discovery process in transition planning. f. Yes, the Offeror is expected to document an overall resiliency strategy and design, so that each tier of services has been adequately designed into the data center architecture. The strategy and design must be reviewed and approved by the Commonwealth prior to implementation. g. See answer to f. h. Yes, See section 15. Disaster Recovery and Business Continuity of Appendix A.

6	Schedule F	3.2.5 Capacity on Demand Services	133-141	a. Does CoPA desire to better manage their capacity plan by having an online data backup capability that can flex as the information requirements expand over the next several years so capacity at the production centers does not have to be added? Does CoPA have detailed knowledge of their data access patterns to provide to a vendor who can then determine what data is eligible to move from tape to online storage, at a lower cost with greater backup recovery success rates then tape? Does CoPA have a written archiving policy, and does it currently move fixed data regularly to lower cost storage? Does CoPA have a requirement for Virtual Server Recovery outside of the primary geography?	~~a. The Commonwealth seeks the best solution for capacity planning. Offerors should include the services they offer in their technical proposal and as part of Schedule I tab 10. Catalog of Services.~~ ~~b. No, the Commonwealth does not have data access patterns to provide to an Offeror. The Commonwealth will work with the selected Offeror to determine the best solution when selecting services from the Service Catalog.~~ ~~c. The Commonwealth currently has a written archiving policy. Fixed data is currently moved regularly to lower cost storage.~~ ~~d. Please clarify or provide example defining "Virtual Server Recovery outside of the primary geography"~~
7	Request for Proposal			How are agency schedule needs accommodated in the instance where those needs will delay or cause the delay in deliverables and milestones?	Identifying these impacts is to be part of the transition planning and need to be taken into consideration by the Offerors in their planning. The agencies have several regularly scheduled "No Maintenance" periods every year. See Exhibit O - 2012 Agency NMRs for the No Maintenance periods that occurred during 2012. See Exhibit R - Transition Considerations for information on identified considerations which could impact transition planning. These are confidential documents. To receive a copy, please contact Sheryl Kimport, the Issuing Officer.
8	Appendix A	7	8	This section states “At its sole cost and expense, Contractor shall maintain the Commonwealth Machines and shall replace each Commonwealth Machine at its respective end of life or as otherwise required to provide the Services.” Will the Commonwealth be providing details on purchase date, warranty, and “end of life” for all systems currently owned by the Commonwealth that will be assumed under this contract?	Exhibit D.1 - EDC - Server Inventory and Exhibit D.14 - EDC Hardware Warranty Information provide information on warranty and maintenance for the equipment in the EDC. Any additional information needed will be documented as part of the discovery process in transition planning. The EDC is the only datacenter which the Offeror will take operational control. These are confidential documents. To receive a copy, please contact Sheryl Kimport, the Issuing Officer.

9	Appendix A Exhibit D.7	13(b)	16-18	What are the typical calendar/schedule limitations for major facility or system work? What are any lockdown/blackout periods?	Identifying schedule limitations for major facility or system work will occur during transition planning. The Commonwealth does not have enterprise-wide "No Maintenance" periods. Each "No Maintenance" period is requested and scheduled by the individual agency. Please refer to ITB-NET015 which describes the process for requesting a "No Maintenance" period and the Commonwealth's approved Enterprise Maintenance Windows. The agencies have several regularly scheduled "No Maintenance" periods every year. See Exhibit O - 2012 Agency NMRs for the No Maintenance periods that occurred during 2012. See Exhibit R - Transition Considerations for information on identified considerations which could impact transition planning. These are confidential documents. To receive a copy, please contact Sheryl Kimport, the Issuing Officer.
10	Schedule F	2.3.4	10, 11	With regard to item 1: DLP (Data Loss Prevention) What is the Commonwealth's expectation with regard to the Offeror's responsibility to "Discover confidential data wherever it is stored, inventory sensitive data, and automatically manage data cleanup" as well as "identify" sensitive and confidential Citizen Personal Identifiable Information (PII) within the Commonwealth's databases, DNS and file systems? How will the Commonwealth contribute to this effort?	The parameters for confidential information will be documented as part of the discovery process in transition planning. The selected Offeror must discover any confidential information that is outside parameters defined by the Commonwealth. The selected Offeror must inform the Commonwealth of any information that is discovered to be outside the parameters defined by the Commonwealth. The Commonwealth will give guidance on resolution of any information which is discovered to be outside the established parameters.

11	Schedule F	3.1.1.5	14	Reference: "The current maintenance contract for the EDC servers is scheduled to expire on June 30, 2014." Confirm that all server maintenance in the EDC is scheduled to expire on 6/30/2014. What about other hardware in the EDC such as storage units, tape drives, etc.? Will the Offeror be financially responsible for maintenance on all data center components including those owned by the Commonwealth?	Not all server maintenance in the EDC is scheduled to expire on 6/30/2014. The server maintenance contract is dynamic. As manufacturer warranties expire, those servers are added to the extended maintenance contract if they are still in use and not refreshed. As servers retire or are refreshed, they are removed from the extended maintenance contract. The Offeror must maintain either the manufacturer's warranty or extended maintenance for all equipment in the EDC. Yes, the selected Offeror will be financially responsible for maintenance on all data center components in the EDC. Exhibit D.1 - EDC - Server Inventory and Exhibit D.14 - EDC Hardware Warranty Information provide information on warranty and maintenance for equipment in the EDC. Any additional information needed will be documented as part of the discovery process in transition planning. These are confidential documents. To receive a copy, please contact Sheryl Kimport, the Issuing Officer.
12	Schedule F	3.2.1.3	42	As it relates to testing infrastructure changes. What is the criteria by which testing environments must be maintained? Must new hardware be tested in a separate 'testing environment' prior to implementation? Is testing in a 'Test environment that my not 100% match production sufficient for testing, or are model office environments that 100% match production required? Is such testing required for antivirus updates?	Unless otherwise approved by the Commonwealth, the Offeror must provide a separate test environment for those changes that impact multiple environments (Dev, Test, Prod) of the same application. This includes SANs, Tape Silos, Firewalls, and other such infrastructure components. Offerors should assume that a test environment must be a 100% match of the production environment; unless the Commonwealth approves a lesser environment for testing. If the component supports only one environment (Dev, Test, Prod) for an application, then Offeror is not required to have separate infrastructure. All changes must follow the implementation plan approved by the Commonwealth.
13	Schedule F	3.2.1.4	44	Do the agency help desks have security restrictions that will need to be remediated to support connectivity?	Yes. Firewall and other security adjustments will be necessary for the Offeror to interface with the agency help desks.
14	Schedule F	3.2.1.5.1	52	What percentage or number of physical hosts in the baseline count are VM hosts, or are they not counted in the physical server count?	The number of physical hosts and VM hosts will be documented as part of the discovery process in transition planning.

15	Schedule F	3.2.1.6	55	(2) Reference: "Assign an Account Manager to each identified agency." Please provide a list of all agencies in scope.	Offeror will provide a minimum of five (5) dedicated Agency Account Managers responsible for understanding all of the services provided by Offeror and providing guidance to the agencies in understanding their datacenter business needs. Offeror must assign an Agency Account Manager to each agency that purchases services through the contract. Not all Agency Account Managers must be assigned to a single agency.
16	Schedule F	3.2.1.8.3	60	This section states that “the Offeror will be solely responsible for the management of all infrastructure software products provided through this contract”. Please explain the use of the words “the management” as required in this section. Who is financially responsible for the installation, troubleshooting, and maintenance of the 3rd party software described in this section?	The Commonwealth is subscribing to managed infrastructure services; therefore, the selected Offeror is responsible for providing and managing the infrastructure and the software needed to operate that infrastructure. This includes licenses, patches, updates, maintenance, etc. Financial responsibility for Third party software is set out in Appendix A - Data Center RFP Terms and Conditions.
17	Schedule F	3.2.2.2	64	This section states “Offeror must work with the Commonwealth agencies to understand the systems involved, and the timeframe of these migrations”. If there are specific and known requirements for agency timelines, please provide those details.	Identifying agency timeline needs is to be part of the transition planning and need to be taken into consideration by the Offeror during development of the detailed transition plan. The Commonwealth does not have enterprise-wide "No Maintenance" periods. Each "No Maintenance" period is requested and scheduled by the individual agency. Please refer to ITB-NET015 which describes the process for requesting a "No Maintenance" period and the Commonwealth's approved Enterprise Maintenance Windows. The agencies have several regularly scheduled "No Maintenance" periods every year. See Exhibit O - 2012 Agency NMRs for the No Maintenance periods that occurred during 2012. See Exhibit R - Transition Considerations for information on identified considerations which could impact transition planning. These are confidential documents. To receive a copy, please contact Sheryl Kimport, the Issuing Officer.

18	Schedule F	Section 2.1 Section 3.2.3(3)	6 85	Which of the Uptime Institute's measures for Tier 3 are required to meet the standard for Tier 3 equivalence? (Tier 3 design, Tier 3 operations, etc.) Will the standard to be used include any optional measures or only minimum requirements? Requirement 2 states "Provide fully redundant environmental Services. To include, but not limited to, HVAC, UPS, conditioned power and distribution, generator backup, automated transfer switch, fire suppression system". Is this requirement for all other facilities other than the EDC or must the Service Provider upgrade the EDC, at their cost, to provide this requirement?	The Offeror must meet two Uptime Institute, LLC Tier III Data Center Site Infrastructure Tier Standards. The first standard is "Data Center Site infrastructure Tier Standard: Topology" at a Tier III level. The second standard is "Data Center Site infrastructure Tier Standard: Operational Sustainability" at a Tier III level. These standards can be found at the Uptime Institute, LLC's website -http://uptimeinstitute.com/. The Offeror must meet the minimum requirements to be considered compliant with the requirement. This requirement applies to all datacenters hosting Commonwealth applications. If, at any time, the selected Offeror determines a datacenter is not compliant with the minimum Tier III requirements, the Offeror must document and report to the Commonwealth, the noncompliance for a determination on possible resolutions. For the purposes of submitting a proposal, the Offerors are to assume that the EDC is compliant with the minimum requirements of a Tier III datacenter.
19	Schedule F	3.2.5	133	We understand the requirement for "short-term" needs as described in this section for IaaS. Please be aware that most 3rd party software for Unisys and IBM mainframe is not available for use in an "On-Demand" model. Please explain how the Commonwealth will acquire the necessary 3rd party software license upgrades to accommodate this requirement and who will have the financial responsible to manage this short-term need.	The Commonwealth is procuring managed services through this RFP. The selected Offeror is responsible for managing the infrastructure and the software needed to operate that infrastructure. This includes licenses, patches, updates, maintenance, etc. for the referenced mainframes. The selected Offeror will have the financial responsibility to manage a short term need.
20	Schedule F	3.3.2.1	150	What is the expected transition timeframe and associated acceptance criteria for all the existing agency service management systems to the Offeror's service management platform?	~~See milestone M-9 ITSM System Integration in Schedule D - Transition Milestones~~

21	Schedule I	TAB 1 Volumetrics		Was the intent to have rounded units in the Volumetrics? The Commonwealth has used a formula to increase/decrease each category of units which leaves partial Servers, GB, etc. After Year 1 Volumes, the Servers/Unix counts are adjusted by a formula that leaves partial devices, which will impact the Total Charges tab because it multiplies PxQ and Q won't be a whole number.	Schedule I - Offeror Pricing Forms has been revised to include rounded units.
22	Schedule I	TAB 1 Volumetrics		There are a number of configurations defined (i.e. Unisys DR Mainframe Config 3 and 4, IaaS Linux/Windows Config 4 and 5) in TAB 1 without corresponding Baseline Unit Volumetrics. Where should the Offeror provide pricing for these configurations and what baseline volumetrics should be used?	Schedule I has been revised to include volumetrics for the referenced configurations. The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. The volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all inclusive representation of every service desired by the Commonwealth.
23	Schedule F	3.2.3.2	88	What is the peak number of batch jobs that need to run in a 24 hour period by agency across all platforms (IBM Mainframe, Unisys, Mainframe, AIX, Windows, etc.)?	The peak number of batch jobs needed in a 24hr period is unknown. The Offeror will be responsible for the batch jobs based on the needs of the agency. This will be documented as part of the discovery process in transition planning.
24	Appendix A	14 (c) (ii)	21	Commonwealth requirement "In contractor's performance and completion of Transition Services, no functionality of the Commonwealth's then current business operations or environment will be discontinued until contractor demonstrates to Commonwealth's reasonable satisfaction that the affected processes and operations have been successfully migrated to contractors target environment and are functioning properly in that environment." This requirement could imply that existing assets cannot be relocated and any proposed application migrations would need to use new or alternative infrastructure to maintain functional parallel application environments. If so, this would impact a service provider's ability to use a lower cost "lift and shift" migration strategy and Server – Managed Only pricing. Is that your intention? Will the Offeror be permitted to relocate the Commonwealth-owned existing hardware platform supporting an application if the hardware has useful life remaining? If agreed by the Commonwealth on a case-by-case basis, can an agency application platform	The Commonwealth does not own all of the infrastructure within the scope of this RFP. Therefore, "lift and shift"is not an option in most cases. For purpose of submitting a proposal, Offerors should assume no assets can be relocated. On a case-by-case basis and with agency approval, an agency application platform may be shut down, packaged, physically relocated to a new data center, and reactivated at the new data center location. For purposes of submitting a proposal, Offerors should, however, assume that no agency assets can be relocated.

				be shut down, packaged, physically relocated to a new data center, and reactivated at the new data center location?	
25	Schedule F - COPA Datacenter Statement of Work	3.3.2.2 3.2.2.5	152 77	In response to Q 134 of Addendum 3 Q&A round 1 part 1, the Commonwealth indicated the Offeror has to perform infrastructure vulnerability testing only. Whereas, in response to Q65 of the Addendum 4 Q&A round 1 part 2, the Commonwealth indicated that the Offeror needs to perform all types of penetration testing including "applications". Can the Commonwealth clarify if the Offeror is required to perform web application vulnerability testing as part of the Baseline security risk and vulnerability assessment and/or the Quarterly vulnerability scan?	The selected Offeror is required to perform host/network/OS level scanning and quarterly PCI scanning. OA is responsible for Web application scanning.
26	Schedule I – Offeror Pricing Forms	Volumetrics		Does Schedule I's volumetrics for physical and virtual servers account for the planned technology refreshes in Commonwealth-owned assets to be migrated from "Co-Lo" or "Managed Only" to "Fully Managed"?	No, the volumetrics provided do not account for planned technology refreshes. It is specifically for pricing evaluation, as set forth in Schedule I. Actual volumes will vary.
27	Schedule I – Offeror Pricing Forms	Managed Services		The Commonwealth has indicated that Contract signing = Effective Date = Start date. The Commonwealth has also stated that Transition is part of the base term of the contract and transition is prior to Steady State. Can "Transition Charges" be billed prior to the DPH/EDC being fully migrated and/or prior to December 31, 2014? If Steady State RU's are not "available" until the DPH/EDC have been fully migrated (which is required by 12/31/14) do the Volumetrics not come into play until 1/1/15 or can RU pricing begin with a fully migrated DPH/EDC and prior to 1/1/15?	~~Schedule I – Offeror Pricing Forms has been revised. Transition costs are now deliverable based and cannot be billed until the Commonwealth accepts the deliverable and all associated milestones. Refer to Schedule D – Transition Milestones and Schedule K – Key Program Deliverables which set forth acceptance criteria and due dates.~~ ~~Applications cannot be billed until the application has been fully transitioned to the Offeror and accepted by the Commonwealth.~~

28	Schedule I – Offeror Pricing Forms	Volumetrics		The current configurations for x86 and pSeries resource units at the service level tier Platinum are incapable of meeting the SLA measurement for infrastructure at 99.999% availability. In the absence of pConfigs that support clustering configurations, how does the Commonwealth wish to deal with the discrepancy?	Schedule J.3 - Datacenter SLA Definitions has been revised to exclude scheduled and approved maintenance windows in availability SLA calculations. Please provide clarification on why the current configurations for x86 and pSeries resource units at the service level tier Platinum are incapable of meeting the SLA measurement for infrastructure at 99.999% availability.
29	Schedule D – Transition Milestones	M-11	4	Please define “operational readiness”. What demonstrates that the facility is “ready”?	Operational readiness is determined by the Commonwealth’s acceptance of the Operational Readiness Report indicating Offeror is ready to transition the Commonwealth’s Applications and Services to other Datacenters.
30	Schedule I – Offeror Pricing Forms	Volumetrics		Do the numbers of servers for x86 configurations 4 and 5 relate to current equipment dedicated to DR? If not, how quickly will a maturing DR posture begin to reach or surpass these levels?	No, the numbers of servers for x86 configurations 4 and 5 do not relate to current equipment dedicated to DR. The Offeror must provide the DR posture ordered by the Commonwealth. Since the infrastructure is to be transitioned to the Offeror's datacenter(s), the maturity of the Commonwealth's DR equipment is irrelevant to the Offerors ability to submit a proposal. Please clarify the question.
31	Exhibit B.4			Does the Offeror have to provide a price for the software listed in Exhibit B.4? If so, where does the Offeror provide a price for third-party software?	~~Schedule I – Offeror Pricing Forms has been revised to include software pricing as part of the Catalog of Services tab.~~
32				Do regulations related to Board of Elections data require that all such data remain within the Commonwealth at all times?	There are no requirements for Board of Elections’ data to remain within the Commonwealth. The data must meet the data protection standards specified in the RFP. The specific requirements for Board of Elections data will be documented as part of the discovery process in transition planning.

33	Exhibit K Schedule J.3 Datacenter SLA Definitions	Datacenter Related Volumetrics SL26	11,12	Of the monthly volumes listed on pages 11 & 12 in Exhibit K, please provide an expected volume breakdown by Priority for Service Incidents and Service Requests so that Offeror can match these volumes to the required SLAs in Schedule J.3: Service Restorals P1: every 15 minutes P2: 30 minutes P3: daily P4: weekly Service Requests P1: Daily P2: Weekly P3: every 2 weeks P4: Monthly	Expected volume breakdown by Priority for Service Incidents and Service Requests will be documented as part of the discovery process in transition planning.
34	Answers to Questions Round #1, Part #2	Q40		Currently EDC provided managed services support includes responsibility for application installation, application support, application troubleshooting, application monitoring, etc. The Commonwealth response to this question implies that application support is in scope for the Offeror. This contradicts with responses to Q 136 and 139 in Round #1, Part #1, which indicate that the Offeror is only responsible for infrastructure. Please clarify.	Currently in Exhibit D.4 - EDC - Application Server Agency Report, applications identified a “MSL” are considered managed service lite. All other applications are fully managed. The services considered managed services lite today would require infrastructure support and not application level support. Fully managed services require the Offeror to provide infrastructure and application level support.
35	Schedule J.3	Section 2.Service Level Details	5-9	For SLAs SL01-SL05, please confirm that the measure of application availability will exclude downtime associated with problems related to Commonwealth application programs and/or any items not under the direct control of the infrastructure and or services being provided by the service provider.	Schedule J.3 has been revised. The following exclusions have been identified. Offeror’s failure to achieve any Service Level will not constitute a Service Level Default or accrue toward a Service Level Termination Event to the extent such failure is directly attributable to any of the following: (i) the failure or unavailability of equipment or other resources for which the Commonwealth is operationally and managerially responsible pursuant to the Contract, (ii) changes made to the environment by the Commonwealth that were not communicated in accordance with the Change Control Procedure or other method agreed upon by the Parties, and (iii) scheduled and approved maintenance windows

36	Appendix A	9(a)	10	As it pertains to this section, "(a) Commonwealth will retain administration of logical and data access security, and Contractor will host Commonwealth security applications software utilized by the Commonwealth in managing logical and data access security, and will not implement configurations that would prevent Commonwealth from managing logical and data access security." Is it the intention of the Commonwealth to control "privileged Root and Admin logon and rights" to servers managed by the Offerer or will "privileged Root and Admin logon and rights" to be controlled by the Offerer? Or, is it the intention of the Commonwealth to control "privileged Root and Admin logon and rights" to servers managed by the Offerer will the Commonwealth agree to restrict such access to only those authorized by the Offerer? Or, is the intention of the Commonwealth to control "privileged Root and Admin logon and rights" to servers managed by the Offerer and not agree to restrict such access to only those authorized by the Offerer, and allows administrative access to Commonwealth or other parties for a managed server, that the Commonwealth agrees to waive any and all SLA's for failures resulting from said access?	The Offeror will be required to manage/control/monitor "privileged Root and Admin logon and rights". The Commonwealth and the selected Offeror will establish an approved process for Commonwealth staff to request "Privileged" access. This process will be documented in the CCPM. Schedule J.3 - Datacenter SLA Definitions has been revised to include exceptions to SLAs.
37	Schedule F	3.2.4.4 & 3.2.4.5	105&111	Is the offeror responsible for performing batch job scheduling functions in a batch scheduling system or will scheduling continue to be performed by the agency with the offeror managing and monitoring batch execution only?	Responsibility for batch processing is determined at an application level and will be documented as part of the discovery process in transition planning. For purposes of submitting a proposal, Offerors should assume the selected Offeror will be responsible for batch job scheduling in a batch scheduling system.
38	Schedule F – CoPA Datacenter Statement of Work	3.3 Transition Services	141 - 155	Does the Commonwealth have a suggested migration/wave schedule for the agencies?	The Commonwealth does not have a suggested migration/wave schedule for the agencies. Transition Milestones are defined in Schedule D - Transition Milestones. Offerors are to propose a transition plan to meet those requirements.

39	Schedule F – CoPA Datacenter Statement of Work	3.3 Transition Services	141 - 155	Do the individual agencies have change freeze periods or business black-out dates that require consideration? If yes, what are they?	Identifying specific agency scheduling needs will be part of the transition planning. The Commonwealth does not have enterprise-wide "No Maintenance" periods. Each "No Maintenance" period is requested and scheduled by the individual agency. Please refer to ITB-NET015 which describes the process for requesting a "No Maintenance" period and the Commonwealth's approved Enterprise Maintenance Windows. The agencies have several regularly scheduled "No Maintenance" periods every year. See Exhibit O - 2012 Agency NMRs for the No Maintenance periods that occurred during 2012. See Exhibit R - Transition Considerations for information on identified considerations which could impact transition planning. These are confidential documents. To receive a copy, please contact Sheryl Kimport, the Issuing Officer.
40	Schedule F – CoPA Datacenter Statement of Work	3.3 Transition Services	141 - 155	Could the Commonwealth please provide the number of images considered: 1) Critical Virtual Images (virtual servers with an outage window tolerance of less than 24 hours and significant business impact); 2) Critical Physical Images (non-virtual servers with an outage window tolerance of less than 24 hours and significant business impact)?	The Commonwealth cannot provide the number of images considered Critical Virtual Images or Critical Physical Images. The criticality of a virtual server will depend on agency requirements and will be documented as part of the discovery process in transition planning. The criticality of a physical server will depend on agency requirements and will be documented as part of the discovery process in transition planning.
41	Schedule F – CoPA Datacenter Statement of Work	3.3 Transition Services	141 - 155	What is the average change rate per day for the data on SAN/NAS?	The Commonwealth cannot provide the average change rate per day for the data on SAN/NAS. This will be documented as part of the discovery process in transition planning.
42	Schedule F – CoPA Datacenter Statement of Work	3.3 Transition Services	141 - 155	Could the Commonwealth please provide application flow documentation (by individual application) including firewall and load balancer requirements?	The requirements of each application vary and will be documented as part of the discovery process in transition planning.
43	Schedule F – CoPA Datacenter Statement of Work	3.3 Transition Services	141 - 155	What are the application limitations (by individual application), such as cannot be virtualized, cannot be combined with other applications, etc.	The requirements of each application vary and will be documented as part of the discovery process in transition planning.

44	Schedule F – CoPA Datacenter Statement of Work	3.3 Transition Services	141 - 155	Does the Commonwealth have limitations or implementation guidelines regarding OS virtualization, such as stacking of workloads within a single OS image using "container" technology?	Limitations and implementation guidelines regarding OS virtualization will depend on agency requirements and will be documented as part of the discovery process in transition planning.
45	Exhibit H.1 DOR Data Center Inventory Exhibit H.2 DOR DPH Asset List Exhibit E.1 DLI Data Center Inventory Template			Could the Commonwealth provide the addresses of the physical location of the remote servers?	See Exhibit S - Datacenter locations for datacenter addresses
46	Exhibit B.1 DPH Asset List Exhibit B.2 DPH Common Wealth Owned DPH IT Exhibit H.1 DOR Data Center Inventory Exhibit H.2 DOR DPH Asset List Exhibit I.9 IES Technical Refresh DP Exhibit I.1 IES DPH COPA Owned IT Assets Exhibit E.1 DLI Data Center Inventory Template			Could the Commonwealth map each server image to its desired Service Level in the RFP and provide such information?	The desired service level of each server image will depend on agency requirements and will be documented as part of the discovery process in transition planning.
47	Exhibit E.1 DLI Data Center Inventory Template			What is the number of server virtual guests per physical server?	The Commonwealth cannot provide the number of server virtual guests per physical server. This will be documented as part of the discovery process in transition planning.

48	Exhibit B.1 DPH Asset List Exhibit B.2 DPH Common Wealth Owned DPH IT Exhibit H.1 DOR Data Center Inventory Exhibit H.2 DOR DPH Asset List Exhibit I.9 IES Technical Refresh DP Exhibit I.1 IES DPH COPA Owned IT Assets Exhibit E.1 DLI Data Center Inventory Template			How many virtual cores per image?	The Commonwealth cannot provide the number of virtual cores per image. This will be documented as part of the discovery process in transition planning.
49	Exhibit B.1 DPH Asset List Exhibit B.2 DPH Common Wealth Owned DPH IT Exhibit H.1 DOR Data Center Inventory Exhibit H.2 DOR DPH Asset List Exhibit I.9 IES Technical Refresh DP Exhibit I.1 IES DPH COPA Owned IT Assets Exhibit E.1 DLI Data Center Inventory Template			How much virtual RAM per image?	The Commonwealth cannot provide the amount of virtual RAM per image. This will be documented as part of the discovery process in transition planning.

50	Exhibit B.1 DPH Asset List Exhibit B.2 DPH Common Wealth Owned DPH IT Exhibit H.1 DOR Data Center Inventory Exhibit H.2 DOR DPH Asset List Exhibit I.9 IES Technical Refresh DP Exhibit I.1 IES DPH COPA Owned IT Assets Exhibit E.1 DLI Data Center Inventory Template			How many virtual NIC ports per image?	The Commonwealth cannot provide the number of NIC ports per image. This will be documented as part of the discovery process in transition planning.
51	Exhibit B.1 DPH Asset List Exhibit B.2 DPH Common Wealth Owned DPH IT Exhibit H.1 DOR Data Center Inventory Exhibit H.2 DOR DPH Asset List Exhibit I.9 IES Technical Refresh DP Exhibit I.1 IES DPH COPA Owned IT Assets Exhibit E.1 DLI Data Center Inventory Template			How many virtual fiber channel ports per image?	The Commonwealth cannot provide the number of virtual fiber channel ports per image. This will be documented as part of the discovery process in transition planning.

52	Exhibit B.1 DPH Asset List Exhibit B.2 DPH Common Wealth Owned DPH IT Exhibit H.1 DOR Data Center Inventory Exhibit H.2 DOR DPH Asset List Exhibit I.9 IES Technical Refresh DP Exhibit I.1 IES DPH COPA Owned IT Assets Exhibit E.1 DLI Data Center Inventory Template			Could the Commonwealth please provide system utilization data (performance and capacity) for each image?	The Commonwealth cannot provide the system utilization data for each image. This will be documented as part of the discovery process in transition planning.
53	Exhibit B.1 DPH Asset List Exhibit B.2 DPH Common Wealth Owned DPH IT Exhibit H.1 DOR Data Center Inventory Exhibit H.2 DOR DPH Asset List Exhibit I.9 IES Technical Refresh DP Exhibit I.1 IES DPH COPA Owned IT Assets Exhibit E.1 DLI Data Center Inventory Template			Could the Commonwealth please provide data regarding the amount of SAN disk in use per physical and logical image?	The Commonwealth cannot provide the amount of SAN disk in use per physical and logical image. This will be documented as part of the discovery process in transition planning.

54	Exhibit B.1 DPH Asset List Exhibit B.2 DPH Common Wealth Owned DPH IT Exhibit H.1 DOR Data Center Inventory Exhibit H.2 DOR DPH Asset List Exhibit I.9 IES Technical Refresh DP Exhibit I.1 IES DPH COPA Owned IT Assets Exhibit E.1 DLI Data Center Inventory Template			DOR Is data replication required for any of the physical and logical images? If yes, could details please be provided?	DOR replicates data from its mainframes to a replication server using Sybase Replication Software. The details will be documented as part of the discovery process in transition planning.
55	Exhibit B.1 DPH Asset List Exhibit B.2 DPH Common Wealth Owned DPH IT Exhibit H.1 DOR Data Center Inventory Exhibit H.2 DOR DPH Asset List Exhibit I.9 IES Technical Refresh DP Exhibit I.1 IES DPH COPA Owned IT Assets Exhibit E.1 DLI Data Center Inventory Template			Could the Commonwealth please provide details regarding third-party contracts in support of the servers, such as maintenance agreements?	The Commonwealth utilizes the IBM maintenance contract for much of its mission-critical equipment (servers, etc), and also uses its Third Party IT Hardware Maintenance contract with Pomeroy for some equipment (including servers). These contracts are available on the Commonwealth's eMarketplace website. The "Third Party IT Hardware Maintenance" contract number is 4400004924. The "IT Hardware Servers – Lot 1" contract number is 4400008767. The "IT Hardware Storage" contract number is 4400008774.

56	Exhibit B.1 DPH Asset List Exhibit B.2 DPH Common Wealth Owned DPH IT Exhibit H.1 DOR Data Center Inventory Exhibit H.2 DOR DPH Asset List Exhibit I.9 IES Technical Refresh DP Exhibit I.1 IES DPH COPA Owned IT Assets Exhibit E.1 DLI Data Center Inventory Template			Is there a requirement to monitor and respond to application alerts and, if so, for which systems and applications?	The Offeror is responsible for monitoring and responding to application alerts for the managed services ordered. The systems and applications that need to be monitored will be documented as part of the discovery process in transition planning and/or when new services are ordered.
57	Exhibit B.1 DPH Asset List Exhibit B.2 DPH Common Wealth Owned DPH IT Exhibit H.1 DOR Data Center Inventory Exhibit H.2 DOR DPH Asset List Exhibit I.9 IES Technical Refresh DP Exhibit I.1 IES DPH COPA Owned IT Assets Exhibit E.1 DLI Data Center Inventory Template			What platform automated monitoring and alert tools are used today?	The following application monitoring tools are currently in use by the Commonwealth: MS SCOM, MS SCCM, Paessler (External URL Testing), CiscoWorks, NIMS, syslog, Vmware vCenter, Idera SQL DM, Oracle OEM, Big Brother, EMC Data Protection Advisor, JC Metasys, IBM TPC, Tivoli ITCAM, SightLine, Wiley, SAP Solutions Manager, IBM Director, Nagius. For purposes of submitting a proposal Offerors should assume none of the Commonwealth monitoring tools may be leveraged.

58	Exhibit B.1 DPH Asset List Exhibit B.2 DPH Common Wealth Owned DPH IT Exhibit H.1 DOR Data Center Inventory Exhibit H.2 DOR DPH Asset List Exhibit I.9 IES Technical Refresh DP Exhibit I.1 IES DPH COPA Owned IT Assets Exhibit E.1 DLI Data Center Inventory Template			Which servers (physical and logical) have Disaster Recovery requirements?	DR requirements for servers (physical and logical) will depend on agency requirements and will be documented as part of the discovery process in transition planning.
59	Exhibit B.1 DPH Asset List Exhibit B.2 DPH Common Wealth Owned DPH IT Exhibit H.1 DOR Data Center Inventory Exhibit H.2 DOR DPH Asset List Exhibit I.9 IES Technical Refresh DP Exhibit I.1 IES DPH COPA Owned IT Assets Exhibit E.1 DLI Data Center Inventory Template			Which servers/images have a high availability requirement?	Server/image high availability requirements will depend on agency requirements and will be documented as part of the discovery process in transition planning.

60	Exhibit B.1 DPH Asset List Exhibit B.2 DPH Common Wealth Owned DPH IT Exhibit H.1 DOR Data Center Inventory Exhibit I.1 IES DPH COPA Owned IT Assets Exhibit E.1 DLI Data Center Inventory Template			Are SVCs being used? If yes: 1) How much usable storage is virtualized using SVCs if any? 2) Can the SVC Clusters see multiple tiers of storage? 3) Do the SVC devices support real-time compression of block storage?	IES and DOR do not use SVCs. DLI uses SVCs. 1) Currently 8TB is virtualized using SVC. L&I has plans to increase this to 43TB. 2) Yes, DS8000 class and XIV class storage. 3) No, this is an add-on license that L&I has not purchased.
61	Exhibit B.1 DPH Asset List Exhibit B.2 DPH Common Wealth Owned DPH IT Exhibit H.1 DOR Data Center Inventory Exhibit I.1 IES DPH COPA Owned IT Assets Exhibit E.1 DLI Data Center Inventory Template			Could the Commonwealth please describe the SAN storage system(s), including total physical disk (size and number of drives), number of partitions and sizes per partitions?	For IES, see Exhibit I.4 and I.11. Information for other agencies will be documented as part of the discovery process in transition planning.

62	Exhibit B.1 DPH Asset List Exhibit B.2 DPH Common Wealth Owned DPH IT Exhibit H.1 DOR Data Center Inventory Exhibit I.1 IES DPH COPA Owned IT Assets Exhibit E.1 DLI Data Center Inventory Template			What management software is being used to manage the storage hardware for performance and capacity?	DOR is using XIV GUI, IBM Storage Manager. For IES, see Exhibits I.2, I.3, I.4 and I.11. Information for other agencies will be documented as part of the discovery process in transition planning.
63	Exhibit B.1 DPH Asset List Exhibit B.2 DPH Common Wealth Owned DPH IT Exhibit H.1 DOR Data Center Inventory Exhibit I.1 IES DPH COPA Owned IT Assets Exhibit E.1 DLI Data Center Inventory Template			Is point-in-time, flash copy or snapshots being used? What is the amount of data flashed or duplicated?	DOR currently uses Snapshots at DPH for the SAP systems with up to 5TB flashed or duplicated. IES uses IBM XIV Snaps. See Exhibits I.4 for additional information. Any additional information needed will be documented as part of the discovery process in transition planning.

64	Exhibit B.1 DPH Asset List Exhibit B.2 DPH Common Wealth Owned DPH IT Exhibit H.1 DOR Data Center Inventory Exhibit I.1 IES DPH COPA Owned IT Assets Exhibit E.1 DLI Data Center Inventory Template			Does the SAN/NAS perform data replication communications with another site? If yes: 1) Total amount of data (GB) replicated between sites? 2) What is the daily data change rate in percentage or GBs? 3) What is the sustained peak/maximum update or data transfer rate to the edge routers and SAN network devices? 4) Is data replication done on a real-time basis or on a periodic time delay basis, such as every 30 minutes, 1 hour, etc.?	The Commonwealth can provide the following information: DOR performs data replication for the imaging Centera which replicates with a box at the Brookwood Street Data Center in Harrisburg. IES performs replication for DPH backup solutions (Data Domain and Avamar) for the applications, databases and operating systems to the DR site. Any additional information needed will be documented as part of the discovery process in transition planning.
65	Exhibit B.1 DPH Asset List Exhibit B.2 DPH Common Wealth Owned DPH IT Exhibit H.1 DOR Data Center Inventory Exhibit I.1 IES DPH COPA Owned IT Assets Exhibit E.1 DLI Data Center Inventory Template			Does the SAN have unique features installed to support backup, archiving, data de-duplication, etc.? Could the Commonwealth please provide a list of such features?	The Commonwealth can provide the following information: DOR has no unique features installed except for the imaging Centera which replicates with a box at the Brookwood Street Data Center in Harrisburg. IES in the DPH uses Data Domain for backup of application database and Avamar to backup operating systems. These products provide archiving and de-duplication. Any additional information needed will be documented as part of the discovery process in transition planning.

66	Exhibit B.1 DPH Asset List Exhibit B.2 DPH Common Wealth Owned DPH IT Exhibit H.1 DOR Data Center Inventory Exhibit I.1 IES DPH COPA Owned IT Assets Exhibit E.1 DLI Data Center Inventory Template			Does solution require peer-to-peer communications of data with another site? If yes: 1) What is the typical and maximum network traffic used by this communication? 2) What is the average daily update or data transfer rate that the edge routers and SAN network devices will need to support? 3) What is the sustained peak/maximum update or data transfer rate the edge routers and SAN network devices will need to support time of day)? 4) Is SAN fabric reporting currently implemented?	The Commonwealth has the following specific information: DOR and IES do not require peer-to-peer communications of data with another site. Any additional information needed will be documented as part of the discovery process in transition planning.
67	Appendix A	9 (a)	10	In the Commonwealth response to questions, round 1, part 1, question #24, the Commonwealth stated that the responsibility for logical security/ID administration remains with the Commonwealth. Does this include privileged users?	Please clarify question to explain "Privileged Users" in the context of this question.
68	Schedule J.3	SL01 – SL05	5*9	Which Commonwealth applications are included in these particular Service Levels? Which applications are assigned to which particular Service Level? Does the Commonwealth require that instrumentation be implemented for each individual application to measure availability?	Applicable SLAs will be determined based on the services ordered. The Commonwealth requires service levels SL01-SL05 to be associated at an application level of reporting. Yes, the Offeror must implement instrumentation to measure availability.
69	Schedule F, Statement of Work	3.1.2-5	17	How many security zones per agency should offerors assume?	The Commonwealth has seven (7) datacenters and each has several security zones. The actual number of security zones will be documented as part of the Discovery process during transition.
70	Schedule F, Statement of Work	2.3.1	8	What is the average utilization and bandwidth provided between each Data Center and end user locations on CopaNet and via PIP? Which will need to connect to the target data centers?	All datacenters are connected to COPANET. The current internet connections are connected to COPANET. See Exhibit P – Enterprise Internet Bandwidth Utilization. The selected Offeror's data centers must connect to COPANET.

71	Schedule A, Defined Terms and Schedule I , Offeror Pricing Forms	General Question	General Question	How many concurrent licensed VPN users will terminate in the EDC or Target Data Centers? How many of each type (IPSec or SSL)?	The Commonwealth is requiring the ability for secure remote access to hosted systems for operational and administration purposes for designated personnel. The Commonwealth currently has VPN services hosted by Verizon as part of its Telecom Contract. The number of licensed site to site VPN tunnels is dependent upon the architecture provided and may vary during the term of the contract. Currently the Commonwealth has 5,619 total VPN users.
72	Exhibit D.2, EDC-Switch Inventory	General Question	General Question	What are the device counts for firewalls, WAN Optimization controllers, Wireless controllers, routers and other appliances by model which the supplier will be responsible for by location?	The Commonwealth can only provide the information that is included in Exhibit D.2 - EDC - Switch Inventory. Additional information will be documented as part of the discovery process in transition planning.
73	Schedule F, Statement of Work	3.2.4.2.7	103	Outside of state regulatory requirements, would the Commonwealth please provide backup retention requirements (e.g., retain 12 months full backups, 5 year annuals, etc.)?	Data retention policies will be determined by IT policy, law, and the requirements of the RFP The Commonwealth has data retention polices. Management Directive 210.5 (Commonwealth of PA State Record Management Programs) and several Information Technology Bulletins on this subject. Management Directives can be found at - http://www.portal.state.pa.us/portal/server.pt/community/policies/10301/management_directives/551950 ITBs can be found at - http://www.portal.state.pa.us/portal/server.pt?open=514&objID=210791&mode=2 Individual agencies may have additional data retention policies, such as IRS Pub 1075, etc. The selected Offeror will identify additional requirements during transition for individual services and comply with those requirements.

74	Schedule F, Statement of Work	3.2.4.2.7	103	Would the Commonwealth please state the current backup schedules (e.g., daily Incremental, weekly full, monthly full, etc.)?	Backup schedules vary by agency and will be documented as part of the discovery process in transition planning.
75	Schedule F, Statement of Work	3.2.4.2.7	103	What is the estimated daily change rate for the backups (e.g., 10% for file backups, 20% for database backups, etc.)?	The daily change rate varies by agency and will be documented as part of the discovery process in transition planning.
76	Exhibit E.1, DLI Datacenter Inventory Template	Applications Tab	rows 62 - 78	Would the Commonwealth please provide the following information regarding each AS400 iSeries server: • Location • Model Number • CPU (type, model, feature, etc.) • RAM GB • DASD Storage information • Operating system version and release • Number of LPARs	The Commonwealth cannot provide the information regarding each AS400 iSeries server. This will be documented as part of the discovery process in transition planning.
77	Revised Schedule F, Statement of Work	3.2.4.4	110 #3	Would the Commonwealth please provide the following regarding Production Control/Scheduling for open systems: • Number of batch jobs per month • •Monthly Abend rate	The Commonwealth can provide the following information regarding Production Control/Scheduling for open systems. IES - SAP batch/job processing is internal to the SAP application software. DOR - 46,793 batch jobs per month; 713 abends per month L&I - There are approximately 51,118 batch jobs that are executed within Dollar Universe per month, in which 36% of those batch jobs are aborted. Note: The Offeror may be required to assume responsibility for all or a subset of an agency's batch operations. This will be determined as part of the discovery process in transition planning.

78	Revised Schedule F, Statement of Work	3.2.4.4	111 #3	Regarding open systems batch processing, what software product is used for batch processing?	IES: SAP application manages/schedules batch processing. Integration file processing is managed by BMC Control M. DOR Redwood CPS, IBM's Tivoli Workload Scheduler. L&I - The Orsyp Dollar Universe Job Scheduling software is the Department of L&I enterprise job scheduler. In addition to Dollar Universe, the Microsoft Windows Task Scheduler, Cron, and mainframe job scheduling are used within the agency.
79	Revised Schedule F, Statement of Work	3.2.4.4	111 #3	Regarding open systems batch processing: • What is the level of automation for batch processing? • Describe any manual intervention required to perform batch job processing to completion.	The Commonwealth can provide the following information regarding open systems batch processing. IES: SAP application manages/schedules batch processing. Integration file processing is managed by BMC Control M. DOR Automation of jobs is about 75-80% on a normal day. L&I - All batch jobs processing within Dollar Universe are automatically processed. Those batch jobs that are aborted are then manually executed to process
80	Exhibit B.1, DPH - Asset List	All Agency Tabs listing server HW assets	N/A	In order to provide a fixed price for transition, would the Commonwealth please provide following information to the asset hardware lists for each server / virtual line entry: • Server name or identifier • Platform operating system and level • TIER classification (PTL, GLD, SLR, BRN, Basic) • Primary Application (DB, App, Web, etc.) • Function (Prod, Dev, test, etc.) • SAN attached? (Y/N). If yes, add storage used / allocated (GB)	Any information in addition to what is included in exhibit B.1 DPH Asset List will be documented as part of the discovery process in transition planning.
81	Revised Schedule F, Statement of Work	3.2.1.4	44	What is the total number of users in-scope for Service Desk support? What is the total number of Authorized Commonwealth users?	For purposes of submitting a proposal, Offerors should consider the number of service desk users as 300 and the total number of Commonwealth users as 300. These figures are estimates and may vary.

82	Exhibit K, Enterprise Remedy and Volumetrics	DC Related Volumetrics	11	What is the monthly average count of service requests expected for this scope of work?	There were approximately 350 service requests in 2012 across all in-scope data centers. The expected volume in unknown and will vary during the term of the contract.
83	Exhibit K, Enterprise Remedy and Volumetrics	DC Related Volumetrics	11	What is the average call handle time (talk time plus wrap-up) for contacts to the Service Desk today?	The average duration for an incoming call coming into the DPH help desk in the month of February was 88 seconds. This is for the DPH help desk only; there is no reporting on the other tier 2 service desks.
84	Exhibit K, Enterprise Remedy and Volumetrics	DC Related Volumetrics	11	Are there additional incident volumes that should be expected above what is listed on page 11? If yes, please provide a monthly average estimate for the additional volume.	In addition to the ticket volumes provided, PennDOT has its own Remedy System and processes approximately 160 tickets per month. Labor and Industry processes approximately 100 server-related tickets per month in its Remedy System. Actual volumes will vary during the term of the contract. The selected Offeror must handle all call volumes which occur over the life of the contract.
85	Exhibit D.7, EDC Facility Summary and Requirements	Voice and Data Network Connectivity	11	Would the Commonwealth please provide the specific requirements, for each connection, including bandwidth, circuit or connection type, services included, location addresses, and NPA/NXX for each served location which the offeror is required to maintain connectivity to the Commonwealth's voice and data networks at offeror's expense	Bandwidth information has been provided in Exhibit P - Enterprise Internet Bandwidth Utilization. The Offeror is required to connect to COPANET. See Exhibit U – COPANET Locations for address and NPA/NXX information. Additional information will be documented as part of the discovery process in transition planning.
86	General Question	N/A	N/A	Would the Commonwealth provide a Middleware instance count along with the number of sites each server serves?	The Middleware instance accounts will vary by agency and will be documented as part of the discovery process in transition planning.
87	General Question	N/A	N/A	Would the Commonwealth provide the rate of change each of the Middleware environments (e.g., sites, apps., etc.) get updated, and the level of effort required on a typical update?	The rate of change for each Middleware environments will vary by agency and will be documented as part of the discovery process in transition planning.
88	Exhibit E.33, DLI - UC Telco Layout	All	All	Please advise which, if any, of the equipment shown in this exhibit should be considered to be in scope for migration, and what type of support is required.	All of the equipment in the referenced exhibit is out of scope for migration.

89	Exhibit E.1 vs other DLI Exhibits	General	N/A	Exhibit E.1 indicates a server/image count of 1360; however a review of the various application architectures appears to indicate a server/image count of well over 2000. We understand, of course, that this is a dynamic environment, and a more precise count would be more readily available during transition planning and due diligence; however, for preliminary planning purposes, which of these should be considered to be more accurate to understand the volume of DLI's IT systems?	1360 is the correct server/image count for Labor and Industry. . The application architecture models show shared servers which are redundant in the overall count.
90	Schedule F, Statement of Work	3.2.4.1	116	Please provide the average monthly MIP usage for each of the Dorado LPARs for the most recent 12 month period?	Monthly MIP usage for each of the Dorado LPARs will be documented as part of the discovery process in transition planning.
91	Schedule F, Statement of Work	3.2.4.1	118-119	Please supply the number of batch processing jobs and ABEND rates for each of the Unisys Dorado Partitions?	The number of batch processing jobs and ABEND rates for each of the Unisys Dorado Partitions will be documented as part of the discovery process in transition planning.
92	Schedule F, Statement of Work	3.2.4.1	116	Please provide performance data for each Unisys Libra machine - the average monthly MIP usage for each of the Libra machines in the previous 12 months?	The performance data for each Unisys Libra machine will be documented as part of the discovery process in transition planning.
93	Schedule F, Statement of Work	3.2.4.1	118-119	Please supply the number of batch processing jobs and ABEND rates for each of the Unisys Libra machines?	The number of batch processing jobs and ABEND rates for each of the Unisys Libra machines will be documented as part of the discovery process in transition planning.
94	Schedule F, Statement of Work	3.2.4.1	94	For the Unisys Dorado Machines, how many physical tapes by type (9840, 36-track, etc.) exist?	The number of physical tapes by tape type will be documented as part of the discovery process in transition planning.
95	Schedule F, Statement of Work	3.2.4.1	94	For the Unisys Dorado Machines, how many virtual tapes by type (9840, 36-track, etc.) exist?	The number of virtual tapes by tape type will be documented as part of the discovery process in transition planning.
96	Schedule F, Statement of Work	3.2.4.1	94	For the Unisys Libra Machines, how many physical tapes by type (LTO-3, 36-track, etc.) exist?	The number of physical tapes by tape type will be documented as part of the discovery process in transition planning.
97	Schedule F, Statement of Work	3.2.4.1	94	For the Unisys Libra Machines, how many virtual tapes by type (LTO-3, 36-track etc.) exist?	The number of virtual tapes by tape type will be documented as part of the discovery process in transition planning.
98	Schedule F, Statement of Work	3.2.4.1	94	RFP states "Provide all tools and apps that are currently being provided, for example MAPPER/APPMAP, browser based terminal emulation access, and middleware components (e.g., OpenTI, IBM WBM & WMQ, etc.) that are critical to agency operations and application usage." For the Unisys Dorado Machines, please provide a list of Unisys Software including operating Systems Software and tools that are being used today, by partition?	Exhibit B.4 - DPH - Third Party Software - Contractor Provided and Exhibit B.10 - DPH - Third Party Software - Commonwealth Provided, Contractor Maintained and Managed contain lists of Third Party software for the DPH. Any additional information will be documented as part of the discovery process in transition planning.

99	Schedule F, Statement of Work	3.2.4.1	94	RFP states "Provide all tools and apps that are currently being provided, for example MAPPER/APPMAP, browser based terminal emulation access, and middleware components (e.g., OpenTI, IBM WBM & WMQ, etc.) that are critical to agency operations and application usage." For the Unisys Libra Machines, please provide a list of Unisys Software including operating Systems software and tools that are being used today?	Exhibit B.4 - DPH - Third Party Software - Contractor Provided and Exhibit B.10 - DPH - Third Party Software - Commonwealth Provided, Contractor Maintained and Managed contain lists of Third Party software for the DPH. Any additional information will be documented as part of the discovery process in transition planning.
100	Exhibit H.3, DOR – DPH COPA Software Asset OBM Mainframe		Tab_Revenue-IBM	Please provide a comprehensive inventory of ALL Software Titles installed on ALL six z/OS LPARS defined on z/Series Processor 2817-603 serial number 85C6F. Please indicate who will hold financial responsibility for each product.	The software titles installed on the six z/OS LPARS will be documented as part of the discovery process in transition planning. Financial responsibility for Third party software is set out in Appendix A - Data Center RFP Terms and Conditions
101	Exhibit B.1, DPH – Asset List		Tab_Mainframes_IBM	Please provide processor configuration for processor 2817-603 serial number 85C6F. Please include: • Number of IFL processors installed • Amount of Memory installed • Number of FICON Channels installed • Number of Escon Channels Installed • Number and type of OSA cards installed • Any other specialty processors installed (ZIIP, ZAAP, ICF, Crypto)	Processor configuration for processor 2817-603 serial number 85C6F will be documented as part of the discovery process in transition planning.
102	Exhibit B.1, DPH – Asset List		Tab_Mainframes_IBM	Please provide processor configuration for processor 2098-J02 serial number 3E5DE. Please include: • Amount of Memory installed • Number of FICON Channels installed • Number of Escon Channels Installed • Number and type of OSA cards installed	Processor configuration for processor 2098-J02 serial number 3E5DE will be documented as part of the discovery process in transition planning.
103	Exhibit B.3, DPH - Commonwealth Software Asset Listing		TAB DOC IBM	Please provide a comprehensive inventory of ALL Software Titles installed on the single z/VSE LPAR defined on z/Series Processor 2098-J02 serial number 3E5DE. Please indicate who will hold financial responsibility for each product.	The software titles installed on the single z/VSE LPAR defined on z\Series Processor 2098-J02 will be documented as part of the discovery process in transition planning. Financial responsibility for Third party software is set out in Appendix A - Data Center RFP Terms and Conditions.

104	Exhibit B.1, DPH - Asset List		Tab_Shared SAN Storage	Are the ESCON Channels still in use for DPW, GAME, and PSP Mainframe systems? Are there any known issues with changing these to FICON?	Escon Channels are not still in use for DPW, GAME, and PSP. FICON is an IBM proprietary technology that is not applicable to Unisys mainframe systems.
105	Exhibit B.1, DPH – Asset List		Tab_Shared SAN Storage	Are the 30 9840 tapes for DPW and the 12 9840 tape drives for PSP ESCON or FICON connected within the SL8500? What Model type are the 9840 tape drives (A, B, C, or Ds)?	The 9840 tape drives are Model C and are connected via FICON to the SL8500 tape silo.
106	Exhibit B.1, DPH – Asset List		TAB_Dedicated DR	Is the data from the DMX3 on the shared SAN Storage Tape replicated to the DMX4 on this tab or is the recovery done by performing tape restores from the 9840s?	A subset of the data from the DMX3 is replicated to the DMX4 and is resident at all times at the DR location. The remainder of the data required for disaster recovery on the DMX4 is restored from tape.
107	Schedule F – COPA Datacenter Statement of Work	3.2.5.5 (12)	142	What is intended with the requirement “The service must provide personal email files (.pst).”? Does the requirement indicate that the Service Provider should support existing .pst files or provide new .pst files? Does this indicate a need to support more than one mailbox with an additional 5GB mailbox limit?	The selected Offeror must support new .pst files and support existing .pst files or migrate the existing .pst to a new .pst file. No, it does not indicate the need to support more than one mailbox with an additional 5GB mailbox limit.
108	Schedule F – COPA Datacenter Statement of Work	3.2.5.5	142	When providing personal archiving capabilities, how much of the archival space should be available to users?	The Commonwealth currently uses the .pst files on local storage for archival purposes. Personal archiving is outside the scope of this RFP. See Exhibit Q - Mailbox Restore Policy for additional information. This is a confidential document. To receive a copy, please contact Sheryl Kimport, the Issuing Officer.
109	Schedule F – COPA Datacenter Statement of Work	3.2.5.5	142	Will there be a need to migrate existing .pst files to personal archives?	The Commonwealth currently uses the .pst files on local storage for archival purposes. The selected Offeror is not required to migrate existing .pst files to personal archives, but must support the ability to access existing archived.pst files and create new .pst archives.
110	Schedule F – COPA Datacenter Statement of Work	3.2.5.5	142	Is the Commonwealth willing to transfer any existing non-expired licenses to the Service Provider?	For the purpose of submitting a proposal, Offerors should assume no licenses will be transferred.
111	Schedule F – COPA Datacenter Statement of Work	3.2.5.5	142	Please confirm that the recovery of existing COPA AD will not be part of DR requirement.	The Commonwealth confirms that the recovery of existing COPA AD will not be part of DR requirement.

112	Schedule F – COPA Datacenter Statement of Work	3.2.5.5	142	Does the Commonwealth have any special retention policies and requirements for recovering messages and mailboxes? If so, what are they?	Mailboxes must not to be deleted earlier than 30 days after account deactivations. Individual mail items must be recoverable for at least 5 days after deletion. See Exhibit Q - Mailbox Restore Policy for additional information. This is a confidential document. To receive a copy, please contact Sheryl Kimport, the Issuing Officer.
113	Schedule F – COPA Datacenter Statement of Work	3.2.5.5	142	Are there any legal hold capabilities required for any of the mailboxes? If so, please define the retention period.	Yes, the Commonwealth requires the mailboxes include legal hold capabilities. The required retention period will vary.
114	RFP	Section I-30 COSTARS PROGRAM	23	Can COSTARS participation be added after the contract is negotiated?	Yes.
115	RFP	Section I-30 COSTARS PROGRAM	23	Given the multi-tenant nature of the environment, does the Offeror need COPA approval to add a COSTARS member to the environment when a PO is received?	Commonwealth approval is required to add a COSTAR member to the environment. COSTARS member must be on a segregated environment, not connected to the Commonwealth shared environment.
116	RFP	Section I-30 COSTARS PROGRAM	23	Will the Commonwealth allow a COSTARS member to participate in the shared environment established for the Commonwealth of Pennsylvania?	No.
117	RFP 6100022698	Part 3	23 of 31	As the Offeror, we do not have the certification ISO 27001, 9001, 20000 and SSAE 16 Audit. However, the Data Center we work with and who will be involved in this RFP, has these certifications. In this situation, would the requipments be met?	Offerors may use subcontractors to meet the RFP requirements. The data center proposed by an Offeror must have the required certifications.
118	Questions and Answers – Round 1 Part 1	*126*		Other than security, does the EDC monitor other items within the EDC (e.g. generators, UPS, etc.) using a building management system (BMS) or a data center infrastructure manager system (DCIM)? If so, can the Offeror utilize these systems? Can the Offeror connect electronically to these systems to receive alerts and alarms to its monitoring systems?	The Commonwealth has a BMS that the Offeror may access for generator, UPS and air handler alerts, monitoring and information. The selected Offeror will be able to connect to the BMS electronically.
119	Questions and Answers – Round 1 Part 1	131		How much load does the balance of the building represent as part of the generator capacity? Can this load be isolated and switched off in the event of an emergency within the computer room (e.g. in case of an extended emergency)?	Approximately 600 amps of service to the building are non-data center load. Under the current configuration this load cannot be switched off.

120	Questions and Answers – Round 1 Part 3 Schedule F	4 3.2.1.4	44	How many tickets/calls are from agencies that do not utilize the Commonwealth's Enterprise Remedy System? Will these tickets/calls add to the call/ticket volumes previously provided?	In addition to the ticket volumes provided, PennDOT has its own Remedy System and processes approximately 160 tickets per month. and Labor and Industry processes approximately 100 server-related tickets per month in its Remedy System. Actual volumes will vary during the term of the contract. The selected Offeror must handle all call volumes which occur over the life of the contract.
121	Questions and Answers – Round 1 Part 3	34		The Commonwealth's Microsoft Exchange Enterprise License Agreement may be less expensive than those that may be purchased by an Offeror. To provide greater savings to the Commonwealth, will the Offeror be granted permission to use this or similar Commonwealth ELAs?	~~For the purpose of submitting a proposal, Offerors should assume they will not be permitted to use the Commonwealth's Microsoft Exchange Enterprise License Agreement.~~
122	Questions and Answers – Round 1 Part 3	40		Will the Commonwealth update Schedule J.3 to reflect the definitions of calculations to remove scheduled and approved downtime?	Schedule J.3 has been revised. The following exclusions have been identified. Offeror's failure to achieve any Service Level will not constitute a Service Level Default or accrue toward a Service Level Termination Event to the extent such failure is directly attributable to any of the following: (i) the failure or unavailability of equipment or other resources for which the Commonwealth is operationally and managerially responsible pursuant to the Contract, (ii) changes made to the environment by the Commonwealth that were not communicated in accordance with the Change Control Procedure or other method agreed upon by the Parties, and (iii) scheduled and approved maintenance windows
123	Questions and Answers – Round 1 Part 3	77		Please provide details on the special power requirements at the Department of Labor and Industry.	There are no special power requirements for the Department of Labor and Industry. The power concerns were listed due to an aging transformer at the Labor and Industry building. The Labor and Industry server farm has no special power requirements in and of itself.
124	Questions and Answers – Round 1 Part 3	117		Will the EDC facility service agreements such as those for generators, switches, batteries, etc. be covered from the EDC Reserve Account?	Operating expenses such as service agreements will not be covered from the EDC Reserve Account.

125	Questions and Answers – Round 1 Part 3	123		Please provide information regarding the HIDS required for each agency that will be relocated or in use within the EDC.	See Exhibit J.4 - Security Agent Standard Tools. This is a confidential document. To receive a copy, please contact Sheryl Kimport, the Issuing Officer.
126	Questions and Answers – Round 1 Part 4	39		How many environments have a requirement for physical segregation? What are their respective area requirements?	Requirements for physical segregation will depend on agency requirements and will be documented as part of the discovery process in transition planning.
127	Questions and Answers – Round 1 Part 4	43		Is this transformer shared with the entire facility housing the EDC including non-data center areas?	The PP&L transformer is shared by the entire building (data center and non-data center).
128	Questions and Answers – Round 1 Part 4	45		Please provide the requirements that agencies will have for managing, submitting and controlling scheduled and unscheduled jobs within the environment.	The selected Offeror will provide all job scheduling in the managed hosting services environment. Commonwealth agencies will manage the jobs in non-managed hosting environments.
129	Questions and Answers – Round 1 Part 3 Schedule F	124 3.2.1.1.1 Financial Management	27	What are the expected data integration requirements between the Offeror's invoicing system and the Commonwealth's Remedy System? What module or application within Remedy, what data forms, and what is the expected output to the Commonwealth's Remedy System?	There are no integration requirements with the Commonwealth's ITSM system (currently Remedy). Invoicing will occur via a file transfer procedure that conforms to a format approved by the Commonwealth. The required data forms and output required from the selected Offeror will be documented as part of the discovery process in transition planning.

130	Questions and Answers – Round 1 Part 4	52 53		Please confirm that answers to these two questions have been reversed.	These answers were reversed. Question 52 from Round 1 Part 4 answer has been revised to read:: The current configuration is: * PSP Production: 4 – Fibre PCI Cards SIOP Interfaces – speed 2 Gb * PSP Development: 4 – Fibre PCI Cards SIOP Interfaces – speed 2 Gb The Commonwealth requires the selected Offeror to provide the services set forth in the RFP according to the contract terms and conditions. This existing infrastructure may not be sufficient for the long term. Offerors must determine the quantity, type, speed, etc. of the equipment required to provide the services throughout the term of the contract. Question 53 from Round 1 Part 4 answer has been revised to read: The current configuration is: PSP Production: 6 – 9840C drives 4 – 36 track drives (5236) PSP Development: 6 – 9840C drives 4 – 36 track drives (5236) The Commonwealth requires the selected Offeror to provide the services set forth in the RFP according to the contract terms and conditions. This existing infrastructure may not be sufficient for the long term. Offerors must determine the quantity, type, speed, etc. of the equipment required to provide the services throughout the term of the contract.

131	Schedule I	Volumemetrics Tab and Managed Services (Only) Tab		In the Volumetrics Tab, under the section of "Other Devices (non-Server) - Managed Only" there are baseline quantities listed for a general group of equipment labeled as "Network, Security, Storage, Appliances, and other non-Server Devices" Please be aware that the service requirements for this group of equipment would vary greatly depending on the specific equipment manufacturer, model number, and the actual number of each type of equipment. For instance, a single "appliance" could range from a very sophisticated database appliance requiring a great deal of labor to a very simple appliance that may not require much labor at all. Given the current requirement to provide a single unit price for this entire group of equipment, please provide details on each type of equipment in this group and the baseline quantities for each type. If this equipment cannot be identified at this time, the Commonwealth may want to consider adding this type of equipment to the service catalog on an as-needed basis in an effort to reduce overall pricing.	"Network, Security, Storage, Appliances, and other non-Server Devices" section of Schedule I - Offeror Pricing Forms has been removed. Schedule I has been revised to include this change.
132	Schedule F – Statement of Work (Amended 2.18.13) Schedule J – all	3.2.4.7 SL01-SL05	128	Which SLAs, if any, apply to database services? If any, how does the Commonwealth see the database service being measured beyond those SLAs applicable to the server resource unit SLAs?	SL01 – SL05 take into consideration every infrastructure component for the application as related to the SLA ordered. The Offeror is responsible for the services ordered. This includes database services. Therefore, the selected Offeror will be responsible to make sure all of the associated services are working as designed and ordered.

133	Schedule F – Statement of Work (Amended 2.18.13)	3.2.4.7	128	For which service tiers (Fully Managed, Managed Only, IaaS, etc.) are database services to be provided?	~~Database services may be required for all Tiers, based on the service ordered by the Commonwealth.~~ ~~Other than those provided for in the rate card in Schedule I there are no Database Administration functions required. The selected Offeror will be required to provide technical assistance to the Commonwealth's DBA staff.~~ ~~Offerors may include a Database Administration as a service in the Service Catalog.~~
134	Schedule D – Transition Milestones Schedule F – Statement of Work (Amended 2.18.13)	M-14 3.3.2	146	In Schedule D – Transition Milestones Document (M-14) the target date for EDC Operational Transition Completion is 12/31/2014. However, Schedule F – Statement of Work (3.3.2) states that the Offeror must assume operations support of the EDC datacenter within 90 days of Contract start date. What is the difference between Operational Transition Completion and Operations support? If these terms are the same, which completion date is actually required?	The EDC Operational Transition Completed milestone due date is 12/31/2014. Schedule F - Datacenter Statement of Work has been revised to remove the reference to "Contract start date + 90 days.
135	Schedule D – Transition Milestones Schedule F – Statement of Work (Amended 2.18.13)	M-14 3.3.2	146	When does the 90-day takeover for the EDC period to begin? What does this takeover entail (e.g. operational take-over of the environment, service desk, ITSM support, etc.)?	The EDC Operational Transition Completed milestone due date is 12/31/2014. Schedule F - Datacenter Statement of Work has been revised to remove the reference to "Contract start date + 90 days. Refer to Schedule D - Transition Milestones for milestone acceptance criteria.
136	Schedule D – Transition Milestones	General		To aid transition, will the Offeror be allowed to install device and security discovery tools within the existing agency environments? If so, what will be required to gain the needed network and device access?	Yes, with Commonwealth approval. Prior to installing these items on the Commonwealth's network, the selected Offeror must have the appropriate background checks and the devices and network requirements must be vetted with the Commonwealth's Chief Information Security Officer to ensure there will be no harm or loss of Commonwealth data or disruption to network resources.
137	Schedule F – Statement of Work (Amended 2.18.13)	2.3.4 #1	11	If security vulnerability assessments of the existing agency environments indicate the need for agency security remediation, will the consequences of this remediation be taken into consideration with regards to the transition timelines and key milestones?	Identifying these impacts will be part of the transition planning and should be taken into consideration by the Offerors in their planning.
138	Schedule J.3 SLAs	General		Please confirm that SLAs will not apply prior to the completion of an agency, DPH, or EDC transitions?	The SLAs will apply once an application is transitioned.

139	Appendix A	II-8	20	Can the Commonwealth please confirm the intent that the proposals are based on the terms and conditions set out in Appendix A so that the Commonwealth can compare proposals on an apples to apples basis, then later intending to negotiate the terms and conditions as highlighted in the RFP submission from the Offeror in good faith after award to the winning proposal?	The intent of Part II-8 is to ensure all proposals are based on the terms and conditions set out in Appendix A. The Issuing Office may, in its sole discretion, accept or reject any requested changes to the terms and conditions. The Issuing Office will reject any proposal that is conditioned on the negotiation of the terms and conditions set out in Appendix A.
140	Schedule F, COPA Data Center Statement of Work	3.2.4.7	Database Services Page 128	Would the Commonwealth please provide the RDMS instances and types executing on all z/Os and z/VSE LPARs (e.g., DB2, IMS, Oracle)?	The Commonwealth can provide the following information regarding RDMS instances. DPW has two AS400 LPARs, both of which run DB2. DOR has the following: • Production - Relational DBMS: DB2P, DB2R, DB2T, DSN • Production Hierarchical DBMS: IMS, IMSB • Test - Relational DBMS: DB2B • Test Hierarchical DBMS: IMSZ PennDOT has the following: RDMS instances: z/OS: IMS is used in Sandbox (PDTT), Pre-Prod (PDT1) and Prod (PDT0) 1 instance pre environment, DB2 is used in Sandbox (PDTT) 1 instance, Pre-Prod (PDT1) 5 instances and Prod (PDT0) 2 instances. z/VM: Oracle is used in Pre-Prod (DOTLNX01) 7 instances and Prod (DOTLNX02) 2 instances. L&I has one (1) instance DB2 z/OS, one instance IMS. Any additional information will be documented as part of the discovery process in transition planning.

141	Schedule F, COPA Data Center Statement of Work	3.2.4.5	Mainframe Services Page 116	Would the Commonwealth please provide the number of CICS regions and MQ Series regions running on all z/OS and z/VSE LPARs?	The Commonwealth can provide the following information regarding the number of CICS regions and MQ Series regions running on all z/OS and z/VSE LPARs. Neither DPW LPAR uses CICS or MQ Series. DOR is running the following: • 10 CICS regions on the production LPAR and 1 CICS region on the Dev/Test LPAR. • WebSphere MQ managers is running 2 on the production LPAR and 1 on the 1 on the Dev/Test LPAR. • DOR is not using z/VSE operating system. Just z/OS. PennDOT uses WMQ in z/OS: Sandbox (PDTT), Pre-Prod (PDT1) and Prod (PDT0 and in z/VM: Pre-Prod (DOTLNX01) and Prod (DOTLNX02). L&I is using 6 IMS, 5 CICS, and 2 MQ

142	Exhibit B.1, DPH-Asset List		Mainframes-IBM Tab	a. Would the Commonwealth please confirm if there are a total of two or three 3584 dedicated tape libraries? b. Please confirm the configuration of these libraries and their functions. For example: 1 – 3584-L53 frame 5 – 3584-D53 frames 8 – 3588-F4A (LTO3 drives) 1 – HA feature code This library is used to back up the z/LINUX environment. c. Are the two TS7740s libraries in a GRID configuration? d. Please confirm that the 3592-J70 controllers are used to support the 3590-H11 tape drives. e. What is the cache size for each TS7740 Virtual Tape Engine? f. Are you currently using encrypting data going to the 3592-E05 and/or 3592-E06 tape drives? I f.1 so, is the Commonwealth using software or hardware encryption? f.2 If the Commonwealth is using hardware encryption, what is used for the key management (i.e., EKM, TKLM, or ISKLM)? f.3 Is the key management software installs in z/platform or on a midrange platform?	a. There are three 3584 dedicated tape libraries. b. Reference Exhibit B1. If questions remain, please provide clarification c. Yes d. The 3592-J70 controllers are used to support the 3590-H11 tape drives e. 16GB f. Data encryption requirements are agency and application specific and will be documented as part of the discovery process in transition planning.

143	Schedule F, COPA Data Center Statement of Work	3.2.4.5	Mainframe Services Page 116	Please provide information on the batch environment including the following data items: 1) Number of batch jobs that execute on all the z/OS, z/VM, and z/VSE LPARs 2) Abend Ratio (number of abends expressed as a percentage of executed jobs) 3) On a monthly basis, the average number of adhoc batch requests 4) On a monthly basis, the average number of change requests to the monthly batch schedules 5) On a monthly basis, the average number of new batch requests added to the batch schedule	The following is the available agency specific information on the batch environment: DPW: 1) Between the two LPARs, there are approximately 40 monthly batch jobs, 40 weekly batch jobs, and 25 daily batch jobs. 2) Abends are rare as are batch job changes. 3) On average, there are approximately 8 ad hoc batch jobs a month. 4) New requests are less than one a month. 5) The average number of batch requests added will be documented as part of the discovery process in transition planning. DOR: 1) The number of batch jobs will be documented as part of the discovery process in transition planning. 2) Abend Ratio around 12 % (49,465 jobs, 602 abends for the month) 3) Average AdHoc requests per month are about 200 to 300(busy month) 4) more than 300 5) The average number of batch requests added will be documented as part of the discovery process in transition planning. PennDOT: PennDOT currently uses IBM Tivoli Workload Scheduler (TWS) for scheduling jobs. PennDOT is responsible for managing, submitting, controlling the TWS applications and DPH IBM monitors the jobs. 1) The number of batch jobs will be documented as part of the discovery process in transition planning. 2) The abend ratio will be documented as part of the discovery process in transition planning. 3) The number of AdHoc batch requests will be documented as part of the discovery process in transition planning. 4) the number of change requests will be documented as part of the discovery process in transition planning. 5) The average number of batch requests added will be documented as part of the discovery process in transition planning. L&I: 1) 1609 2) 5% 3) 25 4) 10 5) 5

144	Schedule F, COPA Data Center Statement of Work	3.2.3.2	Site Operations Page 88	For tape processing, would the Commonwealth please provide the volumes requested below: 1) Number of manual mounts on the z/OS, z/VM, and z/VSE LPARs 2) The number of tapes that are rotated on/off site per month 3) Number of physical tape media in the entire z/OS, z/VSE, and z/VM library by media type (e.g. 3590, 3592)	The following is the agency specific information regarding tape processing: DPW: The two LPARs use a small number of 3584 and 3592 tapes, around two each per month, with a small subset (less than 10%) of these being sent offsite for storage. DOR: For DOR's datacenter, roughly 200-250 a month go in and out. There are 1000 tapes in the system of which about 750-800 are in the library at any given time. L&I: 1) The majority of mounts are virtual. The estimated volume of physical mounts is less than 20 per month. 2) Under the outsourced agreement, our tapes and data are combined with outer shared agency resources. Accurate data is not available for this. 3) 7431 Total Physical tapes 100 – 3592 cartridges 7331 – 3490 cartridges Additional information regarding tape processing will be documented as part of the discovery process in transition planning.
145	Schedule F, COPA Data Center Statement of Work	3.2.4.5	Mainframe Services Page 116	Please confirm that there are no Database Administration functions in scope other than technical assistance to the Commonwealth's DBA staff.	Other than those provided for in the rate card in Schedule I there are no Database Administration functions required. The selected Offeror will be required to provide technical assistance to the Commonwealth's DBA staff. Offerors may include a Database Administration as a service in the Service Catalog.
146	Exhibit I.1, IES - DPH COPA OwnedIT Assets		Rows 123 & 124	Would the Commonwealth please provide details on what the application is for Filenet? Is this P8?	FileNet software is no longer used by IES. The servers listed in Exhibit I.1 (PRDARCI1U, PRDARCW1U) have been decommissioned.

147	Exhibit I.1, IES - DPH COPA OwnedIT Assets		IES Tab	There are several SAP servers included in the list without details of what SAP component they belong to. Would the Commonwealth please provide details onwhat the following servers are: dba01u, dc6dca0u, dc7dca0u, DE2CIA0U, DEVALM01, devdb01u, DEVDQM01, DEVLVC01, IESDC02, prddb01u, prddb02u, PRDDQM01, PRDI3U, PRDSROUTE01 (CTC), qasdb01u, qc6dca0u, qcpapp1u, qcpdca0u, QEPCIA0U, qppdca0u, QVPCIA0U, qwpdca0u, sc2dca0u, STGW6U (CTC)?	dba01u - Development SAP Portal database, dc6dca0u - Development SAP ECC DB/CI, dc7dca0u - Development SAP ECC DB/CI, DE2CIA0U - Development SAP Portal, DEVALM01 - Development HP Quality Center, devdb01u - Development SAP Portal database, DEVDQM01 - Development SAP BOBJ Data Quality Management, DEVLVC01 - Development HP LoadRunner, IESDC02 - IES Domain Controller, prddb01u - Production SAP Portal database, prddb02u - Production non-SAP Oracle databases, PRDDQM01 - Production SAP BOBJ Data Quality Management, PRDI3U - Production MQ Series and SAP Business Connector, PRDSROUTE01 - SAProuter used for connection to SAP for software support, qasdb01u - Quality Control SAP Portal databases, qc6dca0u - Quality Control SAP ECC DB/CI server, qcpapp1u - Quality Control SAP ECC application server, qcpdca0u - Quality Control 2 SAP ECC DB/CI server, QEPCIA0U - Quality Control SAP Portal, qppdca0u - Quality Control 2 SAP ECC DB/CI, QVPCIA0U - Quality Control SAP Portal, qwpdca0u - Quality Control SAP Business Warehouse DB/CI, sc2dca0u - Sandbox SAP ECC DB/CI, STGW6U (CTC) - SAP BOBJ staging server located in CTC DMZ
148	Exhibit I.1, IES - DPH COPA OwnedIT Assets		IES Tab	Are the servers defined as DPH servers, SAP servers? If so, please indicate what SAP Component these are.	The servers designated as DPH systems do not host SAP software. They are used by the DPH for management and support of the AIX or VMWare environments.
149	Schedule F, COPA Data Center Statement of Work	3.2.4.3.8	User Account Management – page 108	Is the Commonwealth requesting that Offerors provide SAP security? If so, would the Commonwealth please provide the total number of SAP users for all production and non-production users who will have access to the systems?	The Commonwealth will perform SAP software application security administration for all SAP systems. The selected Offeror is required to provide operating system level user administration for CoPA staff supporting the SAP applications. All Commonwealth users (Commonwealth employees, business partners, contractors, etc.) are potential SAP users.

150	Exhibit B.1, DPH – Asset List	DOR Tav		The last 13 rows appear to be SAP servers. Would the Commonwealth please confirm that these are indeed SAP servers: EP, BOBJ, BI/BW Java. Also, please clarify what SAP components RMP, Production, Production Master Media Server, and Migration servers are. Are these SAP ABAP, JAVA, NetWeaver systems? Or are they SAP 3rd Party systems?	The following list provides details on the 13 servers, indicating if they are SAP or Non-SAP servers. RVDPHRPX- SAP NetWeaver 7.3 Java Ent. Portal RVDPHRPP- Not currently used; RVDPHROD- SAP NetWeaver 7.3 Java BOBJ CPS RVDPHROX - SAP Netweaver 7.3 Java BOBJ RVDPHROT - SAP Netweaver 7.3 Java BOBJ RVDPHROQ - SAP Netweaver 7.3 Java BOBJ CPS RVDPHRXJ - Not currently used RVPDPHDC1 - Non-SAP Server - SQL Server RVPDPHDC2 - Non - SAP Server - Data Masking Engine RVDPHROP1 - SAP Netweaver 7.3 Java CPS RVDPHROP2 - SAP Netweaver 7.3 Java CPS RVDPHMMBK1 - Non-SAP Server RVDPHDC3 - Non-SAP Server - SQL Server

151	Schedule F, COPA Data Center Statement of Work	3.2.5.5 3		Would the Commonwealth please describe the client workstation OS distribution used in the COPA environment – Windows, MAC, etc.? Please describe the Outlook/email client versions used (i.e., Outlook 2003, etc.), and is there a current program to maintain a minimum standard version?	The Commonwealth currently has various desktop client workstation OS distributed in the COPA environment. 95% of Commonwealth desktop clients utilize Microsoft Windows operating systems (e.g. Windows 7, XP), none of which are older than XP. In addition, the Commonwealth has a limited number of Macintosh and Linux operating systems for desktop clients. Linux desktop clients are mainly used to connect to Virtual desktop Infrastructure (VDI) which uses Windows OS environment. As the Commonwealth use of VDI increases, additional operating systems may be used to connect to VDI. The Commonwealth currently has various Outlook/email client versions distributed in the COPA environment. The Windows based desktop clients use Outlook 2003, 2007, 2010 and a few have Office XP version. The Macintosh OS desktop clients use Mail.
152	Schedule F, COPA Data Center Statement of Work	3.2.5.5 10		Would the Commonwealth please describe the supported mobile device types/OS and breakdown the approximate number of devices by type (Blackberry, Android, iOS, etc.)? Is there a projected growth rate on mobile devices in the environment? Is there a current MDM application in use for the mobile devices?	The Commonwealth cannot provide an approximate number of mobile devices by OS. The service must be able to support iPhone/iPad and Android devices, and Blackberry Enterprise Server. The Commonwealth cannot provide a projected growth rate on mobile devices in the environment. The Commonwealth is implementing Airwatch but does not have a timeframe on when it will be fully rolled out.
153	Schedule F, COPA Data Center Statement of Work	3.2.5.5 15		For encryption, is the ability to encrypt email internally desired or only needed for email sent externally?	Yes, the Commonwealth requires the ability to encrypt email internally as well as externally.
154	Exhibit A, Commonwealth Network Environment	Target Data Center	P2	How many concurrent PSP users should the Offeror assume will connect to the Consolidated Data Center and how many will connect via IPSec vs. SSL VPN, vs. Copanet WAN?	All PSP users connect through COPANET using the same route to the Consolidated Data Center whether they are using IPSEC or SSL VPN.
155	Exhibit A, Commonwealth Network Environment	Target Data Center	P2	How many concurrent NON PSP users should the Offeror assume will connect to the Consolidated Data Center and how many will connect via IPSec vs. SSL VPN, vs. Copanet WAN?	The Commonwealth cannot provide the number of concurrent users. The Commonwealth has provided a bandwidth report as part of Exhibit P – Enterprise Internet Bandwidth Utilization.
156	Schedule F, COPA Data Center Statement of Work	3.2.1.1.4	32	What business partners or third parties will not provide WAN routers and premises equipment to connect the circuits which they are providing, to the cnetwrks in the target data center ?	Currently all Business Partners must provide Ethernet connectivity. The type of premise equipment depends on the connectivity needed and is negotiated with each Business Partner.

157	Schedule F, COPA Data Center Statement of Work	3.2.4.7	Database Management Services	Regarding open systems, would the Commonwealth please provide the database vendor platforms required by the Commonwealth for database management services (i.e., Oracle, MS SQL, DB2, etc.)?	Currently the database vendor platforms vary by agency and applications. DPW has a Database group that manages its Oracle, SQL Server, and Unisys mainframe DMS and RDMS databases. DOR: Oracle, MS SQL, DB2, Sybase, IMS Health: Oracle, MS SQL, Sybase PennDOT: RDMS instances: z/OS: IMS is used in Sandbox (PDTT), Pre-Prod (PDT1) and Prod (PDT0) 1 instance pre environment, DB2 is used in Sandbox (PDTT) 1 instance, Pre-Prod (PDT1) 5 instances and Prod (PDT0) 2 instances. z/VM: Oracle is used in Pre-Prod (DOTLNX01) 7 instances and Prod (DOTLNX02) 2 instances. L&I: Oracle Database, Microsoft SQL Server, DB2 z/OS, IMS, DB2 UDB, Sybase ASE Additional information regarding database vendor platforms will be documented as part of the discovery process in transition planning.
158	Exhibit E.1 – DLI, Datacenter Inventory Template	Applications Tab	rows 62 - 78	Does the Commonwealth own the iSeries (AS400) hardware and LPP program software products? Is the Commonwealth the original purchaser of the iSeries license and LPP program software products and available for transfer to a providers hardware asset?	The iSeries hardware is owned by Unisys. The LPP program is a Labor and Industry in-house written system.
159	Exhibit E.1 – DLI, Datacenter Inventory Template	Applications Tab	rows 62 - 78	What is the long term strategic direction for the iSeries platform?	The Commonwealth plans to move off of the iSeries platform within the next two years.
160	General Question	N/A	N/A	Is Oracle ERP in scope? It is not listed in the software inventory.	PLCB's Oracle ERP solution is not in scope except for the infrastructure hosting that supports the Oracle ERP solution.
161	General Question	N/A	N/A	Does each agency/organization under the Commonwealth have its own security policy or program?	The Commonwealth has defined IT policies (ITBs) and directives that must be followed by the enterprise. In addition, some agencies have more detailed and specific policies depending upon the agency's business requirements.

162	General Question	N/A	N/A	How is DLP implemented today within the Commonwealth? Are there separate instances with different tools? Is it implemented per agency	Currently the Commonwealth uses Cisco Ironport for egress email DLP at the enterprise level.
163	General Question	N/A	N/A	a) Have any data discovery or data reduction initiatives taken place? B)Are there any standards around data storage, retention, encryption, etc.?	a) On a case by case basis by application, data discovery or reduction activities have taken place. No enterprise data discovery or data reduction initiatives have taken place. b) Data retention, data storage, or encryption policies will be determined by IT policy, law, and the requirements of the RFP The Commonwealth's data retention polices. Are set out in Management Directive 210.5 (Commonwealth of PA State Record Management Programs) and several Information Technology Bulletins on this subject. Management Directives and ITBs can be found at http://www.portal.state.pa.us/portal/server.pt/community/policies/10301/management_directives/551950 and http://www.portal.state.pa.us/portal/server.pt?open=514&objID=210791&mode=2 ITBs SEC020 (Data at Rest) and SEC031 (Data in Motion) define the Commonwealth's policies on data at rest and data in motion. Individual agencies may have additional data retention, data storage, or encryption policies, such as the FBI's CJIS Security Policy, IRS Pub 1075, FIPS 140-2, etc. The selected Offeror must identify any additional applicable requirements during transition for individual services and comply with those requirements.
164	General Question	N/A	N/A	How is RSA Archer used today? What information is provided to Archer? What components of Archer are implemented today?	RSA Archer is used to provide audit and compliance assistance within EDC. The following modules are used - Enterprise, Risk, Policy, Threat. At this time there are no data feeds connected to Archer.
165	General Question	N/A	N/A	Is it permissible for Offerors to submit documents not available in Microsoft Office format in Adobe PDF format only (e.g., audited financial statements, insurance documentation, etc.)?	Yes.

166	Schedule I, Offeror Pricing Forms	1.Volumetrics	Row no 190, Col E	Would the Commonwealth please confirm if the total storage listed in baseline quantity includes the Production and Disaster Recovery (DR)? If so, would the Commonwealth provide a breakup of production volumes and DR volumes?	The baseline quantity includes production only. The configuration definitions tab identifies which configurations include DR. Each configuration has associated volumetrics. The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. Actual volumes may vary.
167	Schedule I, Offeror Pricing Forms	1.Volumetrics	Row no 192, Col E	Does the baseline quantity for "server tape stored" include Production and Disaster Recovery (DR)? If so, please provide a breakup of production and DR volumes.	The baseline quantity includes production only. The configuration definitions tab identifies which configurations include DR. Each configuration has associated volumetrics. The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. Actual volumes may vary.
168	Schedule F, COPA Data Center Statement of Work		101	Would the Commonwealth please provide the current Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) categorized by server tier/application?	See B.9 – DPH – Recovery Time Objectives for a list of RTOs for applications in the DPH. The Commonwealth cannot provide RPO documentation; this information will be documented as part of the discovery process in transition planning. This is a confidential document. To receive a copy, please contact Sheryl Kimport, the Issuing Officer.
169	Addendum 7 Questions and Answers Round 1 Part 3	Question #45	7	The Commonwealth's response to question #45, stated: "The 60% requirement stated in Part III-4 applies to all prime contractors. No SDB points will be awarded to an Offeror unless the company serving as the prime contractor directly performs at least 60% of the total contract value." "Total Contract Value" implies the inclusion of labor, facilities, hardware, software, telecommunications, office space, etc. Could the Commonwealth please confirm that the aforementioned components should be included in total contract value?	The 60% requirement in Part III-4 has been deleted and Part II-9 of the RFP has been revised.

170	Addendum 7 Questions and Answers Round 1 Part 3	**Question #45**	7	Related to question #45, the Commonwealth has made no commitment to a baseline volume. As such, legally, there is no financial commitment associated with this contract. In this case the Total Contract Value = $0. Given this, it would be impossible to calculate the percentage of work performed (i.e. the 60% requirement) of total contract value, because the denominator is 0. In such an event, no vendor would qualify for any of the Small Diverse Business Participation points. Is our interpretation correct?	The 60% requirement in Part III-4 has been deleted and Part II-9 of the RFP has been revised.
171	**Request for Proposal**	II-9, B., 1. III-4, C., 1.	21 24	Section II-9, subsection B, item 1, of the RFP on page 21 states "Offerors must include a numerical percentage which represents the total percentage of the work (as a percentage of the total cost in the Cost Submittal) to be performed by the Offeror and not by subcontractors and suppliers." As this relates to the 60% requirement in RFP section III-4, item C.1 on page 24 of the RFP, can the Commonwealth provide guidance on how to meet the 60% requirement given the amount of facilities, hardware, software, telecommunications, office space, etc. that would have to be included in the denominator of this calculation?	The 60% requirement in Part III-4 has been deleted and Part II-9 of the RFP has been revised.
172	Questions and Answers – Round 1 Part 3 RFP	29 11-9, B,2, a	21	The answer to this question restated the requirement to provide a "numerical percentage"; however, the answer did not address how a "dollar amount of each subcontract commitment to a Small Diverse Business" (as called for in the RFP Part II-9, B, 2, page 21) can be provided since the Commonwealth is not committing to a minimum participation. In other words, given that the Commonwealth is unwilling to provide any level of financial commitment or any level of committed participation, please clarify how the "dollar amount" requirement should be calculated.	Part II-9 of the RFP has been revised.
173	General Question			The current contract with the Unisys Corporation-Exhibit 1.02(31), within (Article 34.0- Service Level Credits) document does not exist. Our SLA Manager needs the information within Exhibit 1.02(31) to complete the review of the SLAs. Could you please send us Exhibit 1.02(31)?	The contract documents have been posted on the Pennsylvania Treasury website http://contracts.patreasury.gov/View.aspx?ContractID=228198.

174	General Question			The current contract with the Unisys Corporation- Exhibit 21.01, pages 7-33 are cut off in the PDF file that is found online in the eMarketplace. Could you please send us a copy of the Exhibit 21.01 that includes all of the pages so there are not cut off pages due to a landscape orientation?	The contract documents have been posted on the Pennsylvania Treasury website http://contracts.patreasury.gov/View.aspx?ContractID=228198.

Addendum 16 – New and Revised Answers

Revised Answers

Addendum 3 - Round 1, Part 1					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
24.	Appendix A	9 (a)	10	Will Offeror have any responsibility for logical access (LDAP, Exchange, Active Directory, etc.)?	~~Exchange as a Service is included within the scope of the RFP but the other services such as LDAP and Active Directory will remain under the Commonwealth's control. However, the selected Offeror must provide the equipment to operate these services.~~ **Revised Answer:** Exchange as a Service has been removed from this RFP. Schedule F, I, J.2 and J.3 have been revised to remove exchange as a service.

Addendum 4 - Round 1, Part 2					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
69.	Schedule F	3.2.5 Capacity on Demand Services	133-141	a.□ Does CoPA have difficulty managing peaks and valleys in demand and workload in their test / dev environments? b.□ Is MS Exchange as a service considered in or out of scope? c.□ Can GR resources be utilized for back office functions in our delivery model? d.□ Is CoPA willing to relinquish architectural control in a capacity on demand environment? e.□ Is the target for Image Activation in a capacity on demand environment under 24 hours? f.□ Is CoPA willing to sign up for a minimum baseline? g.□ Is CoPA flexible to change its standardized service request process? h.□ Is CoPA comfortable with the Agencies documenting requirements, but the Offeror defining the technology and service solution against those requirements to optimize across the Data Center? i.□ Is CoPA willing to relinquish control over outage windows and when/ how images are patched for their capacity on demand?	~~a.□ Yes.~~ ~~b.□ In scope.~~ ~~c.□ Please define "GR resources."~~ ~~d.□ No. The Offeror must propose an architecture and the Commonwealth then will approve or disapprove before implementation.~~ ~~e.□ Yes, the Commonwealth is, however, always looking for the ability to deliver services in a shorter interval.~~ ~~f.□ No.~~ ~~g.□ Yes.~~ ~~h.□ No. The Offeror must propose an architecture and the Commonwealth then will approve or disapprove before implementation.~~ ~~i.□ No~~ **Revised Answer:** a.□ Yes. b.□ Exchange as a Service has been removed from this RFP. Schedule F, I, J.2 and J.3 have been revised to remove exchange as a service. c.□ Please define "GR resources." d.□ No. The Offeror must propose an architecture and the Commonwealth then will approve or disapprove before implementation. e.□ Yes, the Commonwealth is, however, always looking for the ability to deliver services in a shorter interval. f.□ No. g.□ Yes. h.□ No. The Offeror must propose an architecture and the Commonwealth then will approve or disapprove before implementation. i.□ No

Addendum 7 - Round 1, Part 3					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
38	Schedule F	2.3.3	10	The services framework graphic notes "Exchange as a Service" as a capacity on-demand/additional service offering. This offering is not described anywhere else in schedule F. Please provide requirements and expectations around this service.	~~Schedule F has been amended and reissued to include requirements.~~ **Revised Answer:** Exchange as a Service has been removed from this RFP. Schedule F, I, J.2 and J.3 have been revised to remove exchange as a service.

Addendum 15 – New Answers					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
121	Questions and Answers – Round 1 Part 3	34		The Commonwealth's Microsoft Exchange Enterprise License Agreement may be less expensive than those that may be purchased by an Offeror. To provide greater savings to the Commonwealth, will the Offeror be granted permission to use this or similar Commonwealth ELAs?	~~For the purpose of submitting a proposal, Offerors should assume they will not be permitted to use the Commonwealth's Microsoft Exchange Enterprise License Agreement.~~ **Revised Answer:** Exchange as a Service has been removed from this RFP. Schedule F, I, J.2 and J.3 have been revised to remove exchange as a service.

Addendum 9 - Round 1, Part 5					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
9	Appendix A	11 (b) (2)	13	Certification specified in this section are those held by individuals rather than the organization. What is the Commonwealth's requirement for quantity of professionals holding those certifications?	~~At a minimum, the Chief Information Security Officer (CISO) provided by the Offeror must maintain current security certifications as stated in referenced section of Appendix A. The Commonwealth has not defined the number of individuals that must hold the referenced certifications. Offerors should propose their best solutions.~~ **Revised Answer:** At a minimum, the Security Manager provided by the Offeror must maintain current security certifications as stated in referenced section of Appendix A. The Commonwealth has not defined the number of individuals that must hold the referenced certifications. Offerors should propose their best solutions.

New Answers

Addendum 16 – New Answers					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Addendum 16 – New Answers					
	Doc	**Sec**	**Pg**	**Question**	**Answer**

Addendum 16 – New Answers					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Addendum 16 – New Answers					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Addendum 16 – New Answers					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Addendum 16 – New Answers					
	Doc	**Sec**	**Pg**	**Question**	**Answer**

Addendum 16 – New Answers					
	Doc	**Sec**	**Pg**	**Question**	**Answer**

Addendum 16 – New Answers					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Addendum 16 – New Answers					
	Doc	**Sec**	**Pg**	**Question**	**Answer**

Addendum 16 – New Answers					
	Doc	**Sec**	**Pg**	**Question**	**Answer**

Addendum 16 – New Answers					
	Doc	**Sec**	**Pg**	**Question**	**Answer**

Addendum 16 – New Answers					
	Doc	**Sec**	**Pg**	**Question**	**Answer**

Addendum 16 – New Answers					
	Doc	**Sec**	**Pg**	**Question**	**Answer**

Addendum 16 – New Answers					
	Doc	**Sec**	**Pg**	**Question**	**Answer**

Addendum 16 – New Answers					
	Doc	**Sec**	**Pg**	**Question**	**Answer**

Addendum 16 – New Answers					
	Doc	**Sec**	**Pg**	**Question**	**Answer**

Addendum 16 – New Answers					
	Doc	**Sec**	**Pg**	**Question**	**Answer**

Addendum 16 – New Answers					
	Doc	**Sec**	**Pg**	**Question**	**Answer**

Addendum 16 – New Answers					
	Doc	**Sec**	**Pg**	**Question**	**Answer**

Addendum 16 – New Answers					
	Doc	**Sec**	**Pg**	**Question**	**Answer**

Addendum 16 – New Answers					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
					A
					A
					A
					A
					A
					A

Addendum 16 – New Answers					
	Doc	**Sec**	**Pg**	**Question**	**Answer**

Addendum 16 – New Answers					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Addendum 16 – New Answers					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Addendum 16 – New Answers					
	Doc	**Sec**	**Pg**	**Question**	**Answer**
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Addendum 16 – New Answers					
	Doc	**Sec**	**Pg**	**Question**	**Answer**

Addendum 16 – New Answers					
	Doc	**Sec**	**Pg**	**Question**	**Answer**

Addendum 16 – New Answers					
	Doc	**Sec**	**Pg**	**Question**	**Answer**

Best and Final Offer - Revised Answers

Revised Answers

Revision for all previously posted answers
Revision: All references to "Sheryl Kimport, Issuing Officer" should reference "Issuing Officer".

Revised answer (original answers posted as Addendum 7 - Round 1, Part 3)					
	Doc	Sec	Pg	Question	Answer
30	Schedule F	3.3	141	"Initial transition approach of the Commonwealth's mainframe and SAP environments requires that the results be as close to the Commonwealth's current configurations as technically possible". Since the configurations described in the exhibits are not reflected in Schedule I, (Pricing Forms) is the Commonwealth financially responsible for paying for any gaps to ensure that these configurations meet or exceed current configurations?	~~Offerors must provide a catalog of services, including pricing, that includes sufficient detail to allow the Commonwealth to order the desired configuration(s) required to satisfy the need of the application owner. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all-inclusive representation of every service desired by the Commonwealth.~~ Offerors must provide the requested catalog of services, including pricing, that includes sufficient detail to allow the Commonwealth to order the desired configuration(s) required to satisfy the need of the application owner. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all-inclusive representation of every service desired by the Commonwealth.
68	Schedule F	3.2.2.2	67	What does the Commonwealth consider to be reasonable timeframe to receive written acceptance regarding ready for use and user acceptance testing? At what level will such approvals be required i.e. system, application, agency, etc.?	~~The Commonwealth will not unreasonably withhold or delay the acceptance or rejection of the Offeror's written notice regarding "ready for use". The range may vary but will generally fall within two (2) days to two (2) weeks based on many factors such as required Commonwealth verifications, Commonwealth personnel availability, complexity of the new environment, etc.~~ The Commonwealth will not unreasonably withhold or delay the acceptance or rejection of the Offeror's written notice regarding "ready for use". The range may vary but will generally fall within two (2) days to two (2) weeks based on many factors such as required Commonwealth verifications, Commonwealth personnel availability, complexity of the new environment, etc.

Revised answer (original answers posted as Addendum 8- Round 1, Part 4)					
	Doc	Sec	Pg	Question	Answer
36	Schedule F	3	12	This Task section states that the Commonwealth has provided detailed information on the current environments in the exhibits. It also states that the Offeror shall utilize the exhibits as the baseline requirements (in terms of services, quantities and bandwidth) for developing its proposal. Be aware that the "Volumetrics", reflected in Schedule I, do not reflect the current services, quantities, or the bandwidths that are reflected in the exhibits. Please explain this inconsistency. If the "Volumetrics" are only to be used for cost evaluation, how will the Commonwealth actual pay for the configurations reflected in the exhibits and being requested in this requirement?	~~Schedule I will be used to evaluate pricing. The Offeror is to provide a catalog of services within the Catalog of Services tab of Schedule I, including rates that are consistent with the rates proposed throughout Schedule I. This service catalog will be used to determine the cost of each service provided to the Commonwealth. The invoice must reflect the items and rates listed in the catalog with quantities purchased.~~ Schedule I will be used to evaluate pricing. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all-inclusive representation of every service desired by the Commonwealth. The Offeror is to provide the services within the Catalog of Services tab of Schedule I, at the rates proposed in Schedule I. This Catalog of Services will be used to determine the cost of each service provided to the Commonwealth. Invoices must reflect the items and rates listed in the catalog with quantities purchased. Changes to the requested catalog will be addressed with the selected Offeror via the contract change control process.
37	Schedule F	3.3.2	143	This section states that "The selected Offeror shall not charge the Commonwealth for any Services currently Provided by the DPH or EDC until all of the Services provided by the DPH and EDC (Group 1) have been successfully transitioned." Can any fees be charged, such as transitions fees or any other fees, prior to transitioning all of the DPH and EDC services? Can any fees be charged to the Commonwealth prior to the expiration date of the existing contract scheduled for December 31, 2014?	~~Section 3.3.2. (Transition Planning/Governance) of Schedule F was revised by Addendum #4. The revised section states the following:~~ ~~The selected Offeror shall not charge the Commonwealth for any Services currently provided by the EDC until all of the Services provided by the EDC have been successfully transitioned.~~ ~~The selected Offeror shall not charge the Commonwealth for any Services currently provided by the DPH until all of the Services provided by the DPH have been successfully transitioned.~~ ~~The selected Offeror shall not charge the Commonwealth for any Services currently provided by an Agency's datacenter (example: DLI, DPW, DOR, DOH, PSP) until all of the Services provided by that datacenter have been successfully transitioned.~~ ~~The selected Offeror may charge the Commonwealth for new services after the contract effective date, excluding services that must be transitioned as described above.~~ The referenced requirement in section 3.3.2 has been deleted. Fees may be charged at any time pursuant to Part IV-3.E of the RFP which has been revised to state: E. **Payment for Services** The selected Offeror may bill for a Service, including those transitioned from the EDC, DPH or a Commonwealth Agency datacenter, once the Commonwealth accepts the Service via ITSM.

74	Schedule I	Top	2	At the top of page 2, there is a reference to “This Exhibit B.5”. Is that correct?	~~The reference is incorrect. The correct reference is to "Schedule I.1"~~ The reference is incorrect. The correct reference is to "Schedule I."

Revised answer (original answers posted as Addendum 9 - Round 1, Part 5)					
	Doc	Sec	Pg	Question	Answer
41	Schedule I Offeror Pricing Forms	4.Managed Services (Only) 10. Catalog of Services		How do unit rates for catalog services tab #10 differ from unit rates to be provided in Managed Services tab #4?	~~The Offeror is to fill Tab #4 (Managed Services Only) with the total cost of the combined catalog items to meet the configuration defined within the Tab.~~ ~~The Offeror is to fill Tab #10 (Catalog of Services) with the individual price point / configuration items that are being offered to the Commonwealth.~~ The Offeror is to fill in Tab #4 (Catalog of Services) with the individual price point / configuration items that are being offered to the Commonwealth.
42	Schedule I	1.Volumetrics		Does the Commonwealth need separate volume metrics for database support services or disaster recovery? Or should these services be allocated across all pricing rates?	~~The Offeror is to provide Database support services within Tab 6 (Technical Staff Rate Card) only. DR services are specified within the scenarios defined within Tab 1 (Volumetrics). Therefore, the Offeror should not allocate these services across all pricing rates. Information provided by the Offeror in Schedule I is intended for cost evaluation purposes only.~~ The Offeror is to provide Database support services within Tab 3 (Technical Staff Rate Card) only. DR services are specified within the scenarios defined within Tab 1 (Volumetrics). Therefore, the Offeror should not allocate these services across all pricing rates. Information provided by the Offeror in Schedule I is intended for cost evaluation purposes only.

Revised answer (original answers posted as Addendum 11 - Round 1, Part 6)					
	Doc	Sec	Pg	Question	Answer
3	Asset Schedules	All	All	Please provide the ages of the assets or should the Offeror make a simplifying assumption such as 20 percent of the assets to be refreshed each year?	~~For the purposes of submitting a proposal Offerors should assume 20% of the assets to be refreshed each year.~~ The Commonwealth is purchasing services that have associated SLA's and the selected Offeror must provide the services within those SLAs. Offerors should use their best judgment on the service life of their infrastructure and how often that infrastructure must be refreshed to meet the SLAs.

7	Schedule F Schedule I			For those services requested in the SOW without a corresponding Baseline Units - Volumetric in Schedule I, does the Commonwealth expect those prices to be included in the Service Catalog? Without a baseline, how will the Commonwealth ensure a level evaluation between bidders? Examples of such services include: DR Planning and Testing, ERP Hosting, Security & Firewall and Database Management Services.	~~1. Yes, provide a price for all services in the catalog.~~ ~~2. The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all-inclusive representation of every service desired by the Commonwealth.~~ 1. Yes, provide a price for all services requested n the Catalog of Services. Additional services will be addressed with the Selected Offeror via the contract change control process. 2. The Commonwealth has established multiple scenarios of infrastructure configurations specifically for pricing evaluation, as set forth in Schedule I. The Volumetrics in Schedule I will be used to evaluate Offerors' cost proposals and are not a minimum commitment or an all-inclusive representation of every service desired by the Commonwealth.

Revised answer (original answers posted as Addendum 11 - Round 2, Part 1)					
	Doc	Sec	Pg	Question	Answer
7	Schedule F	3.2.3.2	89	The Commonwealth requires the offeror to provide a structured disk-2-disk backup approach for systems that currently utilize this approach. Since there appear to be only options to provide pricing for tape, where in Schedule I should the offeror place pricing for their disk-2-disk backup approach?	~~Pricing should be provided in Schedule I, Tab 10 (Catalog of Services).~~ Pricing should be provided in Schedule I, Tab 4 (Catalog of Services).

Revised answer (original answers posted as Addendum 12- Round 1, Part 7)					
	Doc	Sec	Pg	Question	Answer
9	Services Catalog	Schedule C	2	Services Catalog is blank. Can you please provide a catalog of services that are relevant to this project, including GIS services?	~~This was intentionally left blank for the Offerors to provide the proposed catalog for Commonwealth review and evaluation. Schedule I tab 10. Catalog of Services has been revised to include a sample Catalog of Services. GIS projects will be managed in the same manner as other Commonwealth projects. The scope of this procurement does not include outsourcing of GIS specific services.~~ See revised Schedule C, which removes the requirement for Offerors to submit Schedule C as part of the proposal.

Revised answer (original answers posted as Addendum 15, New Answers)

	Doc	Sec	Pg	Question	Answer
3	Schedule F Schedule I Offeror Pricing Forms Schedule J.1			There appear to be differences in storage support definitions between the SOW and Schedule I. The SOW sets forth Basic, Committed and Dedicated in section 3.1.3 on p. 20. Schedule I mentions Tier 1, 2 and 3 are associated with service levels and indicates these are defined in Schedule J.1, but they are not. However, Config 1, 2 and 3 is defined in Schedule I. Could the Commonwealth please reconcile?	~~For purposes of submitting proposals Offerors should assume the Configurations listed in Schedule I - Offeror Pricing Forms are Dedicated. Schedule I has been revised to remove the "Tier" references from Enterprise Storage. Offerors should also include pricing in Schedule I Catalog of Services for Basic and Committed.~~ For purposes of submitting proposals Offerors should assume the Configurations listed in Schedule I - Offeror Pricing Forms are Dedicated. Schedule I has been revised to remove the "Tier" references from Enterprise Storage.
6	Schedule F	3.2.5 Capacity on Demand Services	133-141	a. Does CoPA desire to better manage their capacity plan by having an online data backup capability that can flex as the information requirements expand over the next several years so capacity at the production centers does not have to be added? Does CoPA have detailed knowledge of their data access patterns to provide to a vendor who can then determine what data is eligible to move from tape to online storage, at a lower cost with greater backup recovery success rates then tape? Does CoPA have a written archiving policy, and does it currently move fixed data regularly to lower cost storage? Does CoPA have a requirement for Virtual Server Recovery outside of the primary geography?	~~a. The Commonwealth seeks the best solution for capacity planning. Offerors should include the services they offer in their technical proposal and as part of Schedule I tab 10. Catalog of Services.~~ ~~b. No, the Commonwealth does not have data access patterns to provide to an Offeror. The Commonwealth will work with the selected Offeror to determine the best solution when selecting services from the Service Catalog.~~ ~~c. The Commonwealth currently has a written archiving policy. Fixed data is currently moved regularly to lower cost storage.~~ ~~d. Please clarify or provide example defining "Virtual Server Recovery outside of the primary geography".~~ a. The Commonwealth seeks the best solution for capacity planning. Offerors should include the services they offer in their technical proposal and as part of the requested Schedule I tab 4. Catalog of Services. b. No, the Commonwealth does not have data access patterns to provide to an Offeror. The Commonwealth will work with the selected Offeror to determine the best solution when selecting services from the Service Catalog. c. The Commonwealth currently has a written archiving policy. Fixed data is currently moved regularly to lower cost storage. d. Please clarify or provide example defining "Virtual Server Recovery outside of the primary geography".
20	Schedule F	3.3.2.1	150	What is the expected transition timeframe and associated acceptance criteria for all the existing agency service management systems to the Offeror's service management platform?	~~See milestone M-9 ITSM System Integration in Schedule D - Transition Milestones.~~ See milestone M-8 ITSM System Integration in Schedule D - Transition Milestones.

27	Schedule I – Offeror Pricing Forms	Managed Services		The Commonwealth has indicated that Contract signing = Effective Date = Start date. The Commonwealth has also stated that Transition is part of the base term of the contract and transition is prior to Steady State. Can "Transition Charges" be billed prior to the DPH/EDC being fully migrated and/or prior to December 31, 2014? If Steady State RU's are not "available" until the DPH/EDC have been fully migrated (which is required by 12/31/14) do the Volumetrics not come into play until 1/1/15 or can RU pricing begin with a fully migrated DPH/EDC and prior to 1/1/15?	~~Schedule I – Offeror Pricing Forms has been revised. Transition costs are now deliverable based and cannot be billed until the Commonwealth accepts the deliverable and all associated milestones. Refer to Schedule D – Transition Milestones and Schedule K – Key Program Deliverables which set forth acceptance criteria and due dates.~~ ~~Applications cannot be billed until the application has been fully transitioned to the Offeror and accepted by the Commonwealth.~~ Schedule I - Offeror Pricing Forms has been revised. Transition costs are now to be included as part of the unit cost. Billing will commence upon service acceptance by the Commonwealth. Applications cannot be billed until the application has been fully transitioned to the Offeror and accepted by the Commonwealth.
31	Exhibit B.4			Does the Offeror have to provide a price for the software listed in Exhibit B.4? If so, where does the Offeror provide a price for third-party software?	~~Schedule I – Offeror Pricing Forms has been revised to include software pricing as part of the Catalog of Services tab.~~ Schedule I - Offeror Pricing Forms have been revised to include software pricing as part of Schedule I. Offerors must provide pricing for all software included in the Schedule I.
133	Schedule F – Statement of Work (Amended 2.18.13)	3.2.4.7	128	For which service tiers (Fully Managed, Managed Only, IaaS, etc.) are database services to be provided?	~~Database services may be required for all Tiers, based on the service ordered by the Commonwealth.~~ ~~Other than those provided for in the rate card in Schedule I there are no Database Administration functions required. The selected Offeror will be required to provide technical assistance to the Commonwealth's DBA staff. Offerors may include a Database Administration as a service in the Service Catalog.~~ Database services may be required for all Tiers, based on the service ordered by the Commonwealth. Other than those provided for in the rate card in Schedule I there are no Database Administration functions required. The selected Offeror will be required to provide technical assistance to the Commonwealth's DBA staff.

Revised answer (original answers posted as Addendum 16 – New Answers)					
	Doc	Sec	Pg	Question	Answer

11	Exhibit B.4, Schedule I, Third Party Software – Contractor Provided		Volume metrics Tab	Given certain software products are priced by the application server specifications (platform, # cpu's, # cores, etc.) Oracle for example, would the Commonwealth please provide the software vendors catalog part number that is associated to the quantity listed in B.4, DPH - Third Party Software – Contractor Provided?	~~No, the Commonwealth will not provide vendor catalog part numbers for the software listed in Exhibit B.4 as the proposed configurations are not required to duplicate the current configuration. The Offeror must provide a catalog of monthly single unit prices as part of its proposal. A single unit could be a single MIP, a single core, a single user, a single server, etc.~~ No, the Commonwealth will not provide vendor catalog part numbers for the software listed in Exhibit B.4 as the proposed configurations are not required to duplicate the current configuration. The Offeror must provide the requested catalog of monthly single unit prices as part of its proposal. A single unit could be a single MIP, a single core, a single user, a single server, etc.
19	Schedule D	All	All	The Transition Milestones defined in Schedule D do not align with the definitions found in Schedule I (i.e. M-2). Which set of Milestone definitions should be used for RFP submission?	~~Schedule I has been revised to align with the Milestones defined in Schedule D.~~ Schedule I has been revised and references to the Milestones defined in Schedule D have been removed.
20	Schedule I Exhibit E.43 DL1-UC Software	All 4.6.13		Section 4.6.13 does not appear to be included in Schedule I, Offeror Pricing form. Does the cost for maintenance and support for these software tools need to be included in the Offeror's proposal?	~~Any third party software needed for the Offerors proposed solution in addition to the software as listed in schedule I should be added to the Catalog of Services under "Additional Services." Maintenance and support must be provided for the software as set forth in Appendix A and included in the Offeror's proposal.~~ Offers must provide pricing for all software packages in Schedule I. Any software packages required to maintain the Offeror's proposed solution should be included in the unit prices in Schedule I.
34	6100022698 - Master Questions and Answers (4.16.13)	Item 2 Second question	Page 114	a) Is it correct to assume that all Transition services will be the responsibility of the incumbent and that no cost should be included in the pricing schedule? b) Could a bidder assume that all required Transition work will not need to be priced or that much of the work will be completed by the incumbent? c) If not, could the Commonwealth please clarify so that bidders do not incorrectly assume scope to be completed by the incumbent that actually should be included and evaluated as part of the RFP response?	~~a) No.~~ ~~b) Offerors must provide pricing for transition. See Schedule I tab 3 Transition Charges. Offerors should not assume that much of the work will be completed by the incumbent.~~ ~~c) Offerors should not assume all transition assistance as proposed or assumed necessary will be provided by the incumbent. The selected Offeror will not be responsible to pay for transition assistance provided by the incumbent. For purposes of submitting a proposal, Offerors should assume transition assistance provided by the incumbent will be minimal. The selected Offeror is responsible to fund all other transition costs.~~ a) No. b) Schedule I instructions have been updated to address how transition charges are to be provided. Offerors should not assume that much of the work will be completed by the incumbent. c) Offerors should not assume all transition assistance as proposed or assumed necessary will be provided by the incumbent. The selected Offeror will not be responsible to pay for transition assistance provided by the incumbent. For purposes of submitting a proposal, Offerors should assume transition assistance provided by the incumbent will be minimal. The selected Offeror is responsible to fund all other transition costs.

40	6100022698 - Schedule I - Offeror Pricing Forms – ammended xls	Volumemetrics Transition Charges, Managed Services		Are the prices to be shown on the Transition Charges tab to reflect the transition of the infrastructure counts reflected in the Volumemetrics tab or should the transition charges reflect the price for the relocation of the items shown in the Exhibits? If it is to reflect of the infrastructure counts reflected in the Volumemetrics tab we have no breakdown by agency to spread within the Transition Charges tab; please provide an agency breakdown of the counts within the Volumemetrics tab.	~~Transition Charges in Schedule I on the "Transition Charges" tab should reflect the price for the relocation of the items shown in the Exhibits and not the transition of the infrastructure counts reflected in the Volumemetrics tab.~~ Schedule I instructions have been updated to address how transition charges are to be provided.
47	Schedule K	D-10	23	Are there any differences between deliverables D-10.01 and D-10.02? Only D-10.01 is required for a Transition milestone and there is only 30 days between the two due dates.	~~Schedule I has been revised to align with the Milestones defined in Schedule D.~~ ~~Deliverable D-10.01 is the Gap Analysis Report and D-10.02 is to present the results of the Data Center Gap Analysis along with a Roadmap and Project Plan to address the recommendations identified in the analysis .~~ Deliverable D-10.01 is the Gap Analysis Report and D-10.02 is to present the results of the Data Center Gap Analysis along with a Roadmap and Project Plan to address the recommendations identified in the analysis .
48	Schedule I and Schedule B.4	Volumemetrics		The following items on Schedule I on the Volumemetrics tab under Third Party Software – Commonwealth Provided Contractor Maintained and Managed, but are documented in Exhibit B.4 which is defined as Third Party –Contractor Provided. Should the offeror provide the quote based upon the definition with in Schedule I or Exhibit B.4 for the following products? USPS Correct Address – Schedule I Volumemetrics Row 568; Exhibit B.4 item 204 IBM FileNet – Schedule I Volumemetrics Row 569; Exhibit B.4 item 205 Microsoft Sharepoint (with SA) – Schedule I Volumemetrics Row 570; Exhibit B.4 item 206 IBM Websphere MQ (Processor Value Unit) – Schedule I Volumemetrics Row 571; Exhibit B.4 item 207 Xerox XeroxDocuShare – Schedule I Volumemetrics Row 572; Exhibit B.4 item 208	~~Schedule I has been revised to align with Exhibit B.4.~~ Schedule I has been revised to align with Exhibit B.4. Offers must provide pricing for all requested software packages in Schedule I.

53	Schedule I-Offeror Pricing Forms	Catalog of Services Excel	Row 775	Should we price using BL/LIB with the DSI Virtual Tape, Robotic Devices or stand alone?	~~The Offeror must provide a catalog of monthly single unit prices as part of its proposal. A single unit could be a single MIP, a single core, a single user, a single server, etc. The configuration will be determined as part of transition planning. For purposes of this proposal the Offeror is to use Robotic Devices.~~ The configuration will be determined as part of transition planning. For purposes of submitting a proposal the Offeror is to use Robotic Devices.
91	Master Questions and Answers	#34	125	(a) Please describe in detail the application support to be provided in EDC's Fully Managed services where the Offeror will now assume responsibility for application support (i.e. application design, application development, application maintenance, which applications, products use, etc.). (b) Will this application support be provided as an optional service and billed on a T&M basis or should it now be bundled in one of the Resource Units for both Fully Managed or Managed Only categories in Schedule I?	~~a) Fully managed services require end to end support of all of the backend infrastructure, server hardware, operating systems and applications. It is all inclusive.~~ ~~b) Fully managed support will not be on a T&M basis. The support costs must be built in into the Fully Managed offering. Managed Only services include infrastructure support costs and do not include application level support costs.~~ a) Fully managed services require infrastructure application support including all backend infrastructure, server hardware, operating systems, and all other components of the Offeror's proposed solution. It is all inclusive. b) Infrastructure application support described in part a) above must be included in the unit prices.
98	Schedule I	Transition Charges	Transition Charges tab	On the Transition Charges Tab, M-2 is now Contract Management, but has been left off the Transition Charges Milestone table? Additionally, should Due Diligence now be listed as Data Gathering?	~~Schedule I has been revised to align with the Milestones defined in Schedule D. Yes, Due Diligence is now listed as Data Gathering.~~ Schedule I instructions have been updated to address how transition charges are to be provided.

Best and Final Offer - Questions and Answers (09/11/2013)

No.	Doc	Sec	Pg	Question	Answer
1	6100022698 - Schedule C - Services Catalog (09.03.13) (BAFO).doc	"(4) Mainframe Services - Include both IBM and Unisys Mainframe services"	Pages 4-5	This section states that software should be included, but the associated footnote "exhibit B1 DPH Asset List" on page 5 reflects hardware only. In addition, the mainframe system software listed in DPH Exhibits B.7 and B.8 is not reflected in Schedule I, Tab 5 "Software". By the use of the word "software" in this section, is the Commonwealth also expecting all of the necessary mainframe system software reflected in Exhibits B.7 and B.8 to be included in the resource unit pricing for Mainframe Services?	Yes, mainframe system software required for defined configurations must be included in the resource unit pricing for Mainframe Services.
2	6100022698 - Schedule D - Transition Milestones (09.03.13) (BAFO).docx 6100022698 - Schedule K - Key Program Deliverables (09.03.13) (BAFO).docx	Milestone M-2 D-11 Contract Management Plan	Page 2 Page 24	The BAFO update of Schedule K added Key Deliverable D-11.02 that is due 60 days after the Effective Date. Is Milestone M-2 due at 45 days after contract effective date or 60 days?	Milestone M-2 is due 60 days from the Contract Effective Date. Schedule D has been revised accordingly.

3	6100022698 - Schedule F - Datacenter Statement of Work (09.03.13)(BAFO).docx	2.1 Program Objectives	Page 6	This section states, "The Offeror must utilize the EDC as one of its datacenters and propose a minimum of one additional datacenter to meet the 2+ architecture requirement. It is the Offeror's option to utilize the EDC as one of its primary datacenters within its proposed solution." Throughout the RFP requirements, there is an expectation that the EDC must be used. Based on the above ambiguity, please confirm that the Offeror must utilize the EDC as one of the two data centers required.	Offerors must include the EDC in the proposed 2+ datacenter architecture.
4	6100022698 - Schedule I - Offeror Pricing Forms (09.03.13) (BAFO).xlsx	Tab "Configuration Definitions"	Rows 88, 89, 93, 94, 98, 99, 103, 104, 110, 111, 117, 119, 124, 125, 132, 133, 137, 138	Each of these configurations includes a configuration-related component that is later called out for pricing in tab "4. Catalog of Services" described simply as "Disaster Recovery Server". Does this component represent a duplication of the related configuration's specification (e.g. row 88's specification of "2-way Six-Core 2.4 GHz, 16 GB RAM, Mirrored 146 15K Hard Drives; Windows Server 2008 R2")? If not, what is the specification for the "Disaster Recover Server" noted in each configuration where this item appears?	Yes, this component represents a duplication of the related configuration's specification.

5	6100022698 - Schedule I - Offeror Pricing Forms (09.03.13) (BAFO).xlsx	Tab "Configuration Definitions"	"x86 Server Configurations", rows 95-104	Virtual server configurations for Windows (rows 95 - 99), Linux (rows 100 - 104), and IaaS (rows 129 - 138) include requirements for Firewall/IDS, Site-to-Site VPN, VPN Client, and VLAN. No specifications for these requirements are provided though they are listed as components requiring prices in tab "4. Catalog of Services", rows 196-405. With no other description provided we would anticipate definitions for these items as: • Firewall/IDS - firewall/IDS software running on ESX host or network based hardware which protects and separates the individual images • Site to Site VPN - software running on an ESX host or network based hardware to generate site to site VPN from data center to another facility • VPN Client - Remote administration access client such as RDP or SSH • VLAN - assignment of a VLAN and IP range for the server instance Please confirm or update these definitions and provide detailed specifications for each of Firewall/IDS, Site-to-Site VPN, VPN Client and VLAN components called out for virtual server configurations. These same items do not appear for the physical x86 server configurations in rows 83-94. Are these capabilities also required for physical x86 servers? If so, what would the specifications be for these components in the context of physical x86 server configurations?	Schedule I has been revised. The components and services required to meet the security requirements of the RFP for all compute services, including but not limited to Schedule F Sections 3.2.4.6 and 3.2.2.5, must be included in the base unit pricing for all configurations Scenarios presented in Schedule I are for evaluation purposes only.

6	6100022698 - Schedule I - Offeror Pricing Forms (09.03.13) (BAFO).xlsx	Tab "Configuration Definitions" Tab "1. Volumetrics"	Rows 88, 93, 98, 103, 110, 117, 119, 124, 125, 132, 137 Rows 187-189	Each of these configurations indicate that restoration will be from the "Backup-Site's Local SAN Storage". Please provide specifications for the volume and type of SAN storage that each of these configurations will need to have replicated in the Backup Site's Local SAN Storage. Is this SAN storage included in the volumes provided in tab "1. Volumetrics", rows 187-189? If not, please indicate specifications for the SAN storage that is not incorporated into the volumes provided in tab "1. Volumetrics", rows 187-189.	Actual specifications for volume and type of SAN storage will be based upon services ordered. Scenarios included in Schedule I are for evaluation purposes only. Yes, for evaluation purposes SAN storage is included in the volumes provided in tab "1. Volumetrics" of Schedule I.
7	6100022698 - Schedule I - Offeror Pricing Forms (09.03.13) (BAFO).xlsx	Tab "1. Volumetrics"	NA	With the expectation that AIX server configurations will include all hardware and software to be included in the RU pricing (and not in separate service catalog entries), which exhibits should be used for software and configuration information? The exhibits provided are not consistent with the same level of detail or completeness of information. Reference the exhibits below: Exhibit E.1 for DLI Exhibit H.4 for DOR Exhibits I.2; I.3; I.13 for IES	Base unit pricing for all components must include hardware and software (operating system, system management, and security) required to provide the Offeror's proposed solution for the services requested in the RFP. Scenarios included in Schedule I are for evaluation purposes only. Any additional information needed will be documented as part of the discovery process in transition planning.
8	6100022698 - Schedule I - Offeror Pricing Forms (09.03.13) (BAFO).xlsx	Tab "4. Catalog of Services"	"P-Series Server Configurations", rows 406-491	Row 408 requests pricing for one half of a system core, but each of the resource unit configuration calculations (on rows 440, 450, 460, 470 and 481) treats this configuration item as if a whole core price was provided in cell D408. The pricing sheet appears to need either to double the amounts in column D (cells D440, D450, D460, D470 and D481) for each configuration or to ask for the price of a whole core in row 408. Please indicate the Commonwealth's intent or provide an update to Schedule I.	Schedule I has been revised.

9	6100022698 - Schedule I - Offeror Pricing Forms (09.03.13) (BAFO).xlsx	Tab "5. Software"	Row 42	The EMC Corporation's Symmetrix VMAX Fully Automated Storage Tiering for Virtual Pools (Fast VP) is not available as software separately from an EMC VMAX Disk Storage hardware system. Consequently, this software license is dependent upon the size of the hardware with which it will be used. Please provide the hardware specifications for the related EMC VMAX Disk Storage systems requiring this software.	Refer to Exhibit B.1 Shared SAN Storage lines 72-75 for the referenced hardware specifications.
10	6100022698 - Schedule I - Offeror Pricing Forms (09.03.13) (BAFO).xlsx	Tab "5. Software"	Row 116	Oracle's Exadata Storage Software is not available separately from the purchase of an Oracle Exadata system. Please provide the hardware specifications for the Oracle Exadata system that the Commonwealth will require that will be needing Oracle's Exadata Storage Software.	Refer to Exhibit B.1 DPW lines 1321-1326 for the referenced hardware specifications.
11	6100022698 - Schedule I - Offeror Pricing Forms (09.03.13) (BAFO).xlsx	Tab "5. Software"	Row 58	The Offeror has contacted Marble Computing Inc. to obtain new software licensing for this product. Marble Computing Inc. has informed the Offeror that the Commonwealth is the last client running the "OS DCD III Data Correlation and Documentation System". The vendor will be providing no new releases or software updates. In addition, Marble Computing will not provide any formal maintenance agreements on this software. Has the Commonwealth chosen a software solution to replace this product? If not, please provide a list of product features and functions that the Offeror can use to evaluate potential replacements.	The referenced software title has been removed from Schedule I. The Commonwealth will work with the Selected Offeror to acquire the software as part of transition planning.
12	6100022698 - Schedule I - Offeror Pricing Forms (09.03.13) (BAFO).xlsx	Tab "5. Software"	Row 101	The Offeror has attempted to obtain new license costs from Schema Systems Limited. We have not been successful in contacting this vendor. Is the Commonwealth still utilizing this software or have they chosen a new software solution to replace this product? If not, please provide a list of product features and functions that the Offeror can use to evaluate potential replacements.	The referenced software title has been removed from Schedule I. The Commonwealth will work with the Selected Offeror to acquire the software as part of transition planning.

13	6100022698 - Schedule I - Offeror Pricing Forms (09.03.13) (BAFO).xlsx	Tab "5. Software"	Row 205 Row 278	The Offeror has attempted to obtain new license costs from Western American Data. We have not been successful in contacting this vendor. Is the Commonwealth still utilizing this software or have they chosen a new software solution to replace this product? If not, please provide a list of product features and functions that the Offeror can use to evaluate potential replacements.	The referenced title has been removed from Schedule I. The Commonwealth will work with the Selected Offeror to acquire the software as part of transition planning.
14	6100022698 - Schedule K - Key Program Deliverables (09.03.13) (BAFO).docx	Table of Contents	Pages 2, 25, 27	The table of contents for Schedule K indicates that "D-11 Contract Management Plan" is on page 25 and "Contract Management Plan" is on page 27. No "Contract Management Plan" section appears on page 27 of Schedule K. Is this a typographical error in the Table of Contents or is text missing from Schedule K?	Schedule K has been revised.
15	6100022698 - Master Questions and Answers (09.03.13) (BAFO).docx Best and Final Offers Letter XXXXXXX RFP 6100022698 (09.03.13).pdf	"Revised answer (original answers posted as Addendum 9 - Round 1, Part 5)"	Page 196, item 42	The revised answer regarding Schedule I, "1. Volumetrics", states that "[i]nformation provided by the Offeror in Schedule I is intended for cost evaluation purposes only." However, the "List of Items to Address in BAFO" attached to the Issuing Officer's letter dated September 3, 2013 states that "[t]he 'Grand Total Base Term' will be used to determine the cost score." Please clarify whether the 'Grand Total Base Term' is the sole factor that will be used to determine the cost score or whether other information provided in Schedule I would be used to determine the cost score. If other information provided in Schedule I will be used to determine the cost score, please specify.	The "Grand Total Base Term" within Schedule I, "Tab 2. Total Charges" (cell C40)" will be used to determine the cost score.

16	6100022698 - Master Questions and Answers (09.03.13) (BAFO)	Question 27	199	The offeror Pricing Form has been revised to eliminate milestone Transition payments and the instruction is that Transition costs are now to be included in the unit rates. This seems inconsistent with the Commonwealth's lack of committed volumes. Depending on how the costs are spread across the unit rates and depending on the actual usage by the Commonwealth the offeror could either under-recover or over-recover its Transition costs. Since there are no committed volumes, how does the Commonwealth propose to fairly compensate the offeror for Transition costs?	The Commonwealth understands there is risk to all parties in this initiative. Termination for Convenience Fees were added to limit the Offeror's risk. Transition costs must be included in the service rates over the course of the base contract (7 years).
17	6100022698 - Appendix A - Contract Terms and Conditions (09.03.13) (BAFO)	Section 32.A.1	42	Based on the requirements specified in the RFP, the Commonwealth is asking for significant investments in Transition, datacenter improvements, software licenses, and equipment in its facilities. It is customary for a government customer to allow its vendor to recover unamortized start-up costs in the event of a termination for convenience. The payment formula established under the revised termination for convenience provision seems arbitrary and not related to the size of the offeror's required investment. With very limited payments for termination for convenience, no Transition payments, no committed volumes, and no commitment to purchase the provided assets how does the Commonwealth envision ensuring the offeror is compensated for making the multi-million dollar investments necessary to fulfill the Commonwealth's requirements?	The Commonwealth understands there is risk to all parties in this initiative. Termination for Convenience Fees were added to limit the Offeror's risk. Transition costs must be included in the service rates over the course of the base contract (7 years).

18	6100022698 - Schedule D - Transition Milestones (09.03.13) (BAFO)	M-12, M-13	9-11	We understand that the transition for DPH is now split into two transitions – DPH (1) and DPH (2). Please explain the reason for this split.	The DPH transition is one single transition. Milestones M-12 and M-13 identified in the version of Schedule D provided with the BAFO request are identical to Milestones M-14(A) and M-14(B) identified in the version of Schedule D published prior to the BAFO requests. Milestone M-12 applies to the period of time 18 months after contract execution but prior to 24 months after contract execution. Milestone M-13 applies to the period of time on or after 24 months after contract execution. M-13 only applies if the DPH transition exceeds 24 months after contract execution.
19	6100022698 - Schedule D - Transition Milestones (09.03.13) (BAFO)	M-12	9-10	Define the scope of DPH (1) transition.	The DPH transition is one single transition. Milestones M-12 and M-13 identified in the version of Schedule D provided with the BAFO request are identical to Milestones M-14(A) and M-14(B) identified in the version of Schedule D published prior to the BAFO requests. Milestone M-12 applies to the period of time 18 months after contract execution but prior to 24 months after contract execution. Milestone M-13 applies to the period of time on or after 24 months after contract execution. M-13 only applies if the DPH transition exceeds 24 months after contract execution.
20	6100022698 - Schedule D - Transition Milestones (09.03.13) (BAFO)	M-13	10-11	Define the scope of DPH (2) transition.	The DPH transition is one single transition. Milestones M-12 and M-13 identified in the version of Schedule D provided with the BAFO request are identical to Milestones M-14(A) and M-14(B) identified in the version of Schedule D published prior to the BAFO requests. Milestone M-12 applies to the period of time 18 months after contract execution but prior to 24 months after contract execution. Milestone M-13 applies to the period of time on or after 24 months after contract execution. M-13 only applies if the DPH transition exceeds 24 months after contract execution.